ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA PIJAOS TELECOMUNICACIONES DEL MUNICIPIO DE CAJAMARCA EN EL DEPARTAMENTO DEL TOLIMA.

JAVIER CÁRDENAS CRUZ

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
FACULTAD ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
PROGRAMA ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ D.C.,2019.

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA PIJAOS TELECOMUNICACIONES DEL MUNICIPIO DE CAJAMARCA EN EL DEPARTAMENTO DEL TOLIMA.

PROYECTO DE GRADO PARA OBTENER EL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

JAVIER CÁRDENAS CRUZ

ING. EDGAR ROBERTO DULCE

DIRECTOR DE PROYECTO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

FACULTAD ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

PROGRAMA ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ D.C.

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

Bogotá D.C., Junio 30 del 2019

AGRADECIMIENTO

A mi padre Luis Álvaro que dio amor, confianza, y seguridad y me apoyo en todas mis actividades educativas.

A mi madre Ana Elvira mi motor y pilar fundamental en mi vida, por su amor incondicional, confianza, y apoyo en mis buenas costumbres y educación.

A mi esposa Sandra Marcela y mi hijo Juan José por mi motor que me impulsa para salir adelante en todos mis proyectos de mi vida.

A mi familia que ha sido es y será mi apoyo incondicional para dar consejos y orientación en los trabajos y proyectos de mi vida.

Al Ing. Orlando Marín por permitir llevar a cabo este proyecto de grado en su empresa.

A todos tutores de la universidad UNAD por brindarme conocimientos en todo el periodo educativo de la especialización.

Al Ing. Edgar Roberto Dulce tutor de la universidad UNAD por todo su apoyos y orientación, para la culminación en buenos términos de este proyecto de grado.

CONTENIDO

Pág.

LISTA DE GRÁFICAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

ANEXO A: Encuesta de análisis de seguridad de la información en la empresa Pijaos Telecomunicaciones SAS.

ANEXO B. Evidencia divulgación a empleados.

ANEXO C. Formato política de administración de servidores.

ANEXO D. Consentimiento informado.

ANEXOE. Carta de AVAL de la empresa donde será aplicado el proyecto.

TÍTULO

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA PIJAOS TELECOMUNICACIONES DEL MUNICIPIO DE CAJAMARCA EN EL DEPARTAMENTO DEL TOLIMA.

RESUMEN

La empresa Pijaos Telecomunicaciones SAS, tiene su sede en el Municipio de Cajamarca Tolima, por el momento es la única empresa existente en la zona, que presta el servicio como proyecto WIFI rural y urbano, distribución de equipo tecnológicos, desarrollo de proyectos de telecomunicaciones, vigilancia y seguridad vía internet, y automatización de empresas, se puede afirmar que esta empresa es relativamente nueva y requiere la implementación del sistema de gestión de riesgos, específicamente el análisis y evaluación de riesgos de la información.

La empresa se sostiene gracias a los proyecto en marcha que tienen hoy día en la región, como el proyecto de la doble calzada, túnel de la línea, y la empresa AnglogGoldashanti exploradora de minerales, entre otras, han logrado un equilibrio sustancial en el mercado de la tecnología.

Por responsabilidad social de estas empresas, se ha logrado aumentar la calidad de vida de los pobladores de la región, en especial de los centros educativos donde los niños requieren este tipo de tecnología, la cual está a la vanguardia en todo el mundo.

La intención de la empresa Pijaos Telecomunicaciones S.A.S, es lograr un cubrimiento total en las escuelas más apartadas del Municipio, para así lograr que todos los niños tengan los mismos beneficios, no estén apartados de las nuevas innovaciones, tengan buena calidad y nivel educativo donde se encuentren.

Los habitantes de la región añoran que este tipo de emprendimiento permanezca en el tiempo y sigan siendo apoyados por empresas nacionales e internacionales, que laboran de forma mancomunada con el desarrollo integral de Cajamarca.

Según la nueva investigación de mercados de la región hecha por la alcaldía municipal de Cajamarca, la empresa Pijaos Telecomunicaciones SAS se ha visto afectada por los nuevos sistemas sociales de consultas populares en contra de la minería, la corrupción en los proyectos del estado que se desarrollan allí.

INTRODUCCIÓN

Hoy en día, en el análisis de riesgos de seguridad de la información se ha convertido en un pilar fundamental e importante en la empresa y su adecuada implementación, seguimiento y control ya no es realizada de forma empírica; en la actualidad existen normas y estándares internacionales que son las directrices, las cuales permiten y dan pautas correctas para mitigar el riesgo en las organizaciones.

La preocupación en torno al análisis de riesgos salta las alarmas en todas las organizaciones, sin tener en cuenta su tamaño y sector al que pertenece. Por consiguiente, en la actualidad, el análisis de riesgos por medio de las metodologías existentes, en este caso la metodología Magerit V.3 es pieza fundamental a tener en cuenta en la gestión de las empresas.

Desde el punto de vista económico, la adecuada trazabilidad en los análisis de riesgos en materia de seguridad, reduce gastos que podrían ser altos por posibles delitos a los activos de la información y datos en las empresas, los cuales pueden ser mitigados con antelación.

A nivel nacional e internacional los ataques por ciberdelincuencia se han convertido en una amenaza latente, en especial contra los datos e información de las empresas, este trabajo de especialización espera ser un referente a tener en cuenta en pequeñas y medianas empresas al momento de implementar normas de seguridad con estándares internacionales.

1. DEFINICIÓN DEL PROBLEMA

1.1. CONTEXTO

Según investigación, el mercado empresarial debe contar con empresas contratistas en la región para llevar a cabo programas de sostenibilidad social y ambiental, las cuales tienen una rigurosa política de seguridad de la información al interior; sin embargo, lo relevante es que las empresas contratistas en este caso puntual (Pijaos Telecomunicaciones SAS) deben dar un uso adecuado en la seguridad de la información ante la comunidad, y sus clientes como prestadora de servicios de internet a la zona rural de la región.

El servicio se ha visto afectado en ciertas veredas del Municipio de Cajamarca debido a posibles actos vandálicos al parecer por los mismos moradores, ya que están en desacuerdo en tener recursos de empresas extranjeras; es así que se evidenciado afectación a la infraestructura computacional y todo lo relacionado con esta (torres, fibra óptica, datos etc.).

Mediante el seguimiento a eventos en el Municipio de Cajamarca (Tolima), se obtuvo que de 42 veredas hay un promedio de 4 veredas que no están de acuerdo con la instalación del servicio de internet WIFI rural y programas de desarrollo de empresas privadas que tienen injerencia en la zona, todo lo anterior, debido a continua manipulación por grupos contradictores de la zona.

La problemática se incrementa cuando personas malintencionadas aprovechan los periodos más cercanos de votaciones para elección de alcalde, y gobernadores en el país, ya que se genera desinformación, adulteración de la señal y desprestigio a la imagen de la empresa Pijaos Telecomunicaciones,

Es de conocimiento general que el internet es fundamental para el desarrollo educativo de los estudiantes; es así, que se debería dar prioridad a la formación continua y permitir la instalación del servicio en todas las zonas alejadas del Municipio y evitar la filtración de datos e información de la empresa que más tarde sea empleada para su desprestigio.

Por lo anterior, se formula a continuación la pregunta problema.

¿Cómo el proceso de análisis y evaluación de riesgos ayudará a identificar las vulnerabilidades y amenazas que afectan la seguridad de la información para definir el plan de mejoras que permita mitigar los riesgos encontrados en la empresa Pijaos Telecomunicaciones S.A.S?

2. JUSTIFICACIÓN

Algo muy importante y como parte fundamental del sistema de gestión de seguridad de la información, es mandatorio llevar a cabo un análisis de riesgos exhaustivo en la empresa Pijaos Telecomunicaciones SAS para que le permita identificar sus principales vulnerabilidades de sus activos de información y sus amenazas que podrían explotar las vulnerabilidades. Después de tener identificados los riesgos al interior de la empresa, se deben tomar medidas y controles adecuados para minimizarlos, controlarlos y administrarlos.

Ante cualquier indicio de riesgo de seguridad de la información la empresa debe tomar los controles existentes en el mercado como son las medidas físicas preventivas como la carnetización a todos los empleados desde el nivel gerencial hasta el perfil más bajo existente allí, un sistema de circuito cerrado de televisión de alta definición, auditorías esporádicas del sistema de gestión de seguridad de la información, control de acceso, hombres en vigilancia las 24 horas, herramientas tipo software para aseguramiento de la información (Antivirus licenciado, DNS, VPN,), normas de aseguramiento de la información NAI, entre otros.

La optimización de recursos dentro de la empresa, en gran medida tiene un impacto directo e indirecto sobre la eficiencia y eficacia en lo que respecta a un excelente análisis y evaluación de los riesgos existentes, que deben ser mitigados a su mayor brevedad posible.

La empresa Pijaos Telecomunicaciones SAS debe acogerse a la implementación de las normas y estándares legales existentes sobre el aseguramiento de la información con el fin de realizar internamente la auditoria, el seguimiento y respectivo cumplimiento de las posibles desviaciones encontradas y previo alistamiento para la auditoría externa, de esta manera se logra en un alto porcentaje la mitigación de los riesgos y salvaguardar los pilares de la información tales como la integridad, disponibilidad, trazabilidad, confidencialidad y autenticidad; así mismo, el logro del éxito y continuidad del negocio empresarial.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Identificar y mitigar las vulnerabilidades y amenazas que afectan la seguridad de la información en la empresa Pijaos Telecomunicaciones.

3.2. OBJETIVOS ESPECIFICOS

Identificar los activos informáticos de la empresa Pijaos Telecomunicaciones que están expuestos a vulnerabilidades y amenazas de seguridad de la información

Realizar el proceso de análisis y evaluación de riesgos para determinar el impacto de los mismos en la empresa Pijaos Telecomunicaciones.

Elaborar el informe final de los resultados y establecer el plan de mejoramiento de seguridad para la empresa Pijaos Telecomunicaciones teniendo en cuenta los resultados anteriores.

4. ALCANCE Y DELIMITACIÓN DEL PROYECTO

4.1. ALCANCE

El análisis de riesgos se hace para establecer las vulnerabilidades a que se exponen los datos y la información, tanto en la parte interna del área administrativa y operativa, como en la parte externa de comunidades de la empresa Pijaos Telecomunicaciones del Municipio de Cajamarca Tolima, utilizando la metodología MAGERIT.

Este trabajo permite crear conciencia a directivos, y empleados de la compañía sobre la importancia de proteger los datos y la información de posibles ataques cibernéticos, fuga, fraude, y amenazas en general a través del internet, por medio físico, y divulgaciones no autorizadas.

Las personas responsables de sistemas de la empresa tendrán compromisos en materia de aseguramiento de la información ante los usuarios finales, adicional dar soporte como mesa de ayuda en la solución de posibles inconvenientes de aseguramiento de la información ante posibles fallos en las configuraciones de los equipos, filtración de información, funcionamiento adecuado de los antivirus, spam en los email de cuentas corporativas entre otros.

4.2. DELIMITACION

En cuanto a la delimitación, el trabajo se enfoca en el análisis de riesgos del manejo y uso de los datos y la información en la empresa Pijaos Telecomunicaciones, para evaluar el impacto y dar recomendaciones como oportunidades de mejora ante posibles eventos sensibles en los datos y la información.

El análisis de riesgos va en pro y en relación a posibles desinformaciones que puedan surgir entre los empleados y la comunidad donde se ubica la empresa Pijaos Telecomunicaciones.

El trabajo se llevara a cabo en todo el sistema informático existente en la empresa, para descartar fallas que después se conviertan en vulnerabilidades y/o amenazas.

5. MARCO DE REFERENCIA

5.1 Antecedentes

5.1.1 Nombre de la empresa

Pijaos Telecomunicaciones SAS

5.1.2 Contextualización institucional

La empresa Pijaos Telecomunicaciones SAS se encarga de suministrar el servicio de internet en la zona rural y urbana del Municipio de Cajamarca Tolima; su principal fuente de financiación proviene de las empresas AngloGoldAshanti Colombia, túnel de la línea, y la doble calzada, (éstas dos últimas pertenecen a la concesión Carlos Colín). Así, la empresa puede optimizar recursos y prestar un servicio de calidad en las telecomunicaciones a lugares apartados y beneficiando a niños de bajos recursos en su educación por intermedio del WIFI y automatización tecnológica en las zonas.

5.1.3 Reseña histórica

La empresa Pijaos Telecomunicaciones inicio sus labores en el año 2012 con la venta de sus productos de forma online y posteriormente se fue fortaleciendo en el mercado e instalando una oficina en el Municipio de Cajamarca Tolima. Gracias a la gestión del Ing. Carlos Orlando Marín actual Gerente comercial presento el proyecto de instalación de WIFI a la alcaldía del Municipio, y empresas de la zona para recibir apoyo en contratación de sus servicios y por consiguiente beneficiar a todas las veredas más apartadas del Municipio. En el año 2014 se dio apertura de la sede en la ciudad de Ibagué y ampliando el portafolio de servicios de telecomunicaciones. En año 2016 cuenta con una empresa más fortificada en el Municipio de Cajamarca e Ibagué, ya que cuenta con 40 veredas con cobertura de WIFI rural en escuelas, y gran automatización de ventas de productos tecnológicos.

Algunas veredas no han querido tomar el servicio WIFI en sus veredas por diferencias ideológicas con funcionarios de la alcaldía del Municipio.

Desde entonces, la empresa Pijaos Telecomunicaciones ha venido prestando un excelente servicio a toda la comunidad Cajamarquina, a un costo económico y al alcance de toda la población.

Es una empresa dedicada al desarrollo de proyectos auto-sostenibles en telecomunicaciones. Nace a partir de la unión entre profesionales cajamarquinos aproximadamente hace 5 años, teniendo como líderes a Carlos Orlando Marín Triana, actual gerente comercial y Fernando Javer Moreno Grijalba representante legal.

5.1.4 **Estrategia institucional**

La empresa Pijaos Telecomunicaciones SAS, cuenta con una estrategia institucional de incentivar en atención al cliente, con el fin de brindar seguridad, sentido de pertenencia, oportunidad, continuidad del negocio, eficiencia, eficacia, compromiso social, y ambiental hacia los clientes internos, externos, potenciales y a la comunidad en general. La estrategia de la empresa está orientada a la consolidación de sus procesos tanto administrativos como operativos.

Los procesos a saber son:

- Autorización para el manejo de datos e información tanto personal como empresarial para la debida comercialización de sus productos y servicios como son los planes de internet en post pago, consultas de equipos reportados, central de riesgos, etc.
- Proceso para la venta de post pago, es el manual del proceso de venta de post pago de los productos de Axion Play.
- Manual de Recarga por Cédula, aquí se tiene el manual para la recarga por cédula por parte de los clientes.
- Manual para la venta y gestión de pines, aquí se encuentra el paso a paso para la venta de pines prepago de Axion Play.

5.1.5 **Misión**

Proporcionar servicios de internet a través de redes tecnológicamente actualizadas y modernas, cumpliendo la normativa vigente e impulsando el crecimiento económico y productivo de nuestro municipio, brindando a los habitantes un servicio bajo premisas de calidad y tarifas equitativas. (Carlos Orlando Marín, s.f.)

5.1.6 **Visión**

Para el año 2025 nos comprometemos a sumar todos nuestros esfuerzos para mantener a PIJAOS TELECOMUNICACIONES como la empresa líder en servicios de internet en el municipio de Cajamarca y tener una participación relevante dentro del mercado departamental y nacional. (Carlos Orlando Marín, s.f.)

5.1.7 **Política de Calidad**

La empresa Pijaos Telecomunicaciones SAS tiene la responsabilidad social de generar empleo en la región, suministrar el internet WIFI a costo bajo, garantizar la conectividad hacia las zonas apartadas de la zona urbana, tener clientes y proveedores aliados para su financiación empresarial y posesionarse en el mercado de las comunicaciones como empresa pujante, pionera, y sólida.

La participación en programas educativos dentro del Municipio es alta debido a los convenidos con la alcaldía local, lo cual es un beneficio para los niños de escuelas de la zona rural del Municipio; todo se direcciona a la búsqueda del mejoramiento continuo en sus estándares, para el cumplimiento de su misión y visión.

Se evidencia un trabajo en equipo en la empresa Pijaos Telecomunicaciones que cuenta con un organigrama jerárquico y estructurado de tal forma que está dividida por cadena de mando que pasa por el nivel institucional y operativo.

En la gráfica representativa líneas abajo se visualiza la estructura organizacional de la empresa Pijaos Telecomunicaciones.

La empresa Pijaos Telecomunicaciones tiene procesos internos que se deben destacar como buenas prácticas, propósitos y que aportan en pro de minimizar los riesgos de la información y sus activos, los cuales son lo más valioso de una organización, entre las políticas y procesos se pueden destacar algunos como:

2. Ibid., p. 15

5.1.8 **Política de talento humano**

El área de talento humano de la empresa trabaja activamente por lograr una selección de personal acorde a los lineamientos de la gerencia y presidencia, implementación de estrategias, capacitaciones, control de índices de gestión en empleados, visión y objetivos organizacionales, competencias laborales, mantener los niveles de motivación, y el desarrollo y compromiso en general hacia los empleados y la empresa en general.

5.1.9 **Políticas de talento humano y actividades realizadas**

Desde el área de talento humano aportan y brindan a la empresa un compromiso de alto profesionalismo en el cumplimiento de las metas y objetivos trazados y planeados para el año, con el fin de dar cumplimiento al bienestar y calidad de vida a los empleados, capacitarlos en materia de seguridad y aportar un valor al control de los riesgos de seguridad de la información. Desde el área de talento humano se direcciona todas las actividades en pro del análisis de riesgos de seguridad de la información y son las siguientes:

5.1.10 **Actualización política de seguridad de la información**

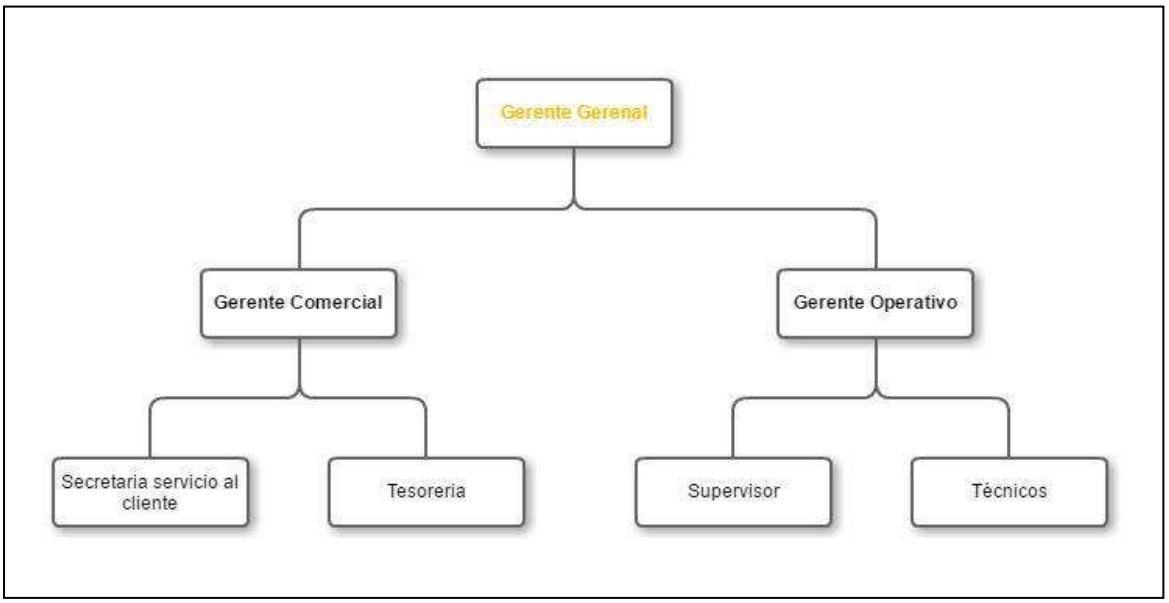
La seguridad de la información se define como un valor importante para el logro de las metas y objetivos que tiene cada área, ya que donde existe cierto grado de amenaza genera un riesgo, daño o peligro a cualquiera de los procesos internos, como algún tipo de afectación a la imagen corporativa en caso de materializarse dicha amenaza.

En materia de seguridad se debe tener en cuenta dos pilares como es la seguridad de la información y la protección de datos. En materia de seguridad de la información se debe proteger los datos en cuanto a su filtración, perdida o algún tipo de modificación a la misma, y en la protección de datos se debe blindar la disponibilidad, confidencialidad, e integridad de datos para su transparencia en todo sentido.

La empresa debe contar con seguridad en los activos más valiosos como son los datos y la información así:

- Hoy día los riesgos y las amenazas existentes hacen que los sistemas cada vez deban someterse a rigurosos procesos de alta seguridad para evitar ser blanco de actos ilícitos e incurrir en pérdidas económicas al interior de la empresa.
- Una falencia es la interconexión de los sistemas en la red de internet lo que los hace más vulnerable y expuestos a todo tipo de amenaza.
- Todos los sistemas tienen un grado de exposición al riesgo lo cual se debe mitigar por medio de procedimientos.

Grafica 1: Organigrama actual.



Fuente: Actual investigación.

Gráfica 2. Mapa de procesos.

Fuente: Código del buen gobierno de la empresa Pijaos Telecomunicaciones

Los mapas de procesos se identifican porque tienen una sucesión de procesos internos de todas las áreas de la empresa con un inicio y final, son muy explicativos y con un alto grado de aprendizaje.

En este mundo globalizado en materia de tecnología que ha traído muchas cambios para el buen desarrollo gracias a la buenas prácticas y metodologías aplicadas para gestionar la seguridad de la información, en especial para un análisis y evaluación de riesgos de alta calidad con la aplicabilidad de la metodología Magerit V.3.

A continuación se nombran algunas de estas metodologías y/o métodos que además son objeto de análisis y referencia para el presente trabajo en lo que concierne a la gestión de riesgos:

- UNE 71504:2008: La norma aplica a los diferentes sistemas de tratamiento de la información, en especial en servicios hacia los procesos que da continuidad del negocio como son; los sistemas legislativo y reglamentario, recursos humanos, informática, comunicaciones, instalaciones, u otros equipamientos auxiliares para un adecuado análisis de riesgos, salvaguardas, riesgos residuales y su gestión.
- MAGERIT “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, esta norma tiene 3 libros, los cuales son de estricta aplicabilidad para el análisis de riesgos y seguridad de la información con el único fin de minimizar los riesgos en las empresas y actualmente está en la versión 3.
- AS/NZS 4360:2004: Consiste en hacer parte de la gestión del riesgo en forma de guía con el objetivo de la norma es estrictamente dar una orientación para la toma de decisiones en las empresas.
- NIST (6) SP 800-30: Esta metodología permite salvaguardas a la información en las empresas con el fin de que sea integra, confidencial, y disponible. Esta norma especializada en la creación de políticas y procedimientos para establecer controles para la seguridad de los datos y la información asociada.
- NIST SP 800-39 “Managing Risk from Information Systems - An Organizational Perspective”: Administra el riesgo de seguridad de la información para todos los procesos en la empresa, en lo que hace referencia a sus funciones, misión, visión e imagen corporativa etc.
- ISO/IEC 27005:2008: Esta norma da directrices para llevar a cabo la gestión del riesgo de seguridad de la información. Esta norma es fácil de fusionar con la norma ISO 27001 y siempre basada en la gestión del riesgo.
- ISM3-RA: Esta norma se caracteriza por tener particularidades especiales como su facilidad, sencillez, rapidez y su economía, utiliza funciones de negocio, se modela según responsabilidades de gestión.

Algunas de ellas como CRAMM son antecedentes incluso para la norma BS7799-3 y por ende para la ISO/IEC 27.005 después.

Existen muchas normas similares a la ISO 27001 en el mercado para un adecuado tratamiento del aseguramiento de la información tanto en su planificación, dirección y Código del buen gobierno de la empresa Pijaos Telecomunicaciones.

Existen microempresas y pymes, las cuales son un referente metodológico ante análisis y automatización del sistema de gestión de seguridad de la información y encargadas de prestar servicios a otras empresas con debilidades o en carencia de buenas prácticas, metodologías y procesos de seguridad.

6. MARCO TEÓRICO

6.1 Análisis de riesgos informáticos

Ante todo se define lo que es un análisis y un riesgo[3] así:

Análisis: Se interpreta como la capacidad para discernir ante un posible evento que puede materializarse al no tomar acciones de seguridad.

Riesgo: Es la probabilidad de ocurrencia de que un evento se materialice por su alta exposición de ocurrencia.

El análisis de riesgos es un estudio detallado que se hace al interior de una empresa y para el caso puntual a la empresa Pijaos Telecomunicaciones SAS, donde se evalúa la información y los datos.

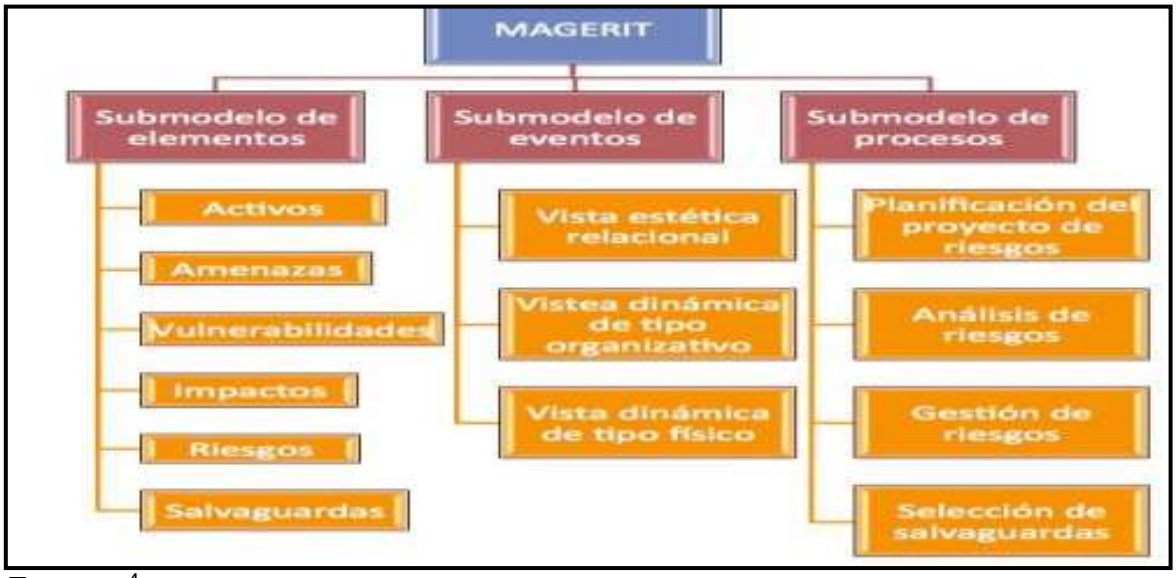
5.2.2 **Metodología Análisis y Evaluación de Riesgos Basado en Magerit V.3**

Esta metodología es aplicada exclusivamente para poder identificar la carencia de controles y como la implementación de planes de mejoramiento continuo al interior de la empresa.

La categoría que se aplicará en el presente proyecto será de forma cualitativa por medio de la estructura Magerit V3.

[3] AMUTIO GÓMEZ, Miguel Ángel; CANDAU, Javier y MAÑAS, José Antonio. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas. Madrid. Portal de Administración Electrónica (PAe). Octubre de 2012. 6,7, p.

Gráfica 3. Estructura MAGERIT.



Fuente. [4]

6.2 Auditoria informática

Las auditorías en materia de seguridad informática se basan en normas, procesos, protocolos, estándares nacionales e internacionales con el único fin de aportar una mejora continua en sus lineamientos internos y de orden empresarial, por medio de herramientas de control interno; otras formas se diluyen de las excelentes relaciones y prácticas con el gobierno local y central o la aplicabilidad de comportamientos transparentes de las empresas observada como un activo valioso, y futurista en el buen desempeño empresarial.

La auditoría de los sistemas de información[5] se lleva a cabo mediante formatos especiales para tal fin, con personal calificado de la entidad auditora y el cliente para dejar evidencias de todo el proceso de auditoría.

---

[4] BOLAÑOS, María Camila, y ROCHA GÁLVIS, Mónica. AUDITORÍAS SI. Madrid. Portal de Administración Electrónica (PAe). 25 Marzo de 2014. [En línea].http://asijav.weebly.com/auditoria-de-sistemas-de-informacioacuten/magerit-v3-metodologa-de-anlisis-y-gestin-de-riesgos-de-los-sistemas-de-informacin

[5] BORGES Ezequiel Llarena. 13 Mayo de 2014. Normas generales para la auditoría de SI. AGSLISACA. {En línea}:http://www.asidom.es/documentos/NormasGeneralesAuditoriaSistemasInformacionISACA.pdf

6.3 Composición del estándar Magerit V.3

Su finalidad radica en el análisis y gestión de los riesgos para la protección de la seguridad de la información en las empresas; Magerit V.3 es “Proceso de Gestión de los Riesgos” (“Implementación de la Gestión de los Riesgos”).

Gráfica 4. Marco de trabajo para la gestión de riesgos.

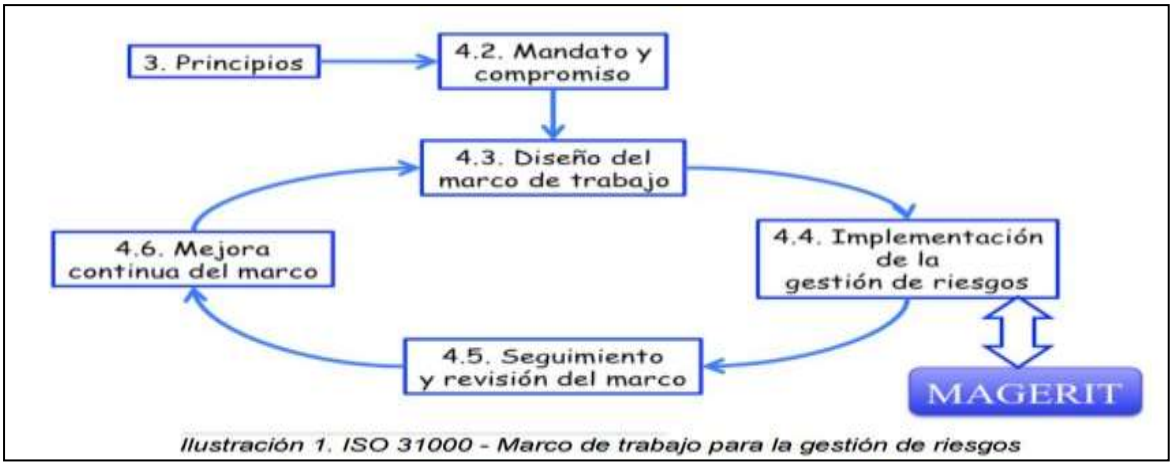


Ilustración 1. ISO 31000 - Marco de trabajo para la gestión de riesgos

Fuente. AMUTIO GÓMEZ, Miguel Ángel. Magerit V.3 Metodología de análisis y gestión de riesgo de los sistemas de información: Libro I Método. 1. Introducción. Madrid: Ministerio de hacienda y administraciones públicas, 2012. Página 7 (127).

Con Magerit se debe alcanzar los siguientes objetivos:

Directos:

- Concientizar a los responsables de los sistemas de información de la existencia de riesgos y la necesidad de minimizarlos a tiempo.
- Ofrecer un método sistemático para realizar el análisis de los riesgos.
- Ayudar a descubrir y planear las medidas oportunas para mantener los riesgos bajo control.

Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Amenazas de seguridad y clasificación

La amenaza: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

7. MARCO CONCEPTUAL Y NORMATIVO

Glosario de términos

- **Activo de información:** Aquello que tiene un costo alto y de vital importancia para la empresa, la información debe ser protegida[6].
- **Análisis de riesgos:** Uso sistemático de la información, para identificar peligros y estimar riesgos[6].
- **Impacto:** Consecuencia de que la amenaza ocurra[6].
- **Ciclo de Deming:** Modelo de mejora permanente en los procesos y sistemas.
- **Causa:** Circunstancia por la cual el riesgo se hace presente[6].
- **Riesgo:** Grado de exposición de un activo que abre las puertas a la materialización de la amenaza[6].
- **Riesgo inherente:** Grado de incertidumbre que hace parte de una actividad, sin gestión en el control[6].
- **Seguridad de la información:** Protección de la confidencialidad, integridad, disponibilidad, y la trazabilidad de la información (ISO 27000-2014).
- **Vulnerabilidad:** Exposición de un activo al riesgo, la cual puede ser aprovechada por una amenaza, aprovechando la falta de controles en la seguridad de la información.
- **PSE:** Proveedor de servicios electrónicos, la cual brinda a los usuarios realizar sus pagos vía internet.
- **Anexo SL:** Es el esquema de la organización internacional de estandarización ISO para los diferentes sistemas de gestión[6].
- **Confidencialidad:** Los componentes del sistema serán accesibles sólo por aquellos usuarios autorizados[6].
- **Integridad:** Los componentes del sistema sólo pueden ser creados y modificados por los usuarios autorizados.
- **Disponibilidad:** Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen. (Aplicar la resiliencia[6)].

  A estas dimensiones canónicas de la seguridad se pueden añadir otras derivadas que acerquen a la percepción de los usuarios de los sistemas de información:

- **Autenticidad:** Propiedad o característica en que una entidad es quien dice ser o bien quién garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información se tiene manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios, se tiene suplantación de identidad[6].
- **Trazabilidad:** Aseguramiento de que en todo momento se podrá determinar quién, qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia[6].
- **Amenazas:** Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización[6].

Impacto potencial: Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema[6].

Impacto acumulado: Es la sumatoria de un activo teniendo en cuenta su valor acumulado de activos y las amenazas a que está expuesto[6].

Impacto repercutido: Es el calculado[6] sobre un activo teniendo en cuenta su valor propio, y las amenazas a que están expuestos los activos de los que depende[6].

[6] AMUTIO GÓMEZ, Miguel Angel; CANDAU, Javier y MAÑAS, José Antonio. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas. Madrid. Portal de Administración Electrónica (PAe). Octubre de 2012. 6,7, p.

8. MARCO LEGAL

Para suplir esta necesidad la empresa Pijaos Telecomunicaciones S.A.S debe tomar como soporte los estándares de las normas:

Ley 1273 de 2009: Mediante este decreto que se refiere a los atentados contra la confidencialidad, integridad, disponibilidad, autenticidad, y trazabilidad de datos y sistemas informáticos.

Por medio de la cual se modifica el Código Penal, se da un nuevo bien jurídico tutelado, llamado “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.

Capítulo I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Artículo 269A: Acceso abusivo a un sistema informático. No se puede acceder a sistemas informático sin previa autorización, mucho menos violentar la seguridad o protección del sistema o la voluntad del que tiene el derecho legítimo, tendrá una multa de 48 a 96 meses de prisión o 100-1000 SMLV. (Cossio, 2019)

Articulo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. La persona que neutralice e impida el acceso a sistemas informáticos, datos de información, o redes de telecomunicaciones, tendrá una multa de 48 a 96 meses de prisión o 100-1000 SMLV. (Cossio, 2019)

Artículo 269C: Interceptación de datos informáticos. Persona que intercepte datos de información incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses. (Cossio, 2019)

Artículo 269E: Uso de software malicioso. La persona que comercialice, transporte, distribuya u otros software de procedencia y con fines dañinos, tendrá una multa de 48 a 96 meses de prisión o 100-1000 SMLV. (Cossio, 2019)

CAPÍTULO II De los atentados informáticos y otras infracciones.

Artículo 269J: Transferencia no consentida de activos. Persona que transfiera activos con perjuicio a otras personas, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 SMLV. (Cossio, 2019).

9. DISEÑO METODOLÓGICO

9.2. METODOLOGÍA DE INVESTIGACIÓN

9.2.1. Investigación aplicada

El objetivo principal es la gestión de problemas específicos para mejorar la calidad de vida de las comunidades y/o sociedades, este tipo de investigación está orientada a la investigación pura, en el caso particular del análisis de riesgos informáticos en la empresa Pijaos Telecomunicaciones del Municipio de Cajamarca Tolima, este tipo de investigación permite la búsqueda de una posible solución a los problemas conocidos o que aún se desconocen de acuerdo a los riesgos informáticos que se pueden presentar o que se están presentando en la empresa, tratando de dar una solución práctica a una problemática definida a través de respuestas a las necesidades que la investigación sugiere y que puede valerse de algún proceso sistemático para el desarrollo como tal del trabajo.

La investigación aplicada esta soportada en aportes teóricos y el desarrollo de actividades tendientes a determinar las posibles causas del problema y evidenciar los hallazgos, que más adelante y gracias a los resultados de la investigación, proporcionaran un marco de trabajo en búsqueda de la aplicabilidad de las posibles soluciones.

A continuación se darán actividades, con el único fin de contrarrestar el problema del proyecto en mención y dar a conocer a la empresa Pijaos Telecomunicaciones S.A.S, al final se tendrán las opciones para diseñar un plan de oportunidades de mejora, según las consecuencias del análisis de riesgos así:

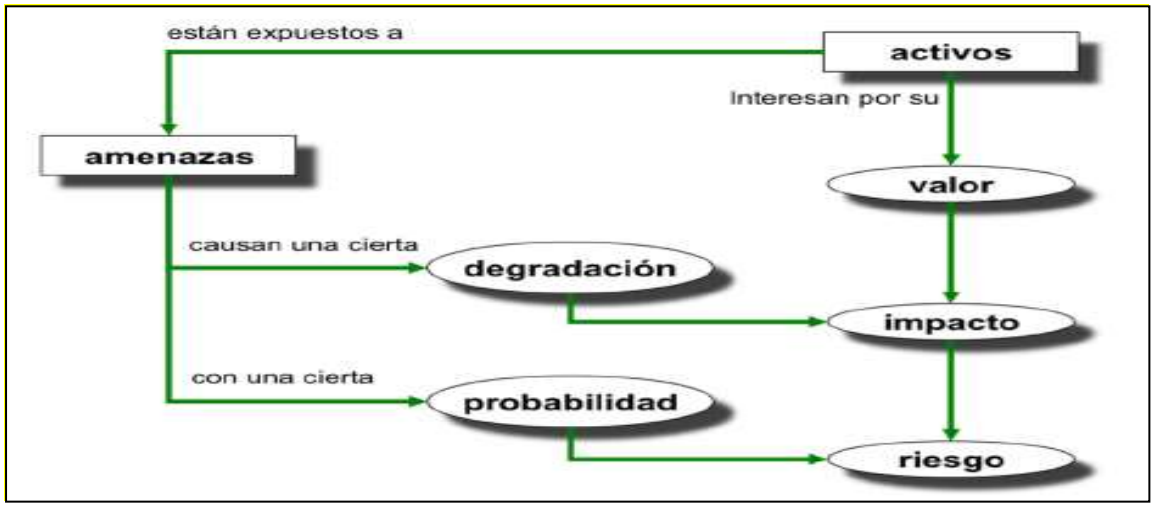
- Concluir los objetivos y delimitar el alcance del problema planteado.
- Recolección de datos e información; Intención de sustraer la mayor cantidad de información posible que tenga la empresa de su estado actual, proyectos en proceso etc., como aporte al análisis de riesgos a desarrollar.
- Elaboración y ejecución del cronograma de actividades de todo el proyecto como análisis de riesgos.
- Recopilación de todo el archivo documental de la empresa; como es procesos, organigrama, normas certificables, antecedentes de análisis de riesgos, conocimiento específico de la actividad económica etc.
- Apreciación estratégica del entorno y lugar de trabajo; Es necesario llevar a cabo una pre evaluación física de instalaciones, activos, controles de acceso, rutas de acceso, sector de vivienda de empleados, para realizar el respectivo análisis de riesgos exhaustivo.

- ➢ Ejecución del análisis de riesgos; Se establecen las falencias a que la empresa está expuesta o es vulnerable y el riesgo final puede ser materializado.
- ➢ Identificación y análisis de vulnerabilidades
- ➢ Análisis de datos y recomendaciones pertinentes
- ➢ Discusión de resultados
- ➢ Obtención de conclusiones

9.3. ANÁLISIS Y EVALUACIÓN DE RIESGOS BASADO EN MAGERIT V3

Por medio del análisis de riesgos la empresa determina la magnitud de los riesgos a que está expuesta y a las consecuencias de no mitigar estos riesgos a la mayor brevedad posible. Se pone en relevancia los elementos en la gráfica No. 5.

Gráfica No. 5 Elementos del análisis de riesgos potenciales.



Fuente. AMUTIO GÓMEZ, Miguel Ángel. Magerit V.3 Metodología de análisis y gestión de riesgo de los sistemas de información: Libro I Método. 3. Método de análisis de riesgos. Madrid: Ministerio de hacienda y administraciones públicas, 2012. Página 32 (127).

Los subprocesos involucrados son:

- ➢ Identificar los activos más sensibles, su asociación, y su valoración.
- ➢ Identificar las amenazas más relevantes dentro de los activos, y valorarlos según su frecuencia de ocurrencia, y degradación en los activos.

- ➢ Determinar las salvaguardas existentes y valorar su utilidad en la implementación.
- ➢ Realizar una estimación del impacto y el riesgo a que están expuestos los activos de la empresa.
- ➢ Dar lectura o análisis del impacto y el riesgo.

Soportados en la metodología Magerit V.3 se desarrollan las fases para el logro del proyecto “Análisis de riesgos de seguridad de la información para la empresa Pijaos Telecomunicaciones del Municipio de Cajamarca en el departamento del Tolima”. El análisis y evaluación de riesgos se hará usando la metodología, la cual contempla las siguientes dimensiones: Confiabilidad, integridad, autenticidad, trazabilidad y disponibilidad.

9.3.1. Proceso P1: Planificación

La etapa en mención es fundamental para una adecuada ejecución del proyecto, y es aquí, donde se planea todo el plan de trabajo para el análisis de riesgos.

9.3.1.1 Actividad A1.1: Estudio de oportunidad

Esta actividad tiene como objeto especial, llevar a cabo un análisis del estado actual de la seguridad de la información de los activos y sistemas tecnológicos de la empresa Pijaos Telecomunicaciones SAS, adicionalmente sirve para crear e incentivar a directivos de la alta gerencia en la implementación del sistema de gestión de seguridad de la información al interior de la empresa.

9.3.1.2 Actividad A1.2: Definición del alcance y objetivos del proyecto

Una vez obtenida la autorización para llevar a cabo el análisis de riesgos a la empresa Pijaos Telecomunicaciones SAS por la alta gerencia, se determina el alcance y los objetivos para su ejecución final y de forma exitosa. En el post análisis de riesgos lo ideal es materializar la implementación del sistema de gestión de seguridad de la información.

9.3.1.3 Actividad A1.3: Planificación del proyecto

Se requiere contar con un cronograma de actividades o plan de trabajo para llevar a buenos términos en tiempo, lugar y espacio el desarrollo del proyecto.

9.3.1.4 Actividad A1.4: Lanzamiento del proyecto

Una vez se tiene el visto bueno por parte del gerente comercial y operativo de la empresa Pijaos Telecomunicaciones S.A.S, se inicia el proceso de análisis de

riesgos y se pone en marcha la técnica de visualización directa y entrevista para la recolección de información, las cuales son las que mejor se adaptan porque los empleados son los directos ejecutores de los sistemas de cómputo, manejo de la información y de los datos actuales de la empresa.

Gráfica No. 6. Proceso de gestión de riesgos.

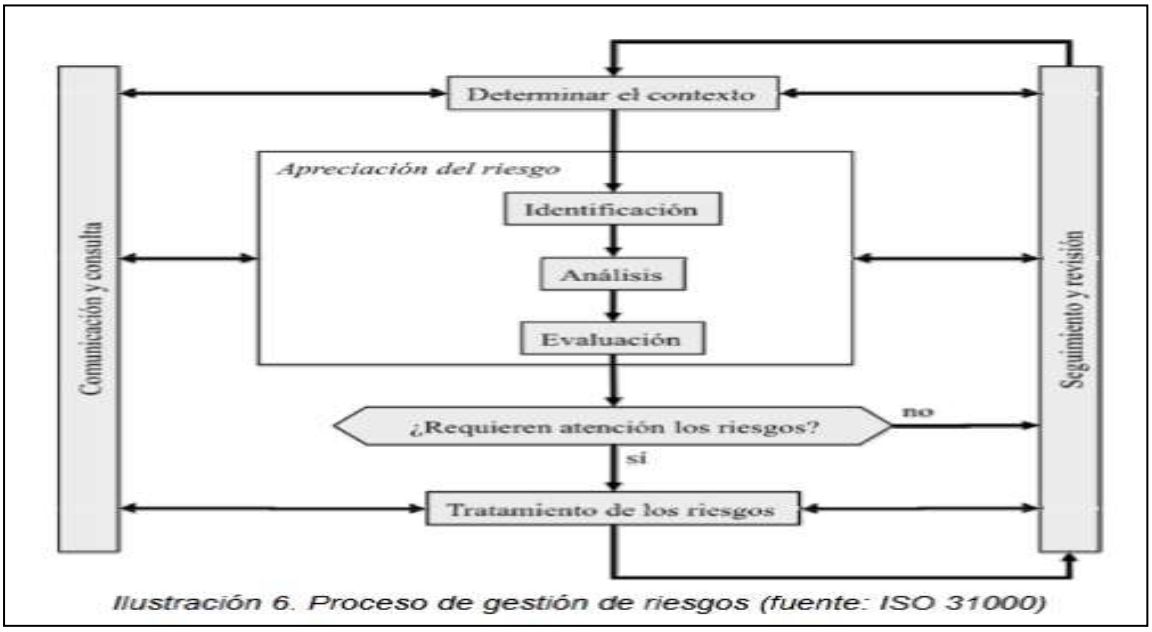


Ilustración 6. Proceso de gestión de riesgos (fuente: ISO 31000)

Fuente: AMUTIO GÓMEZ, Miguel Ángel. Magerit V.3 Metodología de análisis y gestión de riesgo de los sistemas de información: Libro I Método. Proceso de gestión de riesgos. Madrid: Ministerio de hacienda y administraciones públicas, 2012. Página 20 (127).

9.3.2. Proceso P2: Análisis de riesgos (flujo descriptivo de pasos)

El análisis de riesgos que se tiene en marcha para la empresa Pijaos Telecomunicaciones S.A.S obedece a la gran exposición ante amenazas que afrontan las empresas cada día por la ciberdelincuencia, para lo cual debe darse la importancia necesaria para evitar un impacto fuerte a los activos informáticos.

9.3.3. Actividad A2.1: Caracterización y Valoración de los Activos

Se aplican las siguientes tareas (T2)

Tarea 2.1.1: Identificación de los Activos

Los activos en mención líneas abajo, son puntualizados y seleccionados según la metodología Magerit V3 en su libro II (Anexo A, catálogo de elementos).

Tabla 1: Activos de información.

TIPO	NOMBRE DE ACTIVO
[Media] Soportes de información	1.[WIFI] red inalámbrica 2.[Internet] Internet
[AUX] Equipamiento auxiliar	3.[power] fuentes de alimentación 4.[cabling] cableado ;4.1.[fiber] fibra óptica, 4.2.[wire] cable eléctrico 5.[gen] generadores eléctricos
[L] Instalaciones	6.[backup] instalaciones de respaldo
[S] Servicios	7.[ipm] gestión de privilegios 8.[telnet] acceso remoto a cuenta local 9.[idm] gestión de identidades (2)
[P] Personal	10.[ue] usuarios externos 11.[op] operadores 12.[prov] proveedores 13.[com]administradores de comunicaciones
[D] Datos / Información	14.[acl] datos de control de acceso 15.[conf] datos de configuración (1) 16.[password]credenciales (ej. contraseñas)
[HW] Equipos informáticos (hardware)	17. [Network] soporte de la red (8); 17.1. [firewall] cortafuegos: 17.2. [modem] módems. 18.[host] grandes equipos (1) 19.[vhost] equipo virtual
[SW] Aplicaciones (software)	20.[prp] desarrollo propio (in house) 21.[av] antivirus 22.[backup] sistema de backup 23.[os] sistema operativo 24.[ts] servidor de terminales

Fuente: Esta investigación.

Tarea 2.1.2: Dependencias entre Activos

- ➢ Dependencia de los activos de tipo Soporte de información:
  - Personas relacionadas: operadores, administradores
  - Instalaciones que lo acogen
- ➢ Dependencia de los activos de tipo Equipamiento auxiliar:
  - Personas relacionadas: operadores, administradores
- ➢ Dependencia de los activos de tipo Instalaciones:
  - Guardias, encargados de mantenimiento

- ➢ Dependencia de los activos de tipo Servicios:
    - Personas relacionadas: operadores, administradores
- ➢ Dependencia de los activos de tipo Personal:
    - Los datos según acceso autorizado
    - Los servicios que gestionan
- ➢ Dependencia de los activos de tipo Datos / Información:
    - Equipos que los hospedan
    - Líneas de comunicación por las que se transfieren
    - Soportes de información
    - Personas relacionadas: usuarios.
- ➢ Dependencia de los activos de tipo Equipos informáticos
    - Personas relacionadas con este equipo: operadores, administradores
    - Instalaciones que lo acogen
- ➢ Dependencia de los activos de tipo Aplicaciones (software)
    - Personas relacionadas con esta aplicación: operadores, administradores y desarrolladores.

Tarea 2.1.3: Valoración de los Activos

Para hacer efectiva la valoración de los activos según metodología Magerit V3; se usan las dimensiones[9] a saber:

- ➢ [D] Disponibilidad
- ➢ [I] Integridad de los datos
- ➢ [C] Confidencialidad de la información
- ➢ [A] Autenticidad
- ➢ [T] Trazabilidad

9MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. Dimensiones de valoración. Madrid. Portal de Administración Electrónica (PAe). Octubre 2012. 15, 16 p.

Las dimensiones se usan para establecer un sistema métrico en resultados de materialización de una amenaza, y poder establecer el daño en determinada dimensión para la empresa.

Tabla 2: Escala de valoración de activos.

Valor		Criterio	
10	Extremo	E	Daño extremadamente grave
9	Muy alto	MA	Daño muy grave
6-8	Alto	A	Daño grave
3-5	Medio	M	Daño importante
1-2	Bajo	B	Daño menor
0	Despreciable	D	Irrelevante a efectos prácticos

Fuente: Magerit V3-Libro-Catálogo de Elementos.

La metodología Magerit V3. En su libro II-Catalogo de elementos proporciona herramientas para hacer la valoración de cada uno de los activos utilizando la escala estándar (ver Anexo B valoración de activos-Escala estándar).

Tarea 2.1.4: Valoración de activos tipo: Soporte de información.

Tabla 3: Valoración de activos tipo: Soporte de información.

Activo	Dimensiones de seguridad				
	(D)	**(I)**	**(C)**	**(A)**	**(T)**
[wifi] red inalámbrica	**(MA)**	**(MA)**	**(A)**	**(A)**	
[Internet] Internet	**(MA)**	**(A)**	**(A)**	**(A)**	

Fuente: Esta investigación.

(1) [7.cei.a] de alto interés para la competencia
[9.cei.c] causa de pérdidas económicas excepcionalmente elevadas
[7.da]Probablemente cause una interrupción seria de las actividades propias de la organización con un impacto significativo en otras organizaciones.
[3.po] causa de protestas puntuales

La información fue aportada y con ayuda del área de TI de la empresa Pijaos Telecomunicaciones S.A.S (auxiliar, técnico helpdesk, y coordinador de TI).

Tarea 2.1.5: Valoración de activos tipo: Equipamiento auxiliar.

Tabla 4: Valoración de activos tipo: Equipamiento auxiliar.

Activo	Dimensiones de seguridad				
	(D)	**(I)**	**(C)**	**(A)**	**(T)**
[power] fuentes de alimentación	**(MA)**	**(A)**			**(M)**
[cabling] cableado ;4.1.[fiber]fibra óptica, 4.2.[wire]cable eléctrico	**(A)**	**(M)**			**(M)**
[gen] generadores eléctricos.	**(MA)**	**(A)**			

Fuente: Esta investigación.

(2) [9.po] alteración sería del orden público
[4.rto] 4 horas < RTO < 1 día
[6.lbl] Difusión limitada
[9.adm] probablemente impediría seriamente la operación efectiva de la organización, alcanzando a su cierre definitivo.
[7.cei.d] proporciona ganancias o ventajas desmedidas a individuos u organizaciones.

La información fue aportada y con ayuda del área de TI de la empresa Pijaos Telecomunicaciones S.A.S (auxiliar, técnico helpdesk y coordinador de TI).

Tarea 2.1.6: Valoración de activos tipo: Instalaciones.

Tabla 5: Valoración de activos tipo: Instalaciones.

Activo	Dimensiones de seguridad				
	(D)	**(I)**	**(C)**	**(A)**	**(T)**
[backup] instalaciones de respaldo	**(MA)**	**(A)**	**(MA)**		
[GAB] Gabinete de red	**(B)**	**(D)**	**(MA)**		

Fuente: Esta investigación.

(3) [1.si] pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

[1.lro] pudiera causar el incumplimiento leve o técnico de una ley o regulación

[6.pi2] probablemente quebrante seriamente la ley o algún reglamento de protección de información personal

[9.si] probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios

La información fue aportada y con ayuda del área de TI de la empresa Pijaos Telecomunicaciones S.A.S (auxiliar, técnico helpdesk, y coordinador de TI).

Tarea 2.1.7: Valoración de activos tipo: Servicios.

Tabla 6: Valoración de activos tipo: Servicios.

Activo	**Dimensiones de seguridad**				
	(D)	**(I)**	**(C)**	**(A)**	**(T)**
[ipm] gestión de privilegios	**(A)**	**(A)**	**(MA)**	**(A)**	**(B)**
[telnet] acceso remoto a cuenta local	**(MA)**	**(MA)**	**(A)**		
[idm] gestión de identidades (2)	**(MA)**	**(A)**	**(A)**		

Fuente: Esta investigación.

(4) [1.lro] pudiera causar el incumplimiento leve o técnico de una ley o regulación

[1.si] pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

[7.cei.c] causa de graves pérdidas económicas

[5.da] Probablemente cause la interrupción de actividades propias de la organización con impacto en otras organizaciones.

[9.po] alteración sería del orden público

[5.adm] probablemente impediría la operación efectiva de más de una parte de la Organización.

La información fue aportada y con ayuda del área de TI de la empresa Pijaos Telecomunicaciones S.A.S (auxiliar, técnico helpdesk, y coordinador de TI).

Tarea 2.1.8: Valoración de activos tipo: Personal.

Tabla 7: Valoración de activos tipo: Personal.

Activo	Dimensiones de seguridad				
	(D)	**(I)**	**(C)**	**(A)**	**(T)**
[ue] usuarios externos	**(B)**	**(A)**	**(A)**		
[op] operadores	**(MA)**	**(MA)**	**(MA)**		
[prov] proveedores	**(A)**	**(B)**	**(A)**		
[com] administradores de comunicaciones	**(MA)**	**(A)**	**(MA)**		

Fuente: Esta investigación.

(5) [2.pi2] pudiera quebrantar de forma leve leyes o regulaciones
[1.si] pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[6.pi1] probablemente afecte gravemente a un grupo de individuos
[3.po] causa de protestas puntuales
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística

La información fue aportada y con ayuda del área de TI de la empresa Pijaos Telecomunicaciones S.A.S (auxiliar, técnico helpdesk, y coordinador de TI).

Tarea 2.1.9: Valoración de activos tipo: Datos / Información.

Tabla 8: Valoración de activos tipo: Datos / Información.

Activo	Dimensiones de seguridad				
	(D)	**(I)**	**(C)**	**(A)**	**(T)**
[acl] datos de control de acceso	**(MA)**	**(MA)**	**(MA)**	**(A)**	**(A)**
[conf] datos de configuración (1)	**(MA)**	**(MA)**	**(MA)**		

[password] credenciales (ej. contraseñas)	**(MA)**	**(MA)**	**(MA)**		

Fuente: Esta investigación.

(6) [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la organización
[4.crm] Dificulte la investigación o facilite la comisión de delitos
[8.lbl] Confidencial
[4.rto] 4 horas < RTO < 1 día
[1.da] Pudiera causar la interrupción de actividades propias de la Organización

La información fue aportada y con ayuda del área de TI de la empresa Pijaos Telecomunicaciones S.A.S (auxiliar, técnico helpdesk, y coordinador de TI).

Tarea 2.1.10: Valoración de activos tipo: Equipos informáticos (hardware).

Tabla 9: Valoración de activos tipo: Equipos informáticos.

Activo	**Dimensiones de seguridad**				
	(D)	**(I)**	**(C)**	**(A)**	**(T)**
[Network] soporte de la red (8);	**(A)**	**(MA)**	**(MA)**		**(A)**
[firewall] cortafuegos	**(A)**	**(MA)**	**(MA)**	**(MA)**	**(A)**
[modem] módems	**(MA)**	**(A)**	**(MA)**		
[host] grandes equipos (1)	**(M)**	**(M)**	**(M)**		
[vhost] equipo virtual	**(M)**	**(M)**	**(A)**		

Fuente: Esta investigación.

(7) [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la organización
[6.pi2] probablemente quebrante seriamente la ley o algún reglamento de Protección de información personal.
[7.lro] probablemente cause un incumplimiento grave de una ley o regulación

[1.si] pudiera causar una merma en la seguridad o dificultar la investigación de incidente
[7.cei.c] causa de graves pérdidas económicas
[1.da] Pudiera causar la interrupción de actividades propias de la Organización
[10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

La información fue aportada y con ayuda del área de TI de la empresa Pijaos Telecomunicaciones S.A.S (auxiliar, técnico helpdesk, y coordinador de TI).

Tarea 2.1.11: Valoración de activos tipo: Aplicaciones (Software).

Tabla 10: Valoración de activos tipo: Aplicaciones (software).

Activo	**Dimensiones de seguridad**				
	(D)	**(I)**	**(C)**	**(A)**	**(T)**
[av] anti virus	**(MA)**	**(MA)**	**(MA)**	**(A)**	
[backup] sistema de backup	**(A)**	**(MA)**	**(MA)**		
[os] sistema operativo	**(A)**	**(A)**	**(MA)**	**(A)**	
[ts] servidor de terminales	**(B)**	**(A)**			**(A)**

Fuente: Actual investigación.

(8) [6.pi1] probablemente afecte gravemente a un grupo de individuos
[4.pi2] probablemente quebrante leyes o regulaciones
[1.lro] pudiera causar el incumplimiento leve o técnico de una ley o regulación
[3.si] probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente.
[7.cei.a] de alto interés para la competencia

La información fue aportada y con ayuda del área de TI de la empresa Pijaos Telecomunicaciones S.A.S (auxiliar, técnico helpdesk, y coordinador de TI).

9.3.4 Actividad A2.2: Caracterización y Valoración De Las Amenazas.

La actividad tiene las siguientes tareas (T):

La finalidad de la actividad en mención consiste en establecer la degradación del activo; consiste en medir el valor que pierde el activo (%) en dado caso que sea materializada la amenaza.

Las amenazas se han tomado del catálogo de elementos, según metodología Magerit V3-Libro II.

Tarea 2.2.1 Frecuencia de amenazas

Tabla 11: Valor frecuencia de amenazas

4	Muy frecuente	MF	A diario
3	Frecuente	F	Mensual
2	Normal	FN	Una vez al año
1	Poco frecuente	PF	Cada varios años

Fuente: AMUTIO GÓMEZ, Miguel Ángel. Magerit V.3 Metodología de análisis y gestión de riesgo de los sistemas de información: Libro I Método. 3. Criterios de valoración. Madrid: Ministerio de hacienda y administraciones públicas, 2012. Página 19 (127).

Tarea 2.2.2 Degradación de las amenazas

Tabla 12: Valor degradación de amenazas

Valor	Criterio	
100%	MA	Degradación muy alta del activo
80%	A	Degradación alta considerable del activo
50%	M	Degradación mediana del activo
10%	B	Degradación baja del activo
1%	MB	Degradación muy baja del activo

Fuente: Actual Investigación.

Tarea 2.2.3 Identificación y Valoración de Amenazas Tipo: Soporte de Información

Tabla 13: Valoración de Amenazas Tipo: Soporte de Información.

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[N.1] Fuego	FN	MA				
[N.2] Daños por agua	FN	A				
[N.*]Desastres naturales	MF	MA				
[I.6] Corte del suministro eléctrico	F	A				

Fuente: Actual Investigación.

[N.1] Fuego: Esta amenaza es poco normal, pero se valora como una degradación muy alta al 100% de llegase a ser materializada, porque donde se encuentra ubicada la empresa, las lluvias son constantes, así como las tormentas eléctricas, lo que provocaría incendios y daños eléctricos a los sistemas.

[N.2] Daños por agua: La disponibilidad en seguridad de que la amenaza se materialice es alta y una frecuencia normal, porque las estructuras de la empresa son antiguas y obsoletas; existe la probabilidad de que el agua acabe con los recursos del sistema.

[N.*]Desastres naturales: La amenaza se podría materializar por fenómenos sísmicos ya que en la zona de ubicación de la empresa a diario existe este fenómeno por causa del volcán Machín, de ahí su valoración muy alta 100% en la degradación y frecuencia a diario.

[I.6] Corte del suministro eléctrico: Esta amenaza es frecuente con degradación en su disponibilidad alta 80%, porque el fluido eléctrico no es estable en el Municipio debido a constantes lluvias y el poco mantenimiento de transformadores por parte de la empresa Enertolima.

Tarea 2.2.4 Identificación y Valoración de Amenazas Tipo: Equipamiento auxiliar

Tabla 14: Valoración de Amenazas Tipo: Equipamiento auxiliar.

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[A.7] Uso no previsto	N	A	M	M		

[A.11]Acceso no autorizado	FN	MA		A		
[A.23] Manipulación de los equipos	FN	MA		A		
[A.25] Robo	F	MA		MA		
[A.26] Ataque destructivo	PF	MA				
[E.25] Pérdida de equipos	PF	MA		MA		

Fuente: Actual Investigación.

Tarea 2.2.5 Justificación de Amenazas – Equipamiento auxiliar

[A.7] Uso no previsto: La probabilidad de ocurrencia es **N**, debido a que los equipos computacionales siempre están expuestos a ser vulnerados por terceros y pueden ser utilizados para otros fines diferentes a backup de información, monitoreo y trasmisión de señal. Su degradación es de mediano impacto en la dimensión de integridad y confidencialidad porque los recursos están indirectamente relacionados con los servicios y el negocio de la empresa Pijaos Telecomunicaciones SAS; De materializarse esta amenaza se tendría una afectación del 50% en el normal funcionamiento de los servicios.

[A.11]Acceso no autorizado: La dimensión que se afectaría directamente es la Disponibilidad y Confidencialidad y se cataloga como muy alta y alta debido a que si se llega a materializar ocasionaría la intrusión de varias amenazas como (A.25-A.23).

[A.23] Manipulación de los equipos: Se tiene una frecuencia de FN debido a que existe en la empresa una rotación inusual de técnicos, poca aplicabilidad de políticas de seguridad, lo que aumenta la vulnerabilidad a los equipos utilizados en la conectividad de fibra óptica. Su degradación es muy alta en la Disponibilidad y alta en la confidencialidad porque la información de password, usuario, u otros se filtraría para los usuarios finales que cuentan con el servicio. De materializarse esta amenaza se tendría una afectación del 90% en ventas del producto.

[A.25] Robo: Tiene una Disponibilidad y Confidencialidad muy alta en su degradación porque los equipos están muy expuestos en la zona rural, sin seguridad perimétrica. De materializarse esta amenaza se llegaría a un 100% de pérdida del servicio.

[A.26] Ataque destructivo: Se valora muy alta la Disponibilidad de degradación, porque los equipos están expuestos a vandalismo o por filtración de la información de personal interno. El sistema de repetidoras no cuenta con protección alguna.

[E.25] Pérdida de equipos: Tiene una Disponibilidad y Confidencialidad muy alta en su degradación porque los equipos están muy expuestos a robos continuos en la zona, no tienen protección perimétrica, quedan con carencia para prestar el servicio. De materializarse esta amenaza se llegaría a un 100% de pérdida de equipos y por ende del servicio.

Tarea 2.2.6 Identificación y Valoración de Amenazas Tipo: Instalaciones

Tabla 14: Valoración de Amenazas Tipo: Instalaciones

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[A.26] Ataque destructivo	PF	MA				
[E.19] Fugas de información	PF	MA				

Fuente: Actual Investigación.

Tarea 2.2.7 Justificación de Amenazas – Instalaciones

[A.26] Ataque destructivo: Esta amenaza se tuvo en cuenta porque afectaría la disponibilidad en el activo sobre un nivel muy alto debido a la falta de protección de seguridad en los RAT (remote administration tool) de servidores, y cualquier persona no autorizada puede tener acceso.

[E.19] Fugas de información: Se consideró esta amenaza E.19 como afectación muy alta porque hay empleados poco instruidos en seguridad y sin querer revelan la información confidencial de la empresa.

Tarea 2.2.8 Identificación y Valoración de Amenazas Tipo: Servicios

Tabla 15: Valoración de Amenazas Tipo: Servicios

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[E.1] Errores de los usuarios	PF	MA	A	A		
[A.24] Denegación de servicio	PF	MA				

[A.19] Divulgación de información	PF			MA		
[A.5] Suplantación de la identidad del usuario	FN		A	A	A	

Fuente: Actual Investigación.

Tarea 2.2.9 Justificación de Amenazas – Servicios

[E.1] Errores de los usuarios: Se valora de muy alta degradación en la Disponibilidad del activo servicios porque los computadores de escritorio se encuentran en zonas cerradas, lo cual produce recalentamientos y daña los componentes de hardware del sistema. Esta amenaza puede producir reacción con otras amenazas.

[A.24] Denegación de servicio: Su valoración muy alta en la degradación en la dimensión de Disponibilidad, porque la capacidad de almacenamiento en servidores es mínimo con alta demanda de trabajo, lo cual provoca caída de los sistemas.

[A.19] Divulgación de información: Esta amenaza se consideró muy alta en la degradación del activo servicios, porque los usuarios no tienen capacitación y conciencia en materia de seguridad y revelan información confidencial.

[A.5] Suplantación de la identidad del usuario: Se valoró la dimensión de integridad, autenticidad y confidencialidad en una degradación alta, porque la empresa no tiene implementados los procedimientos en uso y manejo de contraseñas para acceder a servicios y se pueden tener con frecuencia.

Tarea 2.2.10 Identificación y Valoración de Amenazas Tipo: Personal

Tabla 16: Valoración de Amenazas Tipo: Personal

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[E.7] Deficiencias en la organización	PF	A				

[E.19] Fugas de información	FN			A		
[A.30] Ingeniería social	PF	A	A	A		

Fuente: Actual Investigación.

Tarea 2.2.11 Justificación de Amenazas – Personal

[E.7] Deficiencias en la organización: Se valoró en la dimensión de Disponibilidad en alta degradación y una poca frecuencia, porque hay una gran cantidad de empleados que toman medidas sobre los activos, con la posibilidad de variar esta gestión, lo podría materializar la amenaza.

[E.19] Fugas de información: Se consideró esta amenaza E.19 como afectación del activo con nivel alto porque hay empleados que no hacen una disposición final del papel con la máquina trituradora sino que lo disponen en la cesta de la basura, lo anterior puede hacer que la amenaza se materialice.

[A.30] Ingeniería social: Se valoró en las dimensiones de Confidencialidad, Integridad y Disponibilidad en alta la degradación, porque existen empleados de la región que al parecer entregan información a terceros o a la competencia, y de materializarse provocaría una afectación a los servicios.

Tarea 2.2.12 Identificación y Valoración de Amenazas Tipo: Datos / Información

Tabla 17: Valoración de Amenazas Tipo: Datos / Información

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[E.1] Errores de los usuarios	PF	A	A	MA		
[E.2] Errores del administrador	PF	A	A	A		

[E.19] Fugas de información	FN			A		

Fuente: Actual Investigación.

Tarea 2.2.13 Justificación de Amenazas – Datos / Información

[E.1] Errores de los usuarios: Se puede poner en consideración la amenaza E.1 de degradación alta en la Disponibilidad, Integridad y muy alta en la Confidencialidad del activo datos / información, porque los usuarios no son capacitados adecuadamente en activos de los computadores de escritorio se encuentran en zonas cerradas, lo cual produce recalentamientos y daña los componentes de hardware del sistema. Esta amenaza puede producir reacción con otras amenazas.

[E.2] Errores del administrador: Se valora en alto, porque dado un error de administrador la Disponibilidad de servicios, y software se verían gravemente afectados, quedando entre dicho el profesionalismo del personal de TI. Su probabilidad de ocurrencia es poco frecuente.

[E.19] Fugas de información: Se consideró esta amenaza E.19 como afectación del activo con nivel alto porque hay empleados que no hacen una disposición final del papel con la máquina trituradora sino que lo disponen en la cesta de la basura, lo anterior puede hacer que la amenaza se materialice.

Tarea 2.2.14 Identificación y Valoración de Amenazas Tipo: Equipos informáticos

Tabla 18: Valoración de Amenazas Tipo: Equipos informáticos

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[A.23] Manipulación de los equipos	PF	A		MA		
[E.23] Errores de mantenimiento/ actualización	PF	A				

de equipos (hardware)						
[N.1] Fuego	PF	MA				

Fuente: Actual Investigación.

Tarea 2.2.15 Justificación de Amenazas – Equipos informáticos

[A.23] Manipulación de los equipos. El grado de degradación es muy alto en la dimensión de Confidencialidad debido a la falta de concientización en políticas de seguridad para un adecuado manejo de los sistemas de cómputo en el área administrativa, así como la Disponibilidades alta ya que cada usuario tiene asignado un sistema de cómputo, lo anterior podría materializar la amenaza.

[E.23] Errores de mantenimiento/ actualización de equipos (hardware): Esta amenaza se valora en la disponibilidad de alta su degradación, porque los equipos de la empresa son antiguos, y hay una política de mantenimiento a los mismos, lo que podría generar la materialización de la amenaza.

[N.1] Fuego: Se valora en muy alto impacto en la dimensión Confidencialidad, porque al presentarse fuego sería un desastre grave ya que todo el material informático u otros relacionados. No se cuenta con la adecuada protección ante esta amenaza por falta de organización y orientación informática en la empresa.

Tarea 2.2.16 Identificación y Valoración de Amenazas Tipo: Aplicaciones

Tabla 19: Valoración de Amenazas Tipo: Aplicaciones

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[A.11] Acceso no autorizado	PF	MA				
[E.4] Errores de configuración	FN	A				
[A.15] Modificación deliberada de información	PF		MA			

[E.8] Difusión de software dañino	PF	A	A	MA		

Fuente: Actual Investigación.

Tarea 2.2.17 Justificación de Amenazas – Aplicaciones

[A.11] Acceso no autorizado. Se valora en muy alta la degradación en el activo aplicaciones, porque de presentarse algún tipo de rompimiento de seguridad al sistema, traería como consecuencia la materialización de la amenaza.

[E.4] Errores de configuración: Se valora en alta la degradación porque en una configuración con errores en los activos en este caso las aplicaciones Informáticas llevaría a ataques como intrusión, y denegación de servicios.

[A.15] Modificación deliberada de información: Afectará la dimensión de integridad en un nivel muy alto, porque de presentarse ataques de modificación de información se van a ver adulterados los datos almacenados en los activos, causando un traumatismos informático y suministrando datos erróneos a la hora de las consultas y transacciones.

[E.8] Difusión de software dañino. Esta amenaza afectaría la degradación del activo aplicaciones en las dimensiones Disponibilidad (alta), Integridad (alta) y Confidencialidad (muy alta), porque en el desconocimiento de normatividad en materia de seguridad de algunos empleados darían apertura a los correos infectados lo que ocasionaría intrusión por robo de información y por ende un fatal riesgo para la información de la empresa.

9.3.5 Actividad A2.3: Caracterización De Las Salvaguardas.

Para contrarrestar las amenazas se elabora la caracterización de salvaguardas. Esta caracterización se lleva a cabo según el grado de criticidad del análisis de riesgos elaborado a la empresa Pijaos Telecomunicaciones SAS, y según catálogo de elementos de Magerit V3 (ver Anexo D).

Tarea 2.3.1 Salvaguardas activos: Protección Generales u Horizontales

Tabla 20: Salvaguardas: protecciones generales y horizontales

Salvaguardas	Dimensión	Evaluación

Identificación y autenticación	**(A), (D), (C), (I), (T)**	90%
Control de acceso lógico	**(A), (D), (C)**	30%
Herramientas de seguridad	**(D), (C), (I), (T), (A)**	80

Fuente: Actual Investigación

Tarea 2.3.2 Descripción de salvaguardas

Identificación y autenticación: Actualmente los sistemas de cómputo no tienen implementada esta técnica de validación de datos a usuarios autorizados, por medio de esta salvaguarda se obtiene el aseguramiento de la información sensible de la empresa, se valora en 90% en las dimensiones autenticidad, disponibilidad, confidencialidad, integridad y trazabilidad porque existe la probabilidad de ser vulnerada, o filtrada la información del usuario hacia un tercero.

Control de acceso lógico: Por medio de esta salvaguarda se protege activos de categoría aplicaciones y servicios en las dimensiones de autenticación, disponibilidad, y confidencialidad de usuarios del servicio, y se valora en un 30% porque existe gran variedad de herramientas para el aseguramiento, pero hay una gran mayoría que son fácilmente vulnerables.

Herramientas de seguridad: La salvaguarda permite evaluar las vulnerabilidades existentes, las cuales deben ser fortalecidas con excelentes herramientas de seguridad como por ejemplo la herramienta de evaluación de seguridad de Microsoft (MSAT), su valoración en 80% obedece a que existe un margen de error en algunas aplicaciones o programas, fallas de actualización en los administradores de TI, y usuarios, fallas de fabricante para su total aseguramiento.

Tarea 2.3.3 Salvaguardas activos: Protección De Los Datos / Información

Tabla 21: Salvaguardas: Protección De Los Datos / Información

Salvaguardas	Dimensión	Evaluación
Protección de la información	**(A), (D), (C), (I)**	80%
Copias de seguridad de los datos (backup)	**(A), (D), (C), (I), (T)**	20%
Cifrado de la información	**(A), (D), (C)**	50%

Fuente: Actual Investigación

Tarea 2.3.4 Descripción de salvaguardas

Protección de la información: Esta salvaguarda permite proteger la información revisando e identificando los requerimientos de confidencialidad o acuerdo de no-divulgación con frecuencia ante los empleados y contratistas de la empresa. Se valora en un 80% porque suelen presentarse algunos casos de filtración, sustracción de la información vía correo, USB, CD, u otros para vender o filtrar a la competencia.

Copias de seguridad de los datos (backup): Se valora en un 20% debido a que las copias de seguridad se hacen en discos externos, CD, u otros medios que no garantizan las dimensiones en disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad; Con esta salvaguarda se debe hacer un procedimiento debidamente documentado para el cumplimiento y transparencia en todas las dimensiones.

Cifrado de la información: Esta salvaguarda permite cifrar con algoritmos matemáticos para almacenar contraseñas de información sensible. Se valora en un 50%, ya que la data que tienen algunos usuarios puede ser alterada para falsear el sitio y obtener acceso administrativo.

Tarea 2.3.5 Salvaguardas Activos: Protección De Los Servicios

Tabla 22: Salvaguardas: Protección De Los Servicios

Salvaguardas	Dimensión	Evaluación
Protección de servicios y aplicaciones web	**(D), (I)**	50%
Se aplican perfiles de seguridad	**(A), (D), (I)**	70%
Aseguramiento de la disponibilidad	**(A), (D), (C)**	50%

Fuente: Actual Investigación

Tarea 2.3.6 Descripción de salvaguardas

Protección de servicios y aplicaciones web: La protección de servicios y aplicaciones web de la empresa Pijaos Telecomunicaciones SAS tiene algunas herramientas de autenticación básica, como el cifrado de paquetes y una seguridad NTFS, pero faltan medidas de control en materia de seguridad para obstruir ataques cibernéticos y que no comprometan las dimensiones de Disponibilidad e Integridad de servicios. La valoración baja obedece porque no hay medidas estrictas en seguridad, se debe optimizar los procesos de cifrado de contraseñas y creación de procesos de cifrado y mantenimiento de las mismas.

Se aplican perfiles de seguridad: Para contrarrestar la amenaza en la empresa ya que no cuenta con los aseguramientos de seguridad necesarios, se deben aplicar perfiles de seguridad robustos a cada usuario que requiere ingresar a los sistemas como encriptación a las copias de seguridad, encriptación de datos, etc. Se valora en medio-alta la dimensión de Autenticidad, Integridad, y Disponibilidad por la necesidad urgente de implementar sistemas seguros con referencia a los perfiles de usuarios para su acceso de servicios.

Aseguramiento de la disponibilidad: Para tener una Disponibilidad permanente en acceso a servicios de los diferentes activos de la empresa se debe tener unos procesos, protocolos e instructivos de paso a paso altamente sofisticados en seguridad para evitar errores, intrusiones, y poner en riesgos los sistemas. Se valora en medio-alto porque la empresa implementa controles más seguros para garantizar el aseguramiento de la Disponibilidad.

Tarea 2.3.7 Salvaguardas Activos: Protección De Los Equipos (Hardware)

Tabla 23**:** Salvaguardas Activos: Protección de los equipos (Hardware)

Salvaguardas	Dimensión	Evaluación
Operación	**(C), (D)**	60%
Protección de los Equipos Informáticos	**(D), (I)**	50%
Cambios (actualizaciones y mantenimiento)	**(D), (C)**	70%

Fuente: Actual Investigación

Tarea 2.3.8 Descripción de salvaguardas

Operación: Esta salvaguarda se requiere en la empresa para mitigar muchos fallos de seguridad en los servicios de los sistemas y manipulación de cómputo, esto se lograría con personal calificado y debidamente capacitado con las normas ISO 27001, 31000, soporte y helpdesk entre otras, tener planes de auditoría y seguimiento en todos los procesos. Su valoración se debe a la forma de manipulación de los equipos.

Protección de los Equipos Informáticos: La empresa tiene falencia en la protección de los equipos informáticos por desconocimiento de las medidas de aseguramiento actuales en el mercado y por el estado de desarrollo de la misma. Esta salvaguarda mitiga esta amenaza con firewall, DNS, antivirus, perfiles de usuario, etc. Su valoración esta en punto medio porque se debe ajustar mejores y mayores medidas de seguridad.

Cambios (actualizaciones y mantenimiento): Los sistemas de cómputo de la empresa requiere cambios sustanciales en versiones nuevas de equipos, sistemas de cableado, dispositivos enlace punto a punto de señal, tecnificar las antenas

transmisoras, etc., y a otros tener un plan de mantenimiento ajustado y de continuo seguimiento para evitar fallos de seguridad.

9.3.6 Proceso P3: Estimación Del Estado De Riesgo

Esta actividad tiene como finalidad analizar datos recopilados en los procesos anteriores y evaluar el estado de riesgo en lo que respecta al impacto y al riesgo. Se proporciona la escala líneas abajo para la valoración de activos, la magnitud del impacto y el riesgo.

Tarea 3.1 Escala calificación: estimación del riesgo

escalas		
impacto	probabilidad	riesgo
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB:** muy raro	**MB:** despreciable

Fuente: Magerit V.3 – Libro III – Guía de técnicas.

9.3.7 Actividad A.3.1: Estimación de impacto

La finalidad de la estimación de impacto es poder establecer el grado de daño o consecuencias sobre los activos en caso de materialización de la amenaza, dentro de las dimensiones de Disponibilidad, Confidencialidad, Integridad, Autenticidad, y Trazabilidad, utilizando la tabla propuesta por Magerit V3.

Según calificación media; se deben revisar nuevamente para modificar, alta y muy alta; se debe dar tratamiento de forma prioritaria y/o urgente.

Tabla 24**: Valores de estimación de impacto**

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

Fuente: Magerit V.3 – Libro II - Catálogo de Elementos.

Impacto acumulado: Es la posibilidad y exposición de impacto de los sistemas en base a la valoración de activos y amenazas sin contar con las salvaguardas y son de atención urgente.

Impacto residual: Es el producto final de fusionar la valoración de amenazas, activos y la eficiencia de salvaguardas tenidas en cuenta.

Tabla 25**: Valoración impacto en activos de información**

ACTIVO	AMENAZA	IMPACTO ACUMULADO					IMPACTO RESIDUAL				
		D	**I**	**C**	**A**	**T**	**D**	**I**	**C**	**A**	**T**
Soporte de información	[N.1] Fuego										
	[N.2]Daños por agua										
	[N.*]Desastres naturales										
	[I.6]Corte del suministro eléctrico										
Equipamiento auxiliar	[A.7]Uso no previsto										
	[A.11]Acceso no autorizado										
	[A.23]Manipulación de los equipos										
	[A.25] Robo										
	[A.26]Ataque destructivo										
	[E.25] Pérdida de equipos										
Instalaciones	[A.26]Ataque destructivo										
	[E.19] Fugas de información										

Servicios	[E.1] Errores de los usuarios										
	[A.24] Denegación de servicio										
	[A.19] Divulgación de información										
	[A.5] Suplantación de la identidad del usuario										

Tabla. 25 a (Continuación)

ACTIVO	AMENAZA	IMPACTO ACUMULADO					IMPACTO RESIDUAL				
		D	**I**	**C**	**A**	**T**	**D**	**I**	**C**	**A**	**T**
Personal	[E.7] Deficiencias en la organización										
	[E.19] Fugas de información										
	[A.30]Ingeniería social										
Datos / Información	[E.1] Errores de los usuarios										
	[E.2] Errores del administrador										
	[E.19] Fugas de información										
Equipos informáticos	[A.23]Manipulación de los equipos										
	[E.23] Errores de mantenimiento/ actualización de equipos (hardware)										
	[N.1] Fuego										

Aplicaciones	[A.11] Acceso no autorizado										
	[E.4] Errores de configuración										
	[A.15]Modificación deliberada de información										
	[E.8] Difusión de software dañino										

Fuente: Actual Investigación

9.3.8 Actividad A.3.2: Estimación del riesgo

La estimación del riesgo se valida en la siguiente escala cualitativa, en referencia al impacto acumulado y frecuencia.

Tabla 26: Valores de frecuencia

Valor			Criterio
100	Muy frecuente	MF	A diario
50	Frecuente	F	Mensual
30	Normal	N	Una vez al año
10	Poco frecuente	PF	Cada varios años

Tabla 27: Criterios de valoración para estimación de riesgo

RIESGO		**FRECUENCIA**			
		PF	**FN**	**F**	**MF**
IMPACTO	MA	M	A	MA	MA
	A	B	A	MA	MA
	M	B	M	A	A
	B	MB	B	M	A
	MB	MB	MB	B	B

Se toman los valores de frecuencia de ocurrencia de cada amenaza contra los activos e impacto acumulado para su gestión urgente.

Tabla 28: Valoración de riesgo en activos de información

ACTIVO	AMENAZA	IMPACTO ACUMULADO					F	RIESGO
		D	I	C	A	T		
Soporte de información	[N.1] Fuego						FN	
	[N.2]Daños por agua						FN	
	[N.*]Desastres naturales						PF	
	[I.6]Corte del suministro eléctrico						F	
Equipamiento auxiliar	[A.7]Uso no previsto						N	
	[A.11]Acceso no autorizado						FN	
	[A.23]Manipulación de los equipos						FN	
	[A.25] Robo						F	
	[A.26]Ataque destructivo						PF	
	[E.25] Pérdida de equipos						PF	
Instalaciones	[A.26]Ataque destructivo						PF	
	[E.19] Fugas de información						PF	
Servicios	[E.1] Errores de los usuarios						PF	
	[A.24] Denegación de servicio						PF	
	[A.19] Divulgación de información						PF	

	[A.5] Suplantación de la identidad del usuario						FN	

Tabla 28 a (Continuación)

ACTIVO	AMENAZA	IMPACTO ACUMULADO					F	RIESGO
		D	I	C	A	T		
Persona	[E.7] Deficiencias en la organización						PF	
	[E.19] Fugas de información						FN	
	[A.30]Ingeniería social						PF	
Datos / Información	[E.1] Errores de los usuarios						PF	
	[E.2] Errores del administrador						PF	
	[E.19] Fugas de información						FN	
Equipos informáticos	[A.23]Manipulación de los equipos						PF	
	[E.23] Errores de mantenimiento/ actualización de equipos (hardware)						PF	
	[N.1] Fuego						PF	
Aplicaciones	[A.11] Acceso no autorizado						PF	
	[E.4] Errores de configuración						FN	

	[A.15]Modificación deliberada de información						PF	
	[E.8] Difusión de software dañino						PF	

Fuente: Actual Investigación

9.3.9 Actividad A.3.3: Estimación del riesgo en todas sus dimensiones

En la estimación del riesgo en cada una de sus dimensiones (Disponibilidad, Integridad, Confidencialidad, y Autenticidad), se hace basado en la metodología Magerit V3, Dimensiones de valoración. En referencia al impacto por probabilidad de ocurrencia.

Tabla 29: Valores de frecuencia (Probabilidad de amenaza- magnitud del daño)

Valor	Criterio
1	**Insignificante** (incluido Ninguna)
2	**Baja**
3	**Mediana**
4	**Alta**

Fuente: Magerit V.3 – Libro II –Dimensiones de Valoración.

Tabla 30: Criterios de valoración

RIESGO	**PROBABILIDAD DE AMENAZA**			
	1	**2**	**3**	**4**
MAGNITUD DEL DAÑO	4	8	12	16
	3	6	9	12
	2	4	6	8
	1	2	3	4

El riesgo es el producto de multiplicar la probabilidad de amenaza por la magnitud del daño y están agrupados así: **Bajo Riesgo** = 1 – 6 (verde) **Medio Riesgo** = 8 – 9 (amarillo) **Alto Riesgo** = 12 – 16 (rojo)

Tabla 31: Valoración de riesgo en activos de información

AMENAZA	Magnitud de daño	Activos/ Probabilidad de amenazas															
		Soporte de información				Equipamiento auxiliar				Instalaciones				Servicios			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
[N.1] Fuego	3			9					12			9			6		
[N.2]Daños por agua	4				16	4				4						12	
[N.*]Desastres naturales	2		4					6				6					8
[I.6]Corte del suministro eléctrico	3			9			6				6				6		
[A.7]Uso no previsto	4	4					8			4					8		
[A.11]Acceso no autorizado	3				12		6						12			9	
[A.23]Manipulación de los equipos	2			9					8			9			6		
[A.25] Robo	3				16	3				4						12	
[A.26]Ataque destructivo	4		4					6				6					8
[E.25] Pérdida de equipos	3			9			6				6				6		
[A.26]Ataque destructivo	2	2					8			4					4		
[E.19] Fugas de información	2				8		6						8			6	
[E.1] Errores de los usuarios	3		4					6				6					8
[A.24] Denegación de servicio	2			6			6				6				6		
[A.19] Divulgación de información	3	3					8			4					6		
[A.5] Suplantación de la identidad del usuario	4				16		8						16			12	

Tabla 31 a (Continuación)

AMENAZA	Magnitud de daño	Activos/ Probabilidad de amenazas															
		Personal				Datos / Información				Equipos informáticos				Aplicaciones			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
[E.7] Deficiencias en la organización	3		6						12			9			6		
[E.19] Fugas de información	4				16	4				4						12	
[A.30]Ingeniería social	2		4					6				6					8
[E.1] Errores de los usuarios	3			9			6				6				6		
[E.2] Errores del administrador	4	4					8			4					8		
[E.19] Fugas de información	3				12		6						12			9	
[A.23]Manipulación de los equipos	2			6					8			6			4		
[E.23] Errores de mantenimiento/ actualización de equipos (hardware)	3				12	3				3						9	
[N.1] Fuego	4		8					12				12					8
[A.11] Acceso no autorizado	3			9			6				6				6		
[E.4] Errores de configuración	2	2					4			2					2		
[A.15]Modificación deliberada de información	2				8		4						8			6	
[E.8] Difusión de software dañino	3		6					9				9					12

Fuente: Actual Investigación

9.3.10 Interpretación De Los Resultados

Los controles son ajustados según resultados de la tabla estimación de riesgos acorde a necesidades y características de los activos.

Soporte de información:

- ➢ La exposición del riesgo es alto en la amenaza de fuego y daños por agua, debido a que en la zona llueve de forma intensa y la estructura de la empresa es antigua como muchas estructuras del Municipio de Cajamarca, y la posibilidad de subsanarlas es remota y es más por cultura e idiosincrasia de la gente.
- ➢ La energía o fluido eléctrico en la zona no es continua ya que constantemente permanece sin este servicio debido a fuertes vientos, lo que produce daños a los sistemas de cómputo y a todo el cableado de internet WIFI de la zona urbana y rural.

Equipamiento auxiliar:

- ➢ El acceso no autorizado tiene un riesgo alto porque no existen políticas ni compromisos de confidencialidad de la información para los usuarios que tienen equipos asignados, de igual forma se genera una mala manipulación de los equipos con riesgos evidentes en la empresa.
- ➢ El robo es frecuente en los activos de la empresa cuando se realizan desplazamiento a las zonas de trabajo especialmente a la zona rural.

Servicios:

- ➢ La empresa presenta cierta alteración de configuración de información por ataque de denegación de servicios o servidores sobrecargados con una frecuencia baja, pero requiere ajustar los procesos de configurar de router y firewall para la detención de direcciones IP inválidas, y bloquear tráfico inusual con el proveedor de internet.

Datos / Información:

- ➢ Se tiene errores de administrador en la empresa como la asignación de una misma contraseña para varios usuarios y la des configuración la lista de empleados para el control de acceso a la empresa, para evitar esta falencia se debe monitorear la disponibilidad de red permanentemente, mejorar la automatización de procesos internos en seguridad y re direccionar el tráfico.

Aplicaciones:

- ➢ El acceso no autorizado, genera un riesgo alto, porque en la empresa algunos usuarios prestan sus correos a terceros para envíos de información, en otros casos algunos empleados dan autorización de acceso a visitantes sin hacer uso de las tarjetas de identificación personal para este fin.

Infraestructura física:

- El cableado estructurado no es el requerido para ciertos fines, es decir no cumple con los requisitos mínimos y sin certificación de la norma RETIE.
- No se tienen sistemas de prevención contra incendios, lo que vulnerable las edificaciones y los sistemas de cómputo en la empresa.
- La estructura de las instalaciones son antiguas, lo que pone en riesgo amenazas con el fuego, perdida de información, daños por agua etc.

10. CONTROLES

OBJETIVO DEL CONTROL	CONTENIDO DEL CONTROL
Política de seguridad de información	
Documentar política de seguridad de información	La dirección general de la empresa debe validar y autorizar la gestión del diseño de la política de seguridad de la información, el cual debe ser notificado, publicado a todos los empleados, clientes y proveedores de la empresa.
Revisión de la política de seguridad de la información	La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.
Organización de la seguridad de la información	
Compromiso de la gerencia con la seguridad de la información	La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.
Coordinación de la seguridad de información	Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.
Asignación de responsabilidades de la seguridad de la información	Se deben definir claramente las responsabilidades de la seguridad de la información.
Acuerdos de confidencialidad	Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información.

Tabla 29 a (Continuación)

OBJETIVO DEL CONTROL	CONTENIDO DEL CONTROL
Gestión de activos	
Inventarios de activos	Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes.
Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.
Seguridad de los recursos humanos	
Roles y responsabilidades	Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización.
Seguridad física y ambiental	
Perímetro de seguridad física	Se debe utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.
Seguridad oficinas	Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.
Seguridad de computadores	
Ubicación protección equipo	El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.

Tabla 29 a (Continuación)

OBJETIVO DEL CONTROL	CONTENIDO DEL CONTROL
Seguridad en el cableado	El cableado de la energía y las telecomunicaciones que llevan data, sostienen los servicios de información deben ser protegidos de la intercepción o daño.
Mantenimiento de equipo	El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.
Protección contra software malicioso	
Controles contra software malicioso	Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.
Copias de seguridad o backup (respaldo de información)	Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.
Gestión de seguridad de redes	
Controles de red	Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.
Seguridad de los servicios de red	Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en-casa o sean abastecidos externamente.
Protección contra software malicioso	
Política de control de acceso	Se debe establecer, documentar y revisar la política de control de acceso.

Tabla 29 a (Continuación)

OBJETIVO DEL CONTROL	CONTENIDO DEL CONTROL
Gestión de privilegios	Se debe restringir y controlar la asignación y uso de los privilegios.
Gestión de la clave del usuario	La asignación de claves se debe controlar a través de un proceso de gestión formal.
Control de acceso a redes	Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.

10.1 Controles de acceso físico

Los servidores y área de comunicaciones estarán custodiados por un sistema de control de acceso físico, con el único fin de tener acceso solo al personal autorizado por el área de seguridad física, TI, y seguridad informática.

10.2 Protección a instalaciones

Se tendrá en cuenta los desastres naturales más conocidos como inundación, conato, detonaciones, marchas pacificas, riesgo público, u otros producidos por el hombre. Actuar en pro y de la mano de los sistemas sanitarios y de seguridad.

10.3 Seguridad física, industrial y ambiental

Controlar los posibles hurtos, conatos y factores ambientales que puedan perjudicar los sistemas informáticos que son los backup de la información y pilar fundamental de la empresa.

10.4 Seguridad del sistema de red (cableado)

El sistema eléctrico y comunicaciones que conducen los datos y dan energía a todos los sistemas de cómputos, e informáticos de la empresa mantendrán respaldados por UPS y planta de energía en los momentos necesarios para dar continuidad al respaldo de la información.

10.5 Ejecución de actividades en áreas protegidas

Se dará aseguramiento a las personas que laboran allí, así como terceros de la empresa, con guardabosques, custodios en la zona.

10.6 Protección contra software malicioso

El área de seguridad informática definirá los controles de detección y prevención ante eventos sensibles de software malicioso y asignará el personal experto para tal fin.

10.7 Controles criptográficos

En el aseguramiento de los servicios, datos y claves de acceso a usuarios, custodiar la información, con la emisión de backup permanentes de la información.

10.8 Control de acceso a aplicaciones

Respecto al acceso de la información en usuarios de aplicaciones, y personal de manejo y confianza como es el personal de TI, será bajo las premisas de la política de control de acceso según la aplicación y los permisos autorizados por su jefe inmediato, coordinador, administrador de sistemas de información.

10.9 Administración de password

Utilizar contraseñas seguras con letras, números y sistema de caracteres.

Cambio de contraseñas de forma permanente con un máximo de 3 meses.

Guardar las contraseñas con utilización de algoritmo de cifrado.

Mantener un registro de ultimas contraseñas asignadas a los usuarios en los últimos dos 2 meses y evitar reasignar las mismas a otros usuarios.

Modificar contraseñas que vienen predeterminadas por los proveedores una vez que se instale el hardware y software (portátiles, router, impresoras, cámaras de circuito cerrado etc.)

10.10 Autenticación de usuarios

Se asignará un usuario único o ID para uso personal e intransferible para todo el personal que tenga algún vínculo con la empresa por ejemplo desarrolladores, programadores, personal TI, operarios, técnicos de soporte.

10.11 Protocolo de conectividad

A los servicios informáticos tendrán acceso por medio de un protocolo de conexión segura, el cual será diseñado para restringir el acceso no autorizado.

10.12 Acceso a sistemas operativos

El área de seguridad informática constantemente realiza un seguimiento a los sistemas operativos para detectar vulnerabilidades, así mismo instalan medidas de seguridad para contrarrestar estos riesgos a los sistemas de cómputo de la empresa.

10.13 Seguridad en correo electrónico

La mala manipulación de los correos aceptando todo email sospechoso que vulnera la red a las cual se encuentran conectados los sistemas operativos.

11. CRONOGRAMA DE ACTIVIDADES

Tabla 29. Cronograma de actividades

	AGO	SEPT				OCT				NOV			DIC	
	SEM 4	SEM 1	SEM 2	SEM 3	SEM 4	SEM 1	SEM 2	SEM 3	SEM 4	SEM 1	SEM 2	SEM 3	SEM 1	SEM 2
Fase 1. Nivelar contenidos de proyecto de grado realizando los ajustes pertinentes.														
Revisión fase 1 con normas NTC 1486.														
Fase 2. Avance de objetivos de proyecto I.														
Fase 3. Avance final con todos los objetivos de proyecto desarrollados.														
Fase 4. Desarrollo de correcciones finales de proyecto.														

Fuente: Actual investigación.

12. CONCLUSIONES

Una vez culminado el proyecto se logra alcanzar todos los objetivos planteados; los controles generados permiten mejorar y normalizar los procesos de la empresa Pijaos Telecomunicaciones S.A.S aplicando las definiciones de seguridad de la información.

Dando aplicabilidad a la metodología MAGERIT V.3 “análisis de riesgos” se mitigó el riesgo existente e identificado en los activos de información y se proporcionó un normal funcionamiento interno de la empresa Pijaos Telecomunicaciones S.A.S.

Los controles y políticas de seguridad de la información resultado de este análisis de riesgos pueden ser tomados como soporte para la implementación del SGSI; en pro de disminuir el clima inminente de riesgo actual, tener a disposición las medidas de control existentes internas requeridas, reducir el grado de exposición de los sistemas que se ejecutan, aumentar la confiabilidad, integridad, autenticidad, trazabilidad y disponibilidad de la información.

Se pudo aprovechar y sacar el máximo rendimiento a los procesos orientados al cumplimiento de los objetivos de la empresa, con el fin de ir en pro de disminuir el riesgo actual a su nivel mínimo o aceptado.

La empresa Pijaos Telecomunicaciones S.A.S actualmente presenta un nivel de riesgo informático considerable, que con el apoyo de la alta gerencia y de todos los empleados es posible disminuir la exposición al riesgo existente

Es importante tener en cuenta, para próximas incorporaciones dar una buena capacitación para todos los empleados y directivos, con el fin de que conozcan la dimensión del problema de llegarse a tener ataques informáticos por no tener los controles y políticas establecidas por la ley, lo cual perjudicaría el capital humano, imagen, marca, presupuesto y empresa como tal.

13. RECOMENDACIONES

Como primera medida el proyecto de “análisis de riesgos de la seguridad de la información para la empresa Pijaos Telecomunicaciones SAS" debe ser socializado a todos los empleados para que sea de su conocimiento y posterior aprobación incluyendo las oportunidades de mejora que puedan surgir y así implementar y ejecutar controles propuestos al interior de la empresa Pijaos Telecomunicaciones SAS.

Implementación del Sistema de Gestión de Seguridad de la Información para proteger el activo valioso de todo empresa “La información”, para cual es necesario tener personal capacitado en seguridad para su debida implementación.

Capacitar al personal del área de TIC en temas de seguridad informática para apoyar el proceso de capacitación a todo el personal que de alguna manera tiene que ver la empresa Pijaos Telecomunicaciones SAS.

Revisar, autorizar y evaluar las políticas generadas dentro de este proyecto.

Los nuevos controles de seguridad resultado del análisis de riesgos deben ser puestos en funcionamiento a la mayor brevedad, toda vez que de esto depende la continuidad del negocio de la empresa Telecomunicaciones SAS.

La alta gerencia, debe tener en cuenta este estudio de seguridad informática, la aplicación e implementación del mismo además de incluir recursos necesarios para el desarrollo de la misma en el año 2018.

Los empleados de la empresa deben recibir un ciclo de capacitación y socialización del desarrollo del proyecto para conocer y adoptar la política de cambio de seguridad informática en pro de las mejores prácticas y/o mejoras de oportunidad.

Las directivas de la empresa deben por medio del área de TIC y de los directos responsables en este campo posibilitar estos cambios, haciendo uso de jornadas pedagógicas de simulacro de desastre informáticos, y así poder comparar los beneficios de los nuevos controles de seguridad.

Incluir dentro de las tareas del equipo de TIC auditorias permanentes y de seguimiento a los activos de información para actualizar controles y contribuir con el desarrollo de mejores prácticas y/o oportunidades de mejora relacionadas con la seguridad de la información.

14. DIVULGACIONES

El proceso de divulgación es muy importante llevar a cabo en la reunión mensual de la empresa Pijaos Telecomunicaciones SAS, con fin de sean notificado y enterado todo el personal de trabajadores de la empresa del análisis de riesgos de seguridad de la información, ya que debe haber una trazabilidad de la información tanto de los altos directivos como el último empleado de la empresa, y sensibilizar a todo el grupo empresarial que es un compromiso de todos analizar, controlar, mitigar y evaluar los riesgo en el activo más preciado que es la seguridad de la información como son los sistemas de cómputo, los cableados, archivos digitales y físicos etc., y que encaja en cada una de las áreas de la compañía.

En las instalaciones de la empresa Pijaos Telecomunicaciones se lleva a cabo la socialización del análisis de riesgos de seguridad de la información, explicando en detalle los pro y los contra, activos con mayor exposición a riesgos, amenazas tanto informáticas como naturales y humanas más frecuentes, riesgos potenciales, controles existentes y adicionales para mitigar el impacto y su posible materialización.

Se explica la matriz de riesgos con la cual fue valorado los activos, riesgos, impactos, probabilidad de amenazas, magnitud del daño en sus diferentes dimensiones como son la disponibilidad, confidencialidad, integridad y autenticidad.

El objetivo principal de la divulgación se enfoca en hacer ver a los empleados de la empresa la magnitud y exposición al riesgo de la información, aún más si cada empleado no aporta su granito de arena al respecto, y las pérdidas económicas que acarrea el hurto, venta, y comercialización de la información por parte de empleados o terceros, como de posibles ataques informáticos a los sistemas de cómputo.

Se deja evidencia en planilla de la asistencia de empleados de la empresa en la sección de anexos con el anexo B.

15. REFERENCIAS BIBLIOGRÁFICAS

ARDITA, Julio, Los desafíos de la ciberseguridad y la ciberdefensa, Argentina, 2016, (Recuperado el: 2 de Septiembre de 2017) http://www.cybsec.com/upload/Ardita_Arias_Segurinfo_AR_2016_Ciberseguridad.pdf

ISO/IEC TR 18044:2004. Information Technology, Security Techniques, Information Security Incident Management. ISO. Octubre de 2004 [En línea].https://www.iso.org/standard/35396.html

Magerit-versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 3-Guía de Técnicas. Magerit.[En línea]. https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/

COCHO, Julián Marcelo, y ROMO ROMERO, Santiago Martín. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea]. http://dis.um.es/~barzana/Curso03_04/MAGERIT.pdf

NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001. Tecnología de la información, técnicas de seguridad sistemas de gestión de la seguridad de la información, Requisitos. Bogotá. ICONTEC. 22 Marzo de 2006 p. 2, 3 ,4.

NTC 5411-1 Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la tecnología de la información y las comunicaciones. Parte 1: Conceptos y modelos para la gestión de la tecnología de la información y las comunicaciones (ISO/IEC 13335-1:2004).

LOPEZ CUENCA, David, Análisis Riesgos Dinámicos en Sistemas de Información, Tesis Universidad Complutense de Madrid Facultad de Informática, Madrid, Junio del 2012.

VALDÉZ CASTRO, Edgar. Tendencias de la auditoría informática. Santiago de Cali. Revisión de tema., 2009. Vol. 8, no. 8, 2 p.

NTC 1486:2008-07-23, Documentación. Presentación de tesis, trabajos de grado y otros trabajos de investigación.

VALENCIA, Cossio Fabio. Ley 1273 de 2009. [en línea], Fecha de publicación del artículo [revisado fecha en la cual lo consultó]. Disponible en Internet: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

16. LISTA DE ANEXOS

Anexo A. Encuesta aplicada de análisis de seguridad de la información en la empresa Pijaos Telecomunicaciones SAS.

Pregunta	Respuesta
Backup	
¿Evidenciar la documentación respaldada, su frecuencia, y su tiempo máximo como archivo vivo?	No se aplica este proceso.
¿Se respalda la información de forma prudencial, ya sea semanal al sistema de información disponible en la empresa?	Se realiza este proceso de forma semanal y monitoreo diario.
¿Existe instructivo para realizar restaurar copias de seguridad?	No.
¿La empresa realiza la buena práctica de encriptar las cintas de copias de seguridad, con fin de no ser recuperados en caso de hurto o pérdida?	No.
¿Cuál es el procedimiento en materia de seguridad de la información en las bases de datos?	Da permisos a nivel dominios. Cada servicio tiene un usuario definido Se definen grupos de dominio y cada uno tiene sus permisos.
Plan de contingencia	
¿Se tiene un plan de contingencia documentado?	No.
¿Hay UPS y generadores en el lugar?, ¿Estos son los suficientes buenos, en caso de fallos de energía cuanto tiempo podrían estos mantener los equipos informáticos funcionando?	1 Hora con plena carga. No hay planta.

Anexo A. (Continuación)

¿Qué clase de protección contra incendios tiene el centro de datos y sala de servidores?	Existen extintores para fuego.
Computador de escritorio y portátiles	
¿Desarrollan políticas para el uso de los dispositivos USB extraíble?	No existen restricciones para utilización de USB.
¿Ejecutar antivirus y anti-spyware en todos los equipos de escritorio o portátiles?	Se ejecuta agente antivirus constantemente. Se actualiza los clientes de antivirus constantemente contra una consola central
¿Desarrollan un procedimiento para garantizar que los computadores de escritorio y portátiles han instalado los últimos parches?	Se actualizan a través de un servicio centralizado de Microsoft
Acceso Remoto	
¿Se documentan las políticas de la empresa sobre acceso remoto?	No existen políticas para el acceso remoto
¿Se controla el acceso dial-up (RAS) y VPN de acceso remoto. Sólo establecer permisos para los que verdaderamente lo necesitan?	Si
¿Qué controles de seguridad se utilizan en las conexiones VPN (MR)?	Autenticación centralizada a través de directorio activo · Acceso a través de Firewall perimetral · Para algunos usuarios críticos se tiene autenticación adicional por certificados digitales (ejemplo proveedores)
Servidores, router, and switches	
¿Cada cuánto se ejecuta software antivirus sobre los servidores?	Se realiza un escaneo completo cada 8 días. Y el antivirus siempre está corriendo por si ocurre alguna amenaza.

Anexo A. (Continuación)

¿Asegurar que los servidores, router y switches tienen los últimos parches instalados?	Se actualizan los parches cada mes
¿Cómo se efectúa el Registrar los log de estos dispositivos a un servidor central de registro?	Los log se trabajan con la herramienta SIEM, que maneja el Log de operaciones del sistema operativo Windows. Con la herramienta LEM de Solar Wind (correlacionador de eventos), registra todos los logs, si hay una alerta critica la notifica al correo. Las alertas críticas están relacionadas con caída de un servicio, llenado de un disco duro, problemas de memoria, alta ocupación del procesador.
¿Quién es el administrador de acceso de estos dispositivos y con qué frecuencia se cambia la contraseña?	El administrador de servidores. Las contraseñas se cambian cada mes.
Software, Red de Internet y externa	
¿Se han realizado pruebas de penetración en la conexión a Internet periódicamente?	Se realizan pruebas de penetración 1 vez al año. Realizadas por un tercero.
¿Cómo se protege la red interna y la zona desmilitarizada de la red?	Se protege con el Firewall y un IPS (Controlador de tráfico) entre las diferentes zonas del firewall o estructura de la red.
¿Utilizan un sistema de prevención de intrusos para poner fin a ataques maliciosos?	Se utiliza IPS Fortinet.
¿Mantienen suficientes registros (logs) de la actividad de red aprobada?	Se hace suficiente registro de Log con SIEM
¿Se cifran los datos confidenciales que se transfieren a través de la red?	No se cifran, solo los que viajan por VPNIPSEC

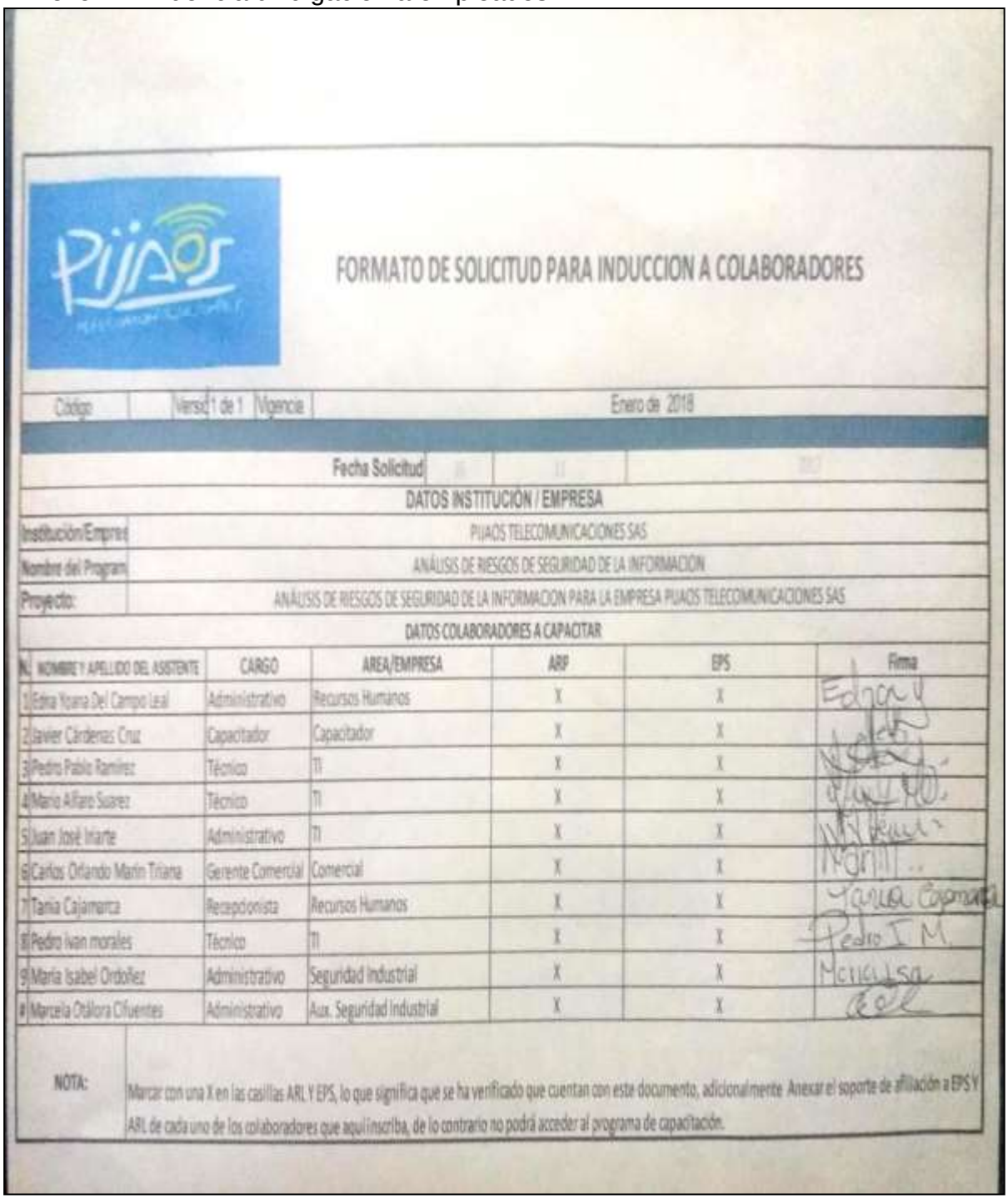
Anexo A. (Continuación)

¿Hay protección en las comunicaciones en redes públicas?	Se manejan certificados digitales para el acceso a páginas públicas, tales como conexión de correo la empresa por internet o él envió de información a bancos
Wireless	
¿Periódicamente se convoca a una compañía externa para realizar una prueba de penetración de las redes de acceso inalámbrico?	Se realiza 1 vez al año
¿Qué forma de encriptación WEP (Privacidad equivalente a cableado) se utiliza?	WPA - WPA2
¿Consideran la posibilidad de utilizar la autenticación 802.1X como un método secundario método de autenticación para usuarios Wireless (además de clave WEP)?	Si se puede considerar
¿Se ha definido la política de seguridad inalámbrica y educar a los usuarios sobre la misma?	En la actualidad no existe documentación de las políticas inalámbricas.
¿Permiten el tráfico desde la red de usuarios Wireless hacia los servicios corporativos?	No se permite
Información	
¿Existen controles para el uso medios removibles (MR)?	No existen
¿Existen procedimientos formales para alta y baja de usuarios (MR) (Acceso no autorizado)?	No
Personal	

Anexo A. (Continuación)

¿Existe concienciación y formación en seguridad para los funcionarios de la entidad (MR)?	En la actualidad no existe.
¿Existe supervisión a terceros dentro de la entidad?	Hay una persona que figura como interventora, pero no existe un seguimiento especifico
Navegación Web	
¿A través de que contralan la navegación en internet (un servidor proxy, un Router o un Firewall)?	FIREWALL
¿Cuáles son los responsables que tienen acceso a determinar quiénes pueden acceder a navegar por internet?	El administrador de la seguridad
¿Documentar el método para reportar que está navegando en la web, a quien se entregan los reportes y con qué frecuencia	La herramienta firewall genera un reporte y seguimiento de usuarios.
¿Cuáles son las reglas para definir una contraseña de usuario?	8 Caracteres · Deben estar conformadas por letras, números y caracteres. · Mayúsculas y minúsculas · No repetir las ultimas 10 contraseñas

Anexo B. Evidencia divulgación a empleados.



FORMATO DE SOLICITUD PARA INDUCCION A COLABORADORES

Código		Versión 1 de 1	Vigencia	Enero de 2018

Fecha Solicitud			

DATOS INSTITUCIÓN / EMPRESA

Institución/Empresa	PIJAOS TELECOMUNICACIONES SAS
Nombre del Programa	ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN
Proyecto:	ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACION PARA LA EMPRESA PIJAOS TELECOMUNICACIONES SAS

DATOS COLABORADORES A CAPACITAR

N.	NOMBRE Y APELLIDO DEL ASISTENTE	CARGO	AREA/EMPRESA	ARP	EPS	Firma
1	Edna Yoana Del Campo Leal	Administrativo	Recursos Humanos	X	X	
2	Javier Cárdenas Cruz	Capacitador	Capacitador	X	X	
3	Pedro Pablo Ramirez	Técnico	TI	X	X	
4	Mario Alfaro Suarez	Técnico	TI	X	X	
5	Juan José Iriarte	Administrativo	TI	X	X	
6	Carlos Orlando Marín Triana	Gerente Comercial	Comercial	X	X	
7	Tania Cajamarca	Recepcionista	Recursos Humanos	X	X	
8	Pedro Ivan morales	Técnico	TI	X	X	
9	María Isabel Ordoñez	Administrativo	Seguridad Industrial	X	X	
10	Marcela Otálora Cifuentes	Administrativo	Aux. Seguridad Industrial	X	X	

NOTA: Marcar con una X en las casillas ARL Y EPS, lo que significa que se ha verificado que cuentan con este documento, adicionalmente Anexar el soporte de afiliación a EPS Y ARL de cada uno de los colaboradores que aquí inscriba, de lo contrario no podrá acceder al programa de capacitación.

Anexo D. Formato Política de seguridad en servidores.

<table>
<tr><td>No. Documento</td><td>1</td><td colspan="3" rowspan="2">POLÍTICA PARA LA ADMINISTRACIÓN DE SERVIDORES</td><td rowspan="3">  </td></tr>
<tr><td>Fecha de elaboración</td><td>20/11/2018</td></tr>
<tr><td>Fecha de actualización</td><td></td><td>Área:</td><td>Elaborado por:</td><td>Aprobado por:</td></tr>
<tr><td>Introducción</td><td colspan="5">Los servidores son fundamentales para dar acceso a la red local de la empresa, velando con las políticas de TIC en los respecta a la disponibilidad, integridad, trazabilidad, autenticidad, y confidencialidad.</td></tr>
<tr><td>Finalidad</td><td colspan="5">La manipulación de servidores se basa en la descripción de los requerimientos y acciones para tratar y eliminar virus de los sistemas de cómputo además de prevenir sus variantes.</td></tr>
<tr><td rowspan="6">Definiciones:</td><td colspan="5">Servidor: Es un sistema de cómputo de una avanzada que provee servicios a otros sistema que suelen llamarse cliente.</td></tr>
<tr><td colspan="5">Servicio web: El servidor web es un programa diseñado para transferir hipertextos, páginas web o páginas HTML (HyperTextMarkupLanguage): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de música.</td></tr>
<tr><td colspan="5">Servidor DNS: Sistema de nombre de dominio, sistema con nombres de dominios.</td></tr>
<tr><td colspan="5">UTM: UnifiedThreat Management (Tratamiento Unificado contra amenazas), dispositivo que permite la gestión unificada de amenazas.</td></tr>
<tr><td colspan="5">Servidor de Correo: Un servidor de correo es una aplicación informática cuya función es parecida al Correo postal solo que en este caso los correos (otras veces llamados mensajes) que circulan, lo hacen a través de redes de transmisión de datos.</td></tr>
<tr><td colspan="5">Sistemas Informático: Tipo de información, recursos en línea, medios de almacenamiento magnético y todas las actividades relacionadas a información computacional, incluyendo cualquier dispositivo capaz de recibir correos.</td></tr>
</table>

Anexo C. (Continuación)

Políticas Para La Administración De Servidores	Se debe garantizar que el sitio físico donde se instalarán los servidores y equipos adicionales para su funcionamiento sea el adecuado. Si es un servidor nuevo se deben considerar algunos de los pasos generales antes de la adecuación del mismo: Instalación del sistema operativo adecuado e idóneo según el servicio que prestará dicho equipo. Si es un sistema operativo de tipo comercial se debe instalar el licenciado por la institución. Se deberán aplicar los respectivos parches de seguridad y actualización correspondientes al sistema instalado y un sistema de protección o antivirus. Se deberá configurar el acceso red de acuerdo a las los servicios prestados; esta configuración va de la mano con la política de configuración y administración de sistemas firewall-UTM. Se deberá generar un documento actualizable con los parámetros de seguridad, configuraciones de servicios en ellos aplicados, logs de auditoría. Se deben actualizar constantemente parches de seguridad, de aplicación o de actualización de componentes o servicios, para garantizar la estabilidad de los servidores. Es aconsejable hacer un mantenimiento físico o hardware de los servidores por lo menos una vez al año. Se debe monitorear constantemente el estado de los servicios y aplicaciones que cada uno de los servidores presta.
Alcance	Esta Política aplica a los encargados directos del mantenimiento y administración de los servidores con los que cuenta la empresa.
Sanciones Disciplinarias	La violación de esta política puede resultar en acciones disciplinarias que puede ocasionar llamado de atención a los empleados y contratistas o consultores.

Anexo D. Consentimiento informado.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
PROGRAMA DE SEGURIDAD INFORMATICA

CONSENTIMIENTO INFORMADO

Yo, Carlos Orlando Marín Triana con cedula de ciudadanía #1.105.611.909 en calidad de Gerente, expreso mi consentimiento para que el-la estudiante del programa de Especialización en Seguridad Informática; Javier Cárdenas Cruz identificado- a con cedula de ciudadanía # 86.043.407 realice el trabajo de campo del curso Proyecto de Seguridad Informática , señalando que he sido debidamente informado-a sobre el proceso, los alcances y las condiciones del ejercicio académico que se va a adelantar.

En constancia firmo:

Carlos Orlando Marin Triana
Gerente
Pijaos Telecomunicaciones S.A.S
e-mail: comercialpijaos@gmail.com
Celular: 314 411 0651

Ciudad: Cajamarca Tolima, Fecha: Marzo 07 de 2016

Universidad Nacional Abierta y a Distancia UNAD

FI-GQ-OCMC-004-007
000-17-03-2010

Anexo E. Carta de AVAL de la empresa donde será aplicado el proyecto.

Cajamarca Tolima, Marzo 18 de 2016

CARTA DE AUTORIZACIÓN

Señores
UNAD
Universidad Nacional Abierta y a Distancia
Ciudad.

Por medio de la presente se da autorización para realizar el proyecto de **Seguridad Informática**, impartido por la universidad UNAD al señor Javier Cárdenas Cruz con cedula de ciudadanía No. 86.043.407 de V/cio.

Este proyecto se desarrollará con fines única y exclusivamente académicos como parte de los requisitos necesarios para acreditar la materia de proyecto en su seguridad informática de su especialización.

Atentamente,

CARLOS ORLANDO MARIN TRIANA
Gerente Comercial
Pijaos telecomunicaciones

Calle 6 N°8-09 oficina 201 Cajamarca, Tolima Celular 3125018979 Tel. 0982-871501
www.pijaostelecomunicacionescolombia.com www.cajamarcadigital.co
Email. pijaostelecomunicaciones@hotmail.com pijaostel@gmail.com