Universidad de Sevilla

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA INFORMÁTICA

GRADO EN INGENIERÍA INFORMÁTICA DEL SOFTWARE

TRABAJO FIN DE GRADO

Desarrollo de una auditoría de ciberseguridad para PYMEs

Realizado por:

Álvaro Ruiz Gutiérrez

Dirigido por:

Alejandro Carrasco Muñoz

Departamento:

Tecnología Electrónica

2024/2025

Índice

Índice de figuras

Índice de cuadros

Agradecimientos

INTENCIONADAMENTE EN BLANCO

Resumen

Las pequeñas y medianas empresas (PYMEs) desempeñan un papel crucial en la economía global, impulsando la creación de empleo y la innovación. Sin embargo, su creciente digitalización ha aumentado su exposición a ciberataques, debido a infraestructuras de seguridad limitadas y recursos insuficientes para enfrentar amenazas sofisticadas. Este proyecto tiene como objetivo principal desarrollar un modelo de auditoría de ciberseguridad adaptado a las PYMEs, basándose en la normativa europea y nacional vigente. Para garantizar su aplicabilidad, se elaborará una guía accesible para usuarios sin conocimientos técnicos previos, permitiéndoles evaluar y mejorar la seguridad de sus entornos digitales.

El proyecto se divide en dos fases principales. En la primera, se establecerá un marco teórico que explore las herramientas más comunes en auditorías de seguridad, las normativas aplicables y las metodologías más utilizadas en el ámbito de la ciberseguridad. Se examinarán los diferentes tipos de auditorías y se proporcionarán estrategias para mitigar estos riesgos. Esta fase permitirá comprender en profundidad las vulnerabilidades específicas del entorno empresarial y cómo abordarlas.

La segunda fase estará dedicada a la implementación práctica de la auditoría, siguiendo una metodología estructurada que abarcará desde el análisis del perímetro de red hasta la evaluación de la seguridad de los datos. Se incluirán pruebas en aplicaciones web, dispositivos IoT y la infraestructura interna de la empresa. Esta parte culminará con un caso práctico que ilustrará el proceso completo de auditoría en un entorno real, proporcionando una visión clara de cómo aplicar las técnicas aprendidas.

El objetivo final de este estudio no es solo facilitar la ejecución de auditorías de ciberseguridad en PYMEs, sino también promover la adopción de buenas prácticas. La guía ofrecerá recomendaciones para la gestión continua de la seguridad, la creación de políticas internas efectivas y la concienciación del personal, asegurando que las empresas no solo cumplan con las normativas vigentes, sino que también desarrollen una cultura de seguridad robusta y sostenible en el tiempo.

Palabras clave: ciberseguridad, auditoría, PYMEs, vulnerabilidades, normativas, metodologías, buenas prácticas.

Abstract

Small and medium-sized enterprises play a crucial role in the global economy, driving job creation and innovation. However, their increasing digitalization has heightened their exposure to cyberattacks due to limited security infrastructures and insufficient resources to face sophisticated threats. This project aims to develop a cybersecurity audit model tailored to SMEs, based on current European and national regulations. To ensure its applicability, an accessible guide will be created for users without prior technical knowledge, enabling them to evaluate and improve the security of their digital environments.

The project is divided into two main phases. The first phase will establish a theoretical framework exploring the most common tools in security audits, applicable regulations, and the most widely used methodologies in cybersecurity. Different types of audits will be examined, and strategies to mitigate risks will be provided. This phase will allow for a deep understanding of the specific vulnerabilities within the business environment and how to address them.

The second phase will focus on the practical implementation of the audit, following a structured methodology that will cover everything from network perimeter analysis to data security evaluation. It will include tests on web applications, IoT devices, and the company's internal infrastructure. This part will culminate in a practical case study illustrating the complete audit process in a real environment, providing a clear view of how to apply the learned techniques.

The ultimate goal of this study is not only to facilitate the execution of cybersecurity audits in SMEs but also to promote the adoption of best practices. The guide will offer recommendations for continuous security management, the creation of effective internal policies, and staff awareness, ensuring that companies not only comply with current regulations but also develop a robust and sustainable security culture over time.

Keywords: cybersecurity, audit, SMEs, vulnerabilities, regulations, methodologies, best practices.

1. Introducción

En el mundo digital actual, la ciberseguridad ya no es una opción, sino una necesidad. Las pequeñas y medianas empresas (PYMEs), pilares fundamentales de la economía global, se encuentran entre los objetivos más vulnerables frente a ciberataques. A pesar de su importancia económica, muchas de estas empresas subestiman su exposición a amenazas digitales, creyendo erróneamente que su tamaño las hace pasar desapercibidas para los ciberdelincuentes. Sin embargo, esta percepción es un error crítico, ya que la limitada infraestructura de seguridad de las PYMEs las convierte en blancos fáciles.

Un claro ejemplo de la creciente amenaza cibernética es el ataque sufrido por el portal de afiliación del sindicato Comisiones Obreras (CCOO) en diciembre de 2023. El atacante explotó una vulnerabilidad en el formulario de afiliación, accediendo a la configuración interna del sitio web. Esta brecha permitió la subida de un archivo malicioso que otorgó control total sobre el sistema, facilitando el acceso a información sensible, incluyendo contraseñas sin la protección adecuada. Como resultado, el atacante alteró la página de inicio de aproximadamente 50 subdominios de ccoo.es, demostrando la facilidad con la que se puede comprometer la seguridad digital de una organización.

Este incidente subraya la necesidad urgente de fortalecer la ciberseguridad en organizaciones de todos los tamaños. Las PYMEs, en particular, son especialmente susceptibles debido a la escasez de recursos y, en muchos casos, a una falta de concienciación sobre las amenazas digitales. La creciente digitalización y la dependencia de sistemas conectados a la red han ampliado la superficie de ataque, exponiendo a estas organizaciones a riesgos significativos.

En este contexto, es crucial que las PYMEs adopten medidas proactivas para proteger sus activos digitales. Este trabajo propone una guía práctica para la realización de auditorías de ciberseguridad, con el objetivo de identificar vulnerabilidades, evaluar riesgos y establecer estrategias de mitigación efectivas. A través de esta guía, se busca empoderar a las PYMEs para que fortalezcan su postura de seguridad y enfrenten con mayor confianza los desafíos del entorno digital actual.

1.1. Objetivos

El objetivo principal de este trabajo es diseñar un modelo de auditoría de ciberseguridad específico para PYMEs, que sea fácil de implementar por personas sin conocimientos técnicos avanzados. Los objetivos específicos incluyen:

- Establecer un marco teórico que contemple las herramientas, técnicas y normativas actuales en ciberseguridad.
- Proponer una metodología de auditoría clara y estructurada.
- Desarrollar un caso práctico en una PYME real para validar la metodología propuesta.
- Redactar un informe detallado que incluya el análisis de riesgos, vulnerabilidades detectadas y recomendaciones de mejora.

1.2. Alcance

El alcance de este trabajo está diseñado para cubrir de manera integral todos los aspectos necesarios para realizar una auditoría de ciberseguridad efectiva en PYMEs, basándose en estándares y metodologías reconocidas internacionalmente.

1. **Marco teórico:** Se explorarán las herramientas más utilizadas en auditorías de ciberseguridad, las normativas relevantes tanto a nivel nacional como europeo, los distintos tipos de auditoría existentes y las recomendaciones de organizaciones como OWASP, SANS y OSSTM.
2. **Requisitos previos:** Se detallarán los conocimientos, habilidades y recursos técnicos necesarios para realizar auditorías efectivas, incluyendo la configuración de entornos de prueba y el uso de herramientas especializadas.
3. **Propuesta de metodología:** Se desarrollará una metodología estructurada que incluirá el análisis del perímetro de red, la seguridad inalámbrica, la identificación de vulnerabilidades en dispositivos IoT, pruebas sobre aplicaciones web, evaluación de la infraestructura interna y análisis de seguridad en endpoints y sistemas de almacenamiento de datos.
4. **Caso práctico:** Se implementará un caso práctico que aplicará la metodología propuesta en un entorno real, permitiendo ilustrar de manera tangible el proceso completo de una auditoría de ciberseguridad.
5. **Informe final:** Elaboración de un documento que refleje el estado actual de la ciberseguridad en la empresa auditada y las recomendaciones pertinentes.

1.3. Motivación

La creciente digitalización ha expuesto a las Pequeñas y Medianas Empresas (PYMEs) a una variedad de ciberamenazas que, de no ser gestionadas adecuadamente, pueden poner en riesgo la continuidad de sus operaciones. A diferencia de las grandes corporaciones, las PYMEs suelen carecer de los recursos humanos y financieros necesarios para implementar medidas robustas de ciberseguridad, lo que las convierte en objetivos atractivos para los ciberdelincuentes.

El aumento en el volumen de software malicioso, que supera los 450.000 nuevos programas diarios según AV-TEST, y el hecho de que el 70 por ciento de los ciberataques en la Península Ibérica afectan a PYMEs, subrayan la urgencia de desarrollar herramientas accesibles y eficaces para proteger a estas organizaciones. Este proyecto surge como respuesta a esa necesidad, proporcionando una guía práctica que permite a cualquier persona, independientemente de su nivel técnico, llevar a cabo una auditoría básica de ciberseguridad.

La implementación del modelo propuesto no solo mejorará la seguridad digital de las PYMEs, sino que también fomentará una mayor concienciación sobre la importancia de la ciberseguridad en el entorno empresarial. De esta manera, se busca fortalecer el tejido empresarial frente a las crecientes amenazas cibernéticas.

1.4. Requisitos formales

Una vez dado un contexto general del trabajo, nos centraremos en describir que requisitos son necesarios para la redacción del documento.

1.4.1. Documentación e información

- Los documentos pueden ser extraídos de *Google Scholar* para su posterior citación, recomendando documentos no más antiguos de 2 o 3 años para asegurar la vigencia de la información.
- Se citarán en el documento en formato APA todos los documentos de los que se ha extraído información.
- Deben contener información relevante y actualizada sobre ciberseguridad en PYMEs, incluyendo normativas, estándares, herramientas y técnicas de auditoría.

1.4.2. Normativas y certificaciones

- Deben ser oficiales y de libre acceso, proporcionadas por organismos reguladores tanto de ámbito europeo como internacional.

1.4.3. Propuesta de metodología de la auditoría

- Debe atender a los requerimientos de ciberseguridad descritos en la documentación oficial.
- Describir las implementaciones de hardware y software necesarias para proteger los sistemas.

1.4.4. Sobre el caso práctico

- Descripción del sistema auditado, incluyendo modelo y vulnerabilidades.
- Aplicación de la metodología de ciberseguridad en la PYME seleccionada.
- Detalle de las pruebas realizadas y la obtención de información sobre riesgos, amenazas y vulnerabilidades.

1.5. Estructura del documento

El documento está organizado en once capítulos que abordan de manera integral todos los aspectos necesarios para realizar una auditoría de ciberseguridad en PYMEs:

- **Agradecimientos:** Reconocimiento a las personas y entidades que han contribuido al desarrollo de este trabajo.
- **Resumen:** Síntesis del contenido, objetivos y resultados del trabajo.
- **Introducción:** Presentación del contexto de la ciberseguridad en PYMEs, objetivos, alcance, motivación, requisitos formales para el desarrollo del proyecto y estructura del documento.
- **Planificación:** Descripción de la organización del trabajo, incluyendo cronograma, recursos utilizados, costes y fases del proyecto.
- **Marco Teórico (Estado del arte):** Análisis de normativas nacionales y europeas aplicables, estándares, herramientas de pentesting y técnicas relevantes en el ámbito de la ciberseguridad para PYMEs.
- **Requisitos:** Definición de los requisitos técnicos, legales y organizativos necesarios para llevar a cabo una auditoría de seguridad.
- **Modelo de auditoría:** Propuesta de un modelo de auditoría dividido en diseño, metodología y fases específicas.
- **Caso Práctico:** Implementación de la auditoría en un entorno real de una PYME, aplicando las herramientas y técnicas descritas.

- **Resultados:** Presentación y análisis de los resultados obtenidos en el caso práctico.
- **Discusión de resultados:** Reflexión sobre los hallazgos, lecciones aprendidas y posibles trabajos futuros.
- **Referencias:** Fuentes consultadas para la realización del trabajo.
- **Anexos:** Material complementario que apoya el desarrollo del caso práctico y la comprensión de la metodología.

2. Planificación

Este capítulo presenta la planificación detallada para el desarrollo del trabajo. Se describirán las fases y tareas específicas a desarrollar, los roles y responsabilidades de los participantes en el proyecto, así como un cronograma que permitirá visualizar el progreso del trabajo a lo largo del tiempo. Además, se identificarán los recursos necesarios para llevar a cabo el proyecto y se realizará un análisis de los costes asociados.

2.1. Fases y lista de actividades

Fase 1: Preparación y selección del tema

- **Reunión inicial**: Primer encuentro con el tutor para explorar posibles temas de interés para el TFG.
- **Investigación y reflexión**: Análisis de las diferentes opciones y selección del tema más adecuado.
- **Adjudicación del TFG**: Confirmación oficial del tema y comienzo de la investigación preliminar.

Fase 2: Desarrollo inicial

- **Inicio del trabajo en el TFG**: Comienzo formal de la redacción y desarrollo del trabajo.
- **Profundización en la investigación**: Ampliación del conocimiento sobre el tema seleccionado.
- **Reunión con el tutor**: Reunión inicial para debatir sobre la estructura y organización del TFG.
- **Reunión con el CTO de la empresa BeeHacker**: Obtención de información adicional y perspectivas del sector.
- **Desarrollo de introducción y planificación**: Definición clara de los objetivos, alcance, motivación y requisitos. También se establecerá la estructura general del documento y la planificación del proyecto.

Fase 3: Desarrollo del Marco Teórico

- **Reunión con el tutor**: Evaluación del avance y orientación sobre el contenido teórico.
- **Iniciar el desarrollo de la parte teórica**: Redacción y compilación de la base teórica del proyecto.
- **Reunión con el CTO de la empresa BeeHacker**: Confirmación y validación de los conceptos teóricos aplicados.
- **Investigación sobre normativas y certificaciones**: Estudio de las regulaciones pertinentes al tema.

Fase 4: Finalización del Marco Teórico

- **Reunión con el tutor**: Verificación del contenido desarrollado hasta el momento.
- **Corrección y ajuste final del marco teórico**: Modificaciones necesarias basadas en las recomendaciones del tutor.
- **Reunión con el tutor**: Confirmación de la versión final del marco teórico.

Fase 5: Implementación y diseño de la auditoría

- **Inicio de la implementación de la guía**: Desarrollo práctico de la guía de auditoría.
- **Desarrollo de la propuesta de metodología**: Creación de un enfoque metodológico para el proyecto.

- **Reunión con el CTO de la empresa BeeHacker**: Ajustes finales en la metodología basada en feedback.
- **Reunión con el tutor para revisar el progreso**: Evaluación de los avances en la implementación.
- **Cierre de la propuesta de metodología**: Finalización y validación del enfoque metodológico.

Fase 6: Caso Práctico

- **Inicio del caso práctico**: Comienzo de la aplicación práctica de la metodología.
- **Desarrollo del caso práctico**: Implementación y evaluación del caso de estudio.
- **Cierre del caso práctico**: Finalización y análisis de resultados.
- **Redacción del informe**: Documentación detallada de los hallazgos y conclusiones sobre el caso práctico.

Fase 7: Revisión y corrección final

- **Reunión con el tutor**: Revisión integral del documento final.
- **Corrección y ajuste final del documento**: Implementación de las correcciones finales antes de la entrega.

En conclusión, este trabajo ha requerido aproximadamente X horas de dedicación. Una parte considerable de este tiempo se destinó a la investigación y estructuración del proyecto, dado que la temática fue seleccionada conjuntamente por el alumno y el tutor, lo que añadió un desafío adicional al tratarse de un área completamente nueva para el alumno. Las primeras fases del proyecto coincidieron con la recuperación de asignaturas pendientes, lo que limitó el tiempo disponible. No obstante, a partir de la tercera fase, especialmente desde inicios de 2025, el Trabajo Fin de Grado pasó a ser la prioridad principal tras la finalización de todas las asignaturas académicas.

2.2. Roles y responsabilidades

Rol	Responsabilidad
Analista/Desarrollador (Alumno)	Planificación y redacción del documento
Analista/Desarrollador (Alumno)	Investigación y análisis de ciberseguridad en PYMEs
Analista/Desarrollador (Alumno)	Desarrollo del marco teórico
Analista/Desarrollador (Alumno)	Agrupación y redacción de requisitos previos para auditoría
Analista/Desarrollador (Alumno)	Identificación y documentación de normativas aplicables
Analista/Desarrollador (Alumno)	Creación de plan de auditoría propio
Analista/Desarrollador (Alumno)	Diseño de la metodología de auditoría
Analista/Desarrollador (Alumno)	Implementación práctica de la auditoría
Analista/Desarrollador (Alumno)	Ejecución del caso práctico
Analista/Desarrollador (Alumno)	Análisis de resultados y redacción del informe final
Jefe de proyecto (Tutor)	Asesoramiento en la selección del tema y enfoque del proyecto
Jefe de proyecto (Tutor)	Orientación y supervisión del trabajo del alumno
Jefe de proyecto (Tutor)	Organizar el desarrollo del caso práctico
Jefe de proyecto (Tutor)	Correcciones y evaluación del proyecto
Jefe de equipo (CTO de BeeHacker)	Proporcionar información técnica relevante y feedback
Jefe de equipo (CTO de BeeHacker)	Validación de la metodología y resultados del caso práctico

Cuadro 1: Distribución de roles y responsabilidades en el proyecto

2.3. Cronograma

uso de la app para hacer el gant con presupuesto, recursos...

2.4. Recursos

2.5. Estimación de costes

3. Marco Teórico (Estado del arte)

QUE HAY?¿? TIPOS DE AUDITORIA, NORMATIVAS, RECOMENDACIONES OWASP10 , HERRAMIENTAS, ETC.

3.1. Principales amenazas y riesgos para PYMEs

3.2. Normativas nacionales aplicables

3.3. Normativas europeas aplicables

3.4. Leyes y regulaciones en ciberseguridad

3.5. Herramientas de pentesting

3.6. Técnicas y buenas prácticas de una auditoría

4. Requisitos

5. Modelo de auditoría

5.1. Diseño

5.2. Propuesta de auditoría

5.3. Metodología de auditoría

6. Caso Práctico

6.1. Implementación de la auditoría

7. Resultados

8. Discusión de resultados o conclusiones

9. Referencias o Bibliografía