UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola Tècnica Superior d'Enginyeria
de Telecomunicació de Barcelona

telecos
BCN

Marco y taxonomía de ciberseguridad para la Pequeña y Mediana Empresa

Trabajo de Final de Grado
presentado en la Escola Tècnica Superior
d'Enginyeria de Telecomunicació de Barcelona
de la Universitat Politècnica de Catalunya
por

Jesús Valero Velasco

En cumplimiento parcial
de los requisitos para la obtención del
GRADO EN INGENIERÍA DE TECNOLOGIAS Y SERVICOS DE TELECOMUNICACIÓN

Director/a: Eva Rodríguez Luna
Ponente: Jesús Valero Velasco

Barcelona, Enero de 2024

Resum

Aquest treball pretén elaborar una guia o recomanació de ciberseguretat a PYMES de qualsevol sector perquè disposin d'un document al qual recórrer quan el negoci s'expandeixi a internet o requereixi d'ell en el seu dia a dia.

Primer es tractarà el context, on s'explica quina situació hi ha actualment, els principals atacs i riscos als quals es veuen exposades les empreses. També es mostrarà els índexs de recuperació i els impactes d'un ciberatac en una Pyme. Finalment, en aquest apartat també veurem la normativa i certificacions de referència en ciberseguretat.

Aquest treball s'ha fet durant la meva experiència laboral en una de les principals consultores del sector, on he visualitzat de primera mà les febleses i les fortaleses de les certificacions de seguretat i a través d'aquestes s'extreu la necessitat d'instruir a petites empreses en seguretat.

Resumen

Este trabajo pretende elaborar una guía o recomendación de ciberseguridad a PYMES de cualquier sector para que dispongan de un documento al que recurrir en cuanto el negocio se expanda a internet o requiera de él en su día a día.

Primero se tratará el contexto, donde se explica qué situación hay actualmente, los principales ataques y riesgos a los que se ven expuestas las empresas. También se mostrará los índices de recuperación y los impactos de un ciberataque en una Pyme. Por último, en este apartado también veremos la normativa y certificaciones de referencia en ciberseguridad.

Este trabajo se ha hecho durante mi experiencia laboral en una de las principales consultoras del sector, donde he visualizado de primera mano las debilidades y las fortalezas de las certificaciones de seguridad y a través de estas se extrae la necesidad de instruir a pequeñas empresas en seguridad.

Summary

The aim of this work is to prepare a cybersecurity guide or recommendation for SMEs in any sector so that they have a document to refer to as soon as the business expands to the Internet or requires it in its day-to-day operations.

First, the context will be discussed, explaining the current situation, the main attacks and risks to which companies are exposed. We will also show the recovery rates and the impacts of a cyber-attack on an SME. Finally, in this section we will also see the regulations and certifications of reference in cybersecurity.

This work has been done during my work experience in one of the main consulting firms in the sector, where my personal experience let me detect the weaknesses and strengths of security certifications and through these the need to instruct small companies in security is extracted.

Agradecimientos

Quisiera expresar mi más sincero agradecimiento a todos aquellos que brindaron su apoyo y contribuyeron al éxito de este trabajo. Agradezco a mis amigos y familiares por su inquebrantable respaldo emocional y motivación constante. A mis valiosos compañeros de trabajo, les agradezco por su colaboración y por compartir sus conocimientos, enriqueciendo así el desarrollo de este proyecto.

Quiero dedicar un agradecimiento especial a Eva Rodriguez Luna, cuya dedicación y orientación fueron fundamentales en cada etapa de este trabajo.

A todos ustedes, mi más profundo agradecimiento. Este proyecto no solo fue un esfuerzo individual, sino el resultado del apoyo y la colaboración de una red invaluable de personas extraordinarias.

Historial de revisión y aprobación

Revisión	Fecha	Autor(es)	Descripción
1.0	23/08/2023	AME	Creación del Documento
1.1	24/12/2023	AME, JPV	Revisión del documento
2.0	08/01/2024	AME, MLO	Versión revisada
3.0	18/01/2024	AME	Versión final

LISTA DE DISTRIBUCIÓN DEL DOCUMENTO

Rol	Apellido(s) y Nombre
Estudiante	Jesús Valero Velasco
Tutor del proyecto	Eva Rodríguez Luna

Escrito por:		Revisado y aprobado por:	
Fecha	18/01/2024	Data	18/01/2024
Nombre	Jesús Valero Velasco	Nombre	Eva Rodríguez Luna
Rol	Autor/a del Proyecto	Rol	Director del Proyecto

Índice general

Índice de figuras

Índice de tablas

Siglas i acrónimos

BOE Boletín Oficial del Estado

CCN Centro Criptográfico Nacional

CCN-STIC Centro Criptográfico Nacional Seguridad Tecnologías de la Información

CNMC Comisión Nacional de los Mercados y la Competencia

DDOS Distributed Denial of Service

ENISA Agencia de la Unión Europea para la Ciberseguridad

ENS Esquema Nacional de seguridad

ETSETB Escola Tècnica d'Enginyeria de Telecomunicació de Barcelona

IASME Information Assurance for Small and Medium Enterprises

ISO International Organization for Standarization

INCIBE Instituto Nacional de Ciberseguridad de España

NIST National Institute of Standards and Technology

RGPD Reglamento general de protección de datos

SGSI Sistema de gestión de la Seguridad de la información

TISAX Trusted Information Security Assessment Exchange

OWASP Open Web Application Security Project

Glosario

Activos confidenciales: Información sensible o crítica para una organización que requiere una protección especial para garantizar su confidencialidad e integridad.

Activos esenciales: Elementos cruciales para la operación de una organización, cuya pérdida o compromiso podría tener un impacto significativo en su funcionamiento.

Bastionado: Proceso de fortalecimiento y aseguramiento de la seguridad de un sistema, red o infraestructura para resistir ataques.

Business Impact Analysis: Evaluación sistemática de los efectos potenciales que la interrupción de procesos y funciones empresariales puede tener en una organización.

Cloud: Almacenamiento y procesamiento de datos en servidores remotos a través de Internet en lugar de en un servidor local.

Ciberdelincuente: Individuo que realiza actividades delictivas en el ámbito cibernético, como ataques, fraudes o robo de información.

Common Criteria: Estándar internacional para la evaluación y certificación de la seguridad de productos y sistemas de tecnologías de la información.

Control de parcheado: Gestión y aplicación de actualizaciones de seguridad y correcciones de software para prevenir vulnerabilidades.

CyberEssential Plus: Certificación que evalúa y garantiza la ciberseguridad de organizaciones, especialmente pymes, mediante estándares establecidos.

Data leaks: Liberación no autorizada de información confidencial o sensible, poniendo en riesgo la privacidad y seguridad de la organización.

Diagramas de red: Representación gráfica de la arquitectura y conexiones de una red informática.

Disinformation o Misinformation: Difusión deliberada de información falsa (desinformación) o la propagación involuntaria de información incorrecta (desinformación).

Dispositivo de almacenamiento extraíble: Dispositivo como USB o disco externo utilizado para almacenar datos que puede ser conectado y desconectado fácilmente de una computadora.

Enmascaramiento de datos: Proceso de ocultar o proteger información sensible mediante técnicas como el cifrado.

Entorno de compartición online: Plataforma o espacio digital donde los usuarios pueden compartir información y colaborar en línea.

Filtrado web: Control de acceso a sitios web basado en reglas para prevenir el acceso a contenido no deseado o malicioso.

Firewall: Barrera de seguridad que controla el tráfico de red y protege una red privada al bloquear o permitir ciertos tipos de comunicación.

GitHub: Plataforma de desarrollo colaborativo que utiliza control de versiones para proyectos de software.

Hacking ético: Práctica de pruebas de seguridad autorizadas para identificar vulnerabilidades en sistemas informáticos.

Indisponibilidad: Estado en el cual un sistema o servicio no está accesible o no funciona correctamente.

Ingeniería Social o Social Engineering: Técnica de manipulación psicológica utilizada para obtener información confidencial o inducir a la gente a realizar acciones específicas.

Log: Registro detallado de eventos o actividades en un sistema o red, utilizado para fines de auditoría y análisis.

Malware: Software malicioso diseñado para dañar, alterar o robar información de un sistema o red.

Medidas de seguridad perimetrales: Estrategias de seguridad implementadas en los bordes de una red para protegerla contra amenazas externas.

Metadatos: Datos que proporcionan información sobre otros datos, como la fecha de creación, autor o ubicación.

Misinformation: Difusión involuntaria de información incorrecta.

Pentest: Prueba de penetración, evaluación de seguridad realizada por expertos para identificar vulnerabilidades en sistemas.

Perfil de Protección (PP): Documento que define los requisitos de seguridad para un producto o sistema específico.

Phishing: Técnica de engaño que utiliza correos electrónicos u otros mensajes para obtener información confidencial de manera fraudulenta.

Plan de salida: Estrategia y procedimientos para la gestión de crisis y la recuperación tras un incidente de seguridad.

Portal web: Sitio en línea que proporciona acceso a recursos, información o servicios a través de un navegador web.

Ransomware: Tipo de malware que cifra archivos y exige un rescate para restaurar el acceso.

Red de invitados: Segmento de red separado para dispositivos de usuarios no confiables o visitantes.

Root kits: Conjunto de herramientas que permiten el acceso no autorizado y ocultan actividades maliciosas en un sistema.

Salvaguardas: Medidas de seguridad implementadas para proteger activos y prevenir o minimizar riesgos.

Segregación de redes: Separación de redes para prevenir el acceso no autorizado y limitar la propagación de amenazas.

Software antimalware: Programa diseñado para detectar y eliminar software malicioso.

Software malicioso: Programas destinados a dañar, alterar o robar información de un sistema o red.

Spyware: Software que recopila información de un usuario sin su conocimiento.

Start-up: Empresa emergente o en fase inicial que busca desarrollar un modelo de negocio escalable.

Supply chain attacks: Ataques que apuntan a comprometer la cadena de suministro de una organización.

Threat against availability, Denial of Service: Amenaza que busca interrumpir o limitar el acceso a servicios, sistemas o redes.

Threat against availability, Internet threats: Amenazas en línea que buscan afectar la disponibilidad de servicios y recursos.

Testing: Evaluación y verificación sistemática del rendimiento y la seguridad de sistemas o aplicaciones.

Troyano: Tipo de malware que se disfraza de un programa legítimo para infiltrarse en un sistema sin ser detectado.

Vulnerabilidades 0 day: Brechas de seguridad en software desconocidas por el proveedor y, por lo tanto, sin parches disponibles.

CAPÍTULO 1

Introducción

Actualmente las PYMES son uno de los principales objetivos de los ciberdelincuentes[1]]. Los datos de la situación actual es que nos encontramos ante muchos vectores de ataque que podrían afectar a una pyme. El principal problema con el que nos encontramos es que no se dispone de una priorización de medidas de seguridad, ni concienciación suficiente como para que esta parte del negocio sea una prioridad para el tejido empresarial. En el caso concreto de las pymes nos encontramos que no solo no se dispone de la voluntad si no que se le agrega la problemática de no disponer de medios suficientes como para cubrir toda una seguridad completa, mucho menos de implantar un sistema de gestión de seguridad de la información (SGSI a partir de ahora) o medidas técnicas que las protejan.

Por tal de entender esto, destacamos que la visión del trabajo sobre la seguridad se centra en un apartado económico, es decir, que siempre se intentará tener el mejor compromiso entre la seguridad, la inversión en ella y el mantenimiento necesario.

Cuando una pyme crece y colabora con otras entidades, se encuentra con la tesitura de que necesita certificarse para llegar a grandes contratos. Muchas veces, pero, la normativa no está pensada para empresas como las pymes, y se centran en aspectos generalistas de la seguridad.

La idea es dar una guía a las pymes a la que puedan recurrir para saber que proteger y cómo priorizar los principales puntos de la seguridad. Esto ayudará principalmente a dos factores:

- Reducir el impacto de un ciberataque sobre ellas.
- Incrementar sus posibilidades de contratos.
- Facilitar la tarea de certificar si se cree oportuno.

[1] https://compartiendoconocimiento.elmundo.es/las-pymes-seran-uno-de-los-principales-objetivos-de-los-ciberataques-en-2023

1.1. Objetivos del trabajo

1.1.1. Objetivos principales

Debido a que la actual normativa de seguridad se centra principalmente en la gran empresa, este trabajo pretender poner el foco en la pyme, la cual representa la mayor parte del tejido empresarial de España. Es por lo que, para adecuar la normativa ya presente, adaptaremos los requisitos y los reflejaremos en una guía fácil de seguir y que posibilite poder reconocer cual es la situación en la que se encuentran.

Uno de los objetivos principales al desarrollar esta guía es proporcionar a las pymes un marco de referencia estructurado y coherente, que les permita comprender y aplicar de manera efectiva los requisitos normativos pertinentes a su industria. Al integrar elementos clave de normativas reconocidas, se busca simplificar el proceso de cumplimiento, eliminando la complejidad inherente a la interpretación y aplicación de diversas regulaciones.

Además, la guía busca ser un instrumento que proporcione claridad y transparencia a las Pymes en relación con los estándares que deben cumplir. Esto implica establecer criterios medibles y objetivos que permitan a las empresas evaluar su desempeño y progreso de manera sistemática. La certificación resultante no solo constituye un reconocimiento formal del cumplimiento normativo, sino que también brinda a las pymes la oportunidad de destacarse en el mercado al demostrar su compromiso con la calidad y la legalidad.

Otro objetivo es fomentar la mejora continua dentro de las pymes. La guía no solo actúa como un medio para alcanzar la certificación, sino que también sirve como una herramienta de gestión que impulsa la excelencia operativa. Al identificar áreas de mejora y establecer prácticas recomendadas, las pymes pueden evolucionar constantemente, adaptándose a los cambios normativos y elevando sus estándares de calidad.

En conclusión, la elaboración de una guía basada en requisitos normativos busca proporcionar a las pymes una herramienta integral que no solo simplifica el camino hacia la certificación, sino que también impulsa la mejora continua, la transparencia y la eficiencia operativa.

1.1.2. Objetivos secundarios

Uno de los objetivos secundarios a destacar es el fortalecimiento de la cultura de cumplimiento normativo dentro de las pymes. Al proporcionar una guía clara y fácil de seguir, se busca fomentar la comprensión y adopción de buenas prácticas empresariales, estableciendo una base sólida para la conformidad con las normativas relevantes. Este proceso de internalización de normas contribuye a la creación de una cultura organizativa que valora la legalidad y la ética en todas las operaciones, generando confianza tanto interna como externamente.

Asimismo, la guía busca mejorar la capacidad de las pymes para enfrentar riesgos y gestionar crisis. Al incorporar requisitos que aborden aspectos críticos de la gestión empresarial, como la seguridad, la continuidad operativa y la protección de datos, se brinda a las empresas una herramienta integral para anticipar, prevenir y responder eficazmente a posibles contingencias. Esto no solo contribuye a la resiliencia empresarial, sino que también eleva la reputación y la confianza de los clientes y proveedores.

Otro objetivo secundario es facilitar la integración de las pymes en cadenas de suministro más amplias y exigentes. La certificación basada en la guía no solo representa un reconocimiento interno, sino que también sirve como un distintivo ante socios comerciales, clientes y proveedores. Al seguir una guía alineada con estándares reconocidos, las pymes pueden aumentar su atractivo como colaboradores comerciales, abriendo oportunidades para la expansión de sus redes y la participación en mercados más competitivos.

1.2. Requisitos y especificaciones

El desarrollo de esta guía conlleva la consecución de diversos hitos que son cruciales para fortalecer la seguridad empresarial y contribuir al bienestar de la organización. Al establecer un marco normativo específico en esta área, se lograrían los siguientes hitos:

Estándares de Seguridad Definidos:

La creación de un cuerpo normativo establece estándares claros y específicos en materia de seguridad para las pymes. Estos estándares proporcionan pautas precisas sobre las prácticas y controles de seguridad que deben implementarse, lo que contribuye a reducir la ambigüedad y a mejorar la comprensión de las medidas de seguridad necesarias.

Gestión Integral de Riesgos:

La certificación de seguridad para pymes impulsa la implementación de un enfoque integral de gestión de riesgos. Al identificar y evaluar los riesgos asociados a la seguridad de la información, la normativa facilita la implementación de medidas preventivas y correctivas, reduciendo la vulnerabilidad de la empresa ante posibles amenazas.

Protección de la Información Sensible:

Un hito fundamental es la protección de la información sensible y confidencial. La certificación establece directrices específicas para asegurar la confidencialidad, integridad y disponibilidad de los datos críticos de la empresa, ya sea información financiera, datos del cliente o propiedad intelectual.

Resiliencia ante Ciberataques:

La implementación de la certificación fortalece la resiliencia de las pymes ante posibles ciberataques. Al adoptar medidas de seguridad robustas y establecer protocolos de respuesta a incidentes, las empresas pueden minimizar el impacto de los ataques cibernéticos y recuperarse de manera más efectiva.

Cumplimiento Normativo y Legal:

La certificación asegura que la empresa cumpla con las leyes y regulaciones en materia de seguridad de la información. Este cumplimiento no solo evita posibles sanciones legales, sino que también refuerza la reputación de la empresa y la confianza de los clientes y socios comerciales.

Mejora Continua en Seguridad:

El cuerpo normativo de seguridad establece un marco para la mejora continua. La certificación no es un evento único, sino un proceso dinámico que fomenta la revisión constante de las prácticas de seguridad y la adaptación a las evoluciones.

1.3. Métodos y procedimientos

La elaboración de este proyecto ha implicado la implementación de un conjunto diverso de métodos y procedimientos, aprovechando fuentes clave como las principales normativas, casos prácticos e informes de instituciones reconocidas. Sin embargo, se ha de abordar de manera crítica la limitación de estos informes, que a menudo presentan dos desafíos significativos: la estadística del superviviente (a estadística solo reporta quien ha sobrevivido a un ataque) y la extrapolación de datos provenientes de empresas que no son pymes.

En primer lugar, se ha realizado un exhaustivo análisis de las principales normativas de seguridad, incluyendo la ISO 27001 [2]y 21002, el marco del NIST, los Criterios Comunes, el Esquema Nacional de Seguridad (ENS[3]) y el estándar CyberEssential Plus[4]. Estas normativas han proporcionado un marco teórico robusto que ha sido adaptado cuidadosamente para ajustarse a las características y necesidades específicas de las pymes, asegurando así su aplicabilidad real en este entorno empresarial.

La utilización de casos prácticos ha enriquecido el proyecto al ofrecer ejemplos concretos de situaciones reales en las que las medidas de seguridad han demostrado ser efectivas o han presentado desafíos específicos. Esta metodología ha permitido extraer lecciones valiosas y aplicarlas de manera práctica, considerando las limitaciones de recursos y la realidad operativa de las pymes.

En relación con los informes de instituciones, cabe reconocer que estos informes a menudo solo registran casos de éxito o aquellos con impacto limitado, y por eso se ha trabajado para equilibrar la perspectiva, considerando tanto los éxitos como los incidentes menos visibles, a fin de obtener una visión más completa y realista de las amenazas y vulnerabilidades.

Al extraer datos provenientes de informes que originalmente se centran en empresas de mayor magnitud, se ha buscado identificar similitudes y diferencias entre las dinámicas de seguridad de grandes corporaciones y las pymes, ajustando cuidadosamente la información para que sea relevante y aplicable a su contexto específico. En resumen, la metodología aplicada ha sido integral, integrando normativas, casos prácticos e informes institucionales, mientras se abordan críticamente las limitaciones inherentes a las estadísticas y la extrapolación de datos.

---

[2] International Organization for Standardization. "ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements." Geneva, Switzerland: ISO, 2013. Estándar ISO 27002

[3] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. (2022). Boletín Oficial del Estado. Recuperado de https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191

[4] Cyber Essentials Plus. (s.f.). National Cyber Security Centre. Recuperado de https://www.ncsc.gov.uk/cyberessentials/overview

1.4. Plan de trabajo

El plan de trabajo se estructura en dos bloques fundamentales: el Estudio Teórico y el Desarrollo Normativo. En el primer bloque, nos sumergiremos en la comprensión profunda del contexto del tejido empresarial y las normativas existentes hasta la fecha. Este proceso se dividirá en tres tareas principales. Inicialmente, se llevará a cabo una investigación detallada para comprender el panorama actual de amenazas cibernéticas, destacando casos de estudio relevantes en el sector empresarial. Seguidamente, se realizará un análisis exhaustivo de las normativas existentes en ciberseguridad a nivel nacional e internacional, evaluando su aplicabilidad a la realidad de la organización. La última tarea consistirá en un estudio minucioso del tejido empresarial, identificando activos críticos, evaluando la infraestructura tecnológica y conduciendo entrevistas con equipos clave para entender los procesos de negocio y las interconexiones.

El segundo bloque, el Desarrollo Normativo, abordará la extrapolación de principios y requisitos fundamentales de las normativas estudiadas en la primera fase. Esto conducirá a la redacción de una norma adaptada específicamente a las necesidades de las pequeñas y medianas empresas (pymes). Simultáneamente, se diseñará un ejemplo teórico que ilustre la aplicación práctica de la norma en un entorno empresarial. Este bloque se distribuirá en tres tareas esenciales.

La coherencia entre ambas fases del plan garantiza una transición fluida desde la adquisición del conocimiento teórico hasta la aplicación práctica en el desarrollo normativo. Este enfoque integral permitirá una comprensión más profunda de las necesidades específicas de la organización y facilitará la creación de un marco normativo sólido y adaptado a las particularidades de las pymes.

El plan establecido permanece sin cambios significativos. Sin embargo, debido a restricciones de tiempo, lamentablemente, no hemos tenido la oportunidad de incluir más ejemplos detallados en las distintas fases del proyecto.

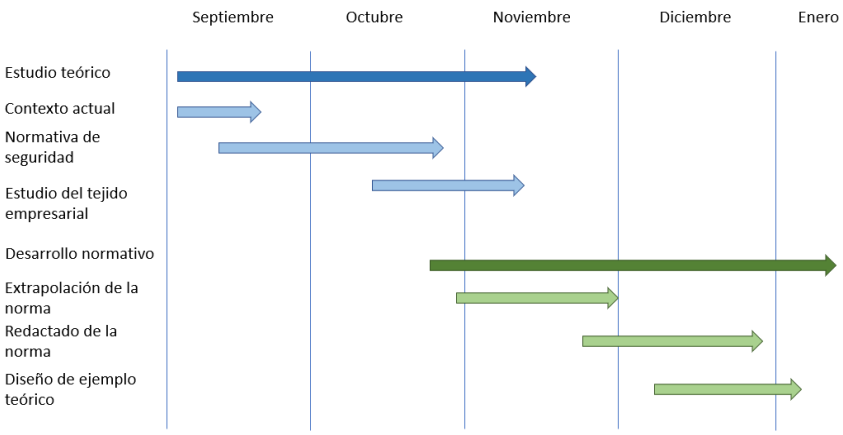

Figura 1. Diagrama Gant del plan de trabajo

En el marco del estudio normativo, se estableció como fecha límite el 15 de noviembre para garantizar una recopilación exhaustiva del contexto empresarial y normativo hasta la fecha. Para el desarrollo normativo, se fijó el 15 de enero como plazo final para la extrapolación de la norma, la redacción específica para pymes y el diseño de un ejemplo teórico. Sin embargo, los demás hitos, que involucraban tareas más complejas y difíciles de cuantificar temporalmente, no fueron asignados a fechas específicas, permitiendo flexibilidad para abordar adecuadamente cada fase del proyecto.

CAPÍTULO 2

Estado del arte de la ciberseguridad

En el contexto global actual, la ciberseguridad ha emergido como un elemento crítico que impulsa y protege las operaciones en la era digital. La interconexión global, el avance tecnológico y la creciente dependencia de las organizaciones en entornos virtuales han generado una complejidad sin precedentes en la gestión de la seguridad de la información.

El aumento constante de amenazas cibernéticas sofisticadas, como el malware, los ataques de ransomware y la ingeniería social, ha puesto de manifiesto la necesidad urgente de una infraestructura digital segura. Los ciberdelincuentes operan a escala global, aprovechando vulnerabilidades en sistemas informáticos, redes y dispositivos para acceder, comprometer y explotar datos confidenciales.

En este panorama, los gobiernos, las empresas y los usuarios individuales se encuentran en una constante carrera para adaptarse y fortalecer sus medidas de ciberseguridad. Las normativas y estándares internacionales, como ISO 27001 y NIST, se han convertido en referentes cruciales para guiar la implementación de prácticas robustas de seguridad de la información.

La ciberseguridad ya no es solo una preocupación tecnológica, sino un componente integral de la resiliencia organizacional y la protección de la privacidad. En este escenario dinámico, la colaboración global, la educación continua y la adaptabilidad son esenciales para enfrentar las amenazas en constante evolución y garantizar un entorno digital seguro y confiable.

2.1. Situación Actual

El mercado actual tiende a usar internet. Según datos del CNMC, la estadística en 2021 tendió al alza y no ha dejado de subir año tras año.

Figura 2. Gráfico evolución del volumen de comercio electrónico en España5

Estos datos reflejan el panorama económico español y de las pymes con relación a la tecnología, muchas de ellas recurriendo al internet o entendiendo el internet como un modelo de negocio.

El Mundo [6]publica que el 60% de las empresas atacadas por un ciberataque se ven obligadas a cerrar. Esto es debido a que la interrupción del servicio continuada o el secuestro de los datos suelen ser impedimentos suficientes. Este mismo artículo alienado con el Instituto Nacional de Ciberseguridad (INCIBE) cuantifica el daño por ciberataque entre 3.000 y 75.000 euros.

[5] Comisión Nacional de los Mercados y la Competencia (CNMC). (2023, 30 de junio). Informe de comercio electrónico IVT22. Recuperado de https://www.cnmc.es/prensa/comercio-electronico-IVT22-20230630

[6]El Mundo. (s.f.). El 60% de las empresas que sufren un ciberataque se ven obligadas a cerrar. Recuperado de https://ahoramascerca.elmundo.es/ciberseguridad/el-60-de-las-empresas-que-sufren-un-ciberataque-se-ven-obligadas-a-cerrar#:~:text=Seg%C3%BAn%20datos%20de%20Kaspersky%20Lab,superarlo%20y%20tengan%20que%20cerrar.

Según la European Union Agency for Cybersecurity o ENISA, en el documento Threat landscape de 2022 durante este último ciclo de 2022 y teniendo en cuenta 2021 los principales ataques son los siguientes:

- Ramsomware: Referido como el secuestro de activos informáticos mediante encriptación.
- Malware: Inyecciones de código malicioso. Dentro de esta categoría están los spyware, troyanos, software malicioso y root kits.
- Social Engeniering: Uso de un gran rango de mecanismos para engañar a la víctima en que ceda información o acceso al atacante. Encontramos como máximo exponente el phising.
- Threat against data: Definimos estos ataques como los cuales pretenden acceder a información protegida distinguiendo entre dos, data breach (ataque intencionado para acceder a esta información) y data leak (de forma no intencionada, revelar o abrir una vulnerabilidad).
- Threat against availability, Denial of service: Los ataques de denegación de servicio son una de las principales amenazas. Este ataque interrumpe la disponibilidad de un servicio online.
- Threats against availability, Internet threats: Aparte de atacar a los servicios online, el internet se ha vuelto imprescindible para muchos negocios. Este ataque se centra en quitar la cobertura de internet en una empresa.
- Disinformation – misinformation: Las campañas de desinformación se han convertido en un ataque para desprestigiar entes políticos y privados. Pese a esto, a las pymes no se les espera como posible ataque y no se analizará durante este trabajo.
- Supply Chain Attacks: Este ataque se centra en la conexión entre proveedores para impedir los principales suministros online de una empresa.

Hemos de tener en cuenta que como también indica el informe, el phishing sigue siendo la mayor fuente de ciberataques. Estos ataques se centran en la falta de concienciación del usuario y en su habilidad de engañar y dar información al atacante.

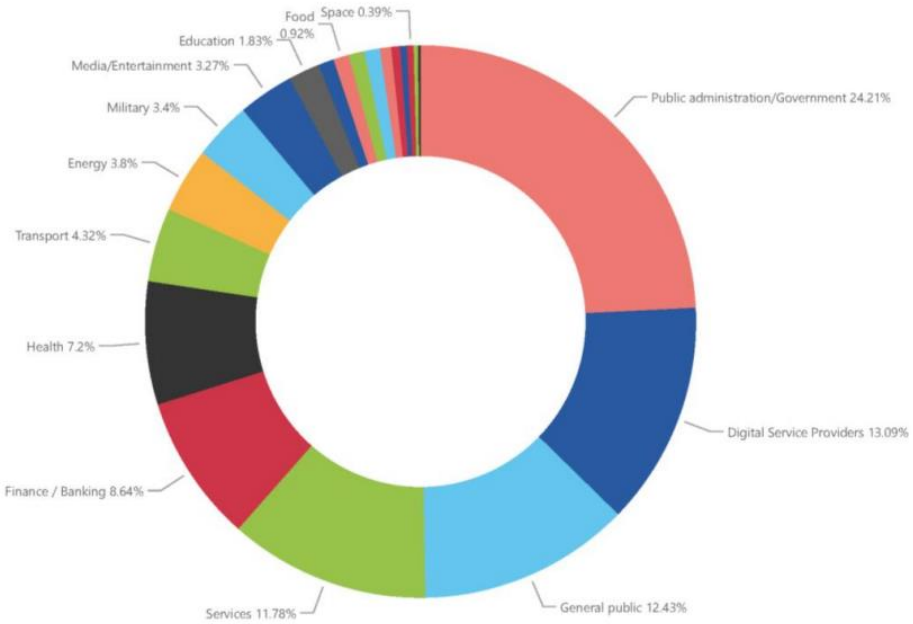

Figura 3 Grafico de objetivos más atacados según su naturaleza

En este gráfico vemos como los servicios representan el 11.77 por ciento de los ataques registrados. Cabe destacar que siempre existe una capa de ataques que no se comunican a los organismos estatales (como el Centro Criptográfico Nacional o el Instituto Nacional de Ciberseguridad) y por tanto se puede entrever que hay una parte que no se contabiliza.

Aun así, nos indica que, aunque se priorizan servicios públicos, se hace también daño al tejido industrial.

Respecto a los principales ataques, se destacan los siguientes factores que pueden comprometer las pymes:

- La forma más efectiva de inicio de ataque es un ramsowares es a través de phishing (punto 3.1.2 reporte ENISA). Esto implica que es vital para la supervivencia a este tipo de ataque la concienciación de los empleados.
- Los ataques sobre vulnerabilidades 0 day suelen se han incrementado al aumentar la madurez de las empresas grandes en materia de seguridad. La conclusión obvia es que cada vez es más necesario tener una política de parcheo adecuada.

2.2. Análisis normativo

En el ámbito empresarial actual, la seguridad de la información se ha erigido como un pilar fundamental para salvaguardar la integridad, confidencialidad y disponibilidad de los datos. En el proceso de elaboración de una guía de seguridad específicamente diseñada para pymes, resulta imperativo examinar las normativas nacionales e internacionales que establecen los estándares y directrices para asegurar entornos empresariales resilientes y protegidos.

Este análisis se centrará en inspeccionar normativas ya conocidas, tales como la ISO 27001 y 21002, el marco del NIST (Instituto Nacional de Estándares y Tecnología), los Criterios Comunes (Common Criteria), el Esquema Nacional de Seguridad (ENS) y el estándar CyberEssential Plus. Cada una de estas normativas representa un conjunto de principios, controles y mejores prácticas que constituyen la columna vertebral para la formulación de estrategias de seguridad robustas y adaptadas a las necesidades específicas de las pymes.

Exploraremos a fondo la contribución de cada normativa, destacando las piezas fundamentales que serán extraídas para la confección de una guía de seguridad clara, accesible y, sobre todo, aplicable. Este enfoque permitirá no solo comprender la variedad de requisitos normativos, sino también discernir las áreas clave.

2.2.1. Estándares de seguridad internacionales

2.2.1.1. ISO 27001 & 27002

ISO 27001 [7]es la normativa de referencia para aspectos de seguridad. Se mantiene en el mercado como la normativa básica de un sistema de seguridad de la información. Esta suele ser requerida por algunas empresas como mínimo de seguridad, pero no ofrece una seguridad integral.

Este estándar se centra en el sistema de gestión de seguridad de la información. Esto último aporta mucha información de lo que pretende el estándar, proteger la información, evitar que se obtenga de cualquier medio no autorizado y disponer de un ciclo de vida correcto y protegido.

Cualquier ISO se obtiene mediante auditoría. Estos procesos, aunque pueden variar según la certificadora, se centra en los siguiente:

1. **Preparación:**

Definición de Objetivos: El primer paso es establecer los objetivos y alcance de la auditoría. Esto implica determinar qué partes del SGSI se auditarán, las fechas y la duración de la auditoría, así como los recursos necesarios.

Selección del Equipo Auditor: Se elige un equipo de auditores competentes y, si es necesario, se nombrará un líder de equipo.

Revisión de documentación: Los auditores revisan la documentación del SGSI, que incluye la política de seguridad, procedimientos, registros y otros documentos relevantes.

2. **Planificación:**

Plan de Auditoría: Se desarrolla un plan de auditoría detallado que incluye los objetivos, el alcance, los criterios de auditoría (generalmente los requisitos de ISO 27001), el programa de auditoría, y la asignación de tareas y responsabilidades.

3. **Ejecución de la Auditoría:**

Entrevistas: Los auditores llevan a cabo entrevistas con el personal relevante para comprender cómo se implementa el SGSI en la práctica.

Revisión de Documentos: Se revisan los registros y documentos para verificar que se estén siguiendo los procedimientos documentados.

Evaluación de Controles: Los auditores evalúan si los controles de seguridad definidos en el SGSI están funcionando como se espera.

[7] International Organization for Standardization. "ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements." Geneva, Switzerland: ISO, 2013. Estándar ISO 27002

4. **Hallazgos y Conclusiones:**

No conformidades y Hallazgos: incumplimiento o no conformidad con los requisitos de ISO 27001, debe establecerse un plan para solventarlo y resolverse en un tiempo pactado.

Hallazgos Positivos: Se reconocen las áreas en las que el SGSI está funcionando efectivamente.

Conclusiones Preliminares: El equipo auditor puede proporcionar conclusiones preliminares durante la auditoría o al finalizarla.

5. **Informe de Auditoría:**

Informe de Auditoría: Se prepara un informe de auditoría que incluye los hallazgos, las no conformidades, las áreas de cumplimiento y cualquier recomendación para mejoras.

6. **Seguimiento:**

Plan de Acción Correctiva: La organización auditada debe desarrollar un plan de acción correctiva para abordar las no conformidades identificadas.

Verificación de Acciones Correctivas: En una auditoría de seguimiento, se verifica si las acciones correctivas se han implementado de manera efectiva.

7. **Cierre de la Auditoría:**

Informe Final: Después de que se hayan implementado las acciones correctivas y se haya verificado su efectividad, se emite un informe final que detalla el estado final de cumplimiento.

8. **Seguimiento Continuo:**

La auditoría ISO 27001 es un proceso continuo. La organización debe mantener su SGSI y llevar a cabo auditorías regulares para garantizar el cumplimiento continuo de los requisitos de seguridad.

Gracias a esto, las empresas confían en que las empresas que obtienen el certificado son seguras y se pueden colaborar con ellas.

2.2.1.2. NIST

NIST[8], o el Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, por sus siglas en inglés), es una agencia del Gobierno de los Estados Unidos que se dedica a promover y fomentar la innovación y la competitividad industrial a través del desarrollo y la promulgación de estándares y pautas, entre otros recursos.

[8] National Institute of Standards and Technology (NIST). (s.f.). Recuperado de https://www.nist.gov/

Dentro de sus estándares se puede encontrar un conjunto con recomendaciones técnicas que propone cómo llevar la seguridad de una organización. Al contrario que el resto, esta no se puede certificar y, por ende, no se puede usar con otras compañías como certificación para asegurar la seguridad de un sistema.

Algunos documentos para destacar son:

- **Marco de Ciberseguridad del NIST (NIST Cybersecurity Framework):** Este marco proporciona una estructura para que las organizaciones comprendan, gestionen y reduzcan sus riesgos de ciberseguridad. Se divide en cinco funciones principales: Identificar, Proteger, Detectar, Responder y Recuperar.
- **Guía NIST SP 800-53[9]:** Esta guía ofrece un conjunto de controles y pautas de seguridad de la información que se utilizan para proteger los sistemas de información y las redes. Estos controles son ampliamente adoptados por organizaciones gubernamentales y privadas.
- **Guía NIST SP 800-171[10]:** Diseñada específicamente para contratistas y proveedores del Gobierno de EE. UU., esta guía establece requisitos para proteger información no clasificada pero sensible.
- **NIST SP 800-30[11]:** Esta guía describe el proceso de gestión de riesgos de ciberseguridad, que incluye la identificación, la evaluación y la mitigación de riesgos en sistemas de información.
- **NIST SP 800-66[12]:** Ofrece orientación sobre la seguridad de la atención médica, incluida la protección de la información médica electrónica

Está escrita desde el punto de vista de la implementación y se hace difícil de seguir para gente no acostumbrada a la lectura técnica normativa. Aun así, es un buen punto para la información de tecnologías complejas y cómo securizar entornos desconocidos.

[9] National Institute of Standards and Technology (NIST). (2020). Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations. Retrieved from https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

[10] National Institute of Standards and Technology (NIST). (2020). Special Publication 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Retrieved from https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

[11] National Institute of Standards and Technology (NIST). (2012). Guide for Conducting Risk Assessments (Special Publication 800-30 Revision 1). Retrieved from https://csrc.nist.gov/pubs/sp/800/30/r1/final

[12] National Institute of Standards and Technology (NIST). (2004). An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (Special Publication 800-66 Revision 1). Retrieved from https://csrc.nist.gov/pubs/sp/800/66/r1/final

2.2.1.3. Common criteria

Common criteria [13]es un sistema apoyado por diferentes países, como Estados Unidos, Reino Unido, Francia, Alemania o España, por ejemplo, certifica productos de carácter tecnológico con un criterio unificado para poder comparar productos IT por su seguridad. Esto ayuda a agencias gubernamentales y empresas a escoger qué tipos de sistemas son de confianza para su adquisición.

Para poder certificar un producto se requiere que el solicitante cumpla con:

- **Perfil de Protección (PP, por sus siglas en inglés):** Un Perfil de Protección es un documento que describe los requisitos de seguridad específicos para un tipo particular de producto o sistema. Define las amenazas que se deben mitigar, los objetivos de seguridad y los requisitos funcionales y de aseguramiento que deben cumplirse.
- **Requisitos Funcionales (FR, por sus siglas en inglés):** Los Requisitos Funcionales describen qué debe hacer el sistema o producto en términos de seguridad. Estos requisitos se dividen en categorías, como identificación y autenticación, control de acceso, auditoría y más.
- **Requisitos de Aseguramiento (AR, por sus siglas en inglés):** Los Requisitos de Aseguramiento se refieren a cómo se debe implementar, mantener y evaluar la seguridad del producto o sistema. Esto incluye aspectos como el diseño seguro, la documentación, la capacitación del personal y la evaluación de la seguridad.
- **Niveles de Evaluación (EAL, por sus siglas en inglés):** Common Criteria utiliza un sistema de Niveles de Evaluación para indicar el grado de rigor y profundidad de la evaluación. Los niveles van desde EAL1 (el más bajo) hasta EAL7 (el más alto). Cuanto mayor sea el nivel, más rigurosos serán los requisitos y las pruebas de seguridad.
- **Documentación de Seguridad:** El fabricante o desarrollador del producto o sistema debe proporcionar una documentación completa que describa cómo se implementan los requisitos de seguridad, cómo se lleva a cabo la gestión de riesgos y cómo se realiza la evaluación de la seguridad.
- **Evaluación Independiente:** La evaluación de Common Criteria generalmente se realiza por un laboratorio independiente de seguridad de la información. Este laboratorio revisa la documentación, realiza pruebas y verifica que el producto o sistema cumpla con los requisitos especificados en el Perfil de Protección.
- **Certificación:** Si el producto o sistema cumple con éxito con los requisitos y las pruebas, puede recibir una certificación que indica su nivel de evaluación y su idoneidad para su uso en entornos de seguridad específicos.

Pese a que este proceso es igual para cualquier producto de seguridad, dependiendo de la naturaleza se distinguen diferentes elementos a evaluar y test.

---

[13] Cyber Essentials Plus. (s.f.). National Cyber Security Centre. Recuperado de https://www.ncsc.gov.uk/cyberessentials/overview

2.2.2. Normativa nacional española

2.2.2.1. Esquema Nacional de Seguridad

Por parte de España se nos presenta Esquema Nacional de Seguridad (ENS a partir de ahora) como normativa de seguridad.

Esta normativa publicada en el BOE tiene como objetivo certificar cierto nivel de seguridad para cualquier empresa que quiera establecer una relación como proveedor para el sistema público.

Esto significa que la normativa, de base, piensa en empresas grandes como objeto de la norma, así como ayuntamientos con menos recursos.

El proceso se resume en una categorización según unos requisitos y posteriormente se deben ajustar tanto medidas documentales como técnicas.

Esta normativa la actualiza el Centro Criptográfica Nacional (CCN a partir de ahora) mediante la aprobación de nuevos BOE que actualizan los principales requisitos, y mediante las guías 800 CCN-STIC (también referidas por la normativa) que permiten referirse a requisitos concretos o procedimientos concretos.

El proceso de certificación es laborioso y necesita de varios procesos para poder concluir que se está certificado. Este proceso es equiparable al de ISO27001 y está descrito en la guía 802 del CCN.

2.2.3. Normativa nacional de otros países

2.2.3.1. CyberEssential Plus

Cyber Essential Plus [14]representa un homólogo a ENS con sus funciones, es decir un mínimo de seguridad para poder trabajar para cualquier entidad pública del país.

Esta normativa, pero es mucho más sencilla que la española, representado solo medidas mínimas técnicas que se requieren, permitiendo certificarse durante un año. Estas son definidas por medidas de protección antimalware para los principales dispositivos y medidas de seguridad perimetrales, concretamente firewalls.

Es importante también mencionar que el proceso de certificación es más barato que el de la española al requerir solo de un cuerpo certificador hacer una auditoría para certificarse.

[14] Cyber Essentials Plus. (s.f.). National Cyber Security Centre. Recuperado de https://www.ncsc.gov.uk/cyberessentials/overview

El proceso de auditoría difiere de ISO y ENS, primero se autoevalúa el solicitante del certificado. Esta autoevaluación consta de un conjunto de preguntas en las que no se requiere evidencias al solicitante, pero sí una descripción detallada. Para obtener el certificado completo, se requiere que se hagan una serie de test técnicos (casi podríamos afirmar que sería un hacking ético) sobre lo que el IASME identifica como los principales riesgos tecnológicos.

2.2.4. Análisis de salvaguardas aplicables

En este apartado después de analizar la norma y ver las amenazas propondremos las principales salvaguardas y su relevancia en el entorno de las pymes. Para esto vamos a relacionar los principales ataques que hemos visto en el informe de ENISA:

- **Ramsomware y Social engeniering – Formación:** Para evitar ataques de ramsomware, hay que evitar la entrada del atacante en nuestros sistemas, normalmente a través de la ingeniería social. La principal recomendación es la concienciación del usuario, donde podemos enseñar procedimientos que eviten que un correo de acceso al sistema del atacante.

- **Malaware - Software Antimalware:** Los antivirus son la mejor solución a los malwares comunes, y permiten que nuestros equipos sean seguros a estos.

- **Threat against data:** Clasificación de información y encriptación: Las mejores medidas para paliar la capacidad de un atacante de ver documentos privados es clasificarlos según sean confidenciales y no, y protegiendo los datos confidenciales encriptándolos correctamente. Esto hace que, aunque el atacante entre, no pueda acceder a la información comprometida. También reduce los data leaks al estar más controlados y debidamente protegidos.

- **Threat against availability, Denial of service:** Paginas de salto y firewall: Las páginas de saltos (portales que permiten redirigirte a otros servicios, pero no son el servicio final) y el firewall pueden detener los famosos DDOS, pero son medidas caras. Además, actualmente los ataques de DDOS suelen ser ataques a servicios concretos que ya han sufrido un problema reputacional.

- **Threats against availability, Internet threats**: Redundancia: la redundancia de servicios de red nos permite no perder la conexión, pero suele ser una solución cara para un ataque que suele ser a empresas con algún objetivo reputacional.

- **Disinformation – misinformation**: Las pymes no son afectadas por este ataque, ya que suelen ser centrados en grandes empresas o gobiernos. Por tal de paliar este tipo de ataques, las grandes empresas o los goboiernos suelen disponer de políticas de comunicación para mitigar el daño reputacional con comunicados.

- **Supply Chain Attacks:** Control de proveedores y análisis de riesgos: Identificando nuestros riesgos y activos (incluyendo proveedores críticos) tenemos salvaguardas o planes de salida preparados cuando nuestros proveedores sufren indisponibilidades. Las pymes, debido a su poco volumen de negocio, son incapaces de poder forzar a los proveedores a controles estrictos o su monitorización, por ellos no disponen de salvaguarda adecuada.

CAPÍTULO 3

Metodología / desarrollo del proyecto

La metodología usada consiste en el contraste directo entre la normativa previamente analizada y la realidad específica de las pymes. Se buscan puntos de alineación, así como posibles brechas o discrepancias. Con base en este contraste, se procede a la adaptación de la normativa, desarrollando un marco específico que sea práctico, realista y efectivo para las pymes, integrando soluciones y mejores prácticas que se ajusten a su tipología y situación particular.

En resumen, la metodología se orienta hacia una personalización y adaptación de la normativa de ciberseguridad a las características únicas de las pymes, garantizando así la implementación de medidas de seguridad que sean efectivas y acordes a su entorno operativo.

3.1. Naturaleza de las empresas

Para poder tener un mejor contexto, resulta muy útil adentrarse en el entramado del tejido empresarial. Comprender la singularidad de cada sector, sus operaciones y sus desafíos específicos es esencial para desarrollar estrategias de seguridad que no solo sean efectivas, sino también adaptadas a las amenazas particulares que enfrenta cada empresa.

En este punto, resaltaremos la necesidad crítica de estudiar a fondo el tejido empresarial, reconociendo que la seguridad no es un enfoque universal, sino una disciplina vinculada a la individualidad de cada sector. Al analizar las características distintivas de diversas industrias podemos identificar amenazas únicas que pueden socavar la integridad, confidencialidad y disponibilidad de la información.

Este enfoque personalizado no solo reconoce la diversidad de los riesgos, sino que también sienta las bases para que una guía de seguridad se convierta en un aliado estratégico.

3.1.1. Naturaleza y categorías

La ciberdelincuencia puede afectar a empresas de todos los tamaños y sectores. Sin embargo, hay ciertos tipos de empresas que son particularmente atractivos para los ciberdelincuentes debido a la naturaleza de sus operaciones, la cantidad de datos sensibles que manejan o su importancia crítica en infraestructuras clave.

Aquí hay una descripción de algunos tipos de empresas que a menudo son objetivo de ciberdelincuentes:[15]

- **Empresas Financieras:**

Bancos, instituciones financieras y plataformas de pago son atractivos debido a la gran cantidad de datos financieros y personales que manejan.

- **Empresas de Tecnología:**

Empresas de tecnología, especialmente aquellas que desarrollan software o almacenan grandes cantidades de datos, son objetivos comunes.

- **Empresas de Salud:**

Las organizaciones del sector de la salud poseen información médica sensible, lo que las convierte en objetivos valiosos.

- **Empresas de Energía e Infraestructuras Críticas:**

Las empresas que operan en sectores críticos como energía, agua y servicios públicos son objetivos debido a las implicaciones potenciales para la seguridad nacional.

- **Empresas de Comercio Electrónico:**

Aquellas que manejan grandes cantidades de información de clientes y transacciones financieras son atractivas para ciberdelincuentes que buscan robar datos o realizar fraudes.

- **Empresas de Defensa y Aeroespacial:**

Estas empresas manejan información altamente clasificada y son objetivos de actores estatales y ciberdelincuentes con motivaciones políticas.

- **Empresas de Investigación y Desarrollo:**

Las organizaciones que lideran la investigación y el desarrollo de tecnologías innovadoras pueden ser objetivos para robar propiedad intelectual.

[15] ENISA Threat Landscape 2022. (2022). European Union Agency for Cybersecurity. Recuperado de https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

- **Empresas de Medios de Comunicación:**

Los ciberdelincuentes pueden atacar empresas de medios para difundir desinformación o comprometer la integridad de la información.

- **Empresas de Cadena de Suministro:**

Las empresas que son parte de cadenas de suministro críticas pueden ser atacadas para afectar indirectamente a otras organizaciones.

- **Empresas de Servicios Gubernamentales:**

Contratistas gubernamentales y organizaciones que manejan información gubernamental pueden ser objetivos para obtener acceso a datos sensibles.

Estos son solo ejemplos y, en realidad, cualquier empresa que almacene información valiosa, maneje transacciones financieras o tenga una presencia en línea significativa podría ser un objetivo potencial para la ciberdelincuencia. La conciencia de la ciberseguridad y la implementación de medidas de protección son fundamentales para todas las empresas en la actualidad.

3.1.2. Características especiales de las pymes

Las pymes son una parte crucial de la economía en muchos países. Aunque la definición exacta de lo que constituye una pyme puede variar según la región y la industria, generalmente se caracterizan por ciertos rasgos comunes. Las pymes suelen tener un número limitado de empleados en comparación con grandes empresas. El rango exacto puede variar según la jurisdicción, pero generalmente, las pymes tienen menos empleados que las grandes corporaciones. Este hecho provoca a su vez dos importantes factores que hay que tener en cuenta, la estructura organizativa de las pymes tiende a ser más plana y menos jerárquica que la de las grandes corporaciones, lo que puede facilitar la comunicación y la toma de decisiones, esto implica que los controles de autorización típicos de una empresa grande han de ser reversionados para esta tipología. También enfrentan desafíos únicos en la gestión de recursos humanos, como la necesidad de que los empleados asuman múltiples roles y funciones, por lo tanto, la segregación de funciones y mínimo privilegio no es operativa para esta estructura empresarial, y se requiere ser más permisivos en estos puntos para no interrumpir la operación de la empresa.

En cuanto al volumen de ventas y facturación, las Pymes tienen números más modestos en comparación con las grandes empresas, y los límites exactos pueden variar según el país y la industria. Muchas Pymes son propiedad de individuos o familias, lo que significa que la toma de decisiones suele ser más centralizada y menos

burocrática en comparación con las grandes corporaciones. Las Pymes a menudo pueden adaptarse rápidamente a los cambios en el mercado debido a su estructura más pequeña y su capacidad para tomar decisiones ágiles. Además, en general, tienen recursos financieros más limitados en comparación con grandes empresas, lo que puede afectar sus capacidades de inversión, expansión y desarrollo. Operan a nivel local o se especializan en nichos de mercado específicos, pudiendo tener una presencia regional fuerte en lugar de operar a escala nacional o internacional. Las pymes a menudo se basan en relaciones personales sólidas tanto con clientes como con proveedores, y la confianza y el trato personal son fundamentales en sus operaciones diarias. Dada su flexibilidad, las pymes pueden ser centros de innovación y adaptabilidad en respuesta a las necesidades cambiantes del mercado. La adopción de tecnología puede variar, pero muchas pymes están buscando cada vez más digitalizarse para mejorar la eficiencia y la competitividad. Es importante tener en cuenta que estas características son generales y pueden variar según la industria y la región. Además, las pymes son muy diversas, y cada una puede tener características únicas que la distinguen de otras en su categoría.

3.1.3. Problemáticas de implantación de la norma

3.1.3.1. Problemáticas estructurales (concienciación, norma de base, desajuste de requisitos, etc…)

La principal problemática de las normas anteriormente mencionadas es su aplicación en el grueso del tejido industrial. Pese el esfuerzo de entidades europeas y nacionales como ENISA o el CCN, la normativa aplicable y de donde muchos esperarían encontrar guías adecuadas para su aplicación se encuentran con que han sido dimensionadas para empresas grandes. Con este último punto nos referimos a que el principal motivo para mantener estos certificados es que entre empresas aseguren un nivel mínimo de seguridad para la colaboración, por ende, se pensaron para la colaboración entre grandes entidades.

Cuando hablamos respecto a pymes, la certificación no se escala ni se priorizan puntos donde quizás sea más importante la seguridad, simplemente se hacen excepciones en puntos que no aplican y se auditan el resto.

Desde un nivel práctico, esto conlleva que las pymes requieren realizar una actualización de sus sistemas de seguridad .

3.1.3.2. Problemáticas del resultado (Certificados no se ven igual según el tamaño y naturaleza de la empresa)

Los certificados han sido pensados para empresas con un tamaño concreto de empresas, por tanto, su valor radica en certificar confianza entre grandes empresas.

Otras certificaciones como TISAX nacen de problemas concretos, en este caso no querían que se filtre información de sus proveedores de automovilismo a raíz del caso Volkswagen con la contaminación.

3.1.3.3. Recertificaciones (mantenimiento y mejora de las evidencias)

Mantener las certificaciones requiere de un esfuerzo económico para las empresas. Por tal de mantener una certificación una empresa debería:

1. Disponer de un cuerpo normativo completo, formado por políticas, normativa y procedimientos técnicos de todos los procesos que se ejecutan en la empresa.
2. Revisión de cumplimiento de los requisitos técnicos de la normativa, asegurando que todos los mínimos son cumplidos.
3. Evidencias de que los procesos se cumplen conforme a los requisitos y de forma segura.
4. Pasar auditorías técnicas de seguridad como pentest o análisis de vulnerabilidades conforme a los requisitos de la mayoría de auditorías.
5. Disponer inventariados de todos los sistemas de la compañía.
6. Realizar análisis de riesgos donde se elaboran planes de acción futuros para mejorar la seguridad.
7. Comprometerse con los planes y mantener estos procesos cuando el cuerpo auditor vuelva para certificar la empresa.

Todos estos puntos son solo el reflejo de un gasto en tiempo y dinero que muchas empresas no pueden asumir. Por tanto, tomar como referencia las normativas de seguridad más conocidas suele ser un proceso no siempre adaptado a empresas que pretenden ser seguras, pero que no tienen grandes recursos o clientes que les brindan estos recursos para ejecutarlos.

CAPÍTULO 4

Resultados

El objetivo de este capítulo es proporcionar una visión integral y comprensiva de la normativa desarrollada, destacando su relevancia, aplicabilidad y los beneficios concretos que aportará a las pymes. Con ello, buscamos no solo establecer un marco normativo robusto, sino también catalizar una mejora significativa en la postura de seguridad cibernética de las empresas, promoviendo la resiliencia y la protección de la información en un entorno empresarial cada vez más digitalizado y desafiante.

4.1 Propuesta de la solución técnica

En este punto nos enfrentamos al desafío de proponer soluciones efectivas sin incurrir en recursos extraordinarios o esfuerzos desmedidos. La premisa es clara: la seguridad empresarial no debe convertirse en una barrera inaccesible para las pymes, sino más bien en un camino trazado con sencillez y pragmatismo.

En aquí donde nos adentramos en la explorar una solución que no solo sea eficaz en la protección de la información crítica, sino que también sea implementable con relativa facilidad. La esencia de esta propuesta radica en la capacidad de adaptarse a la realidad de las pymes, entendiendo sus limitaciones de recursos y optimizando los esfuerzos para lograr un equilibrio entre seguridad y practicidad.

En este contexto, propondremos estrategias que permitan a las pymes fortalecer su postura de seguridad sin comprometer su agilidad ni sacrificar recursos valiosos. Al final, la meta es proporcionar a estas empresas una guía que no solo identifique las mejores prácticas, sino que también ofrezca soluciones realistas y alcanzables, allanando el camino hacia la protección efectiva de la información empresarial en un mundo digital dinámico y desafiante.

4.1.1. Diseño de la solución

4.1.1.1. Objetivos principales de la propuesta

El objetivo principal del trabajo es la priorización de tiempo y medidas de seguridad. Con esta propuesta se pretende:

1. Ordenar de forma adecuada conjuntos de plan de acción para que en un espacio de tiempo acordado se disponga de una base de un SGSI.
2. Definir primer cuerpo normativo y mínimos indispensables para pymes.
3. Definir diferentes áreas de la seguridad donde prestar atención y presentar soluciones actuales de empresas del sector.
4. Preparar una pyme por si quisiera adquirir o demostrar que dispone de los mínimos de una certificación.
5. Proponer recursos online para ayudar a monitorizar los pasos de una pyme.

4.1.1.2. Alcance y grupos aplicables de la normativa

Se define el alcance de la normativa por empresas pequeñas que dispongan parcial o totalmente negocios con conexión a internet. Se diseña la normativa para que se considere desde negocios online con muy poco personal (el caso de menor aplicación) a una start up que dispone de infraestructura de red y desarrollo (el caso más amplio)

Definimos el mínimo de recursos en red como los siguientes:

- Se dispone de un portal web
- Se utilizan entornos de compartición online
- Se dispone de un negocio con programación
- Se dispone de una red en el entorno laboral
- Se teletrabaja
- Se dispone de información en formato digital

Por ende, los negocios que no entrarían son los que no disponen de infraestructura de telecomunicaciones o su negocio no requiere de comunicación online.

Dentro de esta clasificación vamos a hacer un sistema para categorizar el sistema. Dentro de este análisis simple de la norma, se pretende hacer unos controles globales a cualquier empresa que entre dentro del marco de la normativa, con un subconjunto más particular a las siguientes situaciones:

- Dispone de personal suficiente para una repartición más clara de funciones
- Se dispone de una infraestructura de red que ha de ser bastionada
- Hay posibilidad de teletrabajo
- Hay elementos de desarrollo de software
- Articulado de mejores prácticas para la mejora continua.

Estos puntos nos permiten expandir la norma cuando la empresa dispone de estas situaciones comunes dentro de pymes pero que no a todas aplican.

4.1.2. Definición de la propuesta

4.1.2.1. Índice articulado

La guía se compone de los siguientes controles, el detalle de los requisitos se puede encontrar en el Excel adjunto.

En este apartado justificaremos su importancia y el porqué de la elección del articulado.

Aun así, destacamos que muchas veces se requiere a la pyme que escriba sus procesos, esto tiene mucho sentido por varios motivos. El principal es replicar procesos ya estudiados y seguros, lo que garantiza que no se abran vulnerabilidades de forma accidental y por otra parte asegura que los procesos son conocidos. Por último, se precisa documentar lo que se dispone.

1. Cuerpo normativo

El cuerpo normativo es vital en cualquier empresa. El recurso escrito se vuelve imprescindible cuando alguien entra nuevo o cuando se necesita repetir un proceso que no se hace normalmente, pero si con cierta recurrencia.

Además, se identifican la misión y valores de seguridad. Todo esto hace que sea un punto que exigen todas las normas y, además, sea imprescindible para tener procesos definidos y seguros.

1. Cuerpo normativo			
1.1	Políticas de Seguridad	A.5.1	org.1
1.2	Responsable de la política de seguridad	A.5.1	org.1
1.3	Normativa de seguridad	A.5.1	org.2
1.4	Procedimientos de seguridad	A.5.2	org.3
1.5	Distribuir y acceso a la documentación		

Tabla 1. Correlación de ISO/ENS con la normativa de pymes control 1

2. Inventario de activos

El inventariado de activos y sus características nos permiten conocer que disponemos y tecnologías usamos. Este control nos dará apoyo sobre todo el resto de los controles, principalmente el control del parcheado y el análisis de riesgos.

2. Inventario de activos			
2.1	Activos esenciales	A.5.9	op.exp.1
2.2	Tiempo de actualización	A.5.9	op.exp.1
2.3	Activos no esenciales	A.5.9	op.exp.1
2.4	Responsabilidad del activo	A.5.9	op.exp.1
2.5	Localización del activo	A.5.9	op.exp.1

Tabla 2. Correlación de ISO/ENS con la normativa de pymes control 2

3. Mantenimiento y actualizaciones

Las actualizaciones son las principales medidas de seguridad contra vulnerabilidades del software que usamos. Se ha tenido en cuenta que, pese a que en ocasiones la actualización automática genere interrupciones en negocio, se recomienda porque su gestión es mucho más sencilla que un parcheo con despliegues y pruebas.

3. Actualizaciones			
3.1	Actualizaciones automáticas		op.exp.4
3.2	Obsolescencia		op.exp.4
3.3	Actualizaciones pautadas y copia de seguridad		op.exp.4

Tabla 3. Correlación de ISO/ENS con la normativa de pymes control 3

4. Protección antimalware

La principal línea de defensa antimalware. Tenerlo y actualizarlo es importante, pero para el entorno de la pyme no se solicita más control, pese que estas herramientas ofrecen normalmente muchas más capacidades, ya que usar las herramientas de monitorización antimalware puede consumir más recursos de los que una pyme puede o pretende asumir.

4. Protección antimalware			
4.1	Antivirus		op.exp.6
4.2	Antivirus Servidores		op.exp.6
4.3	Actualizaciones antimalware		op.exp.6

Tabla 4. Correlación de ISO/ENS con la normativa de pymes control 4

5. Clasificación de la información

Esta medida se centra en la confidencialidad. Establecer que información es confidencial y cual no es el primer paso para implementar salvaguardas adecuadas a la criticidad de los activos. Al igual que el control de inventario de activos, este es la base del análisis de riesgos y para centrar recursos correctamente.

5. Clasificación de la información			
5.1	Clasificación de información	A5.12 A5.13	mp.info.2
5.2	Responsabilidad de la información privada	A5.12 A5.13	mp.info.2
5.3	Protección según clasificación	A5.12 A5.13	mp.info.2
5.4	Automatización de clasificación y etiquetado	A5.12 A5.13	mp.info.2

Tabla 5. Correlación de ISO/ENS con la normativa de pymes control 5

6. Análisis de riesgos

El análisis es lo que nos dará la priorización de objetivos. Con esto conseguimos disponer de la visión global de la empresa, lo cual en seguridad es muy importante, puesto que se ha de trabajar con toda la información conocida.

6. Análisis de riesgos			
6.1	Valoración de activos		op.pl.1
6.2	Valoración de posibles riesgos		op.pl.1
6.3	Medidas de protección		op.pl.1

Tabla 6. Correlación de ISO/ENS con la normativa de pymes control 6

7. Transferencia de información

En la transferencia de información es donde se puede ubicar muchos ataques, sobre todo de ingeniería social. Normalizando los canales y conociéndolos permite que nuestro ecosistema de seguridad además de manejar bien como traspasamos la información.

7. Transferencia de datos			
7.1	Métodos de transferencia	A5.14	
7.2	Uso aceptable de métodos de transferencia	A5.14	
7.3	Transferencia de información documentada	A5.14	

Tabla 7. Correlación de ISO/ENS con la normativa de pymes control 7

8. Control de acceso

Este control asegura que los recursos están protegidos con usuario y contraseña. Además de mantener procesos para asegurar que cuando se dispone de más personal se asignan privilegios y credenciales correctamente.

8. Control de acceso			
8.1	Documentar métodos de acceso	A5.15	op.acc.1
8.2	Asignar credenciales	A5.17	op.acc.3
8.3	Rigidez de contraseñas	A5.15	op.acc.1
8.4	Cambio de contraseñas	A5.15	op.acc.1
8.5	Asignar privilegios	A5.17	op.acc.3
8.6	Cuentas unipersonales	A5.16	op.acc.2
8.7	Registro de logs	A5.16	op.acc.2

Tabla 8. Correlación de ISO/ENS con la normativa de pymes control 8

9. Usuarios privilegiados

Se definen los perfiles de administrador para que solo se usen para estas funciones, y no sean vulnerables por ser usados para cualquier otra función que lo exponga a un ataque.

9. Usuarios privilegiados			
9.1	Uso aceptable cuenta privilegiada	A8.18	
9.2	Mínimas aplicaciones de cuenta privilegiada	A8.18	
9.3	Monitorización de cuenta	A8.18	

Tabla 9. Correlación de ISO/ENS con la normativa de pymes control 9

10. Manejo de cambios

Los cambios suelen ser una acción para remendar actividades erróneas o activos que no funcionan correctamente, pero si no los documentamos correctamente son peligrosos, al no valorar con toda la información lo que supone. Este control pretende garantizar que los cambios son estudiados y documentados por si se necesitase reconstruir o detectar fallos.

10. Manejo de cambios			
10.1	Procedimiento de cambios	A8.32	op.exp.5
10.2	Registro de cambios	A8.32	op.exp.5
10.3	Pruebas del cambio	A8.32	op.exp.5
10.4	Autorización del cambio	A8.32	op.exp.5
10.5	Actualización de análisis de riesgos		

Tabla 10. Correlación de ISO/ENS con la normativa de pymes control 10

11. Copias de seguridad

Este control pretende mantener copias de seguridad para que siempre que tengamos un problema podamos recurrir a ellas. Pese a esto, se ha de tener en cuenta que es un control que no evita que un atacante pueda hacer daño, ya que muchos de ellos pasan tiempo dentro de la red antes de activarse y al hacer una copia de seguridad queda infectada. Esto implica que no es un método infalible, pero coste/salvaguarda es tremendamente efectivo.

11. Copias de seguridad			
11.1	Copias periódicas	A8.13	
11.2	Pruebas de regresión	A8.13	op.cont.3
11.3	Determinar tiempos de recuperación	A8.13	op.cont.1

Tabla 11. Correlación de ISO/ENS con la normativa de pymes control 11

12. Servicios Cloud

Cloud nos da infraestructura barata y no mantenida por nosotros, lo que a primera vista son todo ventajas competitivas. Aun así, es vital saber que responsabilidades son nuestras y disponer de vías alternativas en caso de que nuestro proveedor cloud no sea tan coste eficiente a lo largo del tiempo.

12. Servicios Cloud			
12.1	Responsabilidad compartida	A5.23	op.nub.1
12.2	Seguridad en cloud	A5.23	op.nub.1
12.3	Certificación del proveedor cloud	A5.23	op.nub.1

Tabla 12. Correlación de ISO/ENS con la normativa de pymes control 12

13. Requisitos Legales

Se ha de revisar que se cumplen con los mínimos legales de seguridad, como el RGPD.

13. Requisitos legales			
13.1	Análisis de legalidad aplicable	A5.31	

Tabla 13. Correlación de ISO/ENS con la normativa de pymes control 13

14. Concienciación

Los ataques de ingeniería social son los más habituales para entrar en los sistemas de la empresa, aprovechándose de que el usuario desconoce cómo identificar una fuente fidedigna de una falsa. Por tal de evitar las vulnerabilidades asociadas a las personas, se debe hacer concienciación.

14. Concienciación			
14.1	Formación obligatoria de entrada	A6.30	
14.2	Constante mejora	A6.30	
14.3	Formación equipos técnicos	A6.30	

Tabla 14. Correlación de ISO/ENS con la normativa de pymes control 14

15. Confidencialidad

La forma de evitar, al menos de forma legal, que una persona revele información dañina para nuestra empresa que pueda afectar a la seguridad (por ejemplo, revelando nuestro cliente y el canal de información para que el atacante sepa hacer ingeniería social) es mediante un contrato de confidencialidad.

15. Confidencialidad			
15.1	Acuerdos de confidencialidad	A6.6	

Tabla 15. Correlación de ISO/ENS con la normativa de pymes control 15

16. Reutilización de equipos

Se asegura que los equipos no contienen información previa que vulnere la confidencialidad de los activos de información para el nuevo usuario, a la vez que se almacena por si se requiere rescatar información.

16. Reutilización de equipos			
16.1	Copia de información	A7.14	
16.2	Borrado previo	A7.14	

Tabla 16. Correlación de ISO/ENS con la normativa de pymes control 16

17. Mesa y pantalla despejadas

Este control pretende que por descuido en el puesto de trabajo no se pueda acceder a la información de forma fácil. Para nuestro caso de estudio, lo más impactante es el uso de papel y mantener la sesión de un portátil abierta cuando se está ausente del puesto de trabajo

17. Mesa y pantalla despejadas			
17.1	Información física	A7.7	
17.2	Cierre de sesión	A7.7	
17.3	Impresoras	A7.7	

Tabla 17. Correlación de ISO/ENS con la normativa de pymes control 17

18. Requisitos seguridad de las aplicaciones

Se requiere que parte de la compra de una aplicación sea estudiar sus métodos de seguridad, para que se opere de forma que no se vulnere de ninguna forma. Esto evitara que los atacantes que conocen nuestras herramientas aprovechen fallos de configuración por nuestra parte.

18. Requisitos de seguridad de las aplicaciones			
18.1	Análisis del aplicativo	A8.26	
18.2	Especialistas técnicos	A8.26	

Tabla 18. Correlación de ISO/ENS con la normativa de pymes control 18

19. Criptografía

La mejor forma de proteger datos confidenciales en reposo es su encriptación. Esto evita que un atacante entre encuentre información suficiente para extender su ataque o acceder a información que comportan multas por la autoridad competente. Se pide que se defina métodos, ya que en una pyme se espera adaptabilidad, pero el conocimiento de las herramientas es indispensable.

19. Criptografía			
19.1	Documentar el método de criptografía	A8.24	
19.2	Datos protegidos	A8.24	

Tabla 19. Correlación de ISO/ENS con la normativa de pymes control 19

20. Filtrado web

Limitando las webs que se pueden alcance desde el equipo de una empresa y con ayuda de monitorización podemos evitar que un usuario acceda a contenido con malware haciendo un uso inadecuado del equipo.

20.Filtrado Web			
20.1	Límite en el acceso a webs	A8.23	
20.2	Monitorización de web	A8.23	

Tabla 20. Correlación de ISO/ENS con la normativa de pymes control 20

21. Manejo de roles

Este control es pensado para empresas con más trabajadores donde se manejan roles según función. Es verdad que una pyme suele disponer de trabajadores con múltiples roles, pero este control ofrece una guía para minimizar privilegios y gestionarlos

21.Manejo de roles			
21.1	Segregación de roles	A5.3	op.acc.4
21.2	Monitorización de roles	A5.4	op.acc.4
21.3	Formación especializada	A5.3	op.acc.4
21.4	Autorización y ejecución de cambios	A5.3	op.acc.4

Tabla 21. Correlación de ISO/ENS con la normativa de pymes control 21

22. Arquitectura de seguridad

Este control se centra en vigilar que la estructura de red sea protegida con firewall y que se disponga de un diagrama. A nivel de seguridad, en infraestructura de red se podrían agregar más controles, pero normalmente consumen recursos económicos y requieren personal especializado. Centrándonos en el mínimo de protección podemos asegurar que estaremos protegidos ante la mayoría de las amenazas.

Otro punto en este control está en el desarrollo de software y en documentar las capas o interconexiones que dispone, por tal de que no se pierda información durante el proceso y se pueda contar siempre con el aspecto de la seguridad.

22.Arquitectura de seguridad			
22.1	Diagramas de red		op.pl.2
22.2	Firewall		op.pl.2
22.3	Capas de desarrollo		op.pl.2

Tabla 22. Correlación de ISO/ENS con la normativa de pymes control 22

23.Controles de red

En este control se hace foco en los administradores de red y en bastionar todos los equipos que forman parte de la infraestructura de red. También se asigna responsables del mantenimiento y se crea un perfil de administrador separado de otros perfiles. Esto ayuda en gran medida al manejo de redes y a no centrar todo el poder de la red en el propietario de la empresa, el cual no debería tener permiso de administrador de todo.

23.Controles de red			
23.1	Bastionado en equipo red	A8.20	
23.2	Responsabilidad de la red	A8.20	
23.3	Perfil de administrador de red	A8.20	

Tabla 23. Correlación de ISO/ENS con la normativa de pymes control 23

24.Segregación de redes

Una vez nos hemos ocupado del bastionado, se ha de tratar la segregación de redes. Esta medida permite que un ataque solo afecte a una capa externa de la red y no pase a dentro de nuestra red. Esto se asegura para las redes internas de diferentes departamentos y la red wifi de invitados, que es un punto externo de ataque.

24. Segregación de redes			
24.1	Separación de equipos	A8.22	
24.2	Red de invitados	A8.22	

Tabla 24. Correlación de ISO/ENS con la normativa de pymes control 24

25.Seguridad en servicios de red

En este control se pide que se vea que los servicios en red cumplen los mínimos de seguridad que tenemos en toda la empresa. Estos controles parecen redundantes, pero en mi experiencia cuando las empresas contratan o subcontratan servicios suelen despreocuparse de la seguridad al hacer responsable al proveedor. Esto recuerda que hemos siempre de tener clara nuestra responsabilidad y la configuración mínima de seguridad.

25. Seguridad en servicios en red			
25.1	Análisis del servicio	A8.21	
25.2	Asegurar mínimos	A8.21	

Tabla 25. Correlación de ISO/ENS con la normativa de pymes control 25

26. Uso aceptable de activos

Cuando se dispone de más empleados, se ha de garantizar que los activos que la empresa brinda solo se usan con fin laboral para minimizar riesgos. Estas guías hacen que los ataques que afecten a un empleado en sus perfiles de usuario fuera de la empresa no se trasladen, por ejemplo.

26. Uso aceptable de activos			
26.1	Normas de uso aceptable	A5.10	

Tabla 26. Correlación de ISO/ENS con la normativa de pymes control 26

27. Equipo fuera de las instalaciones

Este control debería proponer realizar mínimas normas del uso de equipos fuera de instalaciones, sobre todo para el teletrabajo. Este control debería responder al miedo de que teletrabajando se haga en un espacio donde la seguridad física no sea adecuada.

27. Equipo fuera de las instalaciones			
27.1	Atención a los equipos	A7.9	
27.2	Borrado a distancia	A7.9	

Tabla 27. Correlación de ISO/ENS con la normativa de pymes control 27

28. Almacenamiento

Este control se basa en controlar donde están nuestros activos fuera de la empresa y los dispositivos de almacenamiento extraíble. Se recomienda que no se usen, pero cuando es inevitable hay que controlar en todo momento este tipo de activos. La principal razón es que cuando no se usan entornos cloud, la información suele depender de almacenamiento extraíble, conteniendo normalmente activos confidenciales.

28. Almacenamiento			
28.1	Dispositivos de almacenamiento	A7.10	
28.2	Control de activos fuera de oficina	A7.10	

Tabla 28. Correlación de ISO/ENS con la normativa de pymes control 28

29. Desarrollo seguro, testing y datos de prueba

Este control asienta bases mínimas en desarrollo. Se piensa principalmente en startups de desarrollo que pretenden sacar códigos sin bases de seguridad. Se pide el estándar de OWASP para desarrollo seguro, y se dan directrices para el testing y los datos de pruebas

29. Desarrollo seguro, testing y datos de pruebas			
29.1	Desarrollo seguro	A8.28	
29.2	Testing	A8.29	
29.3	Datos de prueba	A8.33	

Tabla 29. Correlación de ISO/ENS con la normativa de pymes control 29

30. Separación de entornos

Se establecen bases para la separación de entornos de desarrollo. Al igual del control anterior, se piensa en criterios de seguridad para un desarrollo seguro dentro de un ecosistema de pocos recursos.

30. Separación de entornos			
30.1	Entornos de desarrollo, pruebas y producción	A8.31	

Tabla 30. Correlación de ISO/ENS con la normativa de pymes control 30

31. Externalización

Este control se basa en pymes que necesitan un desarrollo, pero lo subcontratan. Este desarrollo debería contener mínimos de seguridad y buenas prácticas.

31. Externalización			
31.1	Requisitos para externalización	A8.30	

Tabla 31. Correlación de ISO/ENS con la normativa de pymes control 31

32. Gestión de la capacidad

Este control se basa en medir cuanto se requiere de un recurso antes de disponer de él. Aunque parezca que debería ser obligatorio, muchas situaciones de las pymes esta gestión solo se evalúa para la optimización, y no es un imprescindible en seguridad. Por eso esta categorizado como mejores prácticas.

32. Gestión de la capacidad			
32.1	Gestión de la capacidad del personal	A8.6	op.pl.4
32.2	Gestión de la capacidad de la infraestructura	A8.6	op.pl.4
32.3	Gestión de la capacidad de cloud	A8.6	op.pl.4

Tabla 32. Correlación de ISO/ENS con la normativa de pymes control 32

33. Enmascaramiento de datos

Este control de seguridad es muy bueno para defender la confidencialidad, pero es muy particular a que datos y en que entornos se usan, por ende, se recomienda que se disponga de un proceso, pero no es obligatorio ya que es una salvaguarda que no nos previene de los principales ataques.

33. Enmascaramiento de datos			
33.1	Proceso de enmascararían	A8.11	

Tabla 33. Correlación de ISO/ENS con la normativa de pymes control 33

34. Prevención fuga de datos

La protección de la confidencialidad suele conllevar monitorización y herramientas para el borrado de metadatos. En esta guía se pretende que se tenga como objetivo, pero que no sea tan primordial como otro, manteniéndose en mejores prácticas.

34. Prevención de fuga de datos			
34.1	Metadatos	A8.12	
34.2	Monitorización de canales	A8.13	

Tabla 34. Correlación de ISO/ENS con la normativa de pymes control 34

35. Registro de actividad

Este control es muy eficaz, pero requiere de monitorización, y toda monitorización conlleva un desembolso de recursos económicos altos. Es recomendable tenerlo para mejorar el entorno de seguridad de la empresa, pero el foco de esta guía es la prevención de ataques, no las lecciones aprendidas.

35. Registro de la actividad			
35.1	Registro de eventos		op.exp.8

Tabla 35. Correlación de ISO/ENS con la normativa de pymes control 35

36. Continuidad

Los controles de seguridad de continuidad podrían parecer que para una pyme son vitales, ya que contra más disponibilidad del servicio más dinero. El problema es que las salvaguardas de continuidad pasan por disponer de redundancia y capacidad de recuperación, medidas que comportan mucho dinero y que se han de testear con periodicidad, es por eso que se mantiene como mejores prácticas, ya que hay una carga económica detrás que no es vital para la supervivencia de una empresa.

36. Continuidad			
36.1	Business Impact Analysis	5.29	op.cont.1
36.2	Refuerzo de activos	5.30	op.cont.2

Tabla 36. Correlación de ISO/ENS con la normativa de pymes control 36

4.1.2.2. Acercamiento al desarrollo normativo

La normativa desarrollada se basa en ISO 27001 y ENS como principales normativas de referencia.

Se pretende de forma ordenada y concisa, ayudar a la creación de un manejo seguro de un sistema de gestión de la información.

Cada punto será asignado con los controles ISO 27001 (concretamente los del anexo 27002 donde se encuentran la normativa más técnica) y de controles del ENS. Toda esta guía ha sido realizada con las ISO 27001 (2022) y el BOE 106 (Real Decreto 311/2022), por tanto, su correspondencia de controles puede variar si las normativas cambian.

4.1.2.3. Riesgos y beneficios

Los principales beneficios del marco normativo creado es la introducción de una pyme a lo que conlleva el mantenimiento de su operación de seguridad, así como la visualización de primera mano de los recursos que requiere y los objetivos a proponer.

El riesgo de este tipo de normativas es la dificultad de priorizar medidas sobre otras, ya que la priorización depende del análisis concreto de la situación de la pyme y es difícil para el público no especializado realizarlo. Normalmente se priorizarán las medidas cuyo coste sea menor, lo que implica que no siempre se cubrirán aspectos vitales de gran impacto en las pymes.

4.1.3. Caso teórico

En este apartado, exploraremos las características fundamentales del formato de la norma. Esta estructura ha sido cuidadosamente configurada para garantizar su aplicabilidad, comprensión y ejecución eficaz en entornos empresariales de menor escala.

A modo ilustrativo, presentaremos un ejemplo teórico de implantación de la norma en un entorno empresarial específico. Este caso práctico proporcionará una visión concreta de cómo los principios y requisitos de la normativa pueden aplicarse en situaciones del mundo real, sirviendo como guía práctica para las pymes que buscan fortalecer su seguridad cibernética.

4.1.3.1. Formato de la norma

La norma diseñada incorpora un cuestionario inicial que desempeña un papel crucial en el proceso de evaluación y aplicación. Este cuestionario se basa en los requisitos definidos en el apartado 4.1.1.2, estableciendo preguntas obligatorias destinadas a evaluar la aplicabilidad del grupo de controles diseñados en la normativa.

Preguntas para aplicar controles	
¿Dispone de recursos online o de infraestructura de red de los cuales dependa?	Si
¿Dispone de más de 5 personas?	No
¿Dispone de red propia?	Si
¿Tiene teletrabajo implementado?	Si
¿Se hace desarrollo de código?	Si

Figura 4 Preguntas introducidas en la normativa

Los artículos de la norma se caracterizan por la presencia de títulos definidos, cada uno de los cuales presenta distintos requisitos vinculados directamente a los controles ISO/ENS correspondientes. Esta estructura permite una referencia clara y concisa, facilitando la identificación de los elementos esenciales de la norma y estableciendo una conexión directa con los estándares reconocidos internacionalmente. La asociación de cada requisito con los controles ISO/ENS no solo proporciona claridad en la implementación, sino que también asegura una alineación efectiva con las mejores prácticas y estándares reconocidos en el ámbito de la ciberseguridad.

En línea con el enfoque proactivo hacia la seguridad, la norma también incorpora requisitos de mejores prácticas. Estos requisitos adicionales están diseñados para potenciar a aquellas empresas que buscan alcanzar niveles más avanzados de madurez en seguridad. Estas prácticas recomendadas no solo cumplen con los estándares mínimos definidos en la normativa, sino que van más allá, proporcionando directrices adicionales para fortalecer aún más las defensas cibernéticas y promover una cultura de seguridad sólida en las pymes.

Aplicabilidad	Articulo	Titulo	Norma	Ref. ISO	Ref. ENS
2. Inventario de activos					
Aplica	2.1	Activos esenciales	Se inventaríalos activos vitales para mantener el negocio activo, marcando claramente los campos relevantes (en caso de un soporte físico, se debería marcar el modelo del producto y la versión de software que lleva, numero de serie y fabricante. En caso de Software, marcar nombre, la versión y el fabricante)	**A.5.9**	**op.exp.1**
Aplica	2.2	Tiempo de actualización	Se ha de definir tiempos para actualizar esta información	**A.5.9**	**op.exp.1**
Mejores Prácticas	2.3	Activos no esenciales	Se inventaríalos todos los activos (clasificando los vitales y los no vitales) para mantener el negocio activo, marcando claramente los campos relevantes (en caso de un soporte físico, se debería marcar el modelo del producto y la versión de software que lleva, numero de serie y fabricante. En caso de Software, marcar nombre, la versión y el fabricante)	**A.5.9**	**op.exp.1**
No Aplica	2.4	Responsabilidad del activo	En empresas con responsabilidades distribuidas, se ha de asignar responsables a los activos.	**A.5.9**	**op.exp.1**
Aplica	2.5	Localización del activo	Si los activos no se guardan en la empresa o sus inmediaciones, se debe mantener el registro del lugar donde están.	**A.5.9**	**op.exp.1**

Figura 5 Formato del articulado

4.1.3.2. Ejemplo de aplicación

Dentro de la hoja de cálculo proporcionada, se ha incorporado la columna "Descripción de implementación", destinada a que la pyme describa su situación actual en relación con el control específico. Esta columna permite que la empresa articule detalladamente su enfoque y estado actual en la implementación del control correspondiente.

Además, se ha incluido la columna "Documentación", donde la empresa puede adjuntar o hacer referencia a cualquier documentación interna relevante que respalde la implementación del control específico.

La columna "Nivel de implementación" proporciona un espacio para que la pyme indique el grado de aplicación o ejecución alcanzado en relación con el control en cuestión, permitiendo una evaluación clara de su nivel de conformidad.

Por último, la columna "Evidencias " está destinada a recoger cualquier tipo de prueba o material que respalde la implementación efectiva del control, facilitando así la verificación y auditoría de las medidas adoptadas por la pyme. En conjunto, estas columnas ofrecen un marco estructurado para que la empresa informe y documente su proceso de implementación, promoviendo la transparencia y la eficacia en el cumplimiento de los controles establecidos.

Descripción implementación	Documentación	Nivel de implementación	Evidencia
Se dispone de un PDF con la política de seguridad, donde se tiene el compromiso de la empresa con la seguridad. Se tiene firmado por el responsable de la empresa	Política de seguridad (ruta)	4 - Implementado, documentado	
Se dispone de normas para el uso habitual de las herramientas	Repositorio normativo (ruta)	4 - Implementado, documentado	
No todos los procesos han sido documentados, se hace un esfuerzo por incluir cada vez más procesos		2 - No implementado, documentado y pendiente de implementación	
Toda la documentación se encuentra en el repositorio compartido en red de la oficina			

Figura 6 Parte rellenable por parte de la pyme

4.2 Limitaciones

La guía que se intenta elaborar se encuentra sujeta a diversas limitaciones que surgen de la complejidad de la aplicación de normativas de seguridad en entornos empresariales. Estas limitaciones, aunque no excluyen la validez del proyecto, plantean desafíos significativos que deben abordarse.

En primer lugar, la falta de una prueba directa en una pyme real se presenta como una limitación destacada. La ejecución de normativas de seguridad conlleva riesgos potenciales para la actividad económica de una empresa, y es comprensible que las pymes muestren reticencia a adoptar cambios que puedan afectar a su operatividad. Esta ausencia de validación práctica puede dar lugar a incertidumbres sobre la efectividad real de la guía propuesta.

La dificultad para establecer un marco de tiempo efectivo que refleje resultados reales también se presenta como una limitación relevante. La implementación de medidas de seguridad no siempre produce resultados inmediatos, y la falta de un horizonte temporal preciso puede generar dudas sobre la rapidez con la cual las pymes podrían experimentar mejoras tangibles en su seguridad. Esta incertidumbre temporal podría afectar la percepción de la utilidad y viabilidad de la guía.

Por último, la falta de una prueba directa en el terreno también impide una retroalimentación inmediata y específica de las pymes, lo que podría limitar la capacidad de ajustar y mejorar la guía de manera iterativa. Esta retroalimentación es esencial para garantizar que la guía evolucione de acuerdo con las necesidades cambiantes del entorno empresarial y las demandas de seguridad.

En conclusión, estas limitaciones subrayan la importancia de abordar este proyecto con un enfoque cauteloso. Aunque la ejecución directa en una pyme real puede ser desafiante, se pueden adoptar enfoques como pruebas piloto controladas o simulaciones para mitigar algunas de estas limitaciones y validar la eficacia de la guía de seguridad en condiciones más cercanas a la realidad empresarial.

CAPÍTULO 5

Análisis de sostenibilidad e implicaciones éticas

En el marco del análisis de sostenibilidad e implicaciones éticas para el desarrollo y aplicación de la normativa de ciberseguridad en pymes, se ha elaborado una matriz integral que abarca los aspectos ambientales, económicos y sociales. Además, se destaca la contribución directa de la normativa a varios Objetivos de Desarrollo Sostenible, como el ODS 9 y el ODS 16, al fortalecer la resiliencia cibernética y promover un entorno digital seguro y sostenible. Este enfoque garantiza que la implementación de la normativa no solo fortalezca la seguridad, sino que también aborde consideraciones éticas y de sostenibilidad.

5.1 Matriz de Sostenibilidad

5.1.1. Impacto ambiental

El impacto ambiental de un ataque cibernético se manifiesta de manera significativa debido al derroche de recursos asociado con la interrupción de servicios, la pérdida de datos y la necesidad de realizar acciones de recuperación. Los ciberataques, especialmente aquellos que provocan la paralización de sistemas o la pérdida de información, conllevan un consumo considerable de recursos para restaurar la normalidad operativa. Además, la recuperación implica a menudo la duplicación de esfuerzos y la utilización de recursos adicionales, contribuyendo a un mayor impacto ambiental.

En contraste, fortalecer la seguridad cibernética y prevenir ataques promueve el uso eficiente de recursos al evitar la necesidad de llevar a cabo procesos de recuperación costosos y demandantes en términos de recursos. Al implementar medidas preventivas, se reducen los riesgos de interrupciones operativas y pérdida de datos, evitando así el derroche innecesario de recursos asociado con las consecuencias de un ataque.

En el contexto específico del desarrollo del proyecto de normativa de ciberseguridad para pymes, el consumo de recursos se limita al uso de ordenadores e internet. Este enfoque eficiente garantiza que la implementación de la normativa, al fortalecer la seguridad cibernética, no solo contribuya a la resiliencia empresarial, sino que también minimice su impacto ambiental al evitar la necesidad de reaccionar frente a potenciales ciberataques y las consecuencias ambientales asociadas.

5.1.2. Impacto económico

El desarrollo del proyecto de normativa de ciberseguridad para pymes ha sido llevado a cabo con un enfoque eficiente en términos económicos, incurriendo únicamente en el coste asociado a la participación de los involucrados y el consumo de recursos en línea, como el acceso a internet y la utilización de dispositivos electrónicos. Sin embargo, se reconoce que estos costes podrían ser reducidos significativamente mediante la colaboración y el uso de recursos del estado. La participación activa de instituciones gubernamentales o agencias especializadas en ciberseguridad podría no solo disminuir la carga financiera para los participantes individuales, sino también enriquecer el proyecto con su experiencia y acceso a recursos adicionales. Esta sinergia entre el sector privado y el público no solo optimizaría los recursos financieros, sino que también fortalecería la efectividad y el alcance del proyecto en la creación de un marco normativo robusto y adaptado a las necesidades específicas de las pymes.

5.1.3. Impacto Social

El enfoque del trabajo es mantener una posición neutral en cuanto al impacto social, reconociendo que el fortalecimiento de la protección de las empresas a través de la normativa de ciberseguridad puede tener implicaciones en la dinámica social. Si bien el objetivo primordial es resguardar la integridad y operatividad de las empresas, es importante señalar que el aumento de la seguridad podría dificultar actividades como huelgas cibernéticas contra negocios virtuales. Esta perspectiva neutra busca reconocer las complejidades inherentes a la ciberseguridad, equilibrando la protección empresarial con la consideración de posibles tensiones en el ámbito social.

5.1.4. Implicaciones éticas

La implicación ética central de la normativa de ciberseguridad para pymes reside en su objetivo fundamental de prevenir actividades ilícitas que puedan mermar la capacidad de negocio o incluso forzar el cierre de estas empresas. Al enfocarse en el fortalecimiento de las defensas cibernéticas, la normativa se erige como un mecanismo ético para salvaguardar la integridad y la continuidad operativa de las pymes. Evitar las acciones delictivas en el ámbito cibernético no solo protege los intereses comerciales y la confianza de los clientes, sino que también respeta la ética empresarial al promover un entorno justo, seguro y sostenible para el desarrollo económico de las pequeñas y medianas empresas.

5.1.5. Relación con los Objetivos de Desarrollo Sostenible

La normativa de ciberseguridad para pymes contribuirá directamente a varios Objetivos de Desarrollo Sostenible (ODS), incluyendo el ODS 9 (Industria, Innovación e Infraestructura) y el ODS 16 (Paz, Justicia e Instituciones Sólidas), al fortalecer la resiliencia cibernética y promover un entorno digital seguro y sostenible.

CAPÍTULO 6

Conclusiones y Líneas Futuras

En las conclusiones derivadas de la normativa propuesta para pequeñas y medianas empresas (pymes), se destaca el impacto significativo que esta podría tener en la mejora de la seguridad cibernética en este sector empresarial vital.

6.1 Conclusiones

En conclusión, este estudio exhaustivo sobre la ciberseguridad en las pequeñas y medianas empresas (pymes) ha revelado una serie de desafíos y vulnerabilidades significativas que enfrenta el tejido industrial en este sector. La creciente frecuencia y sofisticación de los ciberataques han expuesto las limitaciones y la necesidad imperante de medidas de seguridad más efectivas.

La propuesta de creación de una normativa específica para las pymes surge como una respuesta estratégica y proactiva a estas amenazas. La normativa desarrollada, resultado de la adaptación y contextualización de estándares globales a la realidad particular de las pymes, presenta un enfoque pragmático y realista para fortalecer la seguridad cibernética en este sector.

Uno de los hallazgos más significativos es que la implementación de esta normativa no solo se traduce en mejoras tangibles en la seguridad de la información, sino que también puede desempeñar un papel crucial en la reducción del impacto y el resentimiento causado por ciberataques. Al establecer pautas claras y prácticas recomendadas, la normativa proporciona un marco sólido para fortalecer las defensas de las pymes, mitigar el riesgo de ataques y, en última instancia, preservar la integridad del tejido industrial.

Es evidente que la seguridad cibernética es una inversión esencial para la resiliencia y sostenibilidad de las pymes en la era digital. La implementación de la normativa propuesta no solo contribuirá a fortalecer la postura de seguridad de las empresas, sino que también fomentará una cultura de conciencia y responsabilidad en torno a la ciberseguridad. Este trabajo subraya la importancia crítica de abordar estas cuestiones de manera proactiva, y la normativa propuesta representa un paso significativo hacia la creación de entornos empresariales más seguros y resilientes.

6.2 Líneas Futuras

La revisión detallada de la normativa de seguridad desarrollada en este estudio ha resaltado la necesidad de una mayor granularidad para abordar de manera más específica las complejidades y desafíos únicos que enfrentan las pequeñas y medianas empresas (pymes). Aunque la normativa actual establece un marco general sólido, se reconoce la importancia de una mayor especificidad para adaptarse de manera más precisa a las particularidades de las pymes.

Este refinamiento en la granularidad de la normativa se plantea como una tarea esencial para el futuro. En próximas fases del proyecto, se trabajará en la identificación y definición más precisa de requisitos y directrices, considerando aspectos más detallados de la infraestructura tecnológica, los procesos operativos y las limitaciones específicas de las pymes.

Además, se reconoce la importancia de la cooperación con instituciones nacionales para llevar a cabo una monitorización efectiva de la aplicación de la normativa en casos reales. La colaboración con organismos gubernamentales, entidades reguladoras y otras instituciones pertinentes permitirá establecer mecanismos de seguimiento, recopilación de datos y evaluación de la implementación de la normativa a nivel nacional. Este enfoque colaborativo no solo garantizará una supervisión más efectiva, sino que también fomentará la coherencia y la alineación con las políticas de ciberseguridad a nivel nacional.

En resumen, la evolución continua de la normativa hacia una mayor granularidad y la colaboración estrecha con instituciones nacionales son pasos cruciales para garantizar una implementación efectiva y adaptada a la realidad de las pymes, contribuyendo así a fortalecer la seguridad cibernética en el tejido empresarial.

Bibliografía

[1] International Organization for Standardization. "ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements." Geneva, Switzerland: ISO, 2013. Estándar ISO 27002

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

[3] Common Criteria. (s.f.). Recuperado de https://www.commoncriteriaportal.org/index.cfm

[4] Cyber Essentials Plus. (s.f.). National Cyber Security Centre. Recuperado de https://www.ncsc.gov.uk/cyberessentials/overview

[5] Metodología Magerit. (s.f.). Recuperado de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=ca

[6] ENISA Threat Landscape 2022. (2022). European Union Agency for Cybersecurity. Recuperado de https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[7] ENISA Threat Landscape 2023. (2023). European Union Agency for Cybersecurity. Recuperado de https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[8] National Institute of Standards and Technology (NIST). (s.f.). Recuperado de https://www.nist.gov/

[9] National Institute of Standards and Technology (NIST). (2020). Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations. Retrieved from https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

[10] National Institute of Standards and Technology (NIST). (2020). Special Publication 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Retrieved from https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

[11] National Institute of Standards and Technology (NIST). (2012). Guide for Conducting Risk Assessments (Special Publication 800-30 Revision 1). Retrieved from https://csrc.nist.gov/pubs/sp/800/30/r1/final

[12] National Institute of Standards and Technology (NIST). (2004). An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (Special Publication 800-66 Revision 1). Retrieved from https://csrc.nist.gov/pubs/sp/800/66/r1/final

APÉNDICE A

Un apéndice

En el apéndice hayamos un breve resumen de los controles de la ISO 27001 y ENS en los que se ha basado la norma.

Apéndice A Controles ISO 27001

A.5 Controles Organizativos

A.5.1 Políticas de la seguridad de la información

Desarrollar y mantener políticas claras que establezcan la dirección y objetivos para la seguridad de la información en la organización.

A.5.2 Roles y Responsabilidades de la seguridad de la información

Definir roles y responsabilidades específicos para garantizar la gestión efectiva de la seguridad de la información.

A.5.3 Segregación de roles

Separar funciones y responsabilidades para reducir el riesgo de conflictos de interés y posibles fraudes.

A.5.4 Manejo de responsabilidades

Establecer procesos para el manejo de responsabilidades en situaciones como cambios de personal o funciones.

A.5.5 Contacto con las autoridades

Establecer procedimientos para el contacto con autoridades relevantes en caso de incidentes de seguridad.

A.5.6 Contacto con grupos de interés especial

Definir procesos para comunicarse con grupos de interés especial, como clientes, en asuntos de seguridad de la información.

A.5.7 Inteligencia de amenazas

Implementar procesos para recopilar, analizar y utilizar inteligencia sobre amenazas para fortalecer la postura de seguridad.

A.5.8 Seguridad de la información en la gestión de proyectos

Integrar consideraciones de seguridad de la información en la gestión de proyectos para mitigar riesgos desde el inicio.

A.5.9 Inventario de Información y otros activos relacionados

Mantener un inventario actualizado de activos de información para gestionar su seguridad de manera efectiva.

A.5.10 Uso aceptable de los activos

Establecer políticas que definan el uso aceptable de los activos de información para prevenir mal uso y garantizar la seguridad.

A.5.11 Devolución de los activos

Establecer procedimientos para la devolución segura de activos de información al finalizar su uso.

A.5.12 Clasificación de la información

Clasificar la información según su importancia y sensibilidad para aplicar medidas de seguridad apropiadas.

A.5.13 Etiquetado de la información

Etiquetar la información de manera que su clasificación sea clara y se puedan aplicar controles adecuados.

A.5.14 Transferencia de información

Establecer controles para garantizar la seguridad durante la transferencia de información dentro y fuera de la organización.

A.5.15 Control de acceso

Implementar controles para garantizar que el acceso a la información esté autorizado y sea gestionado adecuadamente.

A.5.16 Manejo de identidades

Gestionar de manera efectiva las identidades de usuarios, incluyendo la asignación y revocación de privilegios.

A.5.17 Información de autenticación

Proteger la información de autenticación para prevenir accesos no autorizados.

A.5.18 Derechos de Acceso

Definir y gestionar los derechos de acceso para garantizar que los usuarios tengan acceso solo a la información necesaria.

A.5.19 Política de seguridad de la información en las relaciones con los proveedores

Establecer políticas para asegurar que los proveedores cumplan con los estándares de seguridad de la información.

A.5.20 Requisitos de seguridad en contratos con terceros

Incluir requisitos de seguridad de la información en contratos con terceros para garantizar la protección de los activos.

A.5.21 Cadena de suministro de tecnología de la información y de las comunicaciones

Gestionar la seguridad en toda la cadena de suministro de tecnología de la información y comunicaciones.

A.5.22 Control, revisión y cambio de la provisión de servicios del proveedor

Establecer controles y procesos para gestionar y revisar los servicios proporcionados por proveedores externos.

A.5.23 Información de seguridad en servicios Cloud

Establecer controles específicos para garantizar la seguridad de la información almacenada o procesada en servicios en la nube.

A.5.24 Planificación y preparación para manejo de incidentes de la seguridad de la información

Planificar y prepararse para la gestión efectiva de incidentes de seguridad de la información.

A.5.25 Evaluación y decisión sobre los eventos de seguridad de información

Evaluar y tomar decisiones adecuadas en respuesta a eventos de seguridad de la información.

A.5.26 Respuesta a incidentes de seguridad de la información

Establecer procedimientos de respuesta efectivos para abordar y mitigar incidentes de seguridad.

A.5.27 Aprendizaje de los incidentes de seguridad de la información

Realizar análisis de incidentes para aprender y mejorar continuamente las medidas de seguridad.

A.5.28 Recolección de evidencias

Establecer procesos para la recolección efectiva de evidencias en casos de incidentes de seguridad.

A.5.29 Seguridad de la información durante una interrupción

Implementar medidas para garantizar la seguridad de la información durante interrupciones o desastres.

A.5.30 Capacidad de las TIC para la continuidad de negocio

Asegurar que las Tecnologías de la Información y Comunicación (TIC) respalden la continuidad del negocio.

A.5.31 Requisitos legales, regulatorios y contractuales

Cumplir con requisitos legales, regulaciones y contratos relacionados con la seguridad de la información.

A.5.32 Derecho de la propiedad intelectual

Proteger los derechos de propiedad intelectual relacionados con la información de la organización.

A.5.33 Protección de los registros de la organización

Implementar controles para proteger la integridad y autenticidad de los registros de la organización.

A.5.34 Protección y privacidad de la información de carácter personal

Establecer medidas para proteger la privacidad y seguridad de la información personal.

A.5.35 Revisión independiente de la seguridad de la información

Realizar revisiones independientes para evaluar la eficacia de las medidas de seguridad de la información.

A.5.36 Cumplimiento de las políticas y normas de seguridad

Garantizar el cumplimiento continuo de las políticas y normas de seguridad establecidas.

A.5.37 Documentación de procedimientos de operación

Documentar los procedimientos operativos para garantizar la consistencia y eficacia en la implementación de controles.

A.6 Controles de Personal

A.6.1 Control de antecedentes

Realizar verificaciones de antecedentes para asegurar la idoneidad del personal en roles relacionados con la seguridad de la información.

A.6.2 Términos y condiciones de la contratación

Incluir términos y condiciones específicos relacionados con la seguridad de la información en contratos de contratación.

A.6.3 Concienciación seguridad de la información

Desarrollar programas de concienciación para educar al personal sobre prácticas seguras de información.

A.6.4 Procesos disciplinarios

Establecer procesos para abordar y tomar medidas disciplinarias en casos de violaciones de seguridad.

A.6.5 Responsabilidad cuando cesa el trabajo

Definir procesos para gestionar la seguridad de la información cuando los empleados dejan la organización.

A.6.6 Acuerdos de confidencialidad

Establecer acuerdos de confidencialidad para proteger la información sensible de la organización.

A.6.7 Teletrabajo

Establecer controles específicos para garantizar la seguridad de la información cuando los empleados trabajan de forma remota.

A.6.8 Reporte de eventos

Implementar procesos para que el personal informe eventos de seguridad de la información de manera oportuna.

A.7 Controles Físicos

A.7.1 Perímetro de seguridad físico

Establecer y controlar un perímetro físico para proteger las instalaciones de la organización.

A.7.2 Entrada física

Gestionar y controlar el acceso físico a las instalaciones y áreas críticas.

A.7.3 Securizar oficinas, salas y espacios

Implementar medidas de seguridad física en oficinas, salas y otros espacios críticos.

A.7.4 Monitorización de seguridad física

Supervisar y registrar actividades relacionadas con la seguridad física para detectar posibles amenazas.

A.7.5 Protección contra amenazas medioambientales y externas

Implementar controles para proteger las instalaciones contra amenazas ambientales y externas, especialmente importante para CPD (centro de procesado de datos) donde se requiere una disponibilidad 24/7.

A.7.6 Trabajar en áreas seguras

Establecer áreas seguras para la realización de tareas críticas.

A.7.7 Mesa y pantalla despejadas

Fomentar la práctica de mantener escritorios y pantallas despejados para prevenir el acceso no autorizado.

A.7.8 Emplazamiento y protección de equipos

Colocar y proteger equipos de manera que se minimice el riesgo de daño o robo.

A.7.9 Seguridad de los equipos fuera de las instalaciones

Implementar medidas de seguridad para proteger los equipos cuando se encuentran fuera de las instalaciones. Estas medidas comprenden del encriptado de dispositivos a la limitación de acceso a información sin medidas de seguridad extra.

A.7.10 Almacenamiento del Media

Gestionar y controlar el almacenamiento de medios físicos para proteger la información almacenada.

A.7.11 Instalaciones de suministro

Implementar controles para proteger las instalaciones de suministro que pueden afectar las salas técnicas y infraestructura IT que contenga información.

A.7.12 Seguridad del cableado

Proteger el cableado para evitar interferencias y riesgos de seguridad, etiquetando correctamente los diferentes cables aplicados.

A.7.13 Mantenimiento de los equipos

Establecer prácticas de mantenimiento para garantizar el buen funcionamiento y seguridad de los equipos físicos, como servidores, equipo de sala técnicas, infraestructura de IT, etc .

A.7.14 Reutilización o eliminación segura de equipos

Establecer procedimientos para la reutilización segura o eliminación de equipos para proteger la información almacenada.

A.8 Controles Tecnológicos

A.8.1 Dispositivos de usuario

Establecer controles para asegurar la seguridad de los dispositivos utilizados por los usuarios, incluyendo políticas de seguridad, configuraciones seguras y protección contra malware.

A.8.2 Gestión de privilegios de acceso

Gestionar y controlar los privilegios de acceso de los usuarios para garantizar que tengan el nivel de acceso mínimo necesario para realizar sus funciones.

A.8.3 Restricción del acceso a la información

Implementar controles para restringir el acceso a la información sensible, asegurando que solo las personas autorizadas puedan acceder a datos críticos.

A.8.4 Control de acceso al código fuente de los programas

Establecer controles para limitar el acceso y la modificación del código fuente de los programas, garantizando su integridad y seguridad.

A.8.5 Procedimientos seguros de inicio de sesión

Implementar procedimientos seguros para la autenticación y el inicio de sesión, como el uso de contraseñas fuertes, autenticación de dos factores, y políticas de bloqueo de cuentas.

A.8.6 Gestión de capacidades

Gestionar las capacidades de los sistemas para garantizar que los usuarios tengan acceso solo a las funciones y recursos necesarios para realizar sus tareas**.**

A.8.7 Controles contra el código malicioso

Implementar controles, como software antimalware, para proteger los sistemas contra la ejecución de código malicioso.

A.8.8 Manejo de vulnerabilidades tecnológicas

Establecer procesos para identificar, evaluar y gestionar vulnerabilidades en los sistemas y aplicaciones, y aplicar parches de seguridad de manera oportuna.

A.8.9 Manejo de configuración

Gestionar y controlar la configuración de los sistemas y aplicaciones para garantizar que estén configurados de manera segura y cumplan con los requisitos de seguridad establecidos.

A.8.10 Borrado de información

Establecer procesos seguros y eficaces para el borrado de información, asegurando que los datos se eliminen de manera permanente cuando sea necesario mediante borrado de software, o cuando sea necesario, destrucción certificada física.

A.8.11 Enmascaramiento de datos

Implementar técnicas para enmascarar datos sensibles durante las pruebas o en entornos no productivos, protegiendo así la confidencialidad de la información.

A.8.12 Prevención de fuga de datos

Implementar medidas para prevenir la fuga no autorizada de información sensible, controlando el acceso y monitoreando la transmisión de datos.

A.8.13 Copias de seguridad de la información

Establecer y mantener procedimientos para realizar copias de seguridad regulares de la información crítica, asegurando la disponibilidad y la capacidad de recuperación.

A.8.14 Disponibilidad de los recursos de tratamiento de la información

Implementar medidas para garantizar la disponibilidad de los recursos de procesamiento de la información, incluyendo redundancia y planes de continuidad del negocio.

A.8.15 Logging

Registrar eventos de seguridad relevantes para el análisis y seguimiento, facilitando la detección y respuesta a incidentes de seguridad.

A.8.16 Actividades de monitorización

Monitorear activamente las actividades de seguridad de la información para identificar eventos anómalos o incidentes de seguridad.

A.8.17 Sincronización del reloj

Sincronizar los relojes de los sistemas para asegurar una gestión precisa y coherente de los eventos temporales, esencial para la correlación de registros y la auditoría.

A.8.18 Uso de utilidades con privilegios del sistema

Controlar, restringir el acceso y el uso de cuentas privilegiadas del sistema para evitar usos inapropiados y proteger la integridad del sistema.

A.8.19 Instalación de software en sistemas operativos

Establecer controles para la instalación de software en sistemas operativos, asegurando la integridad del sistema y previniendo amenazas de seguridad.

A.8.20 Controles de red

Implementar controles de seguridad en la red para proteger la confidencialidad e integridad de la información, incluyendo firewalls y segmentación de red.

A.8.21 Seguridad de los servicios de red

Aplicar medidas de seguridad a los servicios de red para protegerlos contra amenazas, asegurando su disponibilidad y confiabilidad.

A.8.22 Segregación en redes

Separar lógica y físicamente las redes según los niveles de sensibilidad de la información, reduciendo así el riesgo de accesos no autorizados.

A.8.23 Filtrado de web

Implementar filtros de contenido web para controlar y prevenir el acceso a sitios web no autorizados o maliciosos.

A.8.24 Uso de la criptografía

Utilizar técnicas de criptografía para proteger la confidencialidad e integridad de la información, especialmente en comunicaciones y almacenamiento.

A.8.25 Desarrollo seguro del ciclo de vida

Integrar prácticas de seguridad en todas las fases del ciclo de vida del desarrollo de software para prevenir vulnerabilidades desde el principio.

A.8.26 Requisitos de seguridad de aplicaciones

Establecer y aplicar requisitos de seguridad específicos para las aplicaciones, asegurando su robustez frente a amenazas.

A.8.27 Principios de ingeniería de sistemas seguros

Integrar principios de ingeniería de sistemas seguros para desarrollar sistemas que sean resistentes a amenazas y vulnerabilidades.

A.8.28 Desarrollo seguro

Fomentar prácticas de desarrollo seguro, incluyendo la capacitación del personal y la aplicación de estándares de codificación segura.

A.8.29 Testing seguro durante el desarrollo y aceptación

Realizar pruebas de seguridad de manera continua durante el desarrollo y antes de la aceptación para identificar y corregir posibles vulnerabilidades.

A.8.30 Externalización del desarrollo de software

Establecer controles de seguridad al externalizar el desarrollo de software, asegurando la protección de la información.

A.8.31 Separación de entornos

Mantener ambientes separados para desarrollo, prueba y producción para prevenir riesgos asociados a la interferencia no autorizada.

A.8.32 Manejo de cambios

Implementar controles para gestionar y controlar los cambios en la infraestructura y el software, previniendo riesgos de seguridad.

A.8.33 Datos de prueba

Utilizar datos de prueba que no comprometan la seguridad ni la privacidad de la información.

A.8.34 Controles de auditoría de sistemas de información

Implementar controles para auditar y supervisar los sistemas de información, garantizando la trazabilidad de eventos de seguridad.

Apéndice B Controles ENS

Organizativos (org)

Org 1 Política de Seguridad

Punto donde se especifica la misión y visión con respecto a la seguridad.

Org2 Normativa de seguridad

Proceso disciplinario y responsabilidades.

Org 3 Procedimientos de seguridad Generación de documentación entorno a todos los procesos técnicos que se llevan en la empresa, así como quien la hace. Identificación de comportamiento animales y reporte.

Org 4 Proceso de autorización. Proceso por el cual se autorizan los procesos en la empresa, ya sea creación de usuarios, cambios en la infraestructura y otros. En una PYME no ha de ser tan estricto ya que muchas veces una persona es la encarga de toda la autorización

Planificación (op.pl)

Op.pl.1 Análisis de riesgos.

El análisis de riesgos identifica las principales amenazas de una empresa para tratar la posterior gestión de ellas.

op.pl.2 Arquitectura de seguridad.

Documentar tanto la instalación como la red y los diversos sistemas.

op.pl.3 Adquisición de nuevos componentes.

Proceso por el cual se obtiene y se analiza nuevos productos en un entorno.

op.pl.4 Dimensión/gestión de la capacidad

No los veo tan importante para PYMES

op.pl.5 Componentes certificados

Comprobar que los componentes están de acuerdo al centro criptológico nacional. No los veo tan importante para PYMES

Acceso (op.acc)

Identificación (**op.acc.1**)

Habla de disponer de identificadores únicos y cuando inhabilitar las cuentas.

Requisitos de acceso (**op.acc.2**)

Es referente a asegurar que se dispone de un control de acceso a los recursos que disponemos, así como una distribución correcta de permisos.

Segregación de funciones y tareas (op.acc.3)

Se trata de definir procesos en que la aprobación y la ejecución no pase por la misma persona.

Proceso de gestión de derechos de acceso (**op.acc.4**)

Define que se ha de aplicar mínimo privilegio y que todo acceso por defecto está prohibido salvo autorización expresa

Mecanismo de autenticación (usuarios externos) (op.acc.5)

Implementación de un sistema de autenticación específico para usuarios externos, asegurando la validación segura de su identidad.

Mecanismo de autenticación (usuarios de la organización) (op.acc.6)

Establecimiento de un sistema de autenticación para usuarios internos de la organización, garantizando el acceso seguro a sistemas y datos.

Explotación (op.exp)

Inventario de activos (op.exp.1)

Creación y mantenimiento de un registro completo de los activos de la organización, incluyendo hardware, software y datos.

Configuración de seguridad (op.exp.2)

Establecimiento de configuraciones de seguridad en sistemas y aplicaciones para mitigar riesgos y cumplir con estándares de seguridad.

Gestión de la configuración de seguridad (op.exp.3)

Implementación de procesos para gestionar y supervisar cambios en la configuración de seguridad.

Mantenimiento y actualizaciones de seguridad (op.exp.4)

Realización de mantenimiento periódico y aplicación de actualizaciones de seguridad para proteger contra vulnerabilidades.

Gestión de cambios (op.exp.5)

Implementación de un proceso estructurado para gestionar cambios en infraestructura y sistemas, minimizando riesgos de seguridad.

Protección frente a código dañino (op.exp.6)

Implementación de medidas para proteger sistemas y datos contra códigos maliciosos y amenazas.

Gestión de incidentes (op.exp.7)

Desarrollo y mantenimiento de un plan para gestionar eventos de seguridad de la información.

Registro de la actividad (op.exp.8)

Mantenimiento de registros detallados de actividades relacionadas con la seguridad, útiles para monitoreo y auditoría.

Registro de la gestión de incidentes (op.exp.9)

Documentación detallada de la gestión de incidentes, incluyendo acciones tomadas y lecciones aprendidas.

Protección de claves criptográficas (op.exp.10)

Implementación de medidas específicas para proteger las claves criptográficas utilizadas para la confidencialidad e la información.

Externos (op.ext)

Contratación y acuerdos de nivel de servicio (op.ext.1):

Establecimiento de contratos y acuerdos claros con proveedores externos, incluyendo términos de seguridad y niveles de servicio.

Gestión diaria (op.ext.2):

Implementación de controles y procedimientos para gestionar las operaciones diarias de la organización.

Protección de la cadena de suministro (op.ext.3):

Establecimiento de medidas para proteger la cadena de suministro y garantizar la seguridad de los productos y servicios externos.

Interconexión de sistemas (op.ext.4):

Gestión segura de las interconexiones entre sistemas, especialmente aquellas que involucran comunicaciones externas.

Nube (op.nub)

Protección de servicios en la nube (op.nub.1):

Implementación de controles específicos para proteger servicios y datos almacenados en entornos de nube.

Continuidad (op.cont)

Análisis de impacto (op.cont.1):

Evaluación de las consecuencias de eventos disruptivos en la continuidad del negocio.

Plan de continuidad (op.cont.2):

Desarrollo y mantenimiento de un plan para asegurar la continuidad del negocio en situaciones adversas.

Pruebas periódicas (op.cont.3):

Realización de pruebas regulares del plan de continuidad para garantizar su eficacia.

Medios alternativos (op.cont.4):

Establecimiento de medios alternativos para asegurar la continuidad del negocio en situaciones adversas.

Monitoreo (op.mon)

Detección de intrusión (op.mon.1):

Implementación de sistemas para detectar y responder a posibles intrusiones.

Sistema de métricas (op.mon.2):

Establecimiento de métricas y parámetros para monitorear y evaluar la eficacia de los controles de seguridad.

Vigilancia (op.mon.3):

Realización de vigilancia continua para detectar y responder a amenazas de seguridad.

Infraestructura Física (mp.if)

Áreas separadas y con control de acceso (mp.if.1):

Garantía de áreas físicas separadas y controladas para proteger la seguridad.

Identificación de las personas (mp.if.2):

Implementación de sistemas de identificación de personas para controlar el acceso a áreas críticas.

Acondicionamiento de los locales (mp.if.3):

Aseguramiento del acondicionamiento adecuado de los locales para mantener la integridad de la infraestructura.

Energía eléctrica (mp.if.4):

Implementación de medidas para garantizar el suministro seguro de energía eléctrica.

Protección frente a incendios (mp.if.5):

Implementación de medidas para proteger contra incendios y minimizar riesgos.

Protección frente a inundaciones (mp.if.6):

Implementación de medidas para proteger contra inundaciones y minimizar riesgos.

Registro de entrada y salida de equipamiento (mp.if.7):

Mantenimiento de registros detallados de la entrada y salida de equipamiento.

Personal (mp.per)

Caracterización del puesto de trabajo (mp.per.1):

Descripción y definición de las características del puesto de trabajo en términos de seguridad.

Deberes y obligaciones (mp.per.2):

Establecimiento de deberes y obligaciones para el personal en relación con la seguridad.

Concienciación (mp.per.3):

Desarrollo de programas de concienciación para el personal sobre prácticas seguras.

Formación (mp.per.4):

Implementación de programas de formación para mejorar la competencia del personal en seguridad.

Equipos (mp.eq)

Puesto de trabajo despejado (mp.eq.1):

Garantizar que los puestos de trabajo estén organizados y sin elementos que comprometan la seguridad.

Bloqueo de puesto de trabajo (mp.eq.2):

Implementación de mecanismos de bloqueo para proteger estaciones de trabajo cuando no están en uso.

Protección de dispositivos portátiles (mp.eq.3):

Implementación de controles para proteger dispositivos portátiles y la información que contienen.

Otros dispositivos conectados a la red (mp.eq.4):

Establecimiento de controles para proteger dispositivos adicionales conectados a la red.

Comunicaciones (mp.com)

Perímetro seguro (mp.com.1):

Establecimiento de medidas para asegurar un perímetro seguro alrededor de la infraestructura.

Protección de la confidencialidad (mp.com.2):

Implementación de controles para proteger la confidencialidad de la información en las comunicaciones.

Protección de la integridad y de la autenticidad (mp.com.3):

Implementación de controles para proteger la integridad y autenticidad de la información en las comunicaciones.

Separación de flujos de información en la red (mp.com.4):

Establecimiento de controles para separar flujos de información en la red y prevenir accesos no autorizados.

Seguridad de la Información (mp.si)

Marcado de soportes (mp.si.1):

Implementación de etiquetado para clasificar y marcar soportes de información.

Criptografía (mp.si.2):

Implementación de técnicas de criptografía para proteger la confidencialidad de la información.

Custodia (mp.si.3):

Establecimiento de medidas para la custodia segura de la información.

Transporte (mp.si.4):

Implementación de controles para garantizar la seguridad durante el transporte de la información.

Borrado y destrucción (mp.si.5):

Establecimiento de procedimientos seguros para el borrado y destrucción de información.

Desarrollo de Software (mp.sw)

Desarrollo de aplicaciones (mp.sw.1):

Implementación de controles durante el desarrollo de aplicaciones para garantizar la seguridad.

Aceptación y puesta en servicio (mp.sw.2):

Establecimiento de procesos para la aceptación y puesta en servicio seguro de aplicaciones.

Información (mp.info)

Datos personales (mp.info.1):

Implementación de medidas específicas para proteger datos personales de acuerdo con regulaciones de privacidad.

Calificación de la información (mp.info.2):

Establecimiento de criterios para clasificar la información según su importancia y nivel de seguridad.

Firma electrónica (mp.info.3):

Implementación de sistemas de firma electrónica para garantizar la autenticidad de la información.

Sellos de tiempo (mp.info.4):

Implementación de sellos de tiempo para garantizar la integridad y autenticidad de registros temporales.

Limpieza de documentos (mp.info.5):

Establecimiento de procedimientos para la limpieza segura de documentos, eliminando información sensible.

Copias de seguridad (mp.info.6):

Implementación de procesos de copias de seguridad para garantizar la disponibilidad y recuperación de la información.

Servicios (mp.s)

Protección del correo electrónico (mp.s.1):

Implementación de controles para proteger la seguridad del correo electrónico.

Protección de servicios y aplicaciones web (mp.s.2):

Implementación de controles para proteger servicios y aplicaciones web.

Protección de la navegación web (mp.s.3):

Implementación de medidas para proteger la navegación web de amenazas de seguridad.

Protección frente a denegación de servicio (mp.s.4):

Establecimiento de controles para proteger contra ataques de denegación de servicio.