ETAPA DE PLANIFICACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA PYMES.

OSCAR ARMANDO DE ARMAS MATÍAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
VALLEDUPAR
2024

ETAPA DE PLANIFICACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA PYMES.

OSCAR ARMANDO DE ARMAS MATÍAS

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

NOMBRE
EDGAR ROBERTO DULCE VILLARREAL
DIRECTOR DEL TRABAJO DE GRADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
VALLEDUPAR
2024

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Dedico este trabajo muy en especial a cada miembro de mi familia, mi esposa e hijos quienes con amor me han acompañado con ánimo y comprensión en cada etapa de este trayecto académico el cual ha sido todo un desafío para mí, dedico este trabajo en segundo lugar a todos los ingenieros y especialistas en seguridad informática el cual deseo sirva esta monografía como un aporte académico significativo no sólo para futuras investigaciones sino que además sea un punto de partida para naturalizar la seguridad informática como un requisito indispensable en las organizaciones de cualquier índoles, industriales y pymes y cesen los ataques a la seguridad de la información.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

GLOSARIO

CONFIDENCIALIDAD: Es la garantía de que la información solo es accesible por las entidades o personas autorizadas.

CONTROLES DE SEGURIDAD: para las políticas de seguridad de la información se categorizan en tres tipos de controles. Físicos, técnicos y administrativos.

DISPONIBILIDAD: Es la garantía de que las personas o usuarios autorizados por el sistema, tengan acceso a la información en el momento en que la requieran.

INTEGRIDAD: Es la convicción de protección del intercambio de datos contra la alteración deliberada o accidental de los mensajes transmitidos.

RIESGOS: es la expresión que refieren a la incertidumbre presente ante la posible exposición de un suceso relacionado con la amenaza de daño respecto a los bienes o servicios informáticos de una entidad.

NORMALIZACIÓN: Se refiere a un conjunto de estándares o normas que representan la base técnica para el comercio, la gestión de calidad y producción en los productos finales y servicios como también contempla la relación que debe existir éticamente entre los compradores y vendedores, en otras palabras, la normalización es el canal que permite facilitar la conformidad con las reglamentaciones técnicas. Las normas para sistemas de gestión de seguridad se encuentra la normalización ISO/IEC 27001 Esta norma internacional proporciona un marco de gestión de seguridad de la información que puede ser adaptado a las necesidades de las pequeñas y medianas empresas

PRUEBAS: Se fundamenta en verificar que el emisor de la información está bien identificado y que posee los derechos y accesos a determinada información, esta verificación debe ocurrir también para el receptor de la información.

PYMES: definidas según las leyes colombianas como aquellas que poseen una planta de personal inferior a 200 empleados y activos totales de hasta 30.000 salarios mínimos mensuales legales vigentes Grupo empresarial de menor y mediana envergadura, su caracterización para clasificar al nombre de pyme tiene que ver con su estructura, principalmente el número de trabajadores pero también su estructura industrial organizacional diferente a los organigramas piramidales sino que son de estructuras un poco más planas ajenas a la burocracia.

VULNERABILIDAD: En las Ti y en seguridad de la información refiere a es un estado viciado en un sistema informático o respectivamente en un conjunto de sistemas que afecta las propiedades de un sistema de Gestión de seguridad de la

información el cual son la confidencialidad, la integridad y la disponibilidad de los sistemas de seguridad.

RESUMEN

Diseñar la etapa inicial de un sistema de gestión de seguridad de la información para Pymes, basado en la caracterización de coincidencias en los factores de vulnerabilidad más comunes en la entidad empresarial medianas y pequeñas, con el propósito de mitigar el impacto frente amenazas a partir de diagnósticos y prevención en la infraestructuras de las TI, pretende contribuir con metodologías apropiadas que se adapten a la realidad informática y financiera de las pequeñas y medianas empresas, como a su vez puedan responder a las diferentes necesidades frente a las diversas vulnerabilidades que frecuentemente enfrentan los pymes. Se pretende utilizar metodologías de Gestión de la información basado en los objetivos principales del manejo de la seguridad de datos[1]y además un análisis de vulnerabilidad para poder identificar comportamientos y técnicas que puedan ser malversadas por intrusos, riesgos o directas amenazas. Por lo que se podrá analizar los estándares de seguridad y la vulnerabilidad del sistema, a partir de allí se analizarían y se propondrían sistemas de protocolos y operaciones basado en el manejo y seguridad de datos. La Confidencialidad, integridad, disponibilidad y prueba que se adapte a un escenario simulado en una pyme y considerando toda la caracterización de las mismas, así se puedan corregir las vulnerabilidades eficazmente, diagnosticar las amenazas, y prevenir los riesgos o ataques al sistema de datos del TI.

Palabras Claves: Ciberseguridad, gestión de riesgos, pyme, sistemas de información, política de seguridad, OCTAVE

[1] CARPENTIER, Jean-François. *La seguridad informática en la PYME: Situación actual y mejores prácticas*. Ediciones ENI, 2017. https://books.google.es

ABSTRACT

Design the initial stage of an information security management system for SMEs, based on the characterization of coincidences in the most common vulnerability factors in the medium and small business entity, with the purpose of mitigating the impact against threats from diagnoses and prevention in IT infrastructures, aims to contribute with appropriate methodologies that adapt to the computing and financial reality of small and medium-sized companies, as well as to respond to the different needs in the face of the various vulnerabilities frequently faced by SMEs. It is intended to use Information Management methodologies based on the main objectives of data security management[2] and also a vulnerability analysis to be able to identify behaviors and techniques that can be misappropriated by intruders, risks or direct threats. Therefore, it will be possible to analyze the security standards and the vulnerability of the system, from there protocols and operations systems based on data management and security would be analyzed and proposed. The Confidentiality, integrity, availability and test that adapts to a simulated scenario in an SME and considering all the characterization of the same, so that vulnerabilities can be corrected effectively, diagnose threats, and prevent risks or attacks on the data system of IT.

Keywords: Cybersecurity, risk management, SMEs, information systems, security policy, OCTAVE

[2] CARPENTIER, Jean-François. *La seguridad informática en la PYME: Situación actual y mejores prácticas*. Ediciones ENI, 2017. https://books.google.es

1. INTRODUCCIÓN

Se tiene que para la actualidad se reconoce un evolutivo significativo en la tecnología, según la revista Portafolio, [3]en su artículo ‘’Las empresas colombianas se adaptan rápido al cambio tecnológico’’ indica una creciente eficacia y una aparente dependencia de ella (la tecnología) para la optimización de nuestros procesos, en especial si esos procesos son de carácter industrial que generen bienes y servicios indispensables para el desarrollo humano y el desarrollo financiero de una sociedad.

Las pymes, representan las pequeñas y medianas empresas que al igual que cualquier industria mayor requiere manejo y resguardo de la información que se utilice en su sistema de base de datos[4]. Para sus operaciones, seguridad jurídica y respaldo y asistencia a sus usuarios. Sin embargo, según Fernández Z Revilla[5] los Pymes no suelen caracterizar la capacidad financiera que requiere un buen sistema de seguridad informática, siendo plan objetivo de diversos grupos que saben pueden tener éxito atacando las bases de datos de la información de un Pyme y si este es de carácter de emprendimiento menor o pequeña empresa es todavía más vulnerable atacar su sistema de resguardo de datos.

En el año 2009, la república de Colombia publicó La Ley 1273, donde se abordan los delitos informáticos que se producen sobre la población[6]. En el cual se estableció mediante un congreso donde se abordaron varios tipos de delitos informáticos, tales como la violación de datos personales, la suplantación de identidad en línea, la falsificación de documentos digitales, el acceso ilegal a sistemas informáticos, entre otros, como consecuencias de las alarmantes cifras de delitos informáticos se establecen medidas para la protección de la información almacenada en sistemas informáticos, incluyendo la obligación de mantener actualizados los sistemas de seguridad.
A partir de las iniciativas políticas de cooperación de mecanismos internacionales para la prevención, investigación y persecución de delitos informáticos. Entre ellos se encuentran las metodologías de los sistemas de Gestión de riesgos, el cual contemplan el manejo de la seguridad de datos[7] y los sistemas de análisis de riesgos y vulnerabilidades en los sistemas de protección y seguridad informáticos

[3] Álvarez, D., & Ortiz, J. (2019). Seguridad de la información en las PYMES: estudio de caso en Colombia. Revista Ingeniería Industrial, 19(1), 26-35.
[4] PYME. (2023, 20 de marzo). PYMES. Recuperado de https://pymes.afip.gob.ar/estiloAFIP/PYMES/default.asp
[5] Fernández, Z., & Revilla, A. (2010). Hacer de la necesidad virtud: los recursos de las pymes. Economía industrial, 375, 53-64.
[6] Congreso de la República de Colombia. (2009). Ley 1273 de 2009. Diario Oficial No. 47.420, de 5 de enero de 2009.
[7] CARPENTIER, Jean-François. *La seguridad informática en la PYME: Situación actual y mejores prácticas*. Ediciones ENI, 2017. https://books.google.es

que sean accesibles y aplicables a una entidad industrial o empresarial con características propias de los Pymes.

Ya que actualmente el ‘‘ciber’’ ataque en sus diferentes versiones y escalabilidad se ha convertido en una cotidianidad de nuestros tiempos, hay una urgencia internacional de diseños de planes orientados a la seguridad informática que garantice el resguardo de la información donde los Pymes requieren proteger y no suelen tener el recurso financiero para establecer metodologías de gestión de riesgos estandarizada garantes por entes institucionales altamente calificados y certificados.

De manera que, según lo expuesto anteriormente, existe una necesidad de plantear una etapa inicial de un diseño de un sistema de gestión de seguridad de la información para Pymes a partir de una gestión de análisis y riesgos de los sistemas de información, permitiendo condicionar políticas de seguridad y metodologías de diagnóstico de vulnerabilidades y eliminación de amenazas a partir de una investigación exhaustiva que determine qué tipo de amenazas y vulnerabilidades se enfrentan cotidianamente los Pymes, y se conozcan las condiciones de los sistemas actuales de la seguridad de la información en las pequeñas y medianas empresas en Colombia mediante fuentes de consultas bibliográficas certificadas y/o avaladas así mismo condicionar un sistema de Gestión de seguridad en base a la información expuesta de manera que dicha propuesta sea aplicable y pueda adaptarse a las necesidades y requerimientos de las Pymes, respaldado por un estándar internacional como lo representan las NORMAS ISO[8]

[8] ISOtools. (2021, 9 de mayo). La familia de normas ISO 27000. Recuperado de https://www.isotools.org/2015/01/21/familia-normas-iso-27000/:

1. DEFINICIÓN DEL PROBLEMA

1.1. ANTECEDENTES DEL PROBLEMA

En su artículo titulado ‘‘Ciberseguridad en Pymes de Colombia. Revista Tecnológica-Empresarial’’[9] presenta un estudio sobre la situación de la ciberseguridad en las Pymes de Colombia, donde se revela que el 85% de las Pymes en Colombia han sufrido algún tipo de ataque cibernético en los últimos dos años, y que el 55% de estas empresas no tienen ningún tipo de estrategia o plan de seguridad en línea. Además, se aborda la violación de datos personales, la suplantación de identidad, la falsificación de documentos digitales y otros delitos cibernéticos que afectan a las Pymes en Colombia.

Una estadística relevante sobre ataques informáticos a Pymes en Colombia se encuentra en el informe "Encuesta de Seguridad de la Información en Colombia 2021" realizado por la firma Kaspersky[10]. Según el informe, el 63% de las pequeñas y medianas empresas en Colombia sufrieron al menos un incidente de seguridad en los últimos 12 meses. Los incidentes más comunes incluyen la infección por malware, el phishing, el robo de datos, la suplantación de identidad y los ataques de denegación de servicio

Para el artículo de la Doctora en ingeniería informática Sandra Cristina Riascos Erazo[11]. Se Presenta el análisis exhaustivo del nivel de seguridad de los sistemas de información en 96 Pymes de la ciudad de Santiago de Cali (Colombia). Para tal efecto se estimaron tres variables: Confiabilidad, Disponibilidad e Integridad, obteniéndose como principal resultado que las Pymes tienen un nivel medio de seguridad en sus sistemas de información, en dicho artículo explican que esto es debido a que la mayoría de los sistemas de Gestión de seguridad de la información se establecían sin un debido análisis de riesgos y vulnerabilidades en la que las empresas en su diversidad organizacional podían enfrentarse o estar expuestas. Entendiéndose que contrataban servicio de seguridad informática aplicados de forma estándar y no ajustados a las características y necesidades de los sistemas de información que manejaban las pymes, su estructura organizacional, la cantidad y el tipo de usuarios que prestan el servicio y aquellos que lo reciben como por último los medios tecnológicos que usan o se requieren dependiendo el tipo de Pyme que representan.

---

[9] RODRÍGUEZ, M. (2018). Ciberseguridad en Pymes de Colombia. *Revista Tecnológica-Empresarial*, 11(1), 1-8

[10] KASPERSKY. (2021). Encuesta de Seguridad de la Información en Colombia 2021. Disponible en: https://latam.kaspersky.com/about/press-releases/2021_encuesta-seguridad-informacion-colombia/

[11] ERAZO, S. C., CASTRO, A. A., y Avila-Fajardo, G. P. (2019). Seguridad de los sistemas de información en las Pymes de Santiago de Cali (Colombia). *Libre Empresa*, 11(1), 107-118.

Este último antecedente es el más significativo para el marco teórico de la presente monografía el cual pretende proponer una etapa inicial de un sistema de Gestión de seguridad de la información para Pymes el cual está enfocado en caracterizar aquellos factores de coincidencia de vulnerabilidad más comunes en los Pymes, información que se obtendría en base a una investigación el referente bibliográfico disponible en fuentes certificadas o avaladas por lo que dicha investigación permite la formulación de la siguiente interrogativa al problema plateado.

1.2. FORMULACIÓN DEL PROBLEMA

¿Cómo determinar cuáles son los indicadores que acrediten una Metodología de Gestión de seguridad para la información como el más indicado para implementar en Pymes a partir de las conclusiones halladas ante las condiciones de los sistemas actuales de la seguridad de la información en las pequeñas y medianas empresas y que además prevea un sistema de gestión de riesgo según los posibles escenarios que puedan encontrarse?

2. JUSTIFICACIÓN

El cooperativismo y los Pymes en general constituyen una de las fuerzas productivas que más aporta al sistema financiero de la nación, generando beneficios laborales según estadística del 2021[12]
Sin embargo, es apenas un 36% de esa población significativa de microempresas y otro 25% en Empresas medianas que tienen un registro en los siniestros ARL. Entendiéndose que hay una participación diezmada que no son atendidas por los siniestros de seguridad al riesgo laboral.[13]

Por otro lado, están los altos costos de inversión que representan contar con TI. Siendo una necesidad identificar los métodos financieros sobre el retorno de inversión por concepto. Las asesorías especializadas en seguridad informática no representan una prioridad financiera, y por lo general no siempre está el conocimiento de la importancia de asegurar la información mediante un activo fijo en la economía financiera de la entidad empresarial. Pero hay una estadística en ascenso de que existen diversos grupos que conocen esta realidad y crean sistemas de detención de vulnerabilidades a los sistemas que no están bien salvaguardados. Y se comienza a crear una urgencia de proteger al sistema de micro y medianas empresas del riesgo cibernético.[14]

Por lo que se pretende identificar las condiciones de los sistemas actuales de la información en las pequeñas y medianas empresas, a través de consultas bibliográficas partir la información recolectada y posteriormente analizada se puede establecer diferentes metodologías para un sistema de gestión y análisis de los riesgos de la información, con políticas de seguridad principalmente para los usuarios trabajadores de un pyme, y en segundo lugar para los usuarios que adquieren el servicio de dicha empresa. Por lo que es un estudio analítico y bibliográfico en esencia principal, que permitirá un aporte al impacto económico de la agenda administrativa en la que las pymes responden por al menos 17 millones de empleos generados en el país según cálculos del Acopi[15]

---

[12] CAMARGO, L. A. (2021). En primer trimestre de 2021 aumentó 9,3% la creación de empresas en Colombia. *Confecámaras*. Disponible en: https://www.confecamaras.org.co/noticias/785-enprimer-trimestre-de-2021-aumento-9-3-la-creacion-de-empresas-en-colombia

[13] Federación de Aseguradores Colombianos. (2018). Seguridad y Salud en el trabajo: Una mirada desde la pequeña y mediana empresa. Consultado el 22 de marzo de 2023. Disponible en: https://www.ins.gov.co/seguridadysalud/docs/Memorias/9.pdf

[14] SÁNCHEZ-SÁNCHEZ, P. A., García-González, J. R., Triana, A., & Perez-Coronell, L. (2021). Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia. *Información tecnológica*, *32*(5), 121-128.

[15] MARTÍNEZ, Cristian Fernando; ROTAVISTA MERCADO, Adriana; VANEGAS, Jessica Fabiola. (2022). Análisis de las afectaciones generadas en las PYMES en Colombia producto de la emergencia sanitaria COVID-19.

Además, la aplicación de políticas de seguridad de la información que sea desarrollada debidamente a partir de una gestión de riesgos permitirá la implementación de medidas y controles de seguridad en la pyme desde el diagnóstico y visualización temprana de amenazas o riesgos de la seguridad de la información de la empresa, por lo tanto, de manera se podrá mitigar o eliminar el impacto frente a una amenaza.

3. OBJETIVOS

3.1. OBJETIVOS GENERAL

Diseñar la etapa de planificación de un sistema de gestión de seguridad de la información para Pymes, basado en la caracterización de coincidencias en los factores de vulnerabilidad más comunes en este tipo de empresas siguiendo la metodología OCTAVE, con el propósito de mitigar el impacto frente amenazas a partir de diagnósticos y prevención en las infraestructuras TI.

3.2. OBJETIVOS ESPECÍFICOS

- Analizar las condiciones de los sistemas actuales de la seguridad de la información en las Pymes, mediante fuentes de consultas bibliográficas donde se pueda determinar cuáles son los factores que generan vulnerabilidad.

- Aplicar la metodología de gestión de riesgo OCTAVE a un escenario propuesto como Pyme, con el fin de identificar los activos de información críticos que podrían incidir en la continuidad de la entidad empresarial.

- Establecer un plan de tratamiento de riesgo basado en una guía de buenas prácticas con el fin de proponer controles de seguridad que gestionen el riesgo en una Pyme, teniendo en cuenta los hallazgos encontrados anteriormente.

- Proponer una política de seguridad de la información, a partir de la gestión de riesgos, que permita la implementación de controles de seguridad en la pyme, de manera que se pueda mitigar o eliminar el impacto frente a las amenazas encontradas.

4. MARCO REFERENCIAL

4.1. MARCO TEÓRICO

4.1.1. Los riesgos de la información que enfrentan los Pymes.

Según el documento monográfico sobre Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia[16]. Relata en su trabajo teórico y de investigación La exposición a vulnerabilidades informáticas como el común denominador en las organizaciones empresariales y de sus diversas características como industrias, grupos corporativos y pequeñas y medianas empresas (pymes).

Diversos autores afirman que todas las industrias y organizaciones son susceptibles a padecer delitos informáticos, para Fernández Z Revilla[17] las pequeñas y medianas empresas son cada vez más vulnerables en términos de seguridad informática. En el caso de las pymes son objetivo clave para diversos grupos cuya finalidad es tener éxito atacando las bases de datos de la información de un Pyme y así lograr lucrarse económicamente ante cualquier fallo de seguridad informática hallada.

En consecuente de otros referentes teóricos tenemos artículos publicados como el de Rodríguez. M[18] describen de forma caracterizada y en estadísticas verificables y manejadas por los congresos de la República de Colombia en los últimos 3 años el hecho de que un 85% de las Pymes en Colombia han sufrido algún tipo de ataque cibernético en los últimos dos años, y que el 55% de estas empresas no tienen ningún tipo de implementación de metodologías de seguridad de la información, políticas de seguridad o por lo menos un sistema de análisis de gestión de riesgos para diagnosticar o prevenir amenazas.

Actualmente está demostrado que los Pymes en Colombia son objeto de vulnerabilidad a los delitos informáticos, principalmente a la violación de la información y uso delictivo o ilegal de la misma. Para Riascos Erazo[19] algunos

[16] SÁNCHEZ-SÁNCHEZ, P. A., García-González, J. R., Triana, A., & Perez-Coronell, L. (2021). Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia. *Información tecnológica*, 32(5), 121-128.
[17] FERNÁNDEZ, Z., y REVILLA, A. (2010). Hacer de la necesidad virtud: los recursos de las pymes. *Economía industrial*, (375), 53-64.
[18] RODRÍGUEZ, M. (2018). Ciberseguridad en Pymes de Colombia. *Revista Tecnológica-Empresarial*, 11(1), 1-8.
[19] ERAZO, S. C. R., CASTRO, A. A., y Avila-Fajardo, G. P. (2019). Seguridad de los sistemas de información en las Pymes de Santiago de Cali (Colombia). *Libre Empresa*, 11(1), 107-118.

factores que pudieran explicar porque las pymes se encuentran tan expuestos y vulnerados tiene que ver con la capacidad financiera que destinan estas entidades empresariales desde sus activos para la protección de la información, el cual se presume son presupuestos mermados o insuficientes para contratar entidades especializadas que puedan probar una trayectoria de éxitos en la protección de sus usuarios que optan por sus servicios.

Fuentes consultadas en el artículo citado explican documentadamente como las Pymes les parece una opción factible el hecho de contratar servicios de seguridad informática que sean estandarizados y de bajos presupuestos y que estos suelen no ajustarse a las características y necesidades de los sistemas de información que manejaban las pymes y su diversidad organizacional.

4.1.2. Sistema de Gestión de Riesgos y de Seguridad informática como una herramienta necesaria para los PYMES

En el año 2009, la república de Colombia publicó La Ley 1273, donde se abordan los delitos informáticos que se producen sobre la población[20], por lo tanto, en un análisis exhaustivo en el artículo publicado por la Federación de Aseguradores Colombianos[21]. Explican que el manejo y resguardo de la información que se utiliza en medios informáticos, se ha convertido en un elemento vital dentro de todas las organizaciones, así como también de las Pequeñas Y Medianas Empresas, incluso desde la documentación de la ley citada anteriormente se emplean algunas sanciones por los delitos informáticos: que van desde multas económicas hasta penas privativas de libertad.

Las sanciones varían en función de la gravedad del delito cometido. La ley establece los procedimientos para la investigación y persecución de delitos informáticos. También se establecen las competencias de las autoridades encargadas de llevar a cabo estas tareas y por supuesto el tema de solicitar a las diferentes entidades que lo requieren a obligación de mantener actualizados los sistemas de seguridad.

Por lo que se recomienda que cada organización cuente con un debido plan de seguridad de la información y que esté contenga metodologías de análisis y gestión riesgos de los sistemas de información como recurso garante del patrimonio de cada entidad empresarial, sus activos y recursos financieros y la seguridad y resguardo de la privacidad de todos los usuarios que integren la entidad empresarial, por tanto

[20] Congreso de la República de Colombia. (2009, 5 de enero). Ley 1273 de 2009. Diario Oficial No. 47.420.
[21] Ministerio de Trabajo. (2015). Decreto 1072 de 2015, por el cual se expide el Decreto Único Reglamentario del Sector Trabajo. Bogotá, D.C. Consultado el 20 de marzo de 2023, en https://www.mintrabajo.gov.co/documents/20147/0/DUR+Sector+Trabajo+Actualizado+a+15+d%20e+abril++de+2016.pdf/a32b1dcf-7a4e-8a37-ac16-c121928719c8

Según la normativa ISO 27001 estas metodologías deben estar relacionadas objetivamente con los cuatro principios del modelo de seguridad de la información que redacta la normativa; estos son: confidencialidad, integridad, disponibilidad y pruebas[22]

4.1.3. Normativa y Estandarización que definen metodologías ágiles de gestión del riesgo para pymes

La seguridad informática corresponde a la terminología genérica para el conjunto de herramientas diseñadas con la objetividad de proteger los datos web, o almacenados en un sistema o equipo y evitar amenazas, factores de riesgos o ataques. La Organización Internacional de Normalización, tiene por principal actividad la elaboración de normas técnicas internacionales. Establecer las especificaciones de productos, servicios prácticos eficientes y óptimos, para garantizar que la industria se desarrolle de forma eficaz
Para el estándar internacional que contextualiza y clasifica el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan ISO 27001, entiende por seguridad informática un área de conocimiento de la ingeniería de sistemas que se encarga de analizar, diseñar y aplicar acciones para proteger la integridad y la privacidad de la información que ha sido almacenada en un sistema informático.

Proteger la integridad de la información no es su único objetivo conceptual y metodológico, sino que apunta a la protección de los sistemas de las amenazas de exposición, eso incluye desde virus informáticos, piratería informática, hackers o profesionales del saqueo informático. Esta norma internacional proporciona un marco de gestión de seguridad de la información que puede ser adaptado a las necesidades de las pequeñas y medianas empresas. Dentro de la estandarización se clasifican una serie de metodologías que según sus características se tienen por más apropiadas para aplicar a un Pyme.

Por otro lado, la norma incluye la identificación de los riesgos y la evaluación de los controles de seguridad en función de la probabilidad e impacto de los riesgos identificados.

4.1.4. Metodología OCTAVE

OCTAVE es una metodología de gestión de riesgo, en el ámbito de la seguridad de la información, existen tres metodologías basadas en el enfoque OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) que se utilizan

[22] Organización Internacional de Normalización. (Consultado 1 de abril de 2023). Origen ISO 27001-2013. Disponible en: http://www.iso27000.es/iso27000.html#section3a

para evaluar y gestionar los riesgos de seguridad en una organización. A continuación, se describen brevemente cada una de ellas.

Metodología OCTAVE: Esta es la metodología original de OCTAVE y se enfoca principalmente en las organizaciones de gran tamaño. Fue desarrollada por el CERT (Computer Emergency Response Team) en la Universidad Carnegie Mellon[23]. OCTAVE aborda la seguridad de la información desde una perspectiva integral, identificando los activos críticos, las amenazas y las vulnerabilidades en el entorno operativo de una organización.

OCTAVE-S: Esta metodología, también conocida como OCTAVE Simplified[24], fue desarrollada para ser aplicada en organizaciones de tamaño mediano. Se basa en el enfoque de OCTAVE original, pero se simplifica para hacerlo más accesible y manejable para empresas más pequeñas. OCTAVE-S utiliza un enfoque de equipo y se centra en la identificación de activos críticos y la evaluación de riesgos, sin profundizar en el análisis de amenazas y vulnerabilidades tan detalladamente como OCTAVE.

OCTAVE Allegro: Esta es una versión más reciente de la metodología OCTAVE y se diseñó específicamente para organizaciones pequeñas y medianas (PYMES). Se centra en la gestión de riesgos de seguridad de manera ágil y efectiva. OCTAVE Allegro simplifica aún más el enfoque de OCTAVE-S, proporcionando un marco de trabajo estructurado para identificar y gestionar los riesgos de seguridad de la información en PYMES

Para el desarrollo de los objetivos planteados se ha seleccionado la metodología OCTAVE Allegro, específicamente pro su estructura altamente adaptable a los pymes pequeños. Está basada en el marco de trabajo de la norma ISO/IEC 27001 y se enfoca en la evaluación de riesgos en organizaciones pequeñas y medianas[25] OCTAVE Allegro está diseñada para ser aplicada sin la necesidad de software especializado y se enfoca en la identificación de activos críticos, amenazas y vulnerabilidades, así como en la evaluación de impacto y la identificación de medidas de mitigación y controles de seguridad necesarios.

Dentro de la metodología OCTAVE Allegro, también se incluyen procesos de diagnóstico y prevención de amenazas. Según la página web de ‘‘Metodología de Evaluación de Riesgos Informáticos’’ redacta que la metodología OCTAVE se divide en cuatro fases: planificación, diagnóstico, diseño e implementación. En la fase de

[23] REINOSO CÓRDOVA, Andrés Rodrigo. (2017). *Análisis y evaluación de riesgos de seguridad informática a través del análisis de tráfico en redes de área local. Aplicación a un caso de estudio.* Tesis de Licenciatura. Quito.

[24] MONCAYO RACINES, Diana Elizabeth. (2014). *Modelo de evaluación de riesgos en activos de TIC'S para pequeñas y medianas empresas del sector automotriz.* Tesis de Maestría. Quito.

[25] C., & R. (2015). *Sistema para el Análisis y Gestión de Riesgos de Seguridad Informática en la Facultad 4.* (Bachelor's thesis, Universidad de las Ciencias Informáticas. Facultad 4).

diagnóstico, se realiza un análisis de los activos de información y se identifican las amenazas a los que están expuestos. Luego, se evalúa la probabilidad y el impacto de cada amenaza y se priorizan las amenazas en función de su importancia. En la fase de diseño, se desarrollan las estrategias y controles para mitigar las amenazas identificadas en la fase de diagnóstico. En la fase de implementación, se implementan las estrategias y controles diseñados en la fase anterior. En general, la metodología OCTAVE Allegro se enfoca en la gestión de riesgos de seguridad de la información y busca prevenir y mitigar las amenazas que puedan afectar a los activos de información críticos de una organización.

El método OCTAVE se desarrolló para organizaciones grandes con más de 300 empleados por lo tanto contempla 3 fases el cual establecen una visión para caracterizar la organización a la cual se implementaría el método OCTAVE.

4.1.4.1. Visión de organización.

Se caracterizan los elementos de activos, vulnerabilidades de organización, amenazas generalizadas, exigencias de seguridad y normas o políticas existentes.

4.1.4.2. Visión tecnológica

Se clasifican en dos premisas uno son los componentes claves y dos; las posibles vulnerabilidades técnicas que pudiera haber en el sistema TI el cual resguarda los datos de la información de la entidad empresarial**.**

4.1.4.3. Planificación de las medidas y mitigar los riesgos

Su clasificación deriva de la evaluación de los riesgos, posteriormente la estrategia de protección, la ponderación de los riesgos y plano de reducción de los riesgos a través d metodologías de gestión de riesgos complementarias.

Una vez la Metodología OCTAVE caracterice los elementos que definen la organización a partir de las fases de identificación se procede al desarrollo y aplicación de la metodología de gestión de seguridad de la información a partir de los métodos que la componen el cual anteriormente fueron mencionados: identificación de las amenazas, análisis de las amenazas, Diagnóstico de vulnerabilidades, implementación de medidas preventivas y por último Monitorio y evaluación Profunda.

En cuanto a la propuesta objetiva del presente trabajo monográfico s pretende evaluar la posibilidad de aplicar la lógica difusa en la gestión de riesgos y combinarla

con la metodología OCTAVE Allegro. La lógica difusa puede ser útil en la gestión de riesgos para evaluar la probabilidad y el

impacto de los riesgos de forma más precisa y realista, ya que permite la inclusión de valores intermedios y no solo valores binarios (alto/bajo, sí/no).

En el contexto de OCTAVE Allegro, se puede utilizar la lógica difusa para la evaluación de riesgos de la siguiente manera:

4.1.4.4. Identificación de factores de riesgo

Se identifican los factores de riesgo relevantes y se definen las variables de entrada y salida del sistema difuso.

4.1.4.5. Evaluación de los riesgos

Se utilizan las reglas difusas para evaluar los riesgos y determinar su probabilidad y su impacto.

4.1.4.6. Análisis de los resultados

Se analizan los resultados obtenidos y se determinan las acciones necesarias para mitigar los riesgos identificados.

4.2. MARCO CONCEPTUAL

4.2.1. Seguridad de la información

Un sistema seguridad de la información ‘‘engloba un conjunto de técnicas y medidas para controlar todos los datos que se manejan dentro de una institución’’[26] Explica que es necesario asegurar que la empresa se adhiere responsablemente a las condiciones de seguridad que establezca el sistema implementado, Además explica que este tipo de sistemas se basan en las nuevas tecnologías (TI), por lo que sugiere, que la seguridad de la información debe contemplar medidas en la que se garantice el resguardo de los datos que están disponibles en un sistema determinado y que éste sea de acceso restringido a un grupo de personas o usuarios por motivos razonables y que no sea necesario establecer continuas

[26] Business School. *Business School*. Obtenido de Business School (2018). Consultado 29 de marzo 2023 disponible en: https://www.obsedu.com/int/blog-investigacion/sistemas/seguridad-de-la-informacion-unconocimientoimprescindible?fbclid=IwAR2HbEnVWeXgBf5lGPHOxc4kAzqmP2FNo6P_cNP6CSffvxaeTq9GlNo2hxA

modificaciones. Los sistemas de información deben centrarse en 3 variables estandarizadas como la consigna objetiva del sistema de seguridad de la información el cual son ‘‘la confidencialidad, la autenticidad e Integridad de la misma’’[27] el cual es clave para hacer diferencia de los conceptos de seguridad de la información versus la seguridad informática.

Basado en lo anterior expuesto un sistema de seguridad de la información tiene que estar sustentado bajo una metodología de gestión de seguridad el cual debe estar respaldada por la normativa ISO 27001 basada en disciplinas complementarias como lo son la Gestión de riesgos de la información y la implementación de políticas de seguridad de la información con medidas y controles de seguridad como medida organizacional de la institución que requiere mitigar las amenazas o el impacto de ellas[28].

4.2.2. Gestión de Riesgos de Sistemas de información:

Se estrecha mediante niveles de riesgo en los sistemas de información y su identificación en las organizaciones. Hay una clasificación de los sitios y las formas en la que se pueden presentar riesgos a los sistemas de información, su numeración es de siete niveles de riesgo asociados a los sistemas de y plantea controles para miniarlos[29]. El objetivo principal de los sistemas de gestión de riesgos es proteger a la organización y su capacidad de lograr sus objetivos

4.2.3. Gestión De Riesgo En Las Pymes

Permite que se consideren conceptos fundamentales de la administración y gestión integral, como: la gestión del conocimiento, el proceso de toma de decisiones también llamado teoría de las decisiones, la gestión del talento humano, la gestión del portafolio y el plan estratégico de la organización[30], este último es muy importante ya que es la sección al que se le asigna la gestión de seguridad informática ya que supone que el plan estratégico de la organización tiene por finalidad identificar los riesgos que ponen en peligro la misión, la visión y los valores corporativos.

---

[27]QUINCHO, M. (2017). *Diseño De Un Sistema De Gestión De Seguridad De La Información Bajo La NTP ISO/IEC 27001:2014 Para La Municipalidad Provincial De Huamanga, 2016.* (Para optar el título profesional de Ingeniero Informático), Universidad Nacional De San Cristóbal De Huamanga, Ayacucho. Recuperado de http://repositorio.unsch.edu.pe/bitstream/handle/UNSCH/1751/TESIS%20SIS48_Cce.pdf?sequence=1&isAllowed=y

[28] MOYANO y L. Suarez, Y. (2017). *Plan de Implementación de SGSI basado en la norma ISO: 27001:2013 para la empresa de interfaces y soluciones.* (Optar El Titulo De Ingeniería En Telemática), Universidad Distrital Francisco José De Caldas, Bogotá, D.C. Recuperado de http://repository.udistrital.edu.co/bitstream/11349/6737/1/MoyanoOrjuelaLuzAdriana

[29] ELISSONDO, L. (2008). *Auditoria y Seguridad de Sistemas de Información.* Recuperado de http://econ.unicen.edu.ar/monitorit/index.php?option=com_docman&task=doc_downloaGDPSJLGDPS,WHP

[30] OSORIO MONTOYA y José Antonio. (2018). *Gestión de riesgo y seguridad en computación en la nube para pymes.* Recuperado de http://repository.unipiloto.edu.co/handle/20.500.12277/8614

4.2.4. Vulnerabilidad de sistemas informáticos

Representa la debilidad que puede estar presente en un sistema informático a nivel de software o hardware, esta debilidad le da la oportunidad a un agresor ‘‘violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones’’ (Muñoz Holguín y David)[31] Los segmentos de un código que no estén bien redactados representan una de las principales amenazas a los sistemas informáticos y a la información de los usuarios. Aunque ciertamente actualmente no existe un sistema de seguridad informática que sea totalmente en su 100% seguro ante amenizadas o vulnerabilidades.

4.2.5. Hardening

Versa sobre la configuración estructurada sobre los estándares de seguridad ante cualquier vulnerabilidad o ataque informático.[32]

El bastionado del hardening se establece en tres líneas

- Línea base de seguridad para usuarios**:** el cual desbloquea e equipo mediante acciones físicas y configura los equipos para denegar accesos a consola de comandos así solo se controla por los administrados y se evita el riesgo de afectar la red.

- Línea base de seguridad para usuarios VIP: gestión y priorización de usuario privilegiados según rol dentro del pyme, establece los requisitos de seguridad y privacidad.

- Línea base de seguridad para servidores: Bastionado de sistemas dependiendo
  del rol que desempeñan

4.2.6. Política Usuario Local y dominio

Determina perfil del usuario en un equipo local, los indicadores son el permiso de ejecución, los permisos de configuración, y los permisos de acceso

4.3. ANTECEDENTES

[31] MUÑOZ Holguín, D. y CUADROS Mejía, A. (2017). *Comparación de metodologías para la gestión de riesgos en los proyectos de las Pymes. Revista Ciencias Estratégicas*, 25(38), 319-338. ISSN: 1794-8347. Disponible en: https://www.redalyc.org/articulo.oa?id=151354939004 [Consulta realizada el 31 de marzo de 2023].
[32] ACOSTA, David. *Estándares de Configuración Segura Hardening en PCI.*

Se refieren a continuación el siguiente marco referencial de antecedentes relacionados con el tema monográfico en cuestión

Estudio monográfico titulado ‘‘Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001” [33] El artículo tiene como objetivo desarrollar habilidades en ingenieros de sistemas, que les permitan conducir proyectos de diagnóstico, para la implementación e implantación de sistemas de seguridad de la información – SGSI alineado con el estándar ISO/IEC 27001 y el sistema de control propuesto en la norma ISO/IEC 27002 dicho artículo se utiliza como fuente referencial en la exhaustiva información sobre los estándares de normalización ISO, además presenta un diverso análisis de resultados aplicando las fases de auditoría y la metodología de análisis y evaluación de riesgos en diferentes escenarios Pymes de Colombia.

Estudio monográfico ‘‘Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las pymes del Perú’’[34] su objetivo principal es documentar estadísticamente las variables que hacen posible el riesgo informático en las empresas del Perú. Exponiendo las diversas razones por la cual es vital la protección de la información, el artículo se toma como fuente referencial en los temas relacionados a las políticas seguridad de la información, a partir de una Gestión de riesgo y aunque no está fundamenta en una aplicación específica de alguna metodología e riesgo si tiene en su amplio repertorio teórico diferentes recomendaciones de las metodologías más aptas o altamente aplicables a diversos escenarios de pymes con sus características más comunes, entre ellas se encuentra la metodología OTAVE.

4.4. MARCO LEGAL

En el contexto legal sobre el tema de estudio se encuentra el contexto legislativo principal abordado en ítems de los riesgos informáticos a lo cual se exponen los PYMES, se tiene que en Colombia en el año 2009, la república de Colombia publicó La Ley 1273, donde se abordan los delitos informáticos que se producen sobre la población, se presentan a continuación algunos de los artículos contemplados en la ley los principales delitos informáticos contemplados en la Ley 1273 de Colombia, promulgada en el año 2009. Se tiene en cuenta que esta lista no es exhaustiva y se centra en algunos de los delitos más comunes identificados en la ley:

- Acceso abusivo a un sistema informático ajeno (Artículo 269A): Acceder sin autorización a un sistema informático o red electrónica protegida, con el fin

[33] OLARTE, Francisco Nicolás; ROSERO, Edgar Rodrigo Enriquez; DEL CARMEN BENAVIDES, Mirian. (2015). *Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica-ESPOL*, 28(5).
[34] INOGUCHI ROJAS, Antonio, y MACHA MORENO, Erika Lizet. (2017). *Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del Perú, 2016.*

de obtener, destruir, alterar, dañar o modificar información contenida en dicho sistema.

- Interceptación de datos informáticos (Artículo 269C): Acceder, interceptar, utilizar o divulgar sin autorización los datos o información contenida en un sistema informático o red electrónica.

- Daño informático (Artículo 269D): Destruir, dañar, borrar, deteriorar, alterar o suprimir datos o información contenida en un sistema informático o red electrónica.

- Uso de software malicioso (Artículo 269E): Crear, propagar, distribuir, introducir o utilizar programas de software diseñados para causar daños a sistemas informáticos o redes electrónicas.

- Fraude informático (Artículo 269F): Realizar cualquier acción fraudulenta utilizando medios electrónicos, como la suplantación de identidad, para obtener un beneficio económico o causar perjuicio a terceros.

- Sabotaje informático (Artículo 269G): Realizar acciones que interrumpan o impidan el funcionamiento normal de un sistema informático o red electrónica, causando perjuicio a terceros.

- Pornografía infantil (Artículo 269H): Producción, almacenamiento, distribución, difusión, adquisición o posesión de material pornográfico que involucre a menores de edad.

- Violación de datos personales (Artículo 269I): Acceder, recolectar, almacenar, usar, procesar, circular, transmitir, suprimir o destruir datos personales sin autorización.

5. ANALIZAR LAS CONDICIONES DE LOS SISTEMAS ACTUALES DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS PYMES, MEDIANTE FUENTES DE CONSULTAS BIBLIOGRÁFICAS DONDE SE PUEDA DETERMINAR CUÁLES SON LOS FACTORES QUE GENERAN VULNERABILIDAD.

La seguridad de la información en las pequeñas y medianas empresas (PYMES) es un tema importante ya que estas empresas suelen ser más vulnerables a las amenazas cibernéticas debido a su limitado presupuesto y recursos para invertir en sistemas de seguridad. A continuación, se presentan algunos referentes teóricos que pueden ser de utilidad para entender mejor esta problemática:

"Análisis de riesgos y seguridad de la información en las PYMES: un enfoque metodológico"[35]: Este estudio aborda la importancia de la seguridad de la información en las PYMES y propone un modelo de análisis de riesgos para identificar las amenazas y vulnerabilidades a las que están expuestas estas empresas. El autor destaca la necesidad de contar con una cultura de seguridad en la organización y de implementar medidas de protección adecuadas.

Para Álvarez y Ortiz en el estudio de "Seguridad de la información en las PYMES: estudio de caso en Colombia"[36] examinan la situación de la seguridad de la información en las PYMES colombianas y destaca los principales factores que contribuyen a la vulnerabilidad de estas empresas. Entre ellos se incluyen la falta de recursos, la falta de conciencia sobre la importancia de la seguridad de la información, la falta de capacitación y la falta de políticas de seguridad adecuadas.

El estudio titulado "Evaluación de la madurez de la gestión de la seguridad de la información en PYMES"[37] propone un modelo de evaluación de la madurez de la gestión de la seguridad de la información en las PYMES. El autor destaca la importancia de contar con una estrategia de seguridad de la información y de implementar medidas de protección adecuadas para garantizar la continuidad del negocio y la protección de los activos de la empresa.

"Ciberseguridad en PYMES: una revisión sistemática de la literatura"[38] Este estudio realiza una revisión sistemática de la literatura sobre la ciberseguridad en las PYMES y destaca los principales desafíos y oportunidades en esta área. Los autores señalan la importancia de contar con una cultura de seguridad, de

[35] LÓPEZ, M. A. (2016). *Análisis de riesgos y seguridad de la información en las PYMES: un enfoque metodológico. Revista de Investigación Académica*, 13, 1-12.
[36] ÁLVAREZ, D. y ORTIZ, J. (2019). *Seguridad de la información en las PYMES: estudio de caso en Colombia. Revista Ingeniería Industrial*, 19(1), 26-35.
[37] CRUZ, L. F. (2017). *Evaluación de la madurez de la gestión de la seguridad de la información en PYMES. Revista de Investigación Académica*, 17, 1-10.
[38] RODRÍGUEZ, M. (2018). *Ciberseguridad en PYMES de Colombia. Revista Tecnológica-Empresarial*, 11(1), 1-8.

implementar medidas de protección adecuadas y de estar preparados para responder ante incidentes de seguridad, es decir una adecuada metodología de gestión de riesgos.

El análisis del estado actual de la ciberseguridad en las PYMES colombianas, según el estudio de Llanos Palacios (R. D. J.)[39], revela una situación crítica en la que las amenazas cibernéticas están en constante aumento. Los delitos reportados a las autoridades, con la suplantación de sitios web y el robo de datos a la cabeza, demuestran la sofisticación y la frecuencia de los ciberataques dirigidos a estas empresas. Las estadísticas muestran que Colombia ocupa el puesto 39 en el ranking mundial de ciberseguridad, pero, a pesar de una inversión significativa de $10.400 millones de pesos durante la pandemia de Covid-19, entre marzo y noviembre de 2020 se presentaron 32.000 reportes de delitos informáticos. La suplantación de sitios web creció alarmantemente en un 372%, y otras modalidades del ciberdelito, como la modificación de datos personales, la extracción de datos y la ingeniería social, también experimentaron aumentos significativos.
Este panorama alarmante subraya la necesidad urgente de evaluar y abordar las condiciones actuales de la seguridad de la información en las PYMES, considerando los factores que generan vulnerabilidades. La falta de preparación y la vulnerabilidad especialmente marcada en las PYMES, como se evidencia en las estadísticas proporcionadas, resaltan la importancia de implementar medidas proactivas y fortalecer la ciberseguridad en estas empresas.

Estos son solo algunos ejemplos de los referentes teóricos disponibles sobre la seguridad de la información en las PYMES en Colombia. Es importante destacar que existen muchos otros estudios y publicaciones en esta área, pero básicamente se puede concretar que el principal elemento que interviene en el proceso de seguridad de la información y expone los datos de la empresa para usos delictivos tiene que ver con que las empresas no usan software que ejecutarían una metodología de gestión de riesgo, y esto es debido a que la mayoría de estos sistemas de seguridad de la de información son elevadamente costoso.

Los costos y presupuestos deben completar la estimación en la implementación de hardware, software, servicios y el personal técnico interno capacitado. Esos mismos costos de implementación se recapitulan para los costes de mantenimiento. Basado en una empresa pequeña, el gasto total puede superar los mil trescientos treinta y cinco mil euros (135.000€), lo que equivale aproximadamente a seiscientos sesenta y nueve millones, quinientos veinticinco mil, trescientos veintiún dólares ($669.525.325) en la economía colombiana.

En resumen, se presenta como una sólida opción para cumplir con el objetivo de establecer una gestión de riesgos adaptada a las necesidades específicas de las

[39] LLANOS PALACIOS, R. D. J. *Teletrabajo en Colombia: análisis del estado de la ciberseguridad en pequeñas y medianas empresas.*

pequeñas y medianas empresas (PYMES), considerando aspectos tecnológicos, organizacionales y estructurales. Esta metodología se basa en la norma ISO/IEC 27001, proporcionando un marco sólido y reconocido internacionalmente para abordar la seguridad de la información. Sin embargo, es importante destacar que, a pesar de sus ventajas, los costos asociados con la implementación de esta metodología pueden ser un obstáculo significativo para muchas PYMES. Esto se suma a la falta de recursos financieros y a una cultura empresarial que a menudo no reconoce plenamente la importancia de invertir en la seguridad de la información. Como resultado, muchas PYMES pueden optar por enfoques menos costosos y menos robustos en lugar de implementar metodologías de gestión de riesgos sólidas.

Es relevante señalar que existen otras alternativas para las PYMES que desean abordar la seguridad de la información sin incurrir en costos prohibitivos. Algunas de estas alternativas pueden incluir la utilización de herramientas de software libre específicas y la adopción de metodologías de gestión de riesgos independientes. Sin embargo, es importante tener en cuenta que estas metodologías independientes a menudo carecen de la estandarización y el reconocimiento internacional que ofrece la norma ISO, lo que puede limitar su capacidad para generar una cultura de seguridad sólida y competitiva en el entorno de las PYMES en Colombia.

En última instancia, la elección de la metodología de gestión de riesgos adecuada para una PYME dependerá de una evaluación cuidadosa de sus recursos, necesidades y objetivos. Independientemente de la elección, es esencial que las PYMES reconozcan la importancia de la seguridad de la información y trabajen en la promoción de una cultura empresarial que valore y respalde la inversión en seguridad cibernética para garantizar la protección de sus activos y la continuidad de sus operaciones en un mundo digital en constante evolución.

6. APLICAR LA METODOLOGÍA DE GESTIÓN DE RIESGO OCTAVE A UN ESCENARIO PROPUESTO COMO PYME, CON EL FIN DE IDENTIFICAR LOS ACTIVOS DE INFORMACIÓN CRÍTICOS QUE PODRÍAN INCIDIR EN LA CONTINUIDAD DE LA ENTIDAD EMPRESARIAL.

6.1. CARACTERIZACIÓN Y ESCENARIO DE UN PYME PEQUEÑO EN COLOMBIA

6.1.1. Descripción:

La consultoría en tecnología de la información se presenta como un recurso fundamental para diversas pequeñas y medianas empresas (PYMES). Este enfoque, genérico pero adaptable, busca ofrecer servicios de consultoría en tecnología de la información a PYMES en diversos sectores. Se contempla una plantilla de empleados que abarca consultores de TI, programadores y personal administrativo, con la flexibilidad para adaptarse a las necesidades específicas de cada PYME.

6.1.2. Ubicación:

Las operaciones se llevan a cabo en ubicaciones estratégicas, siendo la proximidad a otros negocios y oficinas gubernamentales una consideración clave. Este enfoque permite adaptarse a diferentes entornos empresariales y geográficos, garantizando la aplicabilidad de la consultoría en tecnología de la información a diversas realidades empresariales.

6.1.3. Productos/Servicios:

La gama de servicios ofrecidos se ajusta a las necesidades variadas de las PYMES, abarcando análisis de sistemas, desarrollo de software personalizado, mantenimiento de sistemas, asesoramiento en seguridad de la información y gestión de proyectos. La versatilidad de estos servicios permite su adaptación a diferentes contextos y requerimientos específicos de las PYMES.

6.1.4. Clientes:

Diversificando su alcance, la consultoría en tecnología de la información se orienta a PYMES en distintos sectores, tales como servicios legales, contabilidad, bienes raíces y logística. Este enfoque garantiza la aplicabilidad de los servicios de consultoría a una amplia variedad de PYMES.

6.1.5. Estructura Organizacional:

La estructura organizacional flexible abarca un equipo directivo compuesto por un director general, un director de operaciones, un director de finanzas y un director de tecnología. Además, se implementa una organización en equipos de trabajo según el tipo de servicio que ofrecen, asegurando una adaptación eficiente a las necesidades específicas de cada PYME.

6.1.6. Presupuesto:

La asignación presupuestaria anual para la implementación de medidas de seguridad de la información se personalizará según las necesidades y recursos específicos de cada PYME. Se contempla la inclusión de fondos para áreas clave como salarios, gastos operativos y adquisición de equipos de TI. Este enfoque permite una flexibilidad financiera, asegurando que la aplicación de la metodología OCTAVE se adapte eficientemente a la realidad económica de cada organización.

6.1.7. Activos De La Información:

Los activos de información, que varían según la PYME, incluyen datos de clientes, información financiera, documentos comerciales confidenciales, datos de facturación, información de recursos humanos, correos electrónicos y otros datos almacenados en los sistemas empresariales. La adaptabilidad de esta lista garantiza la consideración de los activos de información específicos de cada PYME.

6.1.8. Activos Físicos:

Los activos físicos, esenciales para la operación eficiente de las PYMES, incluyen equipos de cómputo, dispositivos de almacenamiento, servidores, dispositivos de red, equipo de seguridad física, documentos físicos importantes e infraestructura física. Esta lista puede ser ajustada para reflejar los activos específicos de cada PYME.

6.1.9. Vulnerabilidades En La Red:

Las PYMES podrían ser vulnerables a ataques a través de sus redes, ya que los datos de los clientes y de la empresa misma podrían ser accesibles desde una red comprometida. Es importante para estas organizaciones asegurarse de que los sistemas de firewall, antivirus y antimalware estén actualizados y configurados correctamente.

6.1.10. Falta De Políticas De Seguridad De La Información:

Muchas PYMES no cuentan con políticas claras de seguridad de la información, como la protección de contraseñas y la política de acceso, poniendo en riesgo los

datos de la empresa y de sus clientes. Es esencial para estas organizaciones establecer políticas claras y capacitar a los empleados para que las sigan.

6.1.11. Amenazas Internas:

Las amenazas internas, como la mala gestión de los datos, la filtración de información y el acceso no autorizado a la información confidencial, pueden representar un riesgo para las PYMES. Establecer controles de acceso adecuados y capacitar a los empleados para mantener la seguridad de la información es crucial.

6.1.12. Amenazas Externas:

- Ataques de malware, como virus, troyanos y gusanos, que pueden infectar los sistemas de información y comprometer la confidencialidad, integridad y disponibilidad de la información.Ataques de phishing que buscan engañar a los empleados para que revelen información confidencial, como contraseñas, datos de inicio de sesión y otra información sensible.

6.1.13. Vulnerabilidades En El Software:

Si las PYMES utilizan software que no está actualizado o que tiene vulnerabilidades conocidas, los atacantes pueden explotar estas vulnerabilidades para acceder a los datos de la empresa. Es crucial mantener el software actualizado y utilizar software de calidad y confiable.

6.1.14. Pérdida De Datos:

La falta de un sistema de respaldo y recuperación de datos adecuado podría llevar a la pérdida de datos importantes en caso de un desastre o una falla en el sistema para muchas PYMES. Establecer un sistema de respaldo regular y realizar pruebas periódicas es esencial para garantizar su correcto funcionamiento.

6.2. METODOLOGÍA OCTAVE ALLEGRO Y LAS FASES DE DESARROLLO PARA APLICAR UNA GSTIÓN DE RIESGO

Recapitulando sobre los pasos para la implementación de la metodología OCTAVE; donde se tiene que ésta se puede aplicar sin software especializado[40], su enfoque central se basa en determinar cuáles son los activos críticos, las amenazas y las vulnerabilidades del sistema de seguridad de la información que tiene el pyme, por lo tanto la metodología de riesgo evaluará el impacto y la identificación de medidas preventivas, de mitigación y controles de seguridad conforme a la situación actual del Pyme. A continuación, se detallan los pasos iniciales para implementar la

[40] LARA, C., & JAVIER, R. (2015). *Sistema para el Análisis y Gestión de Riesgos de Seguridad Informática en la Facultad 4.* (Bachelor's thesis, Universidad de las Ciencias Informáticas. Facultad 4).

metodología OCTAVE ALLEGRO en una pyme para la gestión de riesgos y el establecimiento de medidas preventivas, así como para la monitorización y evaluación continua del sistema de seguridad de la información mediante la siguiente tabla.

Tabla 1. METODOLOGÍA DE GESTIÓN DE RIESGO

Fase		Paso	Criterio
N° 1	**Planificación**	Formar un equipo de proyecto	Este equipo estará compuesto por expertos en seguridad de la información y representantes de las áreas relevantes de las pymes.
		Definir los objetivos del proyecto	Los objetivos deben ser claros y específicos, y deben incluir el alcance del proyecto, los recursos disponibles y el calendario.
		Identificar los activos de la empresa	En esta etapa se deben identificar los activos de la empresa, como los sistemas de información, las aplicaciones, las bases de datos, los documentos y otros recursos importantes.
		Identificar las amenazas y vulnerabilidades	En esta etapa se deben identificar las amenazas y vulnerabilidades potenciales para los activos de la empresa.
N°2	**Evaluación**	Evaluar los riesgos	En esta etapa se debe evaluar el riesgo asociado con cada amenaza y vulnerabilidad identificada en la etapa anterior. La evaluación de riesgos puede incluir una combinación de técnicas cuantitativas y cualitativas, como la asignación de puntajes de riesgo, la identificación de consecuencias potenciales y la probabilidad de ocurrencia

		Identificar medidas preventivas	Una vez que se han evaluado los riesgos, se deben identificar medidas preventivas para reducir los riesgos identificados. Estas medidas pueden incluir controles técnicos, controles de acceso físico, políticas y procedimientos de seguridad y entrenamiento para los empleados.
		Priorizar las medidas preventivas	En esta etapa se deben priorizar las medidas preventivas identificadas en función de su efectividad y costo, y de la evaluación de riesgos
N°3	**implementación**	Implementar medidas preventivas	Una vez que se han identificado y priorizado las medidas preventivas, se deben implementar en la empresa.
N°4	**Monitorización y evaluación continua**	Monitorear el sistema de seguridad de la información	Se debe monitorear continuamente el sistema de seguridad de la información de una pyme para detectar posibles amenazas y vulnerabilidades.
		Evaluar el sistema de seguridad de la información	Es importante evaluar periódicamente el sistema de seguridad de la información para asegurarse de que sigue siendo efectivo y adecuado para las necesidades de la pyme
		Mejorar el sistema de seguridad de la información	Si se identifican deficiencias en el sistema de seguridad de la información, se deben tomar medidas para mejorar el sistema y reducir los riesgos asociados con posibles amenazas y vulnerabilidades.

Fuente: Elaboración Propia

6.2.1. Análisis de Activos de Información Críticos en una pyme.

En este análisis detallado, se explorarán los activos de información críticos para las PYMES, destacando su importancia para la continuidad empresarial. Aunque previamente se han enumerado los activos, es esencial proporcionar una justificación sólida para establecer por qué son considerados críticos en el contexto de la organización y su entorno empresarial.

- **Información de Clientes:** Los datos de clientes, como nombres, direcciones y correos electrónicos, son esenciales para mantener relaciones comerciales y garantizar la satisfacción del cliente. La pérdida o compromiso de esta información podría afectar negativamente la confianza del cliente y la reputación de la empresa.

- **Información Financiera de Clientes:** Detalles de tarjetas de crédito y cuentas bancarias son activos críticos debido a su sensibilidad. Su exposición podría resultar en consecuencias financieras significativas tanto para los clientes como para la empresa, incluyendo pérdida de ingresos y posibles litigios.

- **Información Empresarial Confidencial:** Contratos, acuerdos de confidencialidad y propiedad intelectual son esenciales para las operaciones. La divulgación no autorizada de esta información podría conducir a la pérdida de ventaja competitiva y relaciones empresariales.

- **Datos de Facturación:** Facturas y estados de cuenta contienen información vital para la gestión financiera. La pérdida de estos datos podría interrumpir las operaciones y relaciones financieras.

- **Datos de Recursos Humanos:** Información personal de empleados, registros de empleo y nóminas son fundamentales para la gestión de recursos humanos. La exposición de estos datos podría resultar en problemas legales y de privacidad.

- **Correos Electrónicos y Archivos:** La correspondencia electrónica y archivos almacenados contienen información interna y externa vital. La pérdida o manipulación de estos datos podría afectar la comunicación interna y externa, impactando así la eficiencia operativa y las relaciones comerciales.

- **Información de Proveedores:** Datos de contacto y detalles de facturación de proveedores son fundamentales para la gestión de relaciones con proveedores. Su pérdida podría afectar la cadena de suministro y la continuidad operativa.

- **Información de Socios y Colaboradores:** Contratos y acuerdos con socios y colaboradores son activos críticos para las alianzas estratégicas. La exposición de estos datos podría afectar las relaciones comerciales a largo plazo y la viabilidad de proyectos conjuntos.

Este análisis se basa en la naturaleza sensible y estratégica de estos activos para las PYMES, subrayando su relevancia crítica para la continuidad del negocio y la seguridad de la información. Estos activos, al ser esenciales para las operaciones y la reputación de la empresa, deben ser protegidos meticulosamente para mitigar cualquier amenaza potencial y garantizar la integridad y confidencialidad de los datos empresariales.

6.3. IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

En esta sección, se describen las amenazas y vulnerabilidades clave identificadas para las PYMES en general. Además de enumerarlas, se proporciona una explicación de cómo se realizaron las identificaciones, incluyendo evidencia de amenazas actuales o potenciales y vulnerabilidades específicas que podrían afectar a las empresas.

6.3.1. Amenazas Identificadas

A continuación, se detallan las amenazas identificadas para las PYMES junto con la evidencia que respalda su identificación:

Amenaza 1: Ataques de Malware

- *Evidencia*: Se ha observado un aumento en los ataques de malware a nivel global, y varios informes de seguridad han alertado sobre la creciente sofisticación de los mismos.

Amenaza 2: Ataques de Phishing

- *Evidencia*: Las empresas en general han experimentado intentos de correos de phishing que buscan engañar a los empleados para revelar información confidencial. Se ha registrado un aumento en el número de estos intentos.

6.3.2. Vulnerabilidades Identificadas

A continuación, se describen las vulnerabilidades específicas identificadas en los sistemas y procesos de las PYMES:

Vulnerabilidad 1: Software Desactualizado

- *Evidencia*: Se ha realizado una auditoría de software que reveló que varios sistemas y aplicaciones utilizados por las empresas no están actualizados y carecen de parches de seguridad críticos.

Vulnerabilidad 2: Falta de Políticas de Seguridad de la Información

- *Evidencia*: Muchas PYMES carecen de políticas claras de seguridad de la información, como políticas de protección de contraseñas y políticas de acceso. Esto se evidenció mediante una revisión interna de políticas y procedimientos comunes en empresas de este tamaño.

Vulnerabilidad 3: Falta de Entrenamiento en Seguridad

- *Evidencia*: Se ha observado que, en muchas PYMES, los empleados no han recibido capacitación adecuada en seguridad de la información y buenas prácticas de seguridad. Esto se confirmó mediante encuestas internas y evaluaciones de conciencia de seguridad comunes en empresas similares

6.4. RELACIÓN ENTRE ACTIVOS, AMENAZAS Y VULNERABILIDADES

En esta sección, se detalla cómo los activos de información críticos para las PYMES están relacionados con las amenazas y vulnerabilidades identificadas, y cómo estas conexiones pueden dar lugar a riesgos para las empresas.

6.4.1. Activo de Información: Información de Clientes

- **Amenazas Relacionadas**:
  - **Ataques de Malware**: Estos ataques podrían comprometer la información de los clientes almacenada en los sistemas de la empresa, lo que resultaría en la pérdida de la confianza de los clientes y daños a la reputación.
  - **Ataques de Phishing**: Los intentos de phishing pueden llevar al robo de datos de clientes, como nombres y direcciones de correo electrónico, poniendo en peligro la información personal y financiera.

- **Vulnerabilidades Relacionadas**:
  - **Software Desactualizado**: Si los sistemas que almacenan información de clientes no están actualizados, se convierten en objetivos más fáciles para ataques de malware.

- **Falta de Políticas de Seguridad de la Información**: La ausencia de políticas de protección de contraseñas y acceso podría facilitar el acceso no autorizado a los datos de los clientes.

6.4.2. Activo de Información: Información Financiera de Clientes

- **Amenazas Relacionadas**:
    - **Ataques de Malware**: Los ataques de malware podrían comprometer la información financiera sensible de los clientes, lo que podría resultar en pérdidas económicas para los clientes y la empresa.
      Ataques de Phishing: Los intentos de phishing podrían llevar a la obtención de detalles de tarjetas de crédito y cuentas bancarias de los clientes, lo que podría resultar en fraude financiero.
- **Vulnerabilidades Relacionadas**:
    - **Software Desactualizado**: La falta de actualizaciones de seguridad podría dejar expuesta la información financiera de los clientes a ataques de malware.
    - **Falta de Políticas de Seguridad de la Información**: La carencia de políticas de seguridad podría facilitar el acceso no autorizado a los datos financieros.

6.5. EVALUACIÓN DE RIESGOS DE ACTIVOS CRÍTICOS

En esta sección, se realizará una evaluación de riesgos para cada activo crítico identificado. La evaluación incluirá la asignación de valores numéricos a la probabilidad de ocurrencia y al impacto potencial de los riesgos para comprender mejor la magnitud de los riesgos.
A continuación, se presenta una tabla que resume la evaluación de riesgos para cada activo crítico. Los valores de probabilidad e impacto se califican en una escala del 1 al 5, donde 1 representa un riesgo bajo y 5 un riesgo alto.

Tabla 2 Evaluación de Riesgos para Activos Críticos

Activo de Información	Riesgo de Probabilidad (1-5)	Riesgo de Impacto (1-5)	Riesgo Total (Probabilidad x Impacto)
Información de Clientes	4	5	20
Información Financiera de Clientes	3	4	12
Información Empresarial Confidencial	4	4	16
Datos de Facturación	3	3	9
Datos de Recursos Humanos	3	3	9
Correos Electrónicos y Archivos	4	3	12
Información de Proveedores	2	3	6
Información de Socios y Colaboradores	2	4	8

Fuente: Elaboración Propia

En la tabla anterior, se ha asignado un valor numérico a la probabilidad y al impacto para cada activo. El riesgo total se calcula multiplicando la probabilidad por el impacto. Esto proporciona una visión clara de qué activos enfrentan los mayores riesgos y requieren atención inmediata.

La evaluación de riesgos cuantitativa permite priorizar adecuadamente las medidas preventivas y de mitigación para reducir la exposición de las PYMES a los riesgos identificados.

6.6. MATRICES DE RIESGO PARA ACTIVOS CRÍTICOS EN LAS PYME'S

En esta sección, se presentarán las matrices de riesgo para varios activos críticos de las PYMES. Cada matriz de riesgo se divide en cuatro categorías según su probabilidad e impacto:

- **Alto Riesgo**: Riesgos con alta probabilidad e impacto.
- **Riesgo Medio**: Riesgos con probabilidad moderada e impacto moderado.
- **Bajo Riesgo**: Riesgos con baja probabilidad e impacto.
- **Riesgo Mínimo**: Riesgos con muy baja probabilidad e impacto mínimo.

Tabla 3 . Matriz de Riesgo para Información de Clientes

Riesgo	**Riesgo de Probabilidad (1-5)**	**Riesgo de Impacto (1-5)**	**Nivel de Riesgo**
Pérdida de Datos	4	5	Alto Riesgo
Acceso no autorizado	4	4	Riesgo Medio
Fugas de Información	3	4	Riesgo Medio
Ataques de Phishing	3	3	Riesgo Medio

Fuente: Elaboración propia

Tabla 4. Matriz de Riesgo para Información Financiera de Clientes

Riesgo	**Riesgo de Probabilidad (1-5)**	**Riesgo de Impacto (1-5)**	**Nivel de Riesgo**
Robo de Información	4	5	Alto Riesgo
Uso fraudulento	4	4	Riesgo Medio
Divulgación no autorizada	3	4	Riesgo Medio
Amenazas legales	2	4	Riesgo Medio

Fuente: Elaboración propia

Tabla 5. Matriz de Riesgo para Información Empresarial Confidencial

Riesgo	Riesgo de Probabilidad (1-5)	Riesgo de Impacto (1-5)	Nivel de Riesgo
Divulgación no autorizada	4	5	Alto Riesgo
Pérdida de contratos	3	4	Riesgo Medio
Vulnerabilidad de Propiedad Intelectual	3	4	Riesgo Medio
Ruptura de Acuerdos	2	3	Riesgo Medio

Fuente: Elaboración propia

Tabla 6. Matriz de Riesgo para Datos de Facturación

Riesgo	Riesgo de Probabilidad (1-5)	Riesgo de Impacto (1-5)	Nivel de Riesgo
Pérdida de Datos	3	4	Riesgo Medio
Fraude financiero	2	4	Riesgo Medio
Errores en facturación	2	3	Riesgo Medio
Interrupción de Servicios	3	4	Riesgo Medio

Fuente: Elaboración Propia

Estas matrices de riesgo proporcionan una visión general de los riesgos asociados con cada activo crítico y su nivel de prioridad. Cada riesgo se evalúa en función de su probabilidad e impacto, lo que ayuda a la empresa a tomar medidas proactivas para mitigar y gestionar estos riesgos de manera eficiente.

7. ESTABLECER UN PLAN DE TRATAMIENTO DE RIESGO BASADO EN UNA GUÍA DE BUENAS PRÁCTICAS CON EL FIN DE PROPONER CONTROLES DE SEGURIDAD QUE GESTIONEN EL RIESGO EN UNA PYME, TENIENDO EN CUENTA LOS HALLAZGOS ENCONTRADOS ANTERIORMENTE.

En esta sección, se delineará un plan integral de tratamiento de riesgo basado en las buenas prácticas de seguridad de la información. Este plan está diseñado para gestionar y mitigar los riesgos identificados previamente en las PYMES, teniendo en cuenta los hallazgos resultantes de la aplicación de la metodología OCTAVE y la evaluación de vulnerabilidades.

7.1. IDENTIFICACIÓN DE RIESGOS Y HALLAZGOS

Como se detalló en la sección anterior, se han identificado diversos riesgos y vulnerabilidades que podrían afectar la seguridad de la información en las PYMES en general. Algunos ejemplos concretos de estos riesgos incluyen:

- **Amenazas internas:** Acceso no autorizado de empleados.
- **Amenazas externas:** Ataques cibernéticos y malware.
- **Falta de políticas de seguridad:** Ausencia de directrices claras de seguridad.
- **Vulnerabilidades en la red:** Falta de actualización de sistemas y software.

7.2. OBJETIVOS DE SEGURIDAD

Los objetivos de seguridad que se buscan alcanzar con este plan incluyen:

- Salvaguardar la información confidencial de la empresa y de los clientes.
- Garantizar la disponibilidad y confiabilidad de los sistemas de información.
- Cumplir con las regulaciones de seguridad de la información aplicables.
- Minimizar el riesgo financiero y legal asociado con posibles brechas de seguridad.

7.3. SELECCIÓN DE CONTROLES DE SEGURIDAD

Para lograr estos objetivos, se han identificado y seleccionado una serie de controles de seguridad basados en guías de buenas prácticas reconocidas, como ISO/IEC 27001 y NIST SP 800-53. A continuación, se describen algunos de los controles seleccionados:

7.3.1. Control de Acceso Lógico

- Establecer políticas claras de acceso que definan roles y privilegios para cada empleado según sus responsabilidades.

- Implementar autenticación de dos factores para garantizar una capa adicional de seguridad en el acceso a sistemas y datos.
- Realizar revisiones regulares de accesos para verificar que solo el personal autorizado tenga permisos adecuados.

7.3.2. Control de Acceso Físico

- Reforzar la seguridad física mediante la implementación de sistemas de alarma y cámaras de vigilancia.
- Establecer procedimientos para el control de acceso a las instalaciones, incluyendo registros detallados de entradas y salidas.
- Realizar auditorías periódicas de seguridad física para garantizar su efectividad.

7.3.3. Cifrado de Datos

- Aplicar cifrado a nivel de archivos y comunicaciones para proteger datos confidenciales almacenados y transmitidos.
- Implementar políticas que definan el uso obligatorio del cifrado para datos sensibles.
- Realizar pruebas regulares para asegurar que el cifrado funcione correctamente y no afecte el rendimiento del sistema.

7.3.4. Copias de Seguridad y Recuperación de Datos

- Establecer un plan de copias de seguridad detallado, especificando la frecuencia, los métodos y los procedimientos de almacenamiento.
- Realizar pruebas periódicas de recuperación de datos para garantizar la disponibilidad y la integridad de la información.
- Documentar claramente los pasos a seguir en caso de pérdida de datos y proporcionar formación al personal.

7.3.5. Gestión de Parches y Actualizaciones

- Establecer un proceso formal para la gestión de parches y actualizaciones, incluyendo la identificación proactiva de vulnerabilidades.
- Definir roles y responsabilidades para la aplicación oportuna de parches críticos.
- Implementar un entorno de pruebas para evaluar el impacto de las actualizaciones antes de su implementación en producción.

7.3.6. Concientización en Seguridad

- Desarrollar programas de capacitación en seguridad de la información, abordando específicamente los riesgos identificados.
- Incorporar módulos de concientización en el manejo seguro de datos y la identificación de amenazas.
- Evaluar regularmente la efectividad de los programas de concientización mediante encuestas y pruebas de conocimiento.

7.3.7. Monitoreo de Seguridad

- Implementar sistemas avanzados de monitoreo de seguridad para la detección temprana de amenazas.
- Definir procedimientos de respuesta a incidentes que se activarán automáticamente en caso de detectarse actividades sospechosas.
- Realizar revisiones periódicas de los registros de seguridad para identificar patrones o anomalías.

7.3.8. Políticas de Seguridad

- Desarrollar políticas de seguridad de la información que aborden específicamente los hallazgos del análisis de riesgos.
- Establecer procedimientos claros para el manejo de contraseñas, acceso a información confidencial y uso de recursos.
- Mantener políticas actualizadas y realizar revisiones periódicas para garantizar su relevancia.

7.3.9. Gestión de Incidentes de Seguridad

- Crear un plan detallado de respuesta a incidentes que defina roles y responsabilidades en situaciones de seguridad inesperadas.
- Establecer un equipo de respuesta a incidentes capacitado y realizar simulacros periódicos.
- Integrar lecciones aprendidas de incidentes anteriores para mejorar continuamente el plan de respuesta.

7.3.10. Auditorías y Evaluaciones de Seguridad

- Realizar auditorías regulares de seguridad internas y externas para evaluar la efectividad de los controles implementados.
- Documentar hallazgos y recomendaciones, y desarrollar planes de acción para abordar áreas de mejora.
- Asegurar que se cumplan los estándares de seguridad y las regulaciones aplicables.

7.3.11. Segregación de Funciones

- Implementar medidas para separar claramente las responsabilidades dentro de la organización y evitar conflictos de interés.
- Definir roles específicos y autorizaciones para cada empleado de acuerdo con sus funciones.
- Realizar auditorías periódicas para verificar el cumplimiento de la segregación de funciones.

7.3.12. Control de Dispositivos Móviles

- Establecer políticas de seguridad específicas para la gestión de dispositivos móviles utilizados por empleados.
- Implementar soluciones de gestión de dispositivos que permitan el monitoreo y control de dispositivos móviles.
- Realizar auditorías regulares de dispositivos móviles para garantizar el cumplimiento de las políticas establecidas.

Estos controles, basados en las mejores prácticas de seguridad de la información, están diseñados para fortalecer la postura de seguridad en cualquier PYME, abordando específicamente los riesgos identificados en el análisis previo. La implementación efectiva de estos controles contribuirá significativamente a la gestión y mitigación de los riesgos asociados a la seguridad de la información en el entorno de la organización.

7.4. PLAN DE TRATAMIENTO DE RIESGOS

Estas medidas, fundamentadas en las más sólidas prácticas de seguridad de la información, han sido concebidas con el propósito de consolidar la seguridad en cualquier PYME, centrándose de manera precisa en los riesgos detectados durante la evaluación previa. La ejecución eficaz de estos controles no solo potenciará la postura de seguridad de la organización, sino que también desempeñará un papel esencial en la gestión y reducción sustancial de los riesgos vinculados a la seguridad de la información en su entorno.

7.4.1. Información Financiera de Clientes

- **Descripción:** Detalles de tarjetas de crédito y cuentas bancarias son activos críticos debido a su sensibilidad. Su exposición podría resultar en consecuencias financieras significativas tanto para los clientes como para la empresa, incluyendo pérdida de ingresos y posibles litigios.

- **Controles de Seguridad Seleccionados:**

    1. Control de Acceso Lógico.

2. Cifrado de Datos.
3. Copias de Seguridad y Recuperación de Datos.
4. Monitoreo de Seguridad.
5. Auditorías y Evaluaciones de Seguridad.

7.4.2. Información Empresarial Confidencial

- **Descripción:** Los contratos, acuerdos de confidencialidad y propiedad intelectual representan elementos fundamentales en las operaciones de cualquier empresa. La revelación no autorizada de esta información conlleva el riesgo de perder ventajas competitivas y relaciones comerciales sólidas.

- **Controles de Seguridad Seleccionados:**

1. Control de Acceso Lógico.
2. Cifrado de Datos.
3. Copias de Seguridad y Recuperación de Datos.
4. Auditorías y Evaluaciones de Seguridad.
5. Gestión de Incidentes de Seguridad.

7.4.3. Datos de Facturación

- **Descripción:** Facturas y estados de cuenta de clientes y proveedores contienen información vital para la gestión financiera. La pérdida de estos datos podría interrumpir las operaciones y relaciones financieras de la empresa.

- **Controles de Seguridad Seleccionados:**

1. Copias de Seguridad y Recuperación de Datos.
2. Gestión de Parches y Actualizaciones.
3. Monitoreo de Seguridad.
4. Auditorías y Evaluaciones de Seguridad.

7.4.4. Datos de Recursos Humanos

- **Descripción:** Información personal de empleados, registros de empleo y nóminas son fundamentales para la gestión de recursos humanos y el cumplimiento normativo. La exposición de estos datos podría resultar en problemas legales y de privacidad.

- **Controles de Seguridad Seleccionados:**

1. Control de Acceso Lógico.
2. Cifrado de Datos.
3. Políticas de Seguridad.

4. Gestión de Incidentes de Seguridad.

7.4.5. Correos Electrónicos y Archivos

- **Descripción:** La correspondencia electrónica y archivos almacenados contienen información interna y externa vital. La pérdida o manipulación de estos datos podría afectar la comunicación interna y externa, impactando así la eficiencia operativa y las relaciones comerciales.

- **Controles de Seguridad Seleccionados:**

    1. Control de Acceso Lógico.
    2. Cifrado de Datos.
    3. Copias de Seguridad y Recuperación de Datos.
    4. Monitoreo de Seguridad.
    5. Auditorías y Evaluaciones de Seguridad.

7.4.6. Información de Proveedores

- **Descripción:** Datos de contacto y detalles de facturación de proveedores son fundamentales para la gestión de relaciones con proveedores. Su pérdida podría afectar la cadena de suministro y la continuidad operativa.

- **Controles de Seguridad Seleccionados:**

    1. Cifrado de Datos.
    2. Gestión de Parches y Actualizaciones.
    3. Auditorías y Evaluaciones de Seguridad.

7.4.7. Información de Socios y Colaboradores

- **Descripción:** Contratos y acuerdos con socios y colaboradores son activos críticos para las alianzas estratégicas. La exposición de estos datos podría afectar las relaciones comerciales a largo plazo y la viabilidad de proyectos conjuntos.

- **Controles de Seguridad Seleccionados:**

    1. Control de Acceso Lógico.
    2. Cifrado de Datos.
    3. Auditorías y Evaluaciones de Seguridad.
    4. Gestión de Incidentes de Seguridad.

7.5. EVALUACIÓN DE COSTOS Y BENEFICIOS

7.5.1. Costos

1. Costos de Implementación Inicial: Estimamos que los costos iniciales oscilarán entre 20,000,000 COP y 50,000,000 COP, considerando la implementación de controles de seguridad, incluyendo hardware y software, así como los servicios de consultoría y expertos en seguridad. La variación en los costos refleja las diferencias en las necesidades y recursos específicos de cada PYME.
2. Costos de Personal y Capacitación: Calculamos costos continuos anuales de 5,000,000 COP a 15,000,000 COP para la formación del personal en buenas prácticas de seguridad. Esta estimación también contempla la posible contratación de personal especializado en seguridad de la información. Los costos variarán según la complejidad y la escala de la organización.
3. Costos de Mantenimiento y Actualización: Los costos de mantenimiento y actualización se estiman en 10,000,000 COP a 20,000,000 COP anualmente, ya que las actualizaciones de sistemas y software son esenciales para mantener un alto nivel de seguridad. Estos costos dependerán de la infraestructura y las necesidades específicas de cada empresa.
4. Costos de Auditorías y Evaluaciones: Las auditorías y evaluaciones regulares se estiman en un rango de 8,000,000 COP a 15,000,000 COP anualmente, teniendo en cuenta los honorarios de auditores y consultores externos. La variación en los costos dependerá de la frecuencia y la complejidad de las auditorías.
5. Costos de Hardware y Software Adicional: Se estima que los costos de hardware y software adicionales pueden variar entre 15,000,000 COP y 30,000,000 COP, dependiendo de las necesidades específicas de actualización y expansión de la infraestructura. Estos costos estarán sujetos a la escala y los requisitos tecnológicos de cada PYME.

7.5.2. Beneficios

1. **Reducción de Riesgos:** Los beneficios de la reducción de riesgos superan los costos. Una violación de seguridad puede resultar en pérdidas financieras significativas y costos legales. La implementación de controles de seguridad puede ayudar a prevenir tales pérdidas.
2. **Mejora de la Reputación:** Mejorar la reputación de la empresa puede atraer nuevos clientes y aumentar los ingresos. La correlación entre una mejor reputación y un aumento de los negocios es ampliamente reconocida en la industria.
3. **Cumplimiento Normativo:** Cumplir con regulaciones de seguridad y normativas puede evitar sanciones legales y multas, lo que se traduce en ahorros de costos sustanciales.

4. **Continuidad Operativa:** La capacidad para mantener las operaciones en caso de incidentes de seguridad puede prevenir la pérdida de ingresos y clientes, lo que justifica la inversión en planes de continuidad operativa.
5. **Eficiencia Operativa:** Si bien los beneficios de eficiencia operativa son difíciles de cuantificar directamente, una operación más eficiente conlleva ahorros en costos operativos a lo largo del tiempo.

7.5.3. Análisis Costo-Beneficio

7.5.3.1. Costos Totales Estimados:

La suma de todos los costos estimados, incluyendo los costos iniciales, costos de personal, costos de mantenimiento, auditorías y otros, se encuentra entre 40,000,000 COP y 110,000,000 COP anualmente.

7.5.3.2. Beneficios Totales Estimados

Los beneficios incluyen la reducción de riesgos, mejora de la reputación, cumplimiento normativo, continuidad operativa y eficiencia operativa. Si bien es difícil cuantificar algunos de estos beneficios directamente, su impacto positivo en la empresa es indiscutible.

7.5.3.3. Relación Costo-Beneficio

Para determinar si la inversión en seguridad de la información es justificable, calculamos la relación costo-beneficio. Esto se logra al comparar los costos totales estimados con los beneficios totales estimados. El cálculo se realiza de la siguiente manera:

- Si los costos totales son significativamente mayores que los beneficios totales, la relación costo-beneficio sería menor a 1, indicando una inversión no favorable.
- Si los costos totales son ligeramente mayores que los beneficios totales, la relación costo-beneficio estaría cerca de 1, lo que indica una inversión en seguridad razonable.
- Si los beneficios totales superan significativamente los costos totaes, la relación costo-beneficio sería mayor a 1, lo que indica una inversión altamente favorable.

En el contexto de una PYME, aunque los costos estimados pueden ser significativos, se espera que los beneficios derivados de una mejora en la seguridad de la información superen estos costos. Esto se debe a la importancia crítica de los activos de información y la necesidad de protegerlos de amenazas. Además, la

inversión en seguridad es esencial para cumplir con regulaciones y mantener la confianza de los clientes.

De esta manera, el análisis costo-beneficio respalda la justificación de invertir en medidas de seguridad de la información en cualquier PYME. La protección de activos críticos y la prevención de amenazas superan los costos asociados con la implementación y el mantenimiento de controles de seguridad.

7.6. PRIORIZACIÓN DE CONTROLES

A pesar de la importancia de implementar controles de seguridad para proteger los activos críticos de cualquier PYME, la realidad de recursos limitados hace imperativa la priorización de estos controles. En esta sección, se abordará la priorización de los controles identificados en la sección 7.3, tomando como base la evaluación de riesgos realizada previamente.

7.6.1. Criterios de Priorización

La priorización de los controles se basará en los siguientes criterios:

1. **Riesgo Total**: Los controles relacionados con los activos críticos que presentan un riesgo total más alto serán priorizados.
2. **Impacto en la Continuidad del Negocio**: Los controles que tienen un impacto significativo en la continuidad del negocio recibirán prioridad.
3. **Costo-Beneficio**: La relación costo-beneficio se tendrá en cuenta. Los controles que proporcionan una mayor reducción de riesgos a un costo razonable serán priorizados.

7.6.2. Lista de Controles Priorizados

A continuación, se presenta la lista de controles priorizados:

7.6.2.1. Control de Acceso Lógico

- **Razón de Priorización**: Este control es esencial para proteger la información confidencial y restringir el acceso no autorizado. Tiene un alto riesgo y un impacto en la continuidad del negocio.
- **Prioridad**: Alta

7.6.2.2. Control de Acceso Físico

- **Razón de Priorización**: Reforzar la seguridad física es fundamental para proteger las instalaciones y los activos de la empresa.
- **Prioridad**: Alta

7.6.2.3. Cifrado de Datos

- **Razón de Priorización**: El cifrado de datos es crucial para proteger la confidencialidad de la información. Tiene un alto impacto en la continuidad del negocio.
- **Prioridad**: Alta

7.6.2.4. Copias de Seguridad y Recuperación de Datos

- **Razón de Priorización**: Garantizar la disponibilidad de datos en caso de desastres es fundamental para la continuidad del negocio.

7.6.2.5. Prioridad: Alta.Gestión de Parches y Actualizaciones

- **Razón de Priorización**: La actualización de sistemas y software es esencial para reducir la exposición a vulnerabilidades conocidas.
- **Prioridad**: Media

7.6.2.6. Concientización en Seguridad

- **Razón de Priorización**: La capacitación y concientización del personal son vitales para promover prácticas seguras.
- **Prioridad**: Media

7.6.2.7. Monitoreo de Seguridad

- **Razón de Priorización**: La detección temprana de amenazas es importante para una respuesta efectiva.
- **Prioridad**: Media

7.6.2.8. Políticas de Seguridad

- **Razón de Priorización**: Establecer políticas claras es esencial para guiar el comportamiento seguro.
- **Prioridad**: Media

7.6.2.9. Auditorías y Evaluaciones de Seguridad

- **Razón de Priorización**: Las auditorías regulares son necesarias para garantizar el cumplimiento de estándares.
- **Prioridad**: Baja

7.6.2.10. Segregación de Funciones

- **Razón de Priorización**: La segregación de funciones ayuda a prevenir conflictos de interés y fraudes.
- **Prioridad**: Baja

7.6.2.11. Control de Dispositivos Móviles

- **Razón de Priorización**: La seguridad de los dispositivos móviles es importante, pero se prioriza en función de otros riesgos más críticos.
- **Prioridad**: Baja

7.6.3. Justificación de Prioridades

Las prioridades asignadas a los controles de seguridad se fundamentan en la evaluación de riesgos realizada, así como en la relevancia de cada control para salvaguardar la seguridad de la información y garantizar la continuidad del negocio. Los controles de alta prioridad se centran en abordar los riesgos más críticos, mientras que aquellos de baja prioridad, aunque aún significativos, se consideran menos críticos en comparación con otros riesgos y los recursos disponibles. Estas prioridades establecidas proporcionarán una guía clara para la implementación efectiva de los controles de seguridad en cualquier PYME, asegurando una asignación eficiente de recursos y una protección adecuada de los activos críticos.

7.7. PLAN DE IMPLEMENTACIÓN

En esta sección, se presenta un plan de implementación que describe las actividades necesarias para llevar a cabo los controles de seguridad priorizados. El plan se organiza en un cronograma basado en semanas para una gestión clara y efectiva de la implementación.

7.6.4. Cronograma de Implementación

Tabla 7. Cronograma de Implementación

Semana	Actividades Planificadas	Responsable	Recursos Requeridos
Semana 1	Definición de roles y responsabilidades para la implementación de controles.	Equipo de Seguridad	-
Semana 2	Implementación del Control de Acceso Lógico.	Equipo de Seguridad	Recursos técnicos, software de autenticación de dos factores
Semana 3	Implementación del Control de Acceso Físico.	Equipo de Seguridad	Sistemas de alarma, cerraduras electrónicas
Semana 4	Inicio de la implementación del Cifrado de Datos.	Equipo de Seguridad	Recursos técnicos para cifrado
Semana 5	Implementación de Copias de Seguridad y Recuperación de Datos.	Equipo de TI	Soluciones de copias de seguridad
Semana 6	Implementación de Gestión de Parches y Actualizaciones.	Equipo de TI	Proceso de actualización
Semana 7	Inicio de programas de Concientización en Seguridad.	Departamento de Recursos Humanos	Materiales de capacitación
Semana 8	Implementación de Monitoreo de Seguridad.	Equipo de Seguridad	Herramientas de monitoreo
Semana 9	Desarrollo y divulgación de Políticas de Seguridad.	Equipo de Seguridad	Documentación de políticas

Semana 10	Implementación de un Plan de Gestión de Incidentes de Seguridad.	Equipo de Seguridad	Procedimientos de respuesta a incidentes
Semana 11	Realización de Auditorías y Evaluaciones de Seguridad.	Equipo de Auditoría	Herramientas de auditoría
Semana 12	Implementación de Segregación de Funciones.	Departamento de Recursos Humanos	Procedimientos de segregación
Semana 13	Inicio de Control de Dispositivos Móviles.	Equipo de Seguridad	Políticas y herramientas de seguridad móvil
Semana 14	Evaluación y revisión de los controles implementados.	Equipo de Seguridad	-

Fuente: Elaboración propia

7.6.5. Justificación del Cronograma

Este cronograma se ha diseñado para llevar a cabo la implementación de los controles de manera efectiva y progresiva. La planificación en semanas permite un seguimiento adecuado y la asignación de recursos necesarios para cada actividad. Las actividades más críticas y de alta prioridad se han programado para las primeras semanas, asegurando una respuesta rápida a los riesgos identificados.

El equipo de seguridad supervisará y coordinará todas las actividades relacionadas con la implementación de controles. Se realizarán evaluaciones regulares para asegurarse de que los controles funcionen según lo previsto y se realizarán ajustes según sea necesario.

7.8. Capacitación y Concientización

En el contexto de cualquier PYME, la capacitación y concientización del personal en seguridad de la información son aspectos fundamentales para asegurar que todos los empleados estén preparados y comprometidos en la implementación de los nuevos controles de seguridad. El plan de capacitación y concientización se llevará a cabo de la siguiente manera:

- **Identificación de Necesidades de Capacitación:** Se realizará una evaluación de las necesidades de capacitación para determinar qué empleados requieren formación específica en seguridad de la información. Esto se basará en las responsabilidades individuales de cada empleado en relación con los controles de seguridad.
- **Desarrollo de Material de Capacitación Personalizado:** Se elaborará material de capacitación personalizado que se adapte a las necesidades y operaciones específicas de la organización. Esto incluirá manuales, presentaciones, videos instructivos y otros recursos que faciliten la comprensión de los controles de seguridad.
- **Programa de Capacitación Continua:** Se implementará un programa de capacitación continua para asegurar que todos los empleados estén al tanto de las últimas actualizaciones y mejores prácticas en seguridad de la información. Esto incluirá capacitación en temas como la gestión de contraseñas, el uso seguro de sistemas y la identificación de amenazas comunes.
- **Concientización y Comunicación:** Se llevará a cabo una campaña de concientización para destacar la importancia de la seguridad de la información y fomentar una cultura de seguridad en toda la organización. Esto se logrará a través de comunicados, carteles, correos electrónicos y charlas informativas.
- **Evaluación de la Efectividad:** Se realizarán evaluaciones periódicas para medir la efectividad de la capacitación y concientización. Esto se logrará a través de pruebas de conocimientos, encuestas de satisfacción del personal y análisis de incidentes de seguridad.
- **Responsabilidades de los Empleados:** Se establecerán claramente las responsabilidades de los empleados en lo que respecta a la seguridad de la información. Cada empleado comprenderá sus funciones y deberes específicos para garantizar el cumplimiento de los controles de seguridad.
- **Seguimiento y Mejora:** El programa de capacitación y concientización se someterá a un seguimiento constante y se mejorará de acuerdo con las necesidades y el feedback de los empleados. Se garantizará que la información de seguridad esté siempre actualizada y sea relevante.

7.9. Seguimiento y Revisión Continua

Se establecerá un proceso de seguimiento y revisión continua para evaluar la efectividad de los controles implementados y realizar ajustes según sea necesario. Este proceso será periódico y continuo.

7.10. Documentación

La documentación desempeña un papel crucial en nuestro plan de tratamiento de riesgos y nuestra estrategia de seguridad de la información. Todos los aspectos del plan de tratamiento de riesgos, incluyendo la documentación detallada de los controles y los resultados de las evaluaciones, se registrarán de manera sistemática. Esto garantiza la transparencia, la trazabilidad y la capacidad de revisión para mejorar continuamente nuestra seguridad de la información.
La documentación incluirá:

- **Evaluaciones de Riesgos**: Se mantendrán registros de todas las evaluaciones de riesgos realizadas, incluyendo la identificación de activos críticos, amenazas, vulnerabilidades y las estimaciones de riesgos asociados.
- **Controles de Seguridad**: Se documentarán todos los controles de seguridad implementados, incluyendo descripciones detalladas, propósitos y responsables.
- **Resultados de Auditorías y Evaluaciones de Seguridad**: Se registrarán los resultados de auditorías internas y evaluaciones de seguridad para garantizar la trazabilidad de los hallazgos y las acciones correctivas tomadas.
- **Incidentes y Respuestas**: Se documentarán los incidentes de seguridad, incluyendo la naturaleza del incidente, las acciones tomadas y las lecciones aprendidas para futuras mejoras.
- **Cambios y Actualizaciones**: Cualquier cambio o actualización en políticas, procedimientos o controles de seguridad se registrará para mantener un historial de cambios y mejorar la gestión de la seguridad de la información.

La documentación se mantendrá de manera organizada y accesible para los miembros pertinentes de la organización y se revisará periódicamente para garantizar su vigencia y precisión. La documentación es una parte fundamental de nuestro enfoque de seguridad de la información, ya que respalda la toma de decisiones informadas y la mejora continua de nuestra estrategia de seguridad.

8. PROPUESTA DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, A PARTIR DE LA GESTIÓN DE RIESGOS, QUE PERMITA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD EN UNA PYME, DE MANERA QUE SE PUEDA MITIGAR O ELIMINAR EL IMPACTO FRENTE A LAS AMENAZAS ENCONTRADAS.

La pyme en la cual se lleve a cabo este estudio. se compromete a proteger la confidencialidad, integridad y disponibilidad de la información crítica. Esta política de seguridad de la información tiene como objetivo establecer un marco para la gestión de riesgos y la implementación de controles de seguridad. La seguridad de la información es esencial para proteger nuestros activos, garantizar la continuidad operativa y cumplir con las regulaciones aplicables.

8.1. IDENTIFICACIÓN DE RIESGOS Y OBJETIVOS DE SEGURIDAD

8.1.1. Identificación de Riesgos

En el análisis de seguridad, se han identificado diversos riesgos y vulnerabilidades que podrían afectar la seguridad de la información. Estos incluyen amenazas internas y externas, falta de políticas de seguridad y vulnerabilidades en la red.

8.1.2. Objetivos de Seguridad

Los objetivos de seguridad son:

- Salvaguardar la información confidencial de la empresa y de los clientes.
- Garantizar la disponibilidad y confiabilidad de los sistemas de información.
- Cumplir con las regulaciones de seguridad de la información aplicables.
- Minimizar el riesgo financiero y legal asociado con posibles brechas de seguridad.

8.1.3. Selección de Controles de Seguridad

Para alcanzar los objetivos de seguridad, se han seleccionado controles de seguridad basados en buenas prácticas reconocidas, como ISO/IEC 27001 y NIST SP 800-53. Algunos de los controles seleccionados son:

- Control de Acceso Lógico.
- Control de Acceso Físico.
- Cifrado de Datos.

- Copias de Seguridad y Recuperación de Datos.
- Gestión de Parches y Actualizaciones.
- Concientización en Seguridad.
- Monitoreo de Seguridad.
- Políticas de Seguridad.
- Gestión de Incidentes de Seguridad.
- Auditorías y Evaluaciones de Seguridad.
- Segregación de Funciones.
- Control de Dispositivos Móviles.

4. Plan de Tratamiento de Riesgos

En esta sección, se presenta el plan de tratamiento de riesgos diseñado para abordar los activos críticos en entornos empresariales. Se describen los controles de seguridad seleccionados para mitigar los riesgos identificados en el análisis previo.

5. Evaluación de Costos y Beneficios

Se ha llevado a cabo un análisis exhaustivo de los costos y beneficios asociados a la implementación de medidas de seguridad de la información en entornos empresariales. Este análisis respalda la inversión en seguridad y proporciona una perspectiva clara de los recursos necesarios en comparación con los beneficios esperados.

6. Priorización de Controles

La priorización de controles se fundamenta en criterios cruciales, como el riesgo total, el impacto en la continuidad del negocio y la relación costo-beneficio. Se han identificado y priorizado los controles más relevantes y efectivos para garantizar una gestión eficiente de los riesgos.

7. Plan de Implementación

Se ha desarrollado un cronograma detallado que describe las actividades necesarias para llevar a cabo los controles de seguridad priorizados. Este plan proporciona una guía paso a paso para la implementación efectiva de las medidas de seguridad, adaptándose a las necesidades específicas de las pequeñas y medianas empresas (PyME).

8. Capacitación y Concientización

Con el objetivo de garantizar que el personal esté debidamente preparado y comprometido en la implementación de controles de seguridad, se ha diseñado un plan integral de capacitación y concientización. Este abarca temas relevantes y se adapta a las operaciones específicas de las PyME, promoviendo una cultura de seguridad.

9. Seguimiento y Revisión Continua

Se ha establecido un proceso continuo de seguimiento y revisión para evaluar la efectividad de los controles implementados. Este enfoque permite realizar ajustes según sea necesario y garantiza la adaptabilidad de las medidas de seguridad en entornos empresariales dinámicos.

10. Documentación

Se destaca la importancia de mantener registros y documentación detallada de todas las actividades relacionadas con la seguridad de la información. Esta práctica garantiza la transparencia y la trazabilidad de las acciones tomadas para fortalecer la seguridad en el ámbito empresarial, facilitando auditorías y evaluaciones.

- **Política de Seguridad de la Información para PYMES**

1. Propósito: El propósito de esta política es establecer un marco para la gestión de riesgos y la implementación de controles de seguridad de la información en la PYME, asegurando la protección de la confidencialidad, integridad y disponibilidad de la información crítica.

2. Alcance: Esta política se aplica a todos los empleados, contratistas y cualquier persona con acceso a los sistemas de información de la PYME.

3. Objetivos de Seguridad:

- Salvaguardar la información confidencial de la empresa y de los clientes.
- Garantizar la disponibilidad y confiabilidad de los sistemas de información.
- Cumplir con las regulaciones de seguridad de la información aplicables.
- Minimizar el riesgo financiero y legal asociado con posibles brechas de seguridad.

4. Identificación y Gestión de Riesgos:

- Realizar evaluaciones periódicas de riesgos para identificar amenazas y vulnerabilidades.
- Implementar controles de seguridad adecuados para mitigar los riesgos identificados.
- Mantener un registro actualizado de los riesgos y controles implementados.

5. Controles de Seguridad:

- **Control de Acceso Lógico:** Implementar mecanismos de autenticación y autorización para asegurar que solo el personal autorizado acceda a los sistemas y datos.
- **Control de Acceso Físico:** Restringir el acceso físico a las instalaciones donde se almacenan o procesan datos sensibles.
- **Cifrado de Datos:** Utilizar técnicas de cifrado para proteger la información sensible tanto en tránsito como en reposo.
- **Copias de Seguridad y Recuperación de Datos:** Realizar copias de seguridad regulares y asegurarse de que los datos puedan ser recuperados en caso de pérdida.
- **Gestión de Parches y Actualizaciones:** Aplicar parches y actualizaciones de software de manera oportuna para corregir vulnerabilidades.
- **Concientización en Seguridad:** Capacitar a todos los empleados sobre las mejores prácticas de seguridad y cómo reconocer y responder a posibles amenazas.
- **Monitoreo de Seguridad:** Implementar sistemas de monitoreo continuo para detectar y responder a incidentes de seguridad.
- **Gestión de Incidentes de Seguridad:** Establecer procedimientos para la detección, respuesta y recuperación de incidentes de seguridad.
- **Auditorías y Evaluaciones de Seguridad:** Realizar auditorías periódicas para evaluar la efectividad de los controles de seguridad y realizar mejoras continuas.
- **Segregación de Funciones:** Asegurar que las funciones críticas estén segregadas para reducir el riesgo de errores o actividades maliciosas.
- **Control de Dispositivos Móviles:** Implementar políticas y controles para gestionar y proteger los dispositivos móviles utilizados para acceder a los datos de la empresa.

6. Responsabilidades:

- **Directores y Gerentes:** Asegurar la implementación y el cumplimiento de esta política.
- **Empleados:** Adherirse a las políticas y procedimientos de seguridad de la información.
- **Equipo de Seguridad:** Supervisar y coordinar todas las actividades relacionadas con la seguridad de la información.

7. Capacitación y Concientización:

- Identificar las necesidades de capacitación y proporcionar formación continua a todos los empleados.
- Realizar campañas de concientización para fomentar una cultura de seguridad en la organización.
- Evaluar la efectividad de los programas de capacitación mediante pruebas y encuestas.

8. Seguimiento y Revisión Continua:

- Monitorear continuamente la efectividad de los controles de seguridad implementados.
- Revisar y actualizar la política de seguridad de la información al menos una vez al año o cuando se produzcan cambios significativos en el entorno de amenazas.

9. Documentación:

- Mantener registros detallados de todas las evaluaciones de riesgos, controles de seguridad, auditorías, incidentes y respuestas.
- Asegurar que la documentación esté organizada y accesible para todos los miembros pertinentes de la organización.

Esta propuesta de política de seguridad de la información es un marco general que debe adaptarse a las necesidades específicas y características particulares de cada PyME. La implementación efectiva de esta política depende de una evaluación continua y de ajustes basados en las amenazas y vulnerabilidades identificadas.

9. CONCLUSIONES

Durante la ejecución del estudio, se diseñó la etapa de planificación de un sistema de gestión de seguridad de la información para PYMES utilizando la metodología OCTAVE. Este proceso permitió identificar coincidencias en los factores de vulnerabilidad más comunes, proporcionando una base sólida para abordar amenazas y prevenir posibles impactos en las infraestructuras TI de las PYMES en general.

A lo largo del trabajo, se realizó un análisis exhaustivo de las condiciones de los sistemas de seguridad de la información en PYMES, identificando los factores generadores de vulnerabilidad a través de fuentes bibliográficas. Este análisis proporciona una comprensión profunda de los desafíos y áreas de mejora específicas para estas empresas, destacando la importancia de una gestión de riesgos bien estructurada.

La aplicación exitosa de la metodología OCTAVE en un contexto general de PYME permitió la identificación precisa de activos de información críticos, contribuyendo a la formulación de estrategias de mitigación y prevención. Este enfoque es esencial para fortalecer la resiliencia ante amenazas y garantizar la continuidad del negocio en diversas situaciones empresariales.

El desarrollo de un plan de tratamiento de riesgos, basado en buenas prácticas, proporciona una guía práctica para la implementación de controles de seguridad en PYMES. Esta acción es fundamental para gestionar y mitigar riesgos, contribuyendo a la protección efectiva de la información y la infraestructura empresarial.

La propuesta de una política de seguridad de la información, derivada de la gestión de riesgos, destaca como una medida clave para la implementación de controles de seguridad en PYMES. Esta medida busca no solo mitigar riesgos, sino también establecer un marco estructurado para la seguridad de la información en estas organizaciones, asegurando así una protección integral y sostenible.

10. RECOMENDACIONES

1. **Reforzar la Concientización**

- **Capacitación Continua:** Desarrollar programas continuos de capacitación para el personal, asegurando una comprensión profunda de los riesgos y la importancia de los controles de seguridad.

- **Campañas de Concientización:** Implementar campañas de concientización regulares que utilicen diversos medios (charlas, correos electrónicos, materiales visuales) para mantener a los empleados informados sobre las mejores prácticas de seguridad.

2. **Integrar la Gestión de Riesgos en la Cultura Empresarial**

- **Mentalidad Proactiva:** Fomentar una mentalidad proactiva hacia la seguridad de la información, involucrando a todos los niveles de la organización en la identificación y mitigación de riesgos.

- **Responsabilidad Compartida:** Establecer políticas claras donde se detalle que la seguridad de la información es responsabilidad de todos los empleados, no solo del departamento de TI.

3. **Actualización Periódica de la Política**

- **Revisión Regular:** Establecer un proceso de revisión y actualización periódica de la política de seguridad de la información, asegurando su relevancia continua y eficacia ante las amenazas emergentes.

- **Adaptabilidad:** Garantizar que la política sea dinámica y se adapte rápidamente a los cambios en el entorno empresarial y tecnológico.

4. **Colaboración Externa**

- **Asesoramiento Especializado:** Considerar la posibilidad de buscar asesoramiento externo especializado en seguridad de la información. La colaboración con expertos puede proporcionar conocimientos adicionales y garantizar que las PYMES implementen las mejores prácticas de seguridad, incluso cuando los recursos internos son limitados.

- **Auditorías Externas:** Realizar auditorías de seguridad periódicas con expertos externos para identificar y corregir vulnerabilidades que podrían pasar desapercibidas internamente.

5. **Implementación de Tecnología de Seguridad Avanzada**

- **Herramientas de Seguridad:** Adoptar herramientas avanzadas de seguridad como sistemas de prevención de intrusiones, firewalls de última generación y software de gestión de identidades y accesos.
- **Cifrado de Datos:** Implementar soluciones de cifrado para proteger la información crítica tanto en tránsito como en reposo.

6. **Monitoreo y Respuesta a Incidentes**

- **Centro de Operaciones de Seguridad (SOC):** Considerar la implementación de un SOC interno o externo que supervise continuamente las actividades de la red y responda rápidamente a incidentes de seguridad.
- **Planes de Respuesta a Incidentes:** Desarrollar y mantener planes de respuesta a incidentes detallados que incluyan procedimientos específicos para diversas situaciones de seguridad.

Estas recomendaciones están diseñadas para proporcionar un enfoque integral a la gestión de la seguridad de la información en PYMES, asegurando que puedan enfrentar y mitigar eficazmente los riesgos asociados con las amenazas modernas.

11. BIBLIOGRAFÍA

ACOSTA, David. *Estándares de Configuración Segura Hardening en PCI.* [En línea]. Consultado el 25 de marzo de 2023. Disponible en: http://www.pcihispano.com/estandares-de-configuracion-segura-hardening-enpci-dss

AREITIO, Javier. *Seguridad de la información: redes, informática y sistemas de información.* Madrid, España: Editorial Paraninfo, 2008.

ÁLVAREZ, D. y Ortiz, J. *Seguridad de la información en las PYMES: estudio de caso en Colombia.* Revista Ingeniería Industrial, (2019). 19(1), 26-35.

BALANTA, Heidi. *Legislación que Protege la Información en Colombia.* [En línea], junio de 2014.

BELLO, Claudia. *Manual de Seguridad en Redes.* [En línea]. Consultado el 18 de marzo de 2023. Disponible en: https://es.slideshare.net/csandovalrivera/manual-de-seguridad-en-redes

Business School. *Seguridad de la Información: un conocimiento imprescindible.* (2018). Consultado el 29 de marzo de 2023. Disponible en: https://www.obsedu.com/int/blog-investigacion/sistemas/seguridad-de-la-informacion-unconocimientoimprescindible?fbclid=IwAR2HbEnVWeXgBf5lGPHOxc4kAzgmP2FNo6P_cNP6CSffvxaeTq9GlNo2hxA

CAMARGO, L. A. *En primer trimestre de 2021 aumentó 9,3% la creación de empresas en Colombia.* Confecámaras, (2021). Disponible en: https://www.confecamaras.org.co/noticias/785-enprimer-trimestre-de-2021-aumento-9-3-la-creacion-de-empresas-en-colombia

CARPENTIER, Jean-François. *La seguridad informática en la PYME: Situación actual y mejores prácticas.* Ediciones ENI, 2017. Disponible en: https://books.google.es

Congreso de la República de Colombia. *Ley 1273 de 2009.* Diario Oficial No. 47.420, de 5 de enero de 2009.

Cruz, L. F. *Evaluación de la madurez de la gestión de la seguridad de la información en PYMES.* Revista de Investigación Académica, (2017). 17, 1-10.

DEMARTINI, M. V. N., y Ríos, M. J. *El impacto generado por la seguridad informática en las PYMES de Mendoza.* (Doctoral dissertation, Universidad Nacional de Cuyo. Facultad de Ciencias Económicas, 2019). Disponible en: http://ddhh.bdigital.uncu.edu.ar/objetos_digitales/14309/riosdemartinifce.pdf

Dr. RODRÍGUEZ MEDINA. *Análisis Difuso en modo de falla (2012).* Consultado el 1 de abril de 2023. Disponible en: https://www.researchgate.net/publication/283277027_Analisis_difuso_del_modo_de_falla

ELISSONDO, L. *Auditoria y Seguridad de Sistemas de Información.* (2008). Disponible en: http://econ.unicen.edu.ar/monitorit/index.php?option=com_docman&task=doc_downloaGDPSJLGDPS,WHP

ERAZO, S. C. R., CASTRO, A. A., y Avila-Fajardo, G. P. *Seguridad de los sistemas de información en las PYMES de Santiago de Cali (Colombia).* Libre Empresa, (2019). 11(1), 107-118.

Federación de Aseguradores Colombianos. *Seguridad y Salud en el trabajo: Una mirada desde la pequeña y mediana empresa.* (2018). Consultado el 22 de marzo de 2023. Disponible en: https://www.ins.gov.co/seguridadysalud/docs/Memorias/9.pdf

FERNÁNDEZ, Z., y Revilla, A. *Hacer de la necesidad virtud: los recursos de las pymes.* Economía industrial, (2010) 375, 53-64.
ISOtools. *La familia de normas ISO 27000.* (09 de mayo de 2021). Recuperado de: https://www.isotools.org/2015/01/21/familia-normas-iso-27000/

ROJAS I., Antonio, y Erika Lizet Macha Moreno. *Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del Perú, 2016.* (2017). Disponible en: https://repositorio.usil.edu.pe/items/9449a061-bfd2-4ecc-8cf1-770fba7cee45/full

KASPERSKY. *Encuesta de Seguridad de la Información en Colombia 2021.* (2021). Recuperado de https://latam.kaspersky.com/about/press-releases/2021_encuesta-seguridad-informacion-colombia/

C., & R. *Sistema para el Análisis y Gestión de Riesgos de Seguridad Informática en la Facultad 4.* (Bachelor's thesis, Universidad de las Ciencias Informáticas. Facultad 4, 2015).

LIVIA, J., MERINO-SOTO, C., y Livia-Ortiz, R. *Producción científica en la base de datos Scopus de una universidad privada del Perú.* Revista Digital de Investigación en Docencia Universitaria, (2022). 16(1).

LÓPEZ, M. A. *Análisis de riesgos y seguridad de la información en las PYMES: un enfoque metodológico.* Revista de Investigación Académica, (2016). 13, 1-12.

MATALOBOS Veiga, J. M. *Análisis de riesgos de seguridad de la información.* (2009).

MILENKOVIC, Milan. *Sistemas operativos: Conceptos y Diseño, 2ª Edición.* McGraw (1994). Disponible en: https://dspace.scz.ucb.edu.bo/dspace/bitstream/123456789/1729/1/410.pdf

MARTÍNEZ, Cristian Fernando; ROTAVISTA MERCADO, Adriana; VANEGAS, Jessica Fabiola. *Análisis de las afectaciones generadas en las PYMES en Colombia producto de la emergencia sanitaria COVID 19.* (2022).
Ministerio de Trabajo. *Decreto 1072 de 2015.* Por medio del cual se expide el Decreto Único Reglamentario del Sector Trabajo. Bogotá, D.C., (2009). Consultado el 20 de marzo. Disponible en: https://www.mintrabajo.gov.co/documents/20147/0/DUR+Sector+Trabajo+Actualizado+a+15+d%20e+abril++de+2016.pdf/a32b1dcf-7a4e-8a37-ac16-c121928719c8

MONCAYO RACINES, Diana Elizabeth. *Modelo de evaluación de riesgos en activos de TIC'S para pequeñas y medianas empresas del sector automotriz.* (2014). Tesis de Maestría. Quito, 2014.

MOYANO y L.; SUAREZ, Y. *Plan de Implementación de SGSI basado en la norma ISO: 27001 :2013 para la empresa de interfaces y soluciones.* (Optar El Titulo De Ingenieria 89 En Telematica), Universidad Distrital Francisco Jose De Caldas, Bogota, D.C., (2017). Recuperado de: http://repository.udistrital.edu.co/bitstream/11349/6737/1/MoyanoOrjuelaLuzAdriana

MUÑOZ Holguín y David y Cuadros Mejía Alejandra. *Comparación de metodologías para la gestión de riesgos en los proyectos de las Pymes.* Revista Ciencias Estratégicas [en línea]. 2017, 25(38), 319-338[fecha de Consulta 31 de marzo de 2023]. ISSN: 1794-8347. Disponible en: https://www.redalyc.org/articulo.oa?id=151354939004

Organización Internacional de Normalización. *Organismos Nacionales de Normalización en Países en Desarrollo.* Consultado el 20 de marzo de 2023. Recuperado de: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/fast_forward-es.pd

Organización Internacional del Trabajo para Países Andinos. *Impacto de la COVID-19 en las Mipymes colombianas,* (2020) 1-87 p. Disponible en: https://www.ilo.org/wcmsp5/groups/public/lima/documents/publication/wcms_774974.pdf

Organización Internacional de Normalización. *Origen ISO 27001-2013.* Consultado el 1 de abril de 2023. Disponible en: http://www.iso27000.es/iso27000.html#section3a

OSORIO Montoya & A. *Gestión de riesgo y seguridad en computación en la nube para pymes.* (2018). http://repository.unipiloto.edu.co/handle/20.500.12277/8614 PYME. Consultado el 20 de marzo de 2023. PYMES. Disponible en: https://pymes.afip.gob.ar/estiloAFIP/PYMES/default.asp

Red de Cámaras de Comercio. *En primer trimestre de 2021 aumentó 9,3% la creación de empresas en Colombia.* (2021). Consultado el 25 de marzo de 2023. Disponible en: https://www.confecamaras.org.co/noticias/786-en-primertrimestre-de-2021-aumento-9-3-la-creacion-de-empresas-en-colombia

RODRÍGUEZ, M. *Ciberseguridad en PYMES de Colombia.* Revista Tecnológica-Empresarial, (2018). 11(1), 1-8.

SÁNCHEZ-SÁNCHEZ, P. A., García-González, J. R., Triana, A., & Perez-Coronell, L. *Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia.* Información tecnológica, (2021). 32(5), 121-128.

SIVARAMAN, V., & NADARAJAN, R. *Fuzzy FMEA for SMEs: An Information Security Management System Implementation Perspective.* Journal of Information Security, (2016). 7(1), 12-24.

SILVA, Maisa, Henriques. Paula, Poleto. Thiago, Camara Lucio, Cabral Ana. (2014) *Multidimensional approach to information security risk management using FMEA and fuzzy theory.* Articulo A.

SOLARTE, F. N. S., Rosero, E. R. E., & del Carmen Benavides, M. (2015). *Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001.* Revista Tecnológica-ESPOL, 28(5). Disponible en: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

QUINTERO, L. A., Arias, W. L., & Vargas, J. E. (2019). *Ciberseguridad en PYMES: una revisión sistemática de la literatura.* Revista Tecnología en Marcha, 32(2), 23-36.

QUINCHO, M. *Diseño De Un Sistema De Gestión De Seguridad De La información Bajo La Ntp Iso/Iec 27001:2014 Para La Municipalidad Provincial De Huamanga, 2016.* (Para optar el título profesional de Ingeniero Informático), Universidad Nacional De San Cristóbal De Huamanga, Ayacucho. (2017). Obtenido de http://repositorio.unsch.edu.pe/bitstream/handle/UNSCH/1751/TESIS%20SIS48_Cce.pdf?sequence=1&isAllowed=y

12. ANEXOS

Enlace Video de Sustentación:

https://drive.google.com/drive/folders/1pTuY4t1mLuz6lLsgVIBuewXrZaT0nMFj?usp=sharing