DISEÑO DE UN SGSI BASADO EN LA NORMA ISO 27001 PARA LA EMPRESA MA PEÑALOSA CÍA. S.A.S. SEDE PRINCIPAL CÚCUTA

JOHANNA CAROLINA ARARAT MUÑOZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN DE SEGURIDAD INFORMÁTICA
SAN JOSÉ DE CÚCUTA, NORTE DE SANTANDER
2018

DISEÑO DE UN SGSI BASADO EN LA NORMA ISO 27001 PARA LA EMPRESA MA PEÑALOSA CÍA. S.A.S. SEDE PRINCIPAL CÚCUTA

JOHANNA CAROLINA ARARAT MUÑOZ
27604094

Trabajo de grado para optar al título de Especialista en Seguridad Informática

Director de Proyecto:
Ing. JULIO ALBERTO VARGAS FERNÁNDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN DE SEGURIDAD INFORMÁTICA
SAN JOSÉ DE CÚCUTA, NORTE DE SANTANDER
2018

Nota de aceptación

_____

_____

_____

_____
Firma presidente de jurado

_____
Firma de jurado

_____
Firma de jurado

San José de Cúcuta, 30 de junio 2018

DEDICATORIA

La Vida está llena de retos y de experiencias que nos hacen más fuertes y nos ayudan a creer en nosotros mismos para poder afrontar las situaciones y alcanzar con éxito las metas que nos proponemos. No hay excusas para no cumplir nuestros sueños, porque si los proyectamos lo obtendremos. Realizar esta especialización ha sido uno de mis grandes orgullos como profesional y como persona, ya que quise ser un ejemplo para mis hijos demostrándoles el esfuerzo, dedicación y constancia para poder avanzar en esta etapa de mi vida.

Este gran esfuerzo lo dedico primero que todo a Dios por servirme de guía y llenarme de sabiduría para emprender cada uno de los retos que consigo traía la trayectoria académica. A mí querido esposo que me ha apoyado incondicionalmente y ha sabido comprenderme durante estas largas jornadas de estudio en el que sacrifique tiempo familiar para cumplir mi meta. A mis hijos por ser la fuente motivadora para superarme cada día más y ofrecerles un futuro mejor. A mis padres por su amor y valores inculcados durante mi formación para convertirme en lo que soy hoy. A mi hermano por su apoyo moral y estar ahí en los momentos más importantes de mi vida. A mis demás familiares, compañeros y amigos por animarme en cada paso.

AGRADECIMIENTOS

En primer lugar, agradezco a Dios por sus bendiciones y su protección. También agradecida con aquellas personas me han brindado apoyo moral para la realización de este proyecto.

A la empresa MA PEÑALOSA CÍA S.A.S, directivos y empleados por abrirme las puertas de sus instalaciones y tener la disposición y el tiempo brindado para el proceso de recolección de información y documentación como apoyo para el desarrollo del proyecto.

Al ingeniero Manuel Antonio Sierra y a la ingeniera Helena Clara Isabel Alemán tutores durante el anteproyecto por orientarme con sus contribuciones en los lineamientos y tiempo dedicado a versiones preliminares, al Ingeniero Juan José Cruz por sus retroalimentaciones y colaboración para avances del proyecto.

A mi Director de proyecto en la UNAD, el ingeniero Julio Alberto Vargas Fernández, por su acompañamiento durante el desarrollo del proyecto, su empeño y apoyo para llevar a cabo este logro.

A mis compañeros de cursos por sus aportes, trabajo en equipo los cuales ayudaron a complementar mis conocimientos.

A la Universidad Nacional Abierta y a Distancia y a la Facultad de Tecnología e Ingeniería por ofrecer este tipo de modalidad de estudio, por el acompañamiento y por el apoyo que me ha permitido escalar un nivel más en mi carrera profesional.

A mi familia, amigos y compañeros que confiaron en mis capacidades y se sienten orgullosos de verme cumplir esta meta.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

RESUMEN

El presente proyecto pretende contribuir al mejoramiento de la seguridad de los activos informáticos de MA PEÑALOSA CÍA. S.A.S. en la sede Principal de Cúcuta, manteniendo controlados los riesgos a los que pueden estar expuestos ellos, ya sean por diversos factores humanos intencionales o no intencionales, averías de origen físico o lógico, ambientales o de origen industrial que pueden ocasionar desastres, accidentes o contaminación. Algunas de las causas de estas amenazas se originan por el desconocimiento y la falta de concientización de los usuarios para dar un adecuado manejo a los mismos activos; también por la falta de controles y procedimientos que apoyen los procesos. Se planteará una propuesta de Sistema de Gestión de Seguridad de la información a MA PEÑALOSA CÍA. S.A.S. que establezca políticas y lineamientos para proteger los activos informáticos y permita mitigar los riesgos y vulnerabilidades que puedan afectar la operatividad del negocio.

Palabras claves: SGSI, Vulnerabilidad, Riesgo, Amenaza, Seguridad, Activo, PHVA, Norma ISO, Políticas de seguridad, Controles de seguridad.

ABSTRACT

The present project intends to contribute to the improvement of the security of the computer assets of MA PEÑALOSA CÍA. S.A.S. in the main headquarters of Cúcuta, keeping the risks to which, they may be exposed, whether due to various intentional or unintentional human factors, damage of physical or logical origin, environmental or industrial origin that can cause disasters, accidents or contamination. Some of the causes of these threats originate from the ignorance and lack of awareness of the users to give an adequate management to the same assets; also because of the lack of controls and procedures that support the processes. A proposal of the Information Security Management System will be proposed to MA PEÑALOSA CÍA. S.A.S. that establish policies and guidelines to protect computer assets and mitigate risks and vulnerabilities that may affect the operation of the business.

Keywords: ISMS, Vulnerability, Risk, Threat, Security, Active, PHVA, ISO Standard, Security policies, Security controls.

INTRODUCCION

Muchas empresas se enfocan más en su actividad comercial y en su productividad, dejando a un lado aspectos tan importantes como los de establecer y fortalecer los controles sobre la seguridad de la información y sus datos para prevenir y detectar fraudes en la compañía. Se confían al no creer ser víctimas de ataques y no se preparan para enfrentar si llegara a suceder.

La seguridad de la información no solo es responsabilidad del departamento de tecnología, sino toda la empresa, por eso es importante concientizar a todo el personal sobre las amenazas y las consecuencias que estas generan.

He aquí el grado de importancia de seguir un modelo de seguridad que garantice el manejo adecuado de la información y aseguren los activos vitales a través de normatividades o políticas que regulen las actividades diarias de la empresa. Las cuales deben ser conocidas por todos los empleados a través de capacitaciones, para que se comprometan a hacer buen uso de la información y de los recursos, y finalmente entre todos mantener los principios como la integridad, autenticidad y confidencialidad de la información.

Con la aplicación de este proyecto, se pretende ofrecer a la sede principal MA PEÑALOSA CÍA. S.A.S. una propuesta de un Sistema de Gestión de Seguridad de la información que permitan implementar lineamientos que conlleven a asegurar la información y los demás activos informáticos, utilizando como marco de referencia de la norma ISO 27001, la cual emplea las mejores prácticas para cumplir los objetivos del proyecto.

1. TÍTULO

Diseño de un SGSI basado en la Norma ISO 27001 para la Empresa MA PEÑALOSA CÍA. S.A.S. Sede Principal Cúcuta

2. DEFINICIÓN DEL PROBLEMA

2.1 ANTECEDENTES DEL PROBLEMA

En la actualidad, las empresas y sus sistemas de información se enfrentan diariamente a factores internos y externos que amenazan la integridad, disponibilidad y autenticidad de su información. Siendo la información un activo fundamental para cualquier empresa, debe estar protegida bajo normas, controles y políticas de seguridad que garanticen la continuidad del negocio.

Con más frecuencia se han presentado incidentes a nivel mundial con respecto a ataque informáticos o fraudes, por eso es recomendable brindarle más importancia a la seguridad y si es necesario invertir para llevar una buena gestión, desarrollando las mejores prácticas para la prevención, detección y protección de los datos e información de la empresa.

Aunque no se pueda alcanzar una seguridad total, ya que factores incontrolables como los siniestros ambientales o atentados criminales pueden llegar a presentarse, al tener un excelente sistema de gestión de seguridad de la información, se contarían con planes de contingencia para lograr el restablecimiento eficaz de los daños tanto físicos como lógicos causados.

2.2 FORMULACIÓN

¿En qué medida mejoraría la seguridad informática de MA PEÑALOSA CÍA. S.A.S. con el diseño del SGSI basado en la norma ISO 27001?

2.3 DESCRIPCIÓN

Para MA PEÑALOSA CÍA. S.A.S, la información es de vital importancia incluso para su funcionamiento, por lo que asegurar su protección ante cualquier riesgo es una de las prioridades de la empresa.

Está información está archivada digitalmente en los servidores físicos y otra parte se encuentra en el archivo físico dentro de las instalaciones. En sus bases de datos, se maneja diferente tipo de información relacionada con la actividad diaria que realizan, contiene datos de empleados, proveedores, ventas e información de clientes. En el caso de los clientes es un activo crítico, debido a que la empresa se dedica a la venta y distribución de materiales de construcción y al estar expuesta esta información junto con datos de precios de inventarios a la competencia, afectaría considerablemente la rentabilidad de la empresa.

Para el desarrollo de las actividades diarias de los usuarios de MA PEÑALOSA CÍA. S.A.S, en el ERP SAP BUSINESS ONE, utilizan una arquitectura cliente/servidor, creando la necesidad de estar en red y compartir los recursos informáticos dentro de la empresa, pero la ausencia de un directorio activo o del establecimiento de niveles de seguridad dentro de la red hace aún más vulnerable la información, ya que dentro de ella cualquier empleado tendría a su alcance la información si lo quisiera. Además, la rotación constante de personal produce efectos negativos para la empresa porque la información es manipulada por muchos empleados que pasan por un mismo cargo.

En cuanto al establecimiento donde funciona la Sede Principal de MA PEÑALOSA CÍA. S.A.S. tiene parte de la infraestructura muy antigua, la cual durante estos últimos años ha presentado fallas estructurales y filtraciones, que han comprometido algunos equipos de usuarios. Tampoco existe un cuarto de comunicaciones para ubicar los equipos de comunicaciones y los servidores, quedando expuestos tanto a accesos no autorizados como a condiciones ambientales poco favorables para conservación y buen funcionamiento de los equipos.

Teniendo en cuenta los aspectos mencionados anteriormente, se puede detectar que la seguridad informática establecida en la empresa hasta el momento es limitada e insuficiente, el cual es un error que se encuentra en muchas de las empresas porque se concentran en su actividad comercial y productiva, dejando a un lado aspectos importantes como el de determinar medidas de seguridad que ayuden a prevenir y detectar fraudes informáticos y a salvaguardar los activos de la empresa como hardware, software, redes, comunicaciones, recurso humano e infraestructura física; en el desarrollo de este proyecto, inicialmente se evaluará la situación actual de la seguridad de la información y finalmente se presentará un propuesta que le sirva de apoyo a MA PEÑALOSA CÍA. S.A.S. para implementar un Sistema de Gestión de Seguridad de la Información basada en la Norma ISO 27001, donde se evalúen las amenazas y riesgos a los que está expuesta la empresa y que puedan llegar a afectar la seguridad de la información, con el fin de establecer controles y recomendaciones con los que se puedan minimizar cada una de las amenazas y vulnerabilidades del sistema de información.

3. JUSTIFICACIÓN

La información es poder, es vital para el éxito y sobrevivencia de las empresas en cualquier mercado; es uno de los activos más valiosos que hoy en día posee las empresas y se evidencia a nivel mundial que cada vez más sufre grandes amenazas en cuanto a su confiabilidad y su resguardo. Esto nos indica que uno de los principales objetivos de toda organización es el aseguramiento y la protección de dicha información, así como también de los sistemas que la procesan.

Actualmente MA PEÑALOSA CÍA. S.A.S. Sede Principal – Cúcuta no cuenta con algún Sistema de seguridad confiable que resguarde ésta información, no se manejan políticas de seguridad para hacer frente a diferentes vulnerabilidades externas e internas viéndose expuesta a una difícil recuperación de posibles ataques y daños a nivel directo y colateral, se hace necesario utilizar un mecanismo de protección robusto contra estas posibles amenazas que puedan poner en riesgo todo tipo de seguridad de la información, logrando así fortalecerla de eventuales contratiempos informáticos.

En MA PEÑALOSA CÍA. S.A.S. Sede Principal se requiere que los sistemas de información garanticen un servicio óptimo y se brinde a todos sus usuarios la disponibilidad, integridad y confiabilidad de sus datos. Por eso es necesario que con un SGSI se controle y asegure estos pilares contribuyendo a la fidelidad de sus clientes convirtiendo a MA PEÑALOSA CÍA. S.A.S. en una empresa más competitiva y posicionada en el mercado beneficiando así a todo su personal, proveedores y garantizando un mejor servicio al cliente.

Se debe manejar un SGSI basado en la Norma ISO 27001, quien a través de su estructura de aseguramiento sistemático dispone de procedimientos confiables y avalados internacionalmente para cumplir con los objetivos planteados y justificables.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Entregar un diseño de implementación de un SGSI basado en la Norma ISO 27001 para la Empresa MA PEÑALOSA CÍA. S.A.S. Sede Principal CÚCUTA.

4.2 OBJETIVOS ESPECÍFICOS

- Realizar el levantamiento de la información para hacer un diagnóstico y determinar las condiciones actuales de la Seguridad de la información de MA PEÑALOSA CÍA. S.A.S. de acuerdo al marco de trabajo de la Norma ISO 27001.

- Aplicar la metodología Magerit para la creación del inventario de activos informáticos, realización del análisis de riesgo, amenazas a las que están expuestos los activos informáticos de MA PEÑALOSA CÍA. S.A.S.

- Establecer controles necesarios para mejorar y garantizar la confidencialidad, integridad y disponibilidad de los activos informáticos de MA PEÑALOSA CÍA. S.A.S.

- Plantear lineamientos que permitan mitigar los riesgos significativos y de alto impacto en los activos informáticos de la empresa, garantizando la continuidad de los procesos y/o operaciones de la misma.

- Diseñar y elaborar una propuesta de SGSI para la Empresa MA PEÑALOSA CÍA. S.A.S. basados en la Norma ISO 27001.

5. MARCO REFERENCIAL

5.1 ANTECEDENTES

Con el objeto de contar con una guía para proporcionar un sistema de seguridad de la información robusta se toma a consideración el estándar de seguridad de la información ISO 27001 para crear las políticas y los estándares en seguridad de las bases de datos, siendo esta la norma principal en el manejo de todos los procesos de seguridad. Este estándar está diseñado para generar una serie de recomendaciones en la utilización de mejores prácticas sobre la gestión de seguridad de la información, incluyendo los riesgos y controles en el marco de un Sistema de Gestión de la Información de Seguridad (SGSI).

A inicios de los años 90, se ve la necesidad de crear una guía integrada de normas para establecer un conjunto de criterios de evaluación de seguridad que fueran reconocidas internacionalmente, es cuando el Departamento de Comercio e Industria del Reino Unido (DTI) determina iniciar con el desarrollo de una estructura estándar para reglamentar y salvaguardar la información de las compañías.

En 2005 luego de diferentes versiones y publicaciones del alcance de la norma y los requisitos para un SGSI que fuera certificable, se crea el mecanismo de vía rápida ISO como ISO / IEC 27001:2005, donde se establece la norma internacional certificable, allí se hacen cambios significativos donde se resalta el diseño de los controles, la guía de implementación y muchos más términos ayudando a mantener un sistema eficaz de gestión de seguridad y aplicando un enfoque de mejora continua en cuanto a la administración de los sistemas de información.

En el 2007 se hace una rectificación técnica publicándose una nueva versión de la ISO/IEC: 2005 pasando a ser la ISO 27002:2005 para el código de las mejores prácticas.

Finalmente, para finales del 2013 es revisada y se publican nuevas ediciones de la ISO/IEC 27001 y 27002, donde por el cambiante mundo de la tecnología se hace necesario adicionar reformas para que esta sea más compatible con otras normas de sistemas de seguridad de información, reconociéndose como el mejor estándar de prácticas para demostrar las credenciales de la seguridad de la información.

Dentro de los trabajos relacionados con el tema propuesto para este proyecto. Se encontraron diversos proyectos a nivel nacional, regional y local. A continuación, se mencionan algunos:

Diseño de un Sistema de Gestión de Seguridad de la Información para una Entidad Financiera de Segundo Piso. Trabajo de grado de Carlos Alberto Guzmán Silva del año 2.015 en Bogotá, Colombia. El diseño del sistema se dió, debido a que control

interno realizó una auditoria de la Entidad Financiera para evaluar el estado de seguridad del área de tecnología, a través de pruebas de penetración encontrando que el nivel de exposición era alto y recomendó implementar medidas y controles para crear un modelo de seguridad que ayude a mitigar las vulnerabilidades, basados en el ciclo de mejora continua conocido como ciclo PHVA contemplado en la norma ISO 27001:2013.[1]

Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo. Tesis de grado de Hans Ryan Espinoza Aguinaga del año 2.013 de Lima, Perú. Para el desarrollo del Sistema de Gestión de Seguridad de la Información del proyecto se basó en la norma ISO/IEC 27001:2005 y la ISO 27002 para establecer controles, utilizando además la metodología del ciclo Deming (PHVA) y para el análisis de riesgo la metodología Magerit II.[2]

Diseño del Sistema de Gestión de Seguridad de la Información para el Grupo Empresarial La Ofrenda. Proyecto de grado de Juan David Aguirre Cardona y Catalina Aristizábal Betancourt del año 2.013 de Pereira, Colombia. El proyecto se hace necesario para el Grupo empresarial La Ofrenda S.A., ya que no existe un Sistema de Gestión de Seguridad de la información y este será desarrollado en la Sede Principal de Pereira para mejorar los niveles de seguridad y lograr la certificación en calidad y seguridad de la información, apoyados en la ISO 27001.[3]

Análisis y diseño de un Sistema de Gestión de Seguridad Informática en la empresa Aseguradora Suárez Padilla & Cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. Trabajo de grado de Sandra Yomay Suarez Padilla del año 2015 de Bogotá, Colombia. El proyecto plantea bases para implementar un SGSI, apoyado

[1] GUZMÁN SILVA, Carlos Alberto. Diseño de un Sistema de Gestión de Seguridad de La Información para una Entidad Financiera de Segundo Piso (2015). [En línea], [consultado el 2 de febrero de 2018]. Disponible en Internet: http://repository.poligran.edu.co/bitstream/ 10823/ 746/1/Proyecto%20de%20Grado%20SGSI%20-%20IGM-%20CarlosGuzman%20(FINAL).pdf

[2] ESPINOZA AGUINAGA, Hans Ryan. Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo (2013). [En línea], [consultado el 2 de febrero de 2018]. Disponible en Internet: http://tesis.pucp.edu.pe/repositorio//bitstream/ 123456 789/4957/1/ESPINOZA_HANS_ANALISIS_SISTEMA_GESTION_SEGURIDAD_INFORMACION_ISO_IEC+27001_2005_COMERCIALIZACION_PRODUCTOS_CONSUMO_MASIVO.pdf

[3] AGUIRRE CARDONA, Juan David y ARISTIZABAL BETANCOURT, Catalina. Diseño del Sistema de Gestión de Seguridad de la Información para el Grupo Empresarial La Ofrenda (2013). [En línea], [consultado el 2 de febrero de 2018]. Disponible en Internet: http://repositorio.utp.edu.co/dspace/ bitstream/handle/11059/4117/0058A284.pdf?sequence=1

en el modelo de estándares y normas internacionales ISO/IEC 27001:2016 y el estándar ISO/IEC 27002, abarcando las fases del modelo PHVA del ciclo Deming.[4]

5.2 MARCO TEÓRICO

5.2.1 Seguridad Informática. La seguridad de la información hace referencia a todas a aquellas acciones necesarias para la protección de los datos sensibles y relevantes para los propietarios de los mismos procesos, que requiere que se engloben y accionen un conjunto de medidas organizacionales, técnicas y legales que den lugar al aseguramiento la confidencialidad, la integridad y la disponibilidad de los datos almacenados en sistema, sin importar su origen o tipo de almacenamiento, puede estar en medio físico o digital.

5.2.2 Sistema de Gestión de Seguridad. Un Sistema de Gestión de Seguridad de la Información (SGSI) debe contar con un modelo que tenga en cuenta aspectos tecnológicos, organizativos, cumplimiento de marco legal y la importancia del factor humano. (Wikipedia, 2016).

Figura 1. Sistema de Gestión de Seguridad de la Información

Fuente: (Wikipedia, 2016)

[4] SUAREZ PADILLA, Sandra Yomay. Análisis y diseño de un Sistema de Gestión de Seguridad Informática en la empresa Aseguradora Suárez Padilla & Cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. 2015. Recuperado de: http://repository.unad.edu.co/bitstream/10596/3777/1/20904541.pdf

5.2.3 ISO 27001. Esta norma da lugar a la especificación de requisitos para la documentación y evaluación de los Sistemas de Gestión de la Seguridad de la Información (SGSI), es así como se definen las actividades que se muestran a continuación necesarias para el procedimiento de implementación de la norma ISO27001[5]:

- Definición alcance del SGSI
- Definición de una Política de Seguridad
- Definición de una metodología y criterios para el Análisis y Gestión del Riesgo
- Identificación de riesgos
- Evaluación de los posibles tratamientos del riesgo
- Elaboración de una Declaración de Aplicabilidad de controles y requisitos
- Desarrollo de un Plan de Tratamiento de Riesgos
- Definición de métricas e indicadores de la eficiencia de los controles
- Desarrollo de programas de formación y concienciación en seguridad de la información
- Gestión de recursos y operaciones
- Gestión de incidencias
- Elaboración de procedimientos y documentación asociada.

5.2.4 Ciclo PHVA. Actualmente el alto nivel de exigencia competitiva hacen que las empresas evolucionen y estén en mejora continua, para esto se hace necesario contar con herramientas de mejora en la organización, el ciclo PHVA es un método de gestión de mejora continua ideal para las organizaciones que están en pro del desarrollo y evolución hacia el éxito, está supervisado bajo la norma ISO y cuenta con total aprobación nacional e internacional ya que esto genera reducción de costos, incrementa la rentabilidad financiera y optimiza todas las áreas de productividad dentro de la organización.

El ciclo PHVA (Planear, Hacer, Verificar y Actuar) corresponde a fases del método de gestión de mejora continua donde:

- Planificar, corresponde a la etapa de generación de objetivos, de identificación de los procesos, los cuales dentro del marco de las políticas de la empresa van a determinar los resultados a lograr, tomando también controles de medición para seguir con el proceso.

- Hacer, Aquí se implementan los cambios planteados para la mejora que se generaron en la planificación.

[5] GESCONSULTOR. ISO 27001 – Sistema de Gestión de la Seguridad de la Información. [En línea], [consultado el 2 de mayo de 2018]. Disponible en Internet: http://www. http:/www-gesconsultor.com/iso-27001.html

Figura 2. Ciclo PHVA

Fuente: (3 BP Blogspot - Blogger, 2017)

- Verificar, en esta fase se ajusta la regulación mediante períodos de tiempo para verificar y medir que se esté llevando a cabo la efectividad de los cambios.

- Actuar, ya realizadas las mediciones y la verificación si se determina que los resultados no son los esperados, se entra a desarrollar correcciones y modificaciones que sean necesarias, tomando acciones de mejora continua en el desarrollo de los procesos.

5.3 ESTADO DEL ARTE

Se presentarán estudios previos documentados sobre sistemas de gestión de seguridad Informática realizados a diferentes entidades, la cual se tomaron como referencia basados en sus experiencias y fases de implementación actuales.

Proyección Financiera y Tecnológica requerida para la Implementación del Sistema de Gestión de la Seguridad de la Información (SGSI), bajo la Norma ISO/IEC 27001:2013 en la Empresa INDAIRE Ingeniería S.A.S.[6] Trabajo de grado

[6] ZAQUE GONZÁLEZ, Oscar Javier. Proyección Financiera y Tecnológica requerida para la Implementación del Sistema de Gestión de la Seguridad de la Información (SGSI), Bajo La Norma ISO/IEC 27001:2013 En La Empresa INDAIRE Ingeniería S.A.S. (2016). [En línea], [consultado el 2 de mayo de 2018]. Disponible en Internet: http://repository.unad.edu.co/handle/10596/8595

presentado por Oscar Javier Zaque González a la Universidad Nacional Abierta y a Distancia en el año 2016. Es un proyecto que proporciona las bases de un SGSI para que la empresa responda de la manera más eficiente y minimice los riesgos que se presenten ante las amenazas, el enfoque utilizado es basado en procesos para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el Modelo de Seguridad de la Información y estar orientado a todos los actores y entidades involucradas que permite mantener un proceso de mejora continua brindando una seguridad razonable para la proyección financiera y tecnológica. La proyección incluye todos los aspectos económicos, financieros y tecnológicos requeridos para la implementación de los controles de seguridad planteados en la normativa ISO/IEC 27001:2013, de manera que garantice la operatividad del sistema y el sostenimiento del mismo, bajo el enfoque de mejora continua.

Modelo para la implementación del Sistema General de Seguridad Informática y protocolos de Seguridad Informática en la Oficina TIC de la Alcaldía Municipal de Fusagasugá, basados en la Gestión del Riesgo Informático. Trabajo de grado presentado por Ana Milena Pulido y Jenith Marsella Mantilla en el año 2016. Se trata de una propuesta realizada para generar un modelo de implementación en un SGSI y así fortalecer la infraestructura de tecnologías de la información de la entidad pública, garantizando la sostenibilidad y preservando los pilares fundamentales de la seguridad, como lo son la confiabilidad, integridad y disponibilidad. Este modelo permite reunir la sostenibilidad del conjunto de políticas, estándares y normas para la supervisión y mejora de los procesos.[7]

Análisis para la Implementación de un Sistema de Gestión de la Seguridad de la Información según la Norma ISO 27001 en la Empresa SERVIDOC S.A. Trabajo de grado presentado por Luis Giraldo Cepeda en el año 2016. En esta propuesta se determina la garantía que se cumplan las premisas de la seguridad informática dentro los pilares fundamentales de la seguridad, para la empresa prestadora de servicios de salud. Realiza el análisis para la implementación del SGSI basado en la norma ISO-27001.[8]

Aplicación de un Sistema de Gestión de Seguridad de la Información (SGSI) en el Circuito Cerrado de Televisión (CCTV) Sistema Integrado de Emergencias y Seguridad (SIES) del Municipio de Yacuanquer. Trabajo de grado presentado por

[7] PULIDO, Ana Milena y MARSELLA MANTILLA, Jenith. Modelo para la Implementación del Sistema General de Seguridad Informática y Protocolos de Seguridad Informática en la Oficina TIC de la Alcaldía Municipal de Fusagasugá, basados en la Gestión del Riesgo Informático. (2016). [En línea], [consultado el 2 de mayo de 2018]. Disponible en Internet: http://Repository. Unad.edu.co/handle/10596/6327.

[8] GIRALDO CEPEDA, Luis Enrique. Análisis para la Implementación de un Sistema de Gestión de la Seguridad de la Información Según La Norma ISO 27001 En La Empresa SERVIDOC S.A. (2016). [En línea], [consultado el 2 de mayo de 2018]. Disponible en Internet: http://Repository.Unad.edu.co/handle/10596/6341.

José Hernán Cortes Rosero a la Universidad Nacional Abierta y a Distancia en el año 2016. Trabajo desarrollado para aplicar métodos que permitan proteger el activo más importante la "información" a través de la norma ISO 27000:2013 disminuyendo así los riesgos que se puedan producir ante amenazas directa a los circuitos cerrados de la estación de policía, con ello se recomiendan y se establecen la planificación e implementación de controles basados en un análisis de riesgo. En este caso de uso solo se manejó el estudio y la planificación para la implementación.[9]

5.4 MARCO CONCEPTUAL

Seguridad de la Información: Agrupación de medidas preventivas y correctivas para resguardar y proteger los activos informáticos incluido el activo de la información considerado como el más valioso en una organización a través de los pilares de la información.

Activo: Comprende los recursos documentales, humanos, tecnológicos y físicos para que funcione la empresa a diario, tales como: hardware, software, manuales, procedimientos, normas, personal TI, redes, instalaciones, servicios ofrecidos e Información. Conjunto de datos de forma estructurada y lógica para la comunicación.

Confidencialidad: Privacidad con la que se debe preservar la información almacenada y procesada en un sistema informático, es decir que las herramientas de seguridad empleadas deben proteger al sistema de accesos que no hayan sido autorizados.

Integridad: Se refiere a la importancia y estabilidad de la información almacenada y procesada en el sistema informático. En este principio las herramientas de seguridad deben garantizar que en los procesos de actualización no haya duplicaciones, pero si estén bien sincronizados para que así los elementos del sistema manejen los mismos datos.

Autenticidad: Este principio está basado en la continuidad de acceso a la información almacenada y procesada en un sistema informático. En este principio las herramientas de seguridad deben fortalecer la permanencia del sistema informático para que los usuarios accedan a la información con el tiempo y permanencia que requieran.

[9] CORTES ROSERO, José Hernán. Aplicación de un Sistema de Gestión de Seguridad de la Información (SGSI) en el Circuito Cerrado de Televisión (CCTV) Sistema Integrado de Emergencias y Seguridad (SIES) del Municipio de Yacuanquer. (2016). [En línea], [consultado el 2 de mayo de 2018]. Disponible en Internet: Http://Repository.Unad.edu.co/Handle/10596/6175.

ISO 27001: Norma Internacional emitida por la Organización Internacional de Normalización (ISO) donde describe cómo gestionar la seguridad de información de una empresa[10].

Amenaza: Sucesos que se presentan y causan efectos negativos sobre los recursos anteriormente mencionados y conllevan a la inestabilidad del negocio porque afectan características como la integridad, disponibilidad, autenticidad de la información y de los datos vitales de la empresa.

Vulnerabilidades: Es el conjunto de debilidades que establecen que tan susceptible puede ser la empresa a la hora de recibir una amenaza informática o circunstancial.

Impacto: Nivel de degradación o afectación que pueda ocasionar sobre un activo cuando se presenta una amenaza.

Riesgo: Es la probabilidad de que la amenaza que se pueda presentar en la empresa se convierta en un desastre. Entre más alta sea la vulnerabilidad mayor será el riesgo.

Control: Medidas de protección que se establecen dentro de una empresa para minimizar o eliminar riesgos.

5.5 MARCO CONTEXTUAL

5.5.1 Presentación De La Empresa – MA PEÑALOSA CÍA. S.A.S. Es una empresa cucuteña privada de tipo S.A.S (Sociedad por Acciones Simplificadas) conformada hace más de 70 años. Su actividad económica es la distribución de materiales de construcción para todas las necesidades, de productos de excelente calidad y las marcas más reconocidas en el mercado. Su proveedor Principal es CORONA, pero también están Sika, Eternit, Abracol, Cemex, Firplack, Pavco, entre otros.

Cuentan con más de 7.000 metros cuadrados en bodegas de despachos y logística, 4 puntos de atención y venta, una flota de 15 camiones y camionetas y 14 motos de domicilios.

Todo esto con el sistema más moderno de información SAP BUSINESS ONE, para lograr una respuesta oportuna y real para nuestros clientes.

[10] ADVISERA.COM. ¿Qué es norma ISO 27001?. [En línea], [consultado el 2 de mayo de 2018]. Disponible en Internet: https://advisera.com/27001academy/es/que-es-iso-27001/

La sede principal se encuentra ubicada en el centro de la ciudad de Cúcuta, dos sedes más en la ciudad: una en la Zona Industrial y Atalaya; y otra fuera de la ciudad en Pamplona.

MA PEÑALOSA CÍA. S.A.S. posee dos franquicias con Construrama una red de cadenas de materiales de construcción más grande de Latinoamérica. Las cuales funcionan en las mismas sedes de Atalaya y Pamplona.

Figura 3. Sede Principal de MA PEÑALOSA CÍA. S.A.S.

Fuente: Autor

5.5.2 Razón de ser. M.A. PEÑALOSA CÍA. S.A.S. será reconocida en primer lugar por su actitud ética, tradición de seriedad, tratamiento digno y respetuoso a sus servidores, un alto sentido de responsabilidad para sus clientes y en general hacia la sociedad. Esta premisa primara sobre cualquier otra consideración económica.

Las actuaciones comerciales estarán siempre dentro del marco de la buena fe, la equidad, la transparencia y la ley. Fundamentando su desarrollo sobre valores éticos y morales. Con disposición de brindar siempre seguridad y respaldo a sus clientes, seguridad social a sus colaboradores y progreso a la comunidad.

Los accionistas de M.A. PEÑALOSA CÍA. S.A.S., ofrecen a esta empresa Intangibles valores como son su buen nombre, más de medio siglo de experiencia comercial, además de su capital. Esperando de sus colaboradores, los mejores esfuerzos para la consolidación de una empresa sólida en sus principios y la retribución de esta a la legítima aspiración de un valor agregado a su inversión.

5.5.3 Misión. Atender a cada cliente como a mi familia, ofreciéndole la mejor opción en productos y servicios para la construcción.

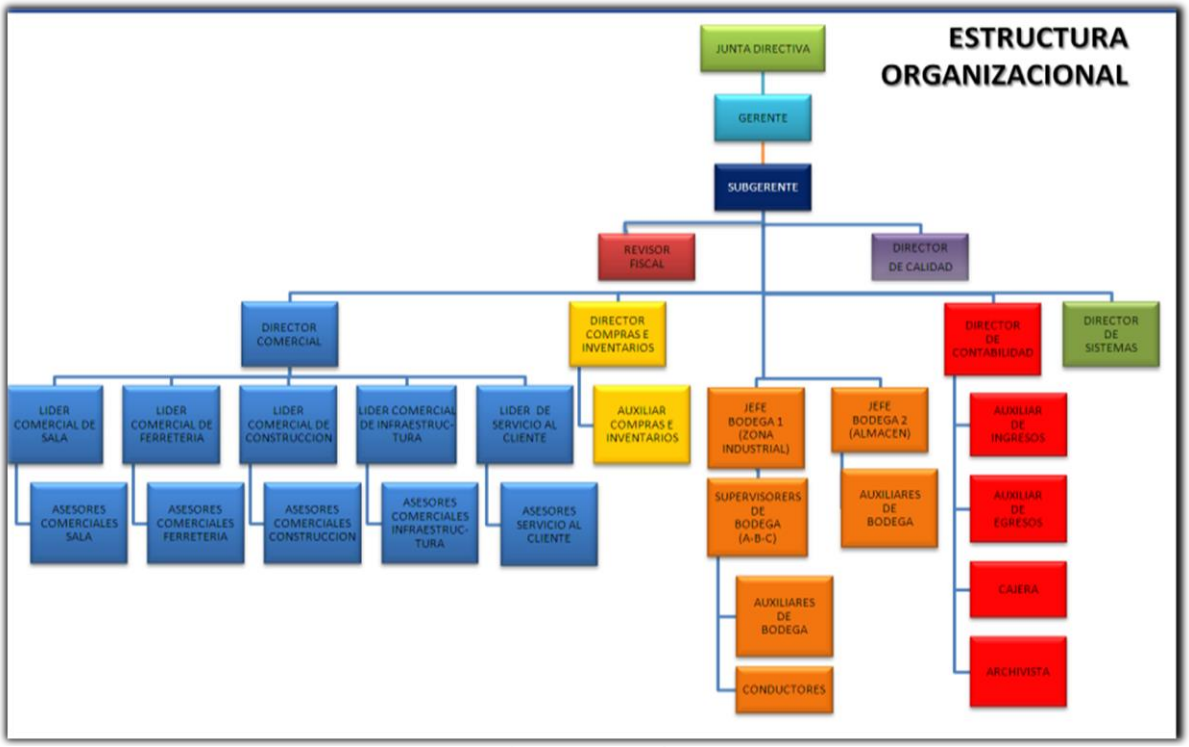
5.5.4 Visión. Ser en el 2023 la primera opción en la comercialización de productos y servicios para la construcción a nivel nacional, con proyección internacional.

5.5.5 Política de calidad. M.A. PEÑALOSA CÍA. S.A.S. tiene como política de calidad:

- Buscar el beneficio de la comunidad.
- Encaminar toda labor que se realice en la compañía a la satisfacción de los clientes.
- Ofrecer productos y servicios competitivos, y de excelente calidad.
- Tener relaciones mutuamente beneficiosas con nuestros colaboradores.
- Buscar la rentabilidad y efectividad de los procesos.

5.5.6 Organigrama

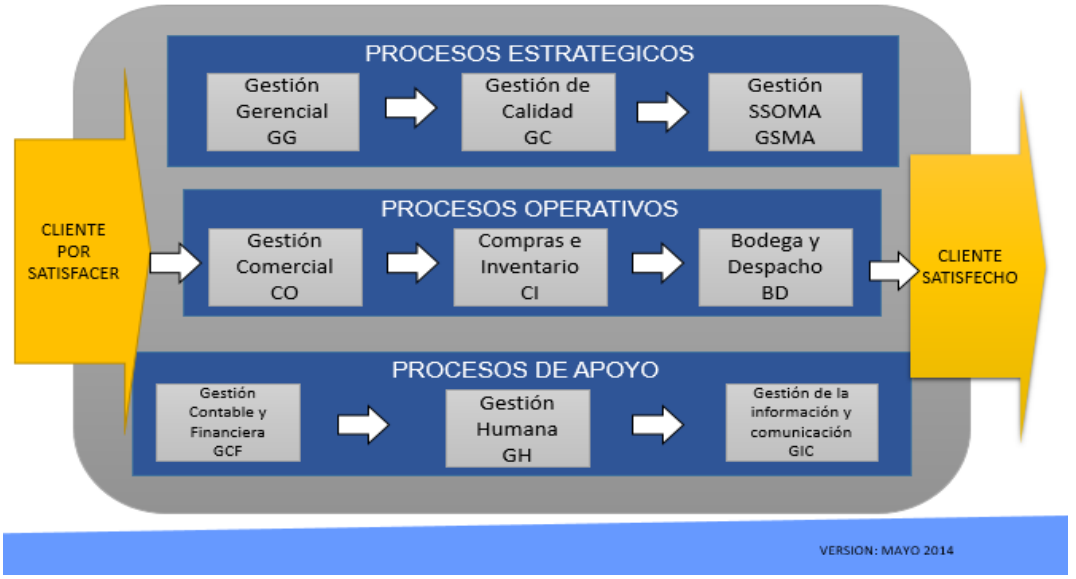
Figura 4. Organigrama de MA PEÑALOSA CÍA. S.A.S.



Fuente: Archivo de SGC de MA PEÑALOSA CÍA. S.A.S.

5.5.7 Macroprocesos

Figura 5. Macroprocesos



Fuente: Archivo de SGC de MA PEÑALOSA CÍA. S.A.S.

5.5.8 Estructura Organizacional. La empresa MA PEÑALOSA CÍA. S.A.S. está constituida por las siguientes áreas:

- Junta directiva. Integrada por el gerente, subgerente y dos socios más. Los cuales son los responsables de tomar las decisiones importantes dentro de la empresa.

- Área Comercial. Área dividida en varios segmentos integrada por:

– Director comercial: Líder encargado de analizar los indicadores de ventas, precios competitivos, rotación de inventario, promoción de productos y programación de eventos comerciales.

– Sala de ventas: ventas al detal, gestión de cartera, mantener actualizado los ambientes de sala.

– Servicio al cliente: Recepción de llamadas y ventas a clientes vía telefónica.

– Construcción: Visitas a clientes constructores, identificación de oportunidades de ventas a través de censo de obras, ventas y cotizaciones, gestión de cartera.

– Ferretería: Visita a clientes ferreteros, hacer recomendación de pedidos, mostrar el portafolio de productos e informar de las promociones de la semana al cliente y gestión de cartera.

– Infraestructura: Visita a obras de tipo infraestructura de Norte de Santander, consultar página para participar en licitaciones, ventas a Alcaldías, Empresas del Gobierno, gestión de cartera.

- Área de calidad. Área responsable de hacer cumplir los procedimientos planteados dentro de la empresa, gestión de recursos humanos y reporte de accidentalidad.

- Área de Proyectos. Personal encargado de impulsar los diferentes puntos ventas de MA PEÑALOSA CÍA. S.A.S. (Sedes) y proyectar e implementar otros puntos de ventas.

- Área de Compras e inventarios. Personal encargado de realizar pedidos de inventario y cargarlos al sistema, realizar traslados entre bodegas, actualizaciones de precios, hacer estudios de rotación del inventario, participa en el proceso de devoluciones de cliente.

- Área de Logística. Responsable de recibir mercancía por parte de proveedores, gestión de bodega y despachos a clientes, recepción de devoluciones de clientes, organizar rutas de entrega.

- Área de contabilidad. Área encargada de la parte financiera de la empresa como pago a proveedores, pago de nómina, gestión de ingresos y egresos, flujo de caja, pago de parafiscales, participa en el proceso de devolución de clientes, gestión de archivos.

- Área de sistemas. Persona encargada del ERP SAP Business One, administradora de las bases de datos, red de comunicaciones, supervisión de mantenimientos correctivos y preventivos de los equipos.

Siendo estas áreas pertenecientes a la Sede Principal al igual que sus activos informáticos como hardware, software, redes, comunicaciones, recursos humanos e infraestructura lo que se incluirán dentro del SGSI planteado. Principalmente los servidores donde reposan la información como bases de datos de clientes, proveedores, inventario, sistema de información.

5.5.9 Recursos Humanos. En la Sede Principal de MA PEÑALOSA CÍA. S.A.S. cuentan con 54 empleados, incluyendo Gerente y Subgerente. Distribuidos de la siguiente manera según área:

Tabla 1. Recursos Humanos

Área		Descripción	Cantidad
Junta Directiva	Gerente	Socio de la empresa	1
	Subgerente	Socio de la empresa	1
	Otros	Socios de la empresa	2
Comercial	Dirección Comercial	Director Comercial	1
	Sala de ventas	Líder de sala y 9 asesores comerciales	10
	Servicio al cliente	Líder de servicio al cliente y 5 asesoras comerciales.	6
	Construcción	Líder de construcción y 4 asesores comerciales.	4
	Ferretería	Líder de Ferretería y 7 asesores comerciales	8
	Infraestructura	2 asesores comerciales	2
Calidad	Director de Calidad	Director de Calidad	1
Proyectos	Director de Proyectos	Director de Proyectos	1
Compras e inventarios	Compras	Director de compras y auxiliar de compras	2
Logística	Bodega	Jefe de bodega y 6 auxiliares	7
Contabilidad		Director de contabilidad, Aux. de egresos, Aux. ingresos, cajera principal, cartera, Revisor fiscal y Archivista	7
Sistemas	Director de Sistemas	Director de Sistemas	1
TOTAL			54

Fuente: Autor

Se debe aclarar que no todos los cincuenta y cuatro empleados hacen uso del sistema y equipos.

5.5.10 Equipos por área de la Sede Principal. En las observaciones realizadas para el levantamiento de inventario de activos informáticos, se identificaron los siguientes equipos informáticos por área:

- Sala de ventas: 4 equipos de escritorio (todos utilizan el sistema, pero comparten usuario y equipos).
- Construcción: 5 equipos portátiles
- Infraestructura: 2 equipos portátiles
- Ferretería: 8 equipos (4 tabletas y 4 portátiles) formado por los cuales a ciertas horas se convierten en usuario remotos, ya que visitan las ferreterías con su equipo y un módem móvil de Internet
- Servicio al cliente: 6 equipos (5 de escritorio y 1 portátil)
- Compras: 2 equipos de escritorio
- Calidad: 1 equipo portátil
- Director Comercial: 1 equipo portátil
- Gerente y Subgerente: 1 portátil
- Sistemas: 1 portátil
- Proyectos:1 portátil
- Bodega: 1 equipo de escritorio
- Contabilidad: 3 portátiles y 4 equipos de escritorio

Se identificaron cinco impresoras activas, de las cuales dos están en calidad de alquiler. A continuación, se mencionan:

- 1 impresora de tóner en red (uso de área administrativa y comercial): Dispositivo en alquiler
- 1 impresora de POS (uso de caja)
- 1 impresora de matriz (uso de auxiliar de egresos)
- 1 impresora de tóner en red (uso de bodega): Dispositivo en alquiler
- 1 impresora de tinta para impresión de portafolios de comerciales

5.5.11 Generalidades del Área de Sistemas. El área de sistemas depende directamente de gerencia, solo existe una persona que ejecuta las actividades del área.

El área de sistemas se encarga de atender los equipos, aplicaciones, la infraestructura y servicios tecnológicos de la empresa, mediante la administración, desarrollo de sistemas de información, mantenimiento y servicios informáticos que ayuden en las actividades realizadas por los empleados.

5.5.12 Macroprocesos Área de Sistemas

5.5.12.1 Proceso de soporte al sistema de información

Objetivo: Administrar y velar por el funcionamiento adecuado de las aplicaciones y sistemas de información usadas en la empresa.

Es responsabilidad del área de sistemas brindar el soporte a usuario en procesos asociados al sistema de información, las redes de comunicaciones. Administrar los recursos de hardware y software propiedad de la empresa y participar en la compra de estos a fin del logro de su misión.

El área de sistemas coordina la generación de los informes que son producidos por la empresa.

5.5.12.2 Proceso mantenimiento

Objetivo: Programar y supervisar la realización de mantenimientos preventivos y correctivos con el fin de conservar la vida útil de los dispositivos propiedad de la empresa. Cubriendo equipos de cómputo, equipos de red, redes de datos y aplicaciones ofimáticas.

5.5.13 Servicios del Área de Sistemas a otras áreas de la empresa

- Soporte a Usuarios Finales

- Comercial: Provee el software y hardware necesario para la realización óptima de actividades del área, brinda una infraestructura de red para la comunicación interna y externa de la empresa, atento a solucionar cualquier eventualidad que se presente y afecte el sistema, programa y supervisa el mantenimiento preventivo y correctivo a dispositivos del área.

- Compras: Provee hardware y software necesario para la actividad, administra las bases de datos de inventario y proveedores, brinda una infraestructura de red para la comunicación con proveedores y gerencia, programa y supervisa el mantenimiento preventivo y correctivo a dispositivos del área

- Bodega: Intercomunica el área de bodega y almacenamiento con la de compras para el manejo del inventario.

- Proyectos: Apoyo en creación en nuevos puntos de ventas, suministrando hardware, software y conexiones de red, internet y telefonía para integrar con la Sede Principal.

- Calidad: Provee hardware y software necesario para la actividad, generación de reportes para indicadores de gestión de procesos y aportar en la creación de procedimientos, instructivos donde estén involucrado los activos informáticos.

- Contabilidad: Provee el hardware necesario para la realización óptima de actividades del área y software para el manejo de ingresos y egresos, base de datos de caja y archivos, programa y supervisa el mantenimiento preventivo y correctivo a dispositivos del área, brinda una infraestructura de red para la comunicación interna.

– Informes personalizados: Dependiendo de la necesidad de los usuarios, se crean informes de indicadores, de inventario, de ventas entre otros que ayuden a los usuarios sobre todo a los líderes de áreas poder analizar información y ejecutar tácticas de mercadeo.

– Almacenamiento Compartido: El área de sistemas debe proveer el servicio de red y el espacio necesario para almacenar y compartir información de forma segura y rápida.

– Impresión y escaneo en red: La disponibilidad del servicio de impresión y escaneo en red es muy importante, ya que de ello depende la generación de la factura al cliente, la gestión de cartera, brindar información al cliente del estado de saldo y los demás procesos que necesitan de soporte físico y firmas para su validez.

– Solución Seguridad Perimetral: Proteger la red de amenazas e intrusiones, monitorear y controlar la navegación de internet asignando perfiles según necesidades del usuario.

5.5.14 Trámites

– Formulario de solicitud falla o eventualidad: En caso de eventualidad en algún dispositivo, datos, infraestructura, no queda registro del hecho. Para los servicios de telefonía o Internet que se requiere intervención del proveedor se solicita y archiva copia del reporte de fallas. Para novedades en los equipos de cómputo, se registran en la hoja de vida de cada uno, para control de cambios de partes, daños, actualizaciones, etc. que se realicen en los mantenimientos correctivos.

– Políticas de seguridad: Actualmente la empresa no aplica ni tiene estipuladas políticas de seguridad informática.

5.5.15 Planos de MA PEÑALOSA CÍA.S.A.S. (Ver Anexo I)

5.6 MARCO LEGAL

Las organizaciones que requieren implementar un sistema integrado basado en la seguridad de la información que sea certificado internacionalmente, requieren desarrollar e implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en las normas ISO/IEC 27001:2013, la cual es el estándar certificable y actualmente aprobado en Colombia por ICONTEC.

La norma ISO/IEC 27001 es la principal de la familia ISO 27000, ya que contiene los requisitos básicos, describe los objetivos y controles recomendados para la seguridad de la información y guía de mejores prácticas para la seguridad.

El objetivo de implementar un sistema el SGSI es brindar seguridad a todos los activos de información más resaltantes en la organización a través de los resultados del análisis de riesgo y otorgando la confiablidad de la seguridad.

En cuanto a nivel estatutario en Colombia, contamos con la Ley 1581 de 2012 de Protección de datos personales, cuyo objeto es desarrollar el derecho constitucional que tiene las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ella en bases de datos o archivos; así como el derecho a la información consagrado la art. 20 de la Constitución Política; Decreto 1377 de 2013 del Ministerio de Comercio, Industria y Turismo en el que reglamenta parcialmente la ley 1581/12.[11]

La Ley 1266 del 31 de diciembre del 2008: Habeas Data. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la información y las comunicaciones TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Esta ley desarrolla una regulación integral del derecho fundamental de las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en banco de datos y en archivos de entidades públicas y privadas.[12]

---

[11] ALCALDÍA DE BOGOTÁ, Ley 1581 del 2012. [En línea], [consultado el 2 de mayo de 2018]. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

[12] COLOMBIA. Congreso de la República. Ley 1266 de 2008. [En línea], [consultado el 2 de mayo de 2018]. Disponible en Internet: https://blogjus.wordpress.com/2009/01/13/ley-1266-de-2008-habeas-data/

Ley 1341 de 2009. Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.[13]

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.[14]

[13] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Ley 1341 de 2009. [En línea], [consultado el 2 de mayo de 2018]. Disponible en Internet: http://www.mintic.gov.co/portal/604/w3-article-3707.html

[14] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Ley 1273 de 2009. Recuperado de: http://www.mintic.gov.co/portal/604/w3-article-3705.html

6. DISEÑO METODOLÓGICO

6.1 TIPO DE INVESTIGACIÓN

La investigación que se planea llevar a cabo corresponde a una investigación de tipo aplicada. En esta investigación se realizará un análisis inicial de la situación actual de la seguridad de los activos informáticos de MA PEÑALOSA CÍA. S.A.S, con el fin de aplicar los conocimientos adquiridos, analizando y clasificando cada activo, detectando las posibles amenazas para finalmente diseñar controles que ayuden a mitigar los riesgos a los que están expuestos los activos informáticos de la empresa.

6.2 HIPÓTESIS

6.2.1 Hipótesis Investigativa. Las aplicaciones de políticas, controles y procedimientos para los distintos procesos contemplados en el Diseño del Sistema de Gestión de Seguridad de la Información para MA PEÑALOSA CÍA. S.A.S. contribuyen a mitigar los riesgos que se presenten y afecten los activos informáticos.

6.2.2 Hipótesis Nula. Las aplicaciones de políticas, controles y procedimientos para los distintos procesos contemplados en el Diseño del Sistema de Gestión de Seguridad de la Información para MA PEÑALOSA CÍA. S.A.S. no contribuyen a mitigar los riesgos que se presenten y afecten los activos informáticos.

6.3 VARIABLES

Tabla 2. Variables de la Hipótesis

Variable	Descripción
Tiempo	Factor medible a través del cronograma de actividades diseñado para el desarrollo de los objetivos propuestos en el proyecto.
Costos	Para el diseño del Sistema de Gestión de Seguridad de la información de MA PEÑALOSA CÍA. S.A.S. es necesario definir los recursos financieros y estimar la inversión realizada.
Recursos	Cantidad de personas necesarias para el levantamiento de la información, análisis y diseño del Sistema de Gestión de Seguridad de la Información.

Fuente: Autor

6.4 POBLACIÓN Y MUESTRA

6.4.1 Población. La Empresa MA PEÑALOSA CÍA. S.A.S. está ubicada en el municipio de Cúcuta departamento de Norte de Santander. Es una empresa dedicada a la distribución de materiales de construcción. Actualmente tiene tres sedes en Cúcuta y una en el municipio de Pamplona. El proyecto está enfocado en la Sede Principal, la cual cuenta con (54) cincuenta y cuatro empleados, distribuidos en las diferentes áreas de la empresa: ferretería, infraestructura, servicio al cliente, bodega, compras, contabilidad, sala de ventas, construcción y sistemas. Se debe aclarar que no todos los empleados tienen acceso al uso de los activos informáticos.

6.4.2 Muestra. En la Sede Principal de MA PEÑALOSA CÍA. S.A.S., no todo el personal tiene acceso a los activos informáticos, por tal razón para la aplicación de entrevistas y encuestas se tendrán en cuenta solo los que tengan acceso a estos, con el fin de revisar los procedimientos implementados, medidas de seguridad existentes, equipos y herramientas involucrados y de esta manera determinar posibles riesgos y amenazas de la información de la Empresa. De los cincuenta y cuatro empleados que conforman la empresa, se tomó como muestra 10 de los empleados, los cuales hacen parte de las distintas áreas de MA PEÑALOSA CÍA. S.A.S.:

- Cuatro (4) asesoras de Servicio al cliente
- Dos (2) de Contabilidad (Contador Auxiliar de egresos y Archivista)
- Una (1) asesora de Sala
- Líder de Bodega
- Una (1) auxiliar de Compras.

6.5 LINEA DE INVESTIGACIÓN

La línea de investigación del proyecto está orientada de acuerdo a la Norma ISO/IEC 27001, por lo cual se puede identificar temas como: Tecnología de la información, Seguridad de la Información, Gestión de Riesgos y Sistema de Gestión de Seguridad de la Información.

6.6 INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

En el desarrollo del proyecto de grado, se aplicaron las siguientes herramientas para la recolección de información:

- Encuestas
- Evidencias fotográficas
- Observación directa
- Entrevistas con el jefe de área de sistemas y directivos de MA PEÑALOSA CÍA S.A.S
- Documentación del sistema de gestión calidad de la empresa.

Se utilizaron otras fuentes de información, tales como tesis, libros y escritos en medios físicos, electrónicos o publicados en Internet; referentes a temas de: SGSI, Norma ISO 27001 y 27002, metodología de MAGERIT e información que contribuya como guía y referencia para este proyecto.

6.7 RECURSOS DISPONIBLES

6.7.1 Recursos Materiales. Los materiales utilizados durante el desarrollo del proyecto fueron: resmas de papel, tóner, tinta, carpetas, sobres, lapiceros, ganchos, llamadas telefónicas y transporte para desplazamientos a la empresa donde se aplicará el proyecto.

6.7.2 Recursos Humanos

6.7.2.1 Proponentes Primarios. Johanna Carolina Ararat Muñoz. Ingeniera de Sistemas egresada de la Universidad Francisco de Paula Santander, desarrolladora del proyecto, y responsable desde hace ocho años del área de sistemas de la empresa MA PEÑALOSA CÍA. S.A.S., ejecutando funciones como: administradora del Sistema de Información, redes de comunicaciones, seguridad perimetral, soporte a usuarios y supervisión de mantenimiento preventivo y correctivo.

6.7.2.2 Proponentes secundarios. MA PEÑALOSA CÍA. S.A.S. Durante el desarrollo del proyecto fue necesario la participación de directivos y empleados de la empresa de la Sede Principal donde fue aplicado el proyecto.

A continuación, se mencionan con detalle:

- Directivos. MA PEÑALOSA CÍA. S.A.S. es una empresa familiar, formada por:

a) Gerente: Juan Esteban Peñalosa Arguijo
b) Subgerente: María Paz Arguijo

c) Socios: Leopoldo Peñalosa Arguijo, María Alejandra Peñalosa Arguijo y Ana María Peñalosa Arguijo.

- Empleados. Para el levantamiento de información fue importante la colaboración de los empleados de la empresa, para conocer sus percepciones sobre el estado actual de la seguridad de la información. Las áreas que participaron en el proyecto fueron:

a) Área Comercial: Yuli Flórez, Alba Peñaloza, Sofía Villamizar y Minerva Maldonado, Asesoras de Servicio al Cliente y Emilse Ortiz de sala de ventas, las cuales permanecen más permanencia dentro de la Sede Principal.

b) Área de Logística: Luis Blanco (Líder de Bodega), persona responsable de la bodega y despachos en la Sede Principal.

c) Área de Contabilidad: Andrés Berbesí (Director de Contabilidad), Claudia Barrera (Auxiliar de egresos) y Adriana Celis (Archivista). Personas que manejan más flujo de documentos y procesos del área.

d) Área de Compras: Delsa Soto (Auxiliar de Compras). Persona responsable de apoyar a la directora de compras, en procesos de carga de mercancía al inventario, procesos de devoluciones, compras de mercancía, contacto con proveedores.

Asesores del Proyecto.

En las distintas fases del proyecto, la Universidad Nacional Abierta a Distancia, dispuso a docentes como asesores metodológicos, los cuales fueron de mucho apoyo para la construcción de este.

- Docente del curso Proyecto de Seguridad I: Helena Clara Isabel Alemán. Ingeniera de Sistemas de la Universidad de Boyacá. Especialista en Pedagogía para el Desarrollo del Aprendizaje Autónomo y Magister en Seguridad Informática.

- Docente del curso Proyecto de Seguridad II: Juan José Cruz. Ingeniero de Sistemas de la Universidad Cooperativa de Colombia. Especialista en Seguridad Informática de la Universidad Piloto de Colombia. Candidato a Magíster en Seguridad Informática de la Universidad Internacional de la Rioja y candidato a Magíster en Docencia Universitaria de la Universidad Broward International.

- Director de Proyecto de grado: Julio Alberto Vargas Fernández. Ingeniero de Sistemas de la Universidad de Cundinamarca. Especialista en seguridad informática de la Universidad Piloto de Colombia.

6.7.3 Recursos Institucionales

- Instalaciones de MA PEÑALOSA CÍA. S.A.S. Sede Principal. Ubicada en la ciudad de Cúcuta, Norte de Santander. Avenida 5 # 8-40 Centro.

- Universidad Nacional Abierta y a Distancia. Universidad pública. Estatal de carácter nacional, financiada por el Estado Colombiano y por recursos propios. Sede principal se encuentra la ciudad de Bogotá D.C.

6.7.4 Recursos Tecnológicos

- Portátil Hp de 15.6" con características: Memoria RAM de 8 Mb, Procesador Intel Core i5, disco duro de 1 T, Sistema Operativo Windows 10 profesional, Office 2013, Acrobat Reader, 7Zip, Skype,
- Software PILAR para el desarrollo de la metodología MAGERIT
- USB
- Cámara fotográfica
- Impresora
- Internet.

6.7.5 Recursos Financieros. El presupuesto está planteado para desarrollar el proyecto en cuatro meses.

Tabla 3. Presupuesto del Proyecto

Presupuesto del Proyecto				
Ítem	Descripción	Valor unitario	Cantidad	Valor Total
1	Ingeniero desarrollador del proyecto	$1.500.000	1	$6.000.000
2	Materiales y suministros	$80.000	6	$480.000
3	Transportes	$150.000	1	$150.000
4	Servicios públicos (luz, internet)	$70.000	6	$420.000
5	Gastos generales	$200.000	1	$200.000
6	Software	$750.000	1	$750.000
7	Horas de ingeniería	$80.000	60	$4.800.000
8	Equipo	$2.300.000	1	$2.300.000
			TOTAL	$15.100.000

Fuente: Autor

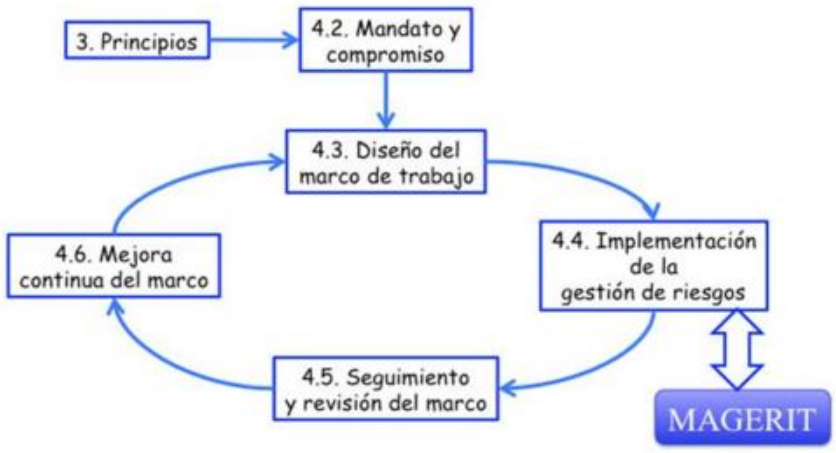
6.8 METODOLOGÍA DE DESARROLLO

6.8.1 Metodología para el análisis de riesgos. La metodología MAGERIT, siglas por la cual significa Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, fue creada por el Consejo superior de Administración Electrónica de España, es de carácter público, enfocada a las administraciones públicas. Dado que el sistema de gestión de Riesgos se hace imprescindible para las guías del buen gobierno por el uso creciente de las tecnologías de Información en el ámbito gubernamental, organizacional y social. El uso desmedido de las tecnologías de Información ha hecho que los activos de información en las organizaciones tengan muchos beneficios alcanzables, pero a su vez incurran en riesgos y vulnerabilidades.

MARGERIT, es creado para toda organización que haga uso de los sistemas de información donde la información sea tratada de manera adecuada garantizando su disponibilidad, confidencialidad e integridad siendo está protegida de manera rigurosa por una metodología de análisis del riesgo, adoptando las mejores prácticas de buen uso, dejando afuera las improvisaciones y las arbitrariedades de los analistas.

Persigue unos objetivos comunes: Concienciar a los responsables directos e indirectos de los riesgos a los cuales puede estar sometida la información y/o los sistemas de información, ofrecer un método sistemático de análisis de riesgos derivados del uso de las SI, ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos controlados, preparar la organización para diferentes procesos como auditorías, acreditaciones, certificaciones.

Figura 6. ISO 31000-Marco de trabajo para la gestión de riesgos



Fuente: (Pae Magerit, 2012)

6.8.2 Metodología para el desarrollo del diseño del SGSI. Inicialmente se visitarán las instalaciones de la empresa MA PEÑALOSA CÍA. S.A.S., para hacer diagnóstico actual de la seguridad de la Información, aplicando encuestas y recopilando evidencias fotográficas de la situación del área tecnológica, para identificar y analizar inventario de activos y seguridad que maneja cada activo, identificación de amenazas y vulnerabilidades, identificación de impactos, análisis y evaluación de riesgos, tratamiento de riesgos y controles de accesos aplicados.

Para el desarrollo de la fase de Planeación del ciclo PHVA como producto del Sistema de Gestión de Seguridad de la Información, se realizarán las actividades que se muestran a continuación necesarias para el procedimiento de implementación de la norma ISO 27001:

- Identificar alcance del Sistema de Gestión de la Seguridad de la Información
- Elaboración de Declaración de aplicabilidad de controles
- Ejecución de lista de chequeo según dominios de la ISO 27002:2013
- Definición y aplicabilidad de metodología para el análisis y gestión de Riesgo (Magerit)
- Elaboración de inventario de activos informáticos
- Identificación y evaluación de riesgos
- Informe de auditoría sobre hallazgos encontrados
- Establecimiento de Políticas de Seguridad que se ajusten a las necesidades de la empresa para garantizar la confidencialidad, integridad y disponibilidad de la información.
- Definición de procedimientos asociados a los hallazgos
- Capacitación y concienciación en seguridad de la información.

6.8.3 Resultados Esperados. La Propuesta de implementación del Sistema de Gestión de Seguridad de la Información, contendrá los siguientes aspectos:

- Diagnóstico actual de la seguridad de la Información de MA PEÑALOSA CÍA S.A.S.

- Desarrollo de la fase de Planeación del ciclo PHVA como producto del Sistema de Gestión de Seguridad de la Información.

- Política general de seguridad de la empresa que incluyan controles para controlar: Aspectos Organizacionales, recursos humanos, gestión de activos, control de acceso, mantenimiento de sistemas informáticos y gestión de incidentes de Seguridad entre otros.

- Compromiso firmado por parte de los directivos de la empresa MA PEÑALOSA CÍA. S.A.S., donde manifiesten el apoyo a la implementación del SGSI.

- Evaluación de riesgos a través de la aplicabilidad de la metodología donde se contempla creación del inventario de activos, identificación de amenazas y vulnerabilidades, valoración de impacto, análisis y evaluación de riesgos.

- Estrategias para Formación y concientización.

Tabla 4. Resultados esperados

Resultado/Producto Esperado	Indicador	Beneficiario
Reconocer la percepción de la organización sobre la seguridad de la información	Encuesta de percepción sobre la seguridad de la información	MA PEÑALOSA CÍA. S.A.S.
Recolección de evidencias de situación actual del área tecnológica	Evidencias fotográficas de la situación actual	MA PEÑALOSA CÍA. S.A.S.
Identificación de los activos informáticos de la organización	Inventario de activos	MA PEÑALOSA CÍA. S.A.S.
Identificación de las amenazas y vulnerabilidades que impactan en los activos informáticos.	Inventario de amenazas, vulnerabilidades	MA PEÑALOSA CÍA. S.A.S.
Propuesta de políticas y controles que ayuden a mitigar los riesgos encontrados.	Planteamiento de las políticas y procedimientos de seguridad de la información	MA PEÑALOSA CÍA. S.A.S.

Fuente: Autor

6.8.4 Cronograma de Actividades. A través del análisis de los objetivos específicos definidos para el proyecto aplicado a MA PEÑALOSA CÍA. S.A.S., se definieron una serie de actividades, las cuales están integradas por unas tareas relevantes que conllevarán al logro de cada uno de los objetivos.

Tabla 5. Detalle de actividades

Fase	Actividad	Tarea especifica
Diagnóstico de Situación actual	Aprobación del proyecto con los directivos de MA PEÑALOSA CÍA S.A.S	Dar a conocer los objetivos y las bondades de implementar un Sistema de Gestión de Seguridad Informática a los directivos.
		Proponer a los directivos de MA PEÑALOSA CÍA. S.A.S implementar un Sistema de Gestión de Seguridad Informática
		Obtener autorización para acceder a documentación de la empresa, toma de evidencias fotográficas, realización de encuestas y entrevistas a usuarios.

Tabla 5. Continuación

Fase	Actividad	Tarea especifica
		Adquirir carta de aprobación para la aplicación del proyecto de Seguridad Informática
	Reconocimiento general de MA PEÑALOSA CÍA. S.A.S.	Identificar áreas y puestos de trabajo establecidos
		Conocer a los empleados de cada área
		Socializar el trabajo a realizar para que los empleados estén enterados sobre el proyecto y participen en el levantamiento de información en caso de requerirse
		Explorar inicialmente de ubicación de cuarto de equipos y área de sistemas
		Analizar de la estructura organizacional de la empresa
		Entender el funcionamiento y actividad comercial de la empresa
	Levantamiento de la información	Diseñar entrevistas y encuestas
		Aplicar encuesta de percepción de la seguridad informática a los empleados
		Realizar entrevista al jefe de sistemas
		Recorrer minuciosamente las áreas de la empresa para toma de evidencias fotográficas de anormalidades encontradas que atentan contra la seguridad informática
	Recopilar información activos informáticos	Identificar los activos informáticos de la empresa
Diseño del SGSI	Realizar la Declaración de Aplicabilidad (SOA)	Enumerar controles de seguridad
		Definir cuáles controles sugeridos en la norma ISO 27001 se tendrán en cuenta el SGSI
		Justificar definir las razones de la aplicación de los controles
		Definir objetivos que se lograrán con los controles a aplicar
		Describir los controles planeados y existentes.
	Evaluar los controles existentes sobre Seguridad Informática	Realizar lista de chequeo para verificar el cumplimiento de controles de acuerdo a los criterios de la norma ISO 27002:2015 que ayuden a complementar la información sobre el estado actual de la seguridad en la empresa
		Análisis de los resultados de la aplicación de lista de chequeo
	Recopilar información de los activos informáticos	Crear inventario de activos informáticos
		Clasificar de los activos informáticos de la empresa
		Definir de dependencia entre activos
		Valorar de los activos informáticos

Tabla 5. Continuación

Fase	Actividad	Tarea especifica
		Identificar y evaluar amenazas y vulnerabilidades que afectan los activos informáticos
	Aplicar metodología para evaluación de riesgos	Realizar un análisis de la probabilidad de ocurrencia e impacto que puedan producir en los activos informáticos.
		Calcular el riesgo y definir el nivel del riesgo
		Realizar análisis de riesgos identificados según niveles tratados.
	Identificar Alcance del SGSI	Identificar delimitaciones de la Propuesta del SGSI
	Realizar análisis de hallazgos	Realizar informe de hallazgos de auditoría
	Determinar Políticas de Seguridad Informática	Definir de Política General
		Definir de Política de Gestión de Activos
		Definir Política de seguridad de los Recursos Humanos
		Definir Política de Manejo de información
		Definir Política de Acceso físico
		Definir Política de copias de respaldo
		Definir Política de uso de internet
		Definir Política de uso de correo electrónico empresarial.
		Definir Política de seguridad del centro de datos
		Definir Política de uso de software
		Definir Política de contraseñas
		Definir Política de protección contra software malicioso
		Definir Política de equipo desatendido
		Definir Política de Acceso remoto
		Definir Política de gestión de incidentes
	Establecer procedimientos de Seguridad Informática	Procedimiento de Altas o Bajas de Usuario
		Procedimiento de Mantenimiento preventivo
		Procedimiento de Mantenimiento Correctivo
		Procedimiento de gestión de Incidentes, Amenazas y Debilidades de Seguridad
		Procedimiento de actualización de sistemas operativos y software
		Procedimiento de Centro de datos
		Procedimiento de Seguridad de Redes
		Procedimiento de Monitoreo de Red y Servicios
Elaboración de la Propuesta de diseño del sistema de Gestión de Seguridad Informática	Elaborar Propuesta de diseño de Sistema de Gestión Seguridad Informática	Socializar Propuesta del Sistema de Gestión de Seguridad Informática con los directivos y a la coordinadora de sistemas
		Entrega de Propuesta del Sistema de Gestión de Seguridad Informática

Fuente: Autor

Tabla 6. Cronograma de Actividades

CRONOGRAMA DE ACTIVIDADES																
NOMBRE DEL PROYECTO: DISEÑO DE UN SGSI BASADO EN LA NORMA ISO 27001 PARA LA EMPRESA MA PEÑALOSA CÍA S.A.S SEDE PRINCIPAL CÚCUTA																
Integrantes: Johanna Carolina Ararat Muñoz	Localidad: MA PEÑALOSA CÍA. S.A.S. SEDE PRINCIPAL- CÚCUTA															
MES / ACTIVIDAD / Semanas	MES 1				MES 2				MES 3				MES 4			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Aprobación del proyecto con los directivos de MA PEÑALOSA CÍA. S.A.S.																
Reconocimiento general de MA PEÑALOSA CÍA. S.A.S.																
Levantamiento de la información																
Realizar la Declaración de Aplicabilidad (SOA)																
Evaluar los controles existentes sobre Seguridad Informática																
Recopilar información de los activos informáticos																
Aplicar metodología para análisis y evaluación de riesgos																
Identificar Alcance del SGSI																
Realizar informe de hallazgos de la Auditoria																
Definir Políticas de Seguridad Informática																
Establecer procedimientos de Seguridad Informática																
Diseñar propuesta del Sistema de Seguridad Informática																

Fuente: Autor

7. DESARROLLO DE LA INVESTIGACIÓN

7.1 CONTROLES DE SEGURIDAD

Los controles son necesarios para prevenir, corregir errores o irregularidades que puedan afectar la operatividad del negocio. Con la aplicabilidad del estándar ISO 27001, basado en el ciclo PHVA, el cual se enfoca en la ejecución de procesos de establecer, implementar, operar y realizar seguimientos para mantener y mejorar el Sistema de Gestión de Seguridad de la Información se pretende asegurar la integridad, confidencialidad y disponibilidad de los sistemas de MA PEÑALOSA CÍA. S.A.S.

Para verificar el cumplimiento de las reglas del negocio se requiere establecer mecanismos de control que permitan mitigar el impacto de las vulnerabilidades y que según el análisis de riesgos deben ser atendidos, ya que causarían daños importantes en la organización, y para este caso se hará un análisis de acuerdo a lo sugerido en la ISO 270002.

Por lo anterior, los dominios contemplados dentro de la Norma ISO 27002:2013[15] son:(ISO/IEC, 2013)

- A.5 Política de la seguridad de la información
- A.6 Organización de la seguridad de la información
- A.7 Seguridad de los Recursos humanos
- A.8 Gestión de Activos
- A.9 Control de acceso
- A.10 Criptografía
- A.11 Seguridad física y ambiental
- A.12 Seguridad de las operaciones
- A.13 Seguridad de las comunicaciones
- A.14 Adquisición, desarrollo y mantenimiento de sistemas
- A.15 Relaciones con los proveedores
- A.16 Gestión de incidentes de seguridad de la información
- A.17 Aspectos de seguridad de la información de la gestión de la continuidad de negocio
- A.18 Cumplimiento

[15] ISO/IEC El portal de ISO 27001 en Español. [En línea], [consultado el 23 de junio de 2017]. Disponible en internet: http://www.iso27000.es/download/ControlesISO27002-2013.pdf

7.2 DECLARACION DE APLICABILIDAD - SOA

En MA PEÑALOSA CÍA. S.A.S., es indispensable que se desarrolle la declaración de aplicabilidad con los controles de seguridad a establecer que sirvan como una medida para contribuir a reforzar los procesos para protección de la información.

La declaración de aplicabilidad está basada en los controles de seguridad establecidos en el estándar ISO/IEC 27001 versión 2013 del Anexo J, la cual contempla 14 dominios, 35 objetivos de control para un total de 114 controles.

7.3 MODELO SOA

El modelo de Declaración de Aplicabilidad (SOA), se resume en términos generales los objetivos de control, las amenazas y vulnerabilidades, los controles seleccionados, controles existentes que deben seguir revisando, justificación de aquellos controles que serán excluidos del análisis y las razones para la selección de los controles detalladas en la tabla 7.

Tabla 7. Razones para la selección de los controles

L	Requisitos legales	Obligatorio cumplimiento por una norma superior a la empresa, de no llevarse a cabo la empresa incurriría en sanciones
O	Obligación contractual	Son aquellas que en la celebración de contratos con las entidades o personas que la empresa debe cumplir,
N	Requerimientos del negocio	Son aquellos que en el desempeño de su actividad ha determinado que se deben realizar
R	Resultados de la evaluación de riesgos	Amenazas evidenciadas en el análisis de riesgos

Fuente: Autor

A continuación, se definen con detalle las cuatro estrategias para abordar los riesgos negativos o amenazas:

- EXCLUIR: se descarta el control porque no tiene aplicabilidad dentro de la empresa o depende de la implementación de un control para tenerse en cuenta.

- TRANSFERIR: significa dar la responsabilidad a un tercero para su administración, pero no significa que se elimina el riesgo.

- ASUMIR: Implica que no se van a tomar medidas frente al riego (Es la dirección quien toma la decisión, teniendo en cuenta que este no aumente)

- MITIGAR: Implantación de medidas que actúen de salvaguardas (Se deben documentar y gestionar)

En el Anexo K, se desarrolló la matriz de declaración de aplicabilidad con esta se pretende concretar los controles y los objetivos por los cuales se considera que estos son necesarios de implementar para afrontar las amenazas y vulnerabilidades identificadas con el fin de mitigar o aceptar los riesgos detectados y garantizar la protección de la información.

8. DIAGNOSTICO DE LA SITUACIÓN ACTUAL

Para establecer el estado actual de la seguridad en la empresa y reforzar la información recopilada en las entrevistas y encuestas y con el fin de abarcar los distintos aspectos se hace necesario realizar una lista de chequeo para verificar el cumplimiento de controles de acuerdo a los criterios de la norma ISO 27002:2013[16], para ello se construye la estructura del Anexo L en la que la Coordinadora del área de Sistemas realiza su registro.

8.1 ANÁLISIS DE RESULTADOS DE LA LISTA DE CHEQUEO POR DOMINIO

De acuerdo a la lista de chequeo Anexo L, aplicada a MA PEÑALOSA CÍA. S.A.S. donde se evaluaron los 114 controles contenidos dentro de la norma ISO 27002:2013, se realizará un análisis del nivel de cumplimiento de cada uno de los controles clasificados por dominio.

8.1.1 Dominio 5: Políticas de seguridad

Figura 7. Análisis de la lista de chequeo del Dominio 5

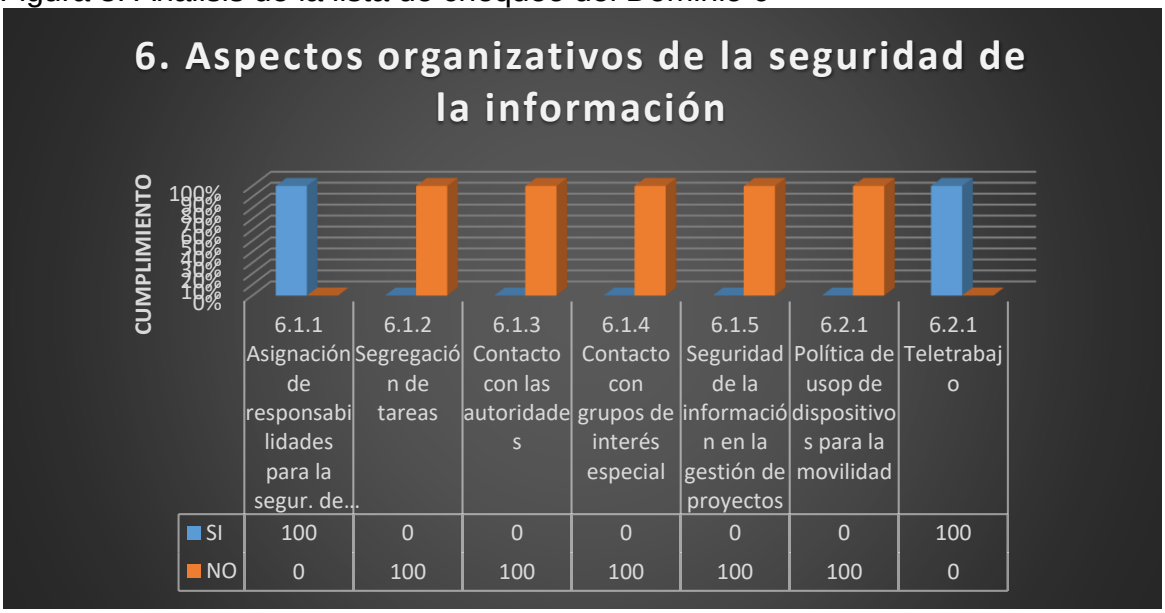
Fuente: Autor

[16] LÓPEZ NEIRA, Agustín. El portal de ISO 27002 en Español. [En línea], [consultado el 2 de febrero de 2016]. Disponible en internet: http://iso27000.es/iso27002.html

De acuerdo al análisis de la lista de chequeo para el dominio 5, corresponde a las políticas de seguridad, es evidente que la empresa no tiene definido políticas de seguridad, quedando expuesta la empresa a muchos riesgos, ya que los usuarios no conocen el reglamento para funcionar al interior de la empresa en cuanto al manejo de activos de la información. Es fundamental el establecimiento, adopción y socialización de las políticas de seguridad de la información en la empresa.

8.1.2 Dominio 6. Aspectos organizativos de la seguridad de la información

Figura 8. Análisis de la lista de chequeo del Dominio 6



Fuente: Autor

El dominio 6 corresponde a los aspectos organizativos de la Seguridad de la Información, según la información recolectada y a la encuesta aplicada a la lista de chequeo de cumplimiento de los controles de la ISO 27002:2013, se puede evidenciar que, en MA PEÑALOSA CÍA. S.A.S., las responsabilidades de seguridad de la información están asignadas a una sola persona, la coordinadora del área de sistemas. Por lo anterior sería un gran riesgo si esta persona se ausenta o falte. Además, debido al exceso de trabajo no se podría ejercer el control adecuado sobre todos los activos informáticos y asegurar la seguridad sobre ellos.

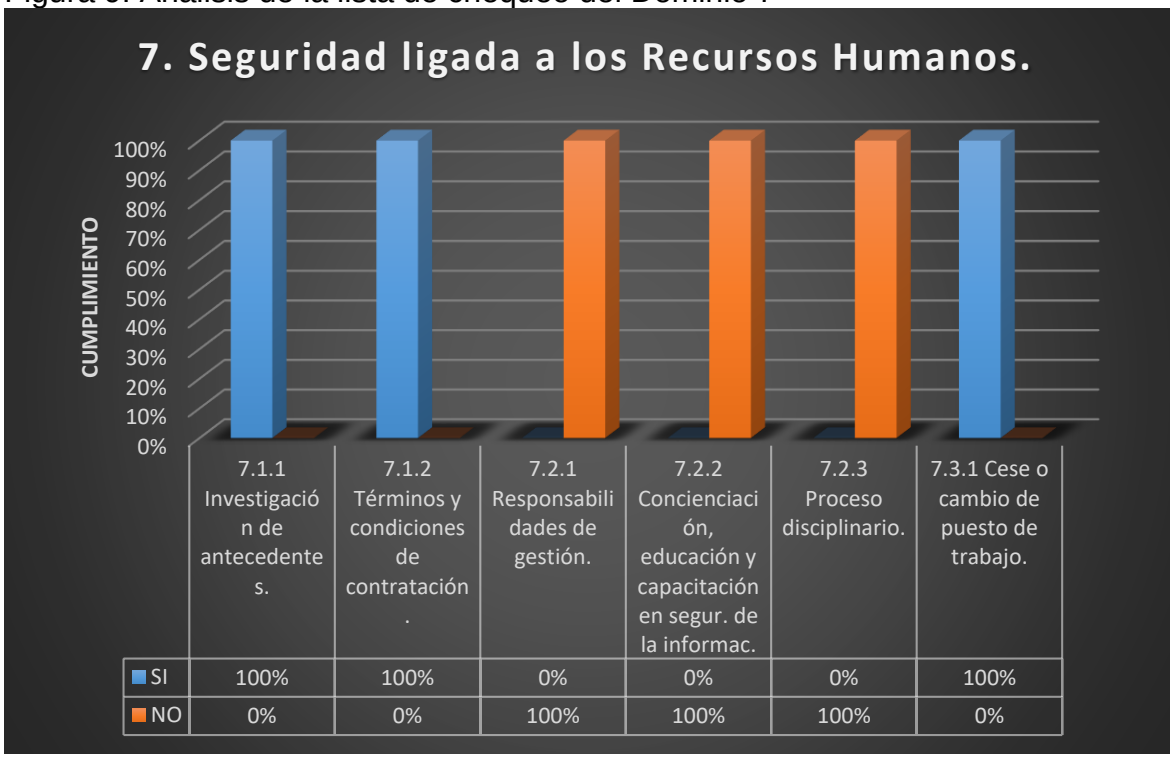
No se mantienen contacto con las autoridades ni con los grupos de interés especial; así como no se contempla la seguridad de la información dentro de la gestión de proyectos.

Para realizar algunas funciones de los asesores comerciales externos de MA PEÑALOSA CÍA. S.A.S., necesitan acceder al sistema desde sus portátiles o Smartphone fuera de las instalaciones de la empresa. No hay una política de uso para este tipo de casos.

No existe la modalidad de teletrabajo, pero puede darse el caso de una incapacidad, donde requiera por fuerza mayor del apoyo del empleado.

8.1.3 Dominio 7: Seguridad ligada a los Recursos Humanos

Figura 9. Análisis de la lista de chequeo del Dominio 7



Fuente: Autor

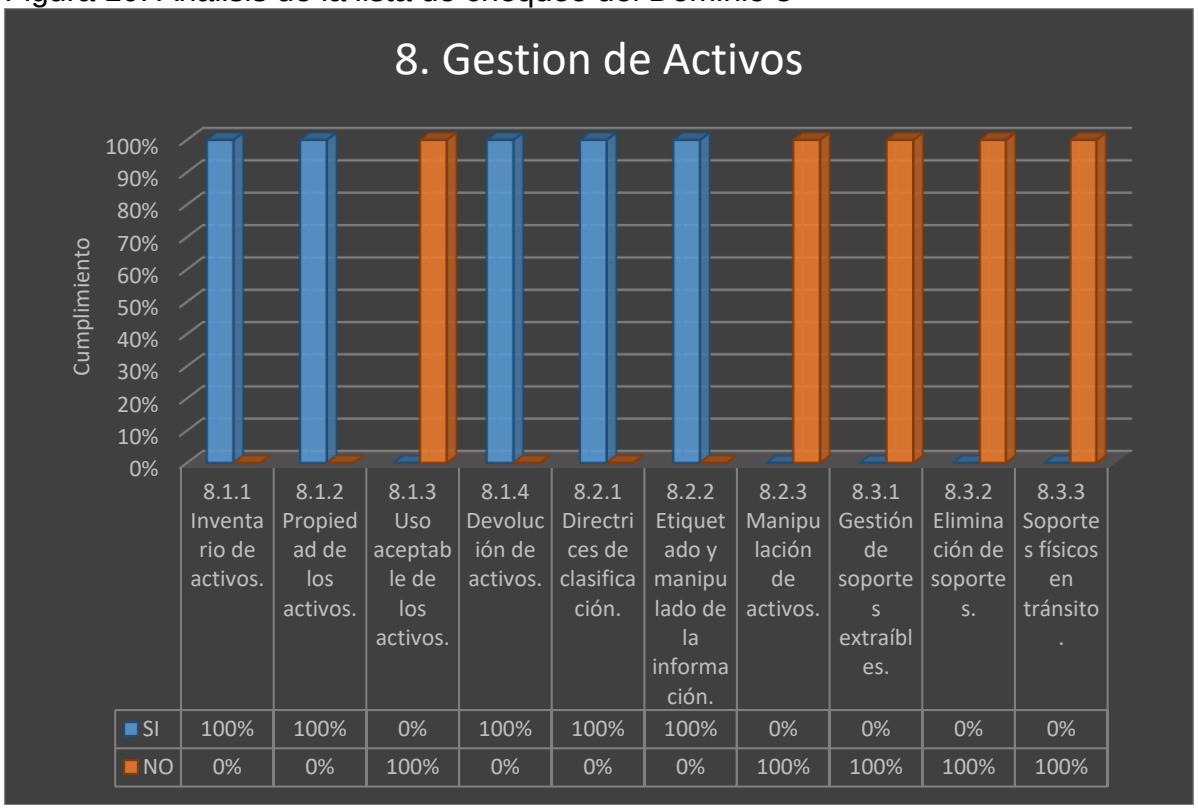
De acuerdo al análisis de la lista de chequeo con respecto al dominio 7, corresponde a la Seguridad ligada a los recursos humanos, refleja que existe cumplimiento en cuanto a la investigación de antecedentes antes de la contratación de personal, llevando a cabo procedimientos para constatar que el personal que ingresa a la empresa cumple con los estándares mínimos exigidos por los entes de control y organismos judiciales, dejando en claro también los términos de la contratación exponiendo las normas, horarios, funciones y responsabilidades que se irán a asumir en el momento en que acepte el cargo.

Se evidencia que falta incluir dentro del proceso de contratación las exigencias necesarias y la cláusula de confidencialidad para prevenir la divulgación de la información y concientizar al personal de las amenazas que existen sobre la seguridad de la información para que estén atentos e informen sobre incidencias que se presenten.

Es necesario programar capacitaciones orientadas a la concientización y conocimiento sobre la seguridad de la información.

8.1.4 Dominio 8: Gestión de Activos

Figura 10. Análisis de la lista de chequeo del Dominio 8



Fuente: Autor

Para el dominio 8, en cuanto al manejo de gestión de activos, se evidencia existencia de inventarios de activos para el reconocimiento de equipos con los que cuenta la empresa, a través de hojas de vida para cada uno de los equipos e historial de mantenimientos. Además de la identificación del usuario a quien se le hace entrega, para el control de uso y seguimiento en cuanto a manejo del activo. Esta responsabilidad está a cargo de la coordinadora de sistemas.

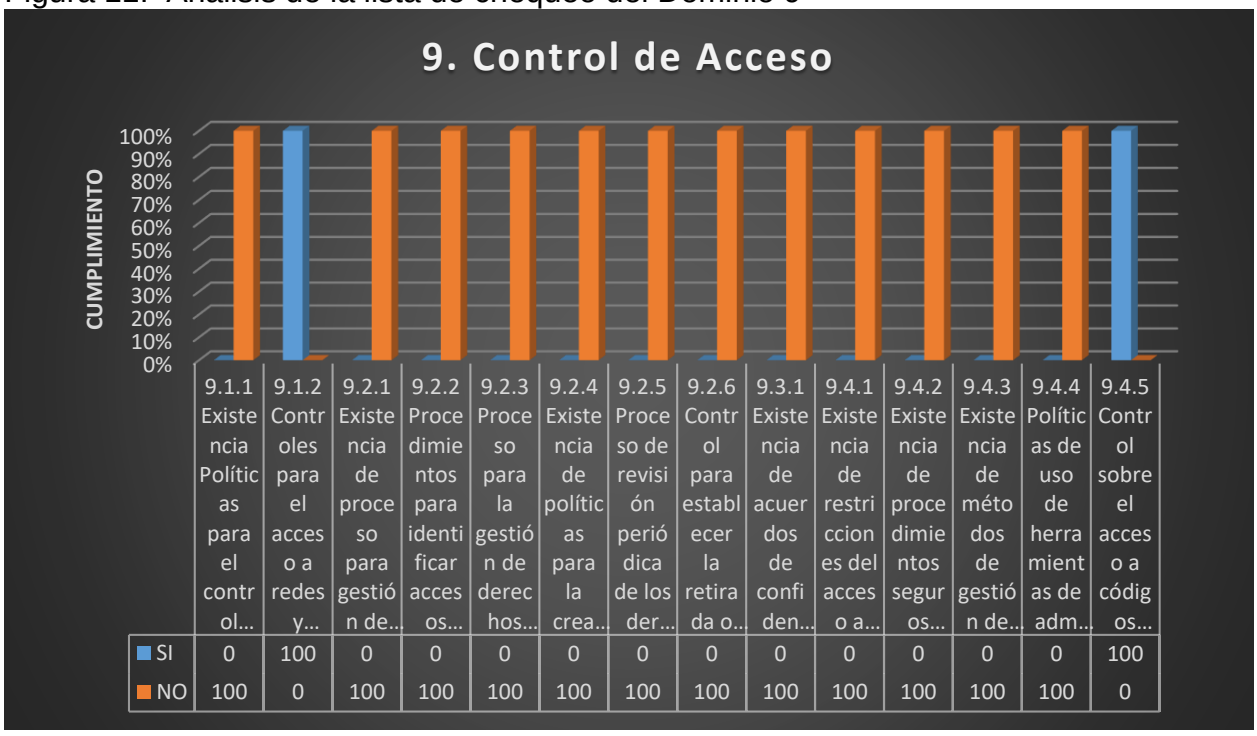
No hay control en la manipulación de la información, es necesario empezar a plantear estrategias que sirva para evitar la fuga de información, además que se debe cumplir con la ley 1581 referente a la protección de datos. Por eso es importante eliminar información que ya no sea necesaria y evitar la utilización de medios extraíbles solo dar los permisos necesarios a los usuarios en cuanto a acceso a la información.

Dentro del personal existen asesores comerciales externos, los cuales pueden representar un riesgo para la seguridad de la información de la empresa sino se cuentan con los controles pertinentes.

En cuanto al uso de medios informáticos extraíbles no existe control en la información almacenada en estos. Estos medios podrían contener infecciones maliciosas y a pesar de que se cuenta con antivirus algunos usuarios desconocen el uso o no aplican el análisis del medio.

8.1.5 Dominio 9: Control de Acceso

Figura 11. Análisis de la lista de chequeo del Dominio 9



Fuente: Autor

Es necesario implementar políticas de control de acceso que permitan gestionar los accesos a las redes y servicios, una solución podría ser el implementar un

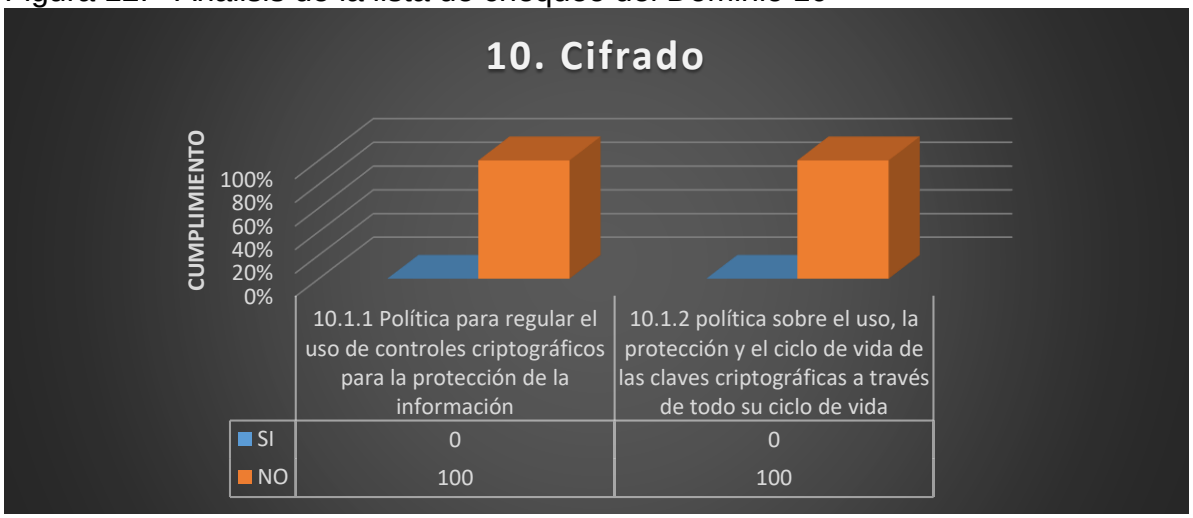
directorio activo donde se definan usuarios, grupos y políticas de seguridad para la información.

No existen políticas para la gestión de usuarios y contraseñas. Solo a través del log de modificaciones y de acceso embebido dentro del sistema de información SAP sirve como apoyo para auditar en caso de necesitarse. Al igual a través de las licencias asignadas y la configuración del usuario en el ERP, permite definir los privilegios de cada usuario, pero no existen procesos. El sistema permite bloquear después de un periodo de inactividad, pero por parte de los usuarios no tienen la política de bloquear sesiones cuando el equipo esta desatendido.

Se evidencia que algunos usuarios comparten claves y esto dificulta en el momento de ejecutar una auditoría y esto se da debido a licencias escasas para acceder al sistema de información.

8.1.6 Dominio 10: Cifrado

Figura 12. Análisis de la lista de chequeo del Dominio 10



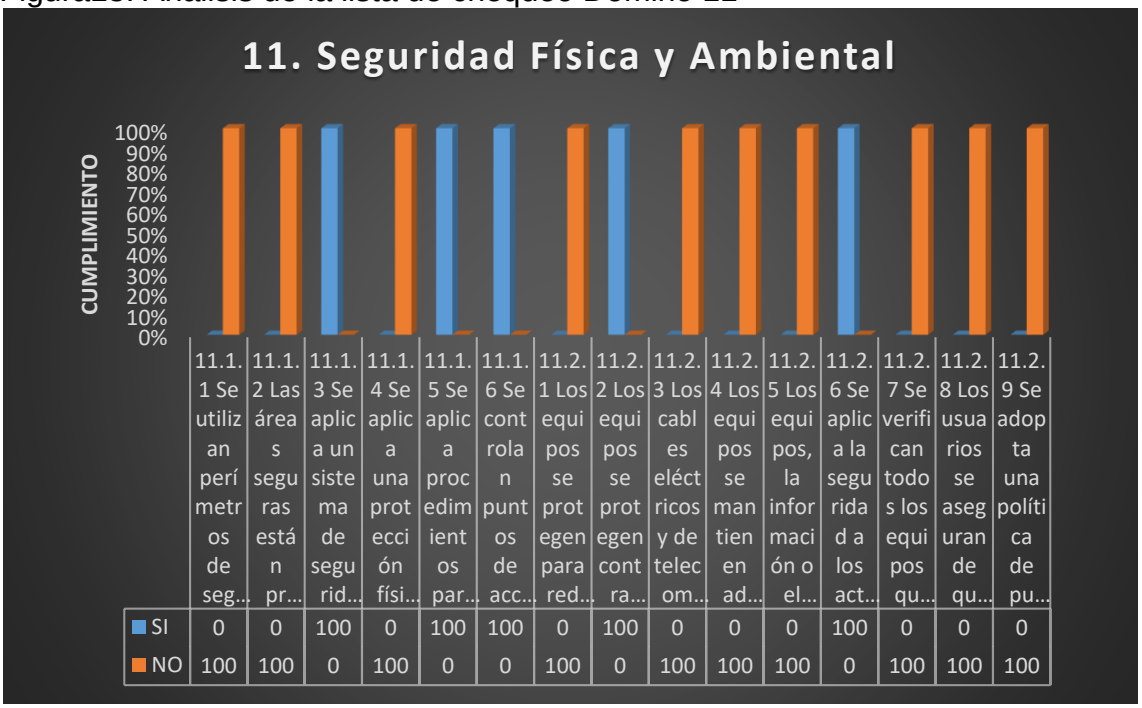
Fuente: Autor

El dominio 10 se relaciona con el cifrado, se evidencia que no se realiza ni aplica ningún tipo de políticas de seguridad para aplicar controles criptográficos y proteger los datos.

Se aplican solo como medida el uso de tokens proporcionados por los bancos para proteger las transacciones bancarias de la empresa.

8.1.7 Dominio 11: Seguridad física y ambiental

Figura13. Análisis de la lista de chequeo Domino 11



Fuente: Autor

De acuerdo al dominio 11 sobre la seguridad física y ambiental, se evidencia que no existe un centro de datos ni las mejores condiciones ambientales que permitan el buen funcionamiento de los activos críticos que soportan la infraestructura tecnológica. Están expuestos a polvo, temperaturas altas e inundaciones.

Por otro lado, las instalaciones físicas de la empresa, mantiene una estructura antigua que podría colapsar y afectar no solo a los equipos informáticos sino al personal de MA PEÑALOSA CÍA. S.A.S.

Se procura que cada equipo este protegido con una UPS sobre todo los más críticos, pero no son suficientes. Al evaluar el estado del cableado de red y eléctrico se detecta que no está en buenas condiciones debido a añadiduras del cableado y exposiciones a las condiciones ambientales ya que es cableado viejo; existe sobrecarga eléctrica en los puntos instalados y en ocasiones se han presentado problemas eléctricos y cortos.

Los equipos no están siendo protegidos para evitar accesos no autorizados Se cuenta con un sistema de alarma y cámaras de vigilancia, pero estas últimas no cubren todas las áreas. Es responsabilidad de la empresa en general que debe estar preparado ante cualquier tipo de eventualidad que puede afectar los equipos físicos.

8.1.8 Dominio 12: Seguridad en la Operativa

Figura 14. Análisis de la lista de chequeo Domino 12

Fuente: Autor

La seguridad Operativa se evalúa dentro del Dominio 12. Se evidencia la carencia de ambiente de pruebas para desplegar liberaciones de versiones nuevas del sistema de información SAP B1. Durante las actualizaciones no se tiene procedimientos ni documentación sobre mejoras del aplicativo para informar a los usuarios sobre cambios implementados.

En cuanto a la generación de copias de seguridad se realiza solo para las bases de datos automáticamente a través de una tarea programada en el SQL Server la cual se almacena en una carpeta compartida restringida y semanalmente se carga en Google drive. No se respaldan información de correo corporativo e información general de cada usuario, por lo que podría presentarse perdida de información en un siniestro ya sea por fallas lógicas de los equipos o por sabotaje de información.

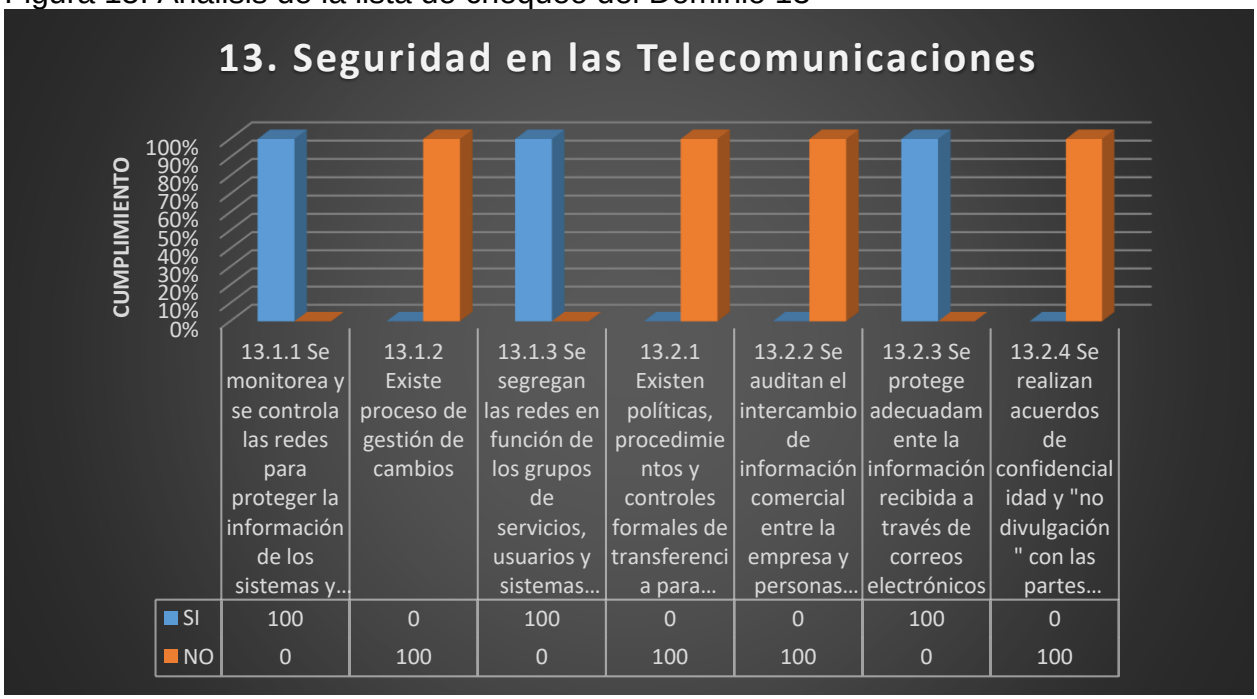
Es necesario establecer controles que hagan menos informales las tareas y establezcan directrices claras en cuanto a la forma de realizar dichos procesos como al implementar cambios, instalación de software y establecer auditorias periódicas a los sistemas de información que se manejan.

Se debe capacitar a los usuarios sobre códigos maliciosos, tanto para tomar medidas preventivas como para enfrentarlos cuando se presenten. A través del

Fortigate y el antivirus no es suficiente si el usuario no toma precauciones y hace buen uso de las herramientas que se le proporcionan.

8.1.9 Dominio 13: Seguridad en las Telecomunicaciones

Figura 15. Análisis de la lista de chequeo del Dominio 13



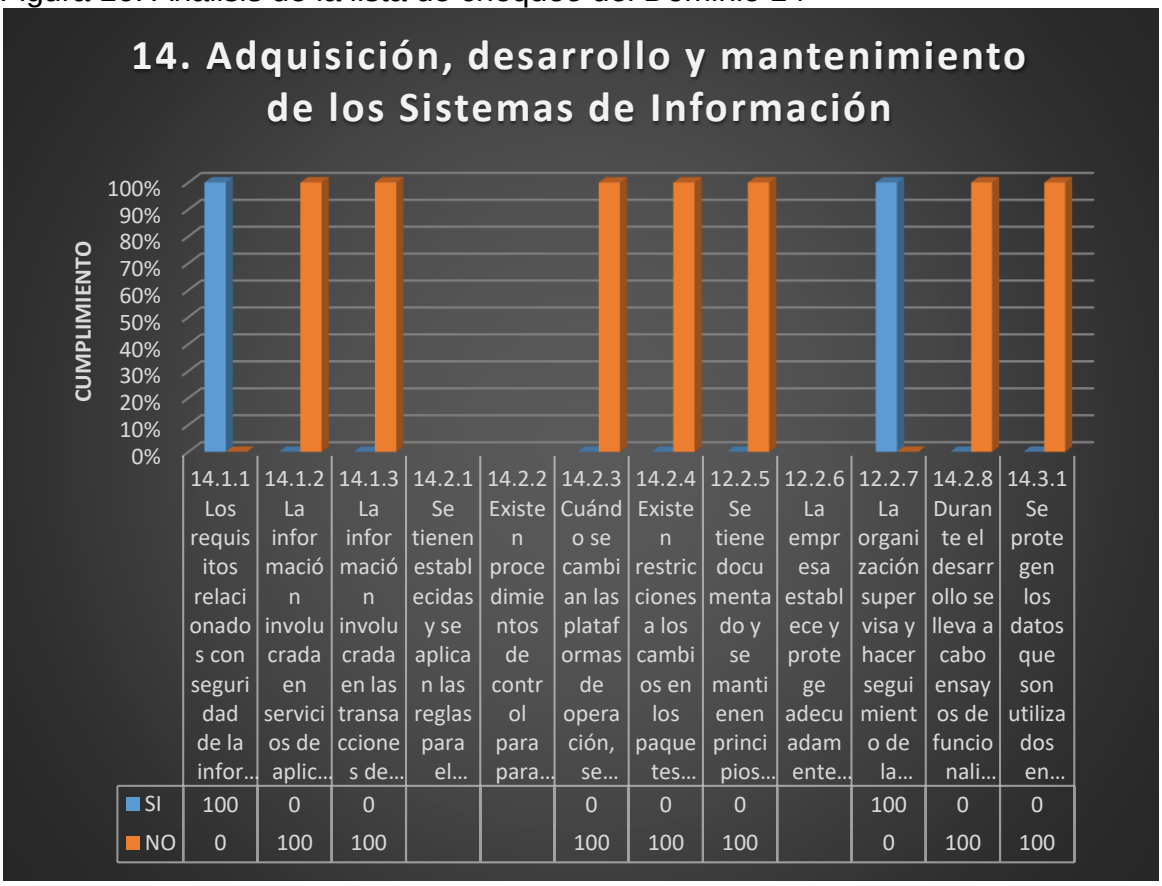
Fuente: Autor

Gracias a la existencia del Fortigate, se logra monitorear y controlar el tráfico de la red, garantizando la seguridad en cuanto a intrusiones externas, filtrando correos maliciosos y acceso a contenidos no autorizados para que los usuarios no tengan tiempo de ocio. Pero existen carencias de procedimientos y políticas que se den a conocer a los usuarios, para que ellos tengan en claro los límites de la utilización de los activos y los servicios; y las precauciones para garantizar la seguridad de la información.

No existe un canal seguro para las conexiones de los usuarios externos y el acceso de los usuarios de las demás sedes, debido al uso de Terminal Server sin la aplicabilidad de una VPN que asegure los datos que viajan a través del canal de comunicaciones establecido con el servidor.

8.1.10 Dominio 14: Adquisición, desarrollo y mantenimiento de los SI.

Figura 16. Análisis de la lista de chequeo del Dominio 14



Fuente: Autor

En el análisis del dominio 14, correspondiente a la adquisición, desarrollo y mantenimiento de los sistemas de información, debido a que no existen desarrollos propios si no contratados, estos contemplan soporte para errores y actualizaciones del sistema, pero MA PEÑALOSA CÍA S.A.S carece de un ambiente de pruebas para realizar las actualizaciones de versiones por lo que se programa estas actualizaciones los fines de semana para no afectar la operatividad de la empresa, en caso de falla se recurre a reestablecer mediante los backups e instaladores anteriores pero con la probabilidad de riesgos para el sistema en general.

Por políticas de SAP el administrador del sistema en este caso la coordinadora del área de sistemas no puede alterar las Bases de Datos de SAP por temas de garantía, por lo que es necesario tomar medidas de precaución para el acceso al servidor de BD cuando no está disponible la coordinadora en casos de incapacidad o vacaciones porque no existe un auxiliar que la apoye en el área.

8.1.11 Dominio 15: Relaciones con Suministradores

Figura 17. Análisis de la lista de chequeo del Dominio 15

Fuente: Autor

Se puede evidenciar que solo se monitorea, revisa y audita la presentación de servicios del proveedor regularmente, pero existen falencias en la calidad del personal de soporte técnico, ya que no existe una política para la ejecución del servicio o una lista de chequeo de las actividades que debe realizar para el caso de los mantenimientos preventivos, donde se detecta olvido o descuido en el servicio, por lo que es indispensable la supervisión de la coordinadora de sistemas. Se ha reportado las falencias a la Gerencia del servicio, pero no se ha tomado medidas correctivas por motivos de amistad con el proveedor.

Se desconocen acuerdos con los proveedores donde se incluya la protección a riesgos de seguridad de la información asociados a los servicios ofrecidos.

No se lleva control del cumplimiento de niveles de servicio de acuerdo a lo establecido en el contrato, ni acuerdos de confidencialidad.

8.1.12 Dominio 16. Gestión de Incidentes

Figura 18. Análisis de la lista de chequeo del Dominio 16

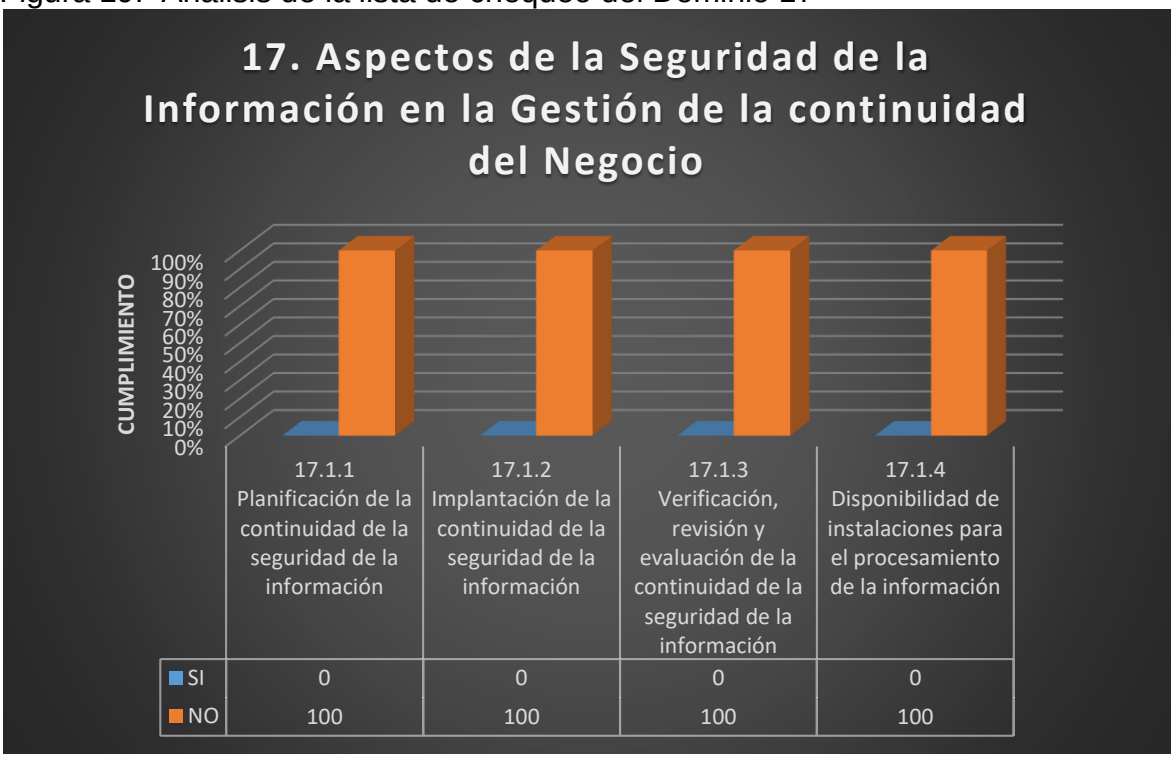
Fuente: Autor

En MA PEÑALOSA CÍA. S.A.S., no existen procedimientos ni canales que permitan informar, gestionar y evaluar incidentes de seguridad de la información de forma rápida. A veces los usuarios por temor a equivocarse al no saber cómo enfrentar incidentes no los reportan. Tampoco una bitácora que permita tener históricos documentados sobre incidentes que permita mitigar los incidentes futuros.

Se debe implementar políticas con la finalidad de que todo el personal de la empresa conozca cómo enfrentar los eventos de seguridad de la información, a quien reportarlas y llevar un control histórico de las ocurrencias de eventos para hacer un análisis e identificar las vulnerabilidades de los sistemas de información, comunicaciones, etc., de tal forma que se apliquen correctivos a tiempo.

8.1.13 Dominio 17. Aspectos de la SI en la Gestión de la Continuidad de Negocio

Figura 19. Análisis de la lista de chequeo del Dominio 17



Fuente: Autor

Teniendo en cuenta los resultados de análisis de la lista de chequeo del dominio 17, MA PEÑALOSA CÍA. S.A.S. necesita analizar y medir las consecuencias las amenazas a la que está expuesta, debe implantar planes de contingencia para asegurar la continuidad de los procesos del negocio y para evitar la indisponibilidad del servicio.

Además, siendo esta la Sede principal, en caso de fallar afecta a las demás sedes por eso es imprescindible contar medidas alternas como canales de internet de backup, servidores en cloud con alta disponibilidad.

8.1.14 Dominio 18. Cumplimiento

Figura 20. Análisis de la lista de chequeo del Dominio 18

Fuente: Autor

La Empresa tiene conocimiento de la normatividad y leyes que debe cumplir para la operatividad del negocio, los cuales se encuentran documentados.

La coordinadora de sistemas mantiene controlado para no incumplir con los derechos de propiedad intelectual, dentro del proceso de mantenimiento preventivo a cada equipo se verifica que no existan software no autorizados instalados y que, en el momento de un formateo, reinstalación o compra de equipos se utilice software licenciados. Pero no hay control sobre software instalado por lo que solo se detecta en los mantenimientos.

En cuanto a protección de datos carece de políticas de confidencialidad y la falta de control de la manipulación de la información, conlleva a riesgos de fuga y robo de información. Violando no solo la ley sino afectando la rentabilidad de la empresa, porque información tan valiosa como clientes potenciales, oportunidades de ventas y precios podrían caer en manos de la competencia.

9. ANÁLISIS DE RIEGOS A TRAVÉS DE MAGERIT

A través de la metodología Magerit, se requiere complementar e identificar más detalladamente información sobre los activos informáticos de MA PEÑALOSA CÍA. S.A.S., los cuales no están inventariados en su totalidad, analizando su grado de valor para la empresa y considerando las amenazas más frecuentes que afectan cada uno de sus activos y su nivel de impacto.

9.1 IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS

Los activos de una empresa, se pueden clasificar según tipo de activo como: Hardware, Software, Datos e información, redes y comunicaciones, personal, localidad y organización. Durante la realización de visitas y entrevistas en las instalaciones de MA PEÑALOSA CÍA. S.A.S., se recolectó información necesaria para la creación del inventario de activos porque la empresa no cuenta con un archivo donde estén inventariados.

A continuación, se clasifican los componentes encontrados para cada tipo de activo.

Tabla 8.Identificación de Activos y sus componentes

Tipo de Activos	Componentes
[OR]Organización	• [PMTO]Proveedor de Mantenimiento De Equipos • [PCOM]Proveedor de Comunicaciones • [PSW]Proveedor de Software • [PSVG]Proveedor de Servicio de Vigilancia • [PIMP]Proveedor de Impresoras • [AIREC]Proveedor de mantenimiento de Aire acondicionado
[DI]Datos e Información	• [BDMAP]Base de datos MA_PENALOSA • [BD_NOM]Base de datos Nomina • [CT]Contratos de servicios y de personal • [FACT]Facturas • [PPPR]Egresos y Recibos de pago • [ECC]Estudios y soportes de crédito de clientes • [BKBD]Backups de base de datos
[IS]Servicios	• [SP]Soporte a usuarios finales • [REPORT]Informes personalizados • [ALMCOMP]Almacenamiento Compartido • [SERVIMP]Impresión y escaneo en red • [SEGPER]Solución Seguridad Perimetral • [SI]Sistema de Información
[SW]Software	• [SAPB1]ERP SAP BUSINESS ONE • [SQL]Motor de BD SQL Server • [OFFICE]Ofimática • [SO]Sistemas Operativos • [ESET]Antivirus ESET Edpoint • [DTW]SAP Business One Data Transfer Workbench

Tipo de Activos	Componentes
Tabla 8. Continuación	• [SAPMV]Solución SAP móvil • [TNS]Nómina TNS
[HW]Hardware	• [SERVER]Servidores • [CELULAR]Smartphone • [IMPSCAN]Impresoras Multifuncionales • [TABLET]Tabletas • [PC]Equipos • [FTG]Fortigate • [EA] Equipos de red
[COM]Comunicaciones	• [WIFI]Red Wifi • [LAN]Red LAN • [WAN]Red WAN
[AUX]Elementos Auxiliares	• [UPS]Sistema de alimentación Interrumpida • [CBL]Cableado de datos • [ELEC]Cableado eléctrico • [VOZ]Cableado telefónico
[SS]Servicios Subcontratados	• [EMAIL]Correo electrónico • [MPLS]Conectividad Red Sede Principal y Sedes • [MTOPC]Mantenimiento de equipos • [INTERNET]Conectividad de internet • [LFMV]Línea Fija – Celulares • [TONER]Alquiler de impresoras
[L]Instalaciones	• [INFRA]Infraestructura Física • [CTEQ]Cuarto de equipos • [ZONA]Zona de accesos, seguridad, oficinas y equipos
[P]Personal	• [ADMIN]Administrador del Sistema • [GERENTE]Gerente • [USER]Usuarios finales

Fuente: Autor

9.1.1 Descripción de activos informáticos. De acuerdo a los activos relacionados, se describe cada uno de ellos para tener más conocimiento acerca de estos y completar la investigación.

Tabla 9. Descripción de Activos

Tipo de Activo	Nombre	Descripción
Organización	Proveedor de Mantenimiento de Equipo	Empresa contratada para proveer el mantenimiento correctivo y preventivo de los equipos de cómputo y equipos de red.
	Proveedor de Comunicaciones	Empresa contratada para proveer los servicios de telefonía fija, telefonía móvil, internet y red MPLS
	Proveedor de Software	Software que comprende varias herramientas para desarrollar labores de oficina. Existen en la Empresa Open Office, Microsoft Office 2003, Microsoft Office 2007, Microsoft Office 2010, Microsoft Office 2013 y office 365.
	Proveedor de servicio de Vigilancia, Alarma y Cámaras de seguridad.	Empresa de vigilancia privada, existe sensores en la parte de bodega y cámara de seguridad en el entono perimetral, para visualizar el acceso y movimientos del personal y usuarios externos dentro de la empresa.

Tipo de Activo	Nombre	Descripción
Tabla 9. Continuación		
	Proveedor de impresoras	Proveedor de servicio alquiler de impresoras, garantizando la calidad de impresión de los documentos, escaneo de documentos y copiado.
	Proveedor de Servicios de Aire acondicionado	Los proveedores de servicio de aire acondicionado, son empresas certificadas y con personal profesional en el área.
Datos e Información	Información Física	Es toda la información física de procesos y servicios que se ofrecen en la empresa, estos documentos pueden ser impresos o formatos de papelería, como contratos de servicios, contratos de recursos humanos, liquidaciones, hojas de vida, facturas, egresos, recibos de pago, estudios y soportes de créditos de los clientes.
	Información Digital	Contiene toda la documentación de manera digital de las ventas y procesos de informes financieros que se registran en los equipos, backups, CD-ROM, DVD, USB, Word, Excel, PDF.
	Base de Datos	Esta información toma relevancia en los asuntos de la empresa ya que las bases de datos contienen una colección de datos la cual se relacionan entre sí y por estar estructuradas de manera que permiten el acceso rápido y la manipulación de estos datos, no están dentro del área de documentos de registros, pero sí se le debe dar el lugar entre los activos de información tipo datos. Base de Datos MA_PENALOSA: contiene información de socios de negocios (clientes-proveedores), ventas, compras, inventario (incluye precios). Base de Datos Nomina: información de datos personales de empleados de la empresa, sueldo, información del contrato, etc.
Servicios	Soporte a usuarios finales	Proveer el software y hardware necesario para la realización optima de actividades del área, brindar una infraestructura de red para la comunicación interna y externa de la empresa, atento a solucionar cualquier eventualidad que se presente y afecte el sistema.
	Informes personalizados	Informes de indicadores, de inventario, de ventas entre otros que ayuden a los usuarios sobre todo a los líderes de áreas poder analizar información y ejecutar tácticas de mercadeo.
	Almacenamiento Compartido	El área de sistemas debe proveer el servicio de red y el espacio necesario para almacenar y compartir información de forma segura y rápida.
	Impresión y escaneo en red	La disponibilidad del servicio de impresión y escaneo en red es muy importante, ya que de ello depende la generación de la factura al cliente, la gestión de cartera, brindar información al cliente del estado de saldo y los demás procesos que necesitan de soporte físico y firmas para su validez.
	Solución Seguridad Perimetral	Proteger la red de amenazas e intrusiones, monitorear y controlar la navegación de internet asignando perfiles según necesidades del usuario.
	Sistema de Información	Garantizar la disponibilidad del Sistema de Información, gestión de licencias, actualizaciones
Software	SAP Business One	Software contable utilizado para el desarrollo de las actividades diarias de la empresa. Comprende módulos de: Ventas, Compras, Inventarios, Producción, Recursos Humanos, Socios de Negocios.

Tipo de Activo	Nombre	Descripción
Tabla 9. Continuación		
	SQL Server 2008R2	Motor de Base de datos utilizada para el ERP
	Ofimática	Software que comprende varias herramientas para desarrollar labores de oficina. Existe en la Empresa Open Office, Microsoft Office 2003, Microsoft Office 2007, Microsoft Office 2010, Microsoft Office 2013 y office 365.
	Sistemas Operativos	Para los equipos que operan dentro de la Sede Principal de MA PEÑALOSA CÍA S.A.S, se encuentran sistemas operativos como: Windows 7 pro, Windows 8 pro, Windows 8.1 pro, Windows 10 Home, Windows server 2003, Windows Server 2008 Standard, Windows 2008 R2 Standard.
	Antivirus	ESET Endpoint Antivirus para PC's, consola Administrativa del Antivirus, ESET File Security para servidores, encargados de detectar, analizar y desinfectar amenazas presentadas en equipos.
	SAP Business One Data Transfer Workbench	Herramienta adicional a SAP para subir archivos planos al sistema.
	Solución SAP Móvil	Addon integrado al ERP para brindar al usuario otra forma más fácil y rápida de acceder al sistema.
	Nómina TNS	Software utilizado para llevar los registros de pagos al trabajador de manera quincenal, descuentos de préstamos, registro de vacaciones, liquidaciones, incapacidades, Pagos de Aportes y parafiscales.
Hardware	Servidores	Los servidores se encuentran en la sede principal. Actualmente se cuenta con tres servidores físicos: • Servidor principal: servidor de base de datos y servidor de aplicaciones • Servidor de archivos: almacenamiento de carpetas compartidas por usuarios • Servidor virtualizado: servidor de Terminal Services y DNS.
	Smartphone	Dispositivos móviles para comunicación con proveedores, clientes, entre empleados y acceder al aplicativo móvil de SAP
	Impresoras Multifuncionales	Impresora a color disponible para impresiones de catálogos comerciales, documentación y avisos de calidad.
	Tabletas	Equipo móvil para acceder al aplicativo SAP y a la información de la empresa
	Equipos	Equipo de escritorio o portátil para acceder al aplicativo SAP y a la información de la empresa
	Fortigate	Dispositivo que sirve para proteger las redes de ataques, intrusiones, spam entre otras amenazas informáticas.
	Equipos de red	Equipos que permitan crear las redes WIFI, LAN y WAN de la empresa.
Redes y Comunicaciones	Red WIFI	Red que permite conectarse de forma inalámbrica de un equipo portátil o Smartphone a otro dispositivo que suministra la señal inalámbrica de MA PEÑALOSA CÍA S.A.S.
	Red LAN	Red necesaria para conectar y comunicar todos los dispositivos de red, equipos, servidores.
	Red WAN	Red necesaria para conectar y comunicar todas las sedes.

Tipo de Activo	Nombre	Descripción
Tabla 9. Continuación		
Elementos Auxiliares	Sistema de alimentación interrumpida	Equipos para proteger los equipos de los altibajos eléctricos y en caso de falta de electricidad permitir que los usuarios puedan guardar la información y realizar apagados de equipos correctamente.
	Cableado de datos	Cableado que soporta la red de datos de la empresa
	Cableado eléctrico	Cableado que soporta la red eléctrica de la empresa.
	Cableado telefónico	Cableado que soporta las comunicaciones telefónicas de la empresa.
Servicios Subcontratados	Correo electrónico	Servicio necesario de comunicación con proveedores, clientes y entre el personal de la empresa.
	Conectividad Red Sede PPAL y otras sedes	Servicio para garantizar la conectividad entre la Sede Principal y las demás sedes a través de la red MPLS
	Mantenimiento de equipos	Servicio de mantenimiento preventivo y correctivo para preservar el buen funcionamiento de los equipos.
	Conectividad de internet	Servicio requerido para todas las áreas de la empresa con el fin de acceder a portales de proveedores para compras, uso de correo, conexión entre sedes, conexión de usuarios remotos, acceso a portales bancarios, DIAN, Comfanorte, Parafiscales, etc.
	Telefonía fija y móviles	Servicio necesario para la comunicación del personal de la empresa con clientes, proveedores.
	Alquiler de impresoras	Se tiene contratado el servicio de alquiler de impresoras para el trabajo pesado de impresión de facturas en las bodegas de todas las sedes y en la parte de administrativa donde el flujo de impresión es alto.
Instalaciones	Infraestructura Física	MA PEÑALOSA CÍA S.A.S, cuenta con una infraestructura física en dos etapas, una construcción muy antigua y deteriorada; otra parte nueva con una infraestructura muy resistente a sismos.
	Cuarto de equipos	Centro de datos destinado para equipos críticos que soportan la infraestructura tecnológica.
	Zona de accesos Seguridad, Oficina, Equipos	Las zonas de acceso no tienen privacidad respecto a donde se encuentran los equipos Informáticos. Aunque en el área administrativa está más limitado el acceso debido a los cubículos de cada puesto de trabajo.
Personal	Administrador del Sistema	Profesional en ingeniería de sistemas, encargada de controlar cada uno de los procesos informáticos y redes de comunicaciones
	Gerente	Es el responsable del buen funcionamiento de la empresa.
	Usuarios	Personal autorizado en la Empresa para ingresar a los sistemas informáticos y redes para el desarrollo y ejecución de las actividades asignadas en la empresa

Fuente: Autor

9.1.2 Inventario de Activos de MA PEÑALOSA CÍA. S.A.S.

Tabla 10. Activos de MA PEÑALOSA CÍA. S.A.S.

Código	Nombre de activo	Tipo de Activo	Función	Ubicación	Propietario / custodio	Cant.
PMTO	Proveedor de Mtto. de equipos	Organización	Proveer mantenimiento de equipos informáticos	N/A	N/A	1
PCOM	Proveedor de comunicaciones	Organización	Proveer internet, telefonía fija y móvil, red MPLS	N/A	N/A	2
PSW	Proveedor de Software	Organización	Proveer Soporte de Software, licencias y actualizaciones	N/A	N/A	4
PSVG	Proveedor de Servicio de vigilancia	Organización	Garantizar la seguridad de la empresa	N/A	N/A	1
PIMP	Proveedor de impresoras	Organización	Proveer impresoras para trabajo pesado de impresión	N/A	N/A	1
AIRE	Proveedor de Mtto. de aires acondicionados	Organización	Proveer mantenimiento de aires acondicionados	N/A	N/A	1
BDMAP	BD MA_PENALOSA	Datos e información	Base de datos de información registrada en el software SAP.	Rack Principal	Coordinadora de sistemas	1
BDNOM	BD Nomina	Datos e información	Base de datos de información de personal registrada en el software TNS.	Rack Principal	Coordinadora de sistemas	1
CT	Contratos de servicios y de personal	Datos e información	Contiene la documentación pertinente a las hojas de vida de los trabajadores, contratos de los trabajadores y de proveedores	Archivo físico	Archivista	>50
FT	Facturas	Datos e información	Copia de factura de ventas de mercancía de MA PEÑALOSA CÍA S.A.S	Archivo físico	Archivista	>1000
PPPR	Egresos y recibos de pago	Datos e información	Copia de registros de pagos recibidos de clientes y pagos efectuados generados en el sistema para proveedores.	Archivo físico	Archivista	>1000

Código	Nombre de activo	Tipo de Activo	Función	Ubicación	Propietario / custodio	Cant.
Tabla 10. Continuación						
ECC	Estudios y soporte de créditos de clientes	Datos e información	Documentación sobre estudios de crédito de cliente, pagares, etc.	Archivo físico	Archivista	>50
BKBD	Backups	Datos e información	Backup para el respaldo de información de BD	Rack Ppal., Google Drive	Coordinadora de sistemas	20
SP	Soporte a usuarios finales	Servicios	Proveer el sw y hw al usuario para la realización de actividades del área, brindar una infraestructura de red para las comunicaciones de la empresa, atento a solucionar cualquier eventualidad que se presente y afecte el sistema.	N/A	Coordinadora de sistemas	N/A
REPORT	Informes personalizados	Servicios	Informes de indicadores, de inventario, de ventas entre otros que ayuden a los usuarios sobre todo a los líderes de áreas poder analizar información y ejecutar tácticas de mercadeo.	N/A	Coordinadora de sistemas	N/A
ALMCOM	Almacenamiento compartido	Servicios	Proveer el servicio de red y el espacio necesario para almacenar y compartir información de forma segura y rápida.	N/A	Coordinadora de sistemas	N/A
SERVIMP	Impresión y escaneo en red	Servicios	Supervisar la disponibilidad y calidad del servicio de impresión y escaneo en red	N/A	Coordinadora de sistemas	N/A
SEGPER	Solución seguridad perimetral	Servicios	Proteger la red de amenazas e intrusiones, monitorear y controlar la navegación de internet asignando perfiles según necesidades del usuario.	N/A	Coordinadora de sistemas	N/A

Código	Nombre de activo	Tipo de Activo	Función	Ubicación	Propietario / custodio	Cant.
Tabla 10. Continuación						
SI	Sistema de información	Servicios	Garantizar la disponibilidad del Sistema de Información, gestión de licencias, actualizaciones	N/A	Coordinadora de sistemas	2
SAPB1	SAP BUSINESS ONE	Software	Gestionar Ventas, Compras, Inventarios, Producción, Recursos Humanos, Clientes, Proveedores	Servidor ppal. de Rack principal	Coordinadora de sistemas	33
SQL	Motor de BD SQL Server	Software	Gestionar Base de Datos de SAP	Servidor ppal. de Rack principal	Coordinadora de sistemas	1
OFFICE	Ofimática	Software	Apoyar ejecución y organización de tareas administrativas	Equipos de usuarios finales	Coordinadora de sistemas	10
SO	Sistemas Operativos	Software	Gestionar recursos de hardware	Equipos de usuarios finales y servidores	Coordinadora de sistemas	43
ESET	Antivirus ESET	Software	Detectar y prevenir amenazas	Equipos de usuarios finales y servidores	Coordinadora de sistemas	43
DTW	SAP B1 DTW	Software	Cargar archivos planos de forma masiva a SAP	Servidor de Rack principal y equipos de compras	Coordinadora de sistemas	3
SAPMV	Solución SAP móvil	Software	Gestionar Ventas, Inventarios, Clientes a través de Smartphone	Smartphone de usuarios remotos	Coordinadora de sistemas	7
TNS	Nomina TNS	Software	Gestionar de recursos humanos	Servidor DNS de Rack principal	Coordinadora de sistemas	1
SERVPPAL	Servidor Principal	Hardware	Soportar bases de datos y aplicaciones	Rack Principal	Coordinadora de sistemas	1
SERVTD	Servidor Terminal Server- DNS	Hardware	Soportar usuarios que acceden de forma remota a la aplicación	Rack Principal	Coordinadora de sistemas	1
SARCH	Servidor de Archivos	Hardware	almacenar carpetas compartidas por usuarios	Rack Principal	Coordinadora de sistemas	1

Código	Nombre de activo	Tipo de Activo	Función	Ubicación	Propietario / custodio	Cant.
Tabla 10. Continuación						
CELULAR	Smartphone	Hardware	Dispositivo celular móvil para comunicaciones con clientes proveedores, demás personal y acceder a la solución de SAP móvil	N/A	Usuarios	20
IMPSCAN	Impresoras multifuncional	Hardware	Imprimir a color catálogos comerciales y documentación de área de calidad	Ferretería	Coordinadora de sistemas	1
TABLET	tabletas	Hardware	Equipos móviles de la empresa	N/A	Asesores ferreteros, Gerente y Coordinadora de sistemas	4
LAPTOP	Equipo portátil	Hardware	Computadores portátiles de la empresa	Todas las áreas de la empresa	Usuarios, Gerente y Coordinadora de sistemas	15
PC	Equipo de escritorio	Hardware	Computadores de escritorio de la empresa	Todas las áreas de la empresa	Usuarios, Gerente y Coordinadora de sistemas	13
ALLONE	Equipo todo en uno	Hardware	Computadores todo en uno de la empresa	Caja Principal	Usuario, Gerente y Coordinadora de sistemas	1
FTG	Fortigate	Hardware	Proteger las redes de ataques, intrusiones, spam entre otras amenazas informáticas.	Rack Principal	Coordinadora de sistemas	1
WIFI	Red WIFI	Comunicaciones	Utilizada por los equipos móviles para acceder a los recursos de la red de la empresa	Rack secundario	Coordinadora de sistemas	1
LAN	Red LAN	Comunicaciones	Red LAN corporativa de la empresa	Rack principal, rack secundario, swcons-fer	Coordinadora de sistemas	1
WAN	Red WAN	Comunicaciones	Red WAN de la empresa	Rack principal	Coordinadora de sistemas	1
UPSEQ	UPS Equipos	Elementos Auxiliares	Sistema de energía de soporte en caso de fallas para cada uno de los equipos	Todas las áreas de la empresa	Coordinadora de sistemas	20

Código	Nombre de activo	Tipo de Activo	Función	Ubicación	Propietario / custodio	Cant.
Tabla 10. Continuación						
UPSCOM	UPS Rack Ppal. y secundario	Elementos Auxiliares	Sistema de energía de soporte en caso de fallas para los racks	Rack Ppal. y secundario	Coordinadora de sistemas	2
CBL	Cableado de datos	Elementos Auxiliares	Cableado que soporta la red de datos de la empresa	Todas las áreas de la empresa	Coordinadora de sistemas	1
ELE	Cableado eléctrico	Elementos Auxiliares	Cableado que soporta la red eléctrica de la empresa.	Todas las áreas de la empresa	Coordinadora de sistemas	1
VOZ	Cableado telefónico	Elementos Auxiliares	Cableado que soporta las comunicaciones telefónicas de la empresa.	Todas las áreas de la empresa	Coordinadora de sistemas	1
EMAIL	Correo electrónico	Servicios subcontratados	Servicio necesario de comunicación con proveedores, clientes y entre el personal de la empresa.	N/A	Coordinadora de sistemas	1
MPLS	Conectividad MPLS	Servicios subcontratados	Garantizar la conectividad entre la Sede Principal y las demás sedes	N/A	Coordinadora de sistemas	1
MTOPC	Mantenimiento de equipos	Servicios subcontratados	Servicio de mantenimiento preventivo y correctivo para preservar el buen funcionamiento de los equipos.	N/A	Coordinadora de sistemas	1
INTERNET	Conectividad de Internet	Servicios subcontratados	Acceder a portales de proveedores, uso de correo, conexión entre sedes, conexión de usuarios remotos, acceso a portales bancarios, DIAN, Comfanorte, Parafiscales, etc.	N/A	Coordinadora de sistemas	2
LFMV	Telefonía fija y móvil	Servicios subcontratados	Servicio necesario para la comunicación del personal de la empresa con clientes, proveedores.	N/A	Coordinadora de sistemas	1

Código	Nombre de activo	Tipo de Activo	Función	Ubicación	Propietario / custodio	Cant.
Tabla 10. Continuación						
TONER	Alquiler de impresoras	Servicios subcontratados	Servicio de alquiler de impresoras para el trabajo pesado de impresión de facturas en las bodegas de todas las sedes y en la parte de administrativa donde el flujo de impresión es alto.	N/A	Coordinadora de sistemas	2
INFRA	Infraestructura física	Instalaciones	Instalaciones físicas de MA PEÑALOSA CÍA S.A.S	N/A	Gerente	1
CTEQ	Cuarto de equipos	Instalaciones	Espacio físico donde se ubican los racks de comunicaciones	N/A	Coordinadora de sistemas	0
ZONA	Zona de accesos, seguridad, oficinas y equipos	Instalaciones	Zonas destinadas para cada departamento de la empresa	N/A	Gerente, Coordinadora de sistemas y usuarios finales	9
ADMIN	Administrador del sistema	Personal	Profesional en ingeniería de sistemas, encargada de controlar cada uno de los procesos informáticos	N/A	N/A	1
GERENTE	Gerente	Personal	Es el responsable del buen funcionamiento de la empresa.	N/A	N/A	1
USER	Usuarios finales	Personal	Personal autorizado para interactuar con los sistemas de información en la ejecución de sus actividades asignadas dentro de la empresa	N/A	N/A	43

Fuente: Autor

9.1.3 Dimensiones de Valoración de Activos. Para evaluar cada uno de los activos informáticos, se establecieron como dimensiones de valoración, las características de la seguridad de la información, respondiendo a preguntas planteadas dentro de la auditoria de seguridad informática por la autora Ester Chicano Tejada[17] tales como:

9.1.3.1 Disponibilidad [D]

¿Qué importancia tiene un activo sino estuviera disponible?

Para evaluar según esta dimensión, se debe considerar con un valor alto, cuando la indisponibilidad del activo puede afectar la continuidad de las operaciones totales o parciales de la empresa. Si por el contrario el activo al estar durante un período de tiempo sin servicio no afecta las actividades del usuario pueden valorar como bajo.

9.1.3.2 Integridad [I]

¿Qué importancia tiene el activo si los datos fueran modificados fuera de control?
Se debe considerar con un valor alto, cuando la alteración o error en los activos informáticos afecte gravemente la empresa y su recuperación no sea fácil y requiere de tiempo o no exista forma de restablecerlo. Si por el contrario el activo al ver cambios no genera impacto sobre las actividades del usuario pueden valorar como bajo.

9.1.3.3 Confidencialidad [C]

¿Qué importancia tendría el activo si fuera conocido por personas no autorizadas?
Se debe considerar con un valor alto, si la divulgación o la exposición pública de los activos informáticos de la empresa pueden ocasionar consecuencias de lo contrario puede ser valorado como bajo.

9.1.3.4 Autenticidad [A]

¿Qué importancia tiene el activo si quien accede a él no es realmente quien se cree que es?

[17] CHICANO TEJADA, Ester. Auditoría de seguridad informática. IFCT0109. [En línea], [consultado el 2 de mayo de 2018]. Disponible en Internet: https://books.google.com.co/books?isbn=8416433232

Se considera alto si al acceder un usuario a los activos no puede controlarse ocasionando graves afectaciones para la empresa, de lo contrario es baja.

9.1.3.5 Trazabilidad [T]

¿Qué importancia tiene el activo si no queda constancia del uso del mismo?

Para evaluar según esta dimensión, el activo debe disponer de algún registro para auditar sino sería difícil analizar cómo se originó, responsables y procesos que se llevaron a cabo.

9.1.4 Niveles de valoración de dimensiones de Activos. De acuerdo a las dimensiones establecidas anteriormente, adicional se debe definir una escala de valores para ser evaluadas a nivel de análisis cualitativo o cuantitativo. A continuación, se define los tipos de análisis para aplicar:

– En el análisis cualitativo, la valoración de los activos se aplica por medio de niveles de importancia. Para el proyecto se aplicará: Muy alto, Alto, Medio, Bajo y despreciable

– El análisis cuantitativo: la valoración de los activos se aplica por medio de escala numérica. Para el proyecto se aplicará: valores de 0 a 10, donde 0 se considera como despreciable y 10 como la calificación más alta e importante atender.

En la tabla 11, se detalla la forma de evaluación para los activos de la empresa de MA PEÑALOSA CÍA. S.A.S.

Tabla 11. Valoración de dimensiones de activos

VALOR CUANTITATIVO	VALOR CUALITATIVO	CRITERIO	DIMENSIONES
0	Despreciable	Daño insignificante para la empresa	D I C A T
1-3	Bajo	Daño medio para la empresa	
4-6	Medio	Daño medio para la empresa	
7-9	Alto	Daño grave para la empresa	
10	Muy alto	Daño muy grave para la empresa	

Fuente: Autor

9.1.5 Valoración de Activos. A continuación, se evaluarán los activos de la MA PEÑALOSA CÍA. S.A.S. con respecto a las dimensiones correspondientes a la integridad, confidencialidad, disponibilidad, trazabilidad y autenticidad, bajo los criterios establecidos.

Tabla 12. Valoración de activos - Estimación del impacto

Tipo Activo	Código	Nombre de activo	Dimensiones					Vr Cualitativo	Vr Cuantitativo
			D	I	C	A	T		
OR	PMTO	Proveedor de Mtto. de equipos	10	8	10	1	1	6	Medio
OR	PCOM	Proveedor de comunicaciones	10	4	9	3	2	6	Medio
OR	PSW	Proveedor de Software	10	5	10	2	5	6	Medio
OR	PSVG	Proveedor de Servicio de vigilancia	10	4	4	1	3	4	Medio
OR	PIMP	Proveedor de impresoras	10	4	1	0	0	3	Bajo
OR	AIRE	Proveedor de Mtto. de aires acondicionados	6	4	1	0	4	3	Bajo
DI	BDMAP	BD MA_PENALOSA	10	10	10	10	10	10	Muy Alto
DI	BDNOM	BD Nomina	10	10	10	10	10	10	Muy Alto
DI	CT	Contratos de servicios y de personal	10	10	10	10	10	10	Muy Alto
DI	FT	Facturas	10	10	10	10	10	10	Muy Alto
DI	PPPR	Egresos y recibos de pago	10	10	10	10	10	10	Muy Alto
DI	ECC	Estudios y soporte de créditos de clientes	10	10	10	10	10	10	Muy Alto
DI	BKBD	Backups	10	10	10	10	10	10	Muy Alto
IS	SP	Soporte a usuarios finales	10	2	0	2	3	3	Bajo
IS	REPORT	Informes personalizados	8	9	10	0	0	5	Medio
IS	ALMCOM	Almacenamiento compartido	5	8	10	9	7	8	Alto
IS	SERVIMP	Impresión y escaneo en red	10	1	3	2	1	3	Bajo
IS	SEGPER	Solución seguridad perimetral	7	4	6	5	6	6	Medio
IS	SI	Sistema de información	10	10	10	10	10	10	Muy Alto
SW	SAPB1	SAP BUSINESS ONE	10	10	10	10	10	10	Muy Alto
SW	SQL	Motor de BD SQL Server	10	10	10	10	10	10	Muy Alto

Tipo Activo	Código	Nombre de activo	Dimensiones					Vr Cualitativo	Vr Cuantitativo
			D	I	C	A	T		
Tabla 11. Continuación									
SW	OFFICE	Ofimática	6	3	0	0	0	2	Bajo
SW	SO	Sistemas Operativos	9	9	6	7	7	8	Alto
SW	ESET	Antivirus ESET	9	5	0	1	3	4	Medio
SW	DTW	SAP B1 DTW	5	6	0	8	9	6	Medio
SW	SAPMV	Solución SAP móvil	2	7	10	9	9	7	Alto
SW	TNS	Nomina TNS	6	9	10	8	7	8	Alto
HW	SERVPPAL	Servidor Principal	10	10	10	10	10	10	Muy Alto
HW	SERVTERDNS	Servidor Terminal Server- DNS	7	4	5	8	9	7	Alto
HW	SARCH	Servidor de Archivos	7	8	10	8	9	8	Alto
HW	CELULAR	Smartphone	4	3	1	0	0	2	Bajo
HW	IMPSCAN	Impresoras multifuncional	1	6	0	0	0	1	Bajo
HW	TABLET	tabletas	6	3	5	5	3	4	Medio
HW	LAPTOP	Equipo portátil	6	4	5	6	3	5	Medio
HW	PC	Equipo de escritorio	6	4	6	6	3	5	Medio
HW	ALLONE	Equipo todo en uno	6	4	6	7	3	5	Medio
HW	FTG	Fortigate	10	10	7	9	10	9	Alto
COM	WIFI	Red WIFI	4	5	5	9	8	6	Medio
COM	LAN	Red LAN	10	7	6	9	3	7	Alto
COM	WAN	Red WAN	5	4	7	6	5	5	Medio
AUX	UPSEQ	UPS Equipos	2	1	0	0	4	1	Bajo
AUX	UPSCOM	UPS Rack Ppal. y secundario	6	2	0	0	4	2	Bajo
AUX	CBL	Cableado de datos	7	9	0	0	1	3	Bajo
AUX	ELE	Cableado eléctrico	7	8	0	0	1	3	Bajo
AUX	VOZ	Cableado telefónico	6	5	0	0	1	2	Bajo
SS	EMAIL	Correo electrónico	5	4	9	6	8	6	Medio
SS	MPLS	Conectividad MPLS	6	2	5	3	1	3	Bajo
SS	MTOPC	Mantenimiento de equipos	9	4	9	2	5	6	Medio
SS	INTERNET	Conectividad de Internet	6	2	5	3	1	3	Bajo
SS	LFMV	Telefonía fija y móvil	10	2	1	0	0	3	Bajo
SS	TONER	Alquiler de impresoras	10	6	0	0	0	3	Bajo
L	INFRA	Infraestructura física	7	10	0	0	0	3	Bajo
L	CTEQ	Cuarto de equipos	9	9	10	8	8	9	Alto

Tipo Activo	Código	Nombre de activo	Dimensiones					Vr Cualitativo	Vr Cuantitativo
			D	I	C	A	T		

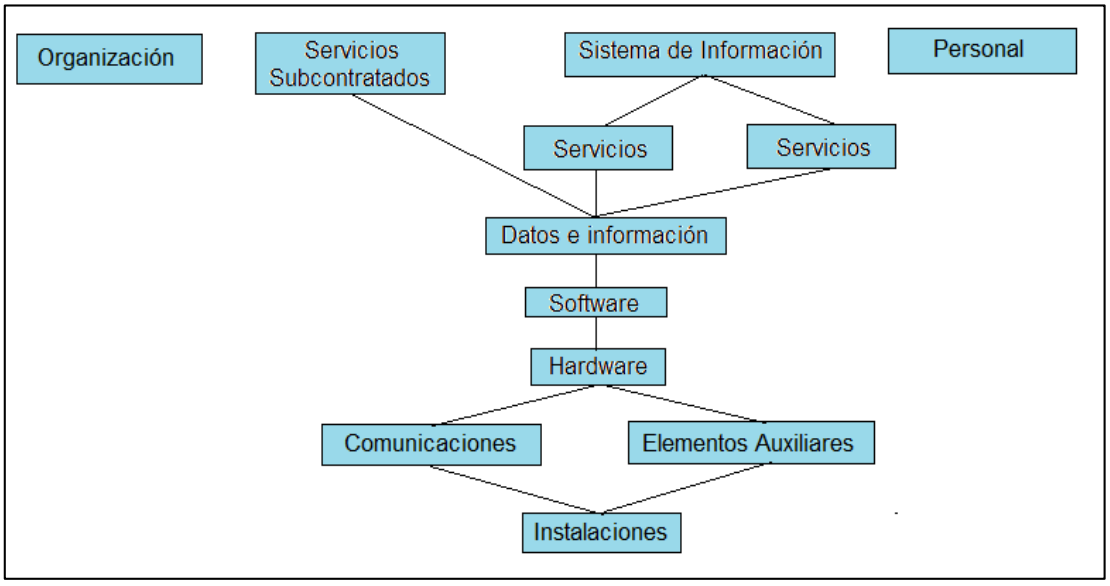
Tabla 11. Continuación

L	ZONA	Zona de accesos, seguridad, oficinas y equipos	2	6	4	0	3	3	Bajo
P	ADMIN	Administrador del sistema	10	8	10	5	3	7	Alto
P	GERENTE	Gerente	7	0	0	0	0	1	Bajo
P	USER	Usuarios finales	3	3	5	8	8	5	Medio

Fuente: Autor

9.1.6 Dependencia de Activos. La metodología Magerit propone dentro de la etapa del análisis de riesgos establecer dependencias entre los activos informáticos de forma jerárquica. Al analizar la relación entre los activos inventariados, se pudo identificar la dependencia entre ellos y el flujo de afectación cuando se presente una amenaza en el activo inferior, el cual traerá repercusiones sobre el activo superior. En la figura 21, se observa el nivel jerárquico.

Figura 21. Dependencia de activos



Fuente: Autor

9.2 IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS

9.2.1 Tipo de Amenazas. Las amenazas son todos aquellos aspectos que pueden afectar a los activos informáticos, ya sean personas de forma intencional o por errores, condiciones ambientales, defectos de fábrica, entre otros. El catálogo de elementos publicado en el libro 2 de Magerit v3[18], describe detalladamente las amenazas a las que pueden estar expuestos los activos informáticos según el tipo de activo. A continuación, se mencionan:

La clasificación de las amenazas que propone MAGERIT:

- DESASTRES NATURALES: Ocasionado por eventos o fenómenos de la naturaleza. Como, por ejemplo: incendios, daños por causa de agua debido a inundaciones, o fenómenos de tipo climático, terremotos, deslizamiento de tierra, contaminación ambiental, erupciones, etc.

- DE ORIGEN INDUSTRIAL: Sucesos ocurridos de forma accidental, producidos por humanos al ejecutar una labor de tipo industrial. En estos tipos de amenazas se contemplan incendios, fugas de agua que provocan inundaciones, accidentes de tráfico, explosiones, sobrecarga eléctrica, contaminación como polvo, radiaciones o averías de origen físico o lógico, fallos de energía eléctrica, malas condiciones ambientales como exceso de calor o humedad, daños en el medio de transmisión de datos o por agotamiento de suministros esenciales como tóner, papel o degradación de los medios de almacenamiento de información como discos, USB.

- ERRORES Y FALLO NO INTENCIONADOS: Errores causados por las personas por desconocimiento o por falta de concentración a la hora de ejecutar una actividad. Dentro de estas amenazas se consideran errores de uso por procesos mal ejecutados, digitación de información doble, borrar accidentalmente un archivo, errores de instalación, configuración u operación causados por el administrador, propagación de virus no intencionados, errores de envíos de información por rutas establecidas incorrectas, fugas, alteraciones o destrucción de información accidentalmente, vulnerabilidades y fallas de los software, pérdida o robo de equipos, problemas generados en los mantenimiento de equipo, insuficiente recursos por la carga de trabajo ejercido y ausencia de personal por incapacidad.

[18] MAGERIT – versión 3.0Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos. [En línea], [consultado el 2 de mayo de 2018]. Disponible en Internet: https://www.ccn-cert.cni.es/documentos-publicos/ 1793-magerit-libro-iii-tecnicas/file.html

- ATAQUES INTENCIONADOS: Daños causados por personas inescrupulosas con el objetivo de destruir, alterar o desestabilizar un proceso por motivos personales para su beneficio o satisfacción. Tales como manipulación de registros, alteración de configuraciones, suplantación de identidad, alteración, destrucción o divulgación de la información, robo de equipos o documentos, extorsión, abuso de privilegios de acceso, uso de información utilización de recursos para fines personales, propagación de virus intencionalmente, accesos no autorizados al uso de activos, interceptar datos a través del análisis de tráfico, copia ilegal de software, sabotaje de equipos, saturación del sistema ocasionando denegación del servicio, destrucción de activos por vandalismo o terrorismo, alteración de programas, invasión de las instalaciones físicas, ingeniería social, huelgas de personal, absentismo laboral.

9.2.2 Identificación de Amenazas. A continuación, se relacionan las amenazas y vulnerabilidades que pueden afectar los diferentes tipos de activos, de acuerdo a los orígenes descritos en el numeral 9.2.1

Tabla 13**.** Identificación de amenazas de acuerdo al activo

ORIGEN	AMENAZA	VULNERABILIDADES
ORGANIZACIÓN		
Desastre Natural[N]	Contaminación ambiental	El proveedor de mantenimientos de equipos, aires acondicionados e impresoras no siempre usa implementos de protección de seguridad para ejecutar sus actividades, como tapabocas.
Origen Industrial[I]	Derrumbes	Debido a la mala infraestructura física, el proveedor debe contar con elementos de protección de seguridad como guantes, casco, escaleras y arnés dependiendo de la actividad a realizar. A veces el proveedor no atiende a las recomendaciones o no posee curso de altura.
DATOS E INFORMACIÓN		
Desastres Naturales[N]	Fuego [N.1]	Este tipo de amenaza atenta gravemente contra la información digital y principalmente la física y muy difícil de reparar.
	Daños por agua [N.2]	Una de las falencias de la infraestructura de MA PEÑALOSA, es su infraestructura física, las goteras e inundaciones ocasionadas por lluvias afecta este activo.
Origen Industrial[I]	Fuego [I.1]	Dentro del inventario en la bodega de MA PEÑALOSA CÍA S.A.S, existen algunos productos que pueden ser inflamables por lo que se requiere de precaución en su manipulación. Cerca del rack principal no existe un extintor que pueda ayudar a controlar la amenaza en caso de presentarse.

ORIGEN	AMENAZA	VULNERABILIDADES
	Tabla 13. Continuación	
	Fluctuaciones o sobrecargas eléctricas	Se evidencia muchos altibajos en el suministro eléctrico, se han presentado cortos eléctricos dentro de las instalaciones, los cuales deben revisarse porque puede ocasionar daños lógicos en equipos y por ende afectación de la información.
	Contaminación Mecánica [I.3]	Dentro de la bodega se encuentra el rack principal y algunas áreas de trabajo con equipos informáticos, estos pueden verse expuestos a productos tipo polvo como cementos y pegos de cerámica que pueden afectar la disponibilidad de algunos soportes de información.
	Cortes del suministro eléctrico [I.6]	Debido a las fluctuaciones o sobrecargas de energía ha provocado cedes de alimentación de potencia que por falta de mantenimiento de las UPS no cubren como debería a los equipos o no son suficientes para todos los equipos. Por lo tanto, el no apagado correcto de los equipos provoca daños o pérdidas de información.
	Condiciones inadecuadas de temperatura o humedad [I.7]	Al no disponer de un centro de datos para los activos críticos que soportan la infraestructura tecnológica, no están en condiciones adecuadas de temperatura y están expuestos a altas temperaturas que podrían ocasionar daños en los equipos.
	Degradación de los soportes de Almacenamiento de la Información [I.10]	No hay controles de seguridad para mantener la disponibilidad de los soportes de información y no se deterioren con el paso del tiempo.
Errores y fallos no intencionados[E]	Alteración accidental de la Información [E.15]	La información puede ser alterada por error humano, afectando muchas veces su integridad. Es necesario tener respaldo de este activo para poder recuperar en caso de presentarse esta amenaza.
	Destrucción de la Información [E.18]	La información puede ser eliminada por error humano, afectando la disponibilidad. Es necesario tener respaldo de este activo para poder recuperar en caso de presentarse esta amenaza.
	Fugas de Información [E.19]	La información puede ser expuesta fácilmente a fugas sino se controla su manipulación. Por error del usuario podría ser enviada a personas ajenas a la empresa o en el caso de documentos importantes no custodiados que dejan encima de algún escritorio o envían a imprimir y no recogen, poniendo en peligro la confidencialidad.
	Pérdida de equipos [E.25]	No existe trazabilidad del uso de los dispositivos de almacenamiento como USB, CD-ROM, dando lugar a la perdida de los mismos, afectando la confiabilidad y la confidencialidad de la información. De igual forma al perderse un equipo, la información que está almacenada dentro de este, podría ser expuesta por la persona que lo tenga en su dominio.

ORIGEN	AMENAZA	VULNERABILIDADES
Tabla 13. Continuación		
Ataques Intencionados[A]	Suplantación de la identidad de los Usuarios [A.5], Abuso de los privilegios de Acceso [A.6]	A pesar de que los usuarios tienen sus niveles de privilegios, los usuarios no bloquean sus sesiones al quedar el equipo desatendido, también se prestan claves; lo que puede conllevar a la suplantación de identidad de usuario. Por otro lado, debido a la falta de auditoría no se podría estar totalmente seguros que alcances tiene los usuarios para acceder a la información, peligrando la confidencialidad, autenticidad e integridad de la información.
	Uso no previsto [A.7]	No hay control de la utilización de los recursos de sistemas de la empresa, los asesores externos debido a la facilidad para ingresar remotamente a la información, podría acceder en horas no laborales para usos malintencionados si quisiera.
	Modificación [A.15], Destrucción [A.18], Divulgación [A.19] y Robo de la información [A.25]	Estas cuatro amenazas pueden ser llevadas a cabo por personas malintencionadas para obtener beneficios propios o venganzas contra la empresa, como ejemplo se menciona destrucción de documentos o alteración de información en pagos recibidos, robo de Backup de base de datos, entre otros.
	Ataque destructivo [A.26]	Esta amenaza podría presentarse en el caso de algún software de propagación maliciosa que afecte la información.
	SERVICIOS	
Origen Industrial[I]	Fluctuaciones o sobrecargas eléctricas	Puede verse afectado el servicio de impresión y escaneo en red, causando la indisponibilidad del servicio por daño en el equipo.
	Fallo de servicios de comunicaciones [I.8]	Por fallas en los servicios de comunicaciones pueden verse afectado los servicios de acceso al sistema de información, generación de informes y almacenamiento compartido de archivos.
	Interrupción de otros servicios y suministros esenciales [I.9]	Puede verse afectado el servicio de impresión por falta de papel o tóner.
Errores y fallos no intencionados[E]	Errores de usuario [E.1]	Los usuarios por mala manipulación de las impresoras podrían afectar el buen funcionamiento de esta, causando la indisponibilidad.
	Errores de Administrador [E.2]	Los informes personalizados podrían no estar ajustado a las necesidades del usuario porque no existe un formato donde se solicite el detalle del requerimiento. Y se caiga en reprocesos.
	Errores de configuración [E.4]	Falta de capacitación para la configuración de la seguridad perimetral, podría presentarse usos imprevistos.
	Alteración [E.15] o destrucción de la información [E.18]	Alteración y borrado de archivos sin intención por falta de directorio activo al igual de borrado informes personalizados por falta de seguridad en los permisos de usuario en el sistema.

ORIGEN	AMENAZA	VULNERABILIDADES
	Tabla 13. Continuación	
	Indisponibilidad del personal [E.28]	Servicios no disponibles por incapacidad o vacaciones de la coordinadora de sistemas., debido a falta de apoyo en el área.
Ataques intencionales [A]	Uso no previsto [A.7]	Se detectan a través de la seguridad perimetral el intento de acceder a páginas de ocio por parte del personal. Se dan permisos para uso de WhatsApp web, pero podría usarse también para fines personales porque se sale de control la aplicación.
	Modificación [A.15] o destrucción de la información [A.18]	Por falta de controles en los accesos al sistema, se ha presentado perdida de informes en el sistema y carpetas del servidor de almacenamiento de archivos compartidos.
	Divulgación de información [A.19]	Los usuarios pueden buscar información en carpetas de los demás usuarios debido a la falta de directorio activo para control de acceso a carpetas.
	SOFTWARE	
Origen Industrial[I]	Avería de origen físico o lógico [I.5]	Ausencia de un cuarto de equipos, en el caso de los servidores, están expuestos a factores ambientales que pueden afectar los componentes de los equipos y por tanto el funcionamiento de este.
Errores y Fallos no intencionales[E]	Errores de usuario [E.1]	Falta más capacitación de los usuarios en el manejo de sistema SAP, SAP DTW, Nómina y ofimática Falta de manuales de procedimientos e instructivos.
	Errores de Administrador [E.2]	Sobrecarga de funciones Falta de manuales de procedimientos Falta de capacitación continua
	Difusión de software dañino [E.8]	Falta de control de instalación de aplicaciones en equipos Falta de capacitación al usuario sobre seguridad informática y prevenciones de amenazas. Falta de políticas de seguridad para uso de medios de almacenamiento externos como USB
	Alteraciones accidentales de información [E.15]	No existen políticas adecuadas de verificación y almacenamiento información.
	Destrucción de información [E.18]	Falta de directorio activo para establecer niveles de seguridad de información Falta de Backup de información de cada área
	Errores de mantenimiento y actualizaciones de programas [E.21]	Falta de planes de actualizaciones de sistemas operativos. Falta de un ambiente de pruebas para hacer actualizaciones de SAP Falta de inventario de software La localización de SAP presenta fallas después de cada actualización, por lo que se mantiene continua comunicación con soporte para que los errores que se vayan presentando se vayan corrigiendo.

ORIGEN	AMENAZA	VULNERABILIDADES
Tabla 13. Continuación		
Ataques intencionales [A]	Suplantación de identidad [A.5]	Falta de monitoreo del log de acceso al sistema No existen políticas de seguridad sobre claves, se comparten accesos entre usuarios.
	Abuso de privilegios de acceso [A.6]	Falta de auditoría en los procesos
	Uso no previsto [A.7]	Falta de control a usuarios externos en el horario de acceso al sistema
	Difusión de software dañino [A.8]	Falta de control en navegación de usuarios externos. Falta de control en instalaciones de software
	Re-encadenamiento de mensajes [A.9]	No existen controles sobre el uso de cuentas de correo electrónico.
	Destrucción de información [A.18]	Falta de control de acceso a la información
	Divulgación de información [A.19]	Falta de controles de confidencialidad de la información
	Manipulación de programas [A.4]	Falta de controles de privilegios de usuarios en la configuración y archivos de configuración del equipo.
	HARDWARE	
Desastres Naturales[N]	Fuego [N.1]	Este tipo de amenaza atenta gravemente contra los activos, solo se tiene póliza de seguros para algunos equipos.
	Daños por agua [N.2]	Afectación de los activos por falencias en infraestructura física, ocasionando goteras e inundaciones.
Origen Industrial [I]	Fuego [I.1]	Dentro del inventario en la bodega de MA PEÑALOSA CÍA S.A.S, existen algunos productos que pueden ser inflamables por lo que se requiere de precaución en su manipulación. Cerca del rack principal no existe un extintor que pueda ayudar a controlar la amenaza en caso de presentarse.
	Fluctuaciones o sobrecargas eléctricas	Se evidencia muchos altibajos en el suministro eléctrico, se han presentado cortos eléctricos dentro de las instalaciones, los cuales deben revisarse porque puede ocasionar daños lógicos en equipos.
	Contaminación mecánica [I.3]	Dentro de la bodega se encuentra el rack principal y algunas áreas de trabajo con equipos informáticos, estos pueden verse expuestos a productos tipo polvo como cementos y pegos de cerámica que pueden afectar la disponibilidad de los activos.
	Avería de origen físico o lógica [I.5]	Degradación del hardware por contaminación o fallas eléctricas.
	Condiciones inadecuadas de temperatura o humedad [I.7]	Al no disponer de un centro de datos para los activos críticos que soportan la infraestructura tecnológica, no están en condiciones adecuadas de temperatura y están expuestos a altas temperaturas que podrían ocasionar daños en los equipos.

ORIGEN	AMENAZA	VULNERABILIDADES

Tabla 13. Continuación

Errores y Fallos no intencionales[E]	Errores de mantenimiento y actualización de hardware [E.23]	Daños al hardware por mala manipulación dentro del mantenimiento realizado.
	Caída del sistema por agotamiento de recursos [E.24]	Falta de controles que permitan medir el rendimiento de los recursos físicos y lógicos, se presenta indisponibilidad del sistema por lentitud o bloqueo en los procesos.
Ataques intencionales[A]	Uso no previsto [A.7]	Uso de los equipos informáticos en actividades no propias de la empresa como juegos, y temas personales
	Denegación de servicio [A.24]	Debido a los recursos insuficientes del servidor para atender tantos usuarios, genera sobrecarga de trabajo provocando denegación del servicio.
	Robo [A.25]	No existen controles sobre del uso del hardware, dando lugar a la perdida de los mismos. Los usuarios de los portátiles no utilizan de manera adecuada la guaya de seguridad.
COMUNICACIONES		
Origen Industrial[I]	Fallo de servicios de comunicaciones	Al presentarse inconvenientes con la red WAN, se presentan problemas de comunicación con las demás sedes en especial la Sede de la Zona industrial donde existe el mayor flujo de proceso de entregas y ocasionaría indisponibilidad del sistema.
Errores y fallos no intencionados[E]	Errores del administrador [E.2]	Cualquier error del administrador en la configuración de las redes de comunicaciones, puede causar la indisponibilidad del servicio.
	Caída del sistema por agotamiento de recursos [E.24]	La comunicación con los servidores de aplicaciones y base de datos se ve afectado por indisponibilidad cuando el canal de comunicaciones está saturado por la cantidad de paquetes transmitidos por los usuarios del sistema.
Ataques Intencionados[A]	Suplantación de la identidad de los Usuarios [A.5], Abuso de los privilegios de Acceso [A.6] y Accesos No Autorizados [A.11]	Debido a que no hay directorio activo implementado, el ingreso a la red y a cualquier dispositivo dentro de ella no es difícil en cuanto a la red LAN. Existe una forma de identificar la contraseña de la red WIFI sin tener mucha experiencia en el tema, lo cual es una vulnerabilidad alta porque pueden integrarse dentro de la red si obtienen los datos de acceso.
	Uso no previsto [A.7]	Para los usuarios externos se dificulta el control de acceso remoto, ya que externamente no hay políticas en los horarios de acceso al sistema, podría usar este tipo de comunicación para extraer información confidencial si lo quisiera.
	Interceptación de información [A.14]	Debido a que los usuarios no utilizan una VPN para acceso externo, podría interceptar la información cuando acceden remotamente por los datos quedan expuestos durante la conexión.

ORIGEN	AMENAZA	VULNERABILIDADES
	Tabla 13. Continuación	
	Denegación de servicio [A.24]	Saturación de los canales de emisión de wifi provocando la caída del sistema o presencia de un virus que está consumiendo recursos de la red.
ELEMENTOS AUXILIARES		
Desastres Naturales[N]	Daños por agua [N.2]	Degradación de los soportes de almacenamiento de la Información. Daño en los componentes lógicos de las UPS
Origen Industrial [I]	Fuego [I.1]	Debido a tantas añadiduras de cable eléctrico podría ocasionarse algún corto y ocasionar incendios.
	Avería de origen físico o lógico [I.5]	Daños en las UPS por falta de mantenimiento y desgaste.
	Degradación de los soportes de almacenamiento de información [I.10]	Deterioro a largo plazo, por las condiciones de instalación de cableados.
Errores y fallos no intencionados[E]	Errores de mtto. y actualización de Hw [E.23]	Daños al hardware por mala manipulación dentro del mantenimiento realizado.
Ataques Intencionados[A]	Acceso no autorizado [A.11]	Por falta de control de acceso, se ha detectado a proveedores utilizar sin permisos el cableado de red para integrarse a la red y conectarse a internet.
	Ataque destructivo [A.26]	Parte del cableado está fuera de canaletas y al alcance de los usuarios o personas externas, podrían hacer corte del cableado en caso de sabotaje.
SERVICIOS SUBCONTRATADOS		
Errores y fallos no intencionados[E]	Errores de los usuarios [E.1]	Por falta de políticas y manuales de procedimientos los usuarios están propensos a cometer errores continuamente.
	Errores de re-encadenamiento [E.9]	Error de envío de información a través de correo electrónico por error del usuario en el destinatario.
	Destrucción de información [E.18]	Destrucción de correos por error del usuario
	Fugas de Información [E.19]	Envío de correos a personas ajenas a las actividades de la empresa por errores del usuario.
	Caída del sistema por agotamiento de recursos [E.24]	Indisponibilidad del servicio por afectación del medio de transmisión afectando el Internet, la telefonía, conectividad de sedes. Bloqueo de correo empresarial a nivel general por mala gestión de conjuración del servidor de correo. Cese de impresiones de facturas o documentos por falta de recursos del proveedor de impresoras o de técnicos.
Ataques Intencionados[A]	Uso no previsto [A.7]	Uso de correo electrónico o impresiones de documentos con fines personales.
	Accesos no autorizados [A.11]	Accesos a correo empresarial de personal que no es propietario de la cuenta por equipo desatendido.

ORIGEN	AMENAZA	VULNERABILIDADES
	Tabla 13. Continuación	
	Destrucción de información [A.18]	Destrucción de correos para borrar evidencias. Destrucción de información por sabotaje del técnico de mantenimiento de equipos.
	Divulgación de información [A.19]	Envío de correos a personas ajenas a las actividades de la empresa con fines delictivos. Divulgación de información por parte del técnico de mantenimiento al tener acceso a equipos.
	Denegación de servicio [A.24]	Indisponibilidad del servicio por afectación del medio de transmisión afectando el Internet, la telefonía, conectividad de sedes. Bloqueo de correo empresarial a nivel general por mala gestión de conjuración del servidor de correo. Cese de impresiones de facturas o documentos por falta de recursos del proveedor de impresoras o de técnicos.
INSTALACIONES		
Desastres Naturales[N]	Fuego [N.1]	La propagación del fuego podría causar graves daños, debido al producto almacenado en bodega. Los extintores no son suficientes para cubrir toda la empresa.
	Daños por agua [N.2]	El mal estado de la infraestructura física, en días lluviosos provoca goteras en varias áreas de la empresa e inundaciones.
	Terremoto	En caso de terremotos o temblores fuertes, parte de la infraestructura antigua podría derrumbarse, afectando a los demás activos.
Origen Industrial [I]	Fuego [I.1]	Dentro de los productos comercializados de MA PEÑALOSA CÍA S.A.S, existen productos inflamables que deben manejarse con cautela y evitar ambientes de excesivo calor para evitar incidentes.
	Fluctuaciones o sobrecargas eléctricas	El mal manejo de instalaciones eléctricas, podría generar una sobrecarga de energía, provocando cortos que dañen las instalaciones.
Ataques Intencionados[A]	Accesos no autorizados [A.11]	Falta de control de acceso a las instalaciones físicas de la empresa.
	Ataque destructivo [A.26]	La instalación de la Sede principal de MA PEÑALOSA CÍA S.A.S está ubicada en el sector del centro de la ciudad de Cúcuta, en esta área son comunes las manifestaciones o marchas y robos de delincuencia común.
PERSONAL		
Desastres Naturales[N]	Daños por Agua [N.2]	El mal estado de la infraestructura física, en días lluviosos provoca malestar en los usuarios porque sus puestos de trabajo pueden verse afectados o sus equipos.
	Derrumbes	Debido a la mala infraestructura física, el personal está expuesto a peligros en caso de un temblor fuerte.

ORIGEN	AMENAZA	VULNERABILIDADES
Tabla 13. Continuación		
Origen Industrial[I]	Fluctuaciones o sobrecargas eléctricas	Se evidencia muchos altibajos en el suministro eléctrico, se han presentado cortos eléctricos dentro de las instalaciones, los cuales puede afectar el personal que este cercano.
Errores y fallos no intencionados[E]	Deficiencias en la organización [E.7]	Falta de manuales y procedimientos, el personal contratado recibe capacitación de otro compañero del área, corriendo el riesgo de que si el personal que los está capacitando no tiene los procesos claros, el que ingresa estaría propenso a cometer errores
	Fuga de información [E.19]	Falta de control en la manipulación de la información digital, información confidencial del personal podría verse expuesta.
	Indisponibilidad del personal [E.28]	Se presentan absentismos por enfermedad, comúnmente a causa de virosis producida por la humedad y demás factores ambientales.
Ataques Intencionados[A]	Indisponibilidad del personal [A.28]	Bajas de personal por recorte de presupuesto.

Fuente: Autor

9.2.3 Valoración de la Amenaza. Las amenazas deben ser valoradas según:

- Frecuencia: medición de la probabilidad de ocurrencia, determinada por el número de veces que sucede una amenaza afectando un activo en un determinado periodo de tiempo.

Tabla 14. Escala de rango de frecuencia de amenazas

Vulnerabilidad	Rango	Valor
Frecuencia muy alta	Puede ocurrir una vez al día	5
Frecuencia alta	Puede ocurrir una vez a la semana	4
Frecuencia media	Puede ocurrir en un mes	3
Frecuencia baja	Puede ocurrir una vez por semestre	2
Frecuencia muy baja	Puede ocurrir en un año o mas	1

Fuente: Autor

- Impacto: nivel de degradación o afectación que pueda ocasionar en un activo dependiendo y evaluando sus dimensiones de seguridad.

Tabla 15. Valoración del impacto

Impacto	Valor	Probabilidad
Muy alto	5	100%
Alto	4	75%
Medio	3	50%
Bajo	2	20%
Muy bajo	1	5%

Fuente: Autor

9.2.4 Valoración del Riesgo. El riesgo se considera como la probabilidad de frecuencia de una amenaza por el impacto causado. A continuación, se presenta la forma de calcularse:

Riesgo = Impacto * Probabilidad

Se definen cuatro niveles de riesgo:

- Crítico: Ocurre con mucha frecuencia con grandes afectaciones a los activos, debe evaluarse y tomar controles necesarios para corregirse.

- Alto: Sucede con frecuencia, pero no la afectación es moderada o viceversa.
- Medio: Se presenta esporádicamente y afecta en un nivel medio, debe evaluarse para tomar medidas.
- Bajo: No se ocasiona con mucha frecuencia y la afectación en los activos es baja proporción, es importante tener el registro en una bitácora.

Tabla 16 Nivel de riesgo

Impacto	Valor
Critico	10
Alto	7-9
Medio	4-6
Bajo	1-3

Fuente: Autor

Tabla 17. Matriz de valoración de riesgos

Activo	Amenaza	[D]	[I]	[C]	[A]	[T]	Frecuencia	Impacto	Riesgo	Nivel de riesgo
ORGANIZACIÓN										
Proveedor de Mtto. de Equipos, impresoras y aires acondicionados	Contaminación ambiental	9					2	20%	1	Bajo
Proveedor de comunicaciones y Servicio de vigilancia	Derrumbes	10					2	20%	1	Bajo
DATOS E INFORMACIÓN										
Base de Datos MA_PENALOSA	Fuego	10					1	100%	2	Bajo
	Daños por Agua	10					2	100%	4	Medio
	Fluctuaciones o sobrecargas eléctricas	10					5	100%	10	Crítico
	Contaminación Mecánica	10					3	100%	6	Medio
	Cortes del suministro eléctrico	10					3	75%	5	Medio
	Condiciones inadecuadas de temperatura o humedad	10					5	100%	10	Crítico
	Degradación de los soportes de Almacenamiento de la Información	10					3	50%	3	Bajo
	Alteración accidental de la Información		10				2	100%	4	Medio
	Destrucción de la Información	10					1	100%	2	Bajo
	Fugas de Información			10			5	100%	10	Crítico
	Pérdida de equipos	10		10			1	75%	2	Bajo
	Suplantación de la identidad de los Usuarios, Abuso de los privilegios de Acceso	10	10	10	10		2	75%	3	Bajo
	Uso no previsto	10	10	10			4	100%	8	Alto
	Ataque destructivo	10					1	100%	2	Bajo
Bases de datos Nomina	Fuego	10					1	100%	2	Bajo
	Daños por Agua	10					2	100%	4	Medio
	Fluctuaciones o sobrecargas eléctricas	10					5	100%	10	Crítico
	Contaminación Mecánica	10					2	100%	4	Medio
	Cortes del suministro eléctrico	10					3	50%	3	Bajo

Activo	Amenaza	[D]	[I]	[C]	[A]	[T]	Frecuencia	Impacto	Riesgo	Nivel de riesgo
	Tabla 17. Continuación									
	Condiciones inadecuadas de temperatura o humedad	10					5	100%	10	Crítico
	Degradación de los soportes de Almacenamiento de la Información	10					3	50%	3	Bajo
	Alteración accidental de la Información		10				1	75%	2	Bajo
	Destrucción de la Información	10					1	100%	2	Bajo
	Fugas de Información			10			1	75%	2	Bajo
	Suplantación de la identidad de los Usuarios, Abuso de los privilegios de Acceso	10	10	10	10		1	75%	2	Bajo
Información Física (Facturas, Egresos, Recibos de pago, Contratos de servicios y de personal, Estudios y soporte de crédito de clientes)	Fuego	10					1	100%	2	Bajo
	Daño por Agua	10					2	100%	4	Medio
	Escapes y Fugas de Información			10			3	100%	6	Medio
	Alteración accidental de la Información		10				2	100%	4	Medio
	Destrucción de la Información	10					2	100%	4	Medio
Backup de base de datos	Fuego	10					1	100%	2	Bajo
	Daños por Agua	10					2	100%	4	Medio
	Degradación de los soportes de Almacenamiento de la Información	10					3	75%	5	Medio
	Alteración accidental de la Información			10			1	75%	2	Bajo
	Destrucción de la Información	10					1	75%	2	Bajo
	Fugas de Información			10			1	100%	2	Bajo
	Pérdida de equipos	10		10			1	100%	2	Bajo
	Suplantación de la identidad de los Usuarios, Abuso de los privilegios de Acceso	10	10	10	10		1	75%	2	Bajo
	Ataque destructivo	10					1	100%	2	Bajo
SERVICIOS										
Soporte a usuarios finales	Errores de Administrador	10	2	0			2	50%	2	Bajo
	Indisponibilidad del personal	10					1	100%	2	Bajo
Informes personalizados	Fallo de servicios de comunicaciones	8					1	5%	0	Bajo

Activo	Amenaza	[D]	[I]	[C]	[A]	[T]	Frecuencia	Impacto	Riesgo	Nivel de riesgo
	Tabla 17. Continuación									
	Errores de Administrador	8	9	10			2	20%	1	Bajo
	Alteración o destrucción de la información	8	9				2	20%	1	Bajo
	Indisponibilidad del personal	8					2	50%	2	Bajo
	Divulgación de información			10			3	75%	5	Medio
Almacenamiento compartido	Fallo de servicios de comunicaciones	5					2	50%	2	Bajo
	Alteración o destrucción de la información	5	8				1	100%	2	Bajo
	Indisponibilidad del personal	5					2	20%	1	Bajo
	Uso no previsto	5	8	10			1	5%	0	Bajo
	Divulgación de información			10			3	75%	5	Medio
Impresión y escaneo en red	Fluctuaciones o sobrecargas eléctricas	10					5	75%	8	Alto
	Interrupción de otros servicios y suministros esenciales	10					3	75%	5	Medio
	Errores de usuario	10	1	3			3	75%	5	Medio
	Indisponibilidad del personal	10					2	20%	1	Bajo
	Uso no previsto	10	1	3			1	5%	0	Bajo
	Divulgación de información			3			2	50%	2	Bajo
Solución seguridad perimetral	Fallo de servicios de comunicaciones	7					1	50%	1	Bajo
	Errores de configuración	7	4	6			1	75%	2	Bajo
	Indisponibilidad del personal	7					2	20%	1	Bajo
	Uso no previsto	7	4	6			5	50%	5	Medio
Sistema de información	Fallo de servicios de comunicaciones	10					2	100%	4	Medio
	Errores de Administrador	10	10	10			2	50%	2	Bajo
	Alteración o destrucción de la información	10	10				3	75%	5	Medio
	Indisponibilidad del personal	10					2	100%	4	Medio
	Divulgación de información			10			3	75%	5	Medio
SOFTWARE										
SAP Business One	Errores de mantenimiento y actualizaciones de programas	10	10				2	100%	4	Medio

Activo	Amenaza	[D]	[I]	[C]	[A]	[T]	Frecuencia	Impacto	Riesgo	Nivel de riesgo
	Tabla 17. Continuación									
	Errores de usuario	10	10	10			5	50%	5	Medio
	Errores de administrador	10	10	10			2	20%	1	Bajo
	Destrucción de información	10					2	50%	2	Bajo
	Fugas y divulgación de información			10			3	100%	6	Medio
	Suplantación de identidad			10	10		3	100%	6	Medio
	Uso no previsto	10	10	10			5	100%	10	Crítico
	Abuso de privilegios			10	10		2	100%	4	Medio
	Caída del sistema por agotamiento de recursos	10					5	100%	10	Crítico
SQL Server 2008R2	Errores del administrador	10	10	10			1	100%	2	Bajo
	Errores de mantenimiento de BD	10	10	10			1	75%	2	Bajo
	Alteraciones accidentales		10				1	100%	2	Bajo
Ofimática	Errores de usuario	6	3	0			4	20%	2	Bajo
	Errores de re-encadenamiento			5			2	75%	3	Bajo
	Fuga de información			6			2	75%	3	Bajo
	Errores de mantenimiento y actualizaciones de programas	6	3				3	20%	1	Bajo
	Difusión de software dañino	6	3	2			1	100%	2	Bajo
Sistemas Operativos	Avería de origen físico o lógico	9					2	50%	2	Bajo
	Difusión de software dañino	9	9	6			1	75%	2	Bajo
	Errores de mantenimiento y actualizaciones de programas	9	9				4	50%	4	Medio
Antivirus	Difusión de software dañino	9	5	0			5	75%	8	Alto
	Errores de mantenimiento y actualizaciones de programas	9	5				1	50%	1	Bajo
SAP B. ONE DTW	Errores de usuario	5	6	0			3	75%	5	Medio
	Error de administrador	5	6	0			1	75%	2	Bajo
Solución SAP Móvil	Error de usuario	2	7	10			2	50%	2	Bajo
	Abuso de privilegios	2	7	10			1	50%	1	Bajo
	Uso no previsto	2	7	10			5	100%	10	Crítico
	Errores de mantenimiento y actualizaciones de programas	2	7				3	20%	1	Bajo

Activo	Amenaza	[D]	[I]	[C]	[A]	[T]	Frecuencia	Impacto	Riesgo	Nivel de riesgo
	Tabla 17. Continuación									
	Suplantación de identidad	2	7	10	10		1	50%	1	Bajo
Nómina TNS	Error de usuario	6	9	10			1	50%	1	Bajo
	Abuso de privilegios	6	9	10			1	75%	2	Bajo
	Suplantación de identidad	6	9	10	10		1	20%	0	Bajo
HARDWARE										
Servidores	Fuego	10	10	10			1	100%	2	Bajo
	Daños por agua	10	10	10			3	100%	6	Medio
	Fluctuaciones o sobrecargas eléctricas	10	10	10			5	100%	10	Crítico
	Contaminación mecánica	10	10	10			5	75%	8	Alto
	Avería de origen físico o lógica	10	10	10			3	100%	6	Medio
	Condiciones inadecuadas de temperatura o humedad	10	10	10			5	100%	10	Crítico
	Errores de mantenimiento y actualización de hardware	10	10	10			2	100%	4	Medio
	Errores de mantenimiento y actualización de software	10	10	10			2	75%	3	Bajo
	Caída del sistema por agotamiento de recursos	10	10	10			5	100%	10	Crítico
	Uso no previsto	10	10	10			3	100%	6	Medio
	Denegación de servicio	10	10	10			3	100%	6	Medio
Smartphone	Daños por agua	4	3	1			3	20%	1	Bajo
	Avería de origen físico o lógica	4	3	1			3	20%	1	Bajo
	Caída del sistema por agotamiento de recursos	4	3	1			2	5%	0	Bajo
Impresora Multifuncional Color		1	6	0			5	5%	1	Bajo
	Uso no previsto	4	3	1			2	5%	0	Bajo
	Robo	4	3	1			2	50%	2	Bajo
	Uso no previsto	1	6	0			4	5%	0	Bajo
Tabletas	Daños por agua	6	3	5			3	75%	5	Medio
	Avería de origen físico o lógica	6	3	5			2	20%	1	Bajo
	Errores de mantenimiento y actualización de hardware	6	3	5			2	20%	1	Bajo
	Errores de mantenimiento y actualización de software	6	3	5			3	50%	3	Bajo

Activo	Amenaza	[D]	[I]	[C]	[A]	[T]	Frecuencia	Impacto	Riesgo	Nivel de riesgo
	Tabla 17. Continuación									
	Caída del sistema por agotamiento de recursos	6	3	5			2	50%	2	Bajo
	Uso no previsto	6	3	5			4	75%	6	Medio
Equipos	Fuego	6	4	6			1	100%	2	Bajo
	Daños por agua	6	4	6			3	100%	6	Medio
	Fluctuaciones o sobrecargas eléctricas	6	4	6			5	75%	8	Alto
	Contaminación mecánica	6	4	6			5	75%	8	Alto
	Avería de origen físico o lógica	6	4	6			2	20%	1	Bajo
	Condiciones inadecuadas de temperatura o humedad	6	4	6			2	50%	2	Bajo
	Errores de mantenimiento y actualización de hardware	6	4	6			1	20%	0	Bajo
	Errores de mantenimiento y actualización de software	6	4	6			3	50%	3	Bajo
	Caída del sistema por agotamiento de recursos	6	4	6			3	50%	3	Bajo
	Uso no previsto	6	4	6			4	20%	2	Bajo
	Denegación de servicio	6	4	6			2	20%	1	Bajo
Fortigate	Fuego	10	10	7			1	100%	2	Bajo
	Daños por agua	10	10	7			1	100%	2	Bajo
	Fluctuaciones o sobrecargas eléctricas	10	10	7			5	100%	10	Crítico
	Contaminación mecánica	10	10	7			5	75%	8	Alto
	Avería de origen físico o lógica	10	10	7			1	75%	2	Bajo
	Errores de mantenimiento y actualización de hardware	10	10	7			1	20%	0	Bajo
	Errores de mantenimiento y actualización de software	10	10	7			2	20%	1	Bajo
	Denegación de servicio	10	10	7			1	100%	2	Bajo
COMUNICACIONES										
Red WIFI	Errores del administrador	4	5	5			2	5%	0	Bajo
	Caída del sistema por agotamiento de recursos	4					3	5%	0	Bajo

Activo	Amenaza	[D]	[I]	[C]	[A]	[T]	Frecuencia	Impacto	Riesgo	Nivel de riesgo
	Tabla 17. Continuación									
	Suplantación de la identidad de los Usuarios, Abuso de los privilegios de Acceso y Accesos No Autorizados	4	5	9	9		3	75%	5	Medio
	Denegación de servicio	4					2	5%	0	Bajo
Red WAN	Fallo de servicios de comunicaciones	5					4	75%	6	Medio
	Errores del administrador	5	4	7			2	75%	3	Bajo
	Caída del sistema por agotamiento de recursos	5					4	75%	6	Medio
	Uso no previsto	5	4	7			3	100%	6	Medio
	Interceptación de información			7			1	100%	2	Bajo
	Denegación de servicio	5	4	7			4	75%	6	Medio
Red LAN	Errores del administrador	10	7	6			2	75%	3	Bajo
	Caída del sistema por agotamiento de recursos	10					2	75%	3	Bajo
	Suplantación de la identidad de los Usuarios, Abuso de los privilegios de Acceso y Accesos No Autorizados	10	7	6	9		2	100%	4	Medio
	Denegación de servicio	10					3	100%	6	Medio
ELEMENTOS AUXILIARES										
UPS	Daños por Agua	6					2	50%	2	Bajo
	Avería de origen físico o lógico	6					2	20%	1	Bajo
	Errores de mantenimiento y actualización de hardware	6					1	20%	0	Bajo
Cableado red de datos	Daños por Agua	7					2	20%	1	Bajo
	Degradación de los soportes de almacenamiento de información	7					2	75%	3	Bajo
	Acceso no autorizado		9	9			4	100%	8	Alto
	Ataque destructivo	7	9	9			1	75%	2	Bajo
Cableado eléctrico	Daños por Agua	7					2	75%	3	Bajo
	Fuego	7					1	100%	2	Bajo
	Degradación de los soportes de almacenamiento de información	7					4	75%	6	Medio

Activo	Amenaza	[D]	[I]	[C]	[A]	[T]	Frecuencia	Impacto	Riesgo	Nivel de riesgo
Tabla 17. Continuación										
Cableado telefónico	Daños por Agua	6					3	75%	5	Medio
	Degradación de los soportes de almacenamiento de información	6					3	75%	5	Medio
	Ataque destructivo	6					1	50%	1	Bajo
SERVICIOS SUBCONTRATADOS										
Correo electrónico	Errores de los usuarios	5	4	9			3	20%	1	Bajo
	Errores de re-encadenamiento			9			1	50%	1	Bajo
	Destrucción de información	5					3	75%	5	Medio
	Fugas de Información			9			4	100%	8	Alto
	Caída del sistema por agotamiento de recursos	5					2	50%	2	Bajo
	Uso no previsto	5	4	9			1	50%	1	Bajo
	Accesos no autorizados		4	9			1	75%	2	Bajo
	Divulgación de información			9			2	75%	3	Bajo
	Denegación de servicio	5					3	75%	5	Medio
Conectividad MPLS	Errores del administrador	6	2	5			1	50%	1	Bajo
	Caída del sistema por agotamiento de recursos	6					4	75%	6	Medio
	Denegación de servicio	6					2	75%	3	Bajo
Mantenimiento de equipos	Destrucción de información	9					1	100%	2	Bajo
	Fugas de Información			9			1	100%	2	Bajo
	Divulgación de información			9			1	75%	2	Bajo
	Denegación de servicio	9					2	50%	2	Bajo
Conectividad de Internet	Errores del administrador	6	2	5			1	75%	2	Bajo
	Caída del sistema por agotamiento de recursos	6					3	75%	5	Medio
	Uso no previsto	6	2	5			5	50%	5	Medio
	Denegación de servicio	6					2	75%	3	Bajo
Telefonía fija y móvil	Caída del sistema por agotamiento de recursos	10					1	50%	1	Bajo
	Uso no previsto	10	2	1			5	20%	2	Bajo
	Denegación de servicio	10					2	75%	3	Bajo
Alquiler de impresoras	Errores de los usuarios	10	6	0			4	75%	6	Medio
	Caída del sistema por agotamiento de recursos	10					4	50%	4	Medio

Activo	Amenaza	[D]	[I]	[C]	[A]	[T]	Frecuencia	Impacto	Riesgo	Nivel de riesgo
	Tabla 17. Continuación									
	Uso no previsto	10	6	0			4	20%	2	Bajo
	Denegación de servicio	10					3	20%	1	Bajo
INSTALACIONES										
Infraestructura Física	Fuego	7					1	100%	2	Bajo
	Daños por Agua	7					3	100%	6	Medio
	Terremoto	7					1	75%	2	Bajo
	Fluctuaciones o sobrecargas eléctricas	7					2	75%	3	Bajo
	Accesos no autorizados		10	2			5	100%	10	Crítico
	Ataque destructivo	7					1	50%	1	Bajo
Centro de datos	Fuego	9					1	100%	2	Bajo
	Daños por Agua	9					3	75%	5	Medio
	Terremoto	9					1	75%	2	Bajo
	Fluctuaciones o sobrecargas eléctricas	9					2	75%	3	Bajo
	Accesos no autorizados		9	10			5	100%	10	Crítico
	Ataque destructivo	9					1	50%	1	Bajo
Zona de Acceso a Seguridad, Oficinas y equipos	Fuego	2					1	100%	2	Bajo
	Daños por Agua	2					3	75%	5	Medio
	Terremoto	2					1	75%	2	Bajo
	Fluctuaciones o sobrecargas eléctricas	2					2	75%	3	Bajo
	Accesos no autorizados		6	4			5	100%	10	Crítico
PERSONAL										
Administrador del Sistema	Derrumbes	10					1	75%	2	Bajo
	Fuga de información			10			1	75%	2	Bajo
	Indisponibilidad del personal	10					2	100%	4	Medio
Gerente	Derrumbes	7					1	75%	2	Bajo
	Deficiencias en la organización	7					1	75%	2	Bajo
	Indisponibilidad del personal	7					2	50%	2	Bajo
Usuarios	Derrumbes	3					1	75%	2	Bajo
	Fuga de información			5			1	75%	2	Bajo
	Indisponibilidad del personal	3					3	50%	3	Bajo

Fuente: Autor

9.2.5 Evaluación de Riesgos. Para cada activo de información, el proceso concluye si el Nivel de Riesgo es bajo, de lo contrario, se determina el tratamiento ya sea para evitar, mitigar o transferir a un tercero, estableciendo controles necesarios.

Tabla 18. Establecimiento de Niveles

Nivel de Riesgo	Tratamiento del riesgo
Critico	Se reduce o mitiga el riesgo por medio de controles detectivos
Alto	Se reduce o mitiga el riesgo por medio de controles preventivos
Medio	Se transfiere el riesgo por ejemplo tomando un seguro.
Bajo	Finaliza el proceso.

Fuente: Autor

9.2.6 Análisis de resultados de la Matriz de Riesgos. La empresa MA PEÑALOSA CÍA. S.A.S., presenta diversas amenazas y vulnerabilidades que puede poner en riesgo sus activos de información. De acuerdo a la matriz de riesgos realizada anteriormente, se analiza la valoración del nivel de riesgo crítico, alto y medio, se evidencia lo siguiente:

Nivel crítico 

Se evidencia diariamente fluctuaciones o sobrecargas eléctricas, debido a malas instalaciones por falta de estudios previos de cargas eléctricas, cables a la intemperie que causan deterioro por falta de canaletas. Todos estos factores afectan en primera medida a los equipos que soportan la infraestructura tecnológica de MA PEÑALOSA CÍA. S.A.S., en especial el Fortigate, responsable de tareas como administración de la red LAN, asignación de direcciones IP por DHCP, detección y prevención de intrusiones, control de navegación. Otros equipos perjudicados son los servidores y demás equipos informáticos, UPS y equipos de red. Estos daños van transcendiendo en cadena afectando otros activos porque al averiarse los componentes lógicos o físicos del hardware como sectores del disco, sufren los sistemas operativos y por ende causan pérdidas de información. Por otro lado, no afecta solo a factores materiales, el personal de MA PEÑALOSA CÍA. S.A.S., puede verse involucrado ya que se generan cortos que atentan contra la integridad del personal.

El deterioro de la infraestructura física de MA PEÑALOSA CÍA. S.A.S., pone en riesgo a todos los activos informáticos, principalmente la seguridad del personal. Gran parte de las instalaciones todavía no se ha reformado y están construidos por material de bahareque, lo que la hace inestable en caso de un temblor fuerte. En varias ocasiones el techo se ha desplomado, pero no se han tomado medidas correctivas.

No se dispone de un cuarto de equipos con las normas necesarias de seguridad, para resguardar los activos críticos que soportan la operación del negocio (servidores, bases de datos, equipos de red (Fortigate), quedando expuestos a factores que puedan afectarlos por condiciones inadecuadas de temperatura y humedad. Actualmente se encuentran ubicado al fondo de la bodega, en el rack principal con llave, en un espacio donde no hay restricción de acceso y a su alrededor guardan productos de tipo polvo como cementos, pegos de cerámica aumentando el peligro de contaminación ambiental para los equipos. El exceso de calor en esta área se debe a la falta de refrigeración necesaria para su buen funcionamiento, por lo cual en cualquier momento podría fallar alguno de los equipos que se alojan en el rack.

No hay ningún control de acceso dentro de las instalaciones de MA PEÑALOSA CÍA. S.A.S., debido a que algunas áreas comerciales como construcción, ferretería e infraestructura, están ubicadas al fondo de la bodega. Es inevitable el paso de clientes, ya que debe recorrer todo el establecimiento para llegar al asesor del área requerido. Y por la falta de cuarto de equipos quedan los activos a la mano de cualquiera que llegue a la empresa y no sea supervisado. A pesar de la existencia de cámaras de seguridad implementadas desde el año pasado, no son suficientes porque no abarcan todas las áreas y no existe una persona responsable de la supervisión de ellas.

Se evidencia la lentitud del sistema de información SAP, debido al crecimiento de usuarios y los requerimientos técnicos, que exige cada vez el Software al migrar a una nueva versión. Debido al agotamiento de recursos como memoria RAM y espacio en disco, se ven afectado los procesos que realiza los usuarios en el sistema, paralizándose la operatividad del negocio por bloqueos inesperados, donde debe intervenir la coordinadora de sistemas para solucionar desde el servidor.

Al no contar con un directorio activo y políticas de acceso, se hace difícil el control de acceso a la información, sobre todo para los usuarios externos, que tienen la facilidad de acceder al sistema desde cualquier ubicación y a cualquier hora, quedando a disposición de ellos y bajo su responsabilidad y ética la manipulación de la información a su alcance.

Es necesario resaltar en esta amenaza la constante rotación de personal, ya que hace vulnerable la información porque al no controlarse, el personal destituido del

cargo podría llevarse información valiosa como la base de datos de clientes y precios.

Nivel Alto 

Dentro del nivel alto, se identifican amenazas mencionadas en el nivel crítico pero su afectación se da en proporciones inferiores para otros activos como los equipos de escritorio, UPS. Ya que el reemplazo de estos puede resolverse en plazos mayores que si se presentara en activos críticos como servidores y equipos de red (Fortigate), los cuales si cesaría la operatividad del negocio. Aunque la información que reposan dentro de estos equipos sigue siendo valiosa y necesitan de Backup para restaurarse en caso de alguna falla de daño en disco.

Uno de los medios por donde existe la probabilidad de fuga de información son los correos electrónicos, ya que no hay implementado alguna herramienta de monitoreo ni controles sobre estos, los cuales lo hace un medio fácil para robar información y luego destruir rastros de las evidencias de envíos de correos.

Otra forma a la que puede exponerse MA PEÑALOSA CÍA. S.A.S. para robo de información se da a través de los puntos de red disponibles, se evidencia que en estos puntos existe un cable de red al alcance de cualquier persona que tenga consigo un portátil y quiera integrarse a la red. Se da el caso de los proveedores que solicitan el uso de internet de MA PEÑALOSA CÍA. S.A.S. y por la confianza de la empresa con ellos, se les facilita tomar esos cables y conectarlo a sus equipos sin autorización.

En este nivel se detecta también la falta de capacitación de los usuarios en el uso del antivirus para analizar los medios de almacenamiento externos como CD, USB y DVD, antes de copiar o abrir archivos con el fin de evitar archivos maliciosos que infecten los equipos y propaguen virus.

Nivel Medio 

Una de las amenazas que afecta los activos de MA PEÑALOSA CÍA. S.A.S. es la inundación causada por las lluvias, aunque se registró como nivel medio debido a la poca frecuencia. Cada vez que llueve fuertemente se presenta problemas en varias de las áreas de la empresa por causa de filtraciones y de mala infraestructura física, que no solo ha ocasionado averías de equipos por el agua sino derrumbes en algunas áreas donde la infraestructura sigue siendo de bahareque.

El deterioro del cableado de red de datos y telefónico es una de las amenazas que afecta el buen funcionamiento del sistema de información que exige buen

rendimiento de la red de datos y por otro lado las comunicaciones. La mayoría de tendido de cable es viejo y no cumple con los estándares de cableado estructurado, este está expuesto a las malas condiciones ambientales y no dentro de tubería o canaleta. No hay una categoría estandarizada para el cable de datos, hay de todo tipo de categoría de cable 5, 5e, 6.

La indisponibilidad del administrador del sistema, aunque tampoco es frecuente la ausencia ya sea por vacaciones o incapacidad. Cuando se presenta tiene un impacto alto, porque no existe otra persona en el área que cubra el tiempo de ausencia y la carga laboral recae en una sola persona que se hace indispensable permanecer disponible durante la operatividad de la empresa.

No se cuenta con un ambiente pruebas para hacer las validaciones pertinentes antes de una migración de versión del sistema de información. Para la realización de las actualizaciones se programa los fines de semana en horario no laboral donde se ejecuta los procesos y pruebas con acompañamiento de un consultor en caso de necesitar asesoría. Si del proceso no se obtiene resultados satisfactorios, se procede a realizar vuelta atrás utilizando el Backup de la base de datos previamente guardada. El no tener un ambiente de pruebas, imposibilita la forma de hacer una evaluación y un test de la migración antes de paso a producción para no causar afectaciones en la base de datos ni en la aplicación.
Aunque existe las restricciones para navegación en internet según niveles de perfiles aplicados. Es frecuente ver el uso no previsto del uso del computador o de impresora para fines no laborales, como almacenamiento de fotos personales, música y documentos personales, navegación en otras páginas que no son de proveedores, como de universidades, el uso de WhatsApp web personal, ya que se da permisos para acceder al WhatsApp de números de la empresa para comunicación rápida con los clientes. Por falta de control de la monitorización de recursos y supervisión de líderes de área que apoyen.

Las interrupciones de otros servicios y suministros esenciales afectan la operatividad de la empresa gravemente, aunque no es frecuente, el hecho de que la impresora de la bodega de la Zona Industrial quede fuera de servicio, paraliza gran parte de las entregas de mercancía ya que esta es la bodega principal. Y aunque se busca otras alternativas como entregas parciales con formatos de papelería, mientras se soluciona no existen procedimientos documentados de cómo proceder ante este incidente y este podría causar faltantes de mercancía y traumas en el sistema.

La falta de acuerdos de confidencialidad, la falta de políticas de seguridad, la falta de capacitaciones sobre tema de seguridad de la información y el buen manejo de la información, hace que los usuarios tengan al alcance información valiosa de la que pudiese sacar provecho si lo deseara. Dentro del sistema de información, se definen perfiles de usuario según el tipo de licenciamiento de SAP y se da acceso a informes previamente autorizado por gerencia, pero aun así es inevitable que los

empleados tengan a su disposición la base de datos de clientes de MA PEÑALOSA CÍA. S.A.S. por consentimiento del gerente para que cada asesor comercial mantenga actualizada la información de los clientes y al mismo tiempo realizar el análisis de mercado. Estas bases de datos son almacenadas en carpetas compartidas en un servidor de acceso general donde cualquiera puede acceder a toda la información sin ningún tipo de restricción porque no existe algún control de seguridad sobre estas carpetas, quedando expuesta la manipulación que se le quiera dar, como eliminación, alteración o robo de la misma.

10. INFORME DE AUDITORIA

A continuación, se presenta un resumen de los hallazgos identificados durante el desarrollo del diseño de la propuesta del Sistema de Gestión de Seguridad de la Información de MA PEÑALOSA CÍA. S.A.S. y algunas recomendaciones para la coordinadora de sistemas.

10.1 HALLAZGOS

Hallazgos 1

Se evidencia que no existe definida una política de seguridad para MA PEÑALOSA CÍA. S.A.S., ni ningún tipo de norma o control establecido para orientar e indicar a los usuarios cómo manejar los asuntos de seguridad.

Recomendaciones

- Definir Políticas de seguridad con el fin de apoyar la toma de decisiones en tareas y procedimientos de forma oportuna a cualquier eventualidad perjudicial o prolongada de las operaciones comerciales de la empresa.

- Divulgar las políticas de seguridad a todos los empleados a través de carteleras informativas de la empresa y realización de capacitaciones.

Hallazgos 2

Se identifica la falta de política para gestión de activos. Se tiene un inventario de los equipos de cómputo, pero no contempla todos los activos informáticos de MA PEÑALOSA CÍA. S.A.S. y sin ningún tipo de codificados que los identifique. No existen regulaciones del uso adecuado y responsabilidades del usuario hacia el equipo a cargo.

Recomendaciones

- Definir una política de gestión de activos con el propósito de alargar la vida útil de los equipos y crear responsabilidad del usuario.

- Se debe actualizar y complementar el inventario de activos para contemplar cada uno de los activos informáticos de MA PEÑALOSA CÍA. S.A.S, identificando el responsable del activo, ubicación, codificación, registro y observaciones del mantenimiento preventivo y correctivo, licencias asociadas, factura de compra y características del activo.

- Se recomienda crear un formato solo para el tránsito de equipos informáticos, ya que actualmente está dentro de la misma carpeta de mercancía, material POP y realizar semanalmente auditoría sobre los registros.

- En el caso de los usuarios externos, se sugiere para el control de los equipos, ya que su tránsito no queda registrado en la carpeta de entrada/salida de mercancía, presentar el equipo completo a la coordinadora de sistemas cada 15 días para controlar el estado de ellos.

- Capacitación a los usuarios sobre el manejo adecuado de los recursos informáticos asignados y sobre medidas de seguridad asociados a ellos.

- Después de creada la política de gestión de activos se deberá informar a los usuarios y en caso de contrataciones nuevas darlas a conocer al personal que ingresa en el momento de recibir los activos designados para la ejecución de sus actividades.

- Establecer procedimiento de altas/bajas de usuario

Hallazgos 3

En el proceso de contratación no se incluye cláusula de confidencialidad ni se capacita al personal a cerca de políticas de seguridad debido a la inexistencia de estas. No existen manuales de procedimientos ni instructivos que cubran todos los procesos a desarrollar por el personal, la capacitación la recibe de otro empleado del área donde trabajará.

Recomendaciones

- Es necesario hacer el levantamiento completo del Sistema de Gestión de Calidad para que, en el proceso de contratación personal, se le entreguen toda la documentación pertinente al cargo a desempeñar como manuales de funciones, procedimientos e instructivos con el fin de que el personal tenga bases y claridad de las actividades a ejecutar.

- Se debe crear una política de seguridad de los recursos humanos que controle la contratación y el término de contrato del personal de MA PEÑALOSA CÍA. S.A.S.

- Con el fin de garantizar la confidencialidad de los datos e información que manejará dentro de MA PEÑALOSA CÍA. S.A.S., se debe incluir de carácter obligatorio dentro del contrato laboral una cláusula de confidencialidad y manifestarle al empleado procesos disciplinarios que implica el no cumplimiento.

- Capacitar al personal en el momento de la contratación sobre las políticas de seguridad.

Hallazgos 4

En los análisis realizados, revela como amenaza la probabilidad de alteración, destrucción, divulgación o robo de la información por falta de control en el manejo de la información y control en el manejo de información en los medios de almacenamiento, motivo por el cual es necesario establecer una política para regular estos riesgos.

Recomendaciones

- Para el control de accesos de usuarios sobre la información es imprescindible la implementación de un directorio activo, ya que centraliza, estandariza y automatiza la gestión de red, gestión de usuarios, seguridad y distribución de recursos.

- Plantear la política de manejo de la información y divulgarla a los usuarios

- Incluir la cláusula de confidencialidad donde el empleado conozca y acepte las condiciones de seguridad que exige la empresa sobre sus activos informáticos.

Hallazgos 5

No hay control de acceso a las instalaciones de MA PEÑALOSA CÍA. S.A.S. El paso de los clientes hacia las áreas de construcción, infraestructura y ferretería ponen en riesgo los activos informáticos y los productos que se almacenan en la bodega. Las cámaras de seguridad no son suficientes para cubrir todo el perímetro de la empresa.

Recomendaciones

- Definir una política de control de acceso que permita regular el acceso de personas externas a la empresa.

- Se debe instalar avisos de señalización para control de paso no autorizado

- Disponer de un espacio en sala para atención de clientes del área de construcción, infraestructura y ferretería, evitando el paso de clientes por bodega, rack principal y otros activos sensibles.

- Instalar cámaras de seguridad en áreas donde no hay cubrimiento.

- Comunicar a asesores de las áreas de construcción, infraestructura y ferretería sobre el espacio que se les destinará para atención de sus clientes.

Hallazgos 6

No hay establecida una política de copias de respaldo, para los procesos de creación de backups de las bases de datos e información de MA PEÑALOSA CÍA S.A.S, son creadas manualmente a criterio de la coordinadora de sistemas y almacenadas en una carpeta en el mismo servidor de base de datos y semanalmente se carga la última copia a una cuenta de Google drive sin encriptar.

Recomendaciones

- Se requiere implementar una política aplicada a la creación de copias de seguridad de la información que contemple la frecuencia, forma de etiquetado, fecha de creación, responsable y ubicación de la copia.

- Las copias de respaldo deben ser automático a través de una tarea programada desde el SQL Server y adicionalmente utilizar un mecanismo de encriptación para luego almacenarse diariamente fuera de las instalaciones de MA PEÑALOSA CÍA. S.A.S.

- En la tarea programada para ejecución de backups se deberá designar una ruta para almacenamiento de ellas. Se recomienda utilizar la carpeta local que se crea de Google Drive para que el proceso quede automáticamente y no dependa del responsable.

- La coordinadora de sistemas deberá semanalmente revisar en la carpeta de Google Drive que se estén guardando satisfactoriamente las copias e ir borrando las copias más antiguas para liberar espacio.

Hallazgos 7

Existen niveles de usuarios para controlar la navegación a través de la solución perimetral (Fortigate), pero el uso no previsto es inevitable y se necesita de una política de uso de internet para establecer medidas de uso.

Recomendaciones

- Definir una política de uso de internet.

- Divulgar política de uso de internet a los usuarios.

- Solicitar capacitación al proveedor sobre el manejo de Fortigate para ajustar niveles de seguridad de navegación.

- Monitorear frecuentemente la navegación y crear reportes quincenales estadísticos sobre el uso del internet.

- Controlar el uso de datos en los móviles de los usuarios remotos para que no los consuman en asuntos personales y ocio.

Hallazgos 8

Se detecta el uso del correo personal para actividades laborales por fallas en el funcionamiento del correo empresarial. Al igual que el uso del correo empresarial para usos personales. También se detecta llegada de correos maliciosos y demoras o problemas de envío y recepción de correos.

Recomendaciones

- Crear una Política de uso de correo electrónico empresarial para establecer directrices sobre el buen manejo del correo.

- Programar capacitación sobre el uso de correo empresarial y las amenazas a través de correos como phishing.

- El usuario debe realizar depuración de correos, borrando regularmente los mensajes que no necesita.

- Capacitar a los usuarios sobre las medidas que se deben tener en cuenta al componer un correo para no ser considerado como SPAM.

Hallazgos 9

La ausencia de un centro de datos es un factor crítico que amenaza los activos informáticos de MA PEÑALOSA CÍA. S.A.S, debido a que no hay control de acceso, inaceptables condiciones ambientales, no existe un extintor cercano en caso de incendio, las UPS no cubren el total de los equipos contenidos dentro del rack principal y están expuestos a desconexión de energía eléctrica.

Recomendaciones

- Implementar con carácter urgente, el centro de datos para resguardar los activos críticos que soportan la infraestructura tecnológica, teniendo en cuenta la norma ANSI/TIA/EIA-569-A**.**

- Establecer políticas sobre el centro de datos que se debe crear para controlar y ofrecer medidas de seguridad garantizando la disponibilidad, integridad y confidencialidad de los activos contenidos dentro de este.

- Realizar estudios de la red eléctrica de MA PEÑALOSA CÍA. S.A.S, con el fin de detectar sobrecargas de energía y fluctuaciones.

- Contemplar y estimar la posibilidad de migrar los servidores a la nube, debido a múltiples amenazas encontradas que pueden afectar la disponibilidad de la información.

- Crear un procedimiento de operaciones del centro de datos con el fin de establecer lineamientos para el correcto funcionamiento del centro de datos de la empresa y respuesta oportuna a eventos que afecten la operatividad.

Hallazgos 10

No existe control en la instalación de software en los equipos, la ausencia de un directorio activo impide la aplicación de políticas de restricción de funcionalidades en los equipos. La coordinadora de sistemas no cuenta con alguna herramienta de control de aplicaciones para monitorear desde una consola por lo que el control

debe hacerse directamente en cada equipo y se realiza cada cuatrimestre en la realización de mantenimientos preventivos. Para las actualizaciones de versiones nuevas de SAP no se tiene ambiente de pruebas para migrar y probar el parche antes de pasarla a producción, aunque se realiza las migraciones en horarios no laborales y se cuentan con copias de respaldo de las bases de datos y los instaladores, resulta riesgoso el proceso y podría causar indisponibilidad del sistema.

Recomendaciones

- Se requiere la definición de una política para uso de software, el cual restrinja las instalaciones no autorizadas de programas.

- Adquirir una herramienta para monitoreo de aplicaciones en los equipos como Solar Winds, Nagios, PRTG con el fin de controlar software pirata.
- La implementación del directorio activo aliviaría muchas de las amenazas que se presentan MA PEÑALOSA CÍA. S.A.S, en este caso aplica también para el control de software instalado.

- Divulgar a los usuarios la política de uso de software.

- Definir ambiente de pruebas y procedimientos para actualizaciones de sistema operativos y software.

Hallazgos 11

Se evidencia falta de política para creación y gestión de contraseñas, los usuarios no cambian con frecuencia las contraseñas, algunos las comparten, utilizan claves débiles para acceder a las aplicaciones y guardan credenciales de inicio de sesión a portales de proveedores en los navegadores.

Recomendaciones

- Definir una política de contraseñas que permita la seguridad de los sistemas de información e ingreso a portales.

- Divulgar la política establecida para conocimiento de todos los usuarios de MA PEÑALOSA CÍA. S.A.S.

- Capacitar al personal sobre las medidas de seguridad que se deben tomar para el manejo de contraseñas.

- Implementar un patrón para generar contraseñas robustas.

Hallazgos 12

Las amenazas rondan a diario a los usuarios, los criminales informáticos van identificando vulnerabilidades de los equipos para seleccionarlos y atacar. Los usuarios de MA PEÑALOSA CÍA. S.A.S. no son conscientes de muchas de estas amenazas, no utilizan o no conocen el uso del antivirus ESET ENDPOINT instalados en sus equipos y se ha detectado a través de la consola del antivirus la presencia de virus en las USB de los usuarios. También se ha detectado ataques que han sido bloqueados desde el Fortigate y correos con contenido maliciosos, el cual el firewall ha logrado detectar en la mayoría de casos.

Recomendaciones

- Capacitar a los usuarios sobre las diferentes amenazas que están expuestos a través de tácticas como ingeniería social, Phishing, pharming
- Capacitar sobre el uso adecuado del antivirus y como analizar los medios de almacenamiento externo a través del antivirus.

- Crear una política de protección contra software malicioso

- Programar el análisis completo de cada equipo con el antivirus por lo menos una vez al mes.

- Crear alertas al correo de la coordinadora de sistemas sobre detección de virus desde el Fortigate y desde la consola del antivirus.

Hallazgos 13

Dejar un equipo desatendido, da lugar a amenazas como sabotaje, robo, destrucción o alteración de la información por descuido del usuario al no bloquear su sesión de usuario.

Recomendaciones

- Implementar una política para equipos desatendidos con el fin de proteger la información.

- Divulgar la política definida sobre equipos desatendidos.

- Capacitar a los usuarios sobre las amenazas al dejar un equipo sin bloqueo de sesión.

Hallazgos 14

El servicio de acceso remoto ofrecido para los usuarios externos, deja una brecha de seguridad para la información de MA PEÑALOSA CÍA. S.A.S, primero porque no se utiliza un canal seguro para las conexiones y segundo porque no existe control sobre horarios para acceder los usuarios al sistema.

Recomendaciones

- Crear una política para control de acceso remoto

- Definir horarios autorizados para conexión de usuarios remotos

- Divulgar política de acceso remoto

- Concientizar a los usuarios sobre el uso adecuado del servicio de acceso remoto.
- Implementar un canal VPN para mejorar la seguridad de transmisión de los datos e información.

- Enfatizar a los usuarios sobre la importancia del manejo de la información a la que tienen alcance y el cumplimiento de los acuerdos de confidencialidad de la información.

- Definir procedimiento para la seguridad de las redes de MA PEÑALOSA CÍA. S.A.S, que incluya la administración del acceso remoto y el monitoreo de la red y los servicios ofrecidos.

Hallazgos 15

Se evidencia la ausencia de control para la gestión de incidentes, no hay bitácoras de seguimiento ni protocolos para reporte de amenazas por parte de los usuarios. Existen casos donde el usuario no informa sobre anomalías.

Recomendaciones

- Establecer una política de gestión de incidentes con el fin de controlar las amenazas presentadas.

- Implementar una bitácora registrando históricos con soluciones aplicadas para atención inmediata.

- Divulgar a los usuarios la política de gestión de incidentes para que conozcan las directrices que deben seguir en caso de una amenaza.

- Realizar una auditoría cada semestre sobre la bitácora de incidentes para identificar fallas e implementar mejoras.

11. SOLUCIÓN A HALLAZGOS DE AUDITORIA

A continuación, se definen algunas políticas basadas en los hallazgos descritos en el informe de auditoría, las cuales servirán como lineamientos para implementar el Sistema de Gestión de Seguridad Informática en MA PEÑALOSA CÍA. S.A.S.

11.1 POLÍTICAS

El Sistema de Gestión de Seguridad de la Información tiene como fin estructurar un sistema de calidad y aseguramiento de la información. Se diseñó para la empresa MA PEÑALOSA CÍA. S.A.S. políticas de seguridad de la información para apoyar la toma de decisiones en tareas y procedimientos de forma oportuna a cualquier eventualidad perjudicial o prolongada de las operaciones comerciales de la empresa.

Cada empleado deberá brindarle capacitación en temas de seguridad de la información y leer las políticas con el fin de conocerlas y aplicarlas, comprometiéndose con el buen uso de los recursos informáticos asignados y preservar la confidencialidad de la información.

11.1.1 Objetivo. Definir e incorporar políticas y medidas de seguridad en el Sistema de Gestión de Seguridad de la Información con el fin de proteger y preservar los activos informáticos y la información garantizando la confidencialidad, integridad y disponibilidad de ellos.

11.1.2 Alcance. Las Políticas de Seguridad de la Información presentadas, se aplican a los activos de información de la empresa MA PEÑALOSA CÍA. S.A.S. de la Sede principal y está orientado a protegerlos de las amenazas que puedan afectarlos.

11.1.3 Nivel de Cumplimiento. Las Políticas de Seguridad que se establezcan dentro del Sistema de Gestión de la seguridad de la Información son necesarias y deben cumplirse por todos los empleados, aprendices Sena, practicantes universitarios o proveedores que tengan acceso a los activos de información de MA PEÑALOSA CÍA. S.A.S.

Debido a la evolución de la tecnología, surgen nuevas amenazas de seguridad no contempladas dentro del documento de políticas de seguridad, MA PEÑALOSA CÍA. S.A.S, tiene derecho a modificar las políticas cuando sea necesario y divulgar

los cambios a los empleados y terceros que les aplique, utilizando estrategias que garanticen la socialización de los mismos.

11.1.4 Sanciones por Incumplimiento. El incumplimiento de cualquier política del presente por negligencia o intencionalmente. MA PEÑALOSA CÍA. S.A.S, tomará las acciones disciplinarias necesarias y legales aplicadas por las autoridades competentes.

11.1.5 Política general. La política de Seguridad y Privacidad de la Información es el compromiso de los directivos de MA PEÑALOSA CÍA. S.A.S con respecto a la protección de los activos informáticos que soportan los procesos de la Empresa y declaran su apoyo a la implementación del Sistema de Gestión de Seguridad de la Información.

MA PEÑALOSA CÍA. S.A.S. Se compromete a proteger la información la información creada, procesada, transmitida o resguardada, orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad y a la continuidad de las operaciones de la empresa. Creando cultura y conciencia de seguridad de la información en los empleados, proveedores y personas que hagan uso de los activos informáticos de la Empresa.

Toda información generada por los empleados, proveedores y practicantes universitarios o aprendices Sena de MA PEÑALOSA CÍA. S.A.S en beneficio y desarrollo de las actividades propias de la empresa es propiedad de MA PEÑALOSA CÍA. S.A.S

MA PEÑALOSA CÍA. S.A.S se compromete a renovar las instalaciones físicas de la empresa a fin de proteger todos los activos informáticos que reposan dentro de la empresa, estableciendo controles de acceso y garantizando adecuadas condiciones ambientales.

MA PEÑALOSA CÍA. S.A.S procura dar cumplimiento a normatividades y leyes creadas para proteger la información.

11.1.6 Política de Gestión de Activos

- La coordinadora de sistemas debe disponer de un inventario de los activos informáticos de MA PEÑALOSA CÍA. S.A.S. y mantenerlo actualizado.

- Es responsabilidad de la coordinadora de sistemas crear una codificación para identificar cada activo informático.

- Es responsabilidad de la coordinadora de sistemas crear una hoja de vida para cada activo informático donde se evidencie toda la información referente a este, factura de compra, datos de licenciamiento de SW e historial de mantenimientos preventivos y correctivos.

- La coordinadora de sistemas debe participar en la definición de pólizas de seguros que cubran los activos informáticos en caso de siniestro.

- La coordinadora de sistemas al asignar equipos a los empleados nuevos, deberá diligenciar de forma completa el formato de entrega de herramientas de trabajo, donde se evidencie descripción de la herramienta entregada, serial, cantidad, observaciones si son necesarias y hacer firmar el formato por el empleado.

- La coordinadora de sistemas es responsable de asegurar con guayas de seguridad los equipos portátiles entregados a los empleados y por parte del empleado es responsable revisar que su equipo de cómputo este siempre asegurado y si no debe informar inmediatamente.

- Una vez finalizado el contrato de trabajo, el empleado deberá hacer entrega de los implementos informáticos a la coordinadora de sistemas, para que este genere un formato donde quede constancia de la entrega de estos y se haga revisión de su estado, a su vez la coordinadora de sistemas validando lo anterior procederá a firmar paz y salvo.

- Para los empleados de ferretería que habitualmente salen con sus equipos portátiles, deben ser cautelosos con la manipulación de los activos y la seguridad de los mismos, en caso de pérdida o robo deberán informar a la coordinadora de sistemas y poner un denuncio a la policía. Deberán presentar los equipos cada 15 días a la coordinadora de sistemas para control de estado del activo.

- Para otros empleados que requieran sacar algún activo informático de las instalaciones de MA PEÑALOSA CÍA. S.A.S, deberá solicitar la carpeta de salida de mercancía al Jefe de Bodega, diligenciar la carpeta de registros y solicitar la firma de autorización a las personas con autoridad.

- Los equipos informáticos asignados son para uso laboral y para almacenamiento de información sus actividades laborales.

- Está prohibido el intercambio de partes como cargadores, mouse o teclados, en caso de requerir cambio por daños o mal funcionamiento debe reportase a la coordinadora de sistemas para su diagnóstico, reparación o reposición.

- Es responsabilidad del empleado mantener su equipo en buenas condiciones, está prohibido pegarle stickers, marcarlos o rayarlos.

11.1.7 Política de seguridad de los recursos humanos

- Es responsabilidad de la líder de calidad, verificar la veracidad de la documentación de la hoja de vida del aspirante al cargo antes de la contratación.

- El Gerente de MA PEÑALOSA CÍA. S.A.S deben exigir que todos los empleados conozcan y cumplan las políticas establecidas para la seguridad de los activos informáticos.

- Al inicio de actividades laborales del empleado nuevo, la líder de calidad debe entregar las funciones y responsabilidades del puesto de trabajo. De igual manera, hacer firmar el acuerdo de confidencialidad, y guardar copia en el archivo junto con la hoja de vida y contrato laboral.

- Al término de contrato algún empleado, la líder de calidad deberá informar a la coordinadora de sistemas para inactivar cuentas de usuario y solicitar la entrega de implementos de trabajo entregados al inicio de contrato.

- Con el propósito de cumplir con la ley de protección de datos, la información confidencial de cada empleado deberá archivarse de forma que solo tendrán acceso las personas autorizadas por el Gerente.

- El Gerente de MA PEÑALOSA CÍA. S.A.S. con apoyo de la coordinadora de sistemas deberán promover capacitaciones a los empleados sobre temas de seguridad de la información con el fin de mantenerlos informados y prevenir amenazas informáticas.

11.1.8 Política de Manejo de Información

- Todo candidato que aspire a un determinado cargo dentro de MA PEÑALOSA CÍA. S.A.S, adicional a su contrato de trabajo deberá firmar un acuerdo de confidencialidad, en el cual acepta las cláusulas donde se comprometen a no divulgar, usar o robar información de la empresa a la cual tenga acceso.

- Es necesario no entregar ningún tipo de información confidencial por teléfono, por celular, por mensajería instantánea, por correo electrónico, hasta no ser verificada la identidad del solicitante.

- La coordinadora de sistemas, como administradora de servidores y bases de datos debe garantizar la confidencialidad de la información y el uso de credenciales de acceso a las diferentes plataformas.

11.1.9 Política de Acceso físico

- Todas las áreas donde se encuentren activos informáticos, así como el acceso a las diferentes oficinas, deben de ser protegidos contra accesos no autorizados, utilizando procedimientos, monitoreo y registro de entrada y salida.

- MA PEÑALOSA CÍA. S.A.S deberá disponer de cámaras de vigilancia para monitorear eventos de seguridad.

- Todos los proveedores y contratistas deben portar en un lugar visible el carnet que los identifica para el acceso a la empresa.

- Los asesores comerciales de construcción, ferretería e infraestructura deberán atender a sus clientes en la sala de ventas para evitar el paso a la bodega.

- Debe contratarse un vigilante para mantener la seguridad dentro de las instalaciones de la empresa.

- La coordinadora de Sistema de Gestión de calidad, debe mantener señalizada las áreas de accesos no autorizados y demarcación de zonas de trabajo.

11.1.10 Política de copias de respaldo

- La coordinadora de sistemas es la responsable de realizar los respaldos de la información almacenada en los servidores y por ende de las bases de datos, a través de una tarea programada desde el SQL Server para que se generen automáticamente, definir el contenido de los respaldos, tipo de respaldo, la frecuencia del respaldo, la codificación para identificarlos y la ubicación de estos.

- La coordinadora de sistemas debe mantener un inventario de las copias de respaldo de la información del sistema de Información, Nómina, configuración del Fortigate, carpeta de archivos compartidos, repositorios de adjuntos del sistema de información, entre otros.

- La coordinadora de sistemas debe verificar la correcta ejecución de los procesos de backup, y el estado del inventario de los respaldos.

- Las copias de seguridad se guardarán con el objetivo de utilizarse en caso de contingencia para la recuperación de la información luego de haberse presentado una amenaza ya sea por ataque de un virus informático, daños lógicos de los equipos, contaminación, catástrofes ambientales o industriales, donde se necesite restaurar el sistema.

- La coordinadora del sistema será la responsable de almacenar las copias de seguridad en un área donde se tenga control de acceso y otra ubicación fuera de las instalaciones de la empresa ya sea de forma física o almacenada en un espacio en la nube como Google Drive donde solo tendrá acceso la coordinadora de sistemas y el gerente.

- La coordinadora de sistemas deberá cifrar las copias de respaldo de la base de datos a través de herramientas como GPG para asegurar la confidencialidad en otro lugar fuera de las instalaciones de MA PEÑALOSA CÍA. S.A.S o en la nube.

- La coordinadora de sistemas deberá mantener en su custodia las claves para desencriptar las copias de seguridad en caso de requerirse.

- Es necesario tener un plan de contingencia en el cual se detalle el uso de las copias de respaldo de la información para restaurar el sistema en caso de un siniestro.

- Los usuarios no podrán guardar información en el servidor de archivos compartidos que no sea pertinente a la empresa. Se prohíbe guardar información personal como fotos, documentos, música o videos.

- La coordinadora de sistemas solo se responsabilizará por realizar copias de seguridad de información de los usuarios que estén contenidas en el servidor de archivos compartidos. Los usuarios son responsables de la información local de sus equipos.

- La coordinadora de sistemas tiene la obligación de entregar al gerente o la persona de reemplazo las claves para desencriptar las copias de seguridad.

11.1.11 Política de uso de internet

- El acceso a internet es un recurso para contribuir a actividades laborales como accesos a portales de proveedores, portales bancarios, portales gubernamentales entre otros según las necesidades del cargo y funciones desempeñadas

- El acceso a redes sociales no es permitido a excepción de la persona encargada del manejo comercial y promocional de la empresa.

- Los empleados autorizados para el uso de Internet, no podrán descargar, copiar, instalar software que necesiten de licenciamiento y que puedan generar sanciones a la empresa por derechos de autor.

- La coordinadora de Sistemas, definirá niveles de acceso a internet aplicado a los usuarios, bloqueando accesos a sitios web que sean categorizados como inapropiados a través del Fortigate y en caso de que se requiera algún permiso especial debe ser autorizado por gerencia.

- Los usuarios son responsables de las actividades que se realicen desde sus equipos hacia internet, por eso la importancia de cuidar sus sesiones.

- Cada usuario es responsable de cualquier evento no deseado que provoque al intentar acceder a algún sitio no autorizado.

- Los empleados autorizados para el uso de Internet deben reportar al área de Sistemas, cualquier anomalía que pueda afectar la seguridad de la información de la empresa.

- No dejar abierto el navegador, cerrar la sesión cuando no se esté utilizando Internet. De esta manera se evita el consumo de ancho de banda innecesario.

- La coordinadora de sistemas debe programar la descarga de las actualizaciones del sistema operativo en horas que no afecte las actividades del negocio.

- Para ingreso a portales bancarios digitar la URL y verificar que sea establezca conexión segura a través de HTTPS y usando el token proporcionado por la entidad bancaria.

- Los usuarios por seguridad no deben guardar credenciales cuando se los pregunte el navegador utilizado al ingresar a algún sitio.

- Solicitar reporte mensual al proveedor de servicios móviles, el consumo de datos de los equipos de los asesores con el fin de monitorear el uso.

11.1.12 Política de uso de correo electrónico empresarial

- El correo empresarial deberá ser creado por la coordinadora de sistemas para los empleados autorizados por gerencia.

- Todos los mensajes tanto enviados o recibidos por medio de correo electrónico empresarial pertenecen a MA PEÑALOSA CÍA. S.A.S y está podrá acceder a ellos cuando lo requiera.

- El correo empresarial solo será utilizado con propósitos laborales.

- Es responsabilidad del empleado evitar que su cuenta de correo electrónico sea utilizada por terceros.

- La coordinadora de sistemas debe supervisar que todos los correos empresariales creados deben configurársele la firma digital del empleado que hará uso.

- No se permite el envío de spam a clientes con fines comerciales

- Será sancionado el uso del correo empresarial para cometer acciones ilícitas.

- El empleado es responsable de cualquier archivo adjunto que envíe a terceros a través del correo empresarial.

- El empleado debe ser precavido con la descarga de archivos adjuntos que reciba de terceros a través del correo empresarial.

- Está prohibido configurar la cuenta de correo empresarial en el dispositivo móvil personal del empleado.

- Es responsabilidad del empleado archivar los mensajes de correos electrónicos para efectos de soportar ante terceros en caso de requerirse.

- La coordinadora de sistemas definirá el tamaño del buzón de acuerdo a las actividades que desempeñará el empleado y a la capacidad del Hosting contratado.

- Está prohibido abrir correos personales dentro de las instalaciones de MA PEÑALOSA CÍA. S.A.S y compartir a los clientes otro tipo de correo que no sea el empresarial.

- Ningún usuario tiene información de la cuenta de correo electrónico empresarial, ya que esta se entrega configurada en el Outlook del equipo asignado.

- La coordinadora de sistemas debe tener un inventario sobre las cuentas de correos creadas y sus respectivas contraseñas.

- La coordinadora de sistemas debe utilizar contraseñas seguras basadas en la política de gestión de contraseñas.

- La coordinadora de sistemas será la encargada de crear y administrar las cuentas de correo de Gmail para la configuración de las cuentas de Google Play Store de los smartphones.

- Los usuarios no podrán configurar cuentas de correos personales en los celulares asignados por la empresa.

- La coordinadora de sistemas podrá desactivar las cuentas de correo que no demuestren su uso durante más de dos (2) meses consecutivos.

- La líder de calidad deberá informar a la coordinadora de sistemas sobre usuarios que saldrán a vacaciones o licencias de trabajo, para desactivar temporalmente las cuentas y configurar un mensaje de respuesta automática, con el fin de evitar que los buzones de mensajes se llenen y bloqueen las demás cuentas.

- Las cuentas de correo serán desactivadas después de 8 días hábiles a partir de la fecha en la cual la persona termine su vinculación con la empresa.

- La coordinadora de sistemas deberá crear medidas de control en el Fortigate y en el servidor de correos para filtrar correos maliciosos con contenidos perjudiciales.

- Al crear correos deben tener en cuenta factores claves para que los analizadores de correos no clasifiquen el correo como SPAM: evitar uso de Mayúsculas en el asunto, uso excesivo de signos de admiración o símbolos, evitar el envío de correos con solo imágenes, entre otros.

11.1.13 Política de seguridad del centro de datos

- MA PEÑALOSA debe disponer de un área restringida para la ubicación de los activos informáticos críticos que soportan la infraestructura tecnológica del sistema de información.

- Este centro de datos debe tener un sistema de refrigeración por aire acondicionado que mantenga la temperatura adecuada, las tomas eléctricas deben estar debidamente organizados e instalados bajo las normas RETIE.

- La coordinadora de sistemas debe garantizar que todos los activos informáticos ubicados dentro del centro de datos estén protegidos con UPS, el cual permita un

tiempo considerable mientras se restablece la energía o se realice un apagado correcto.

- Dentro del centro de datos se prohíbe comer o beber.

- En el centro de datos no debe almacenarse papelería, materiales inflamables o combustibles que generen riesgo de propagación de fuego.

- Las puertas del centro de datos deben permanecer cerradas. La coordinadora de sistemas será el responsable de las llaves del sitio.

- En la realización de mantenimientos dentro del centro de datos o soportes por parte de proveedores del servicio de comunicaciones deberán ser supervisadas por la coordinadora de sistemas.

- Se debe disponer de un extintor tipo C dentro del centro de datos en caso de emergencia.

- Debe controlarse y vigilarse el acceso al centro de datos, ya que contiene los activos informáticos críticos.

- Se debe señalizar el área, informando sobre acceso no autorizado.

11.1.14 Política de uso de software

- No está permitido la descarga ni instalación de software sin autorización previa de la coordinadora de sistemas, con el fin de evitar piratería y sanciones de tipo legal para MA PEÑALOSA CÍA. S.A.S.

- La coordinadora de sistemas deberá mantener inventariada las licencias con sus respectivos soportes de compra y medios de instalación

- La coordinadora de sistemas deberá velar por la vigencia de las licencias del software adquiridos.

- Es responsabilidad de la coordinadora de sistemas, instalar el software necesario para cada equipo de cómputo del empleado de MA PEÑALOSA CÍA. S.A.S.

- En caso de fallas del software y se solicita mantenimiento correctivo en el cual se repare o se actualice deberá quedar registrado en la hoja de vida del equipo de cómputo donde se presentó.

- La coordinadora deberá supervisar los mantenimientos correctivos, en caso de formateo de un equipo, suministrar al técnico los medios de instalación, licencias y exigir no realizar ningún tipo de instalación de software pirata o instalaciones sin autorización previa.

11.1.15 Política de contraseñas

- Es responsabilidad de cada empleado hacer buen uso de las cuentas de usuario asignadas sea para acceso al equipo, acceso remoto o sistemas de información de la empresa, evitando compartir el uso de las cuentas, ni dejando en evidencia los datos de acceso que puedan ser usados por otra persona.

- La coordinadora de sistemas inicialmente asignará la contraseña al empleado, pero deberá configurarse de tal manera que solicite ser inmediatamente cambiada en el primer inicio de sesión, cumpliendo con algunos parámetros de seguridad:

  - Tener mínimo ocho caracteres.

  - La contraseña debe estar compuesta por caracteres: mayúsculas, minúsculas, numéricos y algún carácter especial.

  - La contraseña no debe ser igual o parecida a la anterior.

- La coordinadora de sistemas debe definir una política para que le exija al empleado el cambio de contraseña cada 30 días, el sistema debe informarle al empleado 5 días antes de su vencimiento.

- La coordinadora de sistemas no restablecerá la contraseña a un usuario, a menos que este mismo lo solicite y se identifique a sí mismo.

- Los usuarios deben utilizar diferentes contraseñas de acceso a los diferentes accesos que hayan sido otorgados.

- Todos los empleados que tengan cuentas de usuario deberán cambiar las contraseñas en caso de que exista o haya algún indicio de una posible vulnerabilidad del sistema.

- Si al superar cinco intentos consecutivos al acceder a una cuenta de usuario de equipo o al sistema sin éxito, la cuenta se bloqueará por motivos de seguridad en la cual tendrá que intervenir la coordinadora de sistemas.

- La coordinadora de sistemas debe bloquear inmediatamente las cuentas de usuarios de empleados que se les haya terminado el contrato.

11.1.16 Política de protección contra software malicioso

- Es responsabilidad de la Coordinadora de sistemas gestionar el licenciamiento del antivirus que brinde protección contra software malicioso.

- La Coordinadora de sistemas debe instalar en cada equipo de cómputo y servidores el software antivirus.

- Es responsabilidad de la coordinadora de sistemas monitorear desde la consola del antivirus las actividades anormales que se presentan para mitigar los riesgos.

- Los empleados deben reportar fallas si el antivirus informa alguna falla o detección de virus.

- Los empleados deberán analizar previamente con el antivirus el medio de almacenamiento como USB antes de abrir los archivos contenidos para evitar riesgos de seguridad a MA PEÑALOSA CÍA. S.A.S.

- No está permitida la utilización de medios de almacenamiento virtual que no estén previamente autorizados por la Coordinadora de sistemas.

- Cualquier sospecha de anomalías en el equipo asignado a causa de infección de virus, deberá suspender el uso del equipo e informar inmediatamente a la coordinadora de sistemas para revisión y solución de amenaza.

11.1.17 Política de equipo desatendido

- La Coordinadora de Sistemas debe garantizar que todos los equipos de cómputo estén configurados de tal forma que cuando detecte el sistema periodos de inactividad del empleado, después del tiempo establecido se bloquee la sesión del usuario y requiera de datos de accesos para iniciar sesión.

- Es responsabilidad del empleado al realizar pausas activas o alejarse del puesto de trabajo, bloquear la sesión para evitar suplantación de identidad, sabotajes o robo de información.

- Los usuarios no deben utilizar el sistema de una sesión que no sea el designado.

- El usuario deberá asumir parte de las responsabilidades presenta en su sesión de usuario en caso de algún incidente ya sea por préstamo de credenciales o por no bloquear su sesión.

11.1.18 Política de Acceso remoto

- El servicio de acceso remoto solo será habilitado a usuarios con fines laborales.

- El servicio de acceso remoto debe permitir solo acceso al sistema de información de la empresa y a archivos compartidos en la intranet.

- Los usuarios externos solo aplican para asesores comerciales de ferretería y los usuarios de las demás sedes. En caso de alguna excepción o permiso especial deben ser autorizados por el gerente de MA PEÑALOSA CÍA. S.A.S.

- La coordinadora de sistemas debe definir un canal seguro para la conexión de usuarios externos a través de la configuración y asignación de datos de acceso a los empleados a la VPN de la empresa.

- La Coordinadora de sistemas deberá configurar políticas en el servidor donde se conectan los usuarios remotos para que después de determinado tiempo de inactividad o detección de usuarios desconectados, las sesiones se cierren completamente evitando el consumo de recursos por procesos activos en el servidor sin utilizarse.

- La Coordinadora de sistemas deberá gestionar licencias de usuarios remotos necesarios para el acceso al servidor de Terminal Services.

- Está prohibido utilizar herramientas de soporte de remoto como Anydesk, Team viewer, Zoom, etc. Solo se podrán utilizar con autorización y supervisión de la coordinadora de sistemas.

- La coordinadora de sistemas debe garantizar la disponibilidad del servicio de internet a los usuarios remotos para que accedan al sistema.

11.1.19 Política de gestión de incidentes

- MA PEÑALOSA CÍA. S.A.S, debe establecer procedimientos para la gestión y tratamiento de incidentes de seguridad de la información, con el fin de detección temprana y prevención de incidentes, crear una bitácora de incidentes con su respectiva solución para ir documentando los planes de acción ante determinada incidencia y auditar la respuesta a de incidentes para una mejora continua de cómo enfrentar nuevos incidentes.

- Los empleados están obligados a reportar a la coordinadora de sistemas situaciones sospechosas o anomalías que puedan considerarse como incidencias

de seguridad informática. A su vez la coordinadora de sistemas deberá analizar y valorar la incidencia reportada y comunicarla al Gerente para mantenerlo informado. En última instancia el Gerente evaluará la incidencia y tomará acciones sancionar al implicado o si hay necesidad de recurrir ante las autoridades competentes.

- Toda la información referente a los incidentes reportados, debe ser manejada con discreción y confidencialidad.

11.2 PROCEDIMIENTOS

Con el fin de apoyar en la solución de los hallazgos descritos en el numeral 10. A continuación se presentan algunos procedimientos que pueden aplicarse a MA PEÑALOSA CÍA. S.A.S., para control de algunos procesos que conllevan al mejoramiento y protección de los activos informáticos.

11.2.1 Procedimiento de Gestión de usuarios. El proceso de creación o eliminación de usuarios requiere atención oportuna para que el personal inicie sus actividades laborales y en el caso de cese de actividades por motivos de seguridad, debe bloquearse las cuentas asociadas al usuario que no laborará más en la empresa ya que podría dar lugar a algún delito informático como fuga o robo de información.

Objetivo. Establecer los lineamientos para gestionar usuarios.

Alcance. El procedimiento de gestionar de usuario, considera los pasos a seguir cuando se presentan novedades de empleados ya sea por retiro o ingreso yaplica a empleados de MA PEÑALOSA CÍA. S.A.S., que tendrán acceso a los sistemas de información.

Responsabilidades

Coordinadora de sistemas.

- Vigilar el cumplimiento del procedimiento.

- Asignar cuentas de usuarios para los diferentes accesos según rol a desempeñar.

- Informar a Gerencia en caso de faltantes de licencias de usuario para realizar compra.

- Mantener registro de inventario de cuentas creadas e historial de cambios de usuarios.

Líder de calidad.

- Solicitar e informar a la coordinadora de sistemas la vinculación y desvinculación de empleados que tengan designados equipos de cómputo y acceso al sistema.

Usuario.

- Cumplir con los acuerdos de confidencialidad.

- No compartir credenciales de cuentas de usuarios asignadas con otros empleados.

Descripción

La líder de calidad informa a la coordinadora de sistemas sobre dar alta o baja a un usuario a través de correo electrónico. La solicitud debe indicar datos básicos del empleado como número de documento de identificación, nombre completo, cargo y área.

- Si corresponde a solicitud de creación de nuevo usuario, se debe contar adicionalmente con datos como teléfono, dirección, correo electrónico, así como rol que desempeñará para definir el perfil de la cuenta de usuario. Los datos deben enviarse completos para procesar la solicitud.

- Seguidamente se dan permisos de acceso a la red, se asigna usuario y licencia para SAP B1, asignación de correo empresarial y si es usuario remoto se crea también cuenta de usuario remoto.

- Se envía correo electrónico de respuesta al líder de calidad informando de las cuentas y perfiles creados. Se envía a la cuenta de correo electrónico proporcionada los datos de acceso a SAP y en caso de requerirse la cuenta de remoto con los enlaces de acceso correspondientes. Se envía adjunto copia del manual de políticas de seguridad de la empresa.

- Si la solicitud corresponde a retiro de usuario se debe informar la fecha a partir de la que el usuario ya no tendrá más acceso al sistema de información de la empresa.

- Se realiza la inactivación de las cuentas creadas del usuario en la fecha informada.

- Se envía correo electrónico al líder de calidad y al correo personal del empleado retirado, informando que a partir de la fecha establecida ya no tendrá acceso a los recursos informáticos de la empresa.

11.2.2 Procedimiento Mantenimiento Preventivo. Los activos informáticos correspondientes a hardware y software requirieren de un mantenimiento trimestral, con el fin de alargar la vida útil de los equipos y evitar fallos de los equipos, logrando prevenir las incidencias antes de que estas ocurran.

Objetivo. Crear un cronograma anual de mantenimiento preventivo de los activos informáticos de la empresa que soportan los datos y aplicarlo, con el fin de protegerlos y mantenerlos en condiciones aptas para garantizar el buen funcionamiento y rendimiento del sistema de información.

Alcance. Este procedimiento es aplicable para cubrir el servicio de mantenimiento preventivo de los activos informáticos y de redes que sean de propiedad de la empresa y correspondan a la sede Principal de MA PEÑALOSA CÍA. S.A.S.

Responsabilidades

Coordinadora de sistemas.

- Verificar el cumplimiento del procedimiento.

- Supervisar la ejecución de los mantenimientos preventivos en las fechas estipuladas y bajo las condiciones en las que se contrató el servicio con el proveedor.

- Revisar y firmar los reportes de mantenimiento

- Verificar registros de las actividades y observaciones realizados en la hoja de vida de cada activo informático.

Técnico de mantenimiento.

- Cumplir con el soporte programado.

- Utilizar los implementos de protección necesarios para realizar las actividades de mantenimiento.

- Informar de cualquier novedad que evidencie en los activos informáticos a la coordinadora de sistemas

- Registrar y documentar las actividades realizadas en las hojas de vida de los activos e informes de soporte.

Descripción. La Coordinadora de Sistemas deberá acordar junto con el proveedor contratado de los mantenimientos, la programación anual de los mantenimientos preventivos. El contrato deberá incluir, frecuencia de mantenimientos, sedes las cuales se le harán mantenimiento, cantidad de equipos por sedes, recomendaciones de utilización de implementos de protección necesarios para la realización de las actividades, entregar mensualmente copias del pago de seguridad social y demás parafiscales del técnico encargado y si la actividad a realizar lo requiere deberá certificar curso de altura.

- Elaborar y publicar programa general de mantenimientos preventivos, para que los usuarios estén atentos a la fecha correspondiente a su equipo.

- Informa a los usuarios y a los proveedores sobre la realización de actividades programadas de mantenimiento preventivo.

- En el momento de realización de los mantenimientos preventivos por parte del proveedor, darle las indicaciones y recomendaciones necesarias sobre las actividades a realizar como:

  - Limpieza física de los equipos, si hay algún equipo en garantía no destapar.

  - Limpieza de software: borrado de temporales, análisis del antivirus, revisión de instalación de software no autorizado.

  - Revisión lógica: ejecución de scandisk, desfragmentación del disco.

  - Actualizaciones pendientes de software.

  - Revisión de batería de UPS

- Registrar en cada orden de mantenimientos, la fecha, número de equipo, serial del equipo, actividades realizadas dentro en cada equipo, novedades, fallas encontradas.

- La Coordinadora de sistemas deberá supervisar la jornada de mantenimientos, para verificar el trabajo realizado en cada equipo, dando su aprobación en cada orden de mantenimiento.

- En caso de que el técnico encuentre una falla y sea necesario reemplazar algún componente, como por ejemplo la batería de la UPS, deberá registrarlo e informarle a la coordinadora de Sistemas.

- La Coordinadora de sistemas hará las cotizaciones pertinentes referentes a la parte afectada y si es de cambio urgente, presentará las necesidades al Gerente para que apruebe la asignación de presupuesto.

11.2.3 Procedimiento Mantenimiento Correctivo. El mantenimiento correctivo se origina inesperadamente a causa de una falla o avería en un activo informático por tal motivo no se puede considerar como una actividad planificable, en caso de falla en hardware puede representar costos por cambio o reparación del componente.

Objetivo. Realizar mantenimiento correctivo de los activos informáticos de la empresa, que soportan los datos con el fin reparar daños y reestablecer el buen funcionamiento del mismo.

Alcance. Este procedimiento es aplicable para cubrir el servicio de mantenimiento correctivo de los activos informáticos y de redes que sean de propiedad de la empresa y correspondan a la sede Principal de MA PEÑALOSA CÍA. S.A.S.

Responsabilidades

Coordinadora de sistemas.

- Vigilar el cumplimiento del procedimiento.

- Supervisar las actividades realizadas por el técnico que brinda el soporte, enviado por el proveedor contratado.

- Analizar la valoración del activo dada por el técnico para tomar decisiones.

- Gestionar la compra de la pieza o activo averiado con el Gerente.

- Verificar que el activo que presenta fallas quede funcional.

- Asegurarse de que el registro de las actividades realizadas haya quedado detallado en la hoja de vida del activo informático afectado.

Técnico de mantenimiento.

- Atender el soporte de acuerdo a los niveles de atención contratadas.
- Utilizar los implementos de protección necesarios para realizar las actividades de mantenimiento.

- Informar de cualquier novedad que evidencie en los activos informáticos a la coordinadora de sistemas para cambio de partes.

- Registrar y documentar las actividades realizadas en la hoja de soporte.

Usuario.

- Informar el mal funcionamiento del activo informático.

- Describir las acciones que estaba realizando en el momento de presentar la falla.

- Realizar pruebas sobre el activo para confirmar solución de falla.

Descripción. La Coordinadora de sistemas deberá descartar fallas de primer nivel, con el fin de resolver.

- Si es algo crítico, solicitar el servicio de mantenimiento correctivo al proveedor. Llamando a la línea de soporte, para que se agende el servicio según la prioridad que se le asigne.

- Registrar en la orden de mantenimientos, la fecha, número de equipo, serial del equipo, actividades realizadas dentro en cada equipo, novedades, fallas encontradas.

- En caso de que el técnico encuentre una falla y sea necesario reemplazar algún componente, como por ejemplo la batería de la UPS, deberá registrarlo e informarle a la coordinadora de sistemas.

- La Coordinadora de sistemas hará las cotizaciones pertinentes referentes a la parte afectada y si es de cambio urgente, presentará las necesidades al Gerente para que apruebe la asignación de presupuesto.

- La Coordinadora de sistemas deberá supervisar la jornada de mantenimientos, para verificar el trabajo realizado en cada equipo, dando su aprobación en la orden de mantenimiento.

- Evaluar el servicio prestado para garantizar la calidad de este.

11.2.4 Procedimiento Gestión de Incidentes. La gestión de incidentes consiste en resolver de manera rápida y eficaz, cualquier evento causante de interrupción parcial o total de las actividades realizadas por un activo informático, comprometiendo la confidencialidad, integridad, disponibilidad, autenticidad o confiabilidad de la información.

Objetivo

- Definir responsables que atiendan los incidentes y garanticen la operatividad del negocio, la continuidad y la disponibilidad del servicio.

- Establecer el seguimiento que se debe aplicar a los incidentes de seguridad de la información para ser analizados y clasificados.

- Aplicar salvaguardas adecuadas a los incidentes en la empresa y operaciones de negocio con el fin de mitigar el impacto causado.

- Llevar bitácora de incidencias ocurridas, las cuales incrementa las oportunidades de prevenir las ocurrencias de futuros incidentes.

Alcance. Este procedimiento contempla desde la detección y reporte de Incidentes por parte del usuario, hasta el seguimiento que le dé el responsable de la gestión de incidentes: recepción, análisis de Incidentes, rastreo de ataque, custodia de evidencia, recuperación de datos o sistemas afectados, restauración de la información y registro en bitácora para manejo de incidentes futuros.

Responsabilidades

Coordinadora de sistemas.

- Vigilar el cumplimiento del procedimiento.
- Bloquear conexiones de red del equipo afectado para evitar replicas.
- Resolver la incidencia y solicitar apoyo al proveedor si es necesario.
- Documentar las incidencias para prevenir futuras amenazas.

Usuario.

- Informar incidente inmediatamente a la coordinadora de sistemas.
- Describir las acciones que estaba realizando en el momento de presentar la falla.
- Seguir indicaciones y recomendaciones dadas por la coordinara de sistemas.

Descripción. En el momento en que se detecte comportamientos extraños en el funcionamiento de un equipo o servicio prestado en MA PEÑALOSA CÍA. S.A.S, el usuario tiene la obligación de informar inmediatamente a la coordinadora de Sistemas, la cual validará el incidente e informará al Gerente si el impacto es alto.

A continuación, se detallarán indicaciones de cómo debe proceder la coordinadora de sistemas ante un incidente:

- Desconectar el equipo afectado para aislarlo de la red.

- El usuario responsable del equipo afectado debe brindar información y el apoyo que requiera la coordinadora de sistemas para realizar el levantamiento de información.

- La Coordinadora de sistemas determinará el origen y destino de la incidencia.

- Analizar el impacto causado en el equipo o sistemas involucrados.

- Etiquetar y poner en custodia la evidencia

- Identificar y aplicar el tratamiento o solución al incidente

- Documentar el Incidente en una bitácora, teniendo en cuenta aspectos como:

✓ Fecha
✓ Equipo afectado
✓ Responsable del equipo
✓ Resumen del incidente
✓ Acciones realizadas.
✓ Evidencias recopiladas
✓ Observaciones.
✓ Recomendaciones
✓ Tratamiento de la incidencia.

- Si el incidente tiene probabilidad de replicarse en otros equipos, la coordinadora de sistemas implementará las mismas medidas preventivas en los demás equipos.

- La Coordinadora de sistemas tiene el deber de reportarle al gerente los incidentes presentados si es de alto impacto en el mismo instante o si es de medio o bajo luego de solucionarlo.

- La coordinadora de sistemas deberá dar recomendaciones a los usuarios si es necesario realizar capacitación sobre las medidas preventivas.

- Los usuarios responsables de los equipos involucrados deben acatar las medidas correctivas indicadas por la coordinadora.

- Una vez concluido el proceso de descartes de incidentes o restauración del equipo, la coordinadora de sistemas restablecerá las conexiones de red al equipo.

11.2.5 Procedimiento de actualización de Sistemas Operativos y Software. Los fabricantes de software constantemente están liberando nuevas versiones, parches de actualizaciones aplicadas a sistemas operativos, aplicaciones, controladores de hardware, antivirus para corregir fallas de seguridad, mejoras o corrección de errores para mitigar vulnerabilidades.

Objetivo. Definir los lineamientos para llevar a cabo procesos de actualización y cambios en los sistemas operativos y software.

Alcance. El procedimiento contempla indicaciones para efectuar actualizaciones y cambios en los sistemas operativos y software autorizados por Gerencia y la coordinadora de sistemas.

Responsabilidades

Coordinadora de sistemas.

- Controlar el cumplimiento del procedimiento.

- Mantenerse informada de actualizaciones y mejoras de sistemas operativos y software.

- Tener un ambiente de pruebas para las actualizaciones.

- Programar horarios de actualizaciones para no afectar la operatividad de actividades.

- Informar y solicitar autorización a Gerencia para programación de actualización críticas.

- Realizar pruebas de migraciones en ambiente de pruebas antes de pasar a producción.

- Documentar cambios de sistemas operativos y software para control y seguimiento.

- Solicitar generación de licencias en caso de necesitarse.

Proveedor de software.

- Proveer repositorios para descarga de instaladores de actualizaciones.
- Proveer información sobre mejoras y versiones.
- Proveer licencias
- Ofrecer acompañamiento y canales de soporte

Gerente.

- Dar apoyo y autorización a la coordinadora de sistemas para la realización de actualizaciones.

- Coordinar la seguridad de las instalaciones para trabajar en actualizaciones en días no laborables.

Descripción

- Sistemas Operativos de Servidores

Se deberá abrir una ventana de mantenimiento para programar la actualización del sistema operativo de los servidores. Debido a que para este proceso se requiere el reinicio del servidor, debe programarse en horario que no afecte la actividad laboral.

Algunas actualizaciones pueden generar incompatibilidades con las aplicaciones, por lo tanto, es necesario revisar e investigar sobre los parches liberados por los fabricantes antes de cualquier cambio.

- Sistemas Operativos de PC

Para no afectar el ancho de banda de internet, es necesario configurar en los equipos que el horario para realizar las actualizaciones del sistema operativo se haga en un horario determinado que no afecte las actividades laborales del empleado y evitar que estas no se descarguen en todos los equipos simultáneamente. Por tal motivo no se deben dejar automáticas sino programarse.

- Software de los servidores.

Este tipo de actualizaciones aplica para el ERP SAP B1, proceso complejo donde en ciertos casos se requiere de apoyo del Partern. Estas actualizaciones necesitan programarse en horarios no laborales ya que debe detenerse el servicio por cambio en los archivos de configuración asociados al software. Por recomendaciones del Partern es indispensable tener un ambiente de pruebas, donde se tenga réplica de los servidores y desplegar la actualización y comprobar su buen funcionamiento antes de lanzarlo a producción y generar caos si se presenta fallas.

Para actualizaciones de firmware o sistema de algún hardware como el Fortigate, es necesario tener respaldo de la configuración del equipo y programar una ventana de mantenimiento ya que este equipo soporta toda la administración de la red de MA PEÑALOSA CÍA S.A.S, así que debe ejecutarse en horas fuera de la jornada normal.

En cuanto a Actualizaciones de la consola del Antivirus, es necesario recurrir al uso de la consola para que primero se descargue en el servidor donde se administra la consola y luego se programe su distribución a los demás equipos de cómputo en un horario establecido que no afecte el rendimiento de la red, aunque esto no genera interrupción de las actividades se evidencia lentitud en los equipos, por lo que se recomienda hacerlo en horarios laborales no muy concurridos por clientes.

11.2.6 Procedimiento de Operaciones del Centro de Datos. Es necesario disponer de un sitio seguro y con condiciones adecuadas para establecer un Centro de Datos, en el cual se ubiquen y protejan los activos informáticos más críticos que soportan la infraestructura tecnológica para el funcionamiento del sistema de información y las comunicaciones de MA PEÑALOSA CÍA. S.A.S. Este centro de datos debe estar acondicionado para que la operatividad de la empresa no se interrumpa.

Objetivo. Establecer las normas para crear y mantener el centro de datos de la empresa que contenga los activos informáticos críticos de MA PEÑALOSA CÍA S.A.S.

Alcance. El procedimiento contempla las acciones a implementar para el buen funcionamiento del centro de datos de la empresa en la Sede principal.

Responsabilidades

Coordinadora de sistemas**.**

- Verificar el cumplimiento del procedimiento.

- Controlar el Centro de Datos de la empresa
- Supervisar el acceso al centro de datos.
- Asegurar que los activos ubicados en el centro de datos operen correctamente
- Hacer un chequeo semanalmente de las condiciones del centro de datos para corregir, mejorar y aplicar cambios necesarios.
- Programar y supervisar mantenimientos preventivos de los equipos.

Gerente**.**

- Brindar recursos financieros para mantener las condiciones óptimas del centro de datos de MA PEÑALOSA CÍA. S.A.S.

Descripción.El procedimiento describe medidas que se deben aplicar para el centro de datos que debe crear MA PEÑALOSA CÍA. S.A.S.

- Suministro eléctrico y Sistema de alimentación ininterrumpida

Dentro del centro de datos se resguardan los activos informáticos más importantes que soportan la infraestructura tecnológica del sistema de información y comunicaciones de MA PEÑALOSA CÍA. S.A.S, en caso de fallo del suministro eléctrico, el sistema de alimentación ininterrumpida (UPS) entra a jugar un papel importante para mantener la disponibilidad de los activos como servidores, equipos de redes y comunicaciones.

Las UPS deben cubrir todos los activos informáticos ubicados en el centro de datos previniendo el riesgo ante un corto o fluctuaciones de energía, no solo la caída de la conexión con los servidores generando pérdida de información y de trabajo sino viéndose afectado los componentes lógicos y físicos de los activos.

Se debe realizar una estimación de la duración del tiempo de descarga de las baterías de la UPS para proveer el tiempo con el que se dispone para guardar documentos abiertos y realizar un apago correcto de los equipos para protegerlos de daños, en caso donde el corte de energía eléctrica sobrepasa el tiempo de disponibilidad de la UPS.

- Sistema de Aire acondicionado

Mantener una temperatura adecuada es fundamental dentro del centro de datos, ya que las temperaturas generadas por los equipos y por las condiciones climáticas de la ciudad de Cúcuta resultan bastantes altas y pueden ocasionar problemas a los activos informáticos que se encuentren resguardados en el centro de datos.

Si se presentan fallas en el sistema de aire acondicionado, la coordinadora de sistemas deberá aplicar medidas para mejorar las condiciones de temperatura y controlar el nivel de temperatura, solicitar soporte urgente con el proveedor de mantenimiento de aires acondicionados y si es necesario considerar apagar los equipos mientras se da una solución inmediata.

- Canal de Internet, red MPLS y Central telefónica.

Al presentar caídas del servicio de internet, MPLS o telefonía, afecta las actividades de MA PEÑALOSA CÍA S.A.S, denegando las conexión con las demás sedes en especial con la bodega de la Zona industrial donde existe mayor flujo de despachos; reflejo de caída de ventas de clientes, los cuales intentan comunicarse a la línea fija para realizar pedidos y no consiguen respuesta; bloqueo de accesos a los portales de proveedores para realizar pedidos de mercancía; cese en el envío de cotizaciones y documentos a través de internet, las cuales están siendo solicitadas con urgencia por clientes; algunos datáfonos para pagos con tarjeta de créditos estarían inhabilitados y no se llevaría a cabo la venta. Por lo tanto, se deberán tomar medidas preventivas como otro canal de internet para contingencia y configuradas las IP públicas del servidor como plan opcional cuando la red MPLS no esté disponible; tener disponibles varias líneas celulares para solventar el problema de telefonía fija.

Los equipos propiedad de terceros correspondientes a los servicios subcontratados no deberán ser manipulados internamente, a menos que lo solicite el proveedor. En caso de fallos se deberá reporta a las líneas de atención para soporte, garantizando el cumplimiento de los niveles de atención contratados.

Se deberá supervisar y dar información necesaria a los proveedores de los servicios subcontratados con el fin de dar una rápida solución a alguna falla.

- Equipos de redes y comunicaciones

Los equipos propiedad de terceros correspondientes a los servicios subcontratados no deberán ser manipulados internamente, a menos que el proveedor lo exija para apoyar en caso de soporte remoto o indique las instrucciones telefónicamente.

Se deberá realizar copias de respaldos del Fortigate, con el objeto de respaldar las políticas creadas y las demás configuraciones ante una falla del dispositivo. En caso de avería de este activo debe disponerse de un plan de contingencia debido a que este equipo soporte toda la administración de la red LAN, WAN y WIFI.

11.2.7 Procedimiento de Seguridad de Redes. Los usuarios de MA PEÑALOSA CÍA. S.A.S., para acceder al sistema de información o archivos compartidos, utiliza varios servicios ofrecidos por la administración de la red. Por tal motivo, es necesario establecer medidas que aseguren la integridad, confidencialidad y disponibilidad de la información.

Objetivo. Definir lineamientos para controlar la seguridad de las redes y proteger la transmisión de la información al utilizar los servicios de red.

Alcance. El procedimiento establece medidas solo para MA PEÑALOSA CÍA. S.A.S. Sede Principal.

Responsabilidades

Coordinadora de sistemas.

- Supervisar el cumplimiento del procedimiento.
- Administrar las redes de MA PEÑALOSA CÍA. S.A.S.
- Brindar soporte a usuarios con respecto al acceso a redes de la empresa.
- Asegurar el cumplimiento de los servicios subcontratados de Internet, telefonía y Red MPLS.
- Monitorear las redes de comunicaciones.

Usuarios.

- Proteger las claves de acceso y sesiones a las redes que esté autorizado de MA PEÑALOSA CÍA. S.A.S.

Descripción

Administración de la red y de equipos de conectividad

- El tipo de encriptación aplicada para la contraseña de red WIFI debe ser de WPA2-PSK (AES).
- Los equipos de red y comunicaciones no deberán tener claves por defecto de fábrica, están deberán asignársele una clave segura.

- Solo la coordinadora de sistemas podrá tener acceso y a la administración de los equipos de red que sean propiedad de MA PEÑALOSA CÍA. S.A.S.

- Deberán contemplarse en los mantenimientos preventivos.

Administración de la red privada virtual

- La coordinadora de sistemas deberá crear un canal seguro, utilizando una red privada virtual (VPN) para accesos remotos al sistema de información de MA PEÑALOSA CÍA. S.A.S.

- Se debe establecer horarios y duración de la conexión remota a los servidores para uso del sistema de información.

- Solo tendrán acceso remoto, asesores comerciales del área de ferretería debido a que deben visitar y acceder al sistema desde los clientes. Para excepciones deberá ser autorizado con el Gerente para asignación de licencias y usuario, según disponibilidad de licenciamiento.

Administración de acceso inalámbrico (WIFI)

- La administración del WIFI es responsabilidad de la coordinadora de sistemas y solo el tendrá la clave de acceso para acceder a la red inalámbrica de MA PEÑALOSA CÍA S.A.S.

- Proveedores, clientes o visitantes a la empresa, tendrán acceso a la red WIFI, solo en casos donde el Gerente haya dado previa autorización y se conectarán a una red aislada para visitantes.

- La coordinadora de sistemas deberá cambiar la contraseña y el nombre de la red WIFI con frecuencia para evitar accesos no autorizados, el nombre de la red no deberá ser algo que identifique la empresa como tal, para pasar desapercibida, pero si se deberá usarse como tipo de seguridad WPA2-PSK (AES) para cifrar contraseñas.

- Dentro de la configuración del Fortigate, siendo este el dispositivo que libera las direcciones a las conexiones WIFI, deberá mantener reservadas las direcciones para los dispositivos inalámbricos autorizados identificados a través de sus direcciones MAC, nombre de usuario y dirección IP.

Seguridad del cableado de red de datos

- Todo equipo de cómputo incluyendo equipos portátiles de MA PEÑALOSA CÍA. S.A.S, tendrá asignado una dirección IP estática por red cableada, configurada desde el Fortigate, con el fin de acceder más ágilmente y tener mayor estabilidad de la conexión al sistema de Información SAP B1. Solo se habilitará la red inalámbrica a equipos autorizados y que la requieran para movilidad del equipo.

11.2.8 Procedimiento de Monitoreo de Redes. Los ataques a las redes son muy frecuentes y su transcendencia depende de los controles y mecanismos que se apliquen para monitorear y mantener la seguridad de ellas, pudiéndose detectar oportunamente la amenaza y tomar acciones para minimizar el impacto sobre los activos de información de MA PEÑALOSA CÍA. S.A.S.

Objetivo.Implementar lineamientos para el monitoreo de redes y servicios

Alcance. El procedimiento contempla el monitoreo de redes y servicios asociados a la Sede Principal de MA PEÑALOSA CÍA. S.A.S.

Responsabilidades

Coordinadora de sistemas.

- Asegurar el cumplimiento del procedimiento.

- Monitorear el tráfico de la red y servicios utilizando herramientas confiables que garanticen la optimización de la red.

- Configurar alertas sobre las aplicaciones de monitoreo para facilitar la administración de la red y los servicios.

Descripción

MA PEÑALOSA CÍA. S.A.S. cuenta con un dispositivo para proteger la red local y servicios como correo electrónico, control de navegación entre otros. Este dispositivo es un Fortigate, el cual administra toda la red, asigna direccionamiento DHCP, monitorea y bloquea tráfico de red entrante y saliente según las políticas de configuración establecidas.

Para acceder y monitorear la red desde el Fortigate es necesario tener datos del usuario administrador, conocimientos de redes y otros conocimientos necesarios para el manejo de la interfaz

Es indispensable realizar copias de respaldos del Fortigate, con el objeto de respaldar las políticas creadas y las demás configuraciones ante una falla del dispositivo. En caso de avería de este activo se requiere de un plan de contingencia debido a que este equipo soporte toda la administración de las redes disponibles en MA PEÑALOSA CÍA. S.A.S.

Se deberá analizar con frecuencia los puertos, protocolos y servicios habilitados e identificar si están siendo usados, de lo contrario deshabilitarlos para evitar explotación de vulnerabilidades.

Se debe configurar desde el Fortigate el análisis de los protocolos IMAP y PO, aplicando filtros que ayuden a detectar y bloquear correos maliciosos.

Para mayor control en la seguridad, se requiere analizar frecuentemente los logs de eventos proporcionados por Windows para el caso de los servidores o equipos y aplica también para los dispositivos como el Fortigate, con el fin de revisar la ocurrencia de eventos que puedan perjudicar los sistemas y activos de información.

12. CONCLUSIONES

.
De acuerdo al levantamiento de información realizado, donde dio lugar al conocimiento sobre la empresa, la percepción sobre temas de seguridad de las diferentes personas involucradas con el manejo de los activos informáticos, los resultados del análisis de riesgos a través de Magerit sobre los activos de la información de la empresa MA PEÑALOSA CÍA. S.A.S, se evidencia que es necesario implementar un Sistema de Gestión para la Seguridad de la Información que garantice las características fundamentales de esta como son la integridad, confidencialidad y disponibilidad de la información.

Las principales amenazas detectadas dependen de decisiones e inversiones de los directivos de MA PEÑALOSA CÍA. S.A.S, amenazas como deterioro en la infraestructura física, mal estado del cableado eléctrico que pueden ocasionar graves consecuencias para los activos informáticos.

Existen otras amenazas por falta de políticas, controles de seguridad y ausencia de capacitaciones sobre los riesgos informáticos, lo que conlleva a que los usuarios desconozcan la forma de actuar frente a una amenaza, ocasionando deterioro, daños y mal uso de los activos informáticos y por ende ocasionar la inoperatividad de la empresa.

Es importante resaltar que para que el Sistema de Gestión de la Seguridad de la Información tenga éxito, debe tener el respaldo y total apoyo de los directivos de MA PEÑALOSA CÍA. S.A.S, de nada sirve contar con un SGSI y toda la documentación que concierne si ellos no están comprometidos con darle importancia a la seguridad de la información y a todos los activos informáticos. Ya que finalmente ellos son los que aprueban y dirigen la empresa.

13. RECOMENDACIONES

Es indispensable el compromiso que debe asumir los directivos de MA PEÑALOSA CÍA S.A.S para proyectarlo a sus empleados. Reconociendo la necesidad, aprobando, respaldando y participando activamente en la implementación del Sistema de Gestión de Seguridad Informática.

Una de las falencias graves de MA PEÑALOSA CÍA. S.A.S, es su infraestructura física que pone en riesgo totalmente a todos los activos informáticos, principalmente la seguridad de sus empleados. Es recomendable realizar una estimación para la adecuación de las instalaciones y priorizarlo. Además, debe disponerse un espacio para la construcción de un cuarto de equipos con las normas necesarias de seguridad, para que los activos críticos que soportan la operación del negocio no queden expuestos a factores que puedan afectarlos.

Programar jornadas de sensibilización a los usuarios para aplicar buenas prácticas de las políticas de seguridad y crear hábitos de seguridad, como bloquear sesiones en periodos de inactividad laboral, cambiar periódicamente sus contraseñas.

Se recomienda contratar un auxiliar de sistemas que apoye a la coordinadora del sistema, en tareas básicas y procesos de soporte a usuarios, para equilibrar cargas laborales y la coordinadora se enfoque en actividades funcionales más críticas.

14. DIVULGACIÓN

El presente proyecto será dado a conocer a los estudiantes de la Universidad Nacional Abierta y a Distancia UNAD que estén interesados en investigar sobre Sistema de Gestión de la Seguridad informática a través de los repositorios disponibles en la biblioteca virtual de la Universidad.

Como estrategia para aplicar en MA PEÑALOSA CÍA. S.A.S, con autorización de los directivos de la empresa, se debe estructurar un modelo de implementación del SGSI en coordinación con el Líder de Calidad para definir responsables y tareas.

Las políticas y controles de seguridad de la información definidos en este documento deben analizarse e incorporarse una vez aprobados por Gerencia, dentro del sistema documental de la empresa. Además, programar jornadas de capacitación con el fin de socializarlas con los empleados. Recurrir a los recursos como carteleras informativas de MA PEÑALOSA CÍA. S.A.S., para que estén al alcance de los empleados e incluirse dentro de la inducción de personal.

De igual manera deberán hacer seguimiento y auditar los controles establecidos para medir la eficacia del SGSI y conocer nuevas amenazas para implementar controles no contemplados.

BIBLIOGRAFÍA

ALCALDÍA DE BOGOTA. Obtenido de Ley 1581 del 2012. {En Línea}. {Consulta realizada en octubre del 2017}. Disponible en (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981).

_____. Ley 1266 de 2008. {En Línea}. {Consulta realizada en octubre del 2017}. Disponible en (https://blogjus.wordpress.com/2009/01/13/ley-1266-de-2008-habeas-data/)

_____. Ley 1341 de 2009. {En Línea}. {Consulta realizada en noviembre del 2017}. Disponible en (http://www.mintic.gov.co/portal/604/w3-article-3707.html)

AGUIRRE CARDONA, Juan David y Aristizábal Betancourt, Catalina. Diseño del Sistema de Gestión de Seguridad de la Información para el Grupo Empresarial La Ofrenda (2013). {En Línea}. {Consulta realizada en diciembre del 2017}. Disponible en (http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf?sequence=1)

CAMELO, Leonardo. Seguridad de la Información en Colombia Marco Normativo (Normas y políticas) de un SGSI. 2010. {En Línea}. {Consulta realizada en octubre del 2017}. Disponible en: (http://seguridadinformacioncolombia.blogspot.com.co/2010/experiencia-personal-dificultades-en-la.html)

COLOMBIA. Congreso de la República. Ley 1266 de 2008. [En línea], [consultado el 2 de mayo de 2018]. Disponible en Internet: https://blogjus.wordpress.com/2009/01/13/ley-1266-de-2008-habeas-data/

CORTES ROSERO, José Hernán. Aplicación de un Sistema de Gestión de Seguridad de la Información (SGSI) en el Circuito Cerrado de Televisión (CCTV) Sistema Integrado de Emergencias y Seguridad (SIES) del Municipio de Yacuanquer. (2016). {En Línea}. {Consulta realizada en octubre del 2017}. Disponible en (http://Repository.unad.edu.co/handle/10596/6175)

ESPINOZA AGUINAGA, Hans Ryan. Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo (2013). {En Línea}. {Consulta realizada en noviembre del 2017}. Disponible en (http://tesis.pucp.edu.pe/repositorio/bitstream/123456789/4957/1/ESPINOZA_HANS_ANALISIS_SISTEMA_GESTION_SEGURIDAD_INFORMACION_ISO_IEC+27001_2005_COMERCIALIZACION_PRODUCTOS_CONSUMO_MASIVO.pdf)

GIRALDO CEPEDA, Luis Enrique. Análisis para la Implementación de un Sistema de Gestión de la Seguridad de la Información Según La Norma ISO 27001 En La Empresa SERVIDOC S.A (2016). {En Línea}. {Consulta realizada en noviembre del 2017}. Disponible en (http://Repository.unad.edu.co/handle/10596/6341)

GUZMÁN SILVA, Carlos Alberto. Diseño de un Sistema de Gestión de Seguridad de La Información para una Entidad Financiera de Segundo Piso (2015). {En Línea}. {Consulta realizada en noviembre del 2017}. Disponible en(http://repository.poligran.edu.co/bitstream/10823/746/1/Proyecto%20de%20Grado%20SGSI%20-%20IGM-%20CarlosGuzman%20(FINAL).pdf)

ICONTEC. Certificación del Sistema de Gestión de Seguridad de la Información con ISO/EIC 27001. (2013) {En Línea}. {Consulta realizada en noviembre del 2017}. Disponible en (HYPERLINK "http://icontec.org/")

PULIDO, Ana Milena y Marsella Mantilla, Jenith. Modelo para la Implementación del Sistema General de Seguridad Informática y Protocolos de Seguridad Informática en la Oficina TIC de la Alcaldía Municipal de Fusagasugá, basados en la Gestión del Riesgo Informático.(2016). {En Línea}. {Consulta realizada en diciembre del 2017}. Disponible en (http://Repository.unad.edu.co/handle/10596/6327)

SUAREZ PADILLA, Sandra Yomay (2015). Análisis y diseño de un Sistema de Gestión de Seguridad Informática en la empresa Aseguradora Suárez Padilla & Cía. Ltda, que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. {En Línea}. {Consulta realizada en noviembre del 2017}. Disponible en (http://repository.unad.edu.co/bitstream/19596/3777/1/20904541.pdf)

ZAQUE GONZÁLEZ, Oscar Javier. Proyección Financiera y Tecnológica requerida para la Implementación del Sistema de Gestión de la Seguridad de la Información (SGSI), Bajo La Norma ISO/IEC 27001:2013 En La Empresa INDAIRE Ingeniería S.A.S. (2016). {En Línea}. {Consulta realizada en diciembre del 2017}. Disponible en (http://repository.unad.edu.co/handle/10596/8595)