Desarrollo e implementación de un SOC en una organización

Cristina Cadaveda Fernández

Seguridad empresarial

Nombre Tutor/a de TF
Daniel Brande Hernández
Profesor/a responsable de la asignatura
Victor García Font

06/2023

Universitat Oberta
de Catalunya

Universitat Oberta de Catalunya uoc.edu

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Desarrollo e implementación de un SOC en una organización*
Nombre del autor:	*Cristina Cadaveda Fernández*
Nombre del consultor/a:	*Daniel Brande Hernández*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	*06/2023*
Titulación o programa:	Máster en ciberseguridad y privacidad
Área del Trabajo Final:	*Seguridad empresarial*
Idioma del trabajo:	*Castellano*
Palabras clave	*SOC, ciberseguridad, pyme*

Resumen del Trabajo

La finalidad de este proyecto es la creación de un centro de operaciones de seguridad (SOC) orientado a dar servicio a las pequeñas y medianas empresas españolas. Estudios recientes demuestran que las pymes no están preparadas para responder ante incidentes de seguridad, lo que les lleva a ser un blanco son un blanco fácil para los ciberatacantes, los cuales pueden obtener beneficios con muy poco esfuerzo. Muchas de ellas terminan cerrando su negocio tras sufrir un incidente y el mercado no está preparado para ofrecerles un servicio completo, ya que muchas de las empresas que se dedican a ciberseguridad proporcionan servicios generalistas para llegar a un público mayor.

Este proyecto se ha desarrollado desde una perspectiva teórica, partiendo de las diferentes guías de buenas prácticas que existen. Por un lado, se ha hecho un análisis en profundidad sobre el funcionamiento de los SOC actuales, teniendo en cuenta personas, procesos y tecnología. Por otro lado, se han estudiado las características de las pymes españolas, los tipos de ciberataques que sufren con mayor frecuencia y sus puntos débiles en materia de ciberseguridad.

Finalmente, se ha obtenido una propuesta de SOC con servicios específicamente desarrollados para las pymes españolas, basándose en el presupuesto reducido con el que cuenta la mayoría de ellas, sus características y las amenazas más relevantes a las que están expuestas. Todo ello se ha conseguido en el tiempo y forma planteados al inicio del proyecto.

Abstract

The purpose of this project is to create a security operations center (SOC) aimed at serving small and medium-sized Spanish companies (SMEs). Recent studies show that SMEs are not prepared to respond to security incidents, which makes them an easy target for cyber attackers, who can make a profit with very little effort. Many of them end up closing their business after suffering an incident and the market is not prepared to offer them a complete service, as many of the companies involved in cybersecurity provide generalist services to reach a larger audience.

This project has been developed from a theoretical perspective, based on the different good practice guides that exist. On the one hand, an in-depth analysis has been made on the operation of current SOCs, considering people, processes, and technology. On the other hand, we have studied the characteristics of Spanish SMEs, the types of cyber-attacks they suffer most frequently and their weaknesses in cybersecurity.

Finally, a SOC proposal has been obtained with services specifically developed for Spanish SMEs, based on the reduced budget that most of them have, their characteristics and the most relevant threats to which they are exposed. All this has been achieved in the time and manner proposed at the beginning of the project.

Índice

Lista de figuras

Lista de tablas

1. Introducción

Los ciberataques a organismos públicos y privados han ido en aumento en los últimos años y ninguna industria, tanto grande como pequeña, está exenta de sufrir las consecuencias. La figura 1 muestra con claridad esta situación, obtenida del informe de ciberamenazas y tendencias del 2022 del Centro Criptológico Nacional [1], representa el promedio de ataques semanales que recibe cada sector y el aumento de estos con respecto al año anterior.

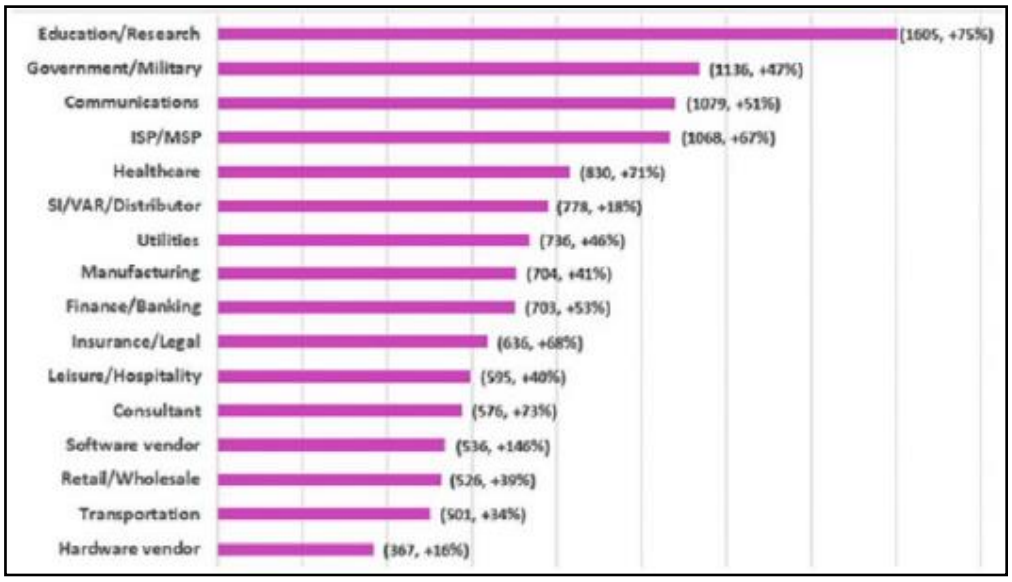

Figura 1: promedio de ataques semanales por sector en España (2021)

Actualmente, el mayor peligro al que se encuentran sometidas empresas y organismos públicos son las denominadas APTs (Amenazas Persistentes Avanzadas), formadas grupos profesionales de ciberdelincuentes perfectamente estructurados y organizados que tienen por objetivo infiltrarse en la red el mayor tiempo posible para robar información confidencial. Utilizan técnicas avanzadas que les permiten el acceso a los sistemas, permanecen dentro de los mismos comprendiendo su funcionamiento y vulnerabilidades y moviéndose a través de la red e incluso permanecen inmóviles durante meses dentro de los sistemas hasta lograr su objetivo. Este tipo de amenazas son muy difíciles de detectar, ya que no generan gran ruido y cada uno de los pasos que llevan a cabo se encuentran cuidadosamente estudiados. [2]
Para contextualizar la gravedad de esta situación, de media las organizaciones tardan 212 días en detectar un ataque de seguridad y 75 en contenerlo [3].
Las APTs conviven también con otro tipo de amenazas más conocidas y no tan sofisticadas, en este caso los ciberdelincuentes suelen buscar una recompensa económica a través técnicas de extorsión, supresión o modificación de la información e interrupciones en el servicio. Este otro tipo de amenazas se detectan con mayor facilidad por las organizaciones, pero pueden causar también grandes daños económicos y de reputación.

El panorama actual hace del cibercrimen un negocio muy rentable, alcanzando un nuevo nivel de comercialización denominado “cybercrime-as-a-service”, en el que se ponen a la venta todas las fases y herramientas de un ciberataque ante los usuarios [4]. El cibercrimen es el tercer tipo de delito más importante, y supone un 0,8% del PIB mundial.
Para hacer frente a esta situación son cada vez más necesarios profesionales cualificados en materia de ciberseguridad y empresas que ofrezcan servicios para detectar, analizar y responder de la mejor forma ante todo tipo de amenazas.

1.1. Contexto y justificación del Trabajo

El punto de partida de este trabajo es la creación de una empresa que brinde servicios de ciberseguridad a pequeñas y medianas empresas, para ello se desarrollará e implementará un centro de operaciones de seguridad (SOC).
Las grandes empresas cuentan con presupuestos en materia de ciberseguridad cada vez más elevados y pueden permitirse tener su propio equipo y las últimas tecnologías del mercado, no así las pequeñas y medianas empresas. Según un estudio realizado por Cisco [5], el 43% de los ciberataques están dirigidos a las pequeñas y medianas empresas y sólo el 14% de ellas consideran estar preparadas para defender sus redes y datos. En muchos, casos estos ciberataques suponen para las pymes el cierre de su negocio, por lo que existe la necesidad de dotarlas de un servicio de ciberseguridad básico con la capacidad de prevenir, detectar y responder ante las principales amenazas que puedan sufrir.
Un centro de operaciones de seguridad (SOC) permite supervisar, analizar, responder y recuperarse ante ciberataques, con la ayuda de diferentes herramientas y profesionales formados en la materia. Algunas de las razones por las que es un elemento esencial a la hora de abordar la ciberseguridad en una organización son [6]:

1. Protección y prevención de amenazas continuada: un centro de operaciones de seguridad trabaja las 24 horas del día y los 365 días del año, lo que permite detectar rápidamente un ciberataque desde sus primeros signos.
2. Respuesta rápida: una vez las amenazas son detectadas, se determina su severidad y se trabaja en eliminarlas lo más rápido posible, reduciendo así las posibles consecuencias.
3. Ahorro de costes: debido a la rápida actuación, los atacantes permanecen menos tiempo dentro de los sistemas lo que minimiza las pérdidas de información o servicio.
4. Mejora de la reputación empresarial: los clientes, empleados, consumidores, proveedores y otras empresas se sentirán más seguros al saber que su información se encuentra debidamente protegida, lo que dejará a la organización en una mejor posición respecto a sus competidores.

El resultado que se pretende obtener con este trabajo es el planteamiento de un centro de operaciones de seguridad, con una cartera de servicios que permita dar una cobertura y respuesta a las ciberamenazas actuales con un coste reducido para el cliente, proporcionando así un servicio íntegro de ciberseguridad que pueda ser asumido por las pymes.

1.2. Objetivos del Trabajo

Los objetivos de este trabajo se dividen en dos grandes bloques, por un lado, se encuentra el estudio en profundidad del funcionamiento de un centro de operaciones, y por otro lado se encuentra la implantación y desarrollo de este mismo con una finalidad concreta.

Los objetivos que permitirán, en primer lugar, conocer cómo funciona un SOC son:

- Estudiar a fondo el funcionamiento actual de los centros de operaciones de seguridad y de su estructura.
- Estudiar los diferentes servicios que proporciona un centro de operaciones de seguridad.
- Estudiar las diferentes herramientas que existen en el mercado.
- Estudiar la normativa y los estándares aplicables en la implantación de un SOC.
- Estudiar los recursos humanos necesarios y sus funciones dentro de un SOC, así como la organización de los mismos.
- Estudiar las principales amenazas a las que se encuentran expuestas las organizaciones hoy en día.

Los objetivos que permitirán, en segundo lugar, implantar un SOC que dará servicio a pequeñas y medianas empresas son:

- Realizar un estudio de mercado de los potenciales clientes y cuáles son las amenazas a las que se encuentran expuestos.
- Plantear una cartera de servicios que cubra la prevención, detección y respuesta de ciberataques, teniendo en cuenta las amenazas más comunes.
- Seleccionar las herramientas del mercado que permitan dar un servicio de seguridad de calidad sin un coste elevado.
- Definir las fases necesarias para la implantación de un SOC.
- Definir los procesos del SOC, su funcionamiento interno y los diferentes roles y responsabilidades del personal.
- Definir la arquitectura de red y sistemas que permita la puesta en marcha y el funcionamiento inininterrumpido.
- Definir los acuerdos a nivel de servicio con el cliente.
- Asegurarse de que el SOC desarrollado cumple con la normativa vigente y sigue unos estándares de calidad.

1.3. Impacto en sostenibilidad, ético-social y de diversidad

Este trabajo se guiará por los objetivos de desarrollo sostenible propuestos por Naciones Unidas [7] y se tratarán de alcanzar las siguientes metas en la implantación del centro de operaciones de seguridad:

- Lograr la igualdad de género y empoderar a todas las mujeres y niñas (SDG5). Tratando de buscar el equilibrio en materia de género en el equipo que forme SOC, tanto en puestos con baja responsabilidad como en aquellos que requieran una responsabilidad más elevada.

- Combatir el cambio climático (SDG13), se seguirá un modelo de trabajo híbrido en el que se animará a realizar el trabajo desde casa, reduciendo así los desplazamientos en coche hasta las oficinas y sus emisiones.
- Educación de calidad (SDG4), se brindará la oportunidad a los trabajadores de acceder a la formación necesaria que permita llevar a cabo sus tareas diarias e ir creciendo profesionalmente.
- Promover el crecimiento económico sostenido (SDG8), inclusivo y sostenible. Permitiendo que las pequeñas y medianas empresas también puedan contar con servicios de ciberseguridad que les protejan ante amenazas y ataques a un coste asumible.

1.4. Enfoque y método seguido

Tal y como se ha comentado anteriormente, este proyecto consiste en el desarrollo de un producto ya existente (SOC), pero con un nicho de mercado muy concreto, ya que estará dirigido a dar servicio a pequeñas y medianas empresas que no puedan costearse un centro de operaciones de seguridad de los ya existentes en el mercado.
Todo el trabajo se realizará de forma teórica, con una estrategia dividida en cuatro fases:

1. Establecer los objetivos y el alcance del trabajo desarrollado, así como plantear los diferentes puntos que se van a tratar en él y la planificación de estos. Este primer punto será cubierto con la entrega de la PEC1.
2. Comprender a fondo el funcionamiento de un SOC: personas, procesos y tecnología. Este estudio del arte se basará en la búsqueda de información principalmente y comprenderá la PEC2.
3. Aplicar el conocimiento aprendido en el punto anterior para desarrollar desde cero un SOC orientado a dar servicios a pymes, de la forma más eficiente posible y cumpliendo los estándares y normativas actuales. La implantación y desarrollo de un SOC real comprenderá la PEC3.
4. Obtener las conclusiones del trabajo, así como las posibles mejoras futuras. Repasar el contenido del proyecto en busca de errores o partes a mejorar y realizar el vídeo de presentación. Estas tareas comprenderán la entrega de la PEC4.

Se seguirá una estrategia en cascada ya que es necesario realizar en orden los apartados mencionados, esto permitirá tener un conocimiento profundo del estado del arte para aplicarlo posteriormente en un caso real. Para estructurar y gestionar el trabajo de la mejor forma posible, se seguirá la metodología ágil SCRUM [8].
Cada una de las entregas PEC será considerada un “sprint”, en que se identificarán las tareas a llevar a cabo y se presentará una parte funcional del proyecto. De esta forma, se pretende aprovechar al máximo el tiempo disponible y cumplir con los plazos establecidos.

1.5. Planificación temporal del Trabajo

Los hitos de los que consta la planificación del trabajo son:

1. Planificación
    a. Esquema de trabajo
    b. Definición de los objetivos del trabajo y el alcance
    c. Análisis de riesgos
    d. Análisis del impacto ético, social y cultural del proyecto
2. Arquitectura de un SOC
    a. Características de un SOC
        i. Definición de un SOC
        ii. Tipos de SOC
        iii. Estructura de un SOC
        iv. Objetivos de un SOC
    b. Mapa de amenazas en ciberseguridad (MITTRE ATTACK)
    c. Principales servicios de un SOC
    d. Normativa y estándares actuales
    e. Recursos tecnológicos de un SOC
    f. Perfiles profesionales de un SOC
3. Desarrollo e implementación de un SOC
    a. Planteamiento actual de la organización
    b. Estudio de mercado
    c. Análisis de viabilidad del proyecto
    d. Catálogo de servicios
    e. Modelo de operaciones
    f. Acuerdos a nivel de servicio
    g. Arquitectura de sistemas y red
    h. Selección de recursos software
    i. Selección de recursos hardware
    j. Normativa y estándares aplicables
    k. Fases de implantación del SOC
4. Conclusiones y futuras mejoras
    a. Evaluación de los resultados obtenidos
    b. Evaluación del impacto
    c. Evaluación de mejoras y líneas de trabajo futuras
5. Entrega del TFM
    a. Memoria final
        i. Repaso del contenido del TFM y correcciones
        ii. Completar apartados incompletos
    b. Presentación en vídeo
    c. Preparar defensa del TFM

Los recursos necesarios para llevar a cabo este trabajo son muy escasos: un ordenador con Windows 11, licencia de Office365 y acceso a Internet que permita consultar las diferentes fuentes de información. La figura 2 muestra la planificación temporal de las diferentes tareas que forman parte del trabajo distribuidas en las PECs y empleando un diagrama de Gantt.

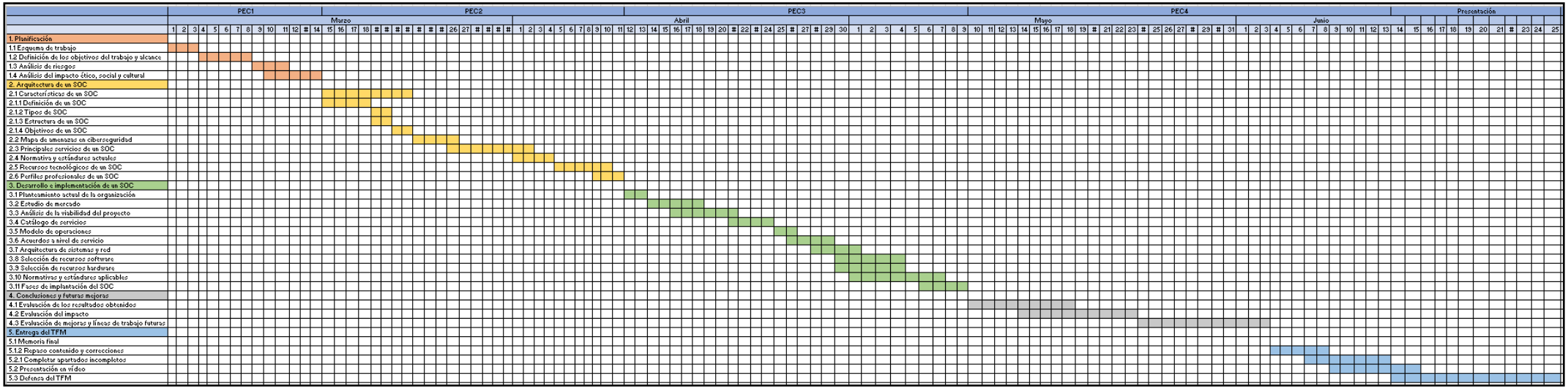

Figura 2: diagrama de Gantt, planificación temporal de las tareas del trabajo fin

1.6. Análisis de riesgos del trabajo

Los riesgos a los que se enfrenta este trabajo final de máster y que pueden provocar el fracaso o un retraso en la planificación de los tiempos, así como sus medidas para mitigarlos, son:

1. Mala estimación de la duración de las diferentes tareas que componen el proyecto. Para mitigar este riesgo se intentará evaluar cuidadosamente los recursos y tiempo necesarios para llevarlos a cabo, dejando al final de cada hito un tiempo prudencial para completar aquellas tareas que no hayan podido ser finalizadas.
2. Falta de recursos hardware y software. Para realizar el trabajo serán necesarios diferentes recursos ya mencionados, como un ordenador personal o licencias de Office, y puede ocurrir que no siempre se tenga acceso a estos. Para mitigar este riesgo se estudiarán siempre diferentes alternativas hardware/software opensource, de forma que si el proceso se estanca se pueda saltar a otra de las opciones.
3. Problemas técnicos. Entre los cuales se pueden encontrar una caída de Internet o de la página web de la universidad, o una pérdida del fichero que contiene el trabajo. Para mitigar este riesgo, se tendrá una copia de seguridad del trabajo en la nube y, además, se ajustarán los tiempos para que el trabajo esté listo uno o dos días antes de la entrega y haya tiempo suficiente para subirlo al campus virtual.

1.7. Breve descripción de los otros capítulos de la memoria

Los siguientes capítulos de este trabajo guardan relación con la estrategia de planificación, ya comentada anteriormente.
El capítulo 2 de la memoria es un estado del arte en el que se estudia en profundidad el funcionamiento, las tecnologías, los servicios y los procesos que tienen lugar en la actualidad en un centro de operaciones de seguridad, proporcionando así una visión lo más completa posible de un SOC.
El capítulo 3 de la memoria trata de aplicar los conocimientos obtenidos a un caso real, construyendo un centro de operaciones de seguridad desde cero y tratando de optimizar costes.
Finalmente, el capítulo 4 de la memoria contendrá las conclusiones obtenidas tras la realización del trabajo, un análisis crítico de la consecución de los objetivos y planificación planteados y las líneas de trabajo futuras que no han podido explorarse en el presente trabajo.

2. Arquitectura de un SOC

Un centro de operaciones de seguridad (SOC) es un elemento esencial a la hora de abordar la ciberseguridad en una organización, permite salvaguardar la confidencialidad, integridad y disponibilidad de la información y servicios. Entre sus funciones se encuentran la monitorización, el análisis, la respuesta y la recuperación ante incidentes de seguridad [9]. Por norma general, un centro de operaciones de seguridad da servicio las 24 horas del día y los 365 días del año.
El objetivo de este capítulo es comprender el funcionamiento de un SOC hoy en día, teniendo en cuenta las personas que trabajan en él y los diferentes roles que desempeñan, los procesos que se llevan a cabo para estructurar y dividir la carga de trabajo de forma óptima y la tecnología que se emplea para ayudar a recopilar y procesar todos los eventos que tienen lugar en la red de la organización.

2.1 Características de un SOC

Dentro de este apartado se explicará la misión de un centro de operaciones de seguridad, los diferentes modelos operaciones que existen y la organización estructural que siguen.

2.1.1 Misión de un SOC

El tamaño de un SOC puede variar dependiendo de la organización o las organizaciones a las que brinde servicio, no obstante, la gran mayoría tiene como misión:

- Prevenir incidentes de seguridad: a través de medidas como la gestión de vulnerabilidades o el bastionado de los sistemas.
- Monitorizar, detectar y analizar alertas que puedan estar relacionadas con incidentes de seguridad.
- Responder de forma rápida a los incidentes, mediante planes de contingencia predefinidos y técnicas de análisis forense.
- Recuperarse de forma rápida ante los incidentes de seguridad, mediante directrices claras a otros equipos (por ejemplo, cambio de contraseñas o restauración de copias de seguridad).
- Asegurarse de que todos los sistemas que conforman la infraestructura de seguridad funcionan correctamente: se recogen los eventos generados en los dispositivos, se procesan, se aplican reglas de filtrado etc.

2.1.1 Modelos de SOC

Existen diferentes tipos de centros de operaciones de seguridad y el enfoque que se les de va a depender del tipo y volumen de la organización a la que se brinden el servicio. Los principales modelos para desplegar y mantener un SOC son [10]:

1. Ad-hoc: es el modelo más extendido en empresas o instutuciones de tamaño pequeño. No existen a penas capacidades de detección y respuesta a incidentes, ni procedimientos de actuación. Generalmente, las labores

relacionadas con la seguridad son realizadas por otros equipos de profesionales, como los adminitradores de red o sistemas.

2. SOC distribuido: es el modelo más extendido en organizaciones de tamaño mediano. Está compuesto por un grupo descentralizado de recursos externos y recursos internos, en el que el personal que desempeña las labores de seguridad puede tener otro tipo de responsabilidades también.
3. SOC centralizado: también denominado SOC dedicado, este modelo es el más frecuente y se encuentra extendido entre organizaciones medianas y de gran tamaño. En el existe una variedad de recursos propios destinados al SOC y personal con roles específicos en el ámbito de la seguridad.
4. SOC como servicio: empleado por medianas y grandes empresas. En este caso, un tercer proveedor mantiene y maneja un SOC en la nube basado en suscripciones.
5. SOC federado: se puede encontrar en organizaciones que han adquirido otras organizaciones pero que no se han integrado entre sí. Está formado por una red de SOCs global que trabajan de forma independiente pero que comparte información, políticas y autoridad.

2.1.2 Estructura de un SOC

La estructura de un SOC es comparable a la estructura de nuestro sistema médico actual: existe una primera línea de defensa, un equipo de respuesta a emergencias, equipos especializados en diferentes ramas de la seguridad y un conjunto de políticas y herramientas que hacen que todos los componentes encajen a la perfección [11].
La estructura está basada en niveles, en el que el nivel superior posee unos conocimientos y responsabilidades más elevados que el anterior:

- Nivel 1: constituye la primera línea de defensa, está formado por analistas que monitorizan, analizan y priorizan constantemente las alertas.
- Nivel 2: se encarga de responder a las alertas tras el triaje inicial realizado por el nivel 1, mediante una metodología y procesos definidos previamente. También se encarga de dar soporte y recomendaciones ante un incidente de seguridad.
- Nivel 3: formado por expertos en ciberseguridad que se encargan de definir la metodología y los procesos a seguir por los niveles 1 y 2, mantener las herramientas de seguridad en correcto funcionamiento, buscar amenzas en la red y responder ante los incidentes de seguridad.
- SOC manager: se encarga de gestionar el equipo y las relaciones con los clientes y proveedores. Es el punto de contacto en incidentes graves.
- Otros roles: dependiendo del tamaño del SOC pueden ser necesarios otros roles para que el equipo funcione correctamente, como expertos en sistemas y redes, consultores de riesgos o gestores de proyectos.

2.1.3 Flujo de trabajo de un SOC

Para entender cómo funciona un centro de operaciones de seguridad podemos observar la figura 3, obtenida del informe [9], donde se muestra en un alto nivel de abstracción el flujo de trabajo habitual:

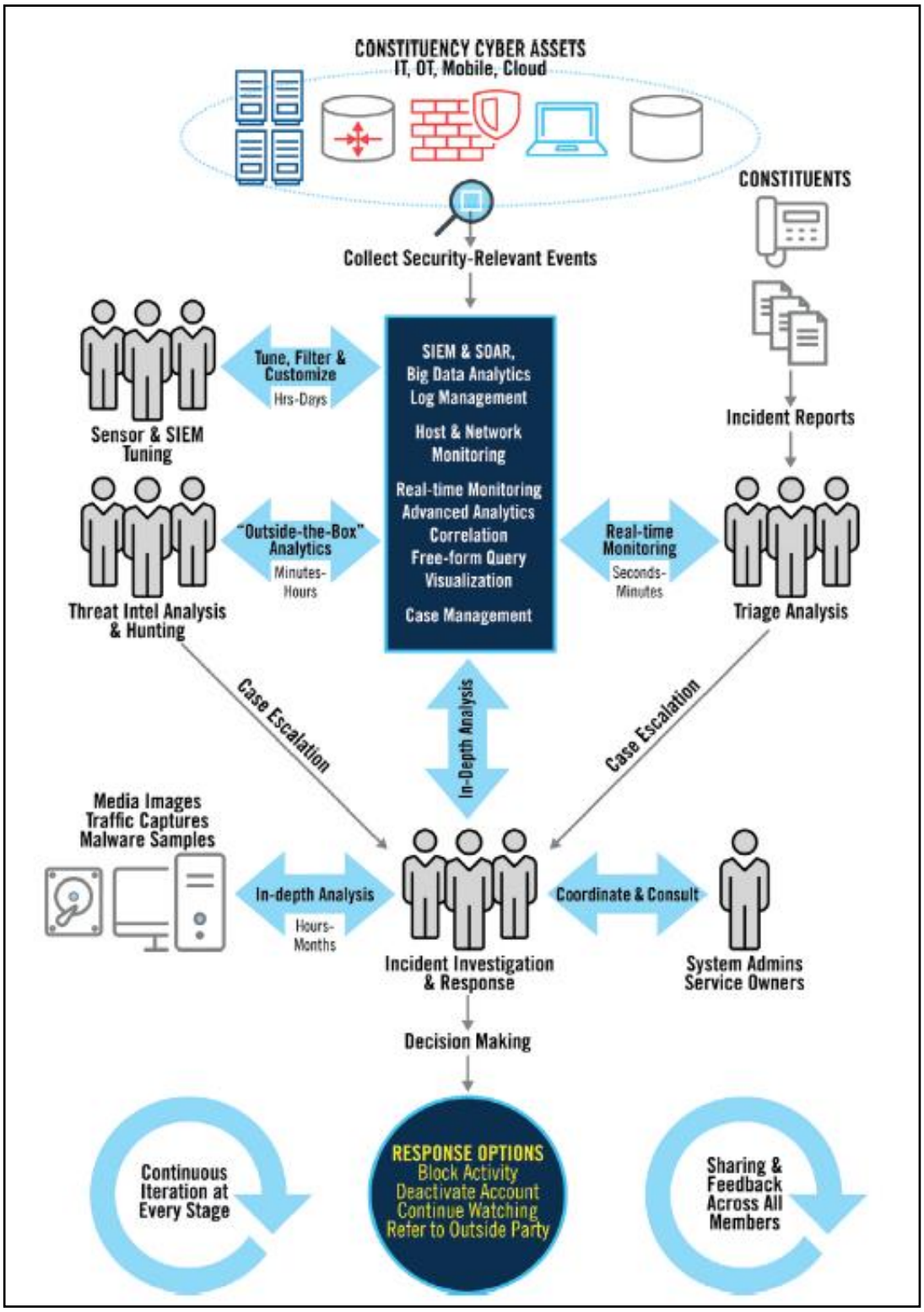

Figura 3: flujo de trabajo básico del funcionamiento de un SOC

En primer lugar, una organización está compuesta por un determinado número de activos (servidores, dispositivos móviles, cuentas de usuario…) que generan gran cantidad de eventos relacionados con su funcionamiento: errores, conexiones, procesos etc.
Un SOC emplea un conjunto de herramientas sofisticadas que correlacionan los eventos de seguridad más importantes y generan alertas de forma continua, en base a indicadores de compromiso (IOC) e indicadores de ataque (IOA). Las alertas son analizadas, en primera instancia, por un equipo de profesionales cualificados de primer nivel (N1) y categorizadas en función de su impacto y urgencia. Una vez realizado el triage inicial, se escalan al nivel 2 (N2, un equipo de analistas con mayor experiencia y cualificación) aquellas alertas que el N1 no ha logrado resolver, en este momento se hace un análisis más en profundidad y se determina si se trata de un incidente real o de un falso positivo. Además del uso de herramientas de seguridad para la detección de ataques, también existen equipos especializados en búsqueda de amenzas (threat hunters), que se encargan de realizar búsquedas proactivas de indicios de ciberataques en toda la infraestructura.
En el caso de que se haya detectado un incidente de seguridad, el equipo de respuesta ante incidentes entra en juego, y se encargará de evaluar la situación y de tomar las medidas necesarias para la contención y erradicación. Una vez resuelto el incidente, se generan reportes y documentación con las conclusiones obtenidas y se corrigen las vulnerabilidades detectadas.
Durante todo el proceso comentado anteriormente, desde el análisis de las alertas hasta la erradicación de un incidente de seguridad, entran en juego diferentes perfiles técnicos y no técnicos que no están relacionados directamente con el ámbito de la ciberseguridad, como pueden ser aquellas personas que se encargan de mantener una correcta relación con el cliente o los administradores de los sistemas que se han visto afectados.
Finalmente, cabe destacar que el objetivo principal de un centro de operaciones de seguridad es dar respuesta a ataques siguiendo el flujo mencionado, no obstante, existen otros servicios de ciberseguridad que aportan gran valor al SOC (como el escaneo de vulnerabilidades o la consultoría de seguridad). Cada uno de los eslabones que conforman el flujo de trabajo de la figura 3 (personas y tecnología) será estudiado en profundidad en los siguientes apartados.

2.2 Mapa de amenazas en ciberseguridad

Para comprender la importancia de implantar un centro de operaciones de seguridad en una organización es necesario analizar las posibles amenazas a las que esta se encuentra expuesta.
El ponarama actual de ciberamenazas es muy complejo y para abordarlo existen diferentes marcos trabajo, en este apartado se empleará el framework MITTRE ATTACK [12], por ser el más completo y extendido en la industria de la ciberseguridad.
ATTACK es una base de conocimiento pública actualizada en tiempo real, que contiene los distintos tipos de ataques que se producen hoy en día, así como medidas para mitigarlos. Está representada en forma de matriz y se basa en tres conceptos clave (TTPs):

- Tácticas: representan las columnas de la matriz y hacen referencia al objetivo que persiguen los atacantes. Existen 14 tácticas.
- Técnicas: representan las filas de la matriz y hacen referencia a cómo, técnicamente hablando, los atacantes consiguen sus objetivos. Existe un gran número de técnicas y subtécnicas y pueden ir cambiando en el tiempo.
- Procedimientos: representan los pasos concretos que un atacante debe seguir para llevar a cabo las tácticas y técnicas.

Un ciberataque puede estar compuesto por un conjunto de tácticas y técnicas. La figura 4 muestra parte de matriz ATTACK:

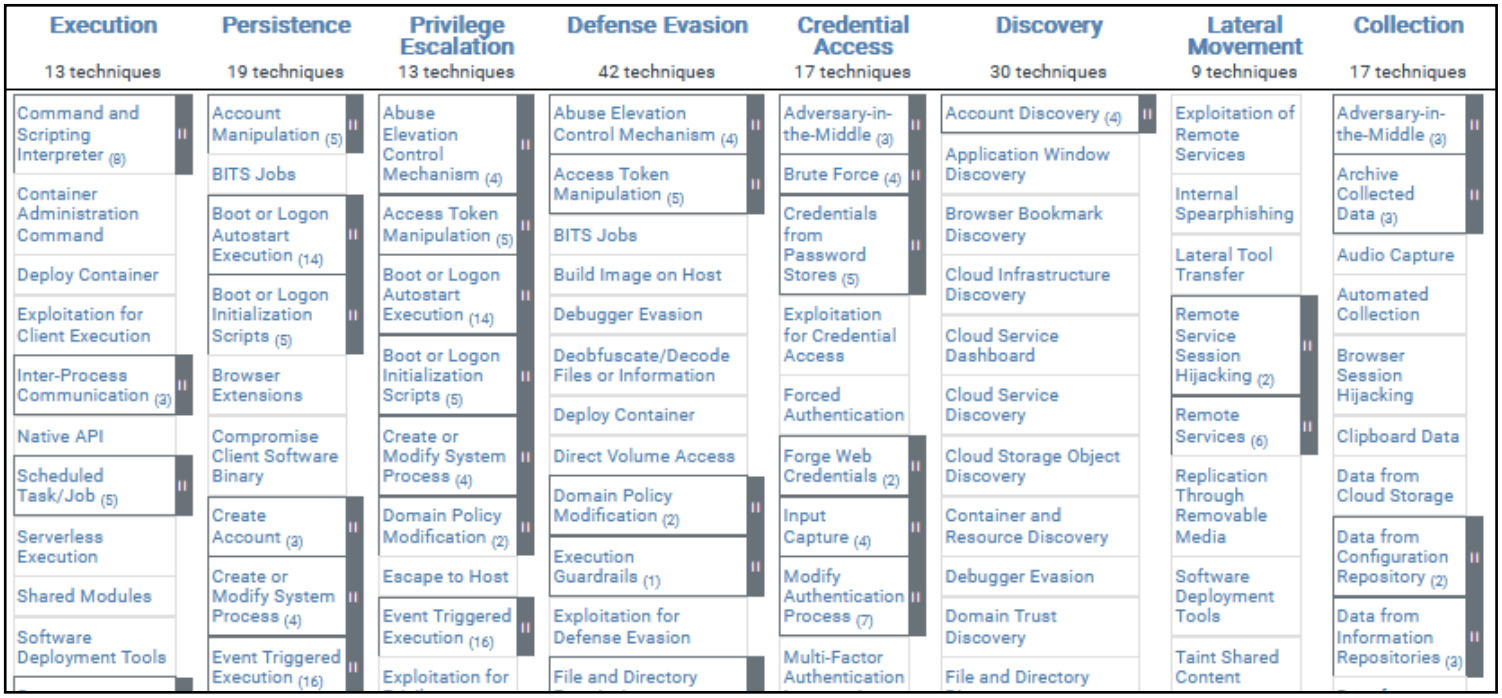

Figura 4: ejemplo de matriz MITTRE ATTACK

Este apartado se centrará en estudiar las 14 tácticas propuestas por MITRE para comprender los objetivos que persiguen los atacantes:

1. Reconocimiento: tiene por objetivo obtener la mayor información posible sobre la víctima, como el mapa de red, qué equipos están activos, qué vulnerabilidades tienen, etc. La calidad de la información obtenida en esta fase permitirá que un ataque sea exitoso o no, por lo que tiene gran importancia.
2. Obtención de recursos: tiene por objetivo crear, comprometer o robar recursos que puedan servir de soporte en fases posteriores del ataque, por ejemplo, mediante la programación de malware o ataques de phishing para el compromiso de cuentas de usuario.
3. Acceso inicial: tiene por objetivo conseguir entrar en la red y los sistemas de la víctima, por ejemplo, mediante el uso de servicios remotos externos (VPN) o cuentas de usuario comprometidas.
4. Ejecución: tiene por objetivo ejecutar código malicioso para comprometer los sistemas, por ejemplo, a través de shell remotas o mediante la apertura de un fichero por parte del usuario.

5. Persistencia: tiene por objetivo que el atacante sea capaz de permanecer en los sistemas la mayor parte del tiempo posible, por ejemplo, a través de la manipulación del código de arranque del sistema o tareas programadas.
6. Escalada de privilegios: tiene por objetivo conseguir mayores privilegios dentro de los sistemas, por ejemplo, a través de la manipulación de tokens de acceso.
7. Evasión de las defensas: tiene por objetivo que el atacante no sea descubierto dentro de los sistemas, por ejemplo, a través de la inhabilitación de software de seguridad como el antivirus.
8. Obtención de credenciales: tiene por objetivo hacerse con otras cuentas de usuario, por ejemplo, a través de ataques de fuerza bruta o tablas rainbow.
9. Descubrimiento: tiene por objetivo obtener la mayor cantidad de información a cerca del entorno donde se encuentra el atacante, por ejemplo, a través de la enumeración de programas y aplicaciones o las configuraciones de usuarios, grupos y permisos.
10. Movimiento lateral: tiene por objetivo desplazarse por los diferentes sistemas que componen la red víctima, por ejemplo, a través del uso de protocolos mal configurados.
11. Recolección de información: tiene por objetivo obtener datos de interés dentro de la red de la víctima, por ejemplo, accediendo a bases de datos o realizando capturas de pantalla con información comprometida.
12. Control remoto: tiene por objetivo que el atacante pueda comunicarse con los sistemas comprometidos desde fuera de la red de la organización, por ejemplo, mediante software de control remoto como TeamViewer.
13. Filtración de información: tiene por objetivo la extracción de información y datos fuera de la red de la víctima, para posteriormente sacar un rédito económico a través de su venta.
14. Impacto: tiene por objetivo interrumpir, manipular o destruir los sistemas de la víctima, por ejemplo, mediante ataques de denegación de servicio o encriptación de datos (ransomware).

Tal y como se puede observar, las amenazas a las que se enfrenta una organización son muchas y muy variadas, por lo que deben ser gestionadas desde un centro de operaciones de seguridad siguiendo un ciclo continuo de prevención, detección, respuesta y recuperación.

2.3 Estudio de los recursos humanos necesarios en un SOC

Las personas que trabajan en un SOC deben tener conocimientos técnicos, pero también ciertas cualidades como la curiosidad o la serenidad a la hora de afrontar situaciones complejas [13]. Encontrar profesionales altamente cualificados es una tarea difícil, algunos de los perfiles más destacados en ciberseguridad hoy en día son:

- Analista de ciberseguridad: es el rol principal de un SOC, se encarga de monitorizar y analizar los eventos de seguridad para identificar posibles amenazas.
- Técnico de respuesta a incidentes y analista forense: se encarga de paliar los incidentes de seguridad y de investigar la causa de los mismos a través de la recopilación de información.

- Threat hunter: su labor es la identificar posibles amenazas persistentes dentro de la red que hayan pasado desapercibidas por herramientas de seguridad automatizadas. Permite detectar más rápido un ataque y ayuda a minimizar su impacto.
- Analista de ciberinteligencia: recolecta y analiza información sobre las amenazas más comunes en cada momento y las diferentes tácticas y técnicas que emplean, con el objetivo de mejorar las defensas de la organización.
- Arquitecto/ingeniero de seguridad: se encarga de diseñar y mantener la infraestructura de seguridad (IDS/IPS, EDR, SIEM…).
- Governance and risk officer: se encarga de la gestión de riesgos de seguridad y de garantizar que las políticas y medidas de seguridad estén alineadas con los objetivos del negocio.
- Responsable del cumplimiento normativo: tiene como función garantizar que la empresa cumpla con todas las regulaciones, estándares y normas, especialmente aquellos relacionados con el tratamiento de datos personales (RGPD). Esté rol no es necesariamente técnico, si no que está más ligado al área de derecho.
- Analista de vulnerabilidades: se encarga de identificar y clasificar las vulnerabilidades que presenta la infraestructura de la organización, también se encarga de trabajar junto con otros equipos para remediarlas.
- Especialista en pruebas de penetración (read team): se encarga de emular el comportamiento de los atacantes mediante pruebas que permiten determinar si existen vulnerabilidades o malas configuraciones en los sistemas.
- Analista de malware: analiza código malicioso para determinar su comportamiento y características, también se encarga de desarrollar contramedidas para evitar la infección, propagación e impacto del mismo.
- Gestor de identidades: es el responsable de asegurarse de que las identidades digitales de los usuarios de la organización están correctamente protegidas, mediante la creación de usuarios, grupos, roles, políticas etc.
- SOC manager o head de ciberseguridad: es el responsable de todo el equipo que conforma el SOC, asignando tareas y responsabilidades a los diferentes miembros, priorizando el trabajo, planificando la estrategia del SOC y asumiendo las responsabilidades de las decisiones que se toman en materia de seguridad.
- Project manager: planifica, organiza, dirige y controla los recursos necesarios para llevar a cabo un proyecto, asegurando que se cumplen los objetivos de costes, tiempo y calidad del mismo.

Tal y como se ha visto, en un SOC existen numerosos perfiles, y no todos ellos deben tener capacidades técnicas. Los roles necesarios pueden variar en función del tamaño y la estructura de la organización, además, una misma persona puede desempeñar uno o varios roles.

2.4 Estudio de los recursos tecnológicos empleados en un SOC

Cada uno de los dispositivos que conforman una red empresarial genera miles de eventos al día acerca de su funcionamiento (comunicaciones, errores, inicios de sesión etc.). Todos esos eventos son recopilados y correlacionados a través de herramientas sofisticadas que detectan y generan alertas en base a patrones de ataque y comportamientos anómalos. El personal de un centro de un centro de operaciones de seguridad y, más en concreto, los analistas de seguridad, emplearán esta tecnología para monitorizar y responder ante incidentes de seguridad.
La figura 5 obtenida de [13], muestra la importancia del empleo de estas herramientas a la hora de reducir la cantidad de información con la que ha de trabajar el personal de un SOC:

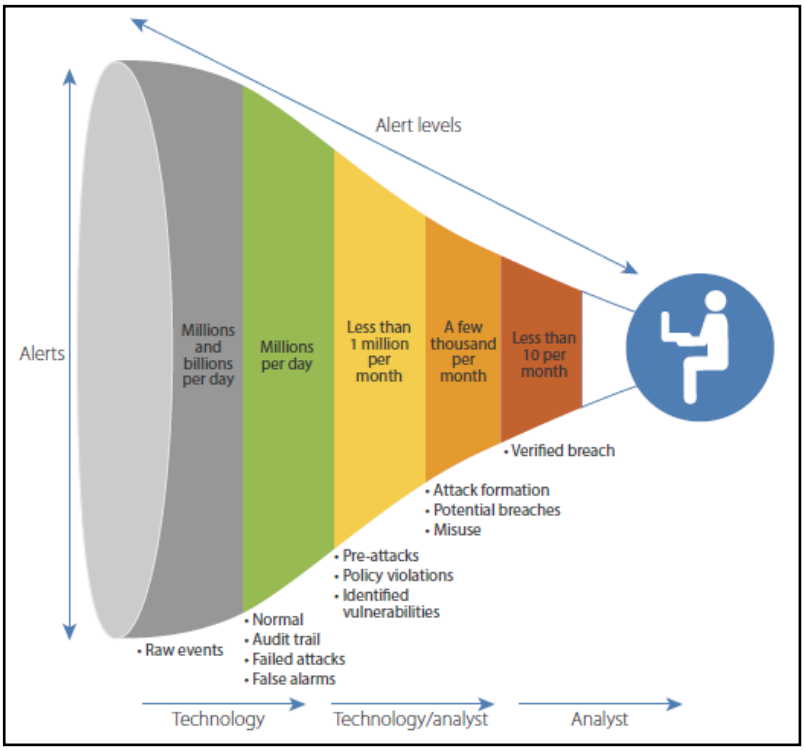

Figura 5: importancia de la tecnología en un SOC

En este apartado se realizará un estudio de la tecnología empleada dentro de un SOC, comprendiendo su funcionamiento y las diferentes alternativas que existen en el mercado.

2.4.1 SIEM

Un SIEM (Security Information and Event Management) es la herramienta central e indispensable de un centro de operaciones de seguridad. Recopila todos los eventos y datos generados por diferentes sistemas en tiempo real (servidores, firewall, equipos personales etc.) y los aglutina dentro de una misma base de datos. Posteriormente,

utiliza técnicas de correlación de eventos y casos de uso para detectar patrones y anomalías características de ataques e incidentes de seguridad [14].
Alguna de las ventajas que ofrece la implementación de un SIEM en una organización son: centralización de alertas, escalabilidad, inteligencia sobre amenazas, creación de informes, auditorías del cumplimiento normativo y detección de incidentes de seguridad en tiempo real.
Las dos herramientas SIEM líderes del mercado hoy en día son Splunk y Microsoft Sentinel, de acuerdo con el cuadrante mágico de Gartner del año 2022, mostrado en la figura 6 [15]:

Figura 6: cuadrante mágico de Gartner para la tecnología SIEM (2022)

Splunk (https://www.splunk.com/) es una solución que se puede implementar tanto en la nube como de forma local. Está pensada para empresas de tamaño mediano o grande y proporciona un análisis de todos los datos que ingesta en tiempo real. Su precio se estima para cada cliente y dependerá de la cantidad de información en GB que procese y almacene.
Azure Sentinel (https://azure.microsoft.com/es-es/products/microsoft-sentinel/), es un SIEM creado por Microsoft y basado únicamente en la nube de Azure. De entre sus características destaca el empleo de inteligencia artifical para ayudar a detectar comportamientos sospechosos. También factura por el volumen de datos ingeridos y almacenados (en GB).

2.4.2 Antivirus

Es las tecnología más ampliamente conocida en ciberseguridad, se emplea para detectar y eliminar software malicioso en equipos, tanto servidores como de usuario final. Su funcionamiento se basa en el escaneo en tiempo real de los ficheros que contiene un sistema en busca de patrones y firmas de virus conocidas, aunque también pueden tener otras funcionalidades secundarias como protección en la web o firewall. Las alertas y eventos generados por el Antivirus pueden ser recogidas por un agente y enviadas a una consola centralizada, donde sean gestionadas por personal especializado.
Dentro del mercado actual, uno de los productos más reconocidos en materia de Antivirus es McAfee (https://www.mcafee.com/es-es/antivirus.html). El producto es de pago y la cuota varía en función del número de dispositivos que se quieran proteger.
El Antivirus es la herramienta más esencial a nivel de seguridad y todo dispositivo debería contar con ella, no obstante, en este trabajo no nos centraremos en estudiarla tan a fondo, ya que el siguiente tipo de tecnología (EDR) es considerada “un paso más allá” del conocido Antivirus, extendiendo sus capacidades de detección.

2.4.3 EDR/NDR/XDR

El objetivo de estas tecnologías es la detección y la respuesta ante amenazas avanzadas [16]. Están basadas en la detección de anomalías, empleando técnicas como el análisis del comportamiento o la integencia artifical son capaces de detectar patrones de ataques. La diferencia principal entre EDR, NDR y XDR es el alcance de la detección de amenazas: un EDR se emplea a nivel de sistemas, un NDR a nivel de red y un XDR engloba a los dos anteriores.
Además, la funcionalidad de estas herramientas va mucho más allá de la detección de amenazas en tiempo real, si no que son también capaces de proporcionar respuestas ante las detecciones: bloqueo de procesos, conexiones, aislamiento del dispositivo de la red o conexión remota al mismo entre otros.
El cuadrante mágico de Gartner para la tecnología EDR [17] en 2022, mostrado en la figura 7, señala que los productos CrowdStrike y Windows Defender son los líderes en el mercado:

Figura 7: cuadrante mágico de Gartner para la tecnología EDR (2022)

Defender for Endpoint (https://www.microsoft.com/es-es/security/business/endpoint-security/microsoft-defender-endpoint) es la tecnología EDR propuesta por Microsoft y está basada en la nube de Azure. Entre sus principales ventajas se encuentra la integración con el resto de productos de la familia de Micorsoft (Defender for Antivirus o Azure Sentinel), y entre sus desventajas se encuentra el bajo rendimiento que presenta en entornos que no sean Windows (por ejemplo, Linux). Alguna de sus características son la protección en tiempo real, el empleo de inteligencia artificial para investigar automáticamente las alertas o el análisis de comportamiento.
Falcon Insight es el EDR propuesto por la empresa tecnológica CrowdStrike (https://www.crowdstrike.com/products/endpoint-security/falcon-insight-edr/). Entre sus características se encuentran la protección de múltiples plataformas y el uso de la inteligencia artificial y aprendizaje automático para la detección de amenazas.

2.4.4 Herramientas de análisis de vulnerabilidades

Las herramientas de análisis de vulnerabilidades permiten tener una visión global de los activos informáticos que conforman una organización para identificar, evaluar y priorizar las vulnerabilidades que se encuentren en los mismos [18]. Siguen un enfoque basado en riesgos donde priorizan y categorizan las vulnerabilidades detectadas para una óptima remediación de las mismas.
Algunos ejemplos de herramientas de gestión de vulnerabilidades que podemos encontrar en el mercado son:

- Nessus (https://es-la.tenable.com/products/nessus): es una de las herramientas más empleadas a nivel empresarial. Permite, entre otas cosas, el escaneo de la infraestructura para la identificación, clasificación y remediación de vulnerabilidades, la generación de reportes y el soporte técnico avanzado. También cuenta con la capacidad de personalizar los escaneos de

vulnerabilidades. Es una herramienta de pago con distintos tipos de licenciamiento y su precio oscila entre los 4000 y 6000 euros anuales.

- OpenVAS (https://www.openvas.org/): es una herramienta de código abierto que permite también la identificación y remediación de vulnerabilidades en sistemas informáticos, así como la creación de informes.
- OWASP ZAP (https://www.zaproxy.org/): es una herramienta de código abierto y multiplataforma que permite detectar vulnerabilidades en aplicaciones web. Entre sus funcionalidades se encuentran la captura de peticiones y respuesta entre client y /servidor web.

2.4.5 Herramientas de análisis forense digital

Este tipo de herramientas son empleadas para recopilar, analizar y presentar evidencia digital de actividades sospechosas o delitos en investigaciones forenses, manteniendo la cadena de custodia [19]. Incluyen el análisis forense de bases de datos, disco, memoria RAM, correo electrónico, archivos, dispositivos móviles etc. Además, permiten recuperar información eliminada, analizar metadatos, crear informes y documentar los hallazgos.
Algunos ejemplos de herramientas de análisis forense que podemos encontrar en el mercado son:

- Volatility (https://www.volatilityfoundation.org/): es una herramienta de código abierto empleada en el análisis de memoria RAM.
- Autopsy (https://www.autopsy.com/): también es una herramienta de código abierto y se emplea para analizar la información contenida en un disco duro, memorias USB o capturas de tráfico de red.

2.4.6 Herramientas de pruebas de penetración (pentesting)

Las herramientas para realizar pruebas de penetración en los sistemas (pentesting) permiten simular ataques de forma real, pudiendo detectar así vulnerabilidades o fallos en la configuración de los sistemas y explotarlos para ver los riesgos a los que se encuentra sometida la organización [20].
Algunos ejemplos de herramientas de pentesting que podemos encontrar en el mercado son:

- Metasploit (https://www.metasploit.com/): es una herramienta de código abierto, aunque contiene algunas funcionalidades de pago. Está formada por una gran variedad de scripts (payloads) que explotan vulnerabilidades conocidas de forma automatizada, entre sus muchas funcionalidades se encuentra la ejecución de comandos o la extracción de información de forma remota.
- Nmap (https://nmap.org/): permite realizar escaneos sobre la red de una organización o determinados sistemas de la misma, con el objetivo de obtener información valiosa como la infraestructura de red o las aplicaciones y sus vulnerabilidades que se encuentran en ejecución en los hosts.

2.4.7 Herramientas de protección

Las herramientas de protección tienen por objetivo garantizar la seguridad de los sistemas y de la red de una organización antes de que ocurra un ataque [21]. Entre sus funcionalidades podemos encontrar la detección y prevención de amenazas, el análisis de comportamiento y la flexibilidad y escalabilidad que ofrecen.
Existen varios tipos de herramientas de protección que pueden ser empleados en un centro de operaciones de seguridad:

- Firewalls/WAF: controlan y limitan el tráfico de red entrante y saliente, pueden ser implementados a través de hardware o software. Un tipo especial de firewall son los WAF (web application firewall) que se emplean para proteger aplicaciones web ante ataques conocidos.
- Sistemas de prevención y detección de intrusiones (IPS/IDS): se basan en el análisis de tráfico de red para identificar patrones de comportamiento sospechosos que puedan estar relacionados con ataques. Los IDS son empleados para detectar intrusiones, mientras que los IPS son empleados para bloquear detecciones.
- Sistemas de protección de correo electrónico: se emplean para detectar y bloquear correos electrónicos sospechosos. Funcionan escaneando los archivos y URLs adjuntos, así como las cabeceras de los emails.
- Sistemas de protección de la navegación (proxy): se emplean para limitar el acceso a Internet por parte de los usuarios de la red, por ejemplo, bloqueando el acceso web a sitios maliciosos o inapropiados. Existen diversos tipos de proxy: web, inverso, SSL, DNS etc.

2.4.8 Herramientas de gestión de tickets

Las herramientas de gestión de tickets permiten centralizar todas las alertas generadas por los diferentes sistemas de prevención y detección en una sola plataforma, de esta forma se garantiza que las incidencias sean atendidas en base a su prioridad y se les dé un seguimiento adecuado [22].
Entre las funcionalidades que presentan se pueden econtrar: notificaciones automáticas, priorización, notificación y registro de incidentes y obtención de informes y métricas relativo a la gestión. Algunas de las herramientas de gestión de tickets más empleadas en la actualidad son:

- ServiceNow (https://www.servicenow.com/es/): está basada en la nube y permite la gestión del ciclo de vida de incidentes, problemas, cambios y solicitudes. Puede configurarse en base a las necesidades de la organización, por lo que su precio es personalizado para cada cliente en base a los servicios que requiera. Admite integraciones con muchas de las herramientas de seguridad.
- OTRS (https://otrs.com/es/home/): es una herramienta de código abierto que puede configuarse tanto en la nube como de forma local. Entre sus funcionalidades destaca su gran nivel de automatización de procesos y flujos de trabajo.

2.5 Normativa y estándares aplicables

Los estándares y normativas existentes proporcionan un marco de trabajo estructurado y bien definido para la gestión y protección de los datos y los sistemas. Su aplicación debe ser de gran importancia para las empresas, en los siguientes subapartados se estudiarán las normativas y estándares más importantes en la actualidad aplicables a un SOC.

2.5.1 ISO 27001

ISO 27001 es una normativa internacional que pretende asegurar la confidencialidad, integridad y disponibilidad de la información y los sistemas que conforman una organización. En ella se define cómo desplegar, verificar y controlar un SGSI (Sistema de Gestión de la Seguridad de la Información) en cualquier tipo de empresa, mediante la definición de una serie de buenas prácticas [23].
El eje central de esta normativa es la evaluación de riesgos relacionados con las amenazas informáticas y se divide en tres apartados principales:

1. Definición del alcance: mediante la identificación de activos, vulnerabilidades, amenazas, requisitos legales y riesgos.
2. Cálculo del riesgo: determinado por la probabilidad de ocurrencia de un riesgo y el impacto que tendría sobre la organización.
3. Plan de tratamiento de riesgos: se seleccionan los controles necesarios para tratar los riesgos y pueden ir destinados a asumir, reducir, eliminar o transferir el riesgo.

La figura 8 muestra la metodología seguida por la norma ISO 27001 para gestionar el riesgo:

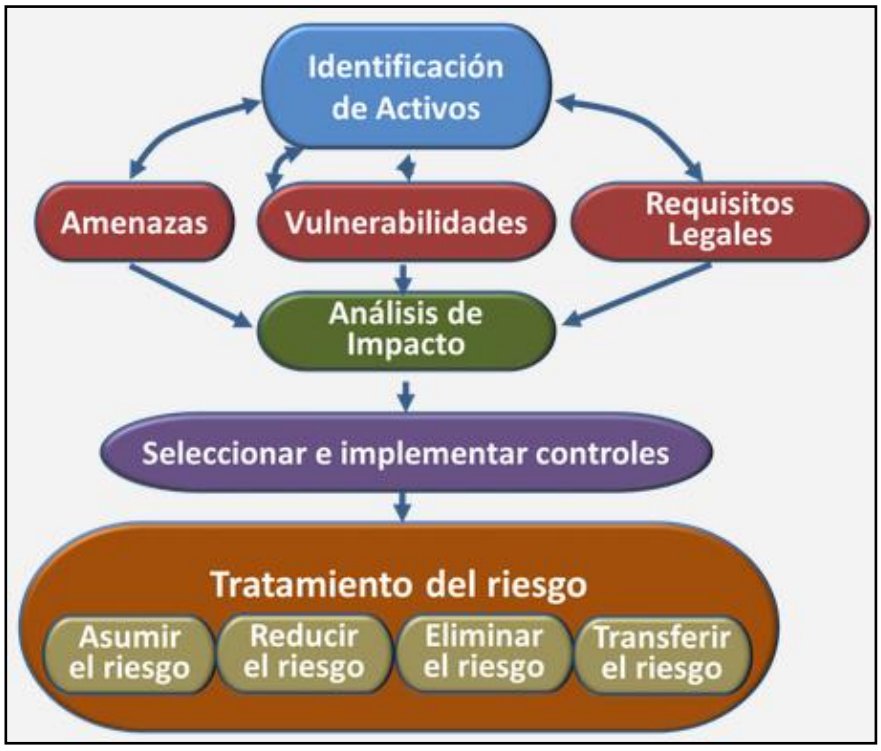

Figura 8: gestión del riesgo según la norma ISO 27001

2.5.2 Reglamento General de Protección de Datos (RGPD)

El Reglamento General de Protección de Datos [24] establece una serie de reglas y principios dentro de la Unión Europea con el objetivo de proteger la privacidad y seguridad de los datos personales de los cuidadanos.
Algunos aspectos importantes del RGPD son:

1. Se aplica a cualquier empresa que trate datos personales de usuarios de la UE, independientemente de su ubicación.
2. Se definen una serie de derechos que los usuarios tienen con respecto a sus datos personales: derecho al olvido, a la supresión, a la modificación, a conocer la finalidad del tratamiento o a la portabilidad de los datos, entre otros.
3. Las empresas están obligadas a implementar las medidas técnicas y organizativas necesarias para que se cumpla la lay. También están obligadas a notificar a las autoridades y usuarios cuando se ha producido una brecha de seguridad.
4. Los usuarios deben dar su consentimiento explícito para recopilar sus datos.

Dentro de un SOC el cumplimiento de esta ley es obligatorio, ya que entre la información que se gestiona pueden encontrarse datos personales de los usuarios. De no cumplir con esta normativa, la organización puede exponerse a duras sanciones y a una pérdida de reputación.

2.5.3 Guías NIST

Las guias desarrolladas por el Instituto Nacional de Estándares y Tecnología [25] constituyen un conjunto de buenas prácticas que se deben llevar a cabo en ciberseguridad. Las tres guías NIST más importantes son:

1. NIST 800-115, guía técnica para evaluaciones y pruebas de seguridad de la información: proporciona un marco de trabajo para la realización de pruebas de vulnerabilidad en los sistemas informáticos y la evaluación y gestión de riesgos de los mismos.
2. NIST 800-94, guía para la prevención y detección de intrusiones en sistemas: proporciona las directrices para la selección, configuración, implementación y mantenimiento de los sistemas con la finalidad de protegerlos. Sigue un enfoque basado en la identificación de riesgos y su gestión.
3. NIST 800-61, guía para la gestión de incidentes de ciberseguridad: se encuentra dividida en planes y políticas de respuesta, gestión de los incidentes y coordinación, y compartición de información entre los diferentes equipos que componen la organización.

2.5.4 ISO 22301

La normativa ISO 22301 establece una serie de controles y medidas que permiten hacer frente a los riesgos a los que se encuentra expuesta la continuidad de negocio de una organización [26]. Esta norma define el concepto de incidente como cualquier evento no planificado que interrumpe la continuidad de las operaciones de la organización (desastres naturales, errores humanos, cortes de suministro etc.). Puede ser empleada por organizaciones de todo tipo y tamaño.

Está diseñada para prevenir, responder y recuperarse ante cualquier tipo de incidente y su aplicabilidad en un centro de operaciones de seguridad garantiza la disponibilidad y la continuidad de las operaciones de seguridad críticas.
Para su implantación, la organización debe realizar en primer lugar un análisis de los riesgos a los que se encuentra expuesta y cómo estos afectan a su negocio. Posteriormente, debe tomar medidas para evitar o reducir la probablidad de que aparezcan, así como planes de recuperación en caso de que los incidentes lleguen a suceder.

2.5.5 Esquema Nacional de Seguridad (ENS)

El Esquema Nacional de Seguridad (ENS) establece un conjunto de medidas y requisitos que deben cumplir todas las entidades públicas y privadas que manejen información clasificada o datos personales. Está desarrollado por el Centro Criptológico Nacional y las Administraciones públicas y tiene por objeto la implantación de una política de seguridad en el uso de los medios electrónicos y garantizar debidamente la protección de la información [27].
Entre los principios básicos del ENS se pueden encontrar los siguientes aplicables a un centro de operaciones de seguridad:

- Gestión de la seguridad de la información y continuidad de negocio: mediante requisitos que incluyen la identificación y evaluación de riesgos y la implantación de medidas de seguridad adecuadas. También incluye la implementación de planes, pruebas y ejercicios de continuidad de negocio.
- Protección de los sistemas: mediante medidas como la autenticación, el cifrado o la gestión de accesos.
- Gestión de incidentes de seguridad: mediante requisitos que incluyen el análisis, notificación y respuesta de incidentes.

2.5.6 ENISA

La Agencia Europea de Ciberseguridad (ENISA) pone a disposición de las organizaciones una guía práctica para el diseño, implantación y operación de un centro de operaciones de seguridad (SOC) o un equipo de respuesta a incidentes de seguridad (CSIRT) [28].
Tal y como muestra la figura 9, la guía de ENISA proporciona una orientación detallada sobre los procesos y actividades necesarios para desplegar un SOC/CSRIT, desde la definición de requisitos iniciales y la evaluación de riesgos hasta la gestión de incidentes o la contratación y formación de personal:

Figura 9: ciclo de implementación de un SOC/CSIRT según la guía ENISA

2.6 Principales servicios de un SOC

El objetivo principal de un centro de operaciones de seguridad es la monitorización de alertas y la respuesta ante incidentes, no obstante, un SOC puede proveer muchas más funcionalidades que ayuden a gestionar de forma global la ciberseguridad de una organización. En este apartado se estudiarán los diferentes servicios que puede brindar un centro de operaciones de seguridad actual.

2.6.1 Monitorización y gestión de alertas

Es el servicio principal de un SOC, se basa en la recopilación de información y eventos generados por las diferentes entidades digitales que conforman una organización (servidores, ordenadores personales, cuentas de usuario, red etc.) y en la correlación de dichos eventos para generar alertas de seguridad.
Dicha monitorización se realiza en tiempo real con ayuda de muchas de las herramientas vistas en el apartado anterior. Las alertas son analizadas por expertos en ciberseguridad, que determinan si se trata de un ataque real, evaluan la prioridad de las mismas y toman medidas de contención.
Es un servicio crítico en cualquier empresa, ya que permite detectar y analizar de manera proactiva los incidentes de seguridad, reduciendo el impacto y alcance de los mismos.

2.6.2 Respuesta a incidentes y análisis forense (CSIRT)

Una vez han sido identificadas las alertas como ataques, estas se convierten en incidentes de seguridad, por lo que es necesario una reacción rápida y coordinada para mitigar las posibles consecuencias.
La guía 800-61 del NIST define cuatro fases en el ciclo de vida de gestión de incidentes de seguridad [29], mostradas en la figura 10:

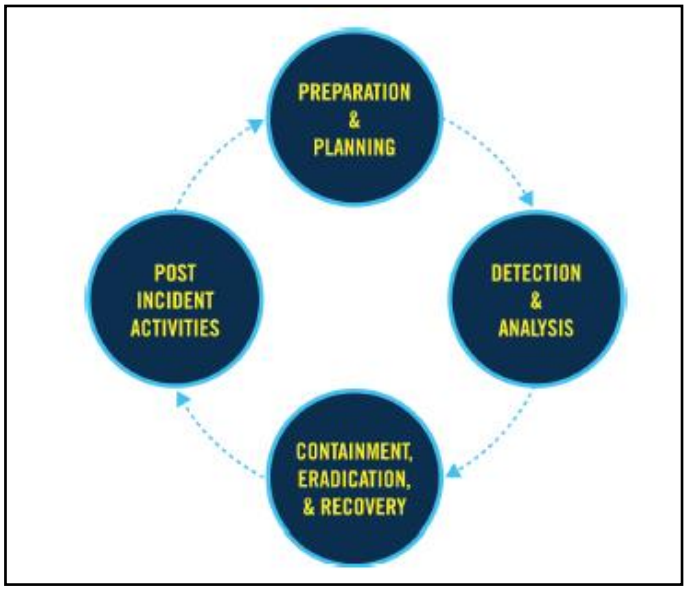

Figura 10: ciclo de vida de la gestión de incidentes, guía NIST 800-61

1. Planificación y preparación: esta fase ayuda a los profesionales a responder al incidente de una forma eficiente, efectiva y completa. En ella, se deben establecer canales de comunicación entre todas las partes involucradas, definir procedimientos de respuesta y escalado o incluir planes para recuperar la información y los servicios ante incidentes graves, entre otros.
2. Detección y análisis: consiste en controlar el incidente para minimizar los riesgos asociados y analizar lo ocurrido, conociendo el contexto del mismo (aplicaciones, sistemas, usuarios comprometidos etc.) y sus posibles conscuencias (fallos, pérdidas de información o servicio etc.).
   Dentro de esta fase, juegan un papel muy importante las técnicas de análisis forense, que permiten determinar cómo se ha producido el incidente y recopilar la evidencia digital que puede ser empleada posteriormente en investigaciones legales.
3. Contención, erradicación y recuperación: se elimina completamente la amenaza de los sistemas, eliminando todo rastro posible. Además, se restauran los sistemas afectados al estado anterior al incidente.
4. Actividades post-incidente: se analiza y documenta el incidente y se implementan medidas de seguridad adicionales para asegurarse de que no vuelva a suceder.

2.6.3 Bastionado de redes y sistemas

El bastionado de redes y sistemas, también denominado hardening, es una medida de protección que tiene por objetivo reducir la superficie de ataque mediante la aplicación de buenas prácticas [30]. Entre las medidas técnicas que se pueden aplicar se encuentran: eliminación de servicios y aplicaciones innecesarios, desactivación de cuentas de usuario no utilizadas, restricción de permisos de usuario, creación de políticas de contraseñas, etc.
Existen diferentes guías y recomendaciones, muchas de ellas proporcionadas por los proveedores, que permiten realizar el proceso de bastionado. Por ejemplo, Microsoft

pone a disposición de los usuarios la “Microsoft Security Baseline”, una guía que permite configurar sus sistemas operativos y aplicaciones de forma segura.
Con el bastionado se logra reducir los riesgos de exposición y construir unos sistemas robustos, mejorando así la seguridad global de la organización.

2.6.4 Threat hunting

El threat hunting es una práctica basada en la búsqueda proactiva de amenazas. Parte de la suposición de que los sistemas y las redes ya han sido comprometidos y trata de buscar indicadores de ataque (IOA) e indicadores de compromiso (IOC) que no hayan sido detectados por las herramientas habituales (EDR, SIEM, Antivirus etc.) [31]. El proceso de threat hunting se divide en tres fases:

1. Hipótesis: de que algún tipo de actividad maliciosa pueda estar afectando a los sistemas de una organización.
2. Análisis: se comprueba si la hipótesis es correcta empleando herramientas y metologías para analizar la información con el objetivo de descubrir TTPs.
3. Descubrimiento: una vez identificadas o descubieras las TTPs, se les hace un seguimiento con el objetivo de obtener visibilidad y detección automática sobre ellas.
4. Resultados: se trata de determinar los hallazgos, su severidad, documentar los descubirmientos, las vulnerabilidades, el tiempo que los sistemas han estado comprometidos etc.

El threat hunting es totalmente complementario con los servicios de monitorización y respuesta a incidentes comentados anteriormente. Esta técnica permite, no sólo detectar ataques sofisticados dentro de la red, si no también nuevos tipos de ataque y actores maliciosos desconocidos hasta el momento.

2.6.5 Threat intelligence

La inteligencia de amenazas es un servicio que procesa información sobre la intención, oportunidad y capacidad que poseen los diferentes actores maliciosos para atacar a una organización, convirtiendo estos datos en inteligencia. Se nutre de diferentes fuentes, tanto internas como externas: foros de cibercriminales, dark web, redes sociales, herramientas OSINT etc. [32]
La fases en las que se divide el ciclo de threat intelligence se muestran en la figura 11:

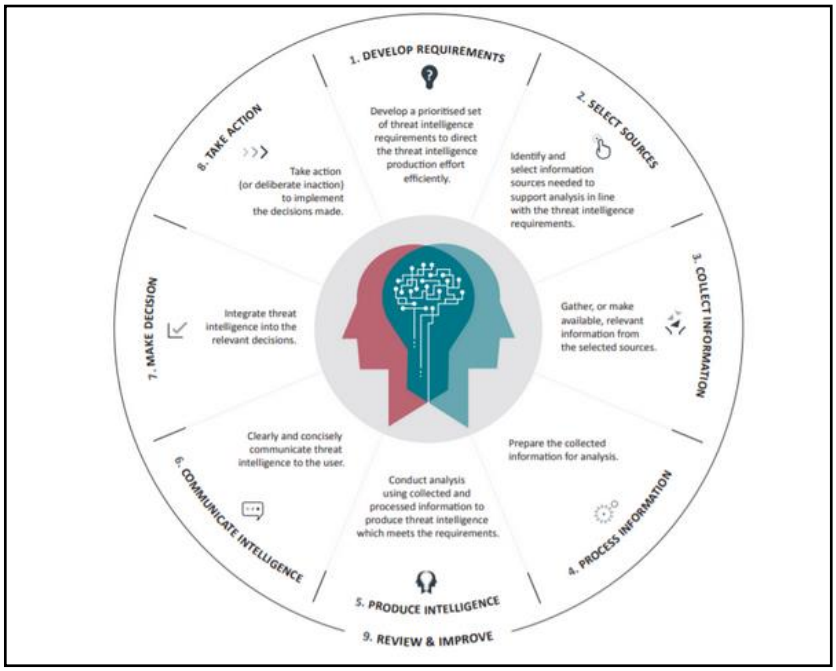

Figura 11: ciclo de vida del threat intelligence

El ciclo de vida se inicia con la identifcación de los objetivos que se pretenden lograr. Posteriormente, se recopila, analiza y enriquece la información usando diferentes fuentes de datos y se evalúa identificando posibles amenazas y sus consecuencias. Finalmente, la información se comparte con las partes interesadas para implementar medidas de protección.

2.6.6 Análisis de vulnerabilidades

En un análisis de vulnerabilidades se identifican y clasifican las debilidades de un sistema, con la finalidad de minimizar la superficie de exposición ante ciberataques. Para ello se emplean herramientas automatizadas que escanean los diferentes sistemas que componen la red en busca de vulnerabilidades ya conocidas [33].
El análisis de vulnerabilidades consta de las siguientes fases:

1. Identificar los activos: durante esta fase se enumeran los sistemas, datos, software, etc. que se va a analizar.
2. Detección de vulnerabilidades: se emplean herramientas automatizadas que escanean los activos en busca de vulnerabilidades registradas en sus bases de datos.
3. Análisis y clasificación: se evalúa el impacto y la gravedad de las vulnerabilidades y se ordenan en función de su prioridad.
4. Informe y medidas correctivas: se genera un informe detallado con las vulnerabilidades encontradas y se toman medidas para solucionarlas (como aplicar parches de seguridad).

2.6.7 Análisis de phishing y malware

El phishing es uno de los tipos de ataque de ingeniería social más empleados hoy en día, consiste en engañar a la víctima para que revele información confidencial (como contraseñas) y el vector de ataque más usado es el correo electrónico. Es la forma más sencilla de realizar un ataque y a la vez la más efectiva [34].

Un SOC puede proveer a sus clientes de un servicio de análisis de phishing, en el que se revisen correo electrónicos u otros mensajes sospechosos, en busca de intentos de obtención de información confidencial. Además del análisis, también se pueden aplicar medidas correctivas en caso de que las detecciones sean positivas, como el bloqueo de direcciones IP o el reseteo de contraseñas de usuario.
Otro servicio que agrega valor añadido a un SOC es el análisis de malware [35], ya que existen códigos que no son detectados por los antivirus tradicionales (bien porque no se habían visto antes o bien porque no están incluidos en sus bases de datos de firmas). Mediante este análisis se determina el comportamiento, funcionalidad y origen de un software potencialmente malicioso. Los analistas emplean técnicas complejas como la ingeniería inversa o el estudio de la distribución y el origen del software.

2.6.8 Formación en ciberseguridad

Un servicio de formación en ciberseguridad tiene por objetivo mejorar el conocimiento y la conciencia sobre ciberseguridad de los empleados de una organización, reduciendo así la probabilidad de incidentes de seguridad [36].
Consiste en un plan que englobe conocimientos sobre buenas prácticas de seguridad, identificación de riesgos y prevención de ataques. Dicha formación puede ser impartida a cualquier nivel organizativo, tanto a personal técnico como a altos directivos y la forma más habitual de hacerlo es a través de cursos en línea.

2.6.9 Pruebas de penetración (pentesting)

El pentesting constituye un conjunto de ataques simulados contra una red o sistema con la finalidad de detectar vulnerabilidades o fallos en la configuración [37]. Para llevarlo a cabo, se traza un plan con un conjunto de ataques dirigidos que permiten evalúar las defensas de los sistemas afectados. Una vez realizadas las pruebas de penetración, se presenta un informe a las partes interesadas con los descubrimientos realizados y la repercusión de estos sobre la organización.
Existen diferentes tipos de pentesting dependiendo de la información con la que cuenta la empresa que va a realizar las pruebas:

- De caja blanca: se dispone de información detallada sobre la infraestructura de sistemas, redes y aplicaciones. De esta forma se simula que el ataque lo realiza un trabajador de la empresa. Este tipo de prueba es la que conlleva menos tiempo y por lo tanto menos costes económicos.
- De caja gris: en este caso se dispone de parte de la información.
- De caja negra: no se dispone de ningún tipo de información a cerca de la empresa a la que se van a realizar las pruebas. Este caso simula un ataque real, por lo que conlleva un mayor tiempo y coste económico.

Un aspecto importante a tener en cuenta cuando se provee servicios de penetración son las cuestiones legales. Deberá firmarse un contrato en el que se incluya la autorización expresa, clara e inequívoca para la vulneración de los sistemas por parte de los interesados.

2.6.10 Consultoría de seguridad

El servicio de consultoria provee asesoramiento por parte de especialistas en ciberseguridad a organizaciones, en la identificación, evaluación y gestión de riesgos en los sistemas y redes. El objetivo es ayudar a los clientes a mejorar la postura en ciberseguridad mediante la implantación de medidas técnicas [38].
La consultoría de seguridad puede englobar otros servicios como la gestión de vulnerabilidades, el diseño de políticas y planes de seguridadla formación de los usuarios etc.
Entre los beneficios que ofrece se encuentran la reducción de riesgos y de la superficie de exposición o la mejora de reputación

2.6.11 Cumplimiento normativo

El servicio de cumplimiento normativo permite ayudar a las organizaciones a cumplir con la legislación vigente en materia de ciberseguridad. Para ello. implementa políticas y procedimientos, evalua periódicamente la adhesión a los nuevos estándares y leyes y aplica medidas correctivas en caso de que se produzcan desviaciones.
Algunas de las leyes que se han de tener en cuenta en materia de ciberseguridad son: la Ley de Protección de Datos, la Ley de Seguridad Nacional, la Ley de Ciberseguridad o el Reglamento General de Protección de Datos.

3. Implementación de un SOC en una organización

El objetivo de este capítulo es implementar un servicio de SOC desde cero, teniendo en cuenta los potenciales clientes, los recursos tecnológicos y humanos necesarios y los principales competidores. Finalmente, se evaluará el proyecto para determinar los riesgos a los que se expone la organización que va a proveer el servicio.

3.1 Identificación del proyecto

Mediante este proyecto se pretende desarrollar un servicio de ciberseguridad orientado a pequeñas y medianas empresas en base a sus necesidades (potenciales atacantes, dimensiones, presupuesto, etc.).
Mientras que las grandes organizaciones cuentan con equipos propios de ciberseguridad y presupuestos elevados, las pymes continúan siendo un blanco fácil para los ciberatacantes. Según [39], el 60% de las pymes europeas que sufre un ciberataque quiebra en los 6 meses siguientes al incidente, lo que remarca la necesidad de diseñar un servicio específico basado en las características de este tipo de empresas.
De acuerdo con el informe “Cifras Pyme 2023” publicado por el ministerio de industria, comercio y turismo [40], en España existen más de dos millones de pequeñas y medianas empresas las cuales componen el 99% del tejido empresarial, tal y como muestra la figura 12:

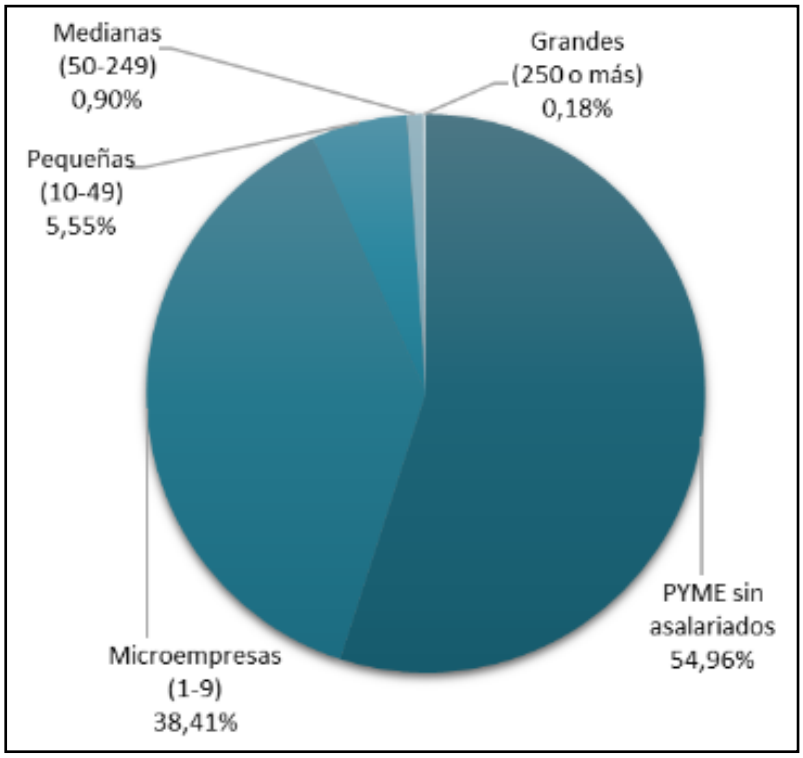

Figura 12: distribución de empresas en España por tamaño

En cuanto la distribución por sectores, nos encontramos ante una situación en la que mayoría de las empresas está dedicada al sector servicios, tal y como muestra la figura 13:

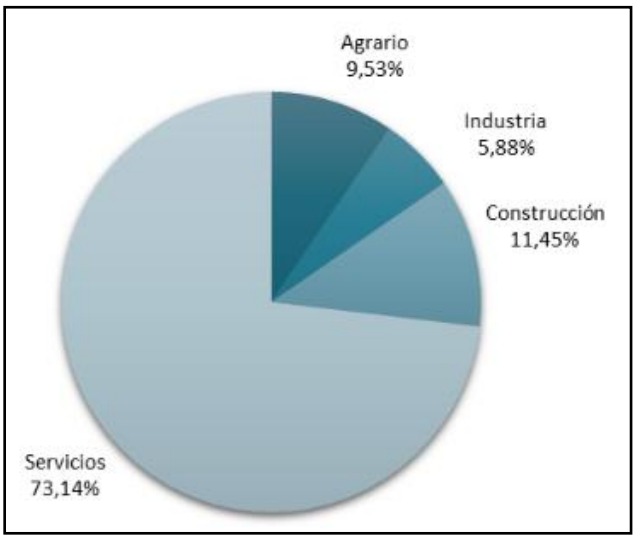

Figura 13: distribución sectorial de las pymes en España

Los datos obtenidos proporcionan un contexto de la situación y cuál será el nicho de mercado del centro de operaciones de seguridad: empresas con pocos trabajadores y orientadas al sector servicios.
Finalmente, es importante destacar que en este trabajo se planteará la creación de una empresa desde cero, teniendo en cuenta los diferentes estados por los que pasará hasta brindar un servicio completo de SOC a sus clientes.

3.2 Estudio de mercado

En este apartado del trabajo se pretende analizar los principales competidores del proyecto, es decir, aquellas empresas ya existentes en el mercado que brindan servicios de ciberseguridad a pymes. Para ello, se ha hecho uso del catálogo de empresas y soluciones de seguridad creado por el Instituto Nacional de Ciberseguridad (INCIBE) [41]. Algunas de estas empresas y sus características son:

- Aplicaziones (www.aplicazion.es): está orienda a pymes y proporciona ingeniería e implantación de soluciones de seguridad.
- Sipy (https://www.sipy.net): proprciona servicios de protección de datos y privacidad, así como auditorías de seguridad. También está orientada a pymes.
- Dagara (https://dagara.net/): orientada a pymes, proporciona servicios de implementación de sistemas de alertas y logs, monitorización y análisis de vulnerabilidades.
- Secuora (www.secuora.es): proporciona servicios de monitorización y respuesta, así como seguridad ofensiva.
- Abast (http://www.abast.es): proporciona servicios de auditoría y consultoría de seguridad.

- Basetis (https://www.basetis.com/): proporciona servicios de consultoría, test de intrusión y vulnerabilidades y SOC.
- Bullhost (https://bullhost.security/): proporciona servicios de prevención, detección y respuesta ante incidentes de seguridad. También realiza auditorías y consultorías de seguridad.
- Seresco (www.seresco.es): ofrece servicios de auditoría y consultoría en ciberseguridad.
- CSB (https://www.csb-consultancy.com): servicios de consultoría, diseño de arquitectura de seguridad y consultoría legal en materia de protección de datos.
- Ewala (https://www.ewala.es/): ofrece servicios de ciberseguridad 100% personalizados a sus clientes, entre los que se encuentran el análisis de vulnerabilidades, la monitorización y respuesta a incidentes o la consultoría.
- Alisec (https://www.alisec.es/): ofrece servicios de seguridad ofensiva (pentesting y análisis de vulnerabilidades) y seguridad defensiva (monitorización, respuesta y remediación de incidentes).
- Gatakka (http://www.gatakka.net): orientada a pymes, ofrece la implantación de soluciones de ciberseguridad opensource (antivirus, sistemas de backup y firewall).
- Ibaru (https://ibaru.es/): proporciona servicios de monitorización de sistemas y red, así como la implantación de soluciones de seguridad.

Aunque no todas las empresas que proporcionan servicios de ciberseguridad a pymes en España se encuentran en el listado previo, éste sirve como referencia para obtener una imagen del estado actual del mercado. Algunas de las conclusiones que se han obtenido a través de él son:

1. Existe una clara diferenciación entre servicios técnicos y de auditoría o jurídicos: la gran mayoría de empresas que ofrece servicios técnicos (gestión de vulnerabilidades, pentesting, respuesta a incidentes etc.) no ofrece servicios de auditoría o asesoramiento jurídico en materia de protección de datos.
2. Muchas de las empresas cuentan con un catálogo de servicios reducido, en dónde se proporcionan los servicios básicos de un SOC, como la monitorización y gestión de alertas o el análisis de vulnerabilidades. Se dejan de lado servicios más avanzados como el threat hunting o threat intelligence.
3. Los servicios que se ofrecen son generalistas y poco orientados a pymes: están pensados para dar servicio a cualquier tipo de cliente, sin tener en cuenta las necesidades o características específicas de las pequeñas y medianas empresas.

Pese a la existencia de estas empresas que ofrecen servicios de seguridad, las estadíticas demuestran que las pymes españolas no están preparadas para afrontar incidentes, ya que sólo el 2% se considera ciberexperta [42]. Además, son el objetivo principal de los atacantes, debido a la facilidad que presentan a la hora de ser atacadas y obtener beneficios, ya que disponen de menos medios o se encuentran más desprotegidas.

Este panorama remarca la necesidad y cabida en el mercado del proyecto planteado en este trabajo, que es la creación de soluciones y servicios que se adapten a las pymes, económica y técnicamente.

3.3 Catálogo de servicios del SOC

Los apartados anteriores han servido para definir cuál es potencial cliente al que irán dirigidos los servicios de ciberseguridad que se planteen en este proyecto, el siguiente paso (y objetivo de este apartado), es determinar sus necesidades y generar una cartera de servicios en base a las amenazas de seguridad a las que se encuentran expuestos.

3.3.1 Estudio de las necesidades en ciberseguridad de las pymes

De acuerdo con el Instituto Nacional de Ciberseguridad [43], la principal amenaza a la que se encuentran expuestas las pequeñas y medianas empresas españolas es la industria del cibercrimen, compuesta por grupos altamente organizados y con fines lucrativos. Algunos de los servicios que ofrecen estos cibercriminales son:

- Malware como servicio: se desarrolla software malicioso en base a las especificaciones del cliente.
- Fraude en transacciones económicas: mediante el cual se consiguen datos bancarios de la víctima. Genera grandes pérdidas económicas y de reputación.
- Intrusiones de red: realizadas generalmente con el objetivo de obtener información, propiedad intelectual o de realizar extorsiones.
- Obtención de información sensible: a través de técnicas de ingeniería social que permiten hacerse con cuentas de usuario y otra información que pueda ser de gran utilidad en posteriores ataques.

La obtención de datos es el objetivo principal de estos atacantes, ya que pueden revender esta información a terceras partes interesadas o emplearlos en futuros ataques. Entre los incidentes de seguridad más habituales que sufren las pymes españolas se encuentran [44]:

1. Ramsomware: es uno de los ataques más comunes hoy en día, se basa en el empleo de un software malicioso que encripta la información contenida en un dispositivo con el objetivo de extorsionar a la víctima y obtener una recompensa económica a cambio de recuperar la información. Generalmente, este software tiene la capacidad de replicarse a través de la red y puede llegar a infectar toda la infraestructura de la organización víctima si ésta no está bien diseñada, por lo que las consecuencias son nefastas.
2. Ataques de ingeniería social: se basan en obtener información a través del engaño. El más común es el phishing en el que, a través de un correo electrónico o un SMS, el atacante se hace pasar por un remitente de confianza para obtener datos confidenciales como contraseñas de usuario.
3. Malware: hace referencia a cualquier tipo de software malicioso. El objetivo más común de estos programas es el robo de información sensible, como los troyanos o keyloggers.
4. Ataques de denegación de servicio: pretenden interrumpir o inhabilitar un servicio en línea y emplean técnicas como la inundación de tráfico, el agotamiento de recursos o la explotación de vulnerabilidades. Pueden acarrear a la víctima pérdidas económicas, de reputación y de servicio.
5. Ataques a aplicaciones web: como el webdefacement que consiste en cambiar la apariencia del sitio web de una organización con el objetivo de repercutir en

su reputación. Otro tipo de ataques, como la inyección SQL o el cross-site-scripting tienen por objetivo extraer información de las bases de datos que se encuentran conectadas con la aplicación web.

6. Brecha de datos: consiste en la publicación no autorizada de información sensible, como información de usuarios o bancaria. El impacto de este tipo de ataque puede ser significativo en forma de sanciones económicas, pérdida de reputación y pérdida de confianza por parte de los clientes y socios.

La figura 14, obtenida del informe de Deloitte sobre el estado de la ciberseguridad en España en 2022 [45], muestra las amenazas de ciberseguridad más habituales a las que están sometidas las empresas:

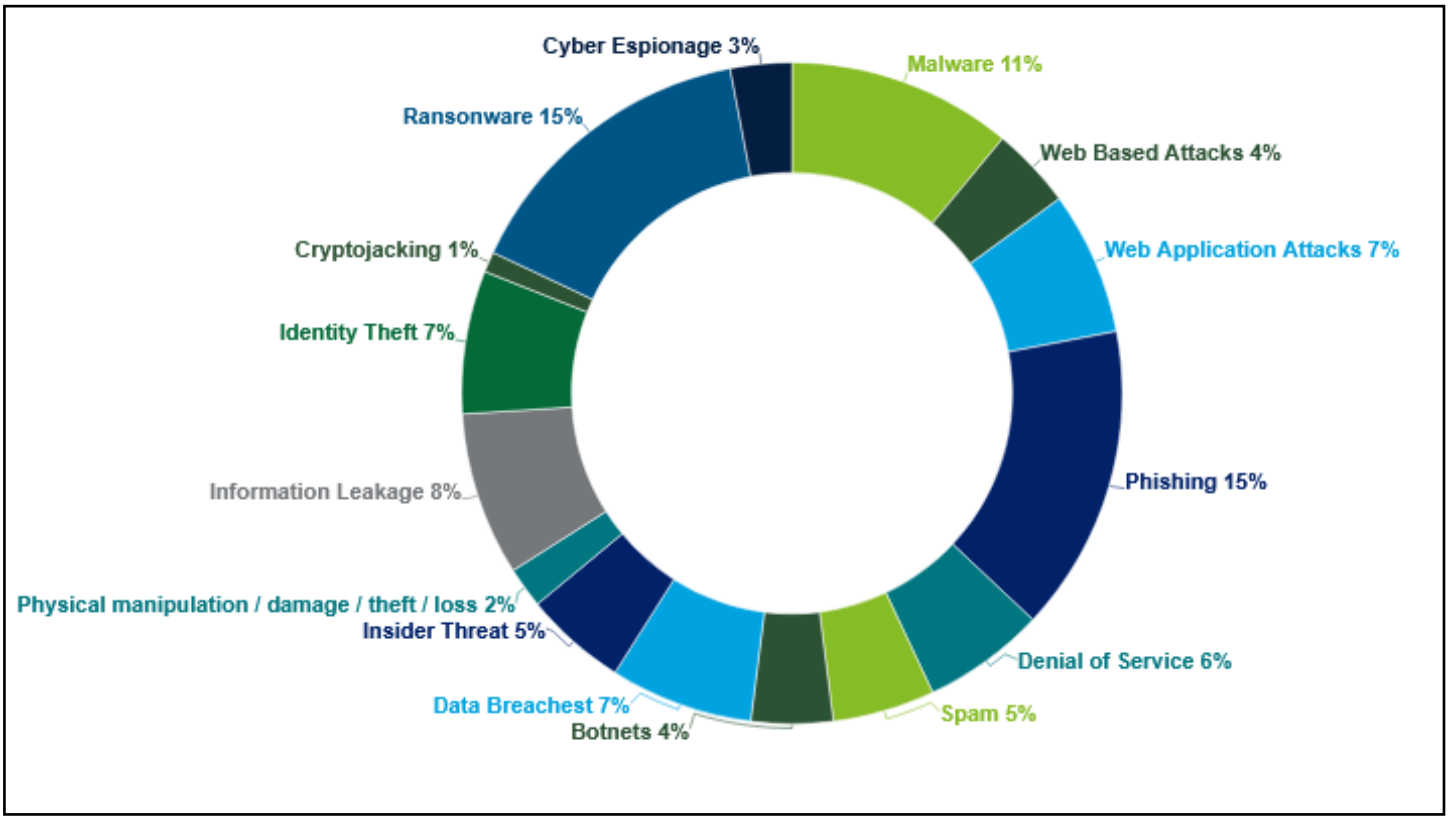

Figura 14: amenazas de ciberseguridad más habituales de las empresas españolas

3.3.2 Diseño del catálogo de servicios

Una vez han sido analizadas las principales amenazas a las que están sometidas las pymes españolas, se plantea la cartera de servicios en base a ellas. La tabla 1 muestra los servicios que proporcionará el SOC a sus clientes, en qué consisten y la justificación de su elección.

Servicio	Descripción	Justificación
Monitorización, detección y respuesta a incidentes	Es el eje central de un SOC y permite detectar y mitigar las consecuencias de un ciberataque.	Este servicio se basará en la monitorización de los eventos que tengan lugar en la infraestructura de las pymes, pudiendo detectar así ataques en tiempo real (como malware o robo de credenciales), dar una respuesta adecuada a ellos y recuperarse de las posibles consecuencias.
Detección de vulnerabilidades	Este servicio pretende escanear la infraestructura del cliente en busca de vulnerabilidades conocidas, generando un informe con sus características (descripción, prioridad etc.) y cómo pueden ser remediadas.	Las vulnerabilidades en los sistemas suponen el punto de entrada de muchos de los atacantes que sufren las pymes, tal y como se ha visto anteriormente, por lo que este servicio resulta necesario a la hora de abordar su seguridad.
Bastionado de sistemas	Junto con el análisis de vulnerabilidades, el bastionado de sistemas permite dar robustez a la infraestructura de sistemas y red y reducir así la superficie de ataque y el alcance de estos. Se realiza aplicando buenas prácticas y configurando los sistemas en base a las recomendaciones de los fabricantes.	Es un servicio que aporta gran valor a las pymes ya que, siguiendo las estadísticas, estas son un blanco fácil para sus atacantes debido a sus pocas medidas de seguridad o a las malas configuraciones de sus sistemas.

Servicio	Descripción	Justificación
Formación en ciberseguridad	Este servicio pretende concienciar y mejorar el conocimiento en ciberseguridad de los empleados de una organización.	El phishing y los ataques de ingeniería social son los ataques más empleados hoy en día para obtener acceso a los sistemas de una pyme de forma sencilla. Por lo que concienciar a los empleados a cerca de este riesgo y de cómo identificarlo y evitarlo es muy importante para reducir al máximo las posibilidades de sufrir un ataque.
Threat hunting	Parte de la hipótesis de que el cliente ya ha sido atacado, es decir, ya hay alguien dentro de sus sistemas y se hace una búsqueda proactiva para tratar de encontrar indicadores de compromiso (IOC) e indicadores de ataque (IOA) que lo demuestren.	Este servicio añade doble valor al SOC: por un lado, las amenazas cada son más sofisticadas y difíciles de detectar a través de las herramientas convencionales, por lo que el threat hunting se vuelve cada vez más demandado; por otro lado, no es un servicio muy común que ofrezcan el resto de los principales competidores, por lo que se convierte en un elemento diferenciador.
Consultoría de ciberseguridad	Proporciona asesoramiento en ciberseguridad a los clientes por parte de especialistas en la materia. Suele ser una buena opción cuándo ya existe un equipo técnico que gestiona los sistemas de la organización, pero que no es especialista en seguridad.	Va a ayudar a las pymes a mejorar su postura en ciberseguridad y minimizar su riesgo a sufrir ciberataques, mediante la identificación, evaluación y gestión de los sistemas y las redes.

Servicio	Descripción	Justificación
Cumplimiento normativo	Este servicio permite ayudar a las organizaciones a cumplir con la legislación vigente en materia de ciberseguridad.	Su implementación en las pymes es de gran importancia, ya que la gran mayoría de ellas trabaja con datos de carácter personal y no es conocedora de las elevadas sanciones a las que se somete en caso de no tratarlos adecuadamente.

Tabla 1: cartera de servicios del SOC propuesto

La cartera de servicios planteada no es muy extensa, pero se encuentra orientada y diseñada siguiendo las necesidades de las pymes, por lo que no habrá servicios que no aporten valor a los clientes o encarezcan el precio del SOC, de forma que podrá ser fácilmente asumida por las pequeñas y medianas empresas españolas.

3.4 Selección de los recursos hardware y software necesarios

Para llevar a cabo los servicios seleccionados, el personal del SOC necesitará unos recursos hardware y software que se detallaran en los siguientes subapartados. Finalmente, se definirá cómo estará montada la infraestructura de red y sistemas del SOC (en la nube, on-premise o híbrida) y cómo encajan dichos recursos hardware y software dentro de ella.

3.4.1 Recursos hardware del SOC

Los recursos hardware estarán compuestos por equipos que permitan a los trabajadores del SOC llevar sus tareas a cabo:

- Ordenadores portátiles personales: para cada uno de los trabajadores del SOC.
- Teléfonos móviles: para los trabajadores, de forma que si ocurre algún incidente de seguridad se pueda contactar con la persona de guardia encargada de dar respuesta al mismo.
- 2 firewall: uno de ellos actuará como firewall de frontera (colocado entre la red de la organización y la red externa) y un segundo firewall interno que actuará como doble protección de los equipos más sensibles de la red. Generalmente, estos dos firewalls suelen ser de diferente fabricante de forma que, si existe una vulnerabilidad en uno de ellos, no afecte al otro y la red quede protegida. Rourter y switch: para enrutar el tráfico entre las diferentes redes.
- 1 servidor físico: que alojará servidores virtuales con diferentes funciones (servidor de ficheros, controlador de dominio, escáner de vulnerabilidades etc.)
- 1 cabina de discos: para almacenar información, como datos sensibles de los clientes.

3.4.2 Recursos software del SOC

Los recursos software están formados principalmente por aquellas herramientas de ciberseguridad que faciliten al equipo del SOC su trabajo. Dichas herramientas deben cumplir las siguientes características con el objetivo de proporcionar un servicio completo a los clientes:

1. Deben ser multi-tenant: es decir, deben poder soportar múltiples clientes a la vez de forma que, mediante asignación de permisos y separación lógica de datos, cada uno vea la información que le corresponde. Esto facilita las labores de trabajo del SOC, ya que tendrá una única visualización de las alertas para todos sus clientes.
2. Deben ser multi-plataforma: es decir, deben soportar los diferentes sistemas operativos del mercado (Linux, Windows y MacOS) sin presentar problemas de rendimiento o compatibilidad.

Siguiendo los requerimientos mencionados, las herramientas software de seguridad del SOC serán:

- Splunk: será la herramienta SIEM empleada por el SOC. Cumple las dos características principales mencionadas anteriormente, además de ser uno de los sistemas de gestión de eventos mejor valorados del mercado.
- CrowdStrike: será la herramienta EDR y Antivirus empleada por el SOC. Además, CrowdStrike ofrece capacidades de respuesta a incidentes, como la conexión en tiempo real a los dispositivos o el aislamiento de red. Es multi-tenant y multi-plataforma, líder en el mercado y ofrece buen soporte técnico en caso de que suceda algún problema.
- ServiceNow: será la herramienta de gestión de tickets empleada por el SOC y el punto principal de gestión de alertas y de comunicación de incidentes con los clientes. Permite la integración con el resto de las herramientas seleccionadas.
- OpenVAS: será la herramienta de escaneo de vulnerabilidades empleada por el SOC. Es la única herramienta open source empleada, no obstante, presenta una gran fiabilidad en la detección de vulnerabilidades, por lo que hará que el precio global de los servicios de ciberseguridad sea más asumible por el cliente.

Además de las herramientas de ciberseguridad, también habrá otro tipo de software que será necesario para que el SOC desarrolle sus funciones:

- Licencias de Windows 11: una por cada ordenador personal. Licencias de Windows server 2019: que permitirán crear servidores virtuales con diferentes roles (controlador de dominio, servidor de ficheros etc.).
- FreeFileSync: permitirá realiza copias de seguridad y almacenarlas en un servidor de backup.
- Office 365: necesaria para que los miembros del SOC tengan acceso a recursos como el correo electrónico, OneDrive, etc.

3.4.3 Arquitectura de sistemas y red de la organización

La figura 15 muestra el diagrama de arquitectura de red y sistemas planteado para el SOC, y su interacción con los diferentes clientes (pymes).

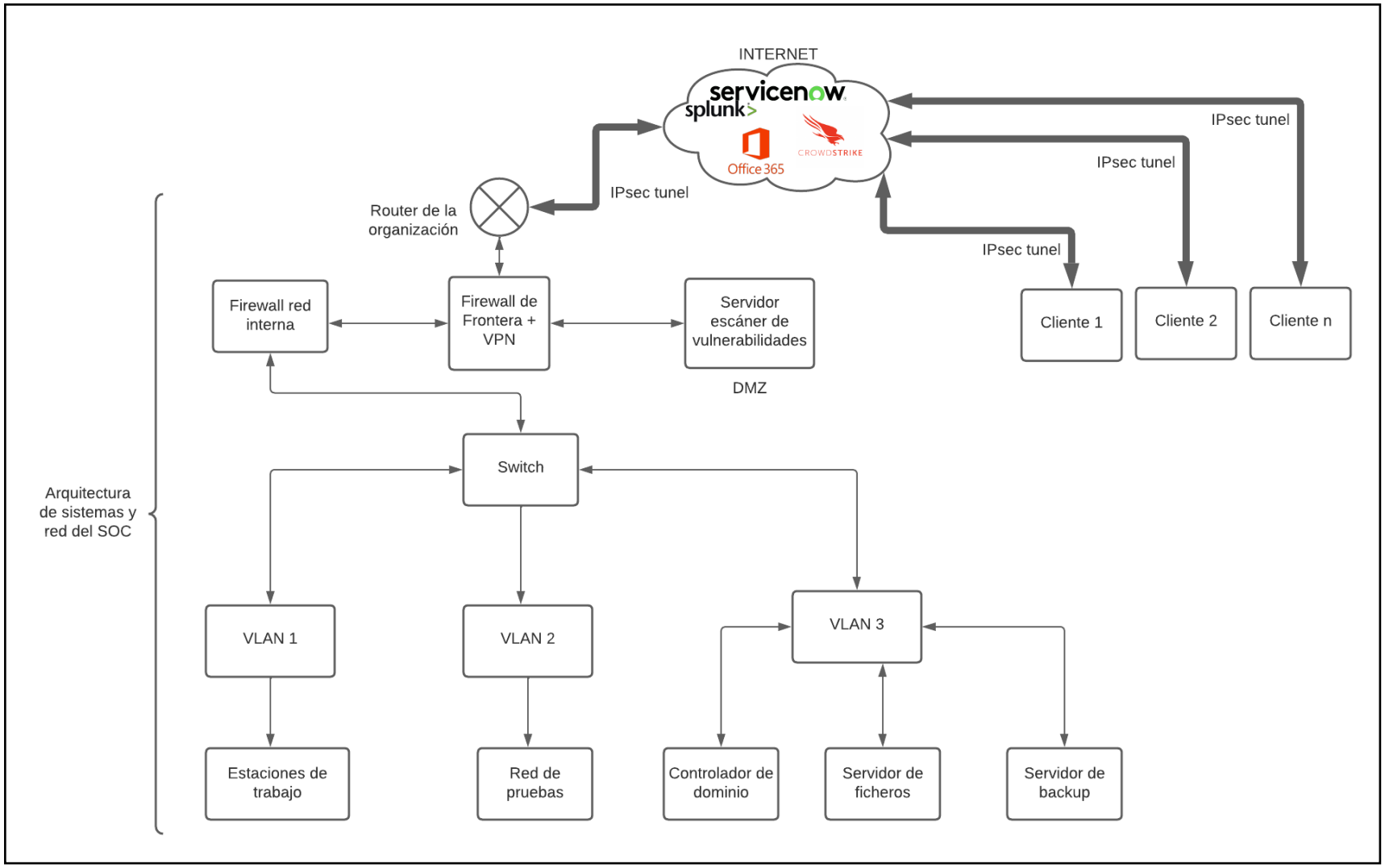

Figura 15: diagrama de red y sistemas del SOC

Tal y como se puede observar, la arquitectura que se plantea en este proyecto es híbrida, es decir, parte de ella se encontrará en el cloud y otra parte en servidores on-premise.

En concreto, aquellos servicios críticos que brindará el SOC, como la monitorización de alertas y la respuesta a incidentes (Splunk, ServiceNow y CrowdStrike) emplearán herramientas basadas en la nube, debido a:

1. Rendimiento: los datos serán procesados y almacenados en la nube de una forma más rápida, ya que las herramientas empleadas están diseñadas para ofrecer este tipo de servicio.
2. Escalabilidad: es mucho fácil redimensionar los sistemas y sus características en función de las necesidades en la nube, lo cual se adapta mejor al tipo de servicio que vende el SOC, en el que el volumen de clientes irá aumentando y fluctuando a lo largo del tiempo.
3. Ahorro de costes: se emplearán únicamente los recursos de computación y almacenamiento necesarios en cada momento, lo que se traduce en un menor precio del servicio.

Por otro lado, el SOC tendrá una infraestructura de red y sistemas propia, donde se podrá almacenar información confidencial sobre los clientes o sobre los trabajadores del propio SOC, proporcionar los servicios de escaneo de vulnerabilidades o realizar pruebas, entre otros. Esta red interna estará compuesta por:

1. Firewall de frontera: permitirá controlar el tráfico entrante y saliente entre Internet y la red del SOC. También tendrá configurada una red VPN para que los trabajadores se puedan conectar de forma remota mediante el protocolo IPsec.
2. Zona desmilitarizada (DMZ): es una red local situada entre la red del SOC e Internet. El objetivo es que las conexiones desde Internet hacia la DMZ estén permitidas, mientras que desde la DMZ hacia la red interna no. En esta red irá un servidor escáner de vulnerabilidades, que permitirá proporcionar el servicio de gestión de vulnerabilidades a los clientes. La elección de situar el servidor en este segmento de red es debido a motivos de seguridad, ya que va a tener contacto con Internet y reduce el riesgo de exposición y el tráfico de la red interna del SOC.
3. Router y switch: estos dos elementos de red permitirán enrutar el tráfico entre las diferentes redes internas y externas (router) y conectar varios dispositivos dentro de una misma red y crear VLANs (switch).
4. VLAN (Virtual Local Area Network): permite segmentar una red física en varias redes lógicas, limitando así la transmisión de datos entre los diferentes dispositivos. En el SOC se emplearán VLANs para aumentar la seguridad, descongestionar la red y controlar las conexiones entre los diferentes dispositivos de la red.
5. Túnel Ipsec: es un método seguro de establecer una conexión entre varias redes e Internet, en el que los paquetes que se envían son encapsulados y cifrados, evitando que sean capturados por terceras personas. Será empleado tanto por los clientes del SOC para enviar sus datos a las herramientas en la nube, como por el propio SOC para establecer una conexión segura (VPN).
6. Estaciones de trabajo: compuestas por los ordenadores de los trabajadores del SOC, tendrán acceso a la red interna y a Internet, lo que les permitirá utilizar

las herramientas de monitorización y gestión de alertas, así como la suite de Office365, basadas en la nube.

7. Red de pruebas: diseñada para realizar cualquier tipo de prueba que necesite llevar a cabo el personal del SOC como, por ejemplo, ver el comportamiento de un archivo malicioso. Se encontrará aislada del resto de la red, por seguridad, y solo admitirá tráfico entrante proveniente de las estaciones de trabajo.
8. Controlador de dominio: es un servidor que permitirá gestionar la autenticación de los usuarios del SOC y las directivas de seguridad. Sólo aceptará comunicaciones entrantes y salientes pertenecientes a la red interna del SOC.
9. Servidor de ficheros: para almacenar información sensible o datos de los clientes. Sólo aceptará comunicaciones entrantes y salientes pertenecientes a la red interna del SOC.
10. Servidor de backup: donde se almacenarán las copias de seguridad. Sólo aceptará comunicaciones entrantes y salientes pertenecientes a la red interna del SOC.

Las pequeñas y medianas empresas cliente y el SOC recogerán los datos generados por sus dispositivos y los enviarán, a través de Internet, a las herramientas en la nube que procesarán la información en busca de indicadores de ataque y compromiso y almacenarán aquellos eventos que puedan tener relevancia en una investigación forense. La recogida de datos en los dispositivos finales y su envío se realiza a través de un proceso que se encuentra en constante ejecución y se denomina comúnmente como “agente”.

Finalmente, cabe destacar que el diagrama de red y sistemas del SOC planteado se ha realizado siguiendo las buenas prácticas de segmentación de red, y teniendo en cuenta la seguridad y protección de los diferentes dispositivos que conforman la arquitectura [46].

3.5 Selección de los recursos humanos necesarios

El objetivo de este apartado es seleccionar los roles que formarán parte del SOC y que permitirán proporcionar los servicios a los clientes. También se definirá sus responsabilidades y papel dentro del equipo.

3.5.1. Roles y responsabilidades del SOC

La tabla 2 muestra los diferentes roles necesarios para la implementación y funcionamiento del centro de operaciones de seguridad planteado en este trabajo:

Puesto	Perfil profesional	Justificación
Project manager	Experiencia en la gestión de proyectos. Habilidades de liderazgo, gestión de equipos y colaboración. Capacidades de planificación y organización. Resolución de problemas y toma de decisiones. Gestión de riesgos y un fuerte compromiso con la entrega exitosa del proyecto.	Este rol será necesario para el proyecto que supone montar un SOC desde cero. Además, también puede encargarse de otro tipo de proyectos, como la integración de nuevos clientes.
Ingeniero de sistemas y red	Conocimientos técnicos de sistemas y redes. Experiencia en la implementación y configuración de dispositivos. Habilidades de identificación y resolución de problemas. Habilidades interpersonales y actualización continua.	Este rol será necesario para montar la infraestructura de sistemas y red propuesta en el apartado anterior y de mantenerla funcionando correctamente.
Arquitecto de seguridad	Conocimientos sólidos en seguridad de la información. Habilidades para diseñar y planificar estratégicamente los sistemas de seguridad. Experiencia en la evaluación de riesgos, gestión de vulnerabilidades, gestión de incidentes y respuesta a emergencias.	Este rol es necesario para configurar y mantener correctamente las diferentes herramientas de seguridad que empleará el SOC: SIEM, Antivirus, EDR etc.
SOC manager	Experiencia en seguridad de la información y gestión de operaciones de seguridad. Habilidades de liderazgo, gestión de equipos, planificación y organización. Actualización continua. Gran capacidad de comunicación con el resto del equipo.	Esta figura es clave para que el SOC funcione con normalidad, se encargará de asignar tareas y responsabilidades, planificar la estrategia del SOC, asumir las responsabilidades de las decisiones que se tomen en materia de seguridad y mantener las relaciones con los clientes.

Puesto	Perfil profesional	Justificación
Analista de ciberseguridad	Conocimiento de los fundamentos técnicos de la seguridad de la información (redes, sistemas, etc.). Experiencia en la monitorización y gestión de alertas. Habilidades analíticas para investigar y analizar los incidentes de seguridad. Debe estar familiarizado con las herramientas de seguridad y en continuo aprendizaje.	Habrá tres niveles de analistas de ciberseguridad, en función de su experiencia y conocimiento. El nivel 1 trabajará a turnos gestionando y categorizando las alertas de seguridad. El nivel 2 realizará una investigación en profundidad de aquellas alertas que no haya podido completar el nivel 1 y, además, llevará a cabo el servicio de escaneo de vulnerabilidades. El nivel 3 estará compuesto por expertos en ciberseguridad altamente cualificados que llevarán a cabo investigaciones complejas y el servicio de consultoría seguridad
Técnico de respuesta a incidentes y threat hunter	Experiencia en la respuesta, detección y mitigación de incidentes de seguridad. Habilidades avanzadas de análisis de datos y forense. Debe estar familiarizado con las herramientas y técnicas de respuesta a incidentes. Capacidad de trabajo en equipo y comunicación.	Permitirá cubrir el servicio de respuesta a incidentes y threat hunting del SOC.
Responsable del cumplimiento normativo	Conocimiento sólido de leyes, regulaciones y normativas. Capacidad de identificar y evaluar los riesgos legales y de establecer mecanismos para garantizar el cumplimiento continuo. Coordinación y colaboración con partes internas y externas.	Permitirá proporcionar a los clientes asesoramiento legal en materia de ciberseguridad.

Tabla 2: selección de perfiles profesionales del SOC

3.5.2. Organigrama y flujo de trabajo del SOC

La figura 16 muestra el organigrama propuesto para el SOC, teniendo en cuenta los perfiles profesionales seleccionados en el subapartado anterior:

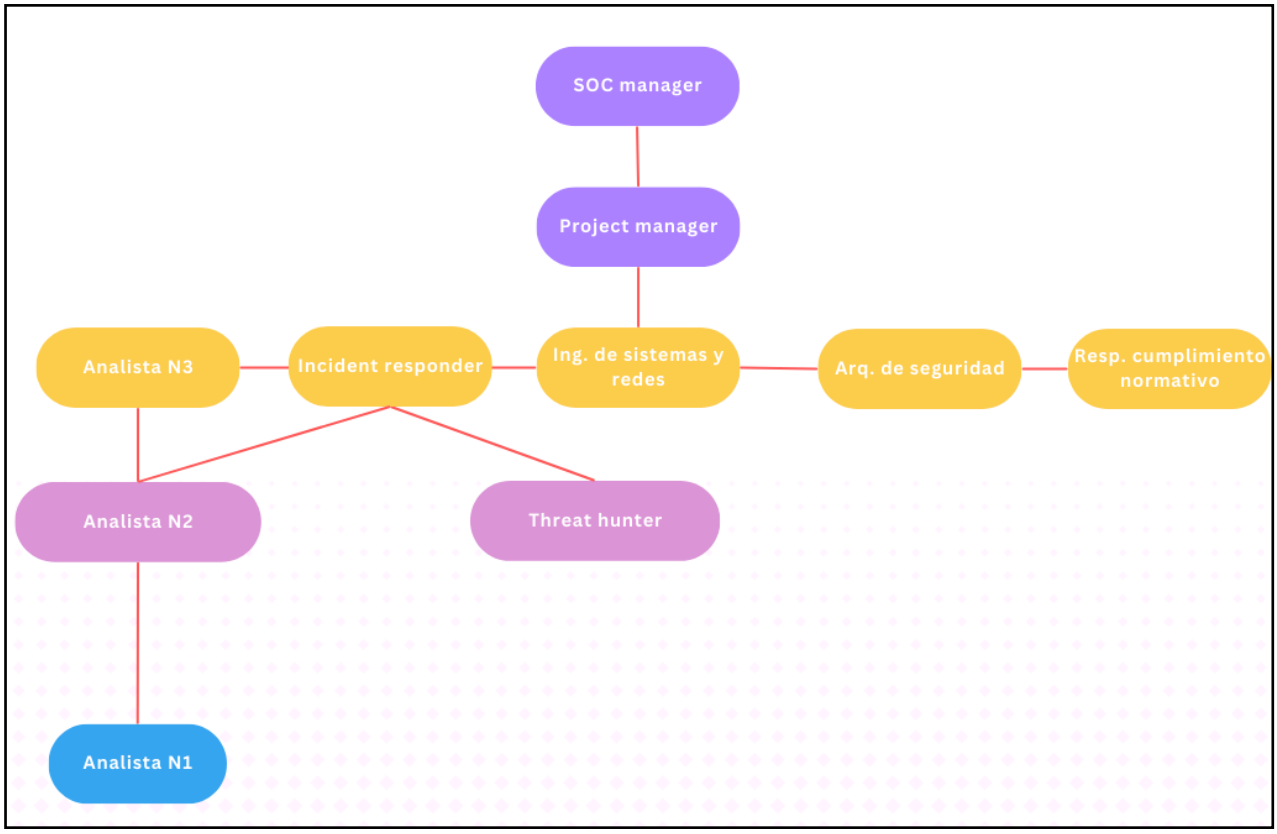

Figura 16: organigrama del SOC

Tal y como se puede observar, el SOC manager es la figura que engloba todo el equipo que forma parte del centro de operaciones, se encargará de que la comunicación fluya entre las diferentes partes, de fijar las tareas y los objetivos, de mantener las relaciones con el cliente y de conseguir la financiación necesaria para que los proyectos salgan adelante. Por debajo del SOC manager se encuentra el project manager, encargado de gestionar los proyectos del resto de personal del SOC, asegurándose de que se cumplen en tiempo y forma.

La monitorización, triage y gestión de alertas será llevada a cabo, en primer lugar, por los analistas de nivel 1. Cuando las alertas requieran un mayor nivel de especialización y conocimientos para ser resueltas, serán escaladas a los analistas de nivel 2 (también dedicados al servicio de gestión de vulnerabilidades). Si estos analistas detectan un incidente de seguridad, entrará en juego el equipo de respuesta a incidentes para aplicar medidas de contención y mitigación; si en caso contrario se necesita un mayor soporte técnico las alertas pueden ser escaladas a un nivel 3 (también dedicado al servicio de consultoría externa). Por otro lado, el threat hunter será encargado de realizar una búsqueda proactiva de amenazas empleando las herramientas de seguridad y los datos almacenados y, en caso de que encuentre alguna amenaza, también escalará las evidencias al equipo de respuesta a incidentes.

El ingeniero de sistemas y el arquitecto de seguridad se encargarán de configurar la infraestructura de sistemas, red y seguridad. También colaborarán con el equipo de analistas y de respuesta a incidentes en caso de que sea necesario tomar medidas correctivas y llevarán a cabo proyectos de integración con nuevos clientes.
Finalmente, el responsable del cumplimiento normativo se encargará de que el propio SOC cumpla con la legislación vigente y proporcionará este mismo servicio a los clientes.

3.6 Funcionamiento del SOC

El tipo de SOC planteado en este trabajo será distribuido, por lo tanto, el personal y las responsabilidades de seguridad estarán repartidas geográficamente en el territorio español. Debido a los siguientes motivos:

1. Escalabilidad: conforme el centro de operaciones de seguridad vaya creciendo y se necesiten más profesionales, será más fácil encontrar talento si se amplía la zona geográfica.
2. Teletrabajo: estará diseñado para permitir el trabajo en remoto, salvo en aquellos casos en los que sea necesario desplazarse hasta el centro de datos en el que se encuentre localizado la red interna del SOC (para realizar labores de mantenimiento). Esto permitirá cumplir con los objetivos de desarrollo sostenible marcados en el capítulo 1 de este trabajo.
3. Cercanía con los clientes: si el objetivo es proporcionar servicios de ciberseguridad a pymes españolas, tener un equipo distribuido geográficamente ayuda a que pueda haber algún miembro del SOC que se encuentre cerca del cliente.

La gestión del servicio del SOC se realizará siguiendo las buenas prácticas propuestas en ITIL v4 [47]. Entre los principios de esta guía se encuentran el enfoque en el valor, el avance iterativo, la colaboración o la automatización. La figura 17 presenta el modelo de gestión de ITIL, basado en las 4 dimensiones: organización y personas, información y tecnología, socios y proveedores y flujos de valor y procesos.

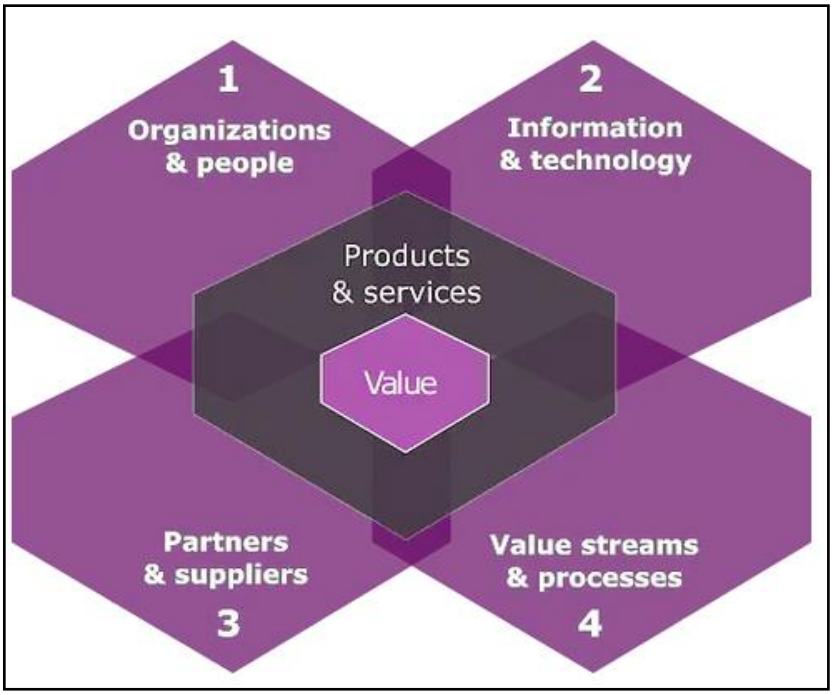

Figura 17: modelo de gestión de servicios de ITIL

Para aplicar estas buenas prácticas, las tareas, incidentes y cambios que reciba el SOC serán categorizadas y resueltas en función de su prioridad:

- En planificación: actividad sin urgencia asociada.
- Prioridad baja: actividad con una fecha límite próxima, pero con un horario flexible.
- Prioridad media: actividad con una fecha límite próxima pero no inmediata.
- Prioridad alta: actividad con una fecha límite próxima e inmediata.
- Prioridad crítica: actividad con una fecha límite próxima que requiere una acción inmediata.

Los tiempos de respuesta a cada una de estas prioridades pueden estar fijados en un acuerdo a nivel de servicio (SLA) con el cliente, basándose en sus necesidades. Se identificarán tres tiempos de respuesta diferentes:

1. Tiempo de resolución de alertas: es el tiempo transcurrido entre que el SOC recibe una alerta generada por alguna de las herramientas de seguridad y cataloga dicha alerta como falso positivo, verdadero positivo o positivo benigno.
2. Tiempo de notificación de incidentes: es el tiempo transcurrido entre que el SOC detecta que se ha producido un incidente de seguridad en la infraestructura del cliente y se lo comunica a este. El canal de comunicación (email, llamada telefónica etc.) será especificado por el cliente.
3. Tiempo de inicio de respuesta a incidentes: es el tiempo transcurrido entre que el SOC detecta un incidente de seguridad en la infraestructura del cliente y comienza a trabajar en su resolución.

Finalmente, el SOC brindará dos tipos de servicio a sus clientes, con sus tiempos de respuesta por defecto, los cuales serán detallados en los siguientes subapartados: servicio 24x7 y servicio 8x5.

3.6.1 Servicio 24x7

Es el tipo de servicio más común que ofrece un SOC, en él se monitorizan y analizan las alertas de seguridad en tiempo real y se responde a los incidentes críticos las 24 horas del día y los 7 días de la semana. Requiere de personal trabajando a turnos para gestionar las alertas y de especialistas de guardia en caso de que ocurra algún incidente.
La figura 18 muestra los tiempos de respuesta por defecto que se le aplicarían a los clientes del SOC en función de la prioridad de las alertas. En ella se especifica, para cada tipo de prioridad, el tiempo por defecto de resolución de una tarea, el horario en que el tiempo de resolución va a contar y la periodicidad con la que se actualizará la situación al cliente.

	Prioridad	Tiempo de actualización del estado al cliente	Horas de trabajo	Tiempo por defecto
Tiempo de resolución de las alertas	Crítica	Comunicación inicial y actualizaciones según requiera el cliente	24x7	4 horas o menos
	Alta	Comunicación inicial y actualizaciones según requiera el cliente	24x7	8 horas o menos
	Media	Bajo demanda del cliente o según vea conveniente el SOC	horario laboral	1,5 días laborales
	Baja	Bajo demanda del cliente o según vea conveniente el SOC	horario laboral	3 días laborales
	Planificación	Bajo demanda del cliente o según vea conveniente el SOC	horario laboral	5 días laborales
Tiempo de notificación de incidentes	Crítica	Comunicación inicial y actualizaciones según requiera el cliente	24x7	1 hora
	Alta	Comunicación inicial y actualizaciones según requiera el cliente	24x7	4 horas o menos
	Media	Bajo demanda del cliente o según vea conveniente el SOC	24x7	8 horas o menos
	Baja	Bajo demanda del cliente o según vea conveniente el SOC	horario laboral	1 día laboral
	Planificación	Bajo demanda del cliente o según vea conveniente el SOC	horario laboral	3 días laborales
Tiempo de inicio de respuesta a incidentes	Crítica	Comunicación inicial y actualizaciones según requiera el cliente	24x7	15 minutos
	Alta	Comunicación inicial y actualizaciones según requiera el cliente	24x7	30 minutos
	Media	Bajo demanda del cliente o según vea conveniente el SOC	24x7	2 horas
	Baja	Bajo demanda del cliente o según vea conveniente el SOC	horario laboral	2 días laborales
	Planificación	Bajo demanda del cliente o según vea conveniente el SOC	horario laboral	5 días laborales

Figura 18: tiempos de respuesta del SOC en el servicio 24x7

Aclaración, entiéndase por horario laboral un turno de trabajo de lunes a viernes y de 8:00 a 17:00.

3.6.2 Servicio 8x5

En el servicio 8x5 se realiza una monitorización y gestión de las alertas e incidentes de seguridad únicamente en horario laboral. Este servicio es apto para aquellas empresas pequeñas que generen pocos eventos de seguridad o que cuenten con un presupuesto muy reducido. La figura 19 muestra los tiempos de respuesta por defecto para este tipo de servicio:

	Prioridad	Tiempo de actualización del estado al cliente	Horas de trabajo	Tiempo por defecto
Tiempo de resolución de las alertas	Crítica	Comunicación inicial y actualizaciones según requiera el cliente	horario laboral	4 horas o menos
	Alta	Comunicación inicial y actualizaciones según requiera el cliente	horario laboral	8 horas o menos
	Media	Bajo demanda del cliente o según vea conveniente el SOC	horario laboral	1,5 días laborales
	Baja	Bajo demanda del cliente o según vea conveniente el SOC	horario laboral	3 días laborales
	Planificación	Bajo demanda del cliente o según vea conveniente el SOC	horario laboral	5 días laborales
Tiempo de notificación de incidentes	Crítica	Comunicación inicial y actualizaciones según requiera el cliente	horario laboral	1 hora o menos
	Alta	Comunicación inicial y actualizaciones según requiera el cliente	horario laboral	4 horas o menos
	Media	Bajo demanda del cliente o según vea conveniente el SOC	horario laboral	8 días laborales
	Baja	Bajo demanda del cliente o según vea conveniente el SOC	horario laboral	1 día laboral
	Planificación	Bajo demanda del cliente o según vea conveniente el SOC	horario laboral	3 días laborales
Tiempo de inicio de respuesta a incidentes	Crítica	Comunicación inicial y actualizaciones según requiera el cliente	horario laboral	15 minutos
	Alta	Comunicación inicial y actualizaciones según requiera el cliente	horario laboral	30 minutos
	Media	Bajo demanda del cliente o según vea conveniente el SOC	horario laboral	2 horas
	Baja	Bajo demanda del cliente o según vea conveniente el SOC	horario laboral	2 días laborales
	Planificación	Bajo demanda del cliente o según vea conveniente el SOC	horario laboral	5 días laborales

Figura 19: tiempos de respuesta del SOC en el servicio 8x5

3.7 Fases de desarrollo del SOC

Para llegar a proporcionar los servicios del SOC de una manera eficiente, es necesario tener en cuenta que existen diferentes fases en el desarrollo de este: desde el diseño de la arquitectura de seguridad y la contratación de personal, hasta la operación de un SOC maduro que incluya todos los servicios seleccionados anteriormente.
La figura 20 representa un cuadro resumen de cada una de las fases que van a conformar el desarrollo del SOC planteado en este trabajo, así como los recursos y tiempo necesarios, cada una de ellas será estudiada con detenimiento en los siguientes subapartados. Para definir estas fases se ha hecho uso de la metodología propuesta por ENISA [28], adaptándola a las necesidades del proyecto.

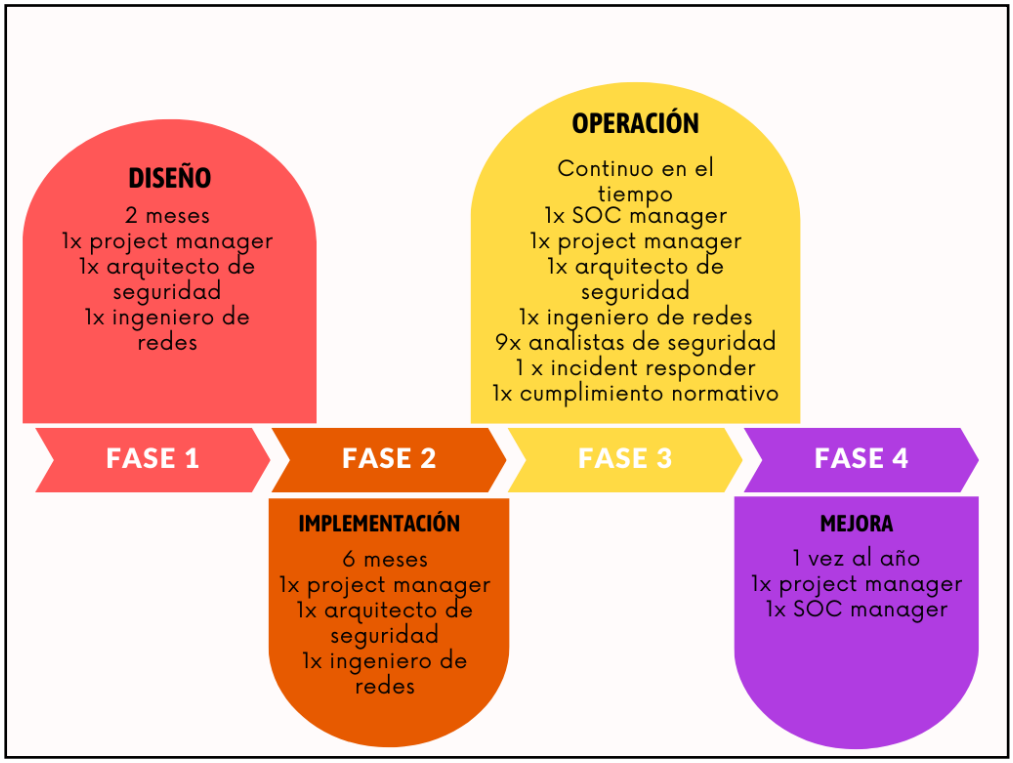

Figura 20: cuadro resumen de las fases de implementación del SOC

3.7.1 Diseño del SOC

Durante esta fase se diseñará la arquitectura de sistemas y red del SOC, la cartera de servicios en base a los potenciales clientes y cómo se van a integrar las herramientas de seguridad en la infraestructura de los clientes. También se crearán guías técnicas sobre el funcionamiento de los sistemas y las buenas prácticas de seguridad que se deben implementar.
Se estima que esta primera fase va a durar 2 meses aproximadamente y los recursos humanos para llevarla a cabo son:

- Ingeniero de sistemas y red: será el encargado de diseñar la infraestructura de sistemas y red de la organización, tanto en la nube como on-premise. Deberá crear documentación técnica teniendo en cuenta factores como la configuración de los sistemas operativos, la elección de los diferentes sistemas o la comunicación entre ellos. El trabajo desarrollado por esta persona ocupará el 25% del tiempo estimado para la fase de diseño.
- Arquitecto de seguridad: será el encargado de seleccionar las mejores herramientas de seguridad que empleará el SOC, así como de preparar guías técnicas sobre su configuración e integración con la infraestructura. También diseñará políticas de seguridad base y fijará las buenas prácticas que deben seguirse para que la infraestructura del SOC sea lo más robusta posible. El trabajo desarrollado por esta persona ocupará el 25% del tiempo estimado para la fase de diseño.
- Project manager: será el encargado de planificar la implementación del SOC en base a las tareas definidas por el ingeniero de sistemas y red y el arquitecto de seguridad. Su rol es de gran importancia para que el proyecto sea existoso, tendrá que asignar los recursos de forma que se cumplan las expectativas de tiempo y calidad. El trabajo desarrollado por esta persona ocupará el 50% del tiempo estimado para la fase de diseño.

El objetivo de la fase de diseño es crear planes detallados del funcionamiento del SOC, que serán empleados en la siguiente fase de implementación. Nótese que esta fase de diseño ya se ha llevado a cabo en los apartados previos de este trabajo.

3.7.2 Implementación del SOC

Durante esta fase se pondrá en marcha el centro de operaciones de seguridad y se llevarán a cabo los planes definidos en la fase previa. Los objetivos que se persiguen en esta fase son la implementación de los servicios del SOC, la preparación de procedimientos detallados y la creación de un equipo sólido. Algunas de las tareas que deben llevarse a cabo son:

- Implementación de la infraestructura del SOC.
- Creación de relaciones contractuales con los proveedores, partes interesadas y socios.
- Implantación de procedimientos de gestión de la seguridad informática
- Desarrollo de un plan de formación para los integrantes del SOC
- Aprobación y puesta en marcha de la estructura organizativa.
- Comunicación de la puesta en marcha del nuevo SOC, así como de los servicios que ofrece.

Se estima que esta primera fase va a durar 6 meses aproximadamente y los recursos humanos para llevarla a cabo son:

- Project manager: es una figura esencial durante todas las fases del SOC, ya que tendrá la responsabilidad de coordinar al resto del personal para que las tareas se cumplan en tiempo y forma. El trabajo desarrollado por esta persona ocupará el 25% del tiempo estimado para la fase de diseño.
- Ingeniero de sistemas y red: se encargará de desplegar los sistemas seleccionados en la fase anterior y de configurarlos correctamente. El trabajo desarrollado por esta persona ocupará el 50% del tiempo estimado para la fase de diseño, esto es debido a que la infraestructura de sistemas y red es extensa e híbrida por lo que su configuración implica más horas de trabajo.
- Arquitecto de seguridad: se encargará de configurar y poner a punto las diferentes herramientas de seguridad para dar servicio a los clientes y de llegar a acuerdos con los proveedores y socios. También desarrollará los planes de formación y realizará entrevistas técnicas para seleccionar el resto de los miembros del SOC. El trabajo desarrollado por esta persona ocupará el 25% del tiempo estimado para la fase de diseño.

Al final de la fase de implementación el SOC estará listo para comenzar a brindar sus servicios básicos, y comenzará la fase de operación.

3.7.3 Operación del SOC

El objetivo de esta fase es que el SOC opere de forma de forma eficiente y efectiva, proporcionando a los clientes los servicios seleccionados. Para ello, se deben llevar a cabo las siguientes tareas:

- Revisión anual del rendimiento: para celebrar los éxitos que se han logrado y remarcar las áreas de mejora.
- Recolección de ideas de mejora: las mejoras propuestas por las partes interesadas y el equipo del SOC serán puestas en común y analizadas para perfeccionar el servicio.
- Aprobación del presupuesto anual: el cual determinará los proyectos e iniciativas que van a poder llevarse a cabo a lo largo del año. Debe estar sujeto a la normativa vigente.
- Revisión periódica de las necesidades de las partes interesadas: dónde se presente el desempeño del centro de operaciones y se traten las expectativas y necesidades de las partes interesadas.
- Medición mensual de KPIs (indicadores clave de rendimiento): empleados para medir el rendimiento de la monitorización y respuesta a incidentes, están vinculados a cada servicio y se pueden usar con fines estadísticos o para implementar mejoras. Algunos de los KPIs que se emplearán en el SOC son:
    - Tiempo de respuesta a incidentes: permite medir el tiempo que el SOC tarda en detectar, analizar y responder ante un incidente de seguridad. Mide la eficacia en la respuesta a incidentes.
    - Porcentaje de detección de amenazas: permite medir la tasa de detección de amenazas por parte del SOC y se puede emplear para evaluar la eficiencia de las herramientas de seguridad.

- Número de incidentes de seguridad resueltos: permite medir el número de incidentes resueltos por el SOC en un determinado periodo de tiempo. Se puede emplear también para medir la eficiencia del SOC en la gestión de incidentes de seguridad.
- Porcentaje de falsos positivos: permite medir el número de falsos positivos detectados por las herramientas de seguridad. También se puede emplear para medir la eficacia y calidad de los sistemas de seguridad.

- Revisión periódica de los recursos humanos del SOC: conforme el centro de operaciones vaya creciendo, es decir, vaya dando servicio a más clientes, será necesario revisar el equipo y los roles en busca de nuevos integrantes. También ocurrirá de forma contraria, si disminuye la carga de trabajo será necesario reorganizar el equipo.

Esta fase de operación no tiene una duración estimada, si no que se alargará en el tiempo mientras el SOC preste sus servicios. No obstante, es necesario tener en cuenta la madurez del centro de operaciones de seguridad, entendiéndose ésta por los recursos disponibles, el número de clientes, los procedimientos implementados, el rendimiento y la solidez de las relaciones establecidas con las partes interesadas. En un centro de operaciones de seguridad el objetivo principal es el de brindar los servicios de monitorización y respuesta ante incidentes de seguridad (servicios básicos), posteriormente si existe la suficiente madurez se le pueden añadir otro tipo de servicios que aporten valor (servicios avanzados). De esta forma, y siguiendo las recomendaciones del informe [9], la figura 21 identifica la tabla de servicios básicos y avanzados del SOC propuesto:

Servicio	Servicio básico	Servicio avanzado
Monitorización, detección y respuesta a incidentes	B	
Formación en ciberseguridad		A
Detección de vulnerabilidades	B	
Bastionado de sistemas		A
Threat hunting		A
Consultoría de ciberseguridad	B	
Cumplimiento normativo		A

Figura 21: categorización de servicios básicos y avanzados del SOC

En una primera fase, se implementarán aquellos servicios considerados como básicos y, cuándo el SOC haya alcanzado su madurez, se implementarán el resto de los servicios avanzados. El tiempo que transcurrirá hasta que el SOC alcance su madurez y brinde todos los servicios planteados dependerá de múltiples factores, no obstante, el objetivo será alcanzar este estado tras un año de su puesta en marcha.

Los perfiles necesarios para iniciar esta fase se muestran a continuación, aunque estos pueden cambiar conforme el centro de operaciones vaya creciendo:

- Analistas de ciberseguridad: se encargarán de monitorizar y analizar las alertas de seguridad 24/7 y trabajarán a turnos. Existirán tres niveles de especialización, nivel 1, nivel 2 y nivel 3. Los niveles superiores también se encargarán de proporcionar los servicios de consultoría, formación en ciberseguridad y escaneo de vulnerabilidades. El número de analistas de

ciberseguridad necesarios dependerá del número de clientes, usuarios, dispositivos, alertas etc., lo normal es comenzar con 7 analistas de nivel 1, 1 analista de nivel 2 y 1 analista de nivel 3. que permitan cubrir la rotación de 24/7 e irán aumentando según las necesidades del negocio. Este rol cubrirá gran parte de los servicios básicos, por lo que estará presente desde el inicio del SOC.

- Incident responder y threat hunter: será el encargado de responder, coordinar y mitigar los incidentes de seguridad, así como de documentar todo el proceso y las lecciones aprendidas. También será encargado de realizar búsquedas de amenazas proactivas en los sistemas de los clientes. Esto rol cubrirá uno de los servicios básicos, por lo que estará presente desde el inicio del SOC. Se comenzará con 1 persona que cubra estas funciones y se irán incorporando nuevos perfiles según vaya siendo necesario.
- Responsable de cumplimiento normativo: será el encargado de proporcionar el servicio de cumplimiento normativo y contará con conocimiento en legislación. Este rol cubre un servicio avanzado, por lo que será incluido una vez el SOC alcance su madurez.
- Arquitecto de seguridad: encargado de mantener y configurar las herramientas de seguridad, tanto para el SOC como para los clientes. Una persona cubrirá este rol desde el inicio de la creación del SOC.
- SOC manager: será el responsable de coordinar el equipo que conforma el SOC y mantener las relaciones con el cliente, de forma que se proporcione un servicio de calidad. Este rol será cubierto por 1 persona desde el inicio de la creación del SOC.
- Project manager: la labor de este perfil será necesaria para gestionar aquellos proyectos relacionados con la integración de nuevos clientes al SOC, así como las posibles mejoras que se puedan realizar. Una persona cubrirá este rol desde el inicio de la creación del SOC.
- Ingeniero de sistemas y redes: encargado de mantener la infraestructura de redes y sistemas (on premise y cloud) funcionando correctamente y cumpliendo con medidas de seguridad como las actualizaciones periódicas. También será el encargado de proporcionar el servicio de bastionado de sistemas. Una persona cubrirá este rol.

3.7.4 Mejora continua del servicio

Esta última fase se centra en seleccionar y aprobar iniciativas que permitan mejorar el centro de operaciones de seguridad y su madurez. Se trata de un proceso continuo, en el que se diseñan, implementan y ponen en marcha las diferentes iniciativas. Los objetivos que se persiguen son:

1. Obtener una lista detallada con las iniciativas de mejora y priorizar aquellas que tengan mayor relevancia para el SOC.
2. Diseñar planes detallados para llevar a cabo cada una de las iniciativas. Deben detallarse los requisitos, expectativas, objetivos y planes de implementación.
3. Obtener un presupuesto que permita poner en marcha dichas iniciativas y cubrir los costes asociados de personal, instalaciones, tecnología etc.

Se espera que esta fase tenga una duración de un mes al año y se realice mientras el SOC continúe operativo. Para llevarla a cabo los perfiles necesarios serán:

- SOC manager: tomará las iniciativas propuestas por el resto del equipo y las partes interesadas y las priorizará. También se encargará de conseguir el presupuesto necesario para llevarlas a cabo.
- Project manager: se encargará asignar el tiempo y recursos necesarios a cada una de las iniciativas y asegurarse de que se cumplen los objetivos.

3.8 Externalización y subcontratación de servicios

El SOC que se plantea en este trabajo está únicamente orientado a dar servicios de ciberseguridad a sus clientes. No obstante, existen muchos otros procesos inherentes a la gestión de una empresa, los cuales serán subcontratados. Algunos de estos procesos son:

- Gestión de recursos humanos: para llevar a cabo temas laborales como el proceso de nóminas, la creación de contratos o la contratación de personal. Será un servicio del que se hará uso de forma continuada.
- Gestión económica y financiera: para llevar a cabo todos los trámites económicos, como el pago a proveedores o el cobro a los clientes y empleados, además de para mantener una buena salud financiera de la empresa cumpliendo con la normativa vigente. También será un servicio del que se hará uso de forma continuada.
- Marketing: para dar a conocer el SOC y los servicios que oferta a través de página web, redes sociales o eventos. Este servicio se contratará bajo demanda en determinados periodos en los que se considere necesario, como tras la etapa de implementación del SOC.
- Captación de talento: para encontrar personal que se ajuste a las posiciones necesarias del SOC. También será un servicio que se requerirá en situaciones puntuales, cuando sea necesario incluir uno o varios miembros al equipo.

Algunas de las ventajas que ofrece al SOC externalizar este tipo de servicios son:

1. Reducción de costes: ya que implica no tener que contratar personal y pagar los gastos asociados a su contratación y capacitación. Además, como el SOC parte desde cero, especialmente en las etapas iniciales, no será necesario destinar un recurso completo a cubrir este tipo de servicios.
2. Flexibilidad: es posible aumentar o disminuir el alcance de los servicios según las necesidades.
3. Mayor enfoque en el negocio principal: permite al SOC enfocarse en su actividad principal, que es la de brindar servicios de ciberseguridad a sus clientes, centrándose en su crecimiento y calidad.

3.9 Análisis de riesgos del SOC

El objetivo de este apartado es analizar los riesgos a los que está sometido el proyecto de creación e implementación de un SOC, y que pueden provocar el fracaso o el retraso en el desarrollo de este. Para ello, la siguiente tabla identifica cada uno de los riesgos, el impacto que tiene sobre el proyecto, la probabilidad de que ocurra (en %) y las medidas que se pueden tomar para mitigarlo [49].

Riesgo	**Impacto**	**Probabilidad de que ocurra (%)**	**Mitigación**
Problemas en la obtención de financiación en alguna de las fases	Medio, supondría un retraso en el avance de los proyectos	30	Encontrar varias fuentes de financiación (no depender sólo de una)
Falta de personal cualificado, debido a la gran demanda del mercado y a la escasez de oferta	Medio, supondría un retraso en el lanzamiento de nuevos proyectos	60	Se ofrecerán salarios competitivos y diferentes beneficios sociales, como un plan de formación.
Sufrir una fuga de datos	Alto, afectaría gravemente a la reputación del SOC y a su capacidad para detectar ciberataques	20	Se aplicarán las medidas de seguridad oportunas para que los sistemas de información del SOC estén protegidos (parcheo, uso de buenas prácticas etc). Además, se monitorizarán y gestionarán los incidentes junto con el resto de los clientes. Se realizarán copias de seguridad de la información.

Riesgo	Impacto	Probabilidad de que ocurra (%)	Mitigación
Caídas en el servicio de la red interna del SOC (Internet, electricidad, fallos en los sistemas)	Medio, afectaría a alguno de los servicios avanzados del SOC y a la disponibilidad de la información almacenada	70	Se aplicará redundancia en los sistemas, de forma que si alguno falla se ponga en marcha automáticamente el otro. Se revisarán los acuerdos a nivel de servicio con el proveedor de Internet para asegurar que la conexión es fiable. Se instalarán sistemas de alimentación ininterrumpida (SAI) para asegurar que los sistemas no se quedan sin electricidad.
Caídas en algunos de los servicios contratados en la nube	Alto, afectaría a los servicios básicos del SOC como la monitorización y gestión de alertas en tiempo real	10	Los servicios en la nube están especialmente diseñados para tener una alta disponibilidad. No obstante, se revisarán los acuerdos a nivel de servicio con los proveedores para asegurarse de que cumplen con los requerimientos del servicio.
Mala planificación en alguna de las fases en las que se divide la implementación del SOC	Medio, supondría un retraso en el avance de los proyectos	50	Contar con una persona con experiencia y formación en la gestión de proyectos (Project manager), que controle que cada uno de ellos se lleva a cabo en tiempo y forma.

Riesgo	Impacto	Probabilidad de que ocurra (%)	Mitigación
Sufrir un ciberataque	Alto, afectaría gravemente a la reputación del SOC y a su capacidad para detectar y mitigar ciberataques	60	Se monitorizarán y gestionarán los incidentes de seguridad de la misma forma que con el resto de los clientes. También se implementarán políticas de seguridad preventivas y se concienciará a los empleados en materia de ciberseguridad.
Fallos en la configuración de las herramientas de seguridad	Medio, afectaría a la capacidad de estas herramientas para detectar y responder de manera correcta a los ataques. Esto permitiría a los atacantes permanecer más tiempo en los sistemas y causar un mayor daño, además de causar una pérdida de reputación de cara a los clientes	40	Implementando procesos de mejora continua que revisen la configuración de las herramientas y sigan las buenas prácticas recomendadas por los proveedores. Realizando pruebas de penetración en los sistemas que permitan determinar si son correctamente detectadas por las herramientas.
Amenazas internas (referidas a empleados con elevados privilegios que comprometan la seguridad de los sistemas en su propio beneficio)	Alto, puede permitir la entrada deliberada a atacantes o extraer información confidencial	10	Estableciendo políticas y controles de acceso. Asignando los mínimos privilegios necesarios para realizar el trabajo.

Riesgo	Impacto	Probabilidad de que ocurra (%)	Mitigación
Incumplimiento de una alguna ley o regulación aplicable al SOC	Medio, afectaría a la reputación del SOC para proporcionar servicios de cumplimiento normativo. También es posible que el incumplimiento venga acompañado de sanciones que afectarían económicamente al negocio.	40	Mediante la contratación de un experto en la legislación vigente, evaluaciones periódicas de los requisitos legales y regulatorios y la implementación de políticas y medidas.
Problemas en la comunicación y colaboración del equipo (el personal del SOC no se integra de manera efectiva)	Medio, puede repercutir en la calidad del servicio que se preste a los clientes	30	Mediante la definición de roles y responsabilidades claras, el uso de herramientas de colaboración y el establecimiento de protocolos de comunicación. En esta situación, la figura del SOC manager es muy importante para que el equipo esté alineado con los objetivos del centro de operaciones.

Tabla 3: análisis de riesgos del proyecto de creación de un SOC

4. Conclusiones y trabajos futuros

El objetivo de este último capítulo es realizar un análisis sobre los resultados obtenidos, las conclusiones a las que se ha llegado y fijar las líneas futuras de trabajo que no han podido ser exploradas en este documento.

4.1 Conclusiones del trabajo

La conclusión más importante extraída tras la realización de este trabajo es la complejidad que supone proveer un servicio de ciberseguridad a una o varias organizaciones. Esto es debido a que el panorama de la seguridad informática es muy cambiante, aparecen y desaparecen amenazas, y las tácticas y técnicas que emplean los ciberatacantes cada vez son más avanzadas. Por otro lado, las herramientas de detección y los algoritmos de emplean también van evolucionando, quedándose muchas de ellas obsoletas en poco tiempo. Además, las necesidades en ciberseguridad pueden ser muy diferentes dependiendo de la organización de la que se trate. Todas estas cuestiones hacen que las empresas dedicadas a la ciberseguridad tengan que revisar periódicamente su cartera de servicios y su misión.
Por otro lado, diseñar un centro de operaciones de seguridad (SOC) desde cero también ha supuesto un reto, en él se han debido de tener en cuenta todo un entramado de personas, procesos y tecnologías. Como conclusión, en el diseño de un SOC es muy importante fijar desde un inicio los objetivos y los potenciales clientes a los que se va a brindar servicio, orientando así todos los esfuerzos en una misma dirección y evitando la pérdida de tiempo y recursos innecesaria. También se ha visto que un SOC ha de pasar por diferentes fases hasta alcanzar su madurez, desde el diseño inicial hasta la puesta en marcha de sus servicios más avanzados, respetando el tiempo de duración de cada una de ellas y el personal involucrado.
Finalmente, y tras los estudios realizados en el presente trabajo, resulta necesario remarcar la necesidad que tienen las pequeñas y medianas empresas españolas de protegerse en materia de ciberseguridad. Tal y como se ha visto, son el blanco más fácil para los atacantes, ya que cuentan con mínimas o inexistentes medidas de seguridad, que hacen que puedan ser atacadas con muy poco esfuerzo. Además, también se les suma un presupuesto muy reducido y la desinformación por parte de sus responsables de las consecuencias que pueda tener sobre su negocio no proteger adecuadamente la información. Por otro lado, las empresas que brindan servicios de ciberseguridad actualmente en España todavía tienen un largo camino para adecuar sus servicios a las necesidades y características de las pymes.

4.2 Análisis del trabajo desarrollado

El resultado del trabajo desarrollado ha sido positivo ya que la propuesta de SOC planteada tiene robustez: está orientada a un nicho de mercado concreto, empleando las herramientas de software de seguridad mejor valoradas en la actualidad y diseñando una cartera de servicios en base al panorama actual de ciberamenazas.
Tras el desarrollo del proyecto, se han logrado alcanzar todos los objetivos planteados inicialmente en el apartado 1.2 de este trabajo: conocer el funcionamiento a fondo de

un SOC y desarrollar teóricamente la implantación de un centro de operaciones de ciberseguridad que dará servicio a pequeñas y medianas empresas.
Respecto a la planificación, se ha seguido un enfoque basado en pruebas de evaluación continua (PECs) donde el objetivo en cada una de las entregas era completar uno de los cuatro capítulos en los que se dividía el trabajo. La metodología seguida basada en la entrega de un producto mínimo viable y el uso de metodologías ágiles ha sido satisfactoria, ya que se ha logrado completar el proyecto en el tiempo y formas previstas.
Por otro lado, cabe destacar que las tareas propuestas dentro de cada una de las entregas, mostradas en la figura 2, han ido cambiando sustancialmente conforme el trabajo se ha ido desarrollando y se ha estudiado en profundidad el funcionamiento de un SOC. Este hecho no ha supuesto un retraso en la planificación global del proyecto y es considerado como normal, debido a que al inicio del proyecto no se contaba con toda la información y conocimientos necesaria sobre la implementación de un centro de operaciones de ciberseguridad.
Finalmente, los riesgos a los que estaba sometido este trabajo, analizados en el apartado 1.6, se han conseguido mitigar aplicando las medidas correctivas propuestas: buena planificación, finalización y entrega de las PECs con suficiente antelación para evitar inesperados fallos técnicos y estudio de herramientas hardware y software alternativas.

4.3 Líneas futuras

Las líneas futuras de este trabajo están enfocadas en dos direcciones: mejorar la operación del SOC planteado e implementar de forma real un centro de operaciones de seguridad.
Para mejorar la operación del SOC es necesario proveer de mayor calidad al servicio o añadir nuevos servicios que proporcionen valor añadido. En este caso, se proponen dos líneas de mejora las cuales no han podido explorarse en el trabajo presente:

- Automatización de procesos: mediante la creación de software que realice las tareas repetitivas, reduciendo la carga de trabajo del SOC y la intervención manual. Algunos ejemplos de inclusión de automatización son: detección y respuesta automatizada mediante inteligencia artificial, orquestación de tareas de seguridad y análisis y correlación de datos de múltiples fuentes.
- Visión 360 de la ciberseguridad: en el proyecto se plantea una cartera de servicios orientada a la detección y respuesta de amenazas monitorizando la red interna de los clientes.

  La visión 360 es un enfoque integral de la ciberseguridad que tiene en cuenta tanto la red interna del cliente, como las amenazas y vulnerabilidades externas a las que se encuentra expuesto. Para ello, se propone incluir el servicio de threat intelligence que permite anticiparse a las amenazas mediante el estudio de campañas de malware, tácticas de ataque o actores maliciosos, entre otros.

Otra de las líneas futuras de este trabajo es aplicar el planteamiento teórico realizado en este trabajo a un caso real, es decir, montar una empresa que brinde el catálogo de servicios de ciberseguridad seleccionados. Para ello, se seguirían las diferentes fases propuestas, se implementaría la infraestructura de red, sistemas y seguridad, se contrataría al personal necesario y se establecerían relaciones con los clientes.

Además, también sería necesario incluir un apartado económico en este documento, teniendo en cuenta el presupuesto del que parte la implementación del SOC y el coste de los diferentes recursos (personal y tecnología).

5. Glosario

- **Alerta de seguridad**. Notificación generada por una herramienta o sistema de seguridad cuando detecta a una actividad o comportamiento sospechoso. Las alertas requieren de análisis en profundidad ya que pueden indicar posibles incidentes de seguridad.
- **APTs**. *Advanced Persistent Threats*. Ataque selectivo de ciberespionaje o cibersabotaje, técnicamente avanzado y sofisticado y muy difícil de detectar. En la gran mayoría de las ocasiones son llevados a cabo por gobiernos con el objetivo de obtener información.
- **Cibercrimen**. Actividad delictiva llevada a cabo con medios electrónicos: extorsión, obtención de información confidencial, intrusión informática, etc.
- **Comportamiento anómalo**. Cualquier comportamiento que se desvia de lo esperado, pudiendo indicar una amenaza de seguridad. Puede ser originado por las personas o por las entidades (servidores, cuentas, aplicaciones) conectadas a una red.
- **CSIRT**. *Computer Security Incident Response Team*. Equipo especializado en gestión y respuesta ante incidentes de ciberseguridad con el objetivo de minimizar su impacto sobre la organización. Normalmente un CSIRT forma parte del SOC.
- **EDR**. *Endpoint Detection and Response*. Herramienta software basada en la detección de anomalías, empleando técnicas como el análisis del comportamiento o la integencia artifical, capaz de detectar patrones de ataque complejos en tiempo real. También proporciona funcionalidades de respuesta a incidentes.
- **Falso negativo**. Hace referencia a la no aparición de una alerta de seguridad por parte de las herramientas de monitorización. En este caso el software de seguridad no detecta una intrusión, amenaza o ciberataque cuando si existe.
- **Falso positivo**. Hace referencia a la detección de una alerta de seguridad errónea por parte de las herramientas de monitorización. En este caso el software de seguridad detecta una intrusión, amenaza o ciberataque cuando en realidad no se ha producido.
- **Incidente de seguridad**. Suceso o evento que compromete la seguridad de un sistema, red o aplicación de una organización. Algunos ejemplos de incidentes de seguridas son ataques, malware, intrusiones o robo de información.
- **IOA**. *Indicators of Attack*. Permite detectar la intención u objetivo de un atacante dentro de un sistema, por ejemplo, filtración de información.
- **IOC**. *Indicators of Compromise*. Evidencia digital en un sistema que indica que su seguridad ha sido comprometida, por ejemplo, malware.
- **Positivo benigno**. Hace referencia a la detección de una alerta de seguridad acertada por parte de las herramientas de monitorización. En este caso el software de seguridad detecta una intrusión, amenaza o ciberataque, pero esta no supone un riesgo para la seguridad de los sistemas. Por ejemplo, se puede detectar el empleo de herramientas de

hacking en un sistema, pero se están se están llevando a cabo pruebas de penetración legítimas en él.

- **Pyme**. *Pequeñas y Medianas Empresas*. Se considera una Pyme aquellas empresas que ocupan a menos de 250 personas; y cuyo volumen de negocios anual no excede de 50 millones de euros, o bien cuyo balance general anual no excede de 43 millones de euros.
- **RGPD**. *Reglamento de Protección de Datos Personales*. Conjunto de reglas y principios que regulan la privacidad y los datos personales de los ciudadanos de la Unión Europea.
- **SDGs**. *Sustainable Development Goals*. Iniciativa propuesta por la organización de Naciones Unidas que busca promover el desarrollo sostenible a nivel mundial. Se compone de 17 objetivos y 169 metas.
- **SIEM.** *Security Information and Event Management*. Herramienta software que recopila los eventos generados por diferentes sistemas (servidores, firewall, equipos personales etc.) en tiempo real y los aglutina dentro de una misma base de datos para detectar patrones y anomalías característicos de ataques e incidentes de seguridad
- **SLA**. *Acuerdo a nivel de servicio*. Contrato que establece los términos y condiciones para la prestación de un servicio entre un cliente y un proveedor, así como la penalización en caso de que este no se cumpla.
- **SOC**. *Centro de Operaciones de Seguridad*. Centro de monitorización, análisis y respuesta a ciberamenazas.
- **TTPs**. *Tácticas, técnicas y procedimientos.* Hacen referencia a las acciones que llevan a cabo y las herramientas que emplean los ciberatacantes.
- **Verdadero positivo***.* Hace referencia a la detección de una alerta de seguridad acertada por parte de las herramientas de monitorización. En este caso el software de seguridad detecta una intrusión, amenaza o ciberataque cuando si se ha producido.
- **Vulnerabilidad***.* debilidad presente en un sistema de información, procedimientos de seguridad, controles internos o implementación que puede ser explotada con objetivos malintencionados.

6. Bibliografía

[1] Ciberamenazas y tendencias: Análisis de las ciberamenazas nacionales e internacionales, de su evolución y tendencias futuras. (2022). Centro Criptológico Nacional. Recuperado el 5 de marzo de 2023, de https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6786-ccn-cert-ia-24-22-ciberamenazas-y-tendencias-edicion-2022-1/file.html

[2] Kaspersky. (2022, 9 marzo). ¿Qué es una amenaza avanzada persistente (APT)? latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/advanced-persistent-threats

[3] Staff, V. B. (2022, 23 mayo). Report: Average time to detect and contain a breach is 287 days. VentureBeat. Recuperado el 5 de marzo de 2023, de https://venturebeat.com/security/report-average-time-to-detect-and-contain-a-breach-is-287-days/

[4] Sophos. (s. f.). Sophos Threat Report. SOPHOS. https://www.sophos.com/en-us/content/security-threat-report

[5] Lukehart, A. (2021b, mayo 20). 10 Small Business Cyber Security Statistics That You Should Know – And How To Improve Them. Cybersecurity Magazine. Recuperado el 5 de marzo de 2023, de https://cybersecurity-magazine.com/10-small-business-cyber-security-statistics-that-you-should-know-and-how-to-improve-them/

[6] S. (2022, 10 agosto). Reasons You Need a Security Operations Center. Silverseal. Recuperado el 19 de marzo de 2023, de https://www.silverseal.net/insights/reasons-you-need-security-operations-center-operators/

[7] THE 17 GOALS | Sustainable Development. (s. f.). https://sdgs.un.org/goals

[8] Apd, R. (2022, 13 enero). Cómo aplicar la metodología Scrum y qué es el método Scrum. APD España. Recuperado el 11 de marzo de 2023, de https://www.apd.es/metodologia-scrum-que-es/

[9] Knerler, K., Parker, I., & Zimmerman, C. (2022). 11 estrategies of a world-class cyber security operations centre. MITTRE. Recuperado el 7 de marzo de 2023, de https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

[10] Samson, R., Jr. (2021, 7 diciembre). Five Security Operations Center Models Compared: Find The Right SOC Model. ClearNetwork, Inc. Recuperado el 7 de marzo de 2023, de https://www.clearnetwork.com/types-of-security-operations-centers-soc/

[11] Ramos, D. (2017, 24 noviembre). A fondo: ¿Cómo funcionan los SOC? Silicon. Recuperado el 16 de marzo de 2023, de https://www.silicon.es/a-fondo-como-funcionan-soc-2362658

[12] MITRE. (s. f.). MITRE ATT&CK®. Recuperado el 16 de marzo de 2023, de https://attack.mitre.org/

[13] Ferrara, E. (2013, 2 agosto). Security Operations Center (SOC) Staffing. Recuperado el 17 de marzo de 2023, de https://dsimg.ubm-us.net/envelope/138933/300232/1380122752_ForresterAnalyst_Report_-_Security_Operations_Center_(SOC)_Staffing.pdf

[14] Microsoft. (s. f.). ¿Qué es SIEM? | Seguridad de. Recuperado el 25 de marzo de 2023, de https://www.microsoft.com/es-es/security/business/security-101/what-is-siem

[15] Magic Quadrant for Security Information and Event Management. (s. f.). Gartner. Recuperado el 25 de marzo de 25d. C., de https://www.gartner.com/doc/reprints?id=1-2AHCXAHG&ct=220701&st=sb
[16] Nomios USA Inc. (2022, 11 octubre). EDR, NDR, XDR, MDR - Different concepts of Detection & Response. Nomios Group. Recuperado el 26 de marzo de 2023, de https://www.nomios.com/news-blog/edr-ndr-xdr-mdr/
[17] Sentonas, M. (2023, 2 marzo). Three Times a Leader: CrowdStrike Named a Leader in Gartner® Magic QuadrantTM for Endpoint Protection Platforms. crowdstrike.com. Recuperado 26 de marzo de 2022, de https://www.crowdstrike.com/blog/crowdstrike-named-a-leader-in-gartner-magic-quadrant-for-epp-three-times-in-a-row/
[18] Microsoft. (s. f.-a). ¿Qué es la administración de vulnerabilidades? | Seguridad de. Recuperado el 2 de abril de 2023, de https://www.microsoft.com/es-es/security/business/security-101/what-is-vulnerability-management
[19] C. (2020, 15 diciembre). Herramientas y software para análisis forense de seguridad informática. Ciberseguridad. Recuperado el 2 de abril de 2023, de https://ciberseguridad.com/servicios/analisis-forense/software/
[20] Informática, S. D. S. (2022, 27 septiembre). Herramientas necesarias en un Pentesting. DragonJAR - Servicios de Seguridad Informática. Recuperado el 2 de abril de 2023, de https://www.dragonjar.org/herramientas-necesarias-en-un-pentesting.xhtml
[21] Mejores sistemas protección red con sistemas IDS/IPS. (s. f.). Blog elhacker.NET. Recuperado el 5 de abril de 2023, de https://blog.elhacker.net/2022/01/mejores-sistemas-para-proteger-red-intrusos-amenazas-sistema-ids-ips.html
[22] Trost, R. (2019, 9 mayo). TIP vs. SIEM vs. Ticketing System – Part 2. ThreatQuotient. Recuperado el 4 de abril de 2023, de https://www.threatq.com/tip-vs-siem-vs-ticketing-system-part-2/
[23] Normas ISO. (s. f.). ISO 27001 - Seguridad de la información: norma ISO IEC 27001/27002. Recuperado el 20 de marzo de 2023, de https://www.normas-iso.com/iso-27001/
[24] Reglamento General de Protección de Datos. (s. f.). Boletín Oficial del Estado. Recuperado el 25 de marzo de 2023, de https://www.boe.es/doue/2016/119/L00001-00088.pdf
[25] Team, A. C. 4. (2022, 5 noviembre). Metodología NIST: Sustento para analistas de ciberseguridad. Tarlogic Security. Recuperado el 26 de marzo de 2023, de https://www.tarlogic.com/es/blog/guias-nist-ciberseguridad/
[26] C. (2020a, julio 3). ISO 22301: Gestión de la Continuidad de Negocio. Ciberseguridad. Recuperado el 3 de abril de 2023, de https://ciberseguridad.com/normativa/espana/iso-22301/
[27] Normas ISO. (s. f.-b). ¿Qué es el Esquema Nacional de Seguridad – ENS? Recuperado el 4 de abril de 2023, de https://www.normas-iso.com/esquema-nacional-de-seguridad/
[28] How to set up CSIRT and SOC. (s. f.). ENISA. Recuperado el 4 de abril de 2023, de https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc
[29] Guía 800-61 del NIST. (s. f.). Recuperado el 7 de abril de 2023, de https://www.ccn-cert.cni.es/gl/gestion-de-incidentes/lucia/23-noticias/291-nuevas-guias-del-national-institute-of-standards-and-technology-nist.html

[30] Tablado, F. (2023, 24 marzo). Bastionado de sistemas y servidores. ¿Qué es y para qué sirve? Grupo Atico34. Recuperado el 7 de abril de 2023, de https://protecciondatos-lopd.com/empresas/bastionado-de-sistemas/
[31] CrowdStrike. (2022, 13 septiembre). What is Cyber Threat Hunting? [Proactive Guide] | CrowdStrike. crowdstrike.com. Recuperado el 8 de abril de 2023, de https://www.crowdstrike.com/cybersecurity-101/threat-hunting/
[32] Rangel, E. D. S. (2022, 18 mayo). Inteligencia de Amenazas Cibernéticas o CTI-Cyber Threat Intelligence. Recuperado el 8 de abril de 2023, de https://blog.a3sec.com/es/inteligencia-de-amenazas-cibern%C3%A9ticas-o-cti-cyber-threat-intelligence
[33] González, I. (2022, 20 diciembre). ¿Cómo hacer un análisis de vulnerabilidad? Thinking for Innovation. Recuperado el 8 de abril de 2023, de https://www.iebschool.com/blog/como-hacer-un-analisis-de-vulnerabilidad-digital-business/
[34] Malwarebytes. (2019, 7 enero). ¿Qué es el phishing? | Cómo protegerse de los ataques de phishing. Recuperado el 8 de abril de 2023, de https://es.malwarebytes.com/phishing/
[35] KeepCoding, R. (2022, 5 septiembre). ¿Qué es el análisis de malware? KeepCoding Bootcamps. Recuperado el 8 de abril de 2023, de https://keepcoding.io/blog/que-es-el-analisis-de-malware/
[36] Agea, O. (2022, 11 julio). ¿Es obligatoria la formación en ciberseguridad? Grupo2000 - Formación, Empleo e Innovación. Recuperado el 8 de abril de 2023, de https://www.grupo2000.es/es-obligatoria-la-formacion-en-ciberseguridad/
[37] ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. (2021, 12 abril). INCIBE. Recuperado el 9 de abril de 2023, de https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas
[38] Rufian, M. (2022, 8 marzo). Consultoría en Ciberseguridad: qué es y cuáles son sus beneficios. Mikel Rufián. Recuperado el 9 de abril de 2023, de https://mikelrufian.com/consultoria-ciberseguridad/
[39] Villena, M. (2022, 22 diciembre). Ciberseguridad y análisis de datos: dos aspectos clave para la digitalización de las pymes en 2023. El PaÃ-s. Recuperado el 12 de abril de 2023, de https://elpais.com/economia/estar-donde-estes/2022-12-22/ciberseguridad-y-analisis-de-datos-dos-aspectos-clave-para-la-digitalizacion-de-las-pymes-en-2023.html
[40] Informe «Cifras PYME» de febrero de 2023. (2023, 14 marzo). Ministerio de industria, comercio y turismo. Recuperado el 12 de abril de 2023, de http://www.ipyme.org/es-ES/noticias/Paginas/detallenoticiaN.aspx?itemID=9898
[41] Catálogo de empresas y soluciones de ciberseguridad. (s. f.). INCIBE. Recuperado el 13 de abril de 2023, de https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad
[42] IT Digital Media Group. (2022, 14 septiembre). Las pymes poco preparadas en ciberseguridad son más atacadas que las ciberexpertas. Seguridad | IT Reseller. Recuperado el 13 de abril de 2023, de https://www.itreseller.es/seguridad/2022/09/las-pymes-poco-preparadas-en-ciberseguridad-son-mas-atacadas-que-las-ciberexpertas
[43] Descubre porqué quieren atacar tu pyme. (2016, 25 mayo). INCIBE. Recuperado 18 de abril de 2023, de https://www.incibe.es/protege-tu-empresa/blog/Descubre-porque-quieren-atacar-tu-pyme

[44] Comonline. (2021, 23 septiembre). Los ciberataques más frecuentes que ponen en peligro a la pyme española. Telefónica. Recuperado el 18 de abril de 2023, de https://www.telefonica.com/es/sala-comunicacion/blog/los-ciberataques-mas-frecuentes-que-ponen-en-peligro-a-la-pyme-espanola/
[45] El estado de la ciberseguridad en España. (s. f.). Deloitte Spain. Recuperado el 18 de abril de 2023, de https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html
[46] Muniz, J. (s. f.). Security Operations Center: Building, Operating, and Maintaining your SOC | Cisco Press. Recuperado el 27 de abril de 2023, de https://www.ciscopress.com/store/security-operations-center-building-operating-and-maintaining-9780134052014
[47] Atlassian. (s. f.). ITIL en la ITSM moderna: una guía completa | Atlassian. Recuperado el 27 de abril de 2023, de https://www.atlassian.com/es/itsm/itil
[48] PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA LA CONTRATACION DE SERVICIOS DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC) Y OFICINA TECNICA DE SEGURIDAD DE LA INFORMACION (OTSI) PARA EMASESA (Expte.: 082/2019). (s/f). Contrataciondelestado.es. Recuperado el 19 de mayo de 2023, de https://contrataciondelestado.es/wps/wcm/connect/c42b4ce2-966c-42b2-9ff8-c8f643f63214/DOC20190925112217PPTP+con+anexos_082-19.pdf?MOD=AJPERES
[49] Santos, D. (2023, 20 enero). ¿Qué es y cómo hacer un análisis de riesgos? HubSpot. Recuperado el 6 de mayo de 2023, de https://blog.hubspot.es/marketing/analisis-de-riesgos