Diseño de un marco de gobierno de ciberseguridad para empresas medianas según el estándar ISO/IEC 27001.

Pablo Núñez Migon

Resumen — El presente estudio propone un marco de gobierno de ciberseguridad diseñado específicamente para empresas medianas, tomando como referencia el estándar internacional ISO/IEC 27001. Los objetivos persiguen la comprensión integral de la familia de estándares ISO/IEC 27000, incluyendo sus términos, definiciones, roles, responsabilidades y principios de gestión de la seguridad. Asimismo, se describe una metodología detallada para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) que permita una adecuada planificación, identificación y tratamiento de riesgos, promoviendo el enfoque de mejora continua. La metodología se fundamenta en un análisis exhaustivo de la ISO/IEC 27001, un análisis comparativo y de cumplimiento con el Esquema Nacional de Seguridad (ENS) y los requerimientos de la Directiva NIS2, y finaliza con el diseño de un marco de ciberseguridad que integra políticas de seguridad, roles y responsabilidades, así como procesos de gestión de riesgos adaptados a las necesidades y características de las empresas medianas, junto con un ejemplo de auditoría aplicada a una empresa mediana.

Palabras Clave — ISO/IEC 27001, Sistema de Gestión de Seguridad de la Información (SGSI), Ciberseguridad en empresas medianas, Gestión de riesgos, Seguridad de la información, Política de seguridad, Gobierno de ciberseguridad.

Abstract — This study proposes a cybersecurity governance framework specifically designed for medium-sized companies, using the international ISO/IEC 27001 standard as a reference. The objectives aim for a comprehensive understanding of the ISO/IEC 27000 family of standards, including its terms, definitions, roles, responsibilities, and security management principles. Additionally, a detailed methodology is described for implementing an Information Security Management System (ISMS) that enables effective planning, risk identification, and treatment, while promoting a continuous improvement approach. The methodology is based on an exhaustive analysis of ISO/IEC 27001, a comparative analysis of and compliance with the National Security Framework (ENS) and the requirements of the NIS2 Directive, and culminates in the design of a cybersecurity framework that integrates security policies, roles and responsibilities, and risk management processes tailored to the needs and characteristics of medium-sized companies.

Index Terms — ISO/IEC 27001, Information Security Management System (ISMS), Cybersecurity in Medium-Sized Enterprises, Risk Management, Information Security, Security Policy, Cybersecurity Governance.

- *E-mail de contacto: pablonmigon@gmail.com*
- *Tecnologías de la Información*
- *Trabajo Tutorizado por Enric Alibech Romero*
- *Curso 2024/25*

1 INTRODUCCIÓN - CONTEXTO DEL TRABAJO

La transformación digital ha dado lugar a nuevos desafios en el mundo empresarial, y la ciberseguridad es uno de los más críticos. Si bien las grandes empresas disponen de los recursos adecuados para implementar sólidas estrategias de seguridad, las pequeñas y medianas empresas, aún enfocadas en la competitividad y el crecimiento, son un objetivo atractivo para quienes desean atacar. La ciberseguridad para la empresa mediana se refiere no solo a la protección de los datos confidenciales y la presentación de una imagen confiable. También significa la protección de su continuidad operativa y el cumplimiento de los marcos normativos existentes. La ISO 27001 es un estándar que maneja la protección de la confidencialidad y riesgos en la seguridad de la información. La norma establece un marco de políticas que cubren todos los aspectos de los procesos de gestión de riesgos. En este proyecto, exploraremos cómo la ISO 27001 define y facilita los pilares fundamentales de la seguridad de la información; la confidencialidad, la integridad y la disponibilidad de la información dentro de una organización, utilizando un enfoque basado en la gestión de riesgos. [1]

2 OBJETIVOS

2.1 Conocimiento Exhaustivo de la familia de estándares ISO/IEC 27000:

- Conocer los términos y las definiciones pertenecientes a las distintas normativas de la familia ISO 27000.
- Comprender la distribución de: roles, responsabilidades y recursos en la organización.
- Conocer las políticas de seguridad y sus propiedades clave: claridad, aplicabilidad, etc.
- Entender la importancia de la documentación y la comunicación efectiva en la gestión de la seguridad.

2.2 Descripción de la metodología para establecer un SGSI según la ISO/IEC 27001:

- Definir los objetivos, las acciones y los métodos de planificación adecuados para la implementación de un SGSI.
- Abordar conceptos relacionados con riesgos: identificación, tratamiento y objetivos de la gestión de riesgos.
- Conocer el proceso operacional: Mejora Continua

2.3 Comprensión del papel del SGSI en la Empresa Mediana:

- Comprensión de las características Clave: Confidencialidad, Integridad y Disponibilidad.
- Integración del SGSI en los procesos corporativos.
- Apreciación y Tratamiento de Riesgos de Seguridad.

3 PLANIFICACIÓN

Debido a la naturaleza del proyecto, la organización se estructurará en función de los siguientes bloques de la metodología.

La planificación temporal se detalla en la Fig.1: Cronograma Organizativo.

TAREA	INICIO	FIN
Informe Inicial		
Lectura Documentación CV	5-9-24	12-9-24
Investigación Pre-Reunión	9-9-24	11-9-24
Reunión de Inicio de Proyecto	17-9-24	17-9-24
Lectura de ISO 27000/1-3	17-9-24	27-9-24
Desarrollo de Objetivos, Planificación y Metodología	17-9-24	22-9-24
Entrega Informe	27-9-24	27-9-24
Estudio del estado del arte de la ISO/IEC 27001		
Lectura de ISO 27000/1-3	3-10-24	5-10-24
Investigación Casos Reales	5-10-24	15-10-24
Redacción del Estudio	10-10-24	15-10-24
Comparativa con marcos alternativos y normativas de obligado cumplimiento		
Lectura de ENS	15-10-24	16-10-24
Lectura de NIS 2	15-10-24	20-10-24
Comparación de Objetivos y Controles	20-10-24	20-10-24
Propuesta de un marco de gobierno de ciberseguridad		
Definición de Objetivos	25-10-24	30-10-24
Definición de Políticas y asignación de Roles	30-10-24	1-11-24
Definición de Controles y clasificación de Riesgos	1-11-24	3-11-24
Redacción de Conclusiones	3-11-24	7-11-24
Revisión de Bibliografía	7-11-24	7-11-24
Informe Final		
Revisión Informe de Progreso II	17-11-24	21-11-24
Organización del Dossier Digital	21-11-24	21-11-24
Revisión de Criterios de Forma	21-11-24	21-11-24
Gestión de Pendientes	21-11-24	6-12-24

4 METODOLOGÍA

Fig 1. Cronograma Organizativo

4.1 Estudio del estado del arte de la ISO/IEC 27001

- Lectura en profundidad de la familia de normativas ISO/IEC 27000.

- Investigación de casos reales de la aplicación de esta norma en empresas medianas.

4.2 Análisis comparativo con marcos alternativos y normativas de obligado cumplimiento

- Comparción de la ISO/IEC 27001 con el Esquema Nacional de Seguridad (ENS) [2], ambos en el contexto de la empresa mediana.
- Análisis de cumplimiento de los controles propuestos en la ISO 27001 con las solicitudes de la NIS2. [3]

4.3 Propuesta de un marco de gobierno de ciberseguridad

- A partir del análisis previo, diseño de una propuesta de marco de gobierno de ciberseguridad para empresas medianas, basado en los principios de la ISO/IEC 27001.
- Esta propuesta incluirá políticas de seguridad, roles y responsabilidades, y procesos de gestión de riesgos adaptados al tamaño y características de las empresas medianas.

5 DESARROLLO

La ISO 27001 establece un marco de trabajo para crear, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema está compuesto por un conjunto de políticas, procesos y controles diseñados para gestionar la seguridad de la información de manera sistemática y estructurada dentro de una organización.

5.1 Objetivos principales del SGSI

Como se ha mencionado anteriormente, el SGSI tiene como objetivo principal proteger los tres pilares fundamentales de la información:

- Confidencialidad: Garantiza que la información solo sea accesible para personas autorizadas, protegiendo su divulgación no autorizada, tanto en almacenamiento como en tránsito.
- Integridad: Asegura que la información se mantenga precisa y completa, previniendo modificaciones no autorizadas.
- Disponibilidad: Asegura que la información esté disponible y accesible cuando sea necesario, evitando su pérdida o destrucción.

Para alcanzar estos objetivos, el SGSI sigue un enfoque orientado al riesgo, que permite a las organizaciones identificar, priorizar y gestionar los riesgos que podrían afectar la seguridad de sus activos de información.

5.2 Metodología para establecer un SGSI según la ISO 27001

La ISO 27001 proporciona un conjunto de pautas de alto nivel para establecer un SGSI efectivo. A continuación, se detallan los pasos clave en este proceso:

- 1. Comprender el contexto de la organización

Se debe realizar un análisis profundo de la organización para identificar las cuestiones internas y externas que puedan influir en la seguridad de la información. Factores como la cultura organizativa, las partes interesadas y los requerimientos legales deben ser considerados para adaptar el SGSI a las necesidades y entorno de la organización.

- 2. Definir el alcance del SGSI

Una vez comprendido el contexto, se debe establecer el alcance del SGSI, determinando qué activos, unidades de negocio, procesos y tecnologías estarán cubiertos. Además, es fundamental prestar atención a proveedores o empresas colaboradoras con las que se comparta algún tipo de infraestructura, ya sea digital o física. Este paso es clave para garantizar que todas las áreas críticas de la organización estén protegidas.

- 3. Establecer políticas de seguridad de la información

Las políticas de seguridad son un conjunto de directrices y procedimientos que deben diseñarse pensando en el contexto organizacional y deben establecer objetivos de seguridad claros. Estas políticas deben ser documentadas, comunicadas de manera efectiva dentro de la organización y estar disponibles para todas las partes interesadas. Además, deben comprometerse con el cumplimiento de los requisitos aplicables y la mejora continua. En la siguiente sección veremos los campos de políticas más habituales.

- 4. Asignación de roles y responsabilidades

La dirección de la empresa debe comprometerse a asignar roles y responsabilidades claras para el SGSI. Esto incluye estudiar qué roles se establecerán, teniendo en cuenta los recursos humanos disponibles y el presupuesto destinado a seguridad. A continuación, debe realizarse la designación de responsables de la gestión de la seguridad de la información, así como la responsabilidad de asegurar el cumplimiento con la ISO 27001 y por ende de las normativas relacionadas. La dirección también debe realizar el reporte periódico sobre el desempeño del sistema.

- 5. Planificación para el SGSI

La organización debe planificar las acciones necesarias para alcanzar los objetivos del SGSI, considerando los riesgos identificados. Además, tiene la tarea fundamental de integrar las acciones y protocolos de seguridad dentro de los procesos operativos de la organización y establecer cómo evaluar su efectividad.

- 6. Gestión de riesgos

La gestión de riesgos se desarrolla en tres fases, conocidas como proceso de apreciación de riesgos:

- Identificación de riesgos: El primer paso es determinar los posibles eventos que puedan surgir y que afecten a los objetivos planteados.
- Análisis de riesgos: Para analizar los riesgos se consideran las causas, el origen, la probabilidad de que esto ocurra y sus posibles consecuencias.
- Evaluación de riesgos: La evaluación de riesgo "implica la comparación de niveles estimados de riesgo con los criterios de riesgo definidos cuando se estableció el contexto, con el objetivo de determinar el tipo de riesgo y la importancia del nivel." ISO 31010.[6]

Tras el proceso de apreciación, debe realizarse el proceso de tratamiento de riesgos.

- Tratamiento de riesgos: En este punto se deben seleccionar y aplicar los controles necesarios para reducir los riesgos a un nivel aceptable.

- 7. Establecimiento de objetivos de seguridad de la información

Los objetivos deben ser coherentes con la política de seguridad, medibles en la medida de lo posible, y deben tener en cuenta los riesgos identificados. Estos objetivos deben ser comunicados a toda la organización y revisados regularmente.

- 8. Asignación de recursos y competencias

La organización debe proporcionar los recursos necesarios para implementar, mantener y mejorar el SGSI. Esto incluye la asignación de personal competente y la realización de formaciones adecuadas, así como la documentación pertinente que evidencie la competencia del personal involucrado.

- 9. Monitoreo y evaluación continua

La organización debe establecer un sistema de monitoreo para evaluar el desempeño del SGSI y la efectividad de los controles implementados. Esto implica medir los resultados de seguridad, realizar auditorías internas para verificar el cumplimiento de la norma y revisar regularmente el sistema a nivel de dirección. La dirección debe asegurarse de que se aborden las acciones correctivas y que el SGSI esté alineado con los cambios internos y externos.

- 10. Mejora continua

Finalmente, el SGSI debe someterse a un ciclo de mejora continua, asegurando que se implementen las acciones correctivas necesarias y que se adapten a los cambios en el entorno de riesgos. Esto garantiza que el sistema evolucione para enfrentar nuevos desafíos de seguridad de la información.

5.4 Comparativa con el Esquema Nacional de Seguridad ENS y con la NIS 2

- 1. ISO/IEC 27001 vs. ENS

Mientras la ISO 27001 es un estándar de buenas prácticas internacional voluntario con directrices a alto nivel, aplicable a cualquier tipo de organización, el ENS es una ley de obligado cumplimiento (**Real Decreto 311/2022)**, que está enfocada al sector público en España; teniendo como objetivo garantizar un nivel adecuado de seguridad en los sistemas de información de la administración y de aquellos proveedores privados que colaboren con ellas. [7]

Dada la flexibilidad que ofrece la norma ISO, puede ser implementada en empresas medianas adaptando el conjunto de medidas a establecer en el marco de control a los recursos y necesidades específicos de la organización. Además, como se establece una estructura que promueve el cumplimiento de los requisitos de seguridad, el ciclo de mejora continua facilita la escalabilidad a medida que la empresa crezca. Por otra parte, el alcance global de los estándares ISO hace que dar cumplimiento a las diversas normativas que existan tanto a nivel internacional como local sea relativamente sencillo; ya que no suelen existir grandes diferencias entre los distintos cuerpos regulatorios.

En el caso del Esquema Nacional de Seguridad (ENS), se aplica a las empresas medianas que operan en sectores críticos, es decir, aquellas que colaboran con el gobierno o gestionan datos de interés público, como empresas de servicios esenciales, telecomunicaciones o salud. Estas empresas tienen un papel importante en garantizar la seguridad de los servicios que son fundamentales para la sociedad.; para estas empresas se imponen requisitos concretos en cuanto a medidas de seguridad, controles y políticas para asegurar el bien común. Es importante destacar que el ENS es de obligado cumplimiento.

A nivel de los controles, la ISO 27001 y su enfoque basado en riesgos proporcionan un marco flexible; sin embargo, el ENS establece directamente controles específicos y hace una clasificación propia en niveles de seguridad, según el tipo de información y el sistema de tratamiento de

datos. Es más restrictivo para asegurar un nivel mínimo de seguridad.

El nivel de seguridad básico aplica a sistemas donde la información es de baja sensibilidad y el impacto de un incidente sería limitado. Controles asociados son la gestión de accesos, autenticación básica o seguridad física.

El nivel medio aplica a sistemas donde el compromiso de la información podría generar un impacto significativo en los servicios y en la privacidad de los datos gestionados. En este caso se exige el cifrado de datos sensibles, el monitoreo y registro de actividades, y un control de accesos serio.

El nivel alto aplica a sistemas críticos, donde un incidente podría causar incluso una crisis de seguridad nacional. Se exige autenticación multifactor, contar con planes de recuperación y continuidad de operación, protección avanzada con sistemas como Endpoint Detect and Respond (EDR) o Intrusion Prevention System (IPS).

A nivel de certificación de los SGSI, la ISO permite y recomienda la certificación por entidades acreditadas internacionalmente. El ENS también contempla la auditoría externa. En ambos se planifica la auditoría interna como parte del proceso de seguridad.

Ambos coinciden también en la necesidad de formación y concienciación del personal para asegurar la competencia respecto a la seguridad de la información; así como en los mecanismos de control y monitorización, ya sean controles de acceso, registro de actividades o procedimientos de respuesta ante incidentes.

- 2. ISO/IEC 27001 y NIS2

La Directiva NIS2 (Network and Information Systems Directive) de la Unión Europea se centra en la resiliencia y seguridad de los sistemas de información en sectores críticos, como las infraestructuras, la salud y los servicios financieros.

Esta directiva establece requisitos de seguridad más estrictos para operadores de servicios esenciales y proveedores de servicios digitales, con un enfoque en la respuesta y recuperación ante incidentes de ciberseguridad.

La NIS2 exige a los estados miembroscrear una estrategia nacional de ciberseguridad y supervisar el cumplimiento de la normativa en las organizaciones críticas. No es un conjunto de pautas y recomendaciones sino una directiva de obligado cumplimiento, que establece que las organizaciones cubiertas deben cumplir con sus requisitos y someterse a auditorías y reportes periódicos.

Como ya se ha comentado anteriormente, la ISO 27001 es de caracter voluntario, aunque algunas organizaciones puedan exigirlo al momento de colaborar o contratar los servicios de una empresa.

Ambas son similares respecto al enfoque de seguridad basado en la gestión de riesgos. La NIS 2 está más centrada en sectores críticos y proveedores de servicios esenciales. En concreto, mientras que la ISO define un total de 114 controles en su Anexo A organizados en dominios como control de acceso, seguridad de activos, gestión de comunicaciones, criptografía, y gestión de incidencias; la directiva NIS 2 define requisitos generales en áreas como gestión de incidentes, información y análisis de amenazas, seguridad en la cadena de suministro, y continuidad del negocio. Exige que los estados miembros definan los controles específicos bajo las pautas que ofrece; en el caso de España por medio del ENS.

Las organizaciones que cumplen con los requisitos pueden obtener la certificación ISO 27001, que generalmente tiene una validez de tres años y requiere auditorías de seguimiento anuales. En el caso de la NIS 2 las organizaciones deben demostrar cumplimiento con auditorías y controles internos, y pueden estar sujetas a inspecciones o auditorías externas por parte de las autoridades nacionales de ciberseguridad. El cumplimiento se evalúa periódicamente y pueden aplicarse sanciones administrativas por incumplimiento, incluyendo multas de hasta un dos por ciento del volumen anual de negocio de la organización. Además, establece responsabilidad legal directa a los cargos ejecutivos de las organizaciones en la supervisión de los requisitos de ciberseguridad.

Como es lógico, el alcance de la NIS 2 se limita a las empresas y estados operando bajo el paraguas de la Unión Europea, no tiene el caracter de aplicación internacional de la ISO.

Para una organización en el ámbito de aplicación de ambas normativas, cumplir con ISO/IEC 27001 puede establecer una buena base para cumplir con NIS2, especialmente en áreas de gestión de riesgos y protección de la información. Sin embargo, cumplir con NIS2 requiere además el enfoque adicional en la resiliencia y notificación de incidentes y una gestión más estricta, especialmente en sectores críticos.

5.5. Medidas de Ciberseguridad

Siguiendo la metodología descrita anteriormente, se propone el siguiente marco de ciberseguridad para empresas medianas, abordando los principios esenciales teniendo en cuenta unas capacidades económicas limitadas.

Como se ha mencionado en la Metodología presentada en el punto 5.2; tras comprender el contexto de la organización y acotar el alcance del sistema de gestión de seguridad de la información, de deben definir las políticas de seguridad.

1. Políticas de seguridad

Las políticas de seguridad son la base del marco de ciberseguridad, y deben estar claramente documentadas,

comunicadas a todos los empleados, y revisadas periódicamente. Para empresas medianas, las políticas clave incluyen:

- Política de seguridad de la información: Establece los principios de protección y define el compromiso con el cumplimiento normativo y la gestión de riesgos.

- Política de control de acceso: Define los niveles de acceso en función de los roles, estableciendo métodos de autenticación y autorización, como la autenticación de múltiples factores para usuarios con permisos elevados.

- Política de gestión de incidentes de seguridad: Establece procedimientos para la identificación, notificación y resolución de incidentes. Incluye roles y responsabilidades claras, y un plan de comunicación para incidentes críticos.

- Política de gestión de riesgos: Define el proceso de identificación, evaluación, y tratamiento de riesgos de seguridad. Esto implica criterios de aceptación del riesgo, priorización de activos críticos y determinación de controles adecuados.

- Política de formación y concienciación en seguridad: Proporciona formación periódica a todos los empleados y una evaluación anual para asegurar que conocen los principios de seguridad, la política de la empresa y los procedimientos específicos en caso de incidentes.

- Política de uso aceptable de recursos y dispositivos: Establece directrices sobre el uso adecuado de los recursos tecnológicos de la empresa, como dispositivos, redes y sistemas de información. Esta política define las prácticas permitidas y prohibidas para proteger la información y los sistemas de accesos indebidos o actividades no autorizadas. Incluye restricciones sobre el acceso a redes externas y el uso de dispositivos personales, así como las consecuencias de incumplimiento.

- Política de teletrabajo y trabajo remoto: Establece las directrices y requisitos de seguridad específicos para los empleados que trabajan desde ubicaciones ajenas al espacio físico de la empresa. Esta política busca asegurar que el teletrabajo no comprometa la seguridad de la información y los sistemas de la organización. Se busca asegurar un acceso seguro, requiere el uso de redes privadas virtuales (VPN) para la conexión a los sistemas de la empresa, además de autenticación multifactor (MFA).

- Política de resiliencia operativa y continuidad del negocio: Esta política tiene como objetivo preparar a la empresa para enfrentar incidentes inesperados, como ciberataques, desastres naturales o fallos en infraestructuras críticas, minimizando la interrupción de los servicios esenciales y garantizando una recuperación rápida. Sus elementos clave incluyen:

  ◦ **Identificación de servicios y activos críticos:** Establece el proceso para identificar y clasificar los sistemas, aplicaciones y datos críticos para la continuidad del negocio. Incluye la designación de los activos que requieren mayor protección y supervisión para reducir el impacto en caso de interrupciones.

  ◦ **Plan de continuidad del negocio (BCP):** Define el marco para mantener las operaciones clave durante incidentes, incluyendo estrategias de redundancia, ubicaciones alternativas de trabajo, y planes de comunicación en situaciones de crisis. El BCP incluye procedimientos para que los empleados mantengan actividades esenciales y se asignan responsables para coordinar y supervisar su ejecución.

  ◦ **Planes de recuperación ante desastres (DRP):** Especifica los procedimientos técnicos para recuperar los sistemas de TI en caso de fallos críticos. Define las prioridades de restauración, los tiempos máximos de recuperación (RTO) - tiempo durante el cual una organización puede tolerar la inactividad sin sufrir consecuencias graves - y los puntos de recuperación (RPO) - cantidad máxima de datos que una organización puede permitirse perder, medida en tiempo, desde la última copia de seguridad hasta la interrupción - aceptables. Incluye estrategias como la replicación de datos y el uso de centros de datos secundarios para asegurar la restauración de sistemas.

  ◦ **Pruebas y simulacros periódicos:** Establece la periodicidad y metodología para realizar pruebas del BCP y DRP, simulando escenarios de crisis para evaluar la efectividad de los planes y la capacidad de respuesta de los equipos. Los resultados de estas pruebas deben documentarse y utilizarse para mejorar los planes.

  ◦ **Capacitación en resiliencia operativa**: Incluye sesiones de formación periódica para empleados clave y equipos de respuesta, asegurando que todos comprendan sus roles durante situaciones de crisis. Este componente garantiza que el personal esté preparado para reaccionar eficazmente en caso de incidentes.

  ◦ **Gestión de comunicación en crisis**: Establece un plan de comunicación para mantener informados a los empleados, clientes y partes interesadas durante una interrupción. Define los canales de comunicación y los mensajes estándar para situaciones de crisis, asegurando que la comunicación sea clara y controlada.

  ◦ **Evaluación post-incidente y mejora continua:** Después de cada incidente o simulacro, se realiza una evaluación detallada de la respuesta y los tiempos de recuperación, identificando áreas de mejora y ajustando los planes según sea necesario. Esto fomenta la resiliencia continua y adapta las políticas a las lecciones aprendidas.

2. Roles y Responsabilidades

Siguiendo la metodología descrita, tras definir unas po-

líticas de seguridad, deben proponerse los roles y responsabilidades adaptados al tamaño y previsible estructura de la empresa:

• **Dirección:** La Dirección tiene la responsabilidad de definir la visión estratégica de ciberseguridad de la empresa y garantizar que se asignen los recursos necesarios para la implementación, operación y mantenimiento del SGSI. Además, debe asegurarse de que se realice una revisión periódica del SGSI para identificar áreas de mejora y asegurar su continua adecuación a las amenazas emergentes. La alta dirección también es responsable de proporcionar la formación y los recursos necesarios al personal involucrado en la gestión de la seguridad de la información. Es su obligación garantizar que las políticas y objetivos de seguridad estén alineados con la estrategia general de la organización y que el cumplimiento de las normativas de seguridad se mantenga dentro de la empresa.

• **Responsable de Seguridad de la Información (**CISO): en empresas medianas, puede ser la persona encargada de TI o, si se dispone de recursos, un consultor externo especializado. Tiene la responsabilidad de supervisar y coordinar la implementación del SGSI, asegurándose de que las políticas y controles de seguridad sean efectivos y adecuados. Además, debe realizar auditorías periódicas de seguridad para identificar vulnerabilidades y garantizar el cumplimiento normativo. Entre sus funciones se incluye la gestión de incidentes de seguridad, liderando la identificación, contención y resolución de estos, así como la implementación de medidas correctivas y preventivas cuando sea necesario. Este perfil requiere formación en ciberseguridad, tecnologías de la información y gestión de riesgos, así como certificaciones reconocidas como CISSP (Certified Information Systems Security Professional) [4], CISA (Certified Information Security Auditor) [5] o ISO/IEC 27001 Lead Implementer o Auditor, que refuercen su capacidad para gestionar la seguridad de la información en la organización.

• **Empleados:** Todos los empleados de la organización-tienen la responsabilidad de comprender y cumplir con las políticas de seguridad establecidas por la empresa. La mayoría de los ataques de ciberseguridad tienen su vector de entrada en los empleados.

• **Responsables de TI y Soporte Técnico:** El equipo de TI juega un papel clave en la implementación de las medidas técnicas para proteger la infraestructura de la información. Esto incluye la implementación y mantenimiento de herramientas de seguridad como firewalls, sistemas de detección de intrusiones, soluciones de cifrado y otras tecnologías que protejan la red y los sistemas. También son responsables de realizar copias de seguridad periódicas, aplicar parches de seguridad, y gestionar los accesos a sistemas críticos. Además, el equipo de TI debe colaborar estrechamente con el CISO para asegurar que las políticas de seguridad se implementen correctamente a nivel técnico.

• **Responsable de Formaciones:** Este rol tiene como objetivo coordinar las actividades de formación y concienciación dentro de la organización, debe organizar y coordinar simulacros de ciberseguridad, como pruebas de phishing, para evaluar y mejorar la capacidad de respuesta de los empleados ante incidentes.

• **Auditores Internos:** Los auditores internos son responsables de realizar auditorías periódicas para garantizar que el SGSI esté cumpliendo su objetivo.

3. Gestión de Riesgos

En la descripción de la metodología, hemos abordado el proceso de gestión de riesgos; esta gestión debe ser dinámica y adaptarse en todo momento al contexto de la empresa. Antes de revisar en profundidad las diferentes fases de la gestión de riesgos, es importante atribuir la responsabilidad de esta.

Generalmente, en organizaciones medianas y grandes que estén estructuradas en áreas o departamentos, cada unidad es responsable de gestionar los riesgos específicos asociados a sus actividades. Por tanto, el responsable de estos riesgos será el cargo de responsabilidad de cada área, y deberá seguir el siguiente procedimiento:

• Identificación de riesgos: El primer paso en la gestión de riesgos es identificar los posibles eventos que puedan afectar los objetivos planteados, determinando los activos de información críticos, como datos confidenciales, aplicaciones de negocio e infraestructura. Es fundamental analizar las amenazas a las que están expuestos, incluyendo riesgos internos, como errores humanos o fallos de hardware, y riesgos externos, como ciberataques. Para realizar una correcta identificación de riesgos, es necesario considerar las causas y el origen de cada riesgo detectado.

Este proceso permite a la organización anticiparse y tomar medidas necesarias para mitigar o evitar la ocurrencia de estos eventos en el futuro.

Aquí se lleva a cabo el inventariado de activos, clasificándolos según criticidad; el listado de potenciales amenazas y la evaluación de vulnerabilidades que podrían ser explotadas ellas; y el estudio de probabilidad de cada evento.

• Análisis de riesgos: El análisis deberá adaptarse a las necesidades y el contexto de la organización, debido a que cada sistema posee controles y procesos distintos que deberán ser atendidos de una forma en particular. Los métodos de análisis pueden ser variados, puede apoyarse de métodos cuantitativos – utilizan datos numéricos y fórmulas -, semicuantitativos – combinan escalas con descripciones - o cualitativos – usan descripciones subjetivas como alto, medio, bajo-.

• Evaluación de riesgos: Utilizar una matriz de evaluación que permita calcular el impacto y la probabilidad de cada riesgo. Esta matriz debe ajustarse y priorizar los riesgos según la potencial afectación en las operaciones. El cálculo elemental es Nivel de Riesgo = Probabilidad de ocurrencia x Impacto.

• Para el tratamiento, existen cuatro tipos de acciones aplicables: mitigación, transferencia, aceptación o evitación. La elección del tratamiento dependerá del nivel de riesgo, los recursos disponibles y los objetivos de la organización.

1. **Mitigación**:
   Consiste en implementar controles y tomar medidas correctivas para reducir la probabilidad de ocurrencia o el impacto del riesgo. Este enfoque busca minimizar la exposición y puede incluir soluciones como firewalls, antivirus, segmentación de redes, copias de seguridad o actualizaciones regulares de software. Por ejemplo, la implementación de un firewall puede reducir significativamente el riesgo de un ataque en la red.
2. **Transferencia**:
   Implica trasladar la responsabilidad del riesgo a un tercero mediante la contratación de seguros o servicios especializados con cláusulas de responsabilidad. Es una opción adecuada para riesgos con un impacto alto que no se pueden eliminar completamente. Por ejemplo, se puede contratar un seguro contra ciberataques o delegar la gestión de la seguridad en un proveedor externo.
3. **Aceptación**:
   Se aplica cuando un riesgo es considerado tolerable y no se implementan medidas adicionales para mitigarlo o transferirlo. Generalmente, esta decisión se toma cuando la probabilidad de ocurrencia o el impacto del riesgo es bajo, o cuando los costes de mitigación o transferencia superan el impacto potencial del riesgo - consecuencias o efectos negativos que un evento de riesgo podría causar si llegara a materializarse -. Los riesgos aceptados deben documentarse y monitorizarse para garantizar que sigan alineados con la tolerancia de riesgo de la organización. En el ámbito de la gestión de información, es común aplicar la aceptación del riesgo en servidores no críticos que no comprometen la continuidad del negocio, ya que el coste de implementar un sistema de redundancia suele ser muy superior al impacto económico del tiempo necesario para recuperar el servidor.
4. **Evitación**:
   Consiste en tomar medidas para eliminar completamente la exposición a un riesgo. Esto implica no involucrarse en actividades o procesos que puedan generar dicho riesgo. Aunque esta opción no siempre es viable, puede aplicarse en situaciones donde los riesgos superan significativamente los beneficios. Por ejemplo, no contratar un proveedor sin las garantías de seguridad suficientes.

El tratamiento de riesgos debe ser un proceso planificado, documentado y revisado periódicamente para adaptarse a los cambios en el entorno y en las operaciones de la organización.

• Monitoreo y revisión: Es fundamental que el SGSI incorpore un monitoreo continuo, revisando la efectividad de los controles de seguridad. Implementar indicadores clave de desempeño (KPI), como el número de incidentes de seguridad resueltos en un periodo determinado o la cantidad de vulnerabilidades críticas detectadas en el plazo de una semana, permite un seguimiento más preciso y un ajuste de los controles conforme a los cambios en el entorno normativo y empresarial.

5. Mejora Continua

La mejora continua y el cumplimiento con la ISO 27001 requieren revisiones y evaluaciones constantes. Para una empresa mediana, se recomienda lo siguiente:

• Auditorías internas: Realizar auditorías periódicas para evaluar si el SGSI cumple con los requisitos internos y con la ISO 27001. Utilizar los resultados para identificar áreas de mejora y para ajustar las políticas de seguridad y los controles.

• Revisión de la dirección: Revisiones periódicas del SGSI para evaluar su alineación con los objetivos empresariales, el desempeño del sistema y posibles áreas de mejora. Se deben tomar en cuenta los cambios regulatorios y tecnológicos para ajustar el SGSI según sea necesario, para ello es recomendable que los miembros del comité de seguridad y la dirección se mantengan informados.

• Actualización de políticas: Las políticas de seguridad deben revisarse y actualizarse periodicamente o cuando surjan nuevos riesgos significativos. Es importante identidicar qué políticas ya no aplican, qué areas no se están cubriendo, y cuales pueden ser más críticas.

6 Proceso de Auditoría

A continuación, se desarrolla un ejemplo real de auditoría de la ISO 27001 en una empresa mediana del sector entretenimiento/ telecomunicaciones.

La auditoría de una norma ISO es un proceso diseñado para evaluar si una organización cumple con los requisitos especificados en la norma, y si el sistema de gestión de seguridad de la información es efectivo.

La ISO 27001 se puede implementar en su totalidad, o por partes. En el caso de implementarse por partes, puede ser por criticidad de los controles, por áreas de la organización, o una implementación limitada por alcance. Este alcance se detallará en el Statement of Applicability, descrito más adelante.

El proceso se lleva a cabo entre dos partes, la parte auditada (la compañía) y la parte auditora (una entidad externa o interna dependiendo del tipo de auditoría).

6.1. Preparativos previos a la auditoría

1. Definición de la fecha y duración: Para una empresa mediana de aproximadamente 200 empleados, la auditoría puede durar entre dos y tres días.
2. Creación del **Plan de auditoría**: Días antes del inicio, la organización debe preparar un plan de auditoría en el que se define el alcance del proceso. Sin embargo, el auditor puede formular preguntas que vayan más allá del alcance

Planificación:

Horario	Lunes 16/12/2024	Martes 17/12/2024	Miércoles 18/12/2024	Jueves 19/12/2024	Viernes 20/12/2024
9:15 - 10:45	ISO 27001: • Contexto de la organización. • Liderazgo • Soporte • Planificación	ISO 27002 - Controles organizativos relacionados con políticas, responsabilidades, información y acceso/autentificación.	ISO 27002 - Controles tecnológicos relacionados con accesos, vulnerabilidades y datos.		ISO 27002 - Controles de personas.
11:15 - 12:45	ISO 27001: • Operación • Evaluación del desempeño • Mejora continua		ISO 27002 - Controles tecnológicos relacionados con seguimiento, sistemas, desarrollo, entornos y cambios.		ISO 27002 - Controles físicos.
14:30 - 16:00		ISO 27002 - Controles organizativos relacionados con proveedores, incidentes, seguridad y otros.			

establecido.

3. Revisión Previa del auditor: El auditor debe revisar resultados de auditorías previas, en caso de haberlas; y analizar la documentación relevante.

6.2. Documentos clave en la auditoría

- La **Política de seguridad de la información:** Como hemos explicado anteriormente, define:

Propósito: Alineado con la ISO, por ejemplo: "Establecer el marco para proteger la información de XXX asegurando su confidencialidad, integridad, etc."

Alcance: Toda la información creada, almacenada o transmitida por la organización, incluyendo empleados, proveedores y stakeholders. También puede ser alcance físico, geográfico…

Principios generales: Como autenticidad, trazabilidad, no repudio, resiliencia o mínimos privilegios.

Responsabilidades:

- Alta dirección: Proporcionar recursos para implementar el SGSI.
- CISO: Coordinar y supervisar la implementación.
- Empleados: Cumplir con las políticas.

Controles: Basados en el Anexo A de la ISO, con recomendaciones detalladas en la ISO 27002.

Cumplimiento y sanciones: Incluye revisión y mejora continua.

- La **evaluación de riesgos,** definida anteriormente.

- El **Statement of Applicability (SoA):** Documento clave en formato tabla (Excel) que detalla los controles selecciónados para gestionar riesgos. Incluye: Los 114 controles del Anexo A, una justificación de su inclusión o exclusión, Referencias a documentos o políticas relacionadas. Sirve como referencia durante la auditoría.

- **Procedimientos operativos**, documentos que describen cómo se deben implementar controles y otras tareas, con el mayor nivel de detalle y precisión posible. Por ejemplo, el procedimiento de gestión de incidentes detalla:

- Definición de incidente de seguridad. Qué se considera un incidente de seguirdad y qué no.
- Alcance del procedimiento.
- Roles y responsabilidades.
- Pasos detallados para la detección, registro, clasificación y evaluación de impacto.

Son documentos muy completos, para crearlos puede ser necesaria la colaboración interdepartamental.

- El **Management Review,** que describe la situación actual de la organización respecto al SGSI, incluyendo el contexto organizativo, eventos relevantes de los meses anteirores a la auditoría, revisión de objetivos y reflexiones, posibles stakeholders y el plan de tratamientos de la evaluación de riesgos. Lo elabora el equipo del comité del SGSI y se firma con anterioridad a la auditoría.

6.3. Etapas de la auditoría

1. **Revisión documental**: primera etapa donde se verifica el nivel de aplicación de la norma. Los criteros incluyen: Actualización de los documentos, alineación con la ISO, impacto práctico de las políticas y procedimientos (nivel de aplicación de las políticas).

2. **Auditoría in-situ**: Dado el modelo de trabajo remoto, se realizan reuniones virtuales. Durante estas entrevistas, el auditor, toma anotaciones de las conversaciones que, en tono amable, mantiene con diversos stakeholders:
   i. Realiza preguntas abiertas o cerradas. Ejemplo: "¿Qué haces si detectas un correo sospechoso?"
   ii. Busca consistencia, comprensión de responsabilidades y evidencia objetiva (logs, reportes de incidentes, etc.).
   iii. Profundiza según sea necesario.
   iv. Ante discrepancias, se toman acciones como solicitar evidencia adicional, entrevistar a otros empleados, reportar hallazgos ("findings").

3. **Clasificación de hallazgos** en No conformidades mayores, si comprometen la eficacia del SGSI pudiendo conllevar a la pérdida de la certificación y al incumplimiento normativo; no conformidades menores, desviaciones puntuales sin un impacto significativo; y observaciones, áreas de mejora o recomendaciones.
4. **Redacción del informe de auditoría**. El informe incluye un resumen ejecutivo, en el que se detalla el alcance, los objetivos y la metodología, los resultados: conformidades, no conformidades y observaciones, la evidencia recopilada y las conclusiones.

6.4. Ciclo de auditoría de la ISO 27001

1. Auditoría inicial: exhaustiva, para evaluar todo el SGSI. En caso de superarla, se obtiene la certificación.

2. Auditorías de seguimiento: anuales, enforcadas en acciones correctivas y mejoras.

3. Auditoría de recertificación: cada tres años, para confirmar la adecuación continua del SGSI.

Una vez entregado el informe de auditoría, existe un plazo de alegaciones en caso de que la organización muestre disconformidades con los resultados obtenidos.

Después de recibir un informe de auditoría, la organización debe analizar los hallazgos y conclusiones presentadas. Este análisis incluye la revisión de las no conformidades, mayores y menores, así como de las observaciones o recomendaciones planteadas por el auditor. El equipo responsable debe asegurarse de entender el impacto de cada hallazgo, identificar las áreas específicas que requieren atención y evaluar las evidencias presentadas. Este proceso inicial permite priorizar los problemas más críticos, especialmente aquellos que podrían comprometer la eficacia del SGSI o su conformidad con la norma.

Una vez identificadas las áreas de mejora, la organización diseña e implementa un plan de acciones correctivas, donde establece los pasos necesarios para resolverlos; asigna responsables, define plazos y asegura los recursos necesarios para abordar los problemas identificados.

Durante la implementación, se monitorea el progreso de las correcciones y se documenta todo el proceso como evidencia de cumplimiento. Una vez completadas, se evalúa la eficacia de las medidas tomadas mediante revisiones internas, pruebas o simulaciones. En auditorías externas, puede ser necesario comunicar los resultados al auditor o incluso someterse a una revisión de seguimiento para confirmar que las no conformidades han sido resueltas de forma satisfactoria. Este enfoque asegura no solo la resolución de los problemas, sino también una mejora continua del SGSI.

7 CONCLUSIONES

Este Trabajo de Fin de Grado se ha centrado en el desarrollo de un marco de gobierno de ciberseguridad adaptado a las necesidades de las empresas medianas, fundamentado en la norma ISO/IEC 27001.

A lo largo del trabajo, se han alcanzado varios objetivos clave. Primero, se ha logrado la comprensión de los estándares ISO/IEC 27000 mediante un análisis exhaustivo de los términos, roles, responsabilidades y principios de gestión de la familia de estándares, estableciendo una base sólida para entender la ciberseguridad en el contexto empresarial. Además, se ha diseñado una metodología detallada para implementar un Sistema de Gestión de Seguridad de la Información (SGSI), que abarca desde la planificación inicial y la identificación de riesgos hasta la mejora continua del sistema, asegurando que el enfoque esté alineado con las mejores prácticas internacionales.

El estudio también incluye una comparativa con normativas nacionales y europeas, como el Esquema Nacional de Seguridad (ENS) y la Directiva NIS2, evidenciando las similitudes y diferencias clave, y mostrando cómo el cumplimiento con ISO/IEC 27001 puede facilitar el alineamiento con otros marcos normativos. Finalmente, se ha propuesto un marco de ciberseguridad práctico que incluye políticas clave, roles y responsabilidades claros, y procesos de gestión de riesgos adaptados a las peculiaridades y necesidades de las empresas medianas.

Este trabajo enfatiza la importancia de la ciberseguridad como un factor crítico para la continuidad operativa y el cumplimiento normativo en un entorno empresarial cada vez más digitalizado. Aunque la implementación de un SGSI puede representar un reto significativo para las empresas medianas, los beneficios asociados, como la reducción de riesgos, o la mejora de la resiliencia, que es especialmente importante para las empresas medianas, ya que, debido a sus recursos limitados, presentan una mayor dificultad para recuperarse de un incidente de ciberseguridad que organizaciones más grandes; el cumplimiento normativo y el incremento de la confianza de los clientes, justifican la inversión.

AGRADECIMIENTOS

Quiero expresar mi agradecimiento a Enric Alibech, por su valiosa orientación, apoyo y consejos a lo largo de todo el proceso de este trabajo.

A mis compañeros de trabajo, cuyo conocimiento y colaboración han sido fundamentales para el desarrollo de este proyecto, gracias por compartir sus ideas y experiencias.

También agradezco a mis compañeros y familiares por su comprensión, paciencia y constante apoyo. Sin la contribución de todos ellos, este trabajo no habría sido posible.

BIBLIOGRAFÍA

[1] ISO/IEC. (2022). ISO/IEC 27001: Information security management systems — Requirements. https://www.iso.org/standard/2700

[2] Gobierno de España. (2022). Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Boletín Oficial del Estado (BOE-A-2022-7191). https://www.boe.es/buscar/doc.php?id=BOE-A-2022-7191

[3] Parlamento Europeo y Consejo de la Unión Europea. (2022). Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifica el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972, y por la que se deroga la Directiva (UE) 2016/1148 (Directiva NIS2). Diario Oficial de la Unión

Europea, L 333, 80-152. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022L2555

[4] (ISC)². (n.d.). Certified Information Systems Security Professional (CISSP). https://www.isc2.org/certifications/cissp

[5] ISACA. (n.d.). Certified Information Systems Auditor (CISA). https://www.isaca.org/credentialing/cisa

[6] ISO. (2019). ISO 31010:2019 Risk management — Risk assessment techniques. https://www.iso.org/standard/65604.html

[7] Gómez, F., & López, A. (2019). Comparativa entre el Esquema Nacional de Seguridad (ENS) y la norma ISO 27001: Implementación de sistemas de gestión de seguridad de la información en el sector público español. Revista de Seguridad y Gestión de Riesgos, 12(3), 45-59. https://www.revistaseguridad.com/articulo/comparativa-iso-27001-ens