DESARROLLO DE MODELO DE GESTION DE RIESGOS PARA LA IMPLEMENTACION DE CONTROLES DE SEGURIDAD PERIMETRAL EN MEDIANAS Y PEQUEÑAS EMPRESAS DEL SECTOR DE T.I.

ARIZA SUAZA JHON HAROLD
RINCÓN LÓPEZ JULIÁN ANDRÉS

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS
FACULTAD TECNOLÓGICA
INGENIERÍA TELEMÁTICA
BOGOTÁ D.C
2025

DESARROLLO DE MODELO DE GESTION DE RIESGOS PARA LA IMPLEMENTACION DE CONTROLES DE SEGURIDAD PERIMETRAL EN MEDIANAS Y PEQUEÑAS EMPRESAS DEL SECTOR DE T.I.

ARIZA SUAZA JHON HAROLD
RINCÓN LÓPEZ JULIÁN ANDRÉS

TRABAJO DE GRADO PRESENTADO COMO REQUISITO PARA OPTAR AL TÍTULO DE:
INGENIERO TELEMÁTICO

TUTOR
Ingeniera Sonia Pinzón

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS
FACULTAD TECNOLÓGICA
INGENIERÍA TELEMÁTICA
BOGOTÁ D.C
2025

Nota de Aceptación

_____

_____

_____

_____

Ing. Sonia Pinzón
Tutor proyecto

_____

Ing. Miguel Ángel Leguizamón
Jurado

Bogotá, 25 de marzo de 2025.

A nuestros padres, el apoyo más importante de nuestras vidas, gracias a ellos hoy podemos hacer este sueño realidad.

AGRADECIMIENTOS

A nuestros padres, quienes fueron el motor principal y gracias a ellos pudimos hacer este sueño realidad.

A nuestros amigos quienes siempre extendieron su apoyo incondicional.

Especiales agradecimientos a la Ingeniera Sonia Pinzón y al Ingeniero Miguel Ángel Leguizamón, quienes fueron pilares fundamentales en el desarrollo de este proyecto, gracias por sus conocimientos, dedicación y paciencia, siempre estarán presentes en nuestra memoria.

A nuestros maestros por todo su conocimiento y dedicación.

CONTENIDO

Para que esta tabla de contenido se actualice automáticamente se deben usar los estilos Titulo 1, Titulo 2 y Titulo 3. Posteriormente haz click sobre la tabla y selecciona actualizar tabla.

Pág.

LISTA DE TABLAS

LISTA DE GRÁFICAS

LISTA DE FIGURAS

Pág

LISTA DE ANEXOS

GLOSARIO

PRIMERA PALABRA: escribe aquí la definición de la primera palabra ordenada por orden alfabético de forma similar a un diccionario.

SEGUNDA PALABRA: escribe aquí la definición de la segunda palabra ordenada por orden alfabético de forma similar a un diccionario.

TERCERA PALABRA: escribe aquí la definición de la tercera palabra ordenada por orden alfabético de forma similar a un diccionario.

RESUMEN

Las pequeñas y medianas empresas (PYMEs) del sector de tecnología de la información (T.I.) enfrentan crecientes desafíos en ciberseguridad debido a la evolución de las amenazas y la falta de estrategias estructuradas para la gestión de riesgos. Este trabajo propone un modelo de gestión de riesgos basado en la norma ISO 27001, con el objetivo de fortalecer la seguridad perimetral y mitigar vulnerabilidades en estas organizaciones.

El modelo se desarrolla utilizando el Ciclo Deming (PDCA: Plan, Do, Check, Act), permitiendo una gestión eficiente y continua de los riesgos. En la fase de planificación (Plan), se identifican activos críticos, amenazas y vulnerabilidades. La fase de implementación (Do) define controles de seguridad alineados con ISO 27001. Posteriormente, en la fase de verificación (Check), se establecen métricas de desempeño, y en la fase de mejora (Act), se optimizan los controles en función de nuevas amenazas.

La metodología aplicada incluye el análisis de normativas, el diseño teórico del modelo y su evaluación en términos técnicos, operativos y económicos. Los resultados indican que la adopción de un modelo estructurado mejora la capacidad de las PYMEs para prevenir y responder a incidentes de seguridad, garantizando el cumplimiento de estándares internacionales.

Como conclusión, el estudio resalta la importancia de implementar modelos de gestión de riesgos en las PYMEs del sector T.I., promoviendo una cultura de ciberseguridad.

PALABRAS CLAVE: Gestión de riesgos, ISO 27001, seguridad perimetral, PYMEs, ciberseguridad, PDCA.

1. INTRODUCCIÓN

El avance tecnológico de la sociedad se ha visto en un crecimiento exponencial desde el año 2000, dando así un crecimiento en la tecnología y en los conocimientos generados a partir de estos avances, en las organizaciones y centros educativos. Al generar conocimiento, los datos alojados por cada una se convierten en un activo, el cual debe ser protegido, preservado y conservado frente a las diferentes situaciones.

Con el crecimiento de las organizaciones, conforme su éxito y su acogida motivan su crecimiento, empieza a proponer grandes retos en los diferentes ámbitos tecnológicos de las mismas, como la necesidad de ampliar ámbitos como: la capacidad de procesamiento, la capacidad a nivel de infraestructura física, la capacidad de la red de la organización, entre otras.

Sin embargo, estas empresas conforme su éxito aumenta muchas veces, descuidan ámbitos tan importantes como el de la seguridad, volviéndose un blanco fácil y potencial para los hackers, esto sucede a nivel mundial según análisis realizados por empresas de antivirus tales como Panda Security, las medianas y pequeñas empresas poseen una probabilidad mayor de ser infectadas mediante un software malicioso o malware. Según este fabricante el 43% de los ataques en el mundo van orientados hacia empresas pymes. Esto, sumado a la baja implementación de controles por parte de las pymes orientados al ámbito de seguridad informática arroja que el 60% no se recupera tras un ataque cibernético.

Estos problemas se confirman según análisis de amenazas detectadas por otros fabricantes de soluciones tecnológicas tal como Cisco, Google, entre otros. Así como firmas de estudio las cuales indican que por un lado alrededor de un 87% de las pymes en un país ejemplo como muestra España, cuenta con algún sistema de seguridad para móviles, y el solo 33% cuenta con un DRP (Disaster Recovery Plan) definido.[1]

A esto también se le puede sumar el aumento significativo de un 72% aproximado en ataques cibernéticos con respecto al año anterior antes de inicios de pandemia, esto según lo expuesto por firmas como Kaspersky[2] y Exsel una compañía de seguros española, dando así un aproximado de 89 ciberataques por minuto.[3]

Es por esto que se empiezan a desarrollar diferentes normas, estándares, procedimientos y controles con el fin de que estos nuevos retos sean simplemente una necesidad para la organización y se puedan solucionar sin mayor problema. Uno de ellos, es el caso de la protección de la información, en el cual el objetivo es que esta solo sea accedida y manipulada por el personal autorizado para tales fines.

---

[1] Las principales amenazas de ciberseguridad para las pequeñas empresas (PYMES) - Kenneth Daniels https://www.widefense.com/recursos/ciberseguridad/pequenas-empresas/ (22/07/2021).

[2] Los ataques informáticos a pymes crecen en el Ecuador - Lizette Abril https://www.elcomercio.com/tendencias/tecnologia/ataques-informaticos-pymes-crecen-ecuador.html (03/09/2021).

[3] Los errores humanos son la causa de la mayoría de ciberataques en pymes - https://cincodias.elpais.com/cincodias/2021/08/07/pyme/1628335909_005029.html (09/082021).

2. OBJETIVOS

2.1 Objetivo general

Plantear un modelo de gestión de riesgos en medianas y pequeñas empresas del sector T.I basado en la norma ISO 27001

2.2 Objetivos específicos

• Identificar las vulnerabilidades de información a partir de los estándares ISO 27001 que se pueden presentar en las pequeñas y medianas empresas del sector T.I.
• Generar el modelo de seguridad que permita controlar las vulnerabilidades y amenazas que se presenten en las pequeñas y medianas empresas del sector T.I.
• Realizar un listado de recomendaciones sobre las posibles herramientas que contribuyan al establecimiento de controles de seguridad.
• Proponer un plan de acción para mitigar los riesgos que se pueden presentar según la norma ISO 27001.
• Desarrollar una página web de ejemplo en donde se plasme el modelo, las recomendaciones y el plan de acción generado a lo largo del proyecto.

3 PLANTEAMIENTO DEL PROBLEMA

3.1 Definición del problema

El crecimiento tecnológico y el avance exponencial de la sociedad desde el año 2000 han llevado a las organizaciones a generar un vasto conocimiento y acumular grandes cantidades de datos. Este crecimiento también implica la necesidad de aumentar la capacidad de procesamiento, infraestructura física y capacidad de red para las organizaciones. Sin embargo, el aumento en el tamaño y la actividad de estas empresas a menudo resulta en un descuido de la seguridad, lo que las convierte en objetivos fáciles para los hackers y ciberdelincuentes.

El principal problema es el riesgo creciente de ataques cibernéticos hacia empresas de todos los tamaños, especialmente pequeñas y medianas empresas (pymes), que presentan mayores vulnerabilidades debido a la falta de medidas de seguridad adecuadas. Según datos de diversas empresas de seguridad informática, el 43% de los ataques a nivel mundial están dirigidos a pymes, y el 60% de estas empresas no se recupera tras un ataque cibernético. Además, solo el 33% de estas empresas cuenta con un plan de recuperación de desastres (DRP), mientras que el aumento de ataques cibernéticos ha alcanzado un 72% en comparación con el año anterior a la pandemia.[4]

Las consecuencias de estos problemas de seguridad incluyen la exposición de datos sensibles, la pérdida de reputación y la interrupción del negocio. Las empresas que no logran proteger sus datos corren el riesgo de sufrir pérdidas económicas significativas, litigios y daño a su imagen. El aumento significativo de ataques cibernéticos, como se refleja en informes de firmas de seguridad y seguros, con un promedio de 89 ciberataques por minuto, resalta la urgencia de abordar estas amenazas. A raíz de esta situación, se han desarrollado normas y estándares para reforzar la seguridad de la información y la infraestructura tecnológica de las empresas, siendo uno de los más destacados la familia de normas ISO 27001.

3.2 Formulación del problema

¿Cómo mejorar la gestión y protección de la información en las pequeñas y medianas empresas del sector T.I. considerando la evaluación y control de riesgos asociados con la seguridad de la información?

[4] Foro Económico Mundial. (2024). Las PYMEs pueden convertir el riesgo de ciberseguridad en una oportunidad: cómo hacerlo. Recuperado de https://es.weforum.org/stories/2024/08/las-pymes-pueden-convertir-el-riesgo-de-ciberseguridad-en-una-oportunidad-como-hacerlo/

3.3 Justificación

El creciente número de ataques cibernéticos contra pequeñas y medianas empresas (PYMEs) demuestra la urgente necesidad de establecer mecanismos efectivos de gestión de riesgos en seguridad de la información. A pesar del avance tecnológico y la acumulación de datos, muchas empresas no cuentan con estrategias de protección adecuadas, lo que las expone a vulnerabilidades críticas y potenciales pérdidas económicas, reputacionales y operativas.

La implementación de un modelo de gestión de riesgos basado en la norma ISO 27001 permite a las PYMEs adoptar un enfoque estructurado para identificar amenazas, evaluar vulnerabilidades y establecer controles efectivos. La aplicación del Ciclo Deming (PDCA) en este modelo facilitará la mejora continua de la seguridad, garantizando que las empresas puedan prevenir, detectar y responder de manera eficaz ante incidentes cibernéticos.

Este trabajo es relevante porque no solo contribuye a reducir la brecha de seguridad en las PYMEs, sino que también fortalece la resiliencia organizacional, asegurando la continuidad del negocio. Además, proporciona una propuesta viable y escalable que puede ser aplicada en múltiples sectores del ámbito tecnológico, alineándose con estándares internacionales y mejores prácticas de seguridad de la información.

Por lo tanto, el desarrollo de un modelo de gestión de riesgos estructurado y adaptable es fundamental para ayudar a las PYMEs a minimizar el impacto de las amenazas cibernéticas y fomentar una cultura de ciberseguridad, protegiendo tanto su infraestructura tecnológica como su información crítica.

4. MARCO DE REFERENCIA

4.1 Marco teórico

La gestión de riesgos y la seguridad de la información se han convertido en áreas críticas de enfoque para las empresas de todos los tamaños, especialmente en el sector de las tecnologías de la información (T.I.), donde la integridad y la protección de los datos son fundamentales. En un contexto digital que avanza rápidamente, las organizaciones deben ser conscientes de que los activos de información, como datos personales, propiedad intelectual y registros financieros, constituyen activos clave para su funcionamiento. Estos activos están constantemente expuestos a amenazas cibernéticas que, si no son gestionadas adecuadamente, pueden comprometer el funcionamiento y la reputación de la organización. La seguridad de la información, en este sentido, no solo es una medida técnica, sino una necesidad estratégica que involucra la cultura organizacional, la estructura operativa y las políticas internas de la empresa.

Para las pequeñas y medianas empresas (PYMES), que a menudo enfrentan limitaciones de recursos y conocimientos especializados, el desarrollo de un modelo eficaz de gestión de riesgos para implementar controles de seguridad perimetral es no solo una necesidad, sino un imperativo estratégico. Dado que muchas de estas organizaciones no cuentan con grandes presupuestos ni con equipos dedicados exclusivamente a la ciberseguridad, deben implementar soluciones escalables y adaptadas a su tamaño y capacidades. Este trabajo se propone plantear un modelo adaptado a las necesidades y capacidades específicas de las PYMES en el sector T.I., abordando tanto los desafíos como las soluciones potenciales que pueden ayudar a mitigar los riesgos de seguridad a los que están expuestas estas organizaciones.

A continuación, se abordan varias áreas clave, comenzando con una revisión de los conceptos fundamentales de la gestión de riesgos y la seguridad perimetral. Se explorarán modelos y marcos de gestión de riesgos reconocidos internacionalmente, como los propuestos por la norma ISO/IEC 27001, que proporcionan directrices para la implementación de medidas de seguridad. También se identificarán las mejores prácticas que puedan ser aplicadas en el contexto de las PYMES. Además, se discutirán las tecnologías específicas de seguridad perimetral, tales como firewalls y sistemas de detección y prevención de intrusiones (IDS/IPS), que son esenciales para la protección de los activos de información en este tipo de organizaciones. La seguridad perimetral juega un rol crucial al proporcionar una primera línea de defensa contra ciberataques que intentan penetrar las redes internas de la empresa.

4.1.1. Seguridad de la Información.

La seguridad de la información es un campo que abarca las políticas, los controles y las tecnologías para proteger los activos de información de una organización, asegurando su confidencialidad, integridad y disponibilidad (ISO/IEC 27001:2013) (International Organization for Standardization, 2013). Esta definición refleja la base de los principios sobre los cuales se construye un sistema robusto de gestión de la seguridad de la información. La confidencialidad garantiza que solo las personas autorizadas puedan acceder a la información. La integridad asegura que los datos sean precisos y completos, sin alteraciones no autorizadas. Finalmente, la disponibilidad permite que la información esté accesible cuando se necesite.

Es fundamental en todas las organizaciones debido a la creciente amenaza de ciberataques y la alta dependencia de la información como activo crítico. La información se ha convertido en un activo estratégico en todos los sectores, desde la banca hasta la salud y la educación, por lo que cualquier pérdida, daño o robo de datos puede tener repercusiones graves para una organización. Las empresas del sector TI, al ser las responsables del desarrollo y gestión de las infraestructuras tecnológicas, están particularmente expuestas a estas amenazas.

El Sistema de Gestión de Seguridad de la Información (SGSI) se encarga de gestionar la seguridad de los datos mediante un marco estructurado que permite identificar y abordar los riesgos relacionados con la información (Samboni, 2018; Prieto y Guarnizo, 2016; Villamil y Miranda, 2017). La implementación de un SGSI no solo protege los datos, sino que también favorece la mejora continua de los procesos de seguridad, al permitir la evaluación constante de amenazas, vulnerabilidades y controles. La adopción de este sistema se facilita mediante el cumplimiento de normas internacionales como la ISO 27001, que ofrece un proceso sistemático y completo para gestionar la seguridad de la información de manera efectiva y eficiente.

4.1.2. Gestión de Riesgos en Seguridad de la información.

El análisis de riesgos es un componente central del SGSI, que permite identificar, evaluar y gestionar las amenazas y vulnerabilidades que afectan a los activos de información. Según la norma ISO/IEC 27005, los riesgos se gestionan a través de un proceso sistemático y documentado que evalúa el impacto de las amenazas y la probabilidad de su ocurrencia (Tapiero & Suárez, 2017; Prieto & Guarnizo, 2016). Este proceso es esencial para priorizar los riesgos según su nivel de severidad y su probabilidad de materialización, permitiendo que las organizaciones implementen medidas de seguridad apropiadas y efectivas.

En este proceso, se identifican activos como datos, hardware, software y redes, los cuales deben ser protegidos contra riesgos como intrusiones no autorizadas, modificación de datos

y fallas del sistema. Además, la evaluación de riesgos también permite a las organizaciones identificar las vulnerabilidades en sus sistemas y redes, y determinar las amenazas que podrían aprovechar estas debilidades. La gestión efectiva de estos riesgos implica la implementación de controles para reducir la exposición a las amenazas y mitigar los impactos potenciales.

4.1.3. Desafíos en las PYMES del Sector T.I.

Las PYMES del sector TI enfrentan desafíos específicos relacionados con la gestión de la seguridad de la información. A menudo, estas empresas carecen de los recursos y el personal capacitado para implementar controles de seguridad adecuados. Según un estudio de Samboni (2018), las PYMES a menudo no priorizan la seguridad de la información debido a la falta de conciencia sobre los riesgos cibernéticos y la falta de presupuesto (Samboni, 2018). Esta falta de priorización es especialmente preocupante en un entorno digital cada vez más amenazado por ransomware, phishing, malware y otros tipos de ciberataques.

Además, debido a la rapidez en la adopción de nuevas tecnologías, las PYMES a menudo operan en un entorno de TI cambiante que requiere actualizaciones constantes en sus sistemas de seguridad (Potes & Sichaca, 2016). Este entorno dinámico exige que las PYMES no solo implementen soluciones de seguridad robustas desde el principio, sino que también mantengan un enfoque proactivo y adaptativo ante la evolución de las amenazas tecnológicas. Las empresas que no invierten adecuadamente en la formación de su personal en ciberseguridad o en tecnologías de protección avanzadas corren el riesgo de ser vulnerables a ataques que podrían comprometer tanto sus sistemas como la confianza de sus clientes.

4.1.4. Implementación de controles de seguridad basados en normas internacionales.

El uso de normas internacionales, como la ISO/IEC 27001 y la ISO/IEC 27002, es crucial para establecer y mantener un sistema de gestión de seguridad de la información eficiente. Estas normas proporcionan directrices para implementar controles de seguridad adaptados al tamaño y las necesidades específicas de las organizaciones, incluidas las PYMES (Lumbaque Figueroa & Duran, 2018). Estas directrices no solo abarcan las medidas preventivas, sino también las acciones correctivas y las estrategias de recuperación ante incidentes de seguridad, garantizando que las organizaciones puedan gestionar los riesgos de manera efectiva y mantener la resiliencia operativa frente a posibles ataques.

La implementación de estos controles permite a las organizaciones evaluar los riesgos de forma proactiva, desarrollar políticas de seguridad claras y asegurarse de que los empleados cumplan con las mejores prácticas en cuanto a la protección de la información. Las políticas de seguridad basadas en estas normas proporcionan un marco coherente para

auditorías de seguridad, gestión de accesos y protección de datos sensibles, elementos esenciales para mantener la seguridad en todo el ciclo de vida de la información. Además, el cumplimiento de estos estándares facilita la certificación ISO, que puede mejorar la reputación de la empresa y generar confianza entre clientes y socios comerciales.

4.2 Marco conceptual

Seguridad perimetral: Son los tipos de herramientas y técnicas de protección informática que tienen como propósito establecer una línea de defensa relacionada con la red interna y toda la prolongación que forma parte del entorno bajo el que se encuentra la tecnología de la información de una empresa.
Red de datos: Una red de datos es una red de telecomunicaciones que permite a los equipos de cómputo intercambiar datos. En las redes de cómputo, dispositivos de computación conectados en red pasan los datos entre sí a lo largo de las conexiones de datos.
Vulnerabilidad: Se entiende por vulnerabilidad a una debilidad propia de un sistema que permite ser atacado y recibir daño, así mismo una vulnerabilidad pone en riesgo los datos y sistemas de una empresa comprometiendo su integridad, privacidad y disponibilidad. Las vulnerabilidades se producen generalmente por una falla de programación, baja protección o falta de actualizaciones.
Amenaza: Una amenaza es la posibilidad de que un sistema vulnerable sea atacado y sufra daños
Riesgo: Se entiende por riesgo toda amenaza que explote alguna vulnerabilidad de uno o varios activos y pueda afectar el funcionamiento de un sistema.
Los riesgos, se clasifican mediante la siguiente ecuación. Riesgo = (amenaza * vulnerabilidad) / contramedida
Disponibilidad: Es la capacidad de tener acceso y de utilizar la información cuando se requiera.
Integridad: Es la precisión, integridad y validez de la información.
Confidencialidad: Es la protección de la información privada o sensible.
Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas.
Descripción de las Etapas del Ciclo de Deming:
Planificar (Plan):
Identificación de Problemas y Objetivos: Se define claramente el problema a resolver o el proceso a mejorar. Se establecen objetivos específicos y se desarrollan hipótesis sobre qué cambios podrían mejorar el proceso.
Desarrollo del Plan de Acción: Se elabora un plan detallado para implementar las mejoras. Esto incluye la definición de los recursos necesarios, la asignación de tareas y la programación de actividades.

Hacer (Do):

Implementación del Plan: Se ejecutan las acciones planeadas, inicialmente en una escala pequeña si es posible, para testear la efectividad de las soluciones propuestas. Esto minimiza el impacto de los errores en la fase de prueba.
Verificar (Check):
Evaluación de Resultados: Se monitorizan y evalúan los resultados de la implementación, comparándolos con los objetivos establecidos inicialmente. Se recolectan datos y se realiza un análisis para verificar la efectividad de las acciones realizadas.
Actuar (Act):
Ajustes y Estándarización: Basándose en el análisis de los datos recogidos, se toman decisiones sobre las próximas acciones. Si los cambios han dado resultado positivo, se estandarizan y se implementan en mayor escala. Si no, se identifican áreas para ajustes adicionales y se inicia un nuevo ciclo PDCA.
Finalmente, es crucial incluir tecnologías específicas que no solo sean efectivas sino también accesibles para las PYMES. Las soluciones de código abierto son particularmente atractivas para estas empresas debido a su coste reducido y la flexibilidad que ofrecen para personalizar y escalar las soluciones de acuerdo con necesidades específicas. A continuación, se describen algunas tecnologías código abierto relevantes para la seguridad perimetral:
pfSense: Es una solución de firewall y enrutador de código abierto altamente configurable basada en FreeBSD. pfSense ofrece funcionalidades avanzadas, que incluyen filtrado de tráfico, NAT, balanceo de carga y la capacidad de configurar VPNs. Es adecuado para empresas que necesitan una solución robusta sin el alto costo de licencias comerciales.
OPNsense: Un fork de pfSense, OPNsense es otro firewall de código abierto que se distingue por su enfoque en la seguridad y la transparencia. Ofrece una interfaz de usuario moderna y fácil de usar, actualizaciones de seguridad regulares y una comunidad activa.
Snort: Es uno de los sistemas de detección de intrusiones más populares y poderosos que también puede funcionar como un sistema de prevención de intrusiones. Snort utiliza un lenguaje de reglas configurables que permite a los usuarios escribir sus propias reglas de detección o modificar las existentes, haciéndolo extremadamente flexible y adaptable a diferentes entornos.
Suricata: Es otro IDS/IPS de código abierto que es conocido por su alto rendimiento y capacidad para realizar análisis en tiempo real del tráfico de red. Suricata es compatible con las reglas de Snort, pero también introduce su propio conjunto de características avanzadas, incluyendo soporte para análisis multihilo y capacidad para procesar grandes volúmenes de datos de manera más eficiente.

4.3 Marco legal

El marco de referencia se rige dentro de los siguientes marcos legales establecidos por la ley colombiana y demás entidades pertinentes.

ISO/IEC 27001: Esta norma agrupa los requerimientos de implantación de un SGSI, esta norma es certificable por entidades externas a la organización. La versión más actualizada de esta norma es la ISO 27000:2013.
ISO/IEC 27002: Es una guía de buenas prácticas para implementar controles de seguridad.
Prohibición del tratamiento de datos sensibles

Para implementar controles de seguridad se debe partir del hecho de que en la organización hay datos sensibles que son los que abarcarían esta norma. Según el artículo 6 de la ley 1581 de 2012: Se prohíbe el tratamiento de datos sensibles excepto cuando:

a. Cuando el titular autoriza de manera explícita su tratamiento, a no ser que la ley no exija dicha autorización.
b. Para proteger el interés vital del dato personal y el titular se encuentra incapacitado, caso en el cual sus representantes deberán dar dicha autorización.
c. Cuando se realice en desarrollo de actividades de funciones, ongs, organismo sin ánimo de lucro.
d. Para el reconocimiento, ejercicio y defensa de un derecho en un proceso judicial.
e. En los casos que tenga una finalidad histórica, estadistica o cientifica, siempre y cuando suprimiendo la identidad de los titulares

Conpes 3701 de 2011
Lineamientos de politica para ciberseguridad y ciberdefensa.
Ley 1273 de 5 de enero de 2009 La ley 1273 del 5 de enero de 2009
Fue creada para sancionar todos aquellos delitos que van en contra del buen uso de la información y aquellos que irrumpen con la propiedad privada, la idea de esta ley fue proteger a todas aquellas personas que cuentan con algún tipo de información financiera y personal.

4.4 Marco histórico (estado del arte)

Para iniciar con el entendimiento del presente proyecto se deben definir primero dos conceptos que por el conjunto de palabra que lo conforman tienden a ser confundidos y relacionados a un mismo significado sin embargo los dos son totalmente diferentes y se podría decir que uno de ellos parte del otro, el primero es seguridad de la información[5] el cual es un concepto ampliamente ligado al ser humano y la forma de comunicarse, de este concepto propiamente no se tiene indicios de describirlo propiamente antes de cristo sin embargo este se liga ampliamente con el concepto de criptografía, del cual si se tienen indicios desde los años 1500 AC con la aparición de la tableta mesopotámica, artilugio el cual tenía de forma cifrada una fórmula para producir la cerámica vitrificada o vidriado cerámico. Después de esto se tienen otros indicios hacia el antiguo continente y el imperio

[5] Seguridad Informatica y Seguridad de la información - Calderon Laura – Universidad Piloto de Colombia. http://polux.unipiloto.edu.co:8080/00001532.pdf

del gran Julio cesar el cual creo unos de los primeros sistemas criptográficos usando un sistema de sustitución en su alfabeto.[6]

Mas adelante hacia finales del siglo XVIII, Thomas Jefferson inventa el primer mecanismo de cifrado cilíndrico, conocido más comúnmente como rueda de Jefferson. Era un cilindro compuesto d 36 discos con 25 letras cada uno en el cual se ordenaban los discos de cierta forma y posteriormente se acomodarían de forma tal con el fin de que el mensaje a enviar se escribiese en una fila del mismo, y posteriormente se escogiese otra fila totalmente diferente en el cilindro y esta combinación seria enviada al destinatario, para que el mismo acomodase sus discos y pudiese encontrar el mensaje enviado, la coincidencia y probabilidad de encontrar dos mensajes bajo la misma clave era muy baja sin embargo esta se podía rectificar inmediatamente con el remitente por la posición de los discos.

Este invento solo se usó después de una mejora realizada por un comandante de las fuerzas de Estados Unidos el cual redujo el número de discos a 20 y 25 letras, este dispositivo tuvo gran acogida en las fuerzas armadas de USA desde 1923 hasta 1942.

Posteriormente en 1923, durante uno de los momentos más difíciles de la historia de la humanidad apareciendo la maquina enigma, un dispositivo el cual a partir de una clave de letras y números, se encargaba de sustituir los caracteres del mensaje mediante combinaciones de unos rotores interconectados entre si y a pesar de su complejidad, esta pudo ser descifrada por la inteligencia polaca y a su vez contribuir a la terminación de la segunda guerra en un periodo menor al esperado gracias al descifrado del funcionamiento y uso de esta máquina.

Ya hacia el año de 1973 tenemos un uso difundido de los algoritmos de cifrado de llaves públicas, y más adelante la aparición del algoritmo DES diseñado por IBM en 1975, y en base a sus vulnerabilidades la aparición del algoritmo RSA que hasta la actualidad es uno de los mejores algoritmos de cifrado existentes hasta el momento.

Hasta este momento hemos tocado el termino de seguridad de la información y su historia, sin embargo vemos que está totalmente relacionado con la historia de la criptografía, básicamente bajo los principios de mantener la información protegida ante personas externas a la comunicación entre emisor y receptor, sin embargo el mantenerla también se refiere a que esta debe de permanecer intacta, y ser accedida solo por las personas que tengan el permiso de acceso a la misma y por ultimo estar disponible en cualquier momento para el remitente.

En base a lo anterior la ISO definió que la seguridad de la información, “se refiere a la confidencialidad, la integridad y la disponibilidad de la información.”

Por otra parte, el termino de seguridad informática se refiere a la utilización de técnicas, métodos, procesos para la protección de sistemas informáticos y la información que estos contengan.

---

[6] Seguridad de la Información: Historia, Terminología y Campo de acción – Varios Autores - https://blog.desdelinux.net/seguridad-informacion-historia-terminologia-campo/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+desdelinuxweb+%28Desde+Linux%29#:~:text=Ciencia%20que%20se%20ocupa%20de,%C2%BB%20y%20la%20%C2%ABRob%C3%B3tica%C2%BB%20.

Dando así que la seguridad informática es una rama de la seguridad de la información que se enfoca a la preservación y protección de los sistemas informáticos y la información en medios digitales.

4.4.1 Fuentes primarias

Valencia D. Francisco J, Orozco A. Mauricio – Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000 (2017) - A-methodology-for-implementing-an-information-security-management-system-based-on-the-family-of-ISO-IEC-27000-standards.pdf (researchgate.net)
El proyecto presentado orienta en la metodología que se debe utilizar para implementar un SGSI y se enfatiza en la familia de normas de interés. Adicionalmente, brinda los pasos para abordar proyectos de este estilo.
Mintic - Guía para la implementación de seguridad de la información en una MIPYME - https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf
La guía propuesta por el Ministerio de Tics, orienta en la implementación de seguridad de la información enfocado en MIPYME, lo cual acerca el objetivo de segmentación que tiene el proyecto actual. Adicional define conceptos claves en la ejecución de estas implementaciones.
Rico Trejos Walter, Saavedra Rivera Serafín, Propuesta para la implementación de un plan de seguridad informática en la alcaldía de Dosquebradas Risaralda - https://repositorio.ucp.edu.co/bitstream/10785/3658/1/CDMIST126.pdf
El análisis de riesgos realizado para la alcaldía de Dosquebradas Risaralda podría ofrecer una base para entender los tipos de riesgos que podrían enfrentarse y cómo mitigarlos en un contexto similar. Adicional, las estrategias y políticas específicas propuestas en el proyecto pueden ser adaptadas o servir como inspiración para desarrollar políticas de seguridad informática adecuadas para el modelo que se quiere realizar.
Macias Xiomara, Dueñas Jose, Implementación de un modelo de seguridad informática en un sistema de monitoreo para los canales de comunicaciones y Datacenter en la empresa Atento SA - https://repository.udistrital.edu.co/bitstream/handle/11349/4258/MaciasMendezXiomaraMayerli2015.pdf?sequence=9&isAllowed=y
Estudiar el modelo de seguridad específico implementado en Atento SA puede proporcionar detalles críticos sobre las tecnologías y estrategias empleadas, adaptándolas según las necesidades de cada Pyme del sector T.I. Además, analizar cómo el proyecto cumplió con los requerimientos legales y normativos relevantes para la seguridad informática, lo que puede ser crucial para adaptar el modelo a los requisitos específicos de la industria T.I.

4.4.2 Fuentes secundarias

Benjumea Carlos, Diseño de una guía de seguridad perimetral escalable y en alta disponibilidad con equipos firewall tipo ngfw - https://repository.unad.edu.co/bitstream/handle/10596/8626/PROYECTO_DE_GRADO_2016.pdf;jsessionid=A7883D366626E529B4FDC77507FFDA33.jvm1?sequence=1
Ya que este es un proyecto que aplica parámetros de seguridad en redes, resulta útil ya que la gran mayoría de Pymes del sector T.I tienes datacenter propios o servicios de red entre sus servicios, por lo tanto es útil entender que características y aspectos se deben tener en cuenta a la hora de plantear el modelo.
Camacho Andres, Lopez John - Diseño de un sistema de seguridad perimetral e interna para la empresa Americas Business Process Services - https://repository.udistrital.edu.co/bitstream/handle/11349/7710/DISE%C3%91O%20DE%20UN%20SISTEMA%20DE%20SEGURIDAD%20PERIMETRAL%20ABPS.pdf?sequence=1&isAllowed=y
Este proyecto se puede tomar como referencia ya que contiene la implementación dentro de una entidad especifica, lo cual resulta útil para identificar aspectos que se deben tener en cuenta a la hora de que cualquier pyme del sector T.I quiera implementar el modelo planteado.

5. METODOLOGÍA

En el desarrollo de este proyecto se utilizará el ciclo Deming, también conocido como PDCA (Plan, Do, Check, Act), como metodología para implantar un sistema de mejora continua. Esta elección se justifica por su capacidad para facilitar el análisis de riesgos en el desarrollo del modelo de seguridad y permitir una mejor arquitectura en la formación del modelo a desarrollar. El ciclo Deming consta de cuatro etapas interconectadas, y cada una de ellas es fundamental para el éxito del proyecto.

A continuación, se desglosa el desarrollo por cada una de las etapas.

1. **Planificar:**

   En esta etapa, se marcará el inicio del proceso de investigación y análisis de la situación actual de las pequeñas y medianas empresas del sector T.I. en cuanto a los mecanismos de seguridad implementados. Se establecerán el alcance, los objetivos y los puntos de medición para verificar y medir los avances. Además, se identificarán los recursos disponibles en la organización y se evaluarán los posibles controles que se pueden implementar.

   Actividades Clave:

   - **Análisis del entorno y diagnóstico de seguridad:**
     - Evaluación del estado actual de la seguridad en las PYMEs del sector TI.
     - Identificación de amenazas y vulnerabilidades en la infraestructura tecnológica de las empresas.
     - Análisis de incidentes pasados y su impacto.
   - **Definición del alcance y objetivos del modelo:**
     - Establecimiento de los criterios de evaluación de riesgos.
     - Delimitación de los activos de información críticos y su nivel de exposición a amenazas.
     - Establecimiento de métricas para medir la eficacia del modelo de seguridad.
   - **Selección de estándares y marcos de referencia:**
     - Adopción de la norma ISO/IEC 27001 para el diseño del modelo de gestión de seguridad.

    - Identificación de herramientas tecnológicas y metodologías complementarias (Análisis de Riesgo OCTAVE, Magerit, NIST).
- **Diseño del modelo de evaluación de riesgos:**
    - Clasificación y priorización de los riesgos según su impacto y probabilidad de ocurrencia.
    - Determinación de controles de seguridad adecuados para mitigar riesgos identificados.

2. Hacer:

La etapa "Hacer" implica la implementación de todos los controles necesarios, basados en el análisis previo realizado en la etapa de Planificación. Aquí se llevarán a cabo acciones concretas para fortalecer la seguridad de la información en las empresas, aplicando las políticas y estándares definidos. En esta etapa se va a generar el modelo de seguridad que permita controlar las vulnerabilidades y amenazas que se presenten en las pequeñas y medianas empresas del sector T.I.

Actividades Clave:

- **Desarrollo del modelo de seguridad:**
    - Creación de una arquitectura de seguridad perimetral basada en firewalls, sistemas IDS/IPS y VPNs.
    - Configuración de mecanismos de autenticación y autorización para el acceso a la información.
    - Implementación de cifrado y protocolos seguros en la transmisión de datos.
- **Capacitación y concienciación:**
    - Formación del personal sobre mejores prácticas en seguridad informática.
    - Simulación de escenarios de ataque y respuesta ante incidentes de seguridad.
- **Pruebas iniciales y ajuste del modelo:**
    - Realización de pruebas en entornos controlados para evaluar la eficacia de los controles implementados.
    - Ajuste de configuraciones de seguridad en función de los resultados obtenidos.

3. Verificar:

En esta etapa, se efectuará el control de todos los procedimientos implementados en el modelo. Se realizarán exámenes periódicos para asegurar la eficacia del modelo de seguridad implementado, se revisarán los niveles de riesgos aceptables y residuales, y se realizarán auditorías internas periódicas para evaluar la efectividad del modelo. En esta etapa se va a realizar un listado de recomendaciones sobre las posibles herramientas que contribuyan al establecimiento de controles de seguridad.

Actividades Clave:

- **Auditorías y monitoreo del sistema de seguridad:**
  - Revisión de registros y eventos de seguridad.
  - Monitoreo en tiempo real de accesos no autorizados e intentos de intrusión.
- **Evaluación de desempeño y análisis de incidentes:**
  - Identificación de brechas de seguridad que puedan haber sido explotadas.
  - Comparación de los resultados obtenidos con las métricas establecidas en la fase de planificación.
- **Revisión de los niveles de riesgo aceptable:**
  - Ajuste de los niveles de criticidad de las amenazas en función de la evolución del entorno digital.
  - Determinación de si los controles aplicados son suficientes o si es necesario reforzarlos.

4. Actuar:

La etapa "Actuar" consiste en desarrollar mejoras a partir de los hallazgos identificados en el modelo y en la aplicación de acciones correctivas y preventivas. Se buscará perfeccionar el modelo de seguridad a medida que se vayan detectando áreas de oportunidad y posibles vulnerabilidades.
En esta última etapa se va a proponer un plan de acción para mitigar los riesgos que se pueden presentar según la norma ISO 27001.

Actividades Clave:

- **Implementación de acciones correctivas y preventivas:**
  - Modificación de los controles de seguridad que no han mostrado el rendimiento esperado.
  - Aplicación de medidas de refuerzo en áreas críticas.
- **Optimización del modelo de seguridad:**
  - Incorporación de nuevas tecnologías y herramientas de seguridad en función de los avances del sector.
  - Automatización de ciertos procesos de gestión de seguridad para reducir errores humanos.
- **Estandarización y documentación:**
  - Creación de guías y manuales para la implementación del modelo en otras organizaciones.
  - Definición de procedimientos para la actualización periódica del modelo.

6 ALCANCES Y DELIMITACIONES

6.1 Alcance

El presente proyecto realizará un análisis de riesgos de los activos y la creación de un modelo para la implementación de controles en base a las políticas de seguridad de la información en la organización. Para la creación de este modelo se va a tomar como referencia estándares y recomendaciones más utilizados a nivel mundial como la norma ISO 27000 y sus derivados (27001 y 27002).

6.2 Delimitaciones

Este proyecto se enfoca en la gestión de riesgos de seguridad de la información en PYMEs del sector T.I., basado en la norma ISO 27001 y utilizando el Ciclo Deming (PDCA) como metodología. Se delimita a un enfoque teórico, sin implementación práctica, y considera únicamente riesgos relacionados con la seguridad perimetral y protección de datos empresariales, excluyendo otros tipos de riesgos. El estudio se centra en empresas con infraestructura digital, utilizando datos recientes (2020-2024), sin levantamiento de información en campo. No se abordará la certificación oficial en ISO 27001 ni el desarrollo de software específico, sino una propuesta metodológica adaptable a organizaciones del sector.

7 FACTIBILIDADES

7.1 Recurso humano

Como recursos humanos se define un grupo de dos consultores de seguridad capacitados en norma ISO/IEC 27001 preferiblemente, para la realización del análisis de riesgos, y levantamiento de información respecto al estado actual de la organización. Estos deben ser preferiblemente ingenieros en telemática o áreas afines con un conocimiento en análisis de vulnerabilidades. Estos ingenieros estarán durante todo el proyecto y se encargarán del levantamiento procesado y obtención de resultados y conclusiones del proyecto. A demás se debe contar con un tutor que oriente a los dos consultores en cualquier duda o dificultad en el momento de la implementación y elaboración del documento. Finalmente, a manera informativa, se lista el personal involucrado en la implementación, aunque este costo sea asumido por las empresas.

TIPO	DESCRIPCION	VALOR-HORA	CANTIDAD	TOTAL
CONSULTORES	Para desarrollar la solución propuesta	50000	10 HORAS SEMANALES	6'000.000
TUTOR	Para asesorar en la construcción del proyecto	40000	2 HORAS SEMANALES	1'200.000

Figura 2. Desglose Recurso Humano. Elaboración propia.

7.2 Recurso informático

Como recursos digitales o ayudas informáticas se definen, dos ordenadores portátiles para realizar la documentación y recopilación del estado actual, así como software especializado para el análisis de la infraestructura tales como wireshark, zenmap, tenable. Se tendrá en cuenta la infraestructura especifica de cada empresa, aunque este costo no esté directamente involucrado con la implementación del proyecto.

TIPO	DESCRIPCION	VALOR-HORA	CANTIDAD	TOTAL
Computadores	Para desarrollar la solución propuesta		1	1'500.000

Figura 3. Desglose Recurso Informático. Elaboración propia.

7.3 Legal

Ya que para los análisis necesarios se utilizarán herramientas de software libre, el proyecto es viable en cuanto a factibilidad legal

8 DESARROLLO DEL PROYECTO

8.1 Fase plan: Análisis de la situación actual y definición del modelo de gestión de riesgos

8.1.1 Análisis del contexto de las pymes del sector T.I

8.1.1.1 Contexto externo

Las pequeñas y medianas empresas (PYMEs) del sector de tecnología de la información (T.I.) operan en un entorno caracterizado por un crecimiento acelerado en la digitalización, la interconectividad y la adopción de nuevas tecnologías. Este escenario ha traído múltiples oportunidades de desarrollo y competitividad, pero también ha incrementado de forma significativa su exposición a amenazas cibernéticas.

Actualmente, las PYMEs están más conectadas que nunca, utilizan servicios en la nube, aplicaciones web, APIs y herramientas colaborativas que, si bien optimizan procesos, también amplían la superficie de ataque. Estas organizaciones suelen contar con infraestructuras híbridas, múltiples dispositivos conectados y acceso remoto, lo cual, si no está debidamente gestionado, representa un riesgo potencial constante.

Los ciberataques como el ransomware, el phishing, las filtraciones de datos y las intrusiones a redes corporativas afectan de forma directa a este tipo de empresas, ya que en la mayoría de los casos no disponen de los recursos suficientes —humanos, técnicos o financieros— para establecer sistemas robustos de defensa. Informes recientes señalan que un alto porcentaje de ataques globales están dirigidos a PYMEs, evidenciando su vulnerabilidad frente al crimen cibernético.

Adicionalmente, la presión del mercado exige cada vez más que las empresas garanticen la confidencialidad, integridad y disponibilidad de la información. La pérdida de datos o la interrupción de servicios no solo impactan económicamente, sino que también afectan la reputación de la empresa y su relación con los clientes.

Este entorno externo, cambiante y desafiante, obliga a las PYMEs del sector T.I. a adoptar enfoques estructurados para la gestión de riesgos de seguridad, a fin de proteger sus activos digitales y mantener su operatividad frente a un panorama de amenazas en constante evolución.

8.1.1.2 Contexto interno

Las pequeñas y medianas empresas del sector de tecnología de la información (T.I.) presentan características particulares que inciden directamente en su capacidad para gestionar la seguridad de la información de manera eficaz. Internamente, estas organizaciones suelen operar con estructuras reducidas, tanto a nivel de personal como de recursos tecnológicos, lo que limita su capacidad de respuesta ante incidentes de seguridad.

Una de las principales debilidades internas es la falta de una cultura organizacional orientada a la ciberseguridad. En muchas ocasiones, las decisiones relacionadas con la protección de la información son tratadas como un tema exclusivamente técnico, y no como un componente estratégico del negocio. Esto se traduce en la ausencia de políticas claras, procesos documentados, y responsables designados para la gestión de riesgos de seguridad de la información.

En cuanto a su infraestructura tecnológica, aunque muchas de estas empresas adoptan soluciones innovadoras como servicios en la nube, plataformas SaaS o sistemas interconectados, no siempre se cuenta con mecanismos adecuados para proteger dichos entornos. El uso de tecnologías modernas, sin una gestión adecuada de accesos, respaldos o monitoreo, puede generar vulnerabilidades críticas dentro del entorno interno.

Además, los activos de información más relevantes para estas organizaciones —como bases de datos de clientes, código fuente, credenciales de acceso, e infraestructura de red— muchas veces no son identificados ni gestionados como activos críticos. La ausencia de un inventario actualizado y una clasificación de activos impide aplicar controles eficaces.

Otro aspecto relevante es la limitación presupuestaria, que restringe la implementación de herramientas especializadas, personal dedicado exclusivamente a seguridad o procesos de capacitación continua. En muchos casos, las decisiones sobre tecnología priorizan la funcionalidad y el bajo costo, dejando en segundo plano los aspectos de seguridad.

Este conjunto de factores internos evidencia la necesidad de implementar modelos de gestión de riesgos accesibles, adaptables y alineados con la realidad de las PYMEs del sector T.I., que les permitan identificar amenazas, proteger sus activos y garantizar la continuidad operativa en un entorno cada vez más expuesto a riesgos digitales.

8.1.1.3 Partes interesadas

En el marco de la gestión de riesgos de seguridad de la información, la norma ISO 27001 establece la necesidad de identificar y comprender las partes interesadas relevantes, es decir, aquellas personas, grupos u organizaciones que afectan o pueden verse afectadas por la seguridad de la información de la empresa. En el caso de las PYMEs del sector T.I., estas partes interesadas desempeñan un papel fundamental en la definición de requerimientos, el cumplimiento de estándares y la continuidad del negocio.

Las principales partes interesadas en este contexto son:

Clientes y usuarios finales: Son los receptores directos de los productos o servicios tecnológicos de la empresa. Esperan que la información que proporcionan —como datos personales, financieros o comerciales— sea protegida adecuadamente. Cualquier brecha de seguridad puede afectar su confianza y generar pérdidas para la organización.

Empleados y colaboradores internos: Participan activamente en los procesos de desarrollo, soporte, administración o comercialización de los servicios. Su comportamiento, nivel de conocimiento en seguridad y acceso a la información los convierte en una parte crítica del sistema de protección, ya que pueden ser tanto una barrera como un vector de riesgo.

Proveedores y aliados tecnológicos: Muchas PYMEs dependen de servicios externos (como hosting, almacenamiento en la nube, plataformas de desarrollo o herramientas de gestión). Estos terceros manejan datos sensibles o tienen acceso a la infraestructura, por lo que sus prácticas de seguridad también afectan a la organización.

Alta dirección y propietarios: Son responsables de tomar decisiones estratégicas, aprobar inversiones en seguridad y definir el nivel de compromiso de la empresa frente a los riesgos de información. Su implicación es clave para la implementación de políticas y modelos eficaces.

Entidades aseguradoras y financieras: En algunos casos, estas organizaciones evalúan el nivel de riesgo tecnológico de las empresas antes de ofrecer cobertura o financiamiento. Un bajo nivel de madurez en seguridad puede limitar el acceso a estos servicios.

Comunidad y entorno digital: Incluye asociaciones del sector, redes de colaboración, foros de desarrolladores y comunidades tecnológicas que influyen en las buenas prácticas, alertan sobre nuevas amenazas y comparten recursos útiles para la protección de activos.

Comprender las necesidades y expectativas de estas partes interesadas permite diseñar un modelo de gestión de riesgos más sólido, adaptado a las realidades del negocio y alineado con las exigencias internas y externas del entorno organizacional.

8.1.1.4 Necesidades y expectativas de las partes interesadas

Identificar las necesidades y expectativas de las partes interesadas permite alinear el sistema de gestión de seguridad de la información con los intereses clave del negocio, garantizando así su eficacia, pertinencia y aceptación. En el contexto de las PYMEs del sector T.I., dichas necesidades se relacionan principalmente con la protección de datos, la disponibilidad de los servicios, el cumplimiento de estándares y la confianza organizacional.

A continuación, se resumen las necesidades y expectativas más relevantes:

Clientes y usuarios finales: Esperan que su información personal, comercial y financiera sea tratada con confidencialidad, integridad y disponibilidad. Exigen que los servicios funcionen sin interrupciones y que sus datos estén protegidos contra accesos no autorizados, pérdida o alteración. También esperan que la empresa cumpla con las leyes de protección de datos.

Empleados y colaboradores: Requieren acceso seguro y controlado a los sistemas e información necesarios para cumplir sus funciones. Esperan que la empresa brinde lineamientos claros, formación en seguridad y herramientas confiables que eviten incidentes que puedan poner en riesgo su trabajo o los datos que manejan.

Proveedores y aliados tecnológicos: Buscan relaciones comerciales seguras, con una gestión clara de accesos, integración de sistemas protegidos y cumplimiento de estándares mínimos de seguridad que garanticen la confianza mutua.

Alta dirección y propietarios: Esperan que la información estratégica de la empresa esté protegida, que los riesgos estén gestionados adecuadamente y que las inversiones en seguridad sean justificadas y efectivas. También buscan minimizar el impacto de posibles incidentes sobre la operatividad y reputación del negocio.

Entidades aseguradoras y financieras: Necesitan garantías sobre el nivel de control que tiene la empresa sobre sus riesgos tecnológicos. Esperan evidencia de cumplimiento de buenas prácticas para poder ofrecer respaldo financiero o coberturas adecuadas.

Comunidad del sector T.I. y entornos colaborativos: Promueven la adopción de estándares como ISO 27001 y esperan que las empresas mantengan prácticas seguras que contribuyan a la confianza y estabilidad del ecosistema digital.

Entender estas necesidades permite orientar correctamente la selección de controles, políticas y medidas de protección dentro del modelo de gestión de riesgos, y asegura que el sistema propuesto sea pertinente y sostenible a largo plazo.

8.1.2 Identificación de activos de información críticos

8.1.2.1 Alcance

El alcance de este modelo de gestión de riesgos se delimita a los activos de información críticos y los procesos tecnológicos esenciales de las pequeñas y medianas empresas (PYMEs) del sector de tecnología de la información (T.I.), con especial énfasis en la seguridad perimetral y la protección de datos en entornos digitales.

Este modelo contempla únicamente el entorno organizacional relacionado con la gestión, almacenamiento, procesamiento y transmisión de información, incluyendo infraestructura tecnológica, redes, plataformas de desarrollo, sistemas de comunicación, software empresarial y servicios en la nube.

La propuesta se enfoca en:

- Procesos relacionados con el desarrollo, operación y soporte de servicios tecnológicos.
- Gestión de bases de datos de clientes y sistemas internos de información.
- Administración de redes, accesos remotos y dispositivos conectados.
- Controles de seguridad técnica y organizativa para proteger la información y garantizar la continuidad del negocio.

Quedan excluidos del alcance:

- Procesos administrativos y financieros no relacionados con tecnología.
- Sistemas offline o fuera del entorno digital de la organización.
- Evaluaciones prácticas en entornos reales (al tratarse de una propuesta teórica).
- Certificación formal en ISO 27001.

Este modelo está diseñado como una herramienta teórica adaptable, con el objetivo de ser implementado en empresas del sector T.I. que cuenten con recursos limitados y requieran

una estructura metodológica clara para gestionar sus riesgos de seguridad de la información de manera progresiva, conforme a los principios de mejora continua del ciclo PDCA.

8.1.2.2 Clasificación de los tipos de activos

En función de los procesos críticos identificados en una PYME del sector T.I., se realizó una clasificación de los activos de información relevantes, agrupándolos por categorías según su naturaleza y función dentro de la organización. Esta clasificación permite estructurar el análisis de riesgos y establecer controles de seguridad adecuados en etapas posteriores.

Categoría	**Descripción del Activo**	**Ejemplo específico**
Información	Datos digitales que tienen valor para la empresa y requieren protección.	Base de datos de clientes, tickets de soporte, información técnica de proyectos, contraseñas, logs.
Personas	Usuarios internos que acceden, gestionan o manipulan información sensible.	Desarrolladores, personal de soporte, administradores de red, gerentes de TI.
Software	Aplicaciones utilizadas para operaciones, desarrollo y gestión de información.	CRM, ERP, sistemas de tickets, herramientas de desarrollo (Git, IDEs), bases de datos (MySQL, PostgreSQL).
Hardware	Equipos físicos utilizados para almacenar, procesar o transportar información.	Servidores, portátiles de desarrollo, routers, switches, UPS.
Redes e Infraestructura	Componentes de red que permiten la comunicación y operación de los servicios tecnológicos.	VPN, firewalls, puntos de acceso Wi-Fi, segmentación de red, cableado estructurado.
Servicios de TI	Servicios tecnológicos, internos o contratados, que soportan los procesos del negocio.	Servicios en la nube (AWS, Azure), hosting de aplicaciones, correo corporativo, backup en la nube.
Documentos	Archivos físicos o digitales que contienen información estructurada o formalizada.	Políticas de seguridad, manuales técnicos, contratos, respaldos, procedimientos operativos.

8.1.2.3 Criterios de criticidad

Una vez clasificados los activos, es necesario determinar su nivel de criticidad para priorizar su protección. Para ello, se aplican los criterios establecidos en el modelo CIA, que evalúa el impacto que tendría una pérdida de confidencialidad, integridad o disponibilidad de cada activo en las operaciones de la empresa.

Cada criterio se valorará en tres niveles: Alta, Media o Baja, y la criticidad general del activo se determinará en función de la combinación de estos factores. A continuación, se presenta una muestra de los activos más representativos evaluados en función de su criticidad dentro de los procesos clave de una PYME del sector T.I.

Categoría	**Activo Representativo**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Criticidad General**
Información	Base de datos de clientes	Alta	Alta	Alta	**Crítico**
Personas	Personal de soporte técnico	Media	Alta	Alta	**Alta**
Software	Plataforma de gestión de proyectos	Alta	Alta	Media	**Crítico**
Hardware	Servidor de respaldo	Media	Alta	Alta	**Crítico**
Infraestructura/Red	Firewall perimetral	Alta	Alta	Alta	**Crítico**
Servicios de TI	Correo corporativo en la nube	Alta	Media	Alta	**Alta**
Documentos	Políticas internas de seguridad	Media	Alta	Media	**Alta**

Dentro de los criterios aplicados se encuentra:

- Alta: Si el compromiso afecta seriamente la operación, la imagen o la legalidad.

- Media: Si el impacto es importante pero no catastrófico.
- Baja: Si la pérdida es tolerable o fácilmente recuperable.

Por su parte la criticidad general se definió como:

- Crítico: Cuando al menos 2 criterios están en nivel Alto.
- Alta: Cuando 1 criterio es Alto y los demás son al menos Medios.
- Moderada o baja: Cuando ningún criterio es Alto.

8.1.3 Evaluación de amenazas y vulnerabilidades actuales

En esta sección se identifican y analizan las amenazas y vulnerabilidades asociadas a los activos de información críticos previamente clasificados. Este análisis tiene como propósito estimar el nivel de exposición de la organización frente a incidentes de seguridad y sentar las bases para la posterior selección de controles según la norma ISO 27001.

8.1.3.2 Matriz de evaluación de riesgos

Para determinar el nivel de riesgo asociado a cada amenaza identificada, se utiliza una matriz de evaluación cualitativa que combina dos variables fundamentales: el impacto que tendría la materialización de la amenaza sobre el activo, y la probabilidad de que dicha amenaza ocurra dadas las condiciones actuales de seguridad. Esta herramienta permite clasificar los riesgos en categorías que orientan la toma de decisiones y la priorización de controles, de acuerdo con el contexto operativo y tecnológico de las PYMEs del sector T.I.

Esta matriz combina los niveles de impacto y probabilidad para estimar el nivel de riesgo asociado a cada amenaza identificada. Se utiliza un enfoque cualitativo, adaptado al contexto de las PYMEs del sector T.I., que permite clasificar los riesgos como Bajo, Moderado, Alto o Crítico.

Impacto / Probabilidad	**Baja**	**Media**	**Alta**
Baja	Bajo	Moderado	Moderado
Media	Moderado	Alto	Alto
Alta	Moderado	Alto	Crítico

8.1.3.3 Evaluación por activo

A continuación, se presenta una tabla que relaciona los activos de información críticos con sus respectivas amenazas potenciales y vulnerabilidades asociadas, identificadas en función del contexto actual de las PYMEs del sector T.I. Esta evaluación permite estimar el nivel de riesgo combinando el impacto que tendría la materialización de la amenaza sobre el activo y la probabilidad de que ocurra, considerando las condiciones actuales de seguridad en este tipo de organizaciones. Esta información servirá de base para la posterior definición de controles de mitigación adecuados.

Activo Crítico	**Amenaza Potencial**	**Vulnerabilidad Asociada**	**Impacto**	**Probabilidad**	**Nivel de Riesgo**
Base de datos de clientes	Fuga de información	Accesos mal configurados / falta de cifrado	Alta	Alta	**Crítico**
Personal de soporte técnico	Ingeniería social	Ausencia de formación en seguridad	Media	Alta	**Alto**
Plataforma de gestión	Inyección SQL	Falta de validación en entradas de usuario	Alta	Media	**Alto**
Servidor de respaldo	Pérdida de datos por ransomware	Software desactualizado / backups no verificados	Alta	Media	**Alto**
Firewall perimetral	Acceso no autorizado	Reglas mal configuradas / firmware obsoleto	Alta	Alta	**Crítico**
Correo corporativo (nube)	Phishing / Suplantación	Falta de autenticación en dos pasos (2FA)	Media	Alta	**Alto**

Políticas de seguridad (doc.)	Modificación no autorizada	Archivos sin restricción de permisos	Media	Media	**Moderado**

8.1.4 Análisis de brechas con respecto a iso27001

Con el fin de evaluar el grado de alineación de la organización con los requerimientos de la norma ISO/IEC 27001, se realizó un análisis de brechas (Gap Analysis) que permite identificar los controles de seguridad implementados, los que se encuentran parcialmente desarrollados y aquellos ausentes. Este análisis proporciona una visión clara del estado actual y orienta la definición de acciones correctivas dentro del modelo propuesto.

Con base en los resultados del análisis de riesgos y el análisis de brechas frente a la norma ISO/IEC 27001, se propone un conjunto de controles de seguridad que permitan mitigar los riesgos identificados y cerrar las brechas detectadas en los activos críticos de las PYMEs del sector T.I. Los controles seleccionados provienen del Anexo A de la norma y han sido priorizados por su aplicabilidad, viabilidad y relevancia para el contexto operativo de estas organizaciones. A continuación, se presenta la tabla con los controles propuestos y su correspondencia con los activos y riesgos asociados:

Control ISO 27001	**Descripción**	**Activo(s) Protegido(s)**	**Riesgo Mitigado**
A.5.1.1 – Política de seguridad	Establecer una política formal de seguridad de la información	Toda la organización	Falta de lineamientos claros para proteger la información

A.6.1.1 – Funciones y responsabilidades	Definir y asignar roles de seguridad dentro de la organización	Personal de TI y soporte	Ausencia de responsables designados para la gestión de riesgos
A.7.2.2 – Concientización y formación	Implementar un programa de formación en seguridad	Personal de soporte técnico	Ingeniería social / errores humanos
A.9.2.1 – Gestión de cuentas de usuario	Controlar el acceso mediante cuentas individuales con privilegios adecuados	Plataforma de gestión, base de datos	Accesos no autorizados
A.9.4.1 – Uso de sistemas de acceso seguro	Implementar autenticación robusta (contraseñas, 2FA)	Correo corporativo, CRM	Suplantación / Phishing
A.12.3.1 – Copias de respaldo	Establecer respaldos periódicos, probados y documentados	Servidor de respaldo, base de datos	Pérdida de datos / ransomware

A.12.6.1 – Gestión de vulnerabilidades	Aplicar actualizaciones y parches de seguridad regularmente	Firewall, software, servidores	Exploits conocidos por software desactualizado
A.13.1.1 – Protección de información en tránsito	Cifrar la información enviada por correo o transferida por red	Datos sensibles en correo y nube	Interceptación de datos
A.13.2.3 – Segregación de redes	Separar redes internas de servicios públicos (DMZ, VLANs)	Infraestructura de red, firewall	Movimiento lateral de amenazas / intrusiones
A.14.2.1 – Validación de entradas	Validar entradas en formularios y consultas de bases de datos	Plataforma de gestión de proyectos	Inyección SQL / corrupción de datos
A.16.1.1 – Reporte de incidentes	Crear un proceso para notificar y registrar incidentes de seguridad	Toda la organización	Falta de respuesta organizada ante incidentes
A.18.1.4 – Evaluación de riesgos periódica	Evaluar riesgos de seguridad al menos una vez al año	Todos los activos	Modelo desactualizado frente a nuevas amenazas

8.1.5 Identificación de necesidades de mejora

La mejora continua es un principio fundamental tanto del modelo PDCA como de la norma ISO/IEC 27001. Una vez definidos los controles y evaluado el nivel de cumplimiento actual, es necesario identificar las necesidades de mejora que permitan fortalecer la eficacia del sistema de gestión de seguridad de la información en las PYMEs del sector T.I.

Estas necesidades surgen a partir de los resultados del análisis de riesgos, el análisis de brechas y la evaluación del cumplimiento de controles. Su identificación permite establecer un ciclo de revisión y ajuste periódico que garantice que el modelo se mantenga actualizado frente a nuevas amenazas, cambios tecnológicos y evolución del entorno organizacional.

A continuación, se detallan las principales necesidades de mejora detectadas en el modelo propuesto:

Área / Dominio	**Necesidad de Mejora**	**Justificación**
Políticas y gobierno de TI	Establecer y revisar periódicamente la política de seguridad de la información	Garantizar alineación con los objetivos del negocio y la evolución del entorno.
Capacitación y cultura interna	Diseñar un programa continuo de formación en seguridad de la información	Reducir el riesgo de errores humanos e ingeniería social.

Procedimientos y documentación	Documentar los procesos de respaldo, gestión de incidentes y control de accesos	Facilitar la trazabilidad, estandarización y cumplimiento de auditorías.
Monitoreo y detección de incidentes	Incorporar herramientas básicas de monitoreo de eventos de seguridad (SIEM o registros de logs)	Mejorar la capacidad de detección y respuesta ante incidentes.
Evaluación de riesgos	Realizar reevaluaciones periódicas de riesgos (al menos una vez por año o ante cambios relevantes)	Mantener el modelo actualizado frente a nuevas amenazas.
Actualización tecnológica	Establecer un plan de mantenimiento para parches, firmware y actualizaciones de software	Reducir la exposición a vulnerabilidades conocidas.

Medición de eficacia de controles	Definir indicadores de desempeño (KPIs) para evaluar la efectividad de los controles implementados	Medir objetivamente el funcionamiento del modelo y su impacto en la seguridad.

La implementación del modelo no debe considerarse como un evento puntual, sino como un proceso cíclico y adaptable. Las necesidades de mejora aquí identificadas permitirán establecer un plan de acción continuo, asegurar el cumplimiento sostenido con ISO 27001, y fortalecer progresivamente la postura de seguridad de la organización ante un entorno tecnológico en constante cambio.

8.1.6 Definición del modelo de gestión de riesgos

El modelo de gestión de riesgos propuesto en este proyecto está diseñado para ser aplicado en pequeñas y medianas empresas (PYMEs) del sector de tecnología de la información (T.I.), y se fundamenta en los principios de la norma ISO/IEC 27001 y en la metodología de mejora continua conocida como Ciclo Deming (PDCA: Plan, Do, Check, Act). Su objetivo principal es establecer una estructura flexible, escalable y eficaz que permita identificar, evaluar, controlar y monitorear los riesgos asociados a la seguridad de la información en entornos organizacionales con recursos limitados.

Este modelo contempla la protección integral de los activos de información críticos, tales como bases de datos, plataformas de software, infraestructura de red, correo corporativo, documentación interna y personal con acceso a información sensible. A partir de la evaluación del contexto interno y externo, la clasificación de activos, la identificación de amenazas y vulnerabilidades, y el análisis de brechas frente a la norma ISO 27001, se construye una arquitectura de controles que prioriza los riesgos más relevantes para el negocio.

8.1.6.1 Planteamiento del objetivo del modelo

El modelo de gestión de riesgos propuesto tiene como objetivo principal fortalecer la seguridad de la información en pequeñas y medianas empresas (PYMEs) del sector T.I., a

través de una estructura metodológica basada en la norma ISO/IEC 27001 y en el enfoque de mejora continua del Ciclo Deming (PDCA).

Este modelo busca proporcionar a las organizaciones una herramienta práctica y adaptable para:

- Identificar y clasificar sus activos de información críticos,
- Evaluar amenazas y vulnerabilidades reales,
- Determinar el nivel de riesgo asociado a cada activo,
- Seleccionar e implementar controles de seguridad apropiados,
- Monitorear la eficacia de dichos controles
- Establecer un ciclo de mejora continua que permita actualizar y optimizar la gestión de riesgos frente a un entorno digital en constante evolución.

La implementación del modelo no pretende reemplazar una certificación formal en ISO 27001, sino servir como una guía estratégica y operativa para reducir la exposición a incidentes de seguridad, mejorar la postura defensiva de las empresas y fomentar una cultura organizacional de ciberseguridad, incluso en contextos con recursos técnicos y financieros limitados.

8.1.6.2 Alcance del modelo

El modelo de gestión de riesgos propuesto en este proyecto está diseñado para ser aplicado en pequeñas y medianas empresas (PYMEs) del sector de tecnología de la información (T.I.), cuyas operaciones dependen en gran medida de sistemas informáticos, redes, datos digitales y plataformas en la nube.

El alcance del modelo se limita a los procesos y activos más críticos relacionados con la seguridad de la información, tales como:

- Gestión de bases de datos de clientes y proyectos,
- Desarrollo y mantenimiento de plataformas o software,
- Administración de redes internas y conexiones externas,

- Uso de servicios en la nube y correo electrónico corporativo,

- Soporte técnico y operación de sistemas.

Este modelo considera exclusivamente los aspectos técnicos y organizativos relacionados con la seguridad perimetral, control de accesos, protección de datos, continuidad del servicio y gestión de incidentes de seguridad informática, en coherencia con los controles establecidos en la norma ISO/IEC 27001.

Quedan fuera del alcance de este modelo:

- Procesos financieros, contables o administrativos no relacionados con la seguridad de la información.

- Procesos fuera del entorno digital o físico de la organización.

- Evaluaciones prácticas en empresas reales (por tratarse de una propuesta teórica).

- La obtención o gestión formal de certificaciones ISO.

El modelo está diseñado para ser adaptable, escalable y progresivamente implementable, permitiendo que las empresas puedan fortalecer su postura de seguridad con base en su capacidad técnica, operativa y económica, sin requerir grandes inversiones iniciales.

8.1.6.3 Selección de los controles alineados con iso27001

Con base en el análisis de activos críticos, amenazas, vulnerabilidades y el análisis de brechas frente a los requerimientos de la norma ISO/IEC 27001, se definieron los controles que conforman el núcleo del modelo de gestión de riesgos propuesto. Estos controles fueron seleccionados estratégicamente del Anexo A de la norma, teniendo en cuenta su relevancia para los riesgos identificados, su aplicabilidad en entornos de PYMEs y su viabilidad de implementación en organizaciones con recursos limitados.

La selección se enfoca en los dominios clave que permiten proteger la información, los sistemas, las redes y los procesos críticos del negocio, especialmente aquellos relacionados con la seguridad perimetral, gestión de accesos, continuidad operativa y respuesta ante incidentes. Asimismo, se priorizaron controles que contribuyen a establecer una estructura organizativa de seguridad y fomentan la concientización interna.

La siguiente tabla resume los controles seleccionados, su propósito y los activos o riesgos a los que están asociados:

Control ISO 27001	**Descripción**	**Activo(s) Protegido(s)**	**Riesgo Mitigado**
A.5.1.1 – Política de seguridad	Establecer una política formal de seguridad de la información	Toda la organización	Falta de lineamientos claros para proteger la información
A.6.1.1 – Funciones y responsabilidades	Definir y asignar roles de seguridad dentro de la organización	Personal de TI y soporte	Ausencia de responsables designados para la gestión de riesgos
A.7.2.2 – Concientización y formación	Implementar un programa de formación en seguridad	Personal de soporte técnico	Ingeniería social / errores humanos
A.9.2.1 – Gestión de cuentas de usuario	Controlar el acceso mediante cuentas individuales con privilegios adecuados	Plataforma de gestión, base de datos	Accesos no autorizados

A.9.4.1 – Uso de sistemas de acceso seguro	Implementar autenticación robusta (contraseñas, 2FA)	Correo corporativo, CRM	Suplantación / Phishing
A.12.3.1 – Copias de respaldo	Establecer respaldos periódicos, probados y documentados	Servidor de respaldo, base de datos	Pérdida de datos / ransomware
A.12.6.1 – Gestión de vulnerabilidades	Aplicar actualizaciones y parches de seguridad regularmente	Firewall, software, servidores	Exploits conocidos por software desactualizado
A.13.1.1 – Protección de información en tránsito	Cifrar la información enviada por correo o transferida por red	Datos sensibles en correo y nube	Interceptación de datos
A.13.2.3 – Segregación de redes	Separar redes internas de servicios públicos (DMZ, VLANs)	Infraestructura de red, firewall	Movimiento lateral de amenazas / intrusiones
A.14.2.1 – Validación de entradas	Validar entradas en formularios y consultas de bases de datos	Plataforma de gestión de proyectos	Inyección SQL / corrupción de datos

A.16.1.1 – Reporte de incidentes	Crear un proceso para notificar y registrar incidentes de seguridad	Toda la organización	Falta de respuesta organizada ante incidentes
A.18.1.4 – Evaluación de riesgos periódica	Evaluar riesgos de seguridad al menos una vez al año	Todos los activos	Modelo desactualizado frente a nuevas amenazas

La elección de estos controles se basó en los siguientes criterios:

- Pertinencia: Capacidad del control para mitigar amenazas identificadas en el análisis de riesgos.
- Aplicabilidad: Adaptación a procesos y recursos típicos de una PYME del sector T.I.
- Viabilidad: Posibilidad de implementación con recursos técnicos, humanos y financieros limitados.
- Impacto: Capacidad del control para reducir el nivel de riesgo de los activos críticos.

La implementación de estos controles proporciona una cobertura integral de los principales riesgos a los que están expuestas las PYMEs del sector T.I., y constituye la base del modelo propuesto. Además, permite establecer una estructura mínima pero efectiva de seguridad de la información, alineada con las buenas prácticas internacionales, sin comprometer la operatividad ni exigir grandes inversiones.

8.1.6.4 Asignación de roles y responsabilidades

Uno de los principios fundamentales del modelo de gestión de riesgos propuesto, en alineación con la norma ISO/IEC 27001, es la definición clara de roles y responsabilidades dentro de la organización. Esta asignación permite asegurar que cada parte involucrada

en los procesos de seguridad de la información conozca sus funciones, obligaciones y límites de actuación, facilitando una gestión más eficaz y organizada.

En el contexto de una pequeña o mediana empresa del sector T.I., con estructuras operativas reducidas, es común que una misma persona cumpla múltiples funciones. Por ello, el modelo propone una asignación de roles flexible pero formal, que se adapte a la realidad de este tipo de organizaciones sin comprometer el control y seguimiento de las actividades clave.

A continuación, se detallan los roles propuestos dentro del modelo, junto con sus principales responsabilidades:

Rol	**Responsabilidades principales**
Responsable de Seguridad (CISO / líder de seguridad)	- Definir políticas de seguridad
	- Coordinar la gestión de riesgos
	- Supervisar la implementación de controles
	- Evaluar incidentes y liderar la respuesta
	- Coordinar auditorías internas
Administrador de TI / Infraestructura	- Gestionar configuraciones de red, firewall y servidores

	- Aplicar actualizaciones y parches de seguridad
	- Administrar copias de respaldo
	- Implementar medidas técnicas definidas por el modelo
Encargado de soporte técnico	- Gestionar accesos de usuarios
	- Brindar soporte en herramientas y plataformas
	- Reportar incidentes detectados
	- Apoyar en la concientización del usuario final
Usuarios internos (colaboradores)	- Cumplir con las políticas de seguridad

	- Proteger sus credenciales de acceso
	- Reportar actividades sospechosas o fallos de seguridad
	- Participar en capacitaciones
Alta Dirección / Gerencia	- Aprobar el modelo de gestión de riesgos
	- Asignar recursos necesarios
	- Supervisar el cumplimiento de políticas
	- Apoyar la cultura de seguridad en la organización

Dado que muchas PYMEs del sector T.I. no cuentan con una estructura compleja ni con personal exclusivo para seguridad de la información, estos roles pueden ser asumidos por miembros existentes del equipo, siempre que sus funciones queden formalmente documentadas y reconocidas. El objetivo no es generar burocracia, sino establecer claridad, trazabilidad y compromiso en la gestión de la seguridad.

La asignación adecuada de roles y responsabilidades permite distribuir eficientemente las tareas, reducir los errores por desconocimiento, y facilitar el seguimiento, control y mejora

del modelo de seguridad. Esta definición, además, fortalece el cumplimiento de los requisitos de ISO 27001, específicamente los relacionados con la organización de la seguridad de la información.

8.1.6.5 Recursos necesarios para su implementación

La implementación del modelo de gestión de riesgos propuesto requiere de una serie de recursos que garanticen su funcionamiento efectivo y sostenible dentro de una pequeña o mediana empresa del sector T.I. Estos recursos deben estar alineados con las capacidades reales de la organización, optimizando su uso y priorizando aquellos que tienen un mayor impacto en la reducción de riesgos y el fortalecimiento de la seguridad de la información.

A continuación, se describen los recursos necesarios clasificados en tres categorías: recursos humanos, tecnológicos y económicos.

8.1.6.5.1 Recursos humanos

Recurso	**Descripción**
Personal responsable de seguridad	Encargado de liderar la implementación del modelo, definir políticas y coordinar acciones.
Administrador de sistemas / redes	Responsable técnico de aplicar controles en infraestructura y redes.

Soporte técnico / Help Desk	Apoyo en la gestión de accesos, seguimiento de incidentes y atención a usuarios.
Personal operativo (usuarios)	Participación activa en el cumplimiento de políticas y reportes de incidentes.

8.1.6.5.2 Recursos tecnológicos

Recurso	**Función**
Plataforma de respaldo	Realizar y verificar copias de seguridad periódicas.
Firewall / Router empresarial	Controlar el tráfico de red y establecer perímetros de seguridad.
Software antivirus y antimalware	Prevenir infecciones y accesos no autorizados.

Herramientas de autenticación	Implementar contraseñas seguras y autenticación de dos factores (2FA).
Servicios de nube seguros	Asegurar la disponibilidad y cifrado de datos en tránsito.
Documentación digital	Almacenamiento de políticas, procedimientos, registros e informes de auditoría.

8.1.6.5.3 Recursos económicos

Recurso	**Uso estimado**
Presupuesto para capacitación	Formación básica en seguridad de la información para todo el personal.

Licencias de software básico	Antivirus, soluciones de backup, herramientas de cifrado o autenticación.
Contratación de soporte externo	Consultoría puntual en seguridad o análisis de vulnerabilidades (opcional).
Tiempo de dedicación interna	Horas hombre para ejecución, monitoreo y mejora continua del modelo.

El modelo ha sido diseñado para ser realista y adaptable, considerando el contexto de las PYMEs y su posible limitación de recursos. No requiere grandes inversiones iniciales ni tecnologías complejas, sino una combinación eficiente de personas, herramientas básicas y buenas prácticas. La correcta asignación y gestión de estos recursos permitirá la implementación progresiva del modelo, sin comprometer la operación diaria ni la sostenibilidad del negocio.

8.2 Fase Do: Desarrollo del modelo y propuesta técnica

La fase Do del ciclo PDCA corresponde a la implementación teórica del modelo de gestión de riesgos, estructurado previamente durante la fase de planificación. En esta etapa se materializa la propuesta mediante la definición de los componentes técnicos y operativos necesarios para poner en marcha el sistema de gestión de seguridad de la información, de acuerdo con los requisitos de la norma ISO/IEC 27001 y adaptado al contexto de las pequeñas y medianas empresas del sector T.I.

El desarrollo incluye la representación visual del modelo, la definición de políticas y procedimientos de seguridad, un plan de implementación progresivo, así como la selección de herramientas tecnológicas viables para organizaciones con recursos limitados. También se contempla una aproximación a posibles soluciones basadas en inteligencia artificial, con el fin de proyectar el modelo hacia escenarios más avanzados de gestión de incidentes.

Esta fase permite demostrar que el modelo no solo es teóricamente sólido, sino que también es técnicamente aplicable y escalable, ofreciendo a las PYMEs una hoja de ruta clara para fortalecer su postura de seguridad de la información de manera realista y sostenible.

8.2.1 Diagramas del modelo

Para facilitar la comprensión del modelo propuesto, se presentan a continuación dos diagramas que representan gráficamente su funcionamiento. Estas representaciones permiten visualizar el flujo de gestión de riesgos desde la identificación hasta la mejora continua, así como el ciclo de respuesta ante incidentes de seguridad de la información dentro de una PYME del sector T.I.

8.2.1.1 Flujo de gestión de riesgos

El flujo de gestión de riesgos propuesto sigue el enfoque metodológico del ciclo PDCA (Plan, Do, Check, Act) y está basado en los lineamientos de la norma ISO/IEC 27001. Este flujo guía la implementación de controles de seguridad a partir de la identificación y análisis de los activos de información críticos.

8.2.1.2 Ciclo de control y respuesta

El ciclo de control y respuesta define cómo actúa la organización ante un incidente de seguridad detectado. Este ciclo fortalece la fase de respuesta y recuperación, permitiendo contener, mitigar y aprender del evento para evitar su repetición.

8.2.2 Definición de políticas y procedimientos de seguridad

Como parte fundamental de la implementación del modelo de gestión de riesgos propuesto, se definen un conjunto de políticas y procedimientos de seguridad de la información que servirán como marco normativo interno para la organización. Estas políticas establecen las reglas básicas que deben ser cumplidas por todo el personal y orientan la aplicación de los controles técnicos y organizativos seleccionados.

La definición de políticas forma parte del dominio A.5 de la norma ISO/IEC 27001, que establece la necesidad de contar con lineamientos documentados, claros y comunicados, como base para garantizar la protección de los activos de información y el cumplimiento normativo.

8.2.2.1 Políticas de uso aceptable de los sistemas

- Define las condiciones bajo las cuales los empleados pueden acceder y utilizar los recursos informáticos (equipos, redes, software y servicios).
- Prohíbe expresamente el uso de sistemas para fines personales, actividades ilícitas o no autorizadas.
- Establece responsabilidades individuales sobre el uso adecuado de las credenciales y la protección de la información.

8.2.2.2 Políticas de respaldos y recuperación

- Establece la obligación de realizar copias de seguridad periódicas de los sistemas y bases de datos críticos.
- Define la periodicidad de los respaldos, el medio utilizado, la retención de copias y los procedimientos de restauración.
- Indica que los respaldos deben probarse de forma regular para garantizar su funcionalidad.

8.2.2.3 Política de gestión de incidentes de seguridad

- Define qué se considera un incidente de seguridad y establece el protocolo de notificación inmediata.
- Establece los roles y responsabilidades durante la atención de incidentes.
- Obliga a documentar todos los eventos, acciones realizadas y aprendizajes generados.

8.2.2.4 Procedimientos Operativos Relacionados

Para apoyar la ejecución de las políticas anteriores, se proponen los siguientes procedimientos:

Procedimiento	**Descripción**
Procedimiento para el cambio de contraseñas	Define cuándo y cómo los usuarios deben actualizar sus credenciales.
Procedimiento de reporte de incidentes	Detalla el canal de comunicación, el formato del reporte y los tiempos de respuesta esperados.
Procedimiento de recuperación desde backups	Instrucciones paso a paso para restaurar sistemas o datos ante una pérdida o incidente.

Procedimiento de alta/baja de usuarios	Proceso formal para crear o eliminar cuentas, asignar permisos y revocar accesos.

.

Estas políticas y procedimientos representan el marco operativo básico de seguridad de la información para la PYME, asegurando que las acciones del personal estén alineadas con los objetivos del modelo. Su implementación contribuye a reducir riesgos operacionales, mejorar la trazabilidad de los procesos y fomentar una cultura organizacional responsable y consciente en el manejo de la información.

8.2.3 Plan de implementación (teórico)

La implementación del modelo de gestión de riesgos requiere una planificación ordenada y realista, que permita aplicar los controles de forma progresiva, considerando los recursos técnicos, humanos y económicos de una pequeña o mediana empresa del sector T.I. A continuación, se plantea un plan de implementación teórico, diseñado para ejecutarse en un período estimado de 6 semanas, que puede ajustarse según la complejidad y madurez de cada organización.

Este plan contempla fases clave como la preparación organizativa, la ejecución técnica de controles y la capacitación del personal, buscando un equilibrio entre seguridad, operatividad y sostenibilidad.

Semana	**Actividad principal**	**Descripción**	**Responsable**
Semana 1	Revisión y aprobación de políticas	Presentar políticas internas de seguridad y obtener aval de la dirección.	Responsable de seguridad / Dirección

Semana 2	Clasificación de activos y asignación de roles	Identificar activos críticos, asignar responsables y documentar.	Administrador de TI
Semana 3	Configuración técnica inicial	Implementar copias de seguridad, configurar firewall y gestionar accesos.	Soporte técnico / Infraestructura
Semana 4	Implementación de controles organizativos y operativos	Activar autenticación 2FA, establecer procesos de reporte de incidentes y validación de accesos.	Responsable de seguridad
Semana 5	Capacitación al personal	Realizar talleres de concientización y simulacros de incidentes.	Área de seguridad / Dirección

Semana 6	Evaluación inicial y retroalimentación del modelo	Medir el cumplimiento de controles, analizar debilidades y proponer ajustes iniciales.	Comité de seguridad / Dirección

- El plan está diseñado para permitir una implementación rápida pero funcional, enfocándose en controles críticos.

- Se recomienda realizar un seguimiento semanal mediante reuniones cortas de avance.

- El resultado de la semana 6 debe alimentar la fase “Check” del ciclo PDCA.

Este plan de implementación ofrece a la empresa una hoja de ruta clara y alcanzable para aplicar el modelo de gestión de riesgos, facilitando el cumplimiento progresivo con la norma ISO/IEC 27001. Su enfoque escalable y práctico permite que incluso organizaciones con recursos limitados puedan iniciar un proceso formal de mejora de su seguridad de la información.

8.2.4 Propuesta tecnológica

La propuesta tecnológica del modelo de gestión de riesgos tiene como objetivo seleccionar y recomendar herramientas que permitan implementar los controles técnicos definidos en el modelo, garantizando la protección de los activos de información críticos de una PYME del sector T.I.

- La elección de las soluciones se basa en criterios de:

- Compatibilidad con entornos pequeños y medianos.

- Bajo costo o código abierto (open source).

- Facilidad de implementación y mantenimiento.

- Cobertura de los controles definidos por ISO/IEC 27001.

8.2.4.1 Herramientas o componentes tecnológicos recomendados

Categoría	**Herramienta / Tecnología**	**Función principal**	**Justificación**
Firewall	pfSense u OPNsense	Control del tráfico entrante y saliente, segmentación de red.	Gratuito, robusto y con interfaz amigable.
Antivirus / EDR	ClamAV, Windows Defender, CrowdStrike Falcon (freemium)	Protección contra malware y amenazas internas.	Soluciones livianas, automatizables y efectivas.
Gestión de respaldos	Restic o Duplicati	Realización de copias de seguridad automáticas, cifradas y programables.	Software libre, eficiente y fácil de configurar.
Gestión de accesos	Autenticación 2FA (Google Authenticator, Authy, Authelia)	Fortalecimiento de la autenticación a servicios internos o en la nube.	Implementación sencilla, multiplataforma.

Monitoreo de red	Nagios, Zabbix, Wireshark	Supervisión de disponibilidad de servicios, análisis de tráfico y detección de fallos.	Soluciones ampliamente adoptadas en entornos PYME.
Detección de amenazas	Wazuh (SIEM + IDS)	Integración de alertas de seguridad, detección de eventos anómalos.	Gratuito, escalable y compatible con entornos Linux/Windows.
Gestión documental	Nextcloud + OnlyOffice	Almacenamiento seguro de políticas, manuales y reportes de incidentes.	Almacenamiento cifrado y colaboración en línea.

8.2.4.2 Alineación con controles ISO/IEC 27001

Estas tecnologías permiten cubrir directamente varios de los controles seleccionados en el modelo, como:

- A.12.3.1 – Copias de respaldo → (Restic, Duplicati)
- A.13.1.1 – Protección en tránsito → (VPN + HTTPS + Firewall)
- A.9.4.1 – Autenticación segura → (2FA con Authenticator o Authelia)
- A.12.6.1 – Gestión de vulnerabilidades → (Wazuh + actualizaciones programadas)
- A.16.1.1 – Gestión de incidentes → (SIEM / Reportes en Nextcloud)

La propuesta tecnológica presentada proporciona una base sólida y asequible para que una PYME implemente controles eficaces sin necesidad de adquirir soluciones costosas. Estas herramientas permiten construir un entorno más seguro, confiable y resiliente, facilitando el cumplimiento con los principios de ISO 27001 y adaptándose a la realidad de organizaciones en crecimiento.

8.2.5 Desarrollo de la página web como medio de difusión del modelo

Como parte del cumplimiento del objetivo específico de desarrollar una página web en donde se plasme el modelo, las recomendaciones y el plan de acción generado a lo largo del proyecto, se diseñó una solución digital de tipo demostrativo que permite visualizar, de manera clara y estructurada, los componentes centrales del modelo de gestión de riesgos propuesto para PYMEs del sector T.I.

La finalidad de esta herramienta es facilitar la comprensión e implementación del modelo, mediante una interfaz intuitiva que organiza la información en secciones clave como: introducción al modelo, identificación de activos, controles sugeridos, cronograma de implementación, políticas de seguridad, recomendaciones y mejora continua. De esta forma, se ofrece a las pequeñas y medianas empresas una referencia práctica y accesible que sirve tanto como material de consulta como de guía para llevar el modelo a la práctica.

La página fue construida utilizando tecnologías web de fácil implementación (HTML, CSS, JavaScript y/o frameworks ligeros), con un diseño responsivo y adaptable a distintos dispositivos. Aunque no busca sustituir una solución empresarial avanzada, sí cumple con el objetivo de presentar de forma visual y navegable los resultados obtenidos en el desarrollo del proyecto, fomentando su apropiación y replicabilidad.

Específicamente fue desarrollada en el Framework Angular con la última versión a la fecha V 19.2.0.

Se estructuró con base en la metodología PDCA utilizando un diseño sobrio y organizado que pueda adaptarse a cualquier organización.

Al ingresar lo primero que se va a encontrar es el HomePage que da una breve introducción al modelo:

Figura 1. Home Page.

Cada una de las opciones se presenta de manera organizada y segmentada.

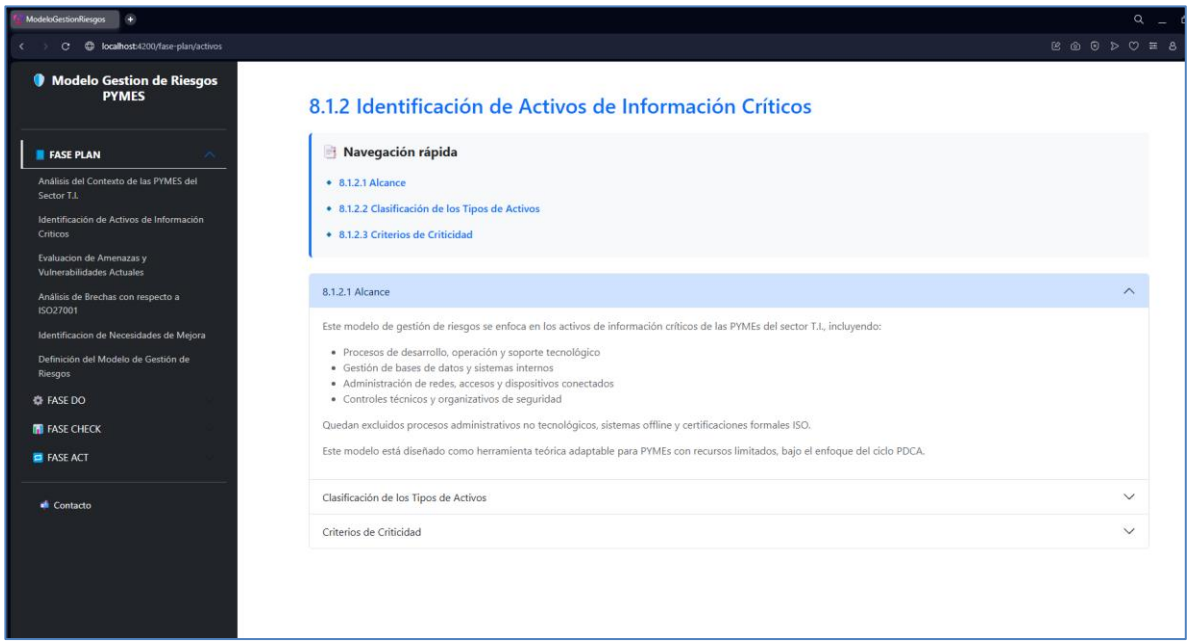

Figura 2. Pagina Activos.

El Side Bar menú se estructuro siguiendo la metodología PDCA.

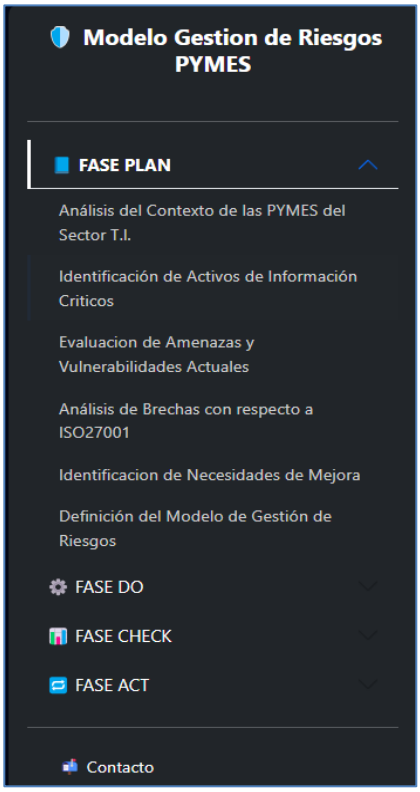

Figura 1. Sidebar Opcion 1.

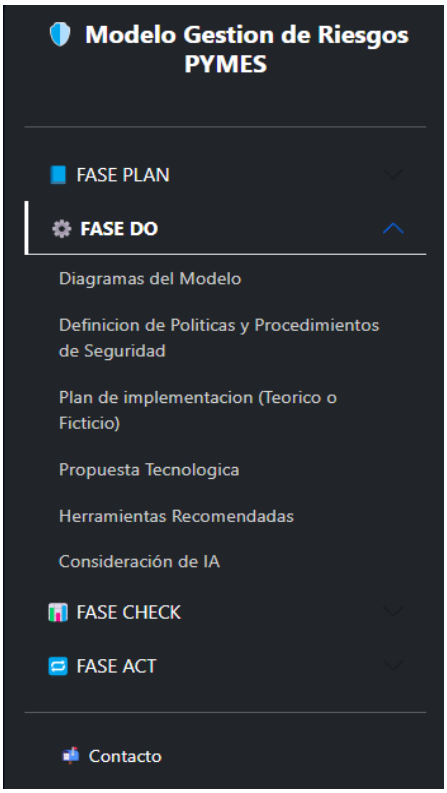

Figura 2 Sidebar Opción 2

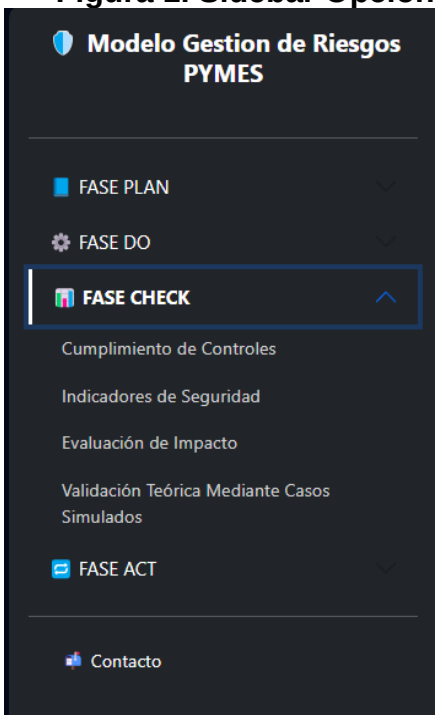

Figura 3. Sidebar Opcion 3

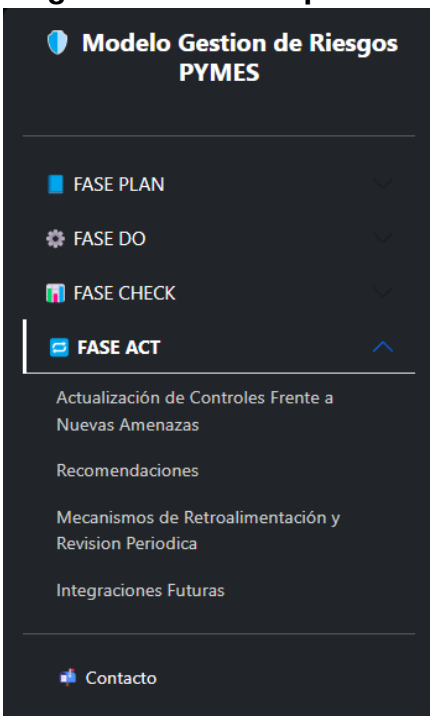

Figura 4.Sidebar Opcion 4

8.3 FASE CHECK: Evaluación del modelo

Esta fase tiene como finalidad realizar la verificación del cumplimiento, efectividad e impacto del modelo propuesto en función de los controles definidos, los objetivos establecidos y los riesgos previamente identificados. A través del análisis de cumplimiento, la definición de indicadores, la evaluación de impacto y la simulación teórica de casos, se busca determinar si el modelo responde adecuadamente a las necesidades de una PYME del sector T.I. en términos de seguridad de la información.

8.3.1 Análisis de cumplimiento de controles propuestos

Una vez definidos los controles de seguridad basados en el Anexo A de la norma ISO/IEC 27001, se realizó un análisis de cumplimiento teórico para verificar la viabilidad de implementación de cada uno en el contexto de una pequeña o mediana empresa del sector T.I. Esta evaluación busca determinar en qué medida los controles propuestos cubren efectivamente los riesgos identificados y si su aplicación es factible con recursos limitados.

La evaluación considera tres criterios:

- Aplicabilidad teórica: ¿Puede una PYME aplicar este control con los recursos y condiciones que posee?

- Cobertura de riesgo: ¿El control cumple con mitigar el riesgo para el cual fue propuesto?

- Nivel de cumplimiento estimado: Grado en el que la empresa, de manera teórica, lograría implementar ese control en su operación real.

Control ISO 27001	**Riesgo que mitiga**	**Aplicabilidad Teórica en PYMEs**	**Cobertura del Riesgo**	**Nivel de Cumplimiento Estimado**
A.5.1.1 – Política de seguridad	Falta de lineamientos y cultura de seguridad	Alta	Alta	Parcial (requiere documentación formal)

A.6.1.1 – Roles y responsabilidades	Ausencia de responsables de seguridad	Alta	Alta	Alta
A.7.2.2 – Formación y concientización	Riesgo por errores humanos o ingeniería social	Alta	Media	Parcial (requiere tiempo y capacitación continua)
A.9.2.1 – Gestión de cuentas	Accesos no autorizados	Alta	Alta	Alta
A.9.4.1 – Autenticación segura (2FA)	Suplantación, phishing	Media	Alta	Parcial (depende de herramientas utilizadas)
A.12.3.1 – Copias de respaldo	Pérdida de información o ransomware	Alta	Alta	Alta
A.12.6.1 – Gestión de vulnerabilidades	Ataques por software desactualizado	Alta	Alta	Parcial (requiere procesos constantes)
A.13.1.1 – Protección en tránsito	Intercepción de datos	Media	Alta	Parcial (requiere cifrado en herramientas)
A.13.2.3 – Segmentación de redes	Movimiento lateral de amenazas	Media	Media	Parcial (requiere configuración técnica)

A.14.2.1 – Validación de entradas	Inyección SQL / corrupción de datos	Alta	Alta	Alta
A.16.1.1 – Gestión de incidentes	Falta de respuesta ante eventos de seguridad	Alta	Alta	Parcial (requiere protocolo definido y cultura de reporte)
A.18.1.4 – Evaluación periódica de riesgos	Desactualización del modelo ante nuevas amenazas	Alta	Alta	Alta

Este análisis muestra que, desde una perspectiva teórica, la mayoría de los controles propuestos son altamente aplicables y relevantes para el entorno de una PYME del sector T.I. No obstante, algunos controles requieren ajustes operativos, capacitación del personal o herramientas mínimas adicionales para alcanzar una implementación completa.

La naturaleza progresiva y adaptable del modelo permite que la implementación de los controles se realice por fases, comenzando con aquellos de mayor impacto y menor complejidad técnica. Esta estrategia asegura que incluso organizaciones con recursos limitados puedan iniciar un proceso sólido y sostenible de gestión de riesgos, conforme a las mejores prácticas de seguridad de la información.

8.3.2 Indicadores de seguridad planteados

Con el fin de evaluar la eficacia del modelo de gestión de riesgos propuesto, se han definido una serie de indicadores clave de seguridad de la información (KPIs) que permiten medir el desempeño de los controles implementados, así como identificar áreas de mejora y realizar seguimiento a la evolución del sistema.

Estos indicadores han sido seleccionados considerando:

- La viabilidad de medición en una PYME con recursos limitados.
- Su relevancia frente a los objetivos del modelo.

- La relación directa con los controles propuestos y los riesgos que se busca mitigar.

La siguiente tabla presenta los indicadores sugeridos, su propósito y forma de medición.

Indicador	**Descripción**	**Unidad de Medida**	**Frecuencia sugerida**
% de controles implementados	Mide el avance en la ejecución del modelo de seguridad	Porcentaje	Trimestral
% de incidentes reportados y documentados	Evalúa la capacidad de detección y la cultura de reporte en la organización	Porcentaje mensual	Mensual
Tiempo promedio de respuesta ante incidentes	Mide la agilidad del equipo frente a un evento de seguridad	Horas / minutos	Por evento
% de copias de seguridad verificadas	Evalúa la confiabilidad de los respaldos ejecutados	Porcentaje	Mensual

% de usuarios capacitados	Mide el alcance de las acciones de formación en seguridad	Porcentaje del personal	Semestral
Frecuencia de evaluación de riesgos	Evalúa si el modelo se actualiza periódicamente frente a nuevas amenazas	Número de evaluaciones realizadas	Anual
% de autenticaciones seguras implementadas	Mide la adopción de 2FA u otros mecanismos seguros de acceso	Porcentaje	Trimestral

Estos indicadores están pensados para que puedan ser monitoreados sin necesidad de herramientas complejas. Su implementación se puede realizar mediante hojas de cálculo, reportes internos y registros de actividades. En fases posteriores, pueden integrarse a sistemas más avanzados de monitoreo si la organización evoluciona.

La medición constante de estos indicadores permitirá a la empresa:

- Verificar si los controles están funcionando como se espera.
- Detectar desviaciones o debilidades en el modelo.
- Tomar decisiones informadas para mejorar la seguridad.

La definición e implementación de indicadores de seguridad constituye un componente esencial dentro del modelo de gestión propuesto, ya que permite establecer un sistema de retroalimentación objetiva y medible que contribuye al ciclo de mejora continua (PDCA). Además, estos indicadores fortalecen la capacidad de la empresa para anticiparse a

incidentes y evaluar su madurez en seguridad de la información con base en evidencia real.

8.3.3 Evaluación de impacto

La implementación de un modelo de gestión de riesgos en seguridad de la información conlleva múltiples impactos en la organización. Esta sección analiza, desde una perspectiva teórica, los efectos esperados del modelo propuesto en diferentes dimensiones de la empresa: técnica, operativa, económica, organizacional y legal.

Dado que el modelo está diseñado para ser adaptable, de bajo costo y escalable, sus beneficios pueden observarse progresivamente a medida que los controles son implementados y los procesos fortalecidos.

Dimensión	**Impacto Esperado**
Técnico	Mejora en la protección de los activos tecnológicos (bases de datos, redes, sistemas), reducción de fallos y vulnerabilidades técnicas. Fortalecimiento de la seguridad perimetral y operativa.

Operativo	Mayor estabilidad en los procesos de TI, claridad en los procedimientos de respaldo, gestión de accesos e incidentes. Disminución de interrupciones por eventos de seguridad.

Económico	Disminución de pérdidas por incidentes cibernéticos, reducción de costos por recuperación de datos, menor dependencia de soluciones externas de alto costo. Optimización de recursos internos.

Organizacional	Mayor conciencia del personal frente a la seguridad, definición clara de roles y responsabilidades, fomento de la cultura de prevención. Mejora de la comunicación y colaboración interdepartamental.

Legal / Normativo	Mejora en el cumplimiento de normativas de protección de datos y estándares internacionales como ISO/IEC 27001. Reducción del riesgo legal ante filtraciones o incidentes de seguridad.

La implementación del modelo tiene un impacto positivo en todas las dimensiones estratégicas de una PYME del sector T.I., especialmente en lo técnico, operativo y organizacional. Estos beneficios no solo contribuyen a reducir la exposición a amenazas y vulnerabilidades, sino que además mejoran la resiliencia digital, optimizan procesos y fortalecen la imagen y la confianza hacia clientes, socios y usuarios.

Este impacto teórico justifica plenamente la propuesta del modelo, reforzando su aplicabilidad en entornos reales y su alineación con buenas prácticas internacionales en seguridad de la información.

8.3.4 Validación teórica mediante casos simulados

Para validar teóricamente la efectividad del modelo propuesto, se plantea un caso simulado en una PYME ficticia del sector T.I., con el fin de observar cómo respondería la organización ante un incidente de seguridad utilizando los controles seleccionados y las fases definidas en el modelo de gestión basado en ISO/IEC 27001 y el ciclo PDCA.

Este ejercicio permite verificar si el modelo responde adecuadamente al riesgo, si los controles funcionan como se espera y si los procedimientos permiten mitigar el impacto del incidente de forma eficaz.

8.3.4.1 Escenario de simulación

- Empresa simulada: Las Mercedes SoftDev S.A.S. – PYME de desarrollo de software, con 20 empleados, datos sensibles de clientes y servidores en la nube.
- Activo afectado: Base de datos de clientes.
- Amenaza: Acceso no autorizado mediante credenciales comprometidas.
- Vulnerabilidad: Falta de autenticación en dos pasos (2FA) y ausencia de monitoreo de accesos.
- Incidente simulado: Un atacante externo accede al CRM utilizando credenciales filtradas y extrae información confidencial.

8.3.4.2 Aplicación del modelo en el caso simulado

Fase del modelo (PDCA)	**Acción realizada**	**Control aplicado (ISO 27001)**
Plan	Se identificó el activo (base de datos), la amenaza (acceso externo) y la vulnerabilidad (falta de 2FA).	A.9.2.1 / A.9.4.1

Do	Se activó el plan de respuesta, se bloqueó el acceso sospechoso y se restauró la base de datos desde el último respaldo.	A.12.3.1 / A.16.1.1
Check	Se documentó el incidente, se evaluó el tiempo de respuesta y se verificó que el respaldo fue exitoso.	A.18.1.4 / A.12.3.1
Act	Se implementó 2FA, se capacitó al personal sobre el incidente y se programaron evaluaciones periódicas de riesgos.	A.7.2.2 / A.18.1.4

8.3.4.3 Resultados esperados

- Tiempo de recuperación estimado: 2 horas.
- Impacto del incidente reducido: gracias al respaldo y la respuesta rápida.
- Aprendizaje organizacional generado: mayor conciencia sobre la gestión de accesos y la importancia del monitoreo.
- Controles fortalecidos tras el incidente: se implementaron medidas adicionales de prevención.

El caso simulado permite validar que el modelo propuesto funciona de forma coherente y efectiva ante un incidente realista, integrando de manera estructurada la identificación, respuesta, recuperación y mejora continua. Aunque no fue implementado en un entorno real, el ejercicio teórico demuestra que el modelo puede ser aplicable, útil y escalable en PYMEs del sector T.I., cumpliendo con los principios fundamentales de ISO/IEC 27001.

8.4 FASE ACT: Plan de mejora continua

La fase ACT representa el último componente del ciclo PDCA y tiene como finalidad consolidar una cultura de mejora continua en la gestión de la seguridad de la información dentro de la organización. A partir de los resultados obtenidos en la fase de verificación (CHECK), se identifican oportunidades de mejora, ajustes necesarios y acciones correctivas que permitan optimizar la eficacia del modelo propuesto y adaptarlo a nuevos riesgos, cambios tecnológicos o necesidades del negocio.

Esta fase es fundamental para asegurar que el sistema de gestión de riesgos no se mantenga estático, sino que evolucione en función del aprendizaje organizacional, los incidentes registrados, los cambios en la infraestructura y las evaluaciones periódicas. A través del plan de mejora continua, se garantiza que los controles sigan siendo pertinentes, los procesos se fortalezcan y los indicadores de seguridad mantengan su tendencia positiva.

En esta sección se presenta una propuesta de acciones concretas, responsables, recursos requeridos y frecuencia de revisión, con el objetivo de mantener la eficacia y sostenibilidad del modelo a largo plazo, en coherencia con los principios de la norma ISO/IEC 27001.

8.4.1 Propuesta para actualizar controles frente a nuevas amenazas

La seguridad de la información es un campo dinámico y en constante evolución. A medida que surgen nuevas amenazas, vulnerabilidades o vectores de ataque, es fundamental que el modelo de gestión de riesgos sea flexible y actualizado regularmente para mantener su efectividad.

En este sentido, el presente modelo contempla la actualización periódica de los controles como parte de su estrategia de mejora continua. Esta actualización debe ser reactiva y proactiva, es decir, debe responder a incidentes ocurridos y también anticiparse a potenciales riesgos emergentes, manteniendo una vigilancia constante del entorno tecnológico.

Aspecto a revisar	**Acción recomendada**	**Frecuencia**	**Responsable**
Nuevas amenazas cibernéticas	Monitorear boletines de seguridad, fuentes oficiales (CERT, OWASP, MITRE, etc.)	Mensual	Responsable de seguridad
Tecnología e infraestructura	Revisar compatibilidad y vulnerabilidades en nuevas herramientas y sistemas	Por cada actualización	Administrador de TI

Controles aplicados	Evaluar si los controles actuales siguen siendo eficaces ante el entorno actual	Trimestral	Responsable de seguridad
Cambios internos en la empresa	Revisar impacto de nuevos procesos, personal o servicios digitales en el modelo	Según necesidad	Dirección y área de TI
Normativas y estándares externos	Verificar si hay cambios en ISO 27001 u otras regulaciones aplicables	Anual	Responsable de cumplimiento

8.4.1.1 Controles sujetos a actualización frecuente (ejemplos clave)

- A.9.4.1 – Autenticación segura: incorporar autenticación biométrica o tokens físicos si el riesgo de suplantación crece.
- A.12.6.1 – Gestión de vulnerabilidades: incluir herramientas automáticas de escaneo si aumenta el riesgo por software no actualizado.
- A.16.1.1 – Reporte de incidentes: adaptar los flujos de reporte a nuevas plataformas colaborativas (como apps de notificación interna).
- A.13.1.1 – Cifrado de información en tránsito: actualizar algoritmos de cifrado si se detecta obsolescencia o riesgo de ruptura.

La actualización de controles frente a nuevas amenazas garantiza que el modelo no pierda vigencia ni eficacia. Incluir este proceso dentro del ciclo de mejora continua permite que la PYME mantenga una postura de seguridad proactiva y resiliente, respondiendo con agilidad a los cambios del entorno y reforzando la confianza en su infraestructura tecnológica.

8.4.2 Recomendaciones para mantener el modelo vigente

Para que el modelo de gestión de riesgos en seguridad de la información mantenga su relevancia, aplicabilidad y efectividad a largo plazo, es indispensable implementar una serie de acciones sistemáticas que garanticen su actualización continua y su alineación con el entorno tecnológico, organizacional y normativo.

Dado que las amenazas evolucionan constantemente y las PYMEs experimentan cambios operativos frecuentes, estas recomendaciones permiten que el modelo se adapte a las necesidades del negocio sin perder su estructura ni su alineación con la norma ISO/IEC 27001.

Recomendación	**Objetivo**
Realizar evaluaciones de riesgos periódicas (al menos una vez al año)	Detectar nuevos activos, amenazas emergentes y vulnerabilidades internas.
Actualizar el inventario de activos de información	Reflejar cambios en infraestructura, software, servicios o personal con acceso a datos.

Monitorear cambios en la normativa aplicable (ISO 27001, legislación local)	Mantener el modelo alineado a las mejores prácticas y evitar sanciones por incumplimiento.
Documentar y revisar políticas y procedimientos regularmente	Asegurar que las políticas sigan siendo pertinentes, claras y entendibles para los usuarios.
Ejecutar simulacros o pruebas de respuesta a incidentes	Evaluar la preparación operativa y mejorar los tiempos de reacción ante eventos reales.
Capacitar al personal de forma continua	Fortalecer la cultura organizacional de seguridad y reducir el riesgo por errores humanos.

Medir indicadores de seguridad establecidos	Identificar tendencias, detectar desviaciones y tomar decisiones basadas en datos.

Se recomienda establecer un proceso de revisión formal del modelo cada 12 meses, o en caso de:

- Cambios estructurales en la empresa (crecimiento, fusión, nuevas sedes).
- Adopción de nuevas tecnologías críticas.
- Incidentes de seguridad relevantes.
- Cambios regulatorios o legales.

Esta revisión debe incluir la participación de al menos: el responsable de seguridad, el administrador de TI, y un representante de la alta dirección.

La vigencia del modelo no depende únicamente de su diseño, sino de la capacidad de la organización para sostenerlo, adaptarlo y mejorarlo de forma constante. Aplicar estas recomendaciones garantiza que el modelo continúe siendo útil, relevante y coherente con el entorno de una PYME del sector T.I., fortaleciendo su resiliencia y nivel de madurez en seguridad de la información.

8.4.3 Mecanismos de retroalimentación y revisión periodica

La sostenibilidad de un modelo de gestión de riesgos depende en gran medida de su capacidad para ser monitoreado, evaluado y ajustado de manera continua. Por ello, esta propuesta contempla una estrategia de seguimiento y revisión periódica, orientada a asegurar que los controles, procedimientos y políticas permanezcan alineados con los objetivos de la organización y con el entorno cambiante de la seguridad de la información.

Esta estrategia responde a los principios de mejora continua establecidos en la fase ACT del ciclo PDCA, así como a los requisitos de revisión y mantenimiento del SGSI indicados en la norma ISO/IEC 27001.

Elemento	Descripción	Frecuencia sugerida
Evaluación de cumplimiento de controles	Verificación del estado de implementación y efectividad de los controles establecidos.	Trimestral o semestral
Revisión de indicadores de seguridad	Análisis de los KPIs definidos para detectar desviaciones o mejoras.	Trimestral
Auditoría interna (formal o informal)	Revisión técnica y documental del modelo, procedimientos y registros.	Anual
Encuestas o feedback del personal	Recopilación de percepciones y sugerencias de los usuarios involucrados en el modelo.	Semestral

Reunión de análisis y decisiones	Espacio formal para revisar hallazgos y definir ajustes o nuevas acciones.	Anual o post-incidente
Actualización del plan de acción	Ajustes a los controles, responsabilidades o prioridades del modelo según nuevas necesidades.	Según resultados de la revisión

8.4.3.1 Ciclo sugerido para la revisión del modelo

1. Recolectar información: a partir de reportes de incidentes, indicadores, encuestas, auditorías.

2. Evaluar resultados: comparar con objetivos, analizar desviaciones y oportunidades.

3. Definir mejoras: ajustar controles, actualizar documentación, incorporar nuevas herramientas o procedimientos.

4. Aprobar y aplicar los cambios: con participación del responsable de seguridad y la dirección.

5. Volver a evaluar: iniciar un nuevo ciclo en el marco del PDCA.

Una estrategia clara de seguimiento y revisión permite mantener el modelo vivo, actualizado y adaptable. Este proceso continuo fortalece la capacidad de la organización para anticiparse a las amenazas, responder con mayor eficacia, y asegurar que el modelo

siga cumpliendo su propósito de proteger los activos de información, incluso en contextos de cambio.

8.5 Cronograma

	Nombre	Duración	Inicio
1	Definir objetivos y alcances del proyecto.	7 días.	11/02/2025
2	Investigar y recopilar información sobre el sector de T.I. y las necesidades de seguridad perimetral para medianas y pequeñas empresas	7 días.	11/02/2025
3	Evaluar la gestión de riesgos de seguridad de la información en pequeñas y medianas empresas de TI con base en estándares ISO 27000.	4 días.	18/02/2025
4	Identificar las vulnerabilidades de información para el diseño del método de evaluación de riesgos en la seguridad de la información.	3 días.	24/02/2025
5	Definir el modelo de seguridad que permita controlar las vulnerabilidades y amenazas que se presenten en las pequeñas y medianas empresas	7 días.	06/03/2025
6	Diseñar una estrategia para la gestión de riesgos.	7 días.	18/03/2025
7	Hacer una lista de herramientas recomendadas para crear un plan de acción ajustado a las condiciones de seguridad de cada empresa.	7 días.	28/03/2025
8	Crear la arquitectura del modelo de implementación basado en un caso real para iniciar la implementación de controles de seguridad perimetral.	7 días.	08/04/2025
9	Desarrollar la primera versión del modelo de gestión de riesgos.	7 días.	18/03/2025
10	Realizar pruebas iniciales de funcionalidad y compatibilidad.	7 días.	28/03/2025
11	Integrar el modelo de gestión de riesgos con soluciones de seguridad perimetral existentes.	7 días.	08/04/2025
12	Realizar pruebas de integración y compatibilidad.	4 días.	15/04/2025
13	Refinar y mejorar la versión inicial del modelo de gestión de riesgos.	3 días.	21/04/2025
14	Implementar nuevas características y funcionalidades.	4 días.	28/04/2025
15	Desarrollar la documentación y el material de capacitación para el modelo de gestión de riesgos.	7 días.	08/05/2025

16	Diseñar un plan de implementación y adopción del modelo de gestión de riesgos para medianas y pequeñas empresas del sector de T.I.	7 días.	20/05/2025
17	Monitorear el desempeño y la retroalimentación del modelo de gestión de riesgos.	3 días.	26/05/2025
18	Identificar oportunidades de mejora y nuevas características para futuras versiones.	1 días.	28/05/2025
19	Presentar los resultados del proyecto y el modelo de gestión de riesgos finalizado.	1 días.	30/05/2025
20	Evaluar el éxito del proyecto y planificar futuros proyectos y mejoras para el modelo de gestión de riesgos.	2 días.	03/06/2025

Tabla 1. Cronograma de ejecución del proyecto. Elaboración propia.

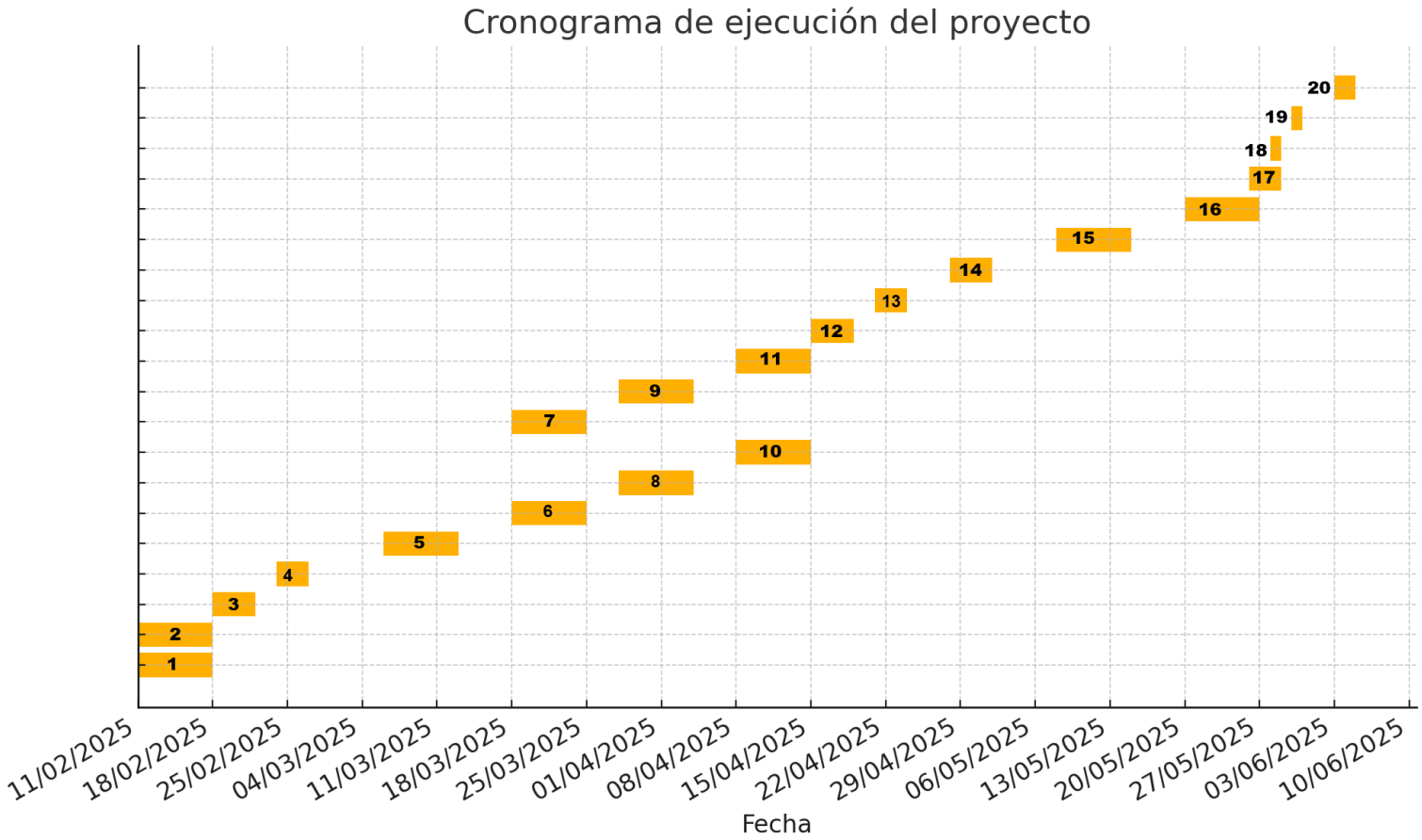

Figura 3. Cronograma de ejecución del proyecto. Elaboración propia.

CONCLUSIONES

1. Se logró cumplir con el objetivo general del proyecto, al plantear un modelo de gestión de riesgos para pequeñas y medianas empresas del sector T.I., alineado con los principios y controles de la norma ISO/IEC 27001. El modelo fue estructurado bajo el enfoque del ciclo PDCA, permitiendo organizar de forma sistemática las fases de identificación, evaluación, control y mejora de la seguridad de la información.
2. A través del análisis del contexto interno y externo de las PYMEs del sector T.I., se pudo evidenciar una alta exposición a riesgos digitales, acompañada de limitaciones en infraestructura, cultura de seguridad, personal especializado y recursos. Esto justificó la necesidad de una solución adaptada a su realidad operativa.
3. Con base en la ISO 27001, se identificaron las vulnerabilidades más comunes que afectan a este tipo de empresas, tales como accesos no controlados, falta de respaldos verificados, ausencia de políticas de seguridad, poca formación del personal y falta de gestión de incidentes. Estas debilidades fueron clave para la selección de los controles propuestos.
4. Se propuso un modelo de seguridad estructurado y progresivo, compuesto por 12 controles seleccionados del Anexo A de la norma ISO/IEC 27001, priorizados según la viabilidad de implementación en contextos con recursos limitados. El modelo plantea medidas técnicas, organizativas y formativas para mitigar amenazas como pérdida de datos, accesos no autorizados, ransomware o suplantación.
5. Se analizaron herramientas y mecanismos clave para la implementación de los controles, incluyendo soluciones tecnológicas básicas, definición de roles internos, indicadores de seguridad y estrategias de capacitación continua. Esto contribuye a la optimización de recursos y al fortalecimiento de la respuesta ante incidentes.
6. Se elaboró una propuesta de plan de acción y mejora continua, que permite mantener el modelo actualizado frente a nuevas amenazas, cambios tecnológicos o crecimiento organizacional. La fase ACT garantiza que el sistema no pierda vigencia y siga alineado con los objetivos de la empresa.
7. Finalmente, se desarrolló una validación teórica mediante un caso simulado, que permitió comprobar que el modelo funciona de forma efectiva en un escenario realista, logrando reducir el impacto del incidente, responder organizadamente y generar aprendizaje organizacional.

RECOMENDACIONES

1. Implementar el modelo de forma gradual, iniciando con los controles de mayor impacto y menor complejidad técnica. Esto permitirá a las PYMEs avanzar progresivamente en la madurez de su gestión de riesgos sin comprometer la operación ni requerir grandes inversiones iniciales.
2. Documentar formalmente políticas, roles y procedimientos, incluso en organizaciones pequeñas. La documentación básica garantiza la trazabilidad, facilita el cumplimiento normativo y fortalece la cultura organizacional en torno a la seguridad.
3. Incluir la seguridad de la información como un eje estratégico, y no únicamente como una responsabilidad técnica. La participación de la alta dirección es clave para asignar recursos, validar decisiones y promover una cultura de seguridad desde el liderazgo.
4. Establecer un plan de formación continua en seguridad de la información para todo el personal. Capacitar a los usuarios ayuda a reducir los riesgos humanos, especialmente en escenarios de ingeniería social, errores operativos o mala gestión de credenciales.
5. Revisar y actualizar el modelo de gestión periódicamente, considerando cambios en el entorno tecnológico, nuevas amenazas, adopción de herramientas digitales o cambios organizacionales. Esta acción debe formar parte del ciclo de mejora continua propuesto (PDCA).
6. Incluir simulacros y ejercicios de prueba como parte del proceso de evaluación y aprendizaje. La práctica fortalece la capacidad de respuesta ante incidentes reales y permite detectar debilidades no visibles en la planificación teórica.
7. Aprovechar herramientas tecnológicas accesibles (como backups en la nube, autenticación en dos pasos, software antivirus y cifrado básico) que no requieren grandes inversiones pero pueden fortalecer significativamente la postura de seguridad.
8. Finalmente, se recomienda que futuros proyectos consideren una implementación práctica del modelo en una empresa real, para validar de forma empírica su aplicabilidad, recopilar métricas y enriquecer el enfoque con datos del entorno operativo.

BIBLIOGRAFÍA

- MINTIC. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. (6, noviembre, 2016). [Consultado el 2, mayo, 2023]. Disponible en Internet: <https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf>.

- TAPIERO TAPIERO, HAWIN ANDREI y SUAREZ RAMIREZ, HEINER. MODELO DE GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN EN EMPRESAS DEL SECTOR ASEGURADOR UTILIZANDO LA NORMA ISO/IEC 27005. (2017). [Consultado el 2, mayo, 2023]. Disponible en Internet: <https://repository.udistrital.edu.co/bitstream/handle/11349/8322/TapieroTapieroHawinAndrei2019.pdf?sequence=1&isAllowed=y>.

- CAMARGO, Erney Alberto Ramírez; PINZON, Miguel Alberto Rinconc. La importancia de la seguridad de la información en el sector público en Colombia. Revista Ibérica de Sistemas e Tecnologias de Informação, 2022, no 46, p. 87-99.

- AREITIO BERTOLÍN, Javier. Seguridad de la información. Redes, informática y sistemas de información. Ediciones Paraninfo, SA, 2008.

- BOCANEGRA DIAZ, Fabian Enrique, et al. Aplicativo para la gestión de incidentes de seguridad de la información en aplicaciones, basado en la NTC-ISO/IEC 27002-27035. Para el caso de uso de la Universidad Distrital.

- ARÉVALO ASCANIO, José Gregorio; BAYONA TRILLOS, Ramón Armando; RICO BAUTISTA, Dewar Willmer. Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. Tecnura, 2015, vol. 19, no 46, p. 123-134.

- ROCHA, Diego, et al. DEFINICIÓN DE UN MODELO DE SEGURIDAD PARA LA RED DE INVESTIGACIÓN DE TECNOLOGÍA AVANZADA DE LA UNIVERSIDAD DISTRITAL “FRANCISCO JOSÉ DE CALDAS” RITA-UD. Redes de Ingeniería, 2011, vol. 2, no 1, p. 113-120.

- TORRES MORALES, SANDRA MILENA y ROJAS CRUZ, JEIMY LORENA. MODELO DE GESTIÓN DE RIESGOS APLICANDO METODOLOGÍA OCTAVE ALLEGRO EN ENTIDADES DEL SECTOR FIDUCIARIO. (2017). [Consultado el 2, mayo, 2023]. Disponible en Internet: <https://repository.udistrital.edu.co/bitstream/handle/11349/6607/TorresMoralesSandraMilena2017.pdf?sequence=1&isAllowed=y>.

- ARÉVALO ASCANIO, José Gregorio; BAYONA TRILLOS, Ramón Armando; RICO BAUTISTA, Dewar Willmer. Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. Tecnura, 2015, vol. 19, no 46, p. 123-134.

- VELASQUEZ-PÉREZ, Torcoroma; CASTRO-SILVA, Hugo Fernando; PÉREZ-PÉREZ, Yesica María. Modelo de gestión de riesgos en proyectos. Aproximación conceptual para proyectos de TI. Revista Ingenio, 2015, vol. 8, no 1, p. 93-100.

- ESPERANZA, Becerra Arias Flor, et al. Diseño de un modelo de gestión de seguridad de la información basado en el estándar ISO 27001: 2013 para la gestión de la información para el caso de estudio Empresa QWERTY SA.

- VILLON GUERRERO, Pablo Leonardo. Modelo de gestión de riesgos para seguridad informática bajo ISO/IEC 27001: 2013 en empresa de entretenimiento y juegos de azar, Lima-2021. 2021.

- MORALES, Mauro Néstor Zevallos. Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte. Revista peruana de computación y sistemas, 2019, vol. 2, no 2, p. 43-60.

- FERNÁNDEZ VARGAS, Alberto Junior; MAYTA AGUILAR, Joel Ricardo. Diseño de un Modelo Sistémico de Gestión de Riesgos de la Seguridad de la Información, Integrando la Metodología Magerit y la Norma ISO 27002: 2013 en Empresas Financieras. 2017.

- COSSIO LUGO, Ricardo Fabio, et al. Diseño de un modelo de gestión de incidentes de seguridad de un SGSI basado en ISO 27001 dentro de una mesa de servicios de TI. 2017.

- CÓRDOVA SALINAS, José María; REMICIO CANALES, Wilian Eusebio. Modelo del Sistema de Gestión de Seguridad de la Información basado en la ISO 27001: 2013 para minimizar los riesgos de seguridad en el área de sistemas de la empresa Quantify Agency. 2022.

- PERUGACHI ESPINOSA, Cristian Alfonso. Modelo de seguridad de gestión de la información basado en la norma ISO 27001, para el data-center de la facultad de Ingeniería en Ciencias Aplicadas, en la Universidad Técnica del Norte. 2018. Tesis de Licenciatura.

- GÓMEZ RAVELO, Cristian Alberto, et al. Diseñar un Sistema de Gestión de la Seguridad de la Información para la Empresa Qwerty SA a partir de la Norma ISO 27001. 2020.

- ARIAS LEÓN, Julián Andrés; RUÍZ CORREA, Juan Guillermo. Definición de un modelo de evaluación de riesgos en seguridad de la información bajo los lineamientos de la norma ISO 27001, utilizando técnicas de redes neuronales. 2019.

- SANDOVAL CHERO, Cesar Arturo. Modelo de la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 orientado a las microempresas. 2023.

- CÉSPEDES VEGA, Charles Richard; RIVERA BARBOZA, Darwin Jair. MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN BASADO EN LA ISO/IEC 27005 PARA EL HOSPITAL PRIVADO JUAN PABLO II DE LA CIUDAD DE CHICLAYO. 2020.

- CÉSPEDES VEGA, Charles Richard; RIVERA BARBOZA, Darwin Jair. MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN BASADO EN LA ISO/IEC 27005 PARA EL HOSPITAL PRIVADO JUAN PABLO II DE LA CIUDAD DE CHICLAYO. 2020.

- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27001:2013. Sistema de gestión de la seguridad de la información. [en línea] Recuperado de http://www.iso27001.com, 2013.

- SAMBONI SAMBONI, EDUARD FERNANDO. Propuesta de modelo de un sistema de gestión de seguridad de la información para pequeñas empresas de desarrollo de software. Monografía para optar al título de Ingeniero en Telemática, Universidad Distrital Francisco José de Caldas, Facultad Tecnológica, Bogotá D.C., 2018.

- PRIETO SARMIENTO, EDWARD JONATHAN y GUARNIZO ARIAS, JONATHAN EFREY. Diseño de un sistema de gestión de seguridad de la información (SGSI) para la empresa Agility S.A.S. Monografía para optar al título de Ingeniero en Telemática, Universidad Distrital Francisco José de Caldas, Facultad Tecnológica, Bogotá D.C., 2016.

- VILLAMIL MARTÍN, ANA LUISA y MIRANDA RODRIGUEZ, FRANCISCO LEONARDO. Diseño de un sistema de gestión de seguridad de la información (SGSI) para las empresas dedicadas a la logística en mensajería. Monografía para optar al título de Ingeniero en Telemática, Universidad Distrital Francisco José de Caldas, Facultad Tecnológica, Bogotá D.C., 2017.

- TAPIERO TAPIERO, HAWIN ANDREI y SUÁREZ RAMÍREZ, HEINER. Modelo de gestión de riesgos de la seguridad de la información en empresas del sector asegurador utilizando la norma ISO/IEC 27005. Monografía para optar al título de Ingeniero en Telemática, Universidad Distrital Francisco José de Caldas, Facultad Tecnológica, Bogotá D.C., 2017.

- PRIETO SARMIENTO, EDWARD JONATHAN y GUARNIZO ARIAS, JONATHAN EFREY. Diseño de un sistema de gestión de seguridad de la información (SGSI) para la empresa Agility S.A.S. Monografía para optar al título de Ingeniero en Telemática, Universidad Distrital Francisco José de Caldas, Facultad Tecnológica, Bogotá D.C., 2016.