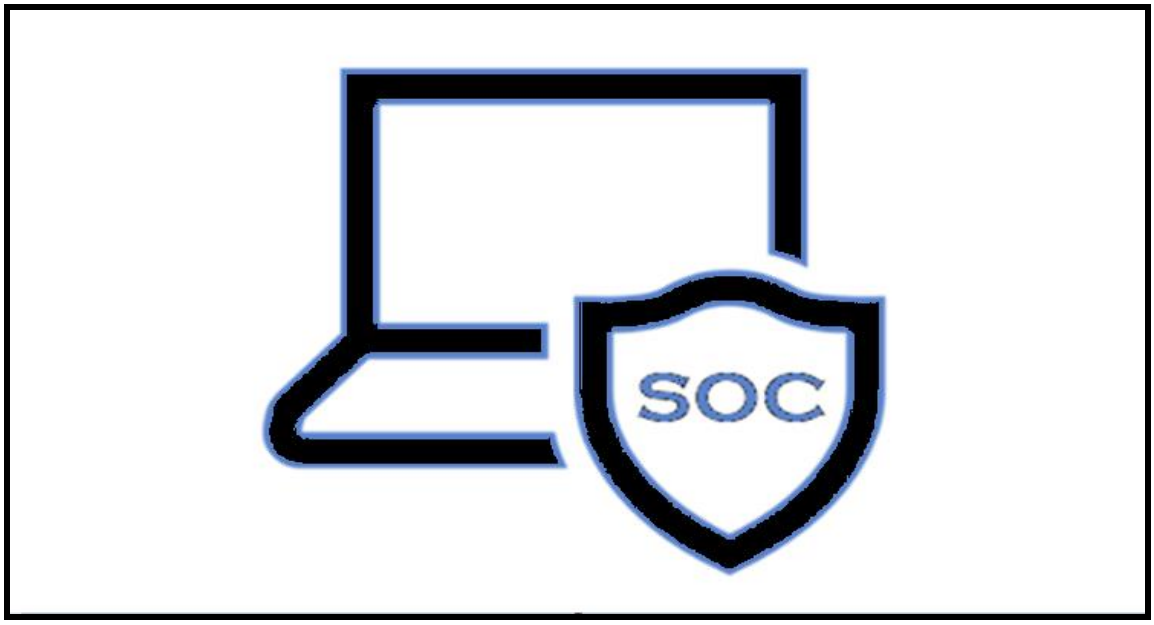

Guía de implementación de un SOC

Antonio Díaz Pérez
Máster Universitario en Ciberseguridad y Privacidad
Seguridad empresarial

Iñaki Moreno Fernández
Víctor García Font y Andreu Pere Isern Deyà

Enero de 2023

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Guía de implementación de un SOC*
Nombre del autor:	*Antonio Díaz Pérez*
Nombre del consultor/a:	*Iñaki Moreno Fernández*
Nombre del PRA:	*Víctor García Font* *Andreu Pere Isern Deyà*
Fecha de entrega (mm/aaaa):	*01/2023*
Titulación o programa:	Máster U. en Ciberseguridad y Privacidad
Área del Trabajo Final:	*Seguridad empresarial*
Idioma del trabajo:	*Español*
Palabras clave	*SOC, Ciberseguridad, Seguridad*

Resumen del Trabajo

Hoy en día, tras la digitalización tecnológica y el auge del teletrabajo, las organizaciones valoran su información como su principal activo y su bien más preciado, ya que no sólo se trata de un conjunto de datos con los que se trabaja, sino del conjunto de datos que proporciona identidad y valor para su funcionamiento y su negocio. Sin embargo, el aumento de la información digital ha provocado también el crecimiento de sus riesgos y amenazas, por lo que las organizaciones se encuentran cada vez más atacadas y se enfrentan a adversarios con técnicas complejas.

Debido a esto, la ciberseguridad se ha convertido en una prioridad y una necesidad para todas las organizaciones, por lo que cada vez más se demandan soluciones que se encarguen de todos los aspectos tácticos, técnicos y operativos para la protección de su información digital. De hecho, en múltiples ocasiones, optan por la implementación de un SOC para cumplir con estas funciones, ya que se trata de un área de ciberseguridad operativa y centralizada que trabaja para la protección de esta información.

Sin embargo, la implementación de los SOC en las organizaciones no siempre tiene el éxito esperado y se consumen muchos más recursos temporales, económicos y de personal del necesario por no disponer del conocimiento y la experiencia adecuada. Por tanto, con este trabajo se propone el estudio y desarrollo de una guía simple de buenas prácticas para la implementación de un SOC que oriente a las diferentes organizaciones en su puesta en funcionamiento.

Abstract

Nowadays, with technological digitalization and the rise of teleworking, organizations value their information as their main asset and their most precious commodity, since it is not only a set of data to work with, but also the data that provide identity and value for their operations and business. However, the growth of digital information has also led to the growth of associated risks and threats, so organizations find themselves increasingly under attack and are facing adversaries using complex techniques.

Because of this, cybersecurity has become a priority and a necessity for all organizations, which is why they are increasingly demanding solutions that take care of all the tactical, technical and operational aspects of protecting their digital information. In fact, they often opt for the implementation of a SOC to fulfil these functions, since it is an operational and centralized cybersecurity area that works for the protection of this information.

However, the implementation of SOCs in organizations is not always as successful as expected. As a matter of fact, temporary resources, as well as economic and staff resources are used in excess due to the lack of adequate knowledge and experience. Therefore, this work proposes the study and development of a simple guide of good practices for the implementation of a SOC to help the different organizations.

Índice

Lista de ilustraciones

Lista de tablas

1. Introducción

1.1 Contexto y justificación del Trabajo

1.1.1 Escenario y estado del arte

Desde un principio, antes de la aparición de los sistemas informáticos en las organizaciones, la información de valor corporativa se elaboraba y procesaba a través de materiales físicos, como son los registros en papel, los documentos fotográficos físicos o las cintas de audio y vídeo, y se almacenaba en lugares únicos y también físicos, como son las salas de archivo o los almacenes de documentos. Esto tenía como consecuencia que el acceso, almacenaje, localización, distribución y gestión de la información supusieran un coste elevado a nivel empresarial y que no se pudiera garantizar su servicio debido a múltiples factores, como pueden ser la facilidad de extravío o degradación de los materiales.

Tras el surgimiento de los sistemas informáticos, se promovió la digitalización de la información en las organizaciones y se comenzaron a generar herramientas y sistemas de procesamiento ágil y de rápido acceso a los datos. Este hecho provocó la creación de los primeros sistemas de información digitales, en donde los datos son su unidad mínima y materia prima y su misión consiste en crearlos, transportarlos, almacenarlos y procesarlos para desembocar, primero, en información y, finalmente, cuando ésta se haya visualizado, estudiado y gestionado, en conocimiento para el negocio.

Asimismo, tras la aparición de los sistemas de información digitales, que resuelven los problemas de la información en materiales físicos, como de espacio, transporte o ubicación, entre otros, cada vez son más las entidades que utilizan la tecnología digital, a través de sistemas digitales o, incluso, de procesos de transformación digital, para satisfacer sus necesidades de negocio sobre la gestión de sus datos, su información y su conocimiento. En consecuencia, la información pasa a convertirse en uno de los activos más importantes y valiosos a nivel estratégico empresarial y, por tanto, su seguridad y protección, a una necesidad básica y fundamental para su negocio.

Por otra parte, a la vez que aumenta el uso de tecnologías y sistemas de información a través de entornos digitales, también aumentan los ataques informáticos hacia las entidades corporativas que las usan. Estos ataques tienen como fin, el hallazgo de sus vulnerabilidades existentes para intentar explotarlas y transgredir o quebrantar sus sistemas. Por tanto, las amenazas a la información de valor de las organizaciones han crecido al mismo tiempo y en la misma medida que su desarrollo digital, lo que ha provocado que se preste mayor importancia y atención a la seguridad informática.

Del mismo modo, las propias entidades han necesitado una reinvención y adecuación constante para mitigar y dar solución a la aparición de las nuevas vulnerabilidades y de los problemas técnicos detectados. Los términos y condiciones de estos ataques varían constantemente y cada vez se desarrollan más sofisticados y elaborados, por lo que también se necesitan soluciones más difíciles y complejas de aplicar. En consecuencia, esto provoca que la seguridad de las tecnologías y sistemas de información se contemple como un elemento fundamental en toda organización y que se empleen recursos en minimizar y manejar los riesgos de seguridad para el negocio.

Tal y como indican el CCN-CERT[1] y la norma establecida UNE-EN ISO/IEC 27001 del año 2022, la **Seguridad de la Información**[2] se define como la salvaguarda o protección de todas las propiedades de la información, como son la confidencialidad, la integridad y la disponibilidad, como pilares fundamentales, y la autenticidad, la responsabilidad, la trazabilidad, la fiabilidad y la precaución del repudio, como características importantes. Asimismo, se describe como el conjunto de medidas preventivas y mitigadoras para defender y proteger todas las cualidades de los datos que componen la información.

Por otra parte, como una parte de la seguridad de la información, se encuentra el concepto de **ciberseguridad**[3], que se define como la práctica o habilidad de salvaguardar y defender todos los sistemas de información interconectados de ataques en formato digital. De hecho, aunque, comúnmente, se expresen como sinónimos, existe una diferencia entre seguridad de la información, seguridad informática y ciberseguridad. La seguridad de la información debe entenderse como el concepto más amplio que engloba a los otros dos y que se refiere como el conjunto de medidas para proteger la información; la seguridad informática como la disciplina que se encarga de asegurar esa información, y la ciberseguridad como la práctica de proteger la información de ataques informáticos o digitales.

De manera genérica, en las organizaciones se comprenden estos tres conceptos de seguridad como el conjunto de actividades y controles técnicos, legales, organizativos y corporativos con los que diseñan sus políticas de seguridad de la información para garantizar y asegurar todas sus dimensiones de posibles ataques digitales. Debido a esto, estas organizaciones requieren de servicios de ciberseguridad que les resguarde la integridad, confidencialidad, autenticidad, disponibilidad, trazabilidad y no repudio de sus datos y sistemas de información, así como de disponer, en caso de necesidad, de procedimientos adaptados para el restablecimiento de sus datos a la mayor brevedad y con el menor impacto posible para su negocio.

Por otra parte, en la actualidad, tras los eventos de más relevantes del panorama internacional de los últimos años, como son, entre otros, la pandemia por el Covid-19, que derivó en la interconexión forzosa de las empresas, o la guerra entre Rusia y Ucrania, que precedió y se impulsó con una ciberguerra, la ciberseguridad ha tomado un papel muy importante para Estados, gobiernos y organizaciones, que requieren de la protección de su información ante el aumento de los ataques informáticos (ciberataques) y las amenazas informáticas (ciberamenazas). De hecho, la mayor preocupación de los propietarios de la información se centra, sobre todo, en las ciberamenazas orientadas a eliminar, modificar o robar su información y a destruir o parar sus servicios.

Dada la amplia variedad de ciberamenazas contra la seguridad de los sistemas de información, cada vez más, las organizaciones y su personal responsable de esta seguridad, establecen diferentes controles para minimizar sus riesgos. Estos controles de seguridad se pueden definir como el conjunto de actividades que forman una barrera de protección basada en estándares internacionales, políticas internas y buenas prácticas para paliar los ataques informáticos y sus incidentes de seguridad. Además, los controles implantados se describen, en su mayoría, entre los siguientes documentos internos para cada organización:

---

[1] https://www.ccn-cert.cni.es/
[2] https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n
[3] https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

- La Política de seguridad de la información.
- El Plan operativo y funcional de seguridad de la información.
- El Plan de gestión de seguridad de los usuarios, de los clientes y del personal.
- La Política de clasificación de los datos, de la información y del conocimiento.
- El Plan de gestión de indicadores de seguridad de la información.
- El Plan de continuidad del negocio.
- El Plan de auditorías y activos de sistemas de información.
- El Plan de respuesta ante eventos e incidentes de seguridad.

Con el paso de los años y gracias al aumento de estas ciberamenazas, las organizaciones han empezado a reconocer la importancia de invertir recursos para la seguridad de su información corporativa. Esta tendencia general se basa en la implementación de un equipo especialista en la gestión de todos los ámbitos de la seguridad de la información que verifique todas las actividades, tanto internas como externas y de entrada como de salida, para gestionar los posibles ataques informáticos y minimizar los riesgos que se puedan detectar en su Política y Planes relacionados con la Seguridad de la información.

Por este motivo, diferentes entidades y organismos se han visto en la necesidad de invertir en la implementación de un SOC (*Security Operations Center*, por sus siglas en inglés, o Centro de Operaciones de Seguridad) o en la creación de una red colaborativa de SOC, como la Red Nacional de SOC (RNS) impulsada por el CCN-CERT. De hecho, un SOC se define como un equipo centralizado que se ocupa de los elementos tácticos, técnicos, procedimentales y operativos relacionados con la ciberseguridad. Además, se dedica a la detección y protección de los activos y sistemas de información en tiempo real y del análisis y respuesta de los eventos e incidentes de seguridad, a través de sus registros o *logs* y mediante recursos tecnológicos y humanos especializados en la anticipación y respuesta ante incidentes de seguridad.

1.1.2 Motivaciones

En base a los elementos indicados en el ámbito de seguridad de la información del panorama actual, se puede observar la importancia de establecer unos buenos criterios y normas para proteger los datos, la información y el conocimiento de las organizaciones. Sin embargo, a pesar de existir múltiples políticas y documentos que avalen la seguridad de la información y de sus controles, no existe un estándar o normativa internacional para la implementación de un SOC basado en buenas prácticas que oriente a las diferentes entidades en su puesta en funcionamiento.

Además, la protección de la seguridad de la información, desde el punto de vista operativo, se trata de un asunto de actualidad internacional en el que cada día se invierte más para su desarrollo e innovación de cara a las diferentes organizaciones. Por tanto, personalmente, considero una buena especialización con la que desarrollar mi presente y futuro académico y profesional. Al fin y al cabo, se trata de un ámbito que protege a toda la sociedad, desde las instituciones y empresas hasta los ciudadanos y clientes, y siempre será un recurso necesario con una alta demanda de especialistas.

Debido a esto, como propuesta de Trabajo de Final de Máster, se propone elaborar una guía para la implementación de un SOC que facilite su creación y desarrollo a toda aquella organización que lo requiera. De esta forma, se ofrece un manual orientativo para la creación de un servicio de seguridad de la información, especializado en la ciberseguridad, que centralice los eventos e incidentes de seguridad, satisfaga las necesidades de protección de activos corporativos y la respuesta de estos incidentes y se ampare en buenas prácticas que culminen en un servicio de calidad y en el éxito del proyecto de su implantación.

1.2 Objetivos del Trabajo

1.2.1 Objetivo principal

1.2.1.1 Documento guía

Dado el crecimiento de los ciberataques a escala internacional de los últimos años, el compromiso de las diferentes entidades y su correspondiente afección en sus labores diarias de negocio, las organizaciones han empezado a destacar la necesidad de disponer de un equipo, como puede ser un SOC, que proteja su información corporativa. Debido a esto, el objetivo principal de este Trabajo se centra en la creación de un documento simple que sirva de guía genérica para la implementación de un SOC, a partir del estudio de sus necesidades básicas y de las buenas prácticas incluidas en las metodologías ágiles y en las normativas relacionadas con la seguridad de la información. De hecho, esta guía será el producto resultante del Trabajo y se añadirá en el en el Capítulo 3 de este documento, en referencia a los Resultados obtenidos.

1.2.2 Objetivos específicos

Asimismo, con el fin de lograr este objetivo principal, de manera parcial se pretenden conseguir diferentes propósitos específicos que darán lugar al éxito de este Trabajo Final de Máster:

1.2.2.1 Análisis del marco preliminar y conceptual de un SOC

Este objetivo específico consiste en el estudio de los conceptos más importantes de la Seguridad de la Información y su relación con la gestión y actividad diaria de un SOC. Su objetivo se fundamenta en la definición y explicación de la seguridad en el ámbito de la información, los riesgos, las amenazas, las vulnerabilidades, los ataques, los incidentes de seguridad y los sistemas de protección, prevención y detección.

1.2.2.2 Análisis del marco metodológico y legal de SOC

Este objetivo específico consiste en el estudio de los estándares, normativas y metodologías internacionales y de las disposiciones legales aplicables a un SOC junto a sus beneficios para su implementación y correcto funcionamiento.

1.2.2.3 Análisis del marco teórico de un SOC

Este propósito específico se basa en el análisis de todo lo relacionado con el concepto de SOC, sus tipos, sus beneficios e inconvenientes, su razón de ser y las diferentes áreas que lo pueden componer, entre otros términos y criterios.

1.2.2.4 Análisis de los requisitos para la implantación de un SOC

Este hito específico se centra en el análisis y el estudio de las necesidades y requisitos, tanto a nivel técnico como de negocio, para la implementación de un SOC. Su objetivo se basa en la enumeración y descripción de los diferentes aspectos necesarios para garantizar una implementación de un SOC de calidad que satisfaga las necesidades por las que se constituye y se desarrolle y madure sobre una base sólida.

1.2.2.5 Análisis de las funciones de un SOC

Este propósito específico se resume en la investigación de las actividades que desarrolla un SOC, como son el tratamiento y gestión de los registros de funcionamiento de los sistemas (*logs*), la integración de los activos, la monitorización y correlación de los eventos de seguridad, los flujos de trabajo, la identificación de las amenazas y el tratamiento y reporte de los incidentes de seguridad, entre otros. Por tanto, su objetivo se centra en la descripción de las tareas básicas que debe realizar este equipo de ciberseguridad.

1.2.2.6 Análisis de servicios y procesos de un SOC

Esta finalidad específica describe el estudio de los diferentes servicios y procesos que, como mínimo, deben formar parte de un SOC para poder alcanzar el cumplimiento con sus funciones. Su objetivo se asienta en la definición del alcance de los servicios básicos que debe ofrecer este equipo y el análisis de sus requisitos específicos y exigibles para garantizar la seguridad de la información de una entidad y las bases para su guía de implementación.

1.2.2.7 Análisis de los roles de un SOC

Este punto específico detalla el análisis de los diferentes roles que se deben estructurar en un SOC y de las funciones que se desempeñan en cada uno de los servicios que ofrece. Su objetivo se centra en la descripción de los diferentes niveles de especialización y en las características que debe tener su personal para gestionar cada uno de los servicios que ofrece un SOC.

1.2.2.8 Análisis de las tecnologías necesarias para un SOC

Este apartado específico explica el estudio de las principales tecnologías que se deben tener presentes para la implantación de un SOC y su correcto funcionamiento. Su objetivo se basa en la descripción de las diferentes herramientas y recursos tecnológicos que se necesitan para llevar a cabo las actividades diarias reactivas y proactivas de todos los servicios de esta área.

1.2.2.9 Análisis de la implementación de un SOC

Este objetivo específico describe el análisis de la implementación de un SOC sobre el que se desarrollará el documento guía. Su objetivo consiste en valorar las diferentes etapas por las que debe pasar el proceso de implementación de un SOC, así como cada uno de sus objetivos y planificación.

1.3 Impacto en sostenibilidad, ético-social y de diversidad

La implementación de un SOC, al igual que cualquier otro proyecto al que deba de enfrentarse cualquier organización de la actualidad, debe alinearse con los objetivos de desarrollo sostenible aprobados por la ONU, en el año 2015, en la Agenda para el Desarrollo Sostenible[4]. De esta manera, tal y como expresa este programa, éste o cualquier otro proyecto se uniría al ideal de la ONU y a su llamamiento universal para intentar conseguir propósitos de alto nivel como resguardar y preservar el planeta, aumentar la calidad de vida de las personas, garantizar la prosperidad y erradicar la pobreza, entre otros. Estos propósitos son diecisiete objetivos globales y se definen como los Objetivos de Desarrollo Sostenible (ODS).
De igual manera, este Trabajo Final de Máster se alinea con estos Objetivos de Desarrollo Sostenible y se organiza en torno a las tres dimensiones que definen las Competencias de Compromiso Ético y Global (CCEG), que se engloban en la sostenibilidad, en la responsabilidad social (RS) y el comportamiento ético y en los derechos humanos, el género y la diversidad. Por tanto, su estudio y desarrollo se realiza sobre principios éticos, íntegros, sostenibles, sensatos, responsables, plurales y respetuosos con las personas, la sociedad y el medio ambiente y se enfoca en la guía simple de un proyecto de implantación tecnológico basado en buenas prácticas globales.

1.3.1 Impacto en Sostenibilidad

La sostenibilidad facilita la reducción del impacto ambiental, promueve el progreso social y genera un desarrollo económico. Por ello, la implementación de un SOC se alinea fundamentalmente con el objetivo noveno[5] de los Objetivos de Desarrollo Sostenible (ODS), ya que consiste en la creación de un equipo tecnológico que, entre otras, debe promover la innovación para garantizar la protección de la información corporativa y guiar en la creación o modificación de infraestructuras resilientes en el ámbito de la seguridad de la información. Además, dado que un SOC puede proteger los sistemas de información de infraestructuras críticas, de manera indirecta también vela por los intereses de los demás objetivos de alto nivel relacionados con la sostenibilidad del negocio de esas infraestructuras.

1.3.2 Impacto en responsabilidad social y comportamiento ético

La responsabilidad social (RS) y el comportamiento ético comprenden la conducta humana, como individuo, y la empresarial, como colectivo, así como sus reglas y sus derechos y deberes en sociedad. Estos aspectos deben trabajarse de manera honesta, justa y transparente, exponerse bajo una comunicación precisa, conveniente

[4] https://www.un.org/sustainabledevelopment/es/development-agenda/
[5] https://www.un.org/sustainabledevelopment/es/infrastructure/

y comprensible y estructurarse bajo el amparo de los reglamentos y normativas legales. Por ello, un buen comportamiento social se fundamenta en la responsabilidad y los valores éticos de su sociedad.

Además, a imagen y semejanza que ocurre con la Sostenibilidad, dado que el cometido principal de un SOC se centra en salvaguardar los sistemas de información y los datos de la organización y de sus usuarios y clientes, se alinea esencialmente con los propósitos octavo[6] y décimo sexto[7] de los Objetivos de Desarrollo Sostenible (ODS). Esto se hace posible, gracias a que un SOC, principalmente, protege la información personal, sensible, intelectual y de valor de los individuos y organizaciones en sociedad, por lo que favorece el crecimiento económico, aumenta el empleo sostenido e inclusivo, impulsa el progreso, fortalece a las entidades e instituciones, vela por los requerimientos legales y mejora la tranquilidad de las personas, entre otros.

1.3.3 Impacto en derechos humanos, género y diversidad

La igualdad de género, raza, origen, condición sexual, ideología y estatus social, entre otros, tiene como significado que cualquier persona se encuentra en las mismas condiciones y mismas circunstancias para el beneficio de sus derechos y libertades fundamentales y de su desarrollo socio-cultural y económico en sociedad. Por tanto, dado que un SOC tiene su negocio en la seguridad de la información, se alinea principalmente con los propósitos quinto[8] y décimo[9] de los Objetivos de Desarrollo Sostenible (ODS), ya que reduce la desigualdad y no distingue ni entre género ni entre las diferentes cualidades de las personas, sino que protege sus datos e información.

Ilustración 1 - Objetivos de desarrollo sostenible (https://www.un.org/).

[6] https://www.un.org/sustainabledevelopment/es/economic-growth/
[7] https://www.un.org/sustainabledevelopment/es/peace-justice/
[8] https://www.un.org/sustainabledevelopment/es/gender-equality/
[9] https://www.un.org/sustainabledevelopment/es/inequality/

1.4 Enfoque y método seguido

Este Trabajo Final, que se compone de la creación de un Plan para la implementación de un SOC y del estudio y análisis de diferentes objetivos específicos para desarrollar este Plan, se debe realizar en base a estándares, paradigmas y procedimientos que respalden su diseño, desarrollo y ejecución con garantías de éxito y sin dependencia de la entidad que lo desee instaurar. Por tanto, dado su propósito basado en acciones activas y reactivas en entornos de incertidumbre, se considera, como opción más eficiente, sustentarse en el uso de las premisas y buenas prácticas de metodologías ágiles de reconocimiento internacional que den resultados eficaces a nivel tecnológico y de negocio.

Por consiguiente, la sección que desarrolla el Plan para la implementación de un SOC, se ejecutará bajo el enfoque metodológico de la suma de los conceptos y términos ágiles de la cultura DevOps y de la estrategia de trabajo de Kanban, dado que su complemento fortalece y mejora los resultados deseados, adapta los procesos a las necesidades del proyecto y los adecúa a la obtención de los productos resultantes que den valor. Por otra parte, la sección que atiende a los diferentes análisis de los objetivos específicos, se realizarán bajo la metodología de investigación exploratoria y descriptiva que profundice en su estudio y obtenga resultados concluyentes. Por tanto, esta combinación se considera la solución más óptima para lograr la satisfacción del Trabajo en su totalidad sin disminuir su calidad.

1.4.1 Metodología para la de creación del Plan de implementación

La creación del Plan de implementación de un SOC, tal y como se ha indicado se guiará por la conjunción de la filosofía colaborativa de DevOps y Kanban.

1.4.1.1 Uso de conceptos DevOps

DevOps se describe como una cultura o filosofía colaborativa basada en los principios de Lean y de las metodologías ágiles para la generación de servicios y productos que se adaptan a las necesidades y plazos de los clientes y con el objetivo de complementar las funciones de desarrollo de software (Dev) y de producción/operación (Ops) en un único proceso integrado y continuo. De hecho, su ciclo de vida persigue la verificación, la automatización, la mejora continua y la innovación, por lo que sus iteraciones y entregas no deben sufrir pausas ni retrasos y su conjunto de actividades debe automatizarse. Además, se fundamenta en el proceso continuo y entrega continua, en base a las siguientes etapas: desarrollo, prueba, integración, despliegue y monitorización.

Por norma general, las organizaciones se enfrentan a problemas de desacuerdos e incompatibilidades de tiempo entre los equipos de desarrollo y los de operaciones. Por ejemplo, en este Trabajo Final se pueden detectar problemas entre los análisis realizados sobre los propósitos específicos y la redacción del entregable final, dado que puede haber partes que tengan resultados favorables para la implementación de un SOC y partes que se descarten. Por tanto, con el fin de dar soluciones ágiles, se propone el uso de las prácticas definidas en los siguientes aportes de DevOps:

- Fortalecer la estructura de TI para garantizar una ventaja competitiva.
- Usar técnicas de gestión que favorezcan el rendimiento y control en TI.
- Potenciar la cultura, colaboración y comunicación organizativa.

- Atender la satisfacción de los equipos de TI para favorecer el compromiso, la productividad y la creatividad de su trabajo.

1.4.1.2 Uso de premisas de Kanban

Kanban se describe como una metodología o estrategia de trabajo ágil que potencia la productividad y efectividad del área de trabajo con la entrega de conocimiento a partir de la gestión, descripción y optimización de los servicios. Además, se basa en ideales de eficiencia y transparencia que se reflejan con la elaboración de un diagrama o tabla que señala el estado en el que se encuentran las diferentes actividades (activadas, en proceso, pendientes y finalizadas, entre otras), por lo que, además de indicar las tareas del equipo, agiliza su priorización, favorece la comunicación, la colaboración y la independencia y mejora la comprensión de los objetivos y de la estrategia del negocio.

Asimismo, Kanban cuenta con varias prácticas fundamentales que se centran en los requisitos y las necesidades de los proyectos, por lo que pueden facilitar la gestión de las diferentes tareas y estudios de cada uno de los objetivos específicos de este Trabajo Final para llegar al éxito en el objetivo principal:

- Lograr un ritmo de trabajo sostenible y enfocado hacia la mejora.
- Orientar sus actividades hacia el rendimiento necesario con el que obtener la satisfacción del cliente.
- Conseguir la competitividad, adaptabilidad y supervivencia de los equipos de trabajo.

Esta metodología ágil, además, se fundamenta en el desarrollo incremental de las tareas y la división del trabajo en partes, por lo que gestiona el estado de cada tarea, a través de técnicas visuales, con la representación de tableros que emulan *post-its* y contienen información de interés sobre sus propósitos. Adicionalmente, también facilita la entrega en cualquier momento, el cambio de prioridades y la visualización constante del flujo de trabajo. Por tanto, se considera un método adecuado para proyectos y trabajos que necesiten definir y flexibilizar la gestión de las tareas, como ocurre en este Trabajo Final.

1.4.1.3 Uso del complemento DevOps y Kanban

La unión entre DevOps y Kanban forma un bloque metodológico ágil y sólido que favorece la gestión de este Trabajo en lo referente a la creación de un plan para la implementación de un SOC. De hecho, gracias a esta unión, el beneficio destaca por las siguientes premisas resultantes:

- Permitir la unión de varios flujos de trabajo y mejorar su comunicación visual por el equipo.
- Poder rechazar tareas sin repercusiones negativas sobre el resultado final.
- Determinar los límites en donde la saturación de las tareas puede afectar a la productividad (límites WIP).
- Permitir la flexibilidad, comodidad y discreción de la gestión de problemas.
- Favorecer la implementación de productos y servicios que se adapten a cualquier necesidad de cambio.

- Potenciar la transformación cultural.
- Aligerar las entregas a través de la automatización y agilidad de los procesos.

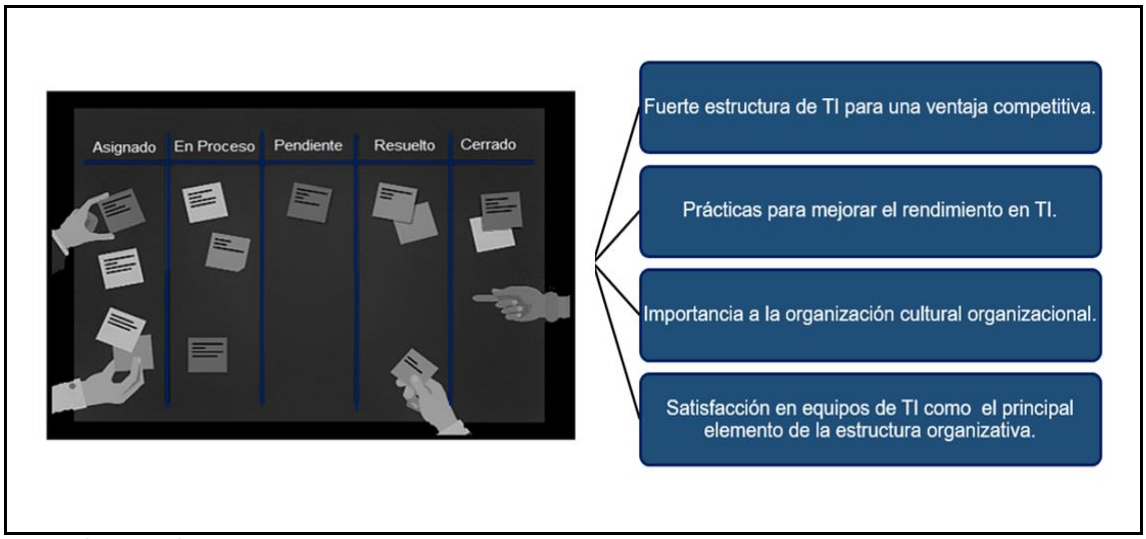

Ilustración 2 - Unión de Tablero Kanban y premisas DevOps.

1.4.2 Metodología para el análisis de objetivos específicos

El estudio y los análisis de los diferentes objetivos específicos, tal y como se ha indicado se guiará por el uso de una metodología de investigación exploratoria y descriptiva.

1.4.2.1 Uso de metodología de investigación exploratoria-descriptiva

Por una parte, la investigación exploratoria facilita el conocimiento de la información de contexto de una investigación, permite aclarar sus problemas, determinar sus prioridades y formular hipótesis, por lo que se centra, principalmente, en el descubrimiento y no siempre proporciona resultados concluyentes. Por otra parte, la investigación descriptiva facilita las características de una investigación, recopila información cuantificable, no permite la influencia en ninguna variable y permite los estudios trasversales, por lo que se centra, fundamentalmente, en la observación del caso.

Debido a esto, se realizará un estudio exploratorio que se relacione con los marcos de referencia teóricos y las buenas prácticas de la actualidad, en lo referente a la Seguridad de la Información y los equipos de ciberseguridad, y se complementará con el estudio descriptivo de la observación de los resultados de diferentes casos de creación de SOC. De esta manera, se obtendrán resultados más fiables que se plasmarán como base del entregable final.

1.5 Planificación del Trabajo

Este Trabajo se inicia el 28 de septiembre de 2022 con la propuesta de proyecto y finaliza el 27 de enero de 2023 con el la defensa del Trabajo de Final de Máster ante el Tribunal. Por tanto, a continuación, se definen los principales hitos del proyecto y sus tareas más importantes con los plazos de tiempo previstos para su solución:

1.5.1 Hito 1: Plan de trabajo (PEC1)

El hito 1 de este Trabajo Final de Máster consiste en la realización del Plan de trabajo del proyecto y se sustenta en la siguiente planificación temporal de tareas parciales:

	Fecha de inicio	Duración (horas)	Fecha de entrega
Hito 1: Plan de Trabajo (PEC1).	**28/09/2022**	**70**	**11/10/2022**
Lectura del plan de estudios y documentación del TFM.	28/09/2022	20	02/10/2022
Definición del Trabajo.	02/10/2022	11	05/10/2022
Reunión de inicialización con el tutor del TFM.	05/10/2022	1	06/10/2022
Descripción del contexto y justificación del Trabajo.	05/10/2022	8	06/10/2022
Definición de los objetivos del Trabajo.	06/10/2022	10	08/10/2022
Establecimiento del enfoque y método seguido	08/10/2022	5	09/10/2022
Estudio del impacto en sostenibilidad, ético-social y de diversidad del Trabajo.	09/10/2022	3	10/10/2022
Descripción de los capítulos de la memoria.	09/10/2022	5	10/10/2022
Redacción y revisión del entregable.	10/10/2022	7	11/10/2022

Tabla 1 - Planificación temporal del hito 1.

Además, a continuación, se presenta el diagrama de Gantt para el primer hito:

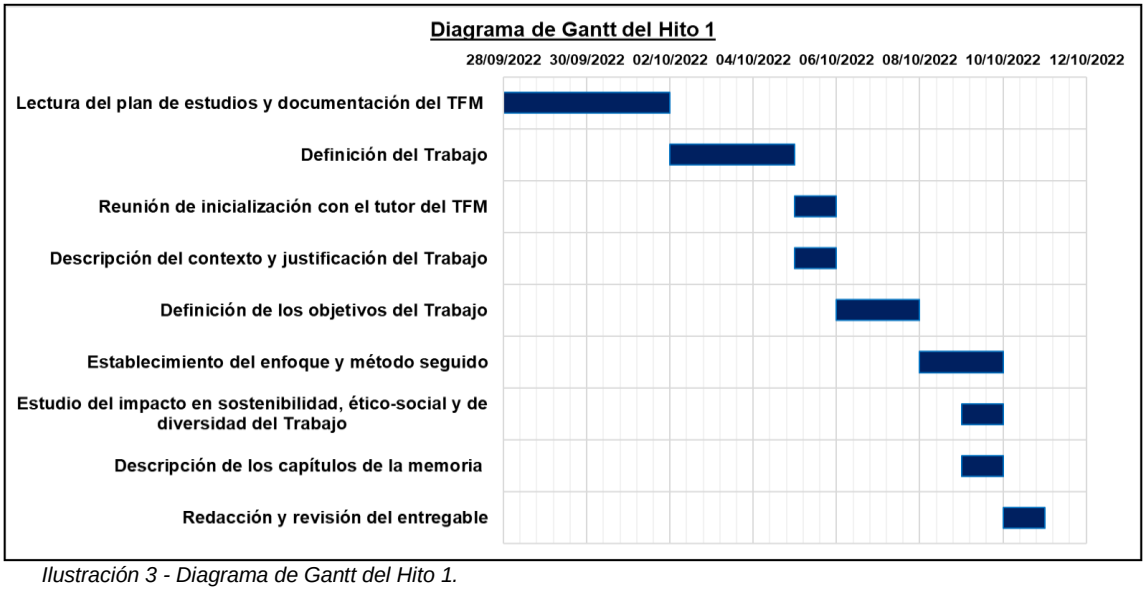

Ilustración 3 - Diagrama de Gantt del Hito 1.

1.5.2 Hito 2: Primera fase de ejecución del Plan de trabajo (PEC2)

El hito 2 de este Trabajo recae en la etapa inicial de la ejecución del Plan de Trabajo y se ampara en la siguiente planificación temporal de actividades necesarias para el cumplimiento de sus objetivos:

	Fecha de inicio	Duración (horas)	Fecha de entrega
Hito 2: Primera fase de ejecución del Plan de Trabajo (PEC2).	**12/10/2022**	**90**	**08/11/2022**
Análisis del marco preliminar para un SOC.	12/10/2022	10	15/10/2022
Estudio de Riesgos, Amenazas y Vulnerabilidades.	15/10/2022	10	19/10/2022
Análisis del marco conceptual de un SOC.	19/10/2022	12	22/10/2022
Sistemas de protección, prevención y detección.	22/10/2022	8	24/10/2022
Estudio de los ataques y los incidentes de seguridad.	24/10/2022	8	26/10/2022
Análisis del marco metodológico, estándares y buenas prácticas para un SOC.	26/10/2022	10	31/10/2022
Reunión de seguimiento con el tutor del TFM (I).	27/10/2022	1	27/10/2022
Definición de un SOC y justificación de su necesidad.	31/10/2022	10	03/11/2022
Análisis de los estándares y normativas legales para un SOC.	03/11/2022	8	05/11/2022
Análisis de los riesgos de este hito.	05/11/2022	4	06/11/2022
Redacción y revisión de este entregable.	06/11/2022	10	08/11/2022

Tabla 2 - Planificación temporal del hito 2.

Seguidamente, también se presenta su diagrama de Gantt:

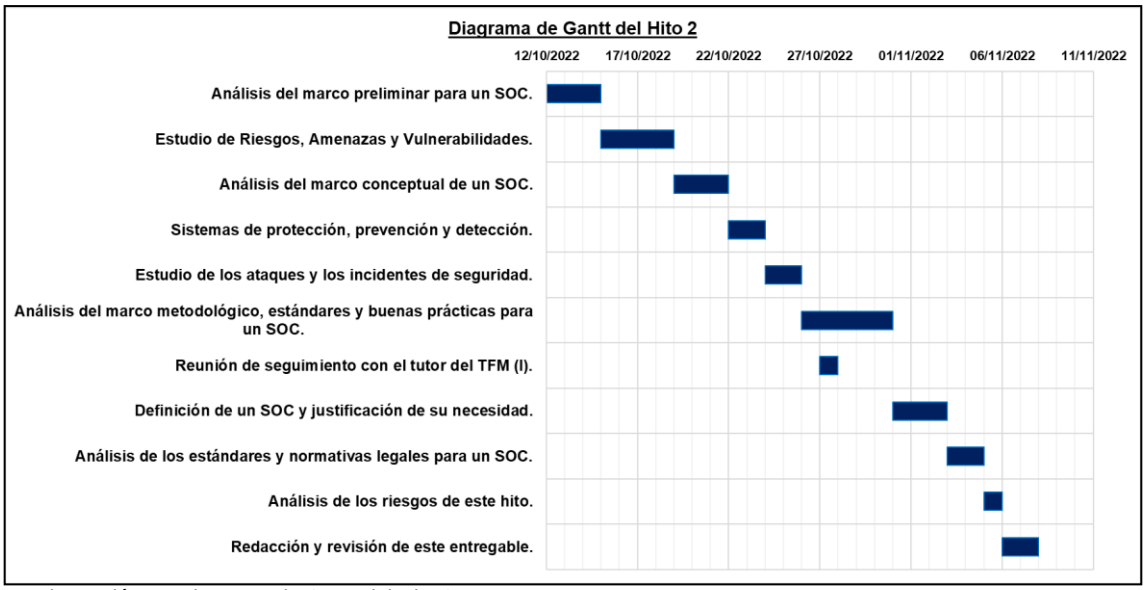

Ilustración 4 - Diagrama de Gantt del Hito 2.

Adicionalmente, se indica que, durante esta etapa del desarrollo del Trabajo, el contenido se encuentra prácticamente orientado al análisis de los marcos preliminar y conceptual, normativo y legal para la gestión y el correcto funcionamiento de un SOC y a la investigación exploratoria y descriptiva de este tipo de implantaciones en organizaciones reales, por lo que se ha previsto un tiempo adecuado para poder completar las diferentes tareas. Debido a esto, se prevé como posible riesgo fundamental, la necesidad de restructurar los resultados de los estudios e investigaciones, dado que las conclusiones deben condensarse para no superar la extensión indicada para este documento.

Por consiguiente, se establece una tabla, a modo de resumen, de los riesgos y las acciones mitigadores que se han considerado para este hito:

#	Riesgo	Acción mitigadora
1	Relación insuficiente entre los resultados de los análisis planificados y su necesidad en un SOC.	Revisión de bibliografía actualizada y en diferentes idiomas.
		Volver a realizar los estudios necesarios y obtener más resultados.
		Reajuste de las horas dedicadas a la planificación de las tareas a cumplir.
2	Necesidad de nuevos objetivos específicos.	Ajuste del alcance del Trabajo.
		Reformulación teórica de los objetivos.
3	Exceso en la extensión de los capítulos de este hito.	Puntualizar más los conceptos necesarios para clarificar mejor los objetivos a cumplir y enviar a los anexos la información complementaria.

Tabla 3 - Riegos del hito 2.

1.5.3 Hito 3: Segunda fase de ejecución del Plan de trabajo (PEC3)

El hito 3 de este Trabajo se centra en la segunda etapa de la ejecución del Plan de trabajo y se apoya en la siguiente planificación temporal de tareas parciales:

	Fecha de inicio	Duración (Horas)	Fecha de entrega
Hito 3:Segunda fase de ejecución del Plan de Trabajo (PEC3).	**09/11/2022**	**100**	**06/12/2022**
Análisis del marco teórico y requisitos de un SOC.	09/11/2022	12	13/11/2022
Definición de tipos de servicios y procesos de un SOC.	13/11/2022	12	18/11/2022
Análisis de los requisitos de cada servicio.	18/11/2022	12	21/11/2022
Análisis de las métricas para cada proceso.	21/11/2022	12	24/11/2022
Definición de los flujos de trabajo de cada servicio.	24/11/2022	10	27/11/2022
Análisis de las tecnologías necesarias para un SOC.	27/11/2022	10	30/11/2022
Reunión de seguimiento con el tutor del TFM (II).	29/11/2022	1	29/11/2022
Análisis de los roles que gestionan un SOC.	30/11/2022	12	03/12/2022
Análisis de los riesgos de este hito.	03/12/2022	8	04/12/2022
Redacción y revisión de este entregable.	04/12/2022	10	06/12/2022

Tabla 4 - Planificación temporal del hito 3.

Asimismo, a continuación, se presenta el diagrama de Gantt para este tercer hito:

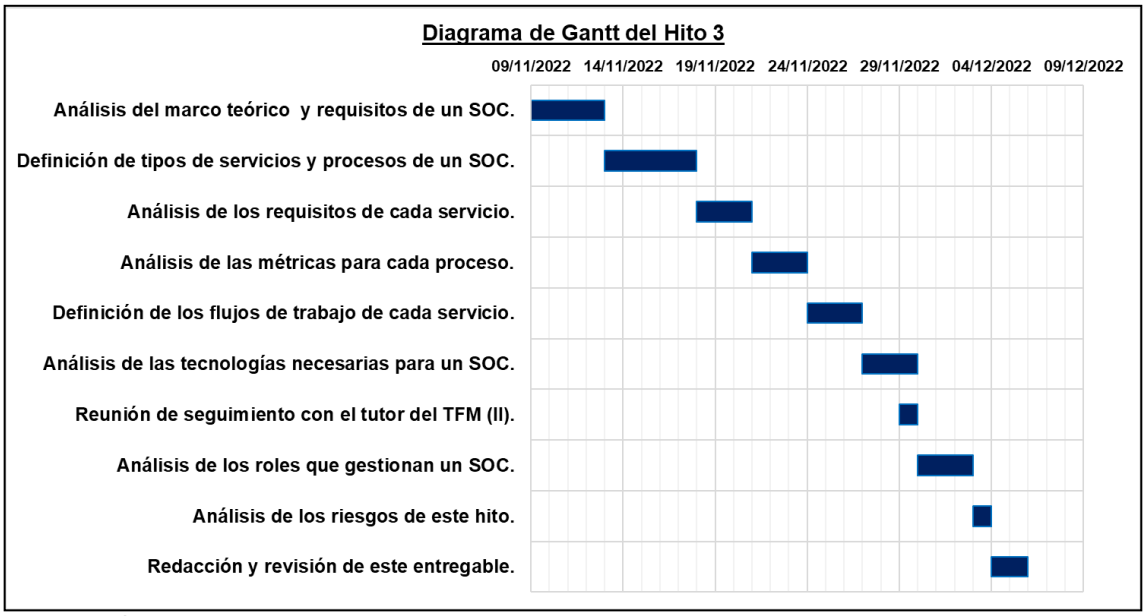

Ilustración 5 - Diagrama de Gantt del Hito 3.

Al igual que en el hito anterior, esta etapa del Trabajo alberga una fuerte carga de elaboración y análisis de elementos importantes para la implementación de un SOC, como son sus funciones, servicios y procesos, roles y tecnologías. Por tanto, como posibles riesgos fundamentales que pueden dificultar el cumplimiento de los objetivos específicos de este hito, se identifican las posibles demoras en la obtención de conclusiones y síntesis de los resultados de los análisis de los diferentes apartados. Igualmente, seguidamente, se establece una tabla, a modo de resumen, de los riesgos y las acciones mitigadores que se han considerado para este hito:

#	Riesgo	Acción mitigadora
1	Demoras en la obtención de conclusiones y síntesis de los resultados del estudio de los diferentes objetivos específicos del hito.	Reajuste de los tiempos establecidos para cada actividad.
		Consulta de artículos especializados y revisión de la bibliografía.
		Atención a los detalles.
		Reordenar los resultados y sintetizar los aspectos más relevantes.
2	Necesidad de nuevos objetivos específicos.	Ajuste del alcance del Trabajo.
		Reformulación teórica de los objetivos.
3	Exceso en la extensión de los capítulos de este hito.	Puntualizar y resumir mejor los conceptos necesarios para el entendimiento y claridad de los objetivos a cumplir y enviar a los anexos la información no esencial.

Tabla 5 - Riegos del hito 3.

1.5.4 Hito 4: Entrega de la memoria del Trabajo

El hito 4 de este Trabajo se basa en la entrega del Trabajo Final de Máster y su memoria, junto a su presentación y el documento guía para la implementación de un SOC. Además, se fundamenta en la siguiente programación temporal de tareas parciales:

	Fecha de inicio	Duración (horas)	Fecha de entrega
Hito 4: Entrega de la memoria del Trabajo.	**07/12/2022**	**84**	**10/01/2023**
Análisis y desarrollo de la guía de implementación para el SOC.	07/12/2022	20	16/12/2022
Completar las conclusiones y el glosario del TFM.	16/12/2022	8	20/12/2022
Corrección de la memoria del Trabajo.	20/12/2022	18	27/12/2022
Reunión de seguimiento con el tutor del TFM (III).	21/12/2022	1	21/12/2022
Revisión final de la memoria del trabajo.	27/12/2022	16	02/01/2023
Creación de la presentación en diapositivas.	02/01/2023	20	09/01/2023
Entrega de la memoria de trabajo.	09/01/2023	1	10/01/2023

Tabla 6 - Planificación temporal del hito 4.

Del mismo modo que en los casos anteriores, a continuación, se indica el diagrama de Gantt para este hito:

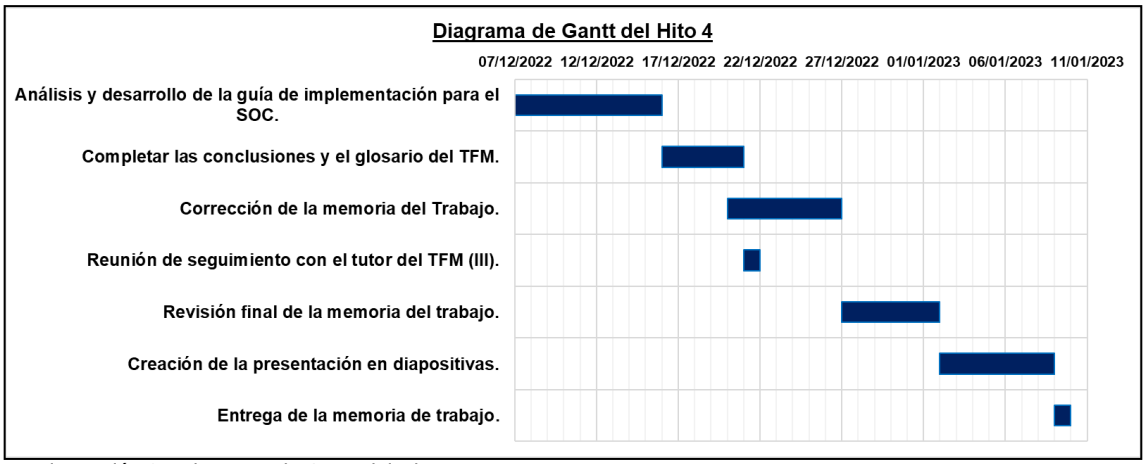

Ilustración 6 - Diagrama de Gantt del Hito 4.

1.5.5 Hito 5: Presentación en vídeo

El hito 5 de este Trabajo consiste en la presentación en vídeo del Trabajo Final de Máster y la explicación de su memoria. Por tanto, se estipula la siguiente programación temporal:

	Fecha de inicio	Duración (horas)	Fecha de entrega
Hito 5: Presentación en vídeo.	**11/01/2023**	**22**	**17/01/2023**
Revisión de las diapositivas de la presentación.	11/01/2023	10	14/01/2023
Grabación en vídeo de la presentación.	12/01/2023	12	17/01/2023

Tabla 7 - Planificación temporal del hito 5.

Seguidamente, se presenta el diagrama de Gantt para este hito:

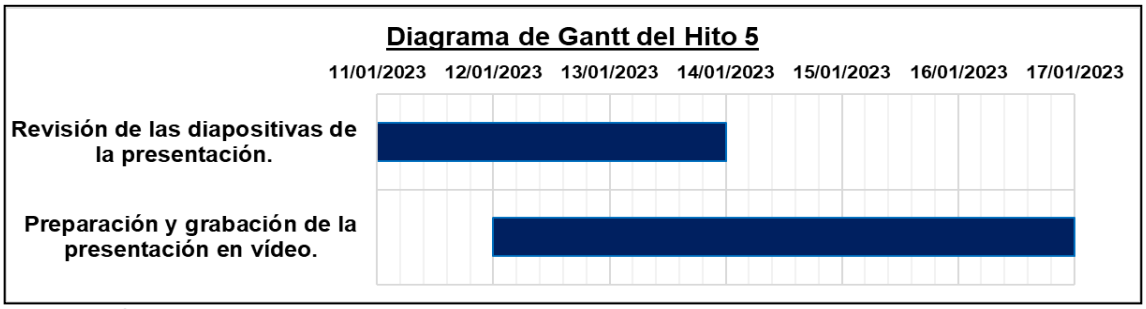

Ilustración 7 - Diagrama de Gantt del Hito 5.

1.5.6 Hito 6: Defensa virtual

El hito 6 de este Trabajo consiste en la defensa virtual del Trabajo Final de Máster ante el Tribunal. Por tanto, se presenta la siguiente programación temporal:

	Fecha de inicio	Duración (horas)	Fecha de entrega
Hito 6: Defensa virtual.	**23/01/2023**	**4**	**27/01/2023**
Preparación y realización de la defensa ante el tribunal.	23/01/2023	3	27/01/2023
Reunión de finalización del TFM con el tutor.	23/01/2023	1	27/01/2023

Tabla 8 - Planificación temporal del hito 6.

Seguidamente, también se muestra el diagrama de Gantt para este hito:

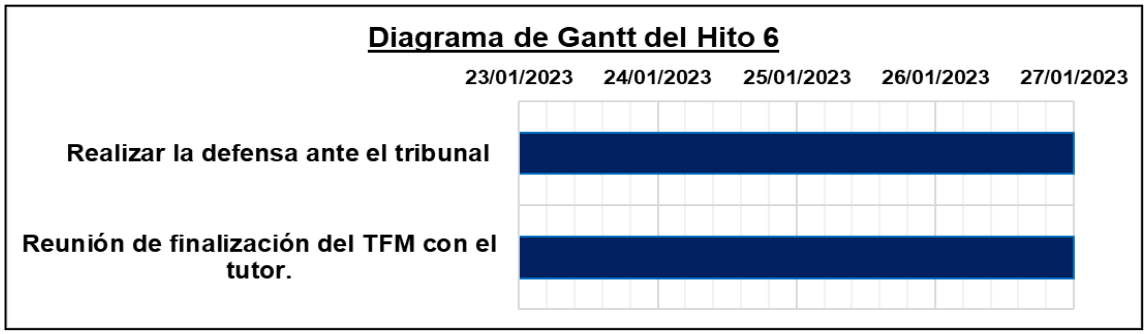

Ilustración 8 - Diagrama de Gantt del Hito 6.

1.5.7 Diagrama de Gantt completo del Trabajo Final de Máster

Finalmente, en la siguiente página se presenta el diagrama de Gantt resultante del proyecto con la unificación de todos los hitos:

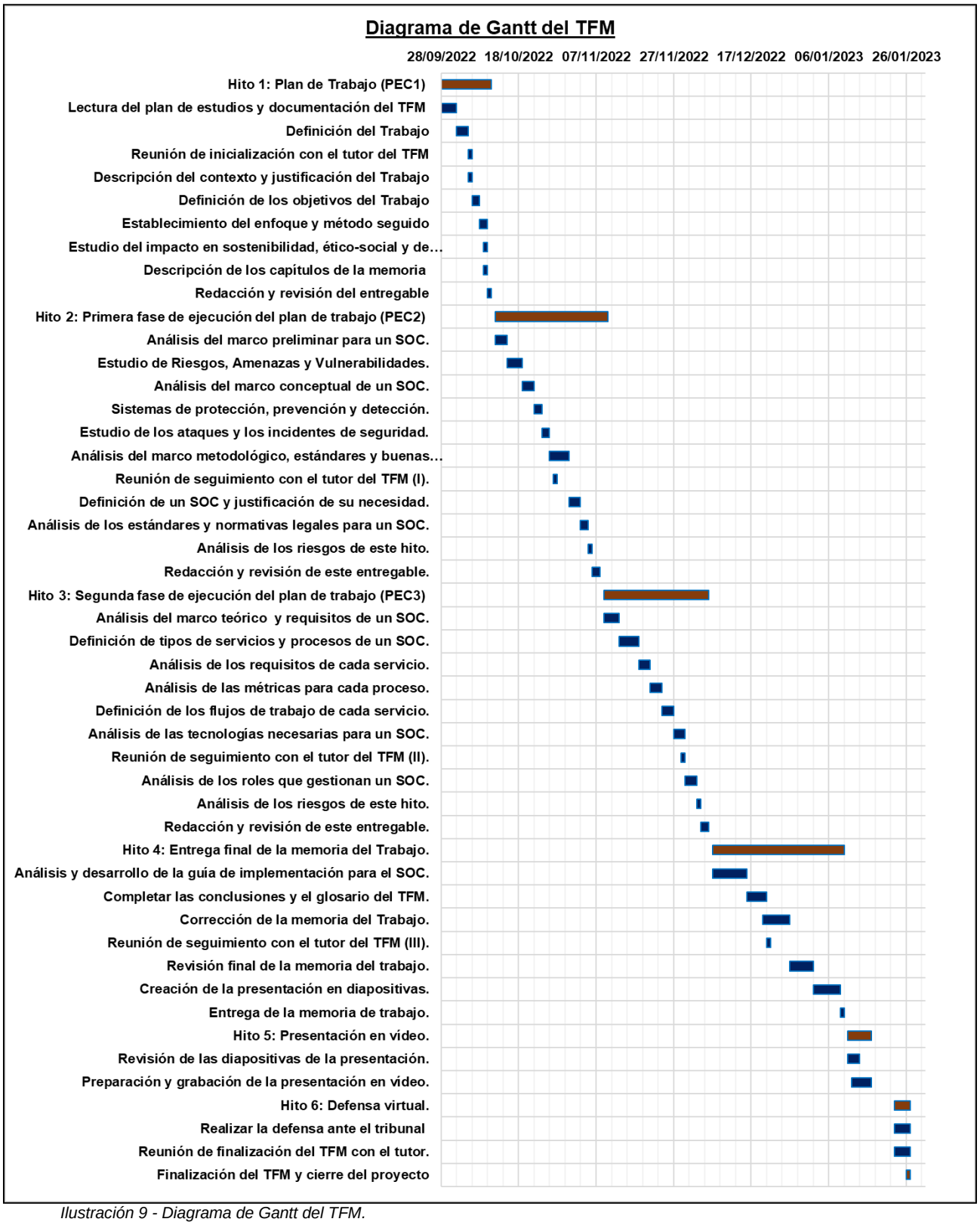

Ilustración 9 - Diagrama de Gantt del TFM.

Además, la planificación temporal completa para el proyecto es la siguiente:

	Fecha de inicio	Duración (horas)	Fecha de entrega
TFM: Guía de implementación de un SOC.	**26/02/2021**	**370**	**21/06/2021**
Hito 1: Plan de Trabajo (PEC1).	28/09/2022	70	11/10/2022
Hito 2: Primera fase de ejecución del Plan de Trabajo (PEC2).	12/10/2022	90	08/11/2022
Hito 3:Segunda fase de ejecución del Plan de Trabajo (PEC3).	09/11/2022	100	06/12/2022
Hito 4: Entrega de la memoria del Trabajo.	07/12/2022	84	10/01/2023
Hito 5: Presentación en vídeo.	11/01/2023	22	17/01/2023
Hito 6: Defensa virtual.	23/01/2023	4	23/01/2023

Tabla 9 - Planificación temporal del TFM.

1.6 Breve sumario de productos obtenidos

Tras la culminación de este Trabajo Final de Máster, se pretende haber cumplido con su objetivo principal y haber creado un documento que sirva de guía para la implementación de un SOC y que sea válido y funcional para toda aquella organización que lo pretenda. Por tanto, a continuación, se detallan los diferentes entregables que se suministrarán:

- Memoria de Trabajo del TFM.
- Guía genérica práctica y simple de implementación de un SOC (Capítulo 3 de este documento, referente a los Resultados).
- Análisis del marco preliminar y conceptual de un SOC (Anexo 1 de este documento).
- Análisis del marco metodológico y legar de un SOC (Anexo 2 de este documento).
- Análisis del marco característico de un SOC (Anexo 3 de este documento).
- Hojas de seguimiento de las diferentes fases de ejecución del Plan de Trabajo del TFM (Anexo 4 y 5 de esta memoria de trabajo).
- Presentación en diapositivas del TFM.
- Presentación en vídeo del TFM.

1.7 Breve descripción de los otros capítulos de la memoria

A continuación, se indica una breve descripción de alto nivel de los demás capítulos en los que se desarrolla este Trabajo Final:

1.7.1 Capítulo 2: Análisis del marco teórico de un SOC

En este capítulo se realizará un análisis de todo lo relacionado con el concepto de SOC y establecerá una explicación de su definición, sus tipos, sus beneficios y su razón de ser. Además, se realizará un análisis y estudio de las buenas prácticas para su diseño, de cara a su implementación. Por ello, se recopilarán y ordenarán todas las acciones que se necesiten para crear la guía final de implementación de este servicio, así como sus estrategias, planteamientos, requisitos mínimos y tipos de implementación, entre otros.

1.7.2 Capítulo 3: Resultados

En este capítulo se incluirá el documento resultante para la guía genérica práctica y simple para la implementación de un SOC, con el que se dará respuesta al objetivo principal del Trabajo.

1.7.3 Capítulo 4: Conclusiones y trabajos futuros

En este capítulo se indica el conjunto de conclusiones obtenidas del Trabajo Final. Además, se añaden las lecciones aprendidas, un análisis crítico del Trabajo, su planificación, su metodología y sus objetivos cumplidos, su reflexión ético-social, de sostenibilidad y de diversidad y una descripción de las líneas de trabajo abiertas a futuro.

1.7.4 Capítulo 5: Glosario

En este capítulo se definen los términos y acrónimos más relevantes de la Memoria de Trabajo.

1.7.5 Capítulo 6: Bibliografía

En este capítulo se reseñan las referencias bibliográficas utilizadas a modo de consulta para el desarrollo del Trabajo.

1.7.6 Capítulo 7: Anexos

En este capítulo se añaden el producto resultante del Trabajo Final y el listado de apartados que tienen un carácter autocontenido:

1.7.6.1 Anexo 1: Análisis del marco preliminar y conceptual de un SOC

En este anexo, se detallará el estudio realizado en profundidad de los conceptos más importantes de la Seguridad de la Información que se relacionan con la gestión y el funcionamiento diario de un SOC. De hecho, se facilitarán las nociones necesarias para el entendimiento de esta área o equipo de ciberseguridad.

1.7.6.2 Anexo 2: Análisis del marco metodológico y legal de un SOC

En este anexo se resumirá el análisis realizado de los estándares, normativas y metodologías internacionales y de las disposiciones legales aplicables a un SOC y sus aportes y beneficios para su implementación.

1.7.6.3 Anexo 3: Análisis del marco característico de un SOC

En este anexo se realizará un análisis de todas las características necesarias para la creación y el buen funcionamiento de un SOC. Por ello, se realizará un análisis de sus funciones, sus servicios y procesos, sus roles y sus posibles tecnologías como los elementos más importantes para su implementación.

1.7.6.4 Anexo 4: Hoja de seguimiento de la primera fase de ejecución del Plan de Trabajo del TFM

En este anexo se realizará un control de seguimiento del alcance, los objetivos, la planificación y los riesgos de las tareas realizadas hasta la primera fase de ejecución del Plan de Trabajo, así como una evaluación del trabajo elaborado en este periodo.

1.7.6.5 Anexo 5: Hoja de seguimiento de la segunda fase de ejecución del Plan de Trabajo del TFM

En este anexo se realizará un control de seguimiento del alcance, los objetivos, la planificación y los riesgos de las tareas realizadas hasta la segunda fase de ejecución del Plan de Trabajo, así como una evaluación del trabajo elaborado en este periodo.

2. Análisis del marco teórico y funcional de la implementación de un SOC

Tras realizar un análisis y estudio del marco preliminar y conceptual de un SOC[10], en donde se resumen los conceptos necesarios para la comprensión de la gestión de la Seguridad de la Información y de la ciberseguridad aplicables al funcionamiento diario de un SOC, y otro análisis y estudio del marco metodológico y legal aplicable a un SOC[11], en donde se citan y definen los estándares, normativas, metodologías internacionales y las disposiciones legales vigentes más importantes y relevantes para este equipo de ciberseguridad, a continuación, se explica y describe el significado que tiene el propio SOC, así como sus objetivos, beneficios, tipos, posibles equipos que lo integran y resto de conceptos y particularidades obtenidos del análisis y estudio de su marco teórico, con el fin de dar a entender los criterios utilizados para su guía básica de implementación.

Asimismo, de cara a la creación de un documento guía para la implementación de un SOC, también se resumen los conceptos, planteamientos, estrategias, requisitos y buenas prácticas obtenidos del análisis y estudio del marco funcional para la implementación de este área de ciberseguridad, que establece las directrices necesarias para diseñarlo e implantarlo en una organización con las garantías necesarias para que se convierta en un proceso más de negocio que la complemente y mejore su ciberseguridad.

2.1 Definición y objetivos de un SOC

Un **SOC** o Centro de Operaciones de Seguridad (*Security Operations Center*, en inglés) se define como un área, servicio o equipo profesional centralizado que se dedica a los elementos tácticos, técnicos, procedimentales y operativos relacionados con la ciberseguridad de una organización. Se trata de un servicio o una unidad técnica que se dedica a la detección y protección de los activos y sistemas de información en tiempo real y al análisis y respuesta de los eventos e incidentes de seguridad, a través de sus registros de *logs* y mediante recursos tecnológicos y humanos especializados en la materia. Por tanto, en base a su naturaleza y su finalidad, en el que, principalmente, se encuentran las características de un Equipo Azul (*Blue Team*)[12], se encarga, entre otros, de los siguientes objetivos:

- Proteger la seguridad de las propiedades de la información[13] y todos sus activos y prevenir, detectar, alertar, analizar, monitorizar y responder a los incidentes de ciberseguridad[14], a partir del uso de tecnologías y capacidades existentes e implantadas en la organización.

[10] Ver el Anexo 1: Análisis del marco preliminar y conceptual de un SOC.
[11] Ver el Anexo 2: Análisis del marco metodológico y legal de un SOC.
[12] Ver el punto 7.1.1.6 del Anexo 1 para más información sobre los diferentes equipos de Seguridad de la Información.
[13] Ver el punto 7.1.1.2 del Anexo 1 para más información sobre las propiedades de la información.
[14] Ver el punto 7.1.3 del Anexo 1 para más información sobre incidentes de ciberseguridad.

- Implantar y administrar las tecnologías de ciberseguridad, gestionar su monitorización en tiempo real y actualizar y optimizar sus configuraciones.
- Gestionar la Seguridad de la Información de los equipos de los puestos de trabajo de los usuarios, de los entornos de servidores y de todos los elementos interconectados en la red de la organización para la que desempeñen sus funciones.
- Analizar las situaciones críticas de Seguridad de la Información realizadas por auditores o por los propios equipos de ciberseguridad y contener, mitigar y/o remediar los eventos e incidentes de ciberseguridad resultantes.
- Gestionar los riesgos, las vulnerabilidades y las amenazas [15] a la ciberseguridad, en donde se debe ser capaz de minimizar la ventana de exposición de los activos de información y de permitir la detección de aquellos elementos que suponen un riesgo para la organización.
- Respetar y cumplir con todos los estándares y requisitos normativos [16] adoptados por la organización, las políticas de negocio decretadas por su alta dirección y las disposiciones legales [17] vigentes en todos sus ámbitos de aplicación, así como en la implementación de todos sus procesos y procedimientos.

2.2 Dominios fundamentales de un SOC

Tras realizar un análisis y estudio del marco característico de un SOC[18], en donde se resume el detalle de los procesos, de las tecnologías y del personal y los roles en los que se fundamenta para su estructura y constitución de los servicios mínimos que debe de prestar para su funcionamiento diario, se concluye con que todo SOC requiere de tres dominios principales en los que se apoya para garantizar el cumplimiento de sus funciones y alinearse con las diferentes áreas de una organización. Por tanto, los **principales dominios** que moldean y caracterizan un SOC, de cara a su implementación, deben ser los siguientes:

Dominios fundamentales	Descripción
Procesos[19]	Se trata del dominio que se enfoca en el detalle de los procedimientos y protocolos que se deben ejecutar para proteger, prevenir, detectar y reaccionar ante los incidentes de ciberseguridad.
Tecnologías[20]	Se trata del dominio que se enfoca en las herramientas y soluciones que se deben usar para ejecutar los procesos de monitorización y gestión de ciberamenazas, brechas e incidentes de ciberseguridad.

[15] Ver el punto 7.1.2 del Anexo 1 para más información sobre la gestión de riesgos, de vulnerabilidades y de amenazas.
[16] Ver los puntos del 7.2.1 al 7.2.14 del Anexo 2 para más información sobre las normativas y estándares más importantes de cara a un SOC.
[17] Ver el punto 7.2.15 del Anexo 2 para más información sobre las disposiciones legales para un SOC en el Estado español.
[18] Ver el Anexo 3: Análisis del marco característico de un SOC.
[19] Ver el punto 7.3.1 del Anexo 3 para más información sobre los procesos de un SOC.
[20] Ver el punto 7.3.2 del Anexo 3 para más información sobre las tecnologías necesarias para un SOC.

Personas[21]	Se trata del dominio que se enfoca en el talento humano que debe ejecutar los procesos del SOC mediante el uso de sus tecnologías, así como de definir sus competencias y su conocimiento y experiencia requerida.

Tabla 10 - Dominios fundamentales de un SOC.

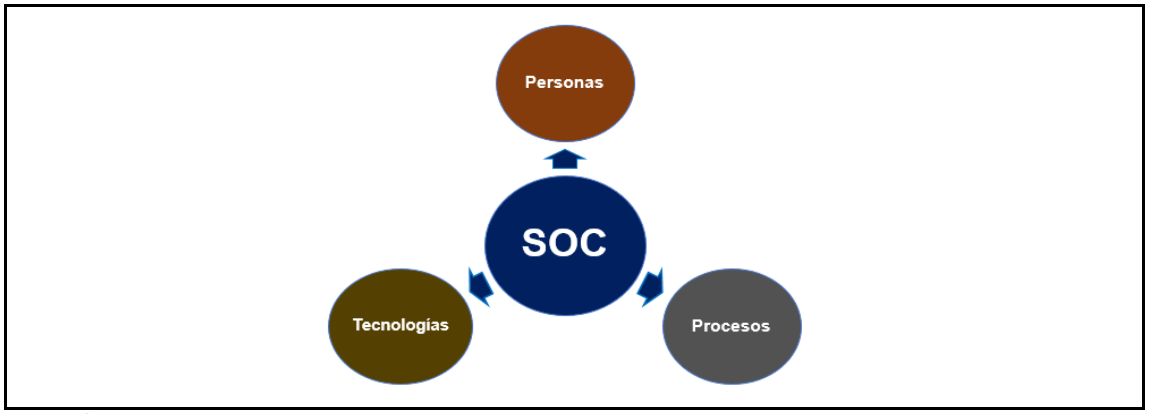

Ilustración 10 - Dominios fundamentales de un SOC.

2.3 Justificación y razón de un SOC

En materia de ciberseguridad, las organizaciones necesitan un equipo, área o servicio que se responsabilice de las actividades y procesos de negocio que prevengan los riesgos y las amenazas a las que se exponen, que detecten los incidentes y las brechas de seguridad en tiempo real y que reaccionen y respondan ante esos sucesos negativos que afecten a todos los procesos de negocio para garantizar su correcta funcionalidad. Además, para poder realizar estas labores de prevención, detección y respuesta, existen tecnologías y herramientas capaces de analizar y monitorizar todo lo que ocurre en la red de una organización y de mostrar alertas sobre sucesos no deseados, capaces de detectar fallos y vulnerabilidades en los sistemas y activos digitales de información y capaces de reaccionar ante estas detecciones, fallos y vulnerabilidades.

Sin embargo, estas tecnologías y herramientas pueden prevenir situaciones deseadas, detectar acciones legítimas y reaccionar ante sucesos intencionados y lícitos que no suponen una amenaza, como, por ejemplo, puede ser un bloqueo ante un intento de explotación de un escáner de vulnerabilidades, en donde se entiende que lo que interesa no es la protección del ataque, sino la verificación de las vulnerabilidades para intentar mitigarlas desde raíz. Este tipo de sucesos deseados por la organización, pero detectados o bloqueados por las herramientas y tecnologías de ciberseguridad se conocen como **falsos positivos**[22]. Por tanto, estas tecnologías y herramientas deben ser gestionadas, alimentadas y configuradas por recursos humanos con conocimientos en ciberseguridad y en el negocio para adaptarlas a la organización en la que desempeñen el uso de sus funciones y evitar los falsos positivos.

[21] Ver el punto 7.3.3 del Anexo 3 para más información sobre el personal y los roles de un SOC.

[22] https://es.wikipedia.org/wiki/Falso_positivo_(inform%C3%A1tica)#:~:text=Un%20falso%20positivo%20en%20inform%C3%A1tica,es%20ning%C3%BAn%20virus%20o%20malware.

En consecuencia, esta necesidad de supervisar el comportamiento de los sistemas de protección de la información justifica la necesidad de disponer de personal especializado en materia de ciberseguridad, que se organice operativamente en un equipo que vele por la seguridad de sus activos de información interconectados, los proteja de todo atacante, interno o externo, y realice una buena gestión de sus funciones para minimizar los incidentes y brechas de seguridad, así como de evitar las pérdidas económicas y de reputación que éstos puedan causar. Este equipo operativo de ciberseguridad dentro de la organización se llama SOC y cumple con todas las necesidades descritas anteriormente para justificar totalmente la inversión que una organización debe hacer para su implementación y explotación. Al fin y al cabo, realizar una buena gestión de la ciberseguridad se considera esencial para el correcto funcionamiento del negocio de toda organización y plantear la implementación de un SOC, la consecuencia de su estado avanzado de madurez en el ámbito de la ciberseguridad.

2.4 Aportaciones y beneficios de un SOC

La integración de un SOC en una organización trae consigo una serie de beneficios que, entre otros, mejoran la seguridad de sus procesos estratégicos y le aportan estabilidad funcional y firmeza en el negocio. Por tanto, algunos beneficios que aporta un SOC pueden ser:

Aportación	Beneficios
Mejora en materia de ciberseguridad	• Centralización de la gestión de la ciberseguridad. • Mejora del control de la seguridad de los activos de información. • Implantación de protocolos de protección, prevención, detección y respuesta de ciberseguridad. • Registro de incidentes de ciberseguridad, evidencias y acciones realizadas. • Mejora de la experiencia organizacional en materia de ciberseguridad.
Eficacia operativa	• Definición de políticas, planes, guías y protocolos de ciberseguridad. • Mejora de las reglas de detección de amenazas. • Prevención y respuestas más ágiles ante posibles amenazas y riesgos. • Inteligencia y análisis rápido de ciberamenazas. • Mejora de la coordinación de investigaciones por eventos de ciberseguridad.

Eficacia tecnológica	• Mejora de las herramientas y tecnologías de ciberseguridad. • Conocimiento y experiencia de tecnologías en materia de ciberseguridad. • Mejora de las configuraciones y reglas de detección. • Mejora de los recursos tecnológicos. • Mejora de la visibilidad del tráfico de red a nivel de ciberseguridad.
Reacción ante amenazas, brechas e incidentes de ciberseguridad.	• Paso de actitud reactiva a una proactiva. • Implantación de estrategias de defensa anticipada. • Disminución de esfuerzos para perseguir las amenazas por detecciones tempranas. • Respuesta ante incidentes en tiempo real.
Minimización de los riesgos	• Disminución de la probabilidad de que se materialicen amenazas. • Reducción de los tiempos de indisponibilidad. • Protección de la información interconectada en la red.
Reducción de los costes a largo plazo	• Disminución de los costes de medidas de seguridad a largo plazo por implantaciones apropiadas para un determinado fin. • Disminución de los costes por equipamiento o licenciamiento innecesario. • Minimización de los costes por daños causados en el negocio por incidentes de ciberseguridad. • Minimización de los costes por incumplimientos legales causados por brechas de ciberseguridad.
Cumplimiento de las normativas	• Capacitación de la Política de Seguridad de la Información. • Monitorización del uso correcto de las regulaciones y normativas de la organización y legalidad vigente. • Centralización del seguimiento operativo de la ciberseguridad.

Tabla 11 - Beneficios de un SOC.

Asimismo, tener esta área de ciberseguridad, requiere de un coste que supone algunos inconvenientes con los que se tiene que lidiar en la organización para conseguir su mayor eficacia y no exceder su alcance fuera de sus competencias. Entre éstos, se pueden observar los siguientes:

- No se trata de una solución barata, sino que requiere un gasto inicial bastante elevado, aunque a la larga se reduzcan los costes.
- No se trata de una solución de negocio global, sino que requiere de los demás procesos de negocio para su correcto funcionamiento.
- Se trata de una solución intrusiva, por lo que puede afectar al funcionamiento de los activos de información de la organización.
- Se requiere de supervisión constante del cumplimiento de contratos y niveles de servicio por externalizar el SOC y/o por el soporte de las herramientas y tecnologías de ciberseguridad.

2.5 Modelos de SOC

Las organizaciones que deseen implantar un SOC entre sus diferentes áreas operativas de su gestión, deben tener en consideración los diferentes modelos de SOC existentes para, en base a su tipo negocio, estructura y tamaño, entre otros factores de interés, poder diseñar e implementar el que más de adecúe a sus intereses estratégicos. Por tanto, entre otros posibles, existen los diferentes modelos:

Modelos de SOC	Descripción
SOC dedicado	Se trata del SOC que se autogestiona por la propia organización y que cuenta con instalaciones dedicadas dentro del área corporativa, personal propio a tiempo completo y un intervalo de operación de 24x7.
SOC distribuido	Se trata del SOC que se cogestiona entre la propia organización y un proveedor externo de servicios de seguridad gestionados (MSSP[23]), que cuenta con parte del personal propio a tiempo completo y parte a tiempo parcial y que se dedica al cumplimiento de sus funciones en un intervalo, generalmente, menor al de 24x7, como podría ser el 8x5.
SOC gestionado	Se trata del SOC que se gestiona por un proveedor externo de servicios de seguridad gestionados (MSSP), que cuenta con sus propias instalaciones y su propio personal y que se dedica al cumplimiento de sus funciones en el intervalo en el que se haya contratado por la organización que lo requiere.
SOC multifuncional	Se trata del SOC que se cogestionado en la propia organización y que cuenta con instalaciones dedicadas dentro del área corporativa y personal propio a tiempo completo que realiza las funciones del SOC como de otras áreas operativas, como puede ser de NOC.
SOC global	Se trata del SOC que gestiona y coordina de manera global los diferentes SOC que tenga una organización entre sus filiales y que facilita información sobre inteligencia de ciberamenazas y experiencia en ciberseguridad sin participar en el ejercicio de sus funciones operacionales.
SOC fusionado	Se trata del SOC avanzado que se autogestiona por la propia organización, que supervisa todas sus iniciativas en el ámbito de la ciberseguridad y que cuenta con las mismas características que un SOC dedicado, pero con funciones sofisticadas, como pueden ser la inteligencia de amenazas o la tecnología operativa, y con la colaboración de otras áreas como las de Operaciones, DevSecOps y/o Desarrollo.
SOC virtual	Se trata del SOC que se gestiona desde la propia organización o por un proveedor externo de servicios de seguridad gestionados (MSSP) y que no cuenta ni instalaciones dedicadas ni personal propio a tiempo completo, sino que se activa de manera reactiva ante un incidente o brecha de seguridad y en un intervalo de operación que puede ser de 24x7 o de cualquier otro rango.

[23] https://secuora.es/blog/que-es-un-mssp-o-proveedor-de-servicios-de-seguridad-gestionados/

SOC como Servicio (SOCaaS)	Se trata del SOC que se gestiona a través de una suscripción a un proveedor externo de servicios de seguridad gestionados (MSSP) o a un programa software contratado en la nube, que cuenta con sus propios recursos y opera con las funciones acordadas para prestar el servicio en el intervalo pactado.

Tabla 12 - Modelos de SOC.

2.6 Desafíos y riesgos de un SOC

Tras los temas de más actualidad de los últimos años, como la pandemia por la COVID-19 y la guerra entre Rusia y Ucrania, así como debido a sus roles de protección, prevención, detección y respuesta, los SOC se han convertido con más fuerza en el epicentro de la ciberseguridad de las organizaciones. Diariamente, se enfrentan a diferentes riesgos que le convierten en una fuerza necesaria para mantener protegidos los activos de información de sus organizaciones y su información confidencial, sensible y privada. Por tanto, estos equipos de ciberseguridad deben identificar y valorar los riesgos para afrontarlos con éxito y mejorar continuamente su gestión de equipo y protección de la organización.

Debido a esto, como en todos los proyectos y servicios operativos, los SOC se enfrentan a desafíos comunes en las organizaciones que les afectan y pueden llevarles al fracaso parcial o total del cumplimiento de sus funciones. Algunos de estos riesgos pueden ser los siguientes:

- Carencia de compromiso de la dirección de la organización y/o del SOC.
- Errores en la gestión del propio SOC.
- Carencia de implicación de los usuarios.
- Ausencia de conocimiento técnico por parte del personal del SOC.
- Errores de configuración o estabilidad de la tecnología.
- Relaciones deficientes con otros departamentos operativos.
- Carencia de supervisión del equipo del SOC.
- Ausencia de dedicación del responsable del SOC.
- Reuniones de seguimiento y control largas y tediosas.
- Documentación insuficiente de progreso y seguimiento.
- Errores de dimensionamiento de los recursos y del tiempo.
- Errores en la gestión de roles y responsabilidades del personal del SOC.
- Ambientes de trabajo tóxico.
- Ausencia de comunicación en el propio SOC o con los clientes.
- Errores en la identificación y análisis de los riesgos.
- Errores en la definición del alcance y complejidad del SOC.

Igualmente, a continuación, se indican los desafíos más importantes a los que se enfrentan los diferentes SOC de manera generalizada junto a algunas de sus posibles soluciones:

Desafíos de un SOC	Detalles
Aumento de las amenazas de ciberseguridad	**Riesgo principal:** Debido al avance de las tecnologías, la mejora del ingenio de los atacantes de ciberseguridad, al incremento del trabajo en remoto y a la falta de información provocada por la pandemia de la COVID-19, el número de amenazas a la seguridad de los activos de información de una organización ha aumentado considerablemente en número y en complejidad.
	Posibles soluciones: • Mejora de las tecnologías de ciberseguridad. • Capacitación continua en materia de ciberseguridad a todo el personal de la organización. • Formación continua al personal del SOC. • Mejora e incremento de las verificaciones, alertas y configuración de la monitorización de eventos de ciberseguridad.
Aumento de las alertas de ciberseguridad	**Riesgo principal:** Debido al aumento de las amenazas de ciberseguridad y a los intentos de los SOC de paliar esta problemática, reciben más eventos de ciberseguridad por segundo (EPS) desde las diferentes tecnologías y trabajan con más chequeos de esos eventos desde los sistemas de monitorización y más alertas sobre las detecciones de sucesos no deseados en los activos de información de la organización. Sin embargo, esto provoca que el número de alertas de ciberseguridad pueda crecer hasta el punto en el que no sea sostenible para el SOC y sólo no pueda atender todas las alertas, sino que se le puedan escapar alertas críticas mientras se atienden otras alertas.
	Posibles soluciones: • Determinar una priorización automática de las alertas de ciberseguridad que se base en el análisis dinámico de los eventos anómalos. • Asumir el riesgo de no atender las alertas no consideradas como importantes o con priorización baja. • Redimensionar el personal del SOC para asumir la carga.

Gestión de múltiples tecnologías de ciberseguridad	**Riesgo principal:** Debido al incremento de las amenazas de ciberseguridad y la complejidad de los ciberataques, las organizaciones cada vez incluyen más herramientas y sistemas que las protejan en sus diferentes vectores de ataque[24], por lo que los SOC cada vez se encuentran con más fuentes de análisis y más eventos que monitorizar y analizar, lo que puede provocar que su personal no sea capaz de abarcar la supervisión de todas estas tecnologías y se puedan escapar eventos e incidentes de ciberseguridad graves.
	Posibles soluciones: • Determinar una priorización de las tecnologías a supervisar. • Centralizar los eventos de todas las tecnologías en un único visor que los correlacione y priorice. • Asumir el riesgo de no atender los eventos de todas las tecnologías. • Redimensionar el personal del SOC para asumir la carga.
Escasez de experiencia en materia de ciberseguridad	**Riesgo principal:** Debido a las necesidades de protección, prevención, detección y respuesta ante amenazas e incidentes de ciberseguridad y a la evolución de las ciberamenazas y sus ciberataques, las organizaciones intentan destinar cada vez más personal a las actividades y tareas que realizan los SOC, así como añadir nuevos servicios, actividades y tareas más complejas que las que ya se realizan. Sin embargo, la experiencia en ciberseguridad no se encuentra con facilidad en el personal de la organización que no se haya dedicado a esta materia y las nuevas habilidades tampoco se adquieren sin formación y práctica, por lo que puede suponer un problema de crecimiento y mejora continua en materia de ciberseguridad para las organizaciones.
	Posibles soluciones: • Formar y capacitar al personal a destinar al SOC antes de asignarle actividades de ciberseguridad y al personal existente en el SOC sobre aquellas tareas complejas que se quieran añadir. • Automatizar procesos para facilitar la integración de nuevo personal y nuevas tareas. • Contratar personal formado en las actividades complejas que se quieran añadir al SOC o subcontratar el servicio a MSSP.

[24] https://keepcoding.io/blog/que-es-un-vector-de-ataque-en-ciberseguridad/

Control de las cargas de trabajo del personal	**Riesgo principal:** Debido al confinamiento mundial por la COVID-19 en el año 2020, las organizaciones se han adaptado a nuevas formas de trabajo, en donde se destacan el trabajo en remoto y las reuniones virtuales. Sin embargo, de manera genérica, estas organizaciones no han desarrollado ni actualizado los procesos de gestión y balanceo de cargas de trabajo del personal de los SOC, sino que han sobrevivido a las circunstancias y han medido los resultados obtenidos de manera grupal sin observar individualmente al personal. Por tanto, existe la posibilidad de que provoque que una parte del equipo se sature con el trabajo que asume y la otra se desmotive por no recibir el suficiente trabajo.
	Posibles soluciones: • Atender a las actividades y tareas que realiza cada recurso humano del SOC. • Realizar una tarea de reparto (*dispatcher*) de actividades para balancear la carga de trabajo y las propias actividades entre el personal del equipo. • Vigilar la salud mental del personal del SOC (estrés, agonía, aburrimiento, motivación…) y remediar cualquier inconveniente que se detecte.
Automatización de tareas y actividades básicas y comunes	**Riesgo principal:** Debido al aumento de las alertas de ciberseguridad, los analistas de los SOC necesitan más tiempo para poder analizar los eventos alertados y determinar los diferentes tipos de casos que se detecten, entre los que se destacan los más repetitivos, que requieren siempre de las mismas acciones de contención, mitigación o solución. Esto puede provocar que, por una parte, el personal se aburre y desmotive por realizar tareas repetitivas y, por otra, que se dejen de atender casos críticos por saturación de tareas monótonas.
	Posibles soluciones: • Analizar las diferentes alertas de ciberseguridad y automatizar todas aquellas que sean repetitivas en cuanto a las acciones a realizar. • Automatizar una priorización de las alertas de ciberseguridad que se base en el análisis dinámico de los eventos alertados. • Automatizar las tareas más administrativas del análisis de los eventos alertados, como la obtención de la información de contexto de los *IoC* o la escritura de esta información obtenida en las herramientas de gestión de *ticketing*.

Retención del talento	**Riesgo principal:** Debido a la aparición del trabajo en remoto como una nueva forma de trabajo masivo en las organizaciones, el personal del SOC y de cualquier ámbito, entre otros factores, tiene la facilidad de encontrar proyectos más enriquecedores para su desarrollo profesional y/o mejores condiciones en otras entidades en las que puede desarrollar sus actividades desde el mismo lugar en el que lo realiza actualmente (en remoto), por lo que retener al personal y su talento puede resultar bastante complicado.
	Posibles soluciones: • Mejora de las condiciones al personal, en donde no sólo se valoren los factores económicos, sino también motivacionales, con horarios flexibles y personales. • Formación en ámbitos de la informática, las telecomunicaciones, la ingeniería en general, la ciberseguridad y los idiomas con certificaciones o formación reglada, en donde se puedan crear contratos de permanencia. • Atender a las necesidades de crecimiento profesional del personal del SOC.

Tabla 13 - Desafíos a los que se enfrenta un SOC.

2.7 Funciones que realiza un SOC

La estrategia global de un SOC se debe focalizar, principalmente, en la gestión de las ciberamenazas[25] de una organización y en la resolución de sus incidentes de ciberseguridad[26], a través de la protección de sus activos de información, la prevención los riesgos que le supongan, la detección de las que han conseguido ser explotadas y la respuesta ante esa explotación por convertirse en posibles incidentes de ciberseguridad. Por este motivo, entre las funciones básicas de un SOC, se encuentran las siguientes:

Funciones básicas	Descripción
Monitorización de las redes y los activos	Se trata de la supervisión continua de los diferentes elementos interconectados en la red de la organización para detectar amenazas de ciberseguridad mediante las diferentes herramientas, sistemas y automatismos de Seguridad de la Información de la organización.
Detección y reacción de incidentes de ciberseguridad	Se trata del descubrimiento de sucesos no deseados que pueden poner en riesgo la Seguridad de la Información de una organización y su análisis y reacción ante las consecuencias que éste pueda tener.
Descubrimiento y mantenimiento de los activos	Se trata del control de todos los sistemas, herramientas y tecnologías que posee la organización para descubrir y reaccionar ante cualquier intruso y para verificar, gestionar y actualizar los activos inventariados.

[25] Ver el punto 7.1.2.4 del Anexo 1 para más información sobre la gestión de las ciberamenazas.
[26] Ver el punto 7.1.3 del Anexo 1 para más información sobre incidentes de ciberseguridad.

Gestión de las vulnerabilidades	Se trata de la verificación continua, identificación y el análisis sistemático de las debilidades y errores de los diferentes activos de información de una organización, con el fin de parchearlos y mitigarlos o solventarlos.
Mantenimiento de los registros *logs* de los activos	Se trata del almacenamiento de todo el historial de comunicaciones y actividades que realizan los diferentes activos de información de una organización para localizar las acciones que han podido ser el origen de un suceso sospechoso o una anomalía.
Categorización de las alertas	Se trata de la clasificación de la criticidad de las alertas que se detecten por eventos o incidentes de ciberseguridad en base a su potencial impacto y gravedad en los activos de información, con el fin de tratar las más críticas y urgentes antes que las demás.
Gestión de la tecnología de ciberseguridad	Se trata de la implementación, administración, supervisión y mantenimiento de las herramientas, sistemas y aplicaciones de Seguridad de la Información con las que se protegen los activos de información de una organización, se previenen, detectan y reaccionan ante las amenazas de ciberseguridad para su correcto uso y funcionamiento.
Gestión de copias de seguridad	Se trata de la administración, mantenimiento, almacenaje y ejecución de las copias de seguridad de los datos más importantes de los activos de información de una organización, con el fin de poder recuperar cualquier activo afectado por un incidente de seguridad mediante la información correcta que ha sido almacenada cuando no se encontraba afectado.
Gestión del cumplimiento normativo	Se trata del control y seguimiento del cumplimiento de los estándares y requisitos normativos y legales adoptados por la organización, sus políticas de negocio y la implementación de todos sus procesos y procedimientos al respecto

Tabla 14 - Funciones básicas de un SOC.

Asimismo, con el paso del tiempo y el trabajo diario, la organización y los diferentes Equipos de Seguridad de la Información[27] adquieren más experiencia y, por consiguiente, mayor grado de madurez. Por tanto, además de las funciones básicas, los diferentes SOC también pasan a realizar funciones más avanzadas que le conceden más responsabilidades, mayor criterio y más reputación dentro de la propia organización. Por tanto, entre las funciones avanzadas más importantes para un SOC, se pueden señalar las siguientes:

Funciones avanzadas	Descripción
Creación de controles, políticas y directrices de ciberseguridad	Se trata del desarrollo y establecimiento de procedimientos y políticas de ciberseguridad en una organización para determinar lo que se considere aceptable y lo que no y para indicar los pasos a seguir ante una situación concreta de este ámbito.

[27] Ver el punto 7.1.1.6 del Anexo 1 para más información sobre los diferentes equipos de Seguridad de la Información

Monitorización del comportamiento de los activos	Se trata de la supervisión continua del comportamiento de todos los elementos interconectados en la red de la organización para establecer medidas reactivas o proactivas ante sucesos extraños o no deseados. Debido a esto, se debe realizar un estudio previo de las actividades que realizan esos activos de información para controlar sus actividades y valorar las que se puedan considerar sospechosas.
Formación interna en materia de ciberseguridad	Se trata de la enseñanza y concienciación en materia de ciberseguridad a los usuarios internos y externos intervinientes de una organización ante las diferentes situaciones que pueden poner en peligro su información y la de la propia organización.
Inteligencia de ciberamenazas	Se trata de la identificación, monitorización y rastreo de indicadores de compromiso (*IoC*)[28] que pueden indicar una potencial amenaza de ciberseguridad en alguno de los activos de información de una organización.
Notificación precoz de vulnerabilidades y amenazas	Se trata de la detección, alerta y comunicación de debilidades e indicadores de compromiso (*IoC*) que pueden indicar una potencial amenaza de ciberseguridad en un estado inicial, antes de que se pueda producir una amenaza o suceso no deseado, en alguno de los activos de información de una organización.
***Service Desk* de ciberseguridad**	Se trata del conjunto de recursos, herramientas y personal humano que realiza las tareas de recepción y diagnóstico inicial de los problemas de ciberseguridad notificados por los usuarios a la organización para su tramitación con el SOC u otro departamento operativo de Seguridad de la Información de la organización.
Cibervigilancia de activos de información digitales	Se trata de la monitorización continua de información de los activos y datos de una organización en las redes interna (por segmentación) y externa (Internet) para detectar fugas de información y brechas de ciberseguridad.
Análisis forense de Seguridad de la Información	Se trata de la identificación, recuperación y estudio de los datos de los activos de información de una organización para obtener algún tipo de información desconocida, dañada, perdida o que puede haber constituido algún tipo de delito.

Tabla 15 - Funciones avanzadas de un SOC.

2.8 Áreas centrales de servicios de un SOC

La gestión de la ciberseguridad requiere de una serie de servicios y actividades para garantizar un nivel de seguridad adecuado. Por ello, todo SOC debe establecer un Plan de Servicios que defina todos los servicios, procesos y funciones que se prestan a la organización de manera estructurada en diferentes dominios. Estos dominios se conocen como **Áreas centrales de servicios** y, como mínimo, de manera generalizada, se deben establecer los siguientes:

[28] https://www.cronup.com/la-importancia-de-los-indicadores-de-compromiso-ioc-en-la-ciberseguridad/

Áreas centrales de SOC	Descripción
Área de gestión de eventos de ciberseguridad **(*Cybersecurity Events and Incidents Management Area*)**	Se trata del área del SOC que engloba los mecanismos de detección y respuesta[29] ante ciberincidentes y los servicios de monitorización, de análisis de los eventos de seguridad y de análisis, contención, mitigación y remediación. Sus principales procesos pueden ser: • Monitorización y detección de eventos e incidentes de ciberseguridad. • Análisis de eventos e incidentes de ciberseguridad. • Coordinación de la gestión de los eventos e incidentes de ciberseguridad. • Presentación de informes de incidentes de ciberseguridad. • Análisis de artefactos y pruebas forenses. • Mitigación de las ciberamenazas y recuperación de los servicios afectados. • Soporte a la gestión de crisis de ciberseguridad.
Área de gestión de riesgos y vulnerabilidades **(*Risk and Vulnerability Management Area*)**	Se trata del área del SOC que engloba los mecanismos de prevención [30] y los servicios de análisis de riesgos y debilidades, así como la generación y procesado de sus informes. Sus principales procesos pueden ser: • Descubrimiento e investigación de vulnerabilidades y riesgos. • Presentación de informes de vulnerabilidad y riesgos. • Coordinación de la gestión de las vulnerabilidades y riesgos. • Análisis de las vulnerabilidades y riesgos. • Comunicación de las vulnerabilidades y riesgos. • Reacción y respuesta ante las vulnerabilidades y riesgos.
Área de gestión de la transferencia de conocimientos **(*Knowledge Transfer Management Area*)**	Se trata del área del SOC que engloba los mecanismos de formación y los servicios de capacitación, educación y sensibilización del personal de la organización, sus usuarios, clientes y asociados. Sus principales procesos pueden ser: • Concienciación y sensibilización en materia de ciberseguridad. • Formación y educación sobre Seguridad de la Información. • Ejercicios de ciberseguridad • Asesoramiento técnico, normativo y legal en materia de ciberseguridad.

[29] Ver el punto 7.1.4.3 del Anexo 1 para más información sobre los mecanismos de detección y respuesta.
[30] Ver el punto 7.1.4.2 del Anexo 1 para más información sobre los mecanismos de prevención.

Área de gestión del Estado actual **(*Situational Awareness Management Area*)**	Se trata del área del SOC que engloba los mecanismos de notificación y alerta y los servicios de obtención y análisis de datos. Sus principales procesos pueden ser: • Adquisición y recolección de datos e información. • Análisis y síntesis de datos e información • Comunicación y reporte de la actualidad de la ciberseguridad de la organización.

Tabla 16 - Áreas centrales de un SOC.

Por consiguiente, en base a estas áreas centrales de servicios, de acuerdo con la alta dirección de la organización en la que se desee implementar un SOC y en consideración con los recursos con los que se cuente, la persona responsable del SOC debe decidir, definir y validar los servicios se deben prestar para cumplir con los objetivos de ciberseguridad del negocio en la organización. Además, estos servicios se deben cumplir según los acuerdos de nivel de servicio (ANS o SLA)[31] y se deben mejorar continuamente según los reportes de actualidad detectados en auditorías y avances de las amenazas, la tecnología y las investigaciones.

2.9 Estrategias para definir un SOC

Toda organización que desee poder prevenir, detectar y reaccionar ante incidentes de ciberseguridad necesita diseñar e implementar un SOC que le garantice la gestión de estas actividades. Por tanto, para poder ponerlas en funcionamiento y bajo la responsabilidad de este equipo de ciberseguridad, necesitan **definir correctamente su paradigma estratégico** de Seguridad de la información para que alineen la ciberseguridad con sus estrategias de negocio y diseñen la Política de Seguridad de la Información y los Planes de gestión de ciberseguridad. De hecho, deben ser capaces de seleccionar una estrategia de ciberseguridad para que les garantice la protección de sus activos de información y que, a su vez, puedan servirles para el diseño del SOC, de cara a su implementación.

A continuación, se presentan algunas de las estrategias más utilizadas por los responsables de Seguridad de la Información de las organizaciones:

- **Estrategias de ciberseguridad por permisos y registros:**

Estrategias	Descripción
Promiscua	Estrategia que permite el acceso y uso de los recursos, pero que apenas los registra.
Permisiva	Estrategia que permite el acceso y uso de los recursos, salvo los bloqueados manualmente, y que los registra todos.
Prudente	Estrategia que no permite todos los accesos ni uso de los recursos, pero que conoce y registra todo lo que sucede.
Paranoica	Estrategia que bloquea todos los accesos y usos de los recursos, salvo los permitidos manualmente, y que los registra todos.

Tabla 17 - Estrategias de ciberseguridad por permisos y registros.

[31] https://es.wikipedia.org/wiki/Acuerdo_de_nivel_de_servicio

- **Estrategias de ciberseguridad por aceptación/denegación**:

Estrategias	Descripción
Aceptación por defecto	Estrategia que permite todo lo que no se prohíbe explícitamente.
Denegación por defecto	Estrategia que prohíbe todo lo que no se permite explícitamente.

Tabla 18 - Estrategias de ciberseguridad por defecto.

Por consiguiente, las organizaciones deben definir, en primer lugar, su estrategia en materia de Seguridad de la Información para, más tarde, de forma consecuente, suministrar la infraestructura conveniente para el funcionamiento del SOC. Además, esta estrategia de Seguridad de la Información depende de lo que la organización desee proteger y de los intervalos de tiempo en los que lo desee proteger para realizar una inversión acorde a sus necesidades de negocio. Esto quiere decir que la implementación de un SOC depende de las necesidades de la organización, de su tamaño y de sus requisitos, por lo que el primer paso, antes de iniciar el diseño del SOC que se desee implantar consiste en analizar las necesidades, el funcionamiento, las capacidades de los procesos y los objetivos de la organización.

Asimismo, una vez se hayan analizado las características de la organización y se comience a diseñar el SOC, se considera importante que se establezca un programa de cooperación y comunicación que alinee las diferentes áreas de una organización y sus responsabilidades, procesos, productos y procedimientos vigentes para garantizar el correcto funcionamiento de sus operaciones de ciberseguridad. Por tanto, la organización debe atender a los diferentes dominios o factores importantes que moldean y caracterizan un SOC para implementar correctamente esta área de ciberseguridad bajo sus intereses de negocio.

2.10 Tipos de implementaciones de un SOC

Al igual que ocurre con los diferentes modelos para la Gestión de la Seguridad de la información[32], toda organización que requiera de la integración y explotación de un SOC para realizar una gestión de su ciberseguridad acorde a sus requisitos básicos de negocio, puede plantear diferentes tipos de implementaciones:

2.10.1 Implementación de un SOC interno

Se trata de la implementación de esta área operativa de ciberseguridad dentro de la propia estructura jerárquica de la organización y en conjunción con sus procesos de negocio, por lo que requiere de, entre otros, las siguientes características para garantizar su correcta integración:

[32] Ver el punto 7.1.1.4 del Anexo 1 para más información sobre los tipos de Gestión de la Seguridad de la información.

- Contratación de personal capacitado y experimentado en materia de ciberseguridad para los diferentes niveles del SOC.
- Definición del marco metodológico y de la estrategia por el que se rige el funcionamiento del SOC.
- Asignación presupuestaria para la implementación, mantenimiento y mejora continua del SOC, sus herramientas y personal humano.
- Definición de los servicios y procesos de negocio del SOC.
- Definición de los protocolos de asignación, clasificación y respuesta ante incidentes de ciberseguridad.

2.10.2 Implementación por contratación de un SOC externo

Se trata de la implementación de esta área operativa de ciberseguridad en los procesos de negocio de una organización mediante el contrato del servicio a una organización externa que realice las funciones de gestión de la ciberseguridad, por lo que requiere de, entre otros, las siguientes características para garantizar su correcta integración:

- Definición de las métricas necesarias para el control de las actividades de la organización externa para con la interna.
- Definición del traspaso de registros, datos e información de la organización interna para la explotación de la organización externa.
- Establecimiento de los protocolos de actuación de la organización externa con la información obtenida y correlacionada de la organización interna.
- Definición de procesos para el traspaso y visualización de información detallada sobre el estado de la ciberseguridad de manera continuada de la organización externa a la interna.
- Definición de los acuerdos de nivel de servicio (SLA) que debe cumplir la organización externa sobre la interna.
- Establecimiento del intervalo de presentación y entrega de los diferentes tipos informes ejecutivos, técnicos y funcionales sobre el servicio prestado por la organización externa.
- Definición de los protocolos de gestión, notificación y registro de todos los análisis, investigación, evidencias y actividades realizadas en los incidentes de ciberseguridad por la empresa externa sobre los activos de información de la organización interna.

2.11 Cuestiones previas a la implementación de un SOC

Toda organización que desee ser capaz de detectar y reaccionar ante incidentes de ciberseguridad, debe plantearse la implementación de un SOC. Por tanto, para llevar a cabo este hecho, una vez se han definido las estrategias que se desean implantar en materia de ciberseguridad, gracias a sus necesidades y requerimientos, se necesitan plantear una serie de cuestiones necesarias para acotar el alcance del proyecto y, con sus respuestas, conocer su nivel actual de ciberseguridad para guiar el diseño del SOC. A continuación, se exponen algunas de las cuestiones e incógnitas más importantes a realizar antes de la implementación de un SOC:

Cuestiones previas para crear un SOC	Descripción
¿Cuáles son las prioridades en materia de ciberseguridad?	Se necesita que se responda a las preocupaciones de la organización por la que desea la implementación de un SOC y se indique si su objetivo principal se centra en la protección de los activos de información, en el cumplimiento normativo y legal, en su propio modelo de negocio o en otro aspecto.
¿Con qué condiciones cuenta la organización para destinar a la ciberseguridad?	Se necesita que se responda a las condiciones presupuestarias, tecnológicas, de personal y de infraestructura de las que dispone la organización para invertir en ciberseguridad. Por tanto, se requiere que se indique si dispone de suficiente presupuesto para acometer el proyecto de implementación de un SOC, si cuenta ya con tecnología actual de ciberseguridad para su uso y si dispone de personal especializado en esta materia.
¿Qué necesidades del ámbito de la ciberseguridad tiene la organización?	Se necesita que se responda a los requisitos más importantes de la organización y se indique, en base a las condiciones con las que ya cuenta, si necesita algún equipamiento tecnológico concreto, algún un tipo de rol específico para su personal o realizar pruebas de penetración[33], por ejemplo.
¿Qué tipo de implementación y formato de SOC se quiere desarrollar?	Se necesita que se responda a si se desea implementar un SOC interno[34], con toda la información en la infraestructura corporativa, o un SOC externo[35], con la información en un proveedor de servicios, así como que se indique el modelo de SOC[36] que se quiere desarrollar.
¿Qué disponibilidad y horarios de actividad se requieren para la ciberseguridad?	Se necesita que se responda al tipo de servicio que se requiere para la protección de los activos de información de una organización y se indique si se requiere 24x7, 8x5 u otro formato en horas x días de la semana.
¿Qué activos de información debo proteger?	Se necesita que se responda al tipo de activos de información que se necesita proteger para garantizar la seguridad y continuidad de los procesos de negocio durante toda su actividad.
¿Qué activos de información presentan vulnerabilidades?	Se necesita que se responda al tipo de activos de información que se encuentran desactualizados o con debilidades para valorar el coste de sus actualizaciones y remediaciones.
¿Qué tipos de ataque reciben los activos de información?	Se necesita que se responda al tipo de ataques que más se reciben en la organización para balancear correctamente los procesos y recursos tecnológicos y humanos de protección, prevención, detección y respuesta.

Tabla 19 - Cuestiones previas a la implantación de un SOC.

Además, este ejercicio requiere que sus diseñadores sean lo más objetivos y realistas posibles para poder contestar adecuadamente y realizar, entre otros, un correcto dimensionamiento del equipo de trabajo, una asignación presupuestaria adecuada de la tecnología y una elección eficiente de los procesos, roles y servicios.

[33] Ver el punto 7.1.4.2.1 del Anexo 1 para más información sobre las Principales medidas de prevención, como las pruebas de penetración.
[34] Ver el punto 2.10.1 para más información sobre la implementación de SOC internos.
[35] Ver el punto 2.10.2 para más información sobre la implementación de SOC externos.
[36] Ver el punto 2.5 para más información sobre los Modelos de SOC.

2.12 Requisitos mínimos para definir un SOC

La definición de un SOC necesita tener en consideración todos los aspectos técnicos y funcionales de la organización en la que se desee implementar para conseguir alinear todos sus procesos de negocio con los de ciberseguridad en sus diferentes áreas y estructuras funcionales para proteger sus objetivos empresariales y organizativos. Por ello, también se necesitan tener en consideración todos los aspectos relacionados con la gestión interna, como son la publicitación de la nueva área de ciberseguridad a todo el personal de la organización, el conocimiento de sus labores y la comunicación de sus Planes de acción para su correcto funcionamiento. Por tanto, a continuación, se indican algunos de los principales requisitos básicos que toda organización necesita para definir un SOC:

Requisitos mínimos para la definición de un SOC	Descripción
Área de Seguridad de la Información	Toda organización necesita que se realice una supervisión continua y exhaustiva de todas las actividades que se ejecutan para el correcto funcionamiento de los diferentes procesos de negocio, por lo que, en materia de ciberseguridad, también se necesita que exista un área responsable que se encargue de diseñar, implementar y supervisar el correcto funcionamiento del SOC y que, por ejemplo, puede estar situado en la alta dirección de la organización.
Control de riesgos y disponibilidad	Toda organización necesita que se minimicen los riesgos de Seguridad de la Información a los que se encuentran expuestos y las interrupciones de disponibilidad que atentan contra su negocio, por lo que requiere que el SOC se diseñe para que cumpla con estas necesidades.
Asignación de responsabilidades	Toda organización necesita que se designen y atribuyan los roles y responsabilidades de los diferentes procesos de negocio, entre los que se encuentran los de ciberseguridad, por lo que se requiere que se determinen, documenten y notifiquen la atribución de competencias del SOC y su personal.
Registro de las amenazas	Toda organización precisa que se controlen, prevengan y gestionen todas las amenazas a la seguridad de sus activos de información que puedan afectar a sus procesos de negocio, sus clientes, su reputación y, entre otros, su economía, por lo que requiere que el SOC se construya para alertar y reaccionar con rapidez, con el fin de protegerla de todos esos posibles sucesos negativos.
Disminución de la sobrecarga administrativa	Toda organización necesita que sus diferentes áreas y equipos se coordinen y se integren para generar la menor sobrecarga administrativa al personal humano, con el fin de que puedan cumplir con sus funciones y procesos de negocio de manera ágil. Por tanto, se requiere que el SOC y sus procesos de ciberseguridad se diseñen con los suficientes permisos, privilegios y controles para que no requieran de trámites administrativos que retrasen su operatividad y protección.

Creación de documentación	Toda organización precisa de procedimientos, manuales y documentación específica sobre los servicios y procesos de negocio, entre los que entran los de ciberseguridad, del funcionamiento interno del SOC y de su integración con las demás áreas de la organización, por lo que se requiere que se genere, mantenga y gestione el ciclo de vida de toda la documentación necesaria para el establecimiento del SOC en la organización y su interrelación con las demás áreas.
Auditorías de Seguridad de la Información	Toda organización necesita que se verifique el estado de sus controles en materia de ciberseguridad para cumplir con las disposiciones normativas, regulaciones legales vigentes y políticas internas, con el fin de plantear la posibilidad de buscar certificaciones y reconocimiento por reputación, por lo que requiere que el SOC se diseñe para que cumpla y verifique el cumplimiento de todas estas características por todas las partes.
Notificación y recuperación de problemas	Toda organización necesita que registren y comuniquen todos los sucesos, eventos e incidentes de seguridad con mayor criticidad localizados en su red y se responda y recuperen los servicios que puedan verse afectados, por lo que se requiere que el SOC se diseñe con las herramientas necesarias para poder garantizar el registro y la recuperación de todos los sucesos negativos de los diferentes servicios y procesos de negocio de la organización.
Herramientas basadas en roles	Toda organización necesita que sus herramientas soporten diferentes roles y niveles de actividad para cumplir con las distintas responsabilidades y separar la información para que sólo la vea el personal autorizado, por lo que se requiere que se diseñen el SOC y sus herramientas para que puedan soportar y visualizar diferentes vistas de información.
Aprendizaje de los problemas e incidentes	Toda organización necesita que se alimente una base de datos de conocimiento con la información de todos los problemas ocurridos en sus procesos de negocio para evitar que vuelvan a ocurrir o actuar lo más rápido posible para su solución, por lo que, en materia de ciberseguridad, se necesita que se diseñe el SOC con personal capacitado para realizar acciones forenses sobre los incidentes de seguridad detectados y anotar todas sus características, acciones realizadas y soluciones aplicadas.
Gestión de registros de ciberseguridad	Toda organización necesita que sus alertas y sucesos de ciberseguridad se correlacionen y se centralicen en una única vista para entender el comportamiento de los eventos e incidentes de seguridad en sus diferentes etapas, así como que se verifique su impacto, criticidad y veracidad, por lo que se requiere que el SOC se diseñe para que configure la ingesta de los registros de *logs* de los sistemas de información en un único punto y su posible relación en las diferentes partes del reconocimiento y, además, gestione estos eventos resultantes y actúe en consecuencia.

Tecnología y herramientas potentes	Toda organización necesita que sus tecnologías y herramientas cumplan con todas las necesidades de la organización para garantizar un buen funcionamiento de sus procesos de negocio, por lo que se requiere que, para el diseño de un SOC, se utilicen y actualicen las herramientas en materia de Seguridad de la Información que ya están disponibles en la organización y se integren todas aquellas que sean necesarias para mejorar los procesos de negocio.
Rango de cobertura	Toda organización precisa que se monitorice la actividad de todos sus activos y sistemas de información para generar valor en materia de ciberseguridad, por lo que se requiere que el SOC se diseñe para que, en su implantación y mantenimiento diario, dé soporte y cobertura a todos los dispositivos de red de la organización, desde el perímetro hasta los servidores y puestos de usuario.
Respuestas rápidas ante problemas de ciberseguridad	Toda organización necesita que se actúe en tiempo real o lo antes posible ante un cualquier ciberincidente de seguridad que le afecte, por lo que se necesita que se configuren el SOC y todas sus herramientas para que se detecten las alertas en tiempo real y se reaccione ante ellas lo antes posible para solucionar o mitigar el problema que éstos puedan causar en la mayor celeridad posible.
Intervalo de actividad	Toda organización requiere que la gestión de su ciberseguridad se realice durante todo el tiempo que desarrolla sus actividades de negocio y se expone ante posibles riesgos y amenazas, por lo que se necesita que se diseñe el SOC para que realice sus funciones durante todo el intervalo de tiempo en el que se desarrolla el negocio, sea 24x7 (24 horas de los 7 días de la semana), 16x5 (16 horas diarias durante 5 días) o cualquier otro intervalo.
Integración de la ciberseguridad en la organización	Toda organización necesita combinar sus diferentes áreas funcionales y operativas con el área de ciberseguridad para garantizar su correcta protección, por lo que se necesita que se diseñen los procesos de negocio que desarrolle el SOC junto con los demás procesos de negocio y el propio SOC junto a las demás áreas funcionales, como puede ser un NOC[37] (Centro de Operaciones de Red), para facilitar la prevención, detección y reacción ante incidentes y brechas de ciberseguridad y maximizar la eficacia de los procesos de negocio.
Talento Humano	Toda organización necesita de personal experto y capacitado para ejecutar las funciones que se le hayan asignado para los diferentes procesos de negocio, por lo que, en materia de ciberseguridad, también se requiere de personal especializado en este ámbito para realizar un correcto análisis y reacción ante los diferentes sucesos negativos a los que se pueda ver expuesta la organización para la que trabaja.

[37] https://es.wikipedia.org/wiki/Centro_de_Control_de_la_Red

Publicación interna de la existencia del SOC y de sus funciones	Las organizaciones deben comunicar internamente a todo su personal la estrategia en materia de ciberseguridad que supone la inclusión de un SOC en sus áreas de negocio y asegurarse de que comprenden su funcionamiento y su ámbito de actuación intrusivo para que, entre otros: • No se sientan vigilados ni bloqueados en su trabajo diario, sino respaldados y protegidos digitalmente, en cuanto a la información que procesan y las amenazas a la ciberseguridad que reciben. • No confundan el SOC como un servicio de asistencia de TI, sino que conozcan que se trata de un área que verifica los eventos y problemas de ciberseguridad de los activos de información de manera horizontal en toda la organización.
Suministro de la infraestructura y las tecnologías en materia de ciberseguridad	Las organizaciones deben proporcionar una infraestructura tecnológica en materia de ciberseguridad que cubra las necesidades de protección, prevención, detección y respuesta ante las amenazas e incidentes de ciberseguridad que puedan sufrir. No sólo se puede considerar suficiente con las tecnologías y herramientas ya disponibles por la organización e integradas en la fase de diseño, sino que también se requiere que se evalúe y se invierta en los sistemas o mecanismos mínimos que cubran todos los posibles vectores de ataque y sean lo suficientemente apropiados para la experiencia y el respaldo de las funciones de un SOC. Además, como mínimo, debe de suministrarse e integrarse un SIEM para correlacionar todos los eventos de ciberseguridad y emitir alertas ante sucesos no deseados o anómalos.

Tabla 20 - Requisitos mínimos para diseñar un SOC.

2.13 Fases para la implementación de un SOC

La implementación de un SOC se trata de una actividad larga que no sólo consiste en un proyecto para instalar herramientas, contratar personal, crear procesos y asignar roles, sino que requiere de un análisis previo de la organización y de su negocio y de un desarrollo continuo para la planificación de distintas etapas de implantación y madurez, que, además de los procesos, la tecnología, el personal y los roles, también realice los análisis de riesgos, la elección de las estrategias de ciberseguridad, la elección de la metodología de funcionamiento y del tipo de implementación y del seguimiento del correcto funcionamiento del propio servicio, entre otras directrices. De hecho, tal y como expresa ENISA (Agencia de la Unión Europea para la Ciberseguridad)[38] en sus diferentes documentos publicados al respecto[39], se le debe dar especial atención a la creación de una buena planificación, por lo que se debe de estructurar en un cronograma que contemple diferentes fases como las que se indican a continuación:

[38] https://www.enisa.europa.eu/
[39] Ver el Capítulo 6 en relación sobre la bibliografía de consulta sobre ENISA.

Fases para la implementación de un SOC	Descripción
Fase 1: Preparación	Se trata del punto de partida de la implementación de un SOC, que se centra en indicar las razones, los requisitos y la necesidad de su implementación, en aprobar el presupuesto inicial y en establecer las características necesarias para la definición del SOC en la siguiente fase, entre otros factores importantes.
Fase 2: Diseño	Se trata de la etapa que se centra en la definición del SOC, en la preparación de las diferentes políticas y planes de ejecución del SOC y en su implantación en la organización, entre otros factores importantes.
Fase 3: Aplicación	Se trata de la etapa que se centra en la elaboración y estructura del equipo de trabajo del SOC y su asignación de roles, en la implantación de su tecnología de trabajo, en la creación de los procesos que debe seguir y en el establecimiento de los servicios que se desean ofrecer desde el SOC, entre otros factores importantes.
Fase 4: Operaciones	Se trata de la etapa que se centra en la prestación de los servicios de ciberseguridad por parte del SOC a la organización, a través de los procesos creados que ejecuta su equipo de trabajo y mediante las herramientas funcionales integradas, entre otros factores importantes.
Fase 5: Mejora continua	Se trata de la etapa que se centra en el seguimiento y la revisión del funcionamiento del SOC para su crecimiento y mejora, a través de estudios de rendimiento, iniciativas de mejora y aprobación de nuevo presupuesto para volver a la fase de Diseño (fase 2) de manera cíclica, entre otros factores importantes.

Tabla 21 - Fases para la implementación de un SOC.

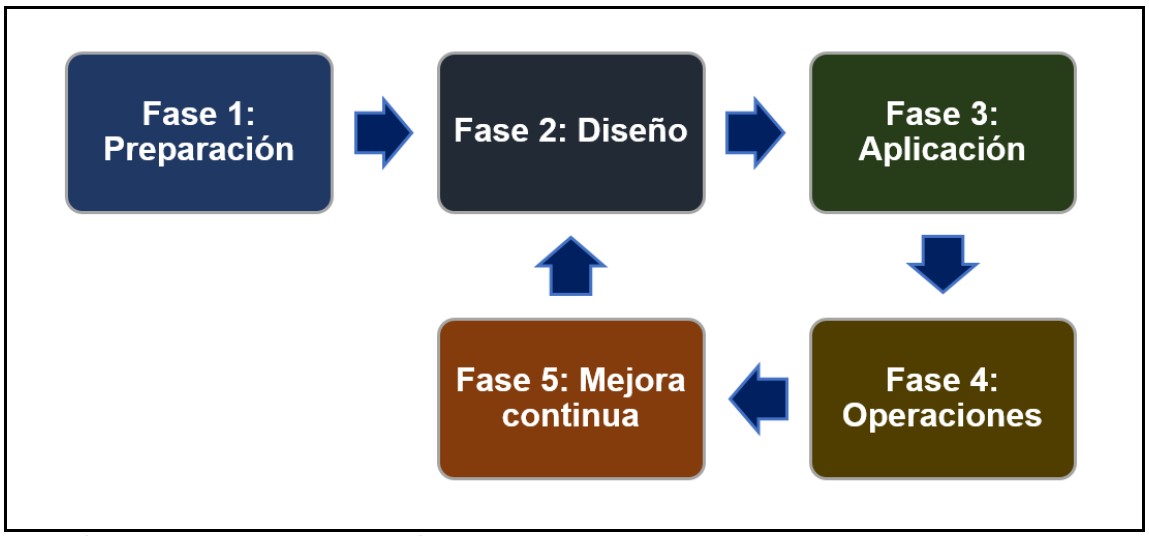

Ilustración 11 - Fases para la implementación de un SOC.

3. Resultados

Universitat Oberta de Catalunya
uoc.edu

Guía simple para la implementación de un SOC

Antonio Díaz Pérez
Máster Universitario en Ciberseguridad y Privacidad
Seguridad empresarial

Iñaki Moreno Fernández
Víctor García Font y Andreu Pere Isern Deyà

Enero de 2023

Índice

1. Introducción

El presente documento ofrece una **guía genérica práctica y simple** para el establecimiento de un SOC a cualquier organización que se encuentre interesada en su implementación, por lo que, básicamente, resume los diferentes análisis y estudios realizados y abordados en todos los capítulos y anexos de este Trabajo Final de Máster y ofrece una orientación práctica para su ejecución.

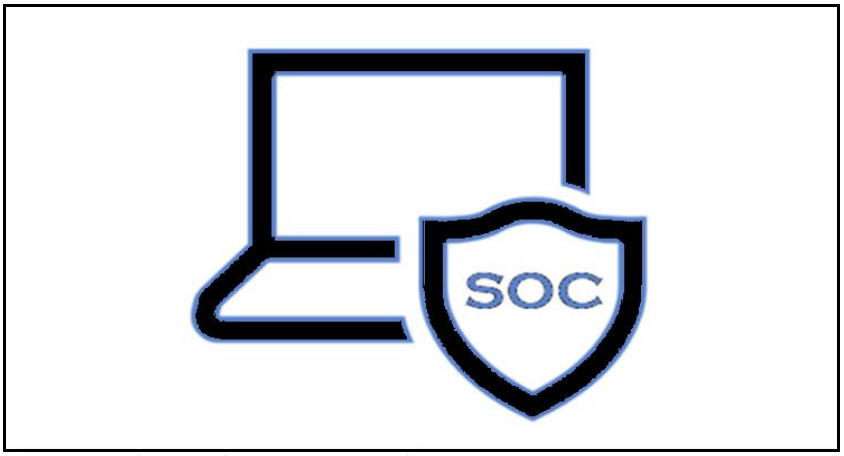

Ilustración 1 - Guía de implementación de un SOC.

Además, establece que la implementación de un SOC se trata de una actividad cíclica y duradera que requiere del desarrollo continuo de la estructura y planificación de un cronograma que contemple las diferentes etapas de implantación y madurez, como las que se indican a continuación:

- **Fase 1: Preparación.**
- **Fase 2: Diseño.**
- **Fase 3: Aplicación.**
- **Fase 4: Operaciones.**
- **Fase 5: Mejora continua.**

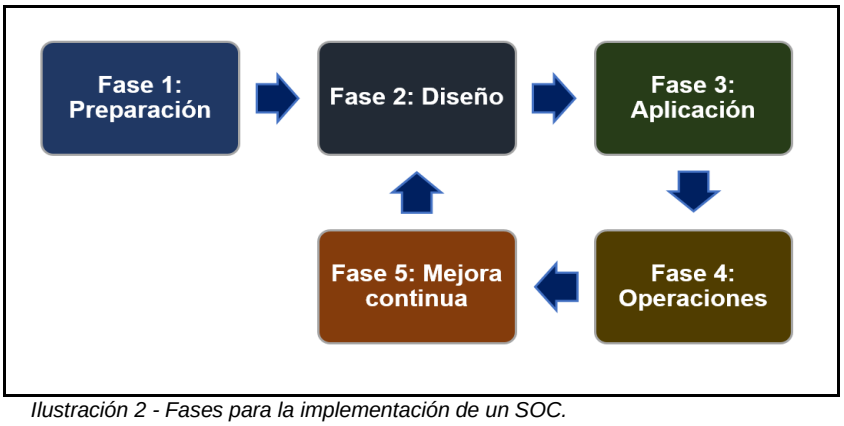

Ilustración 2 - Fases para la implementación de un SOC.

2. Hoja de ruta para la implementación de un SOC

La implementación de un SOC requiere del diseño previo de una **hoja de ruta** que sitúe cronológicamente la evolución del SOC en sus diferentes fases de madurez. Por tanto, se deben desarrollar un conjunto de normas e instrucciones, llamadas **directrices de buenas prácticas**, para la orientación de su puesta en funcionamiento con las suficientes garantías de éxito. Debido a esto, a continuación, se desarrollan las directrices necesarias, constituidas en sus diferentes fases, para satisfacer todas las necesidades organizativas de planificación y ejecución del desarrollo continuo, diseño, implementación y puesta en marcha de un SOC:

2.1 Fase 1: Preparación

Se trata del punto de partida de la implementación de un SOC, que se centra en indicar las razones, los requisitos y la necesidad de su implementación, en aprobar el presupuesto inicial y en establecer las características necesarias para la definición del SOC en la siguiente fase, entre otros factores importantes. Esta fase, normalmente, dura entre 2 y 12 meses y requiere de las siguientes actividades:

2.1.1 Justificación y razón del SOC

El paso inicial para la implementación de un SOC se centra en su definición, propósito y justificación con las partes interesadas y la alta dirección de toda organización. Para ello, se recomienda que se realicen las siguientes acciones:

#	Acciones	Descripción
1	**Comprensión de las necesidades**	Identificar a los clientes de la organización, a los usuarios y a las partes intervinientes para comprender, evaluar y planificar la satisfacción de sus expectativas y necesidades en materia de ciberseguridad (gestión de incidentes de ciberseguridad, cumplimiento normativo, concienciación…) a través del diseño de un SOC.
2	**Justificación de un SOC**	Documentar la idea inicial y las razones por las que se requiere un SOC y mostrar a la alta dirección de la organización el valor real que puede aportar, con el fin de justificar su implementación y su presupuesto inicial.
3	**Concienciación sobre ciberseguridad**	Mantener reuniones de concienciación en materia de ciberseguridad con los intervinientes y la alta dirección de la organización en busca de apoyos para la creación e implementación de un SOC.
4	**Aportaciones y beneficios de un SOC**	Elaborar un documento formal con las aportaciones y los beneficios que aporta un SOC a la organización para la mejora de la seguridad de sus procesos estratégicos y de su estabilidad funcional y firmeza en el negocio.

Tabla 1 - Definición y justificación del SOC.

2.1.2 Normativas y alineación de procesos con el SOC

Una vez se ha justificado la integración de un SOC en la organización, se deben determinar las metodologías necesarias para su establecimiento y alinear los procesos de negocio de la organización con los de ciberseguridad. Por tanto, entre otras, se sugieren las siguientes actividades:

#	Acciones	Descripción
1	**Selección de la metodología y las normativas**	Seleccionar la metodología y las normativas[40] que se consideren más óptimas y beneficiosas para el establecimiento del SOC en la organización y para la alineación de sus procesos de negocio con los de la ciberseguridad.
2	**Análisis de las disposiciones legales**	Estudiar las disposiciones y normativas legales[41] en materia de Seguridad de la Información para garantizar el cumplimiento de una correcta definición e implementación del SOC.
3	**Alineación de procesos**	Establecer las directrices necesarias para alinear los procesos de negocio de la organización con los de ciberseguridad que desarrollará el SOC, con el fin de integrar los servicios que ofrezca y mejorar su protección de la información.

Tabla 2 - Normativas y alineación de procesos de negocio con el SOC.

2.1.3 Características estratégicas para la implementación del SOC

Una vez se han seleccionado la metodología y las normativas la integración de un SOC en la organización, se deben establecer las estrategias para definirlo, el tipo de implementación y modelo de SOC que se requiere y el rango de operatividad, entre otros. Por tanto, se propone que se realicen las siguientes tareas:

#	Acciones	Descripción
1	**Definición de la estrategia**	Definir el paradigma estratégico[42] de Seguridad de la información para definir el SOC y que confluyan las estrategias de negocio de la organización con la inclusión de la ciberseguridad y se diseñen la Política de Seguridad de la Información y todos sus Planes de gestión.
2	**Elección del tipo de implementación y modelo de SOC**	Seleccionar el tipo[43] y modelo[44] de implementación del SOC que se desea implantar en la organización para realizar una definición del SOC que se adecúe a las necesidades de la organización.

[40] Ver los puntos del 7.2.1 al 7.2.14 del Anexo 2 para más información sobre las metodologías y normativas más usuales para el establecimiento de un SOC.
[41] Ver el punto 7.2.15 del Anexo 2 para más información sobre las disposiciones legales para un SOC en el Estado español.
[42] Ver el punto 2.9 para más información sobre las Estrategias para definir un SOC.
[43] Ver el punto 2.10 para más información sobre los Tipos de implementaciones de un SOC.
[44] Ver el punto 2.5 para más información sobre los Modelos de SOC.

3	**Selección del intervalo de actividad**	Analizar y escoger el rango de operatividad del SOC para que su definición se ajuste a todo el tiempo en el que la organización desarrolla sus actividades de negocio y se expone ante posibles riesgos y amenazas. Estos intervalos pueden ser 24x7 (24 horas de los 7 días de la semana), 16x5 (16 horas diarias durante 5 días) o cualquier otro.
4	**Cuestionario previo al diseño del SOC**	Plantear y responder una serie de cuestiones previas [45] relacionadas, entre otros, con las prioridades y condiciones de la organización, los activos a proteger, las vulnerabilidades actuales y los ataques que más se reciben recibidos, con el fin de poder definir su alcance y conocer su nivel actual de ciberseguridad para guiar en el diseño y la implementación del SOC.

Tabla 3 - Características estratégicas para la implementación del SOC.

2.1.4 Alcance, objetivos y responsabilidades del SOC

Tras el establecimiento de las características estratégicas para la implementación de un SOC, el siguiente paso recomendado se centra en la definición de su alcance, sus propósitos y sus responsabilidades. Para ello, se recomienda que, entre otras, se realicen las siguientes acciones:

#	Acciones	Descripción
1	**Denotación del alcance y los objetivos a alcanzar**	Documentar de manera formal el alcance del SOC y los objetivos que se desean alcanzar para la detección y protección de los activos y sistemas de información en tiempo real y al análisis y respuesta de los eventos e incidentes de seguridad de la organización.
2	**Definición de las responsabilidades del SOC**	Documentar de manera formal las responsabilidades que debe asumir el SOC en materia de ciberseguridad para con la organización, con el fin de que se cumplan todas sus funciones[46] y los ANS pactados.

Tabla 4 - Alcance, objetivos y responsabilidades del SOC.

2.1.5 Requisitos mínimos, presupuesto inicial y cronograma del SOC

Una vez se han definido el SOC y su estructura, se deben planificar y responder a los requisitos mínimos que se necesitan para definir y diseñar un SOC, así como desarrollar un cronograma aproximado de alto nivel con sus diferentes etapas de implantación y, en base a ello, solicitar el presupuesto inicial para su implementación a la alta dirección. Por tanto, se recomienda que se realicen las siguientes acciones:

[45] Ver el punto 2.11 para más información sobre cuestiones previas para el diseño de un SOC.
[46] Ver el punto 2.7 para más información sobre las funciones que realiza un SOC.

#	Acciones	Descripción
1	**Planificación de requisitos mínimos previos**	Considerar todos los aspectos técnicos y funcionales de la organización, como requisitos mínimos para definir el SOC[47], para conseguir un diseño que alinee todos sus procesos de ciberseguridad con los de negocio desde cada una de sus áreas funcionales y con el fin de proteger sus objetivos organizativos y empresariales, así como planificar todos los aspectos relacionados con la gestión interna, como son la publicitación de la nueva área de ciberseguridad a todo el personal de la organización, el conocimiento de sus labores y la comunicación de sus Planes de acción necesarios para el correcto funcionamiento SOC, entre otros.
2	**Desarrollo del cronograma**	Desarrollar un cronograma aproximado de alto nivel requiere de calcular el tiempo y los recursos necesarios para poder abordar todas y cada una de las actividades de las diferentes etapas de implantación de un SOC, como el que se ilustra a continuación en base al tiempo:  *Ilustración 3 – Desarrollo del cronograma aproximado para la implementación de un SOC.*
3	**Cálculo de los costes para el presupuesto**	Identificar todos aquellos recursos que provocan un coste para el cálculo del presupuesto inicial que necesita la implementación de un SOC en la organización, como pueden ser, entre otras: • Los salarios del personal del SOC. • El gasto en las instalaciones del SOC. • El gasto en servicios de consultoría (legal, tecnológica…). • Formación del personal del SOC en competencias y servicios. • Adquisición de la tecnología y de sus respectivas licencias.

Tabla 5 – Requisitos mínimos, presupuesto inicial y cronograma de alto nivel para el SOC.

Página 5

[47] Ver el punto 2.12 para más información sobre los requisitos mínimos para definir un SOC.

2.2 Fase 2: Diseño

Se trata de la etapa que se centra en la definición del SOC, en la preparación de las diferentes políticas y planes de ejecución del SOC y en su implantación en la organización, entre otros factores importantes. Normalmente, esta fase dura entre 3 y 6 meses y requiere de las siguientes actividades:

2.2.1 Nombre y definición del SOC y de su estructura

Una vez realizadas las actividades necesarias para la preparación de la implementación del SOC, se debe comenzar la fase de diseño, con el establecimiento del nombre del SOC y su definición y estructura formal. Por tanto, se recomienda que se realicen las siguientes acciones:

#	Acciones	Descripción
1	**Nombrar el SOC**	Diseñar el nombre que debe recibir el SOC para identificarlo en la organización y en el resto de intervinientes, colaboradores y demás equipos de ciberseguridad externos.
2	**Definición del SOC a implementar**	Crear un documento formal con la definición del SOC que se desea implementar, en base a sus peculiaridades y a la información característica basada en el RCF 2350[48], que aporta, entre otros, su autoridad, sus requisitos, objetivos, alcance, responsabilidades, misión, actividades y servicios.
3	**Definición de la estructura del SOC**	Crear un documento formal con la estructura jerárquica del SOC en la organización y con la información necesaria para definir las responsabilidades de sus partes intervinientes, justificar su financiación, indicar su propietario y los encargados de su dirección, supervisión y seguimiento, enunciar los acuerdos con la alta dirección de la organización y definir la manera y la periodicidad de sus reportes.

Tabla 6 - Nombre y definición del SOC y de su estructura.

2.2.2 Servicios del SOC y sus procesos y flujos de trabajo

Tras la definición formal del SOC, en donde se indican los servicios que desea ofrecer el SOC, se debe diseñar y desarrollar el catálogo de servicios indicados junto a sus procesos, actividades y flujos de trabajo. Por consiguiente, se recomienda que se realicen las siguientes acciones:

[48] Ver el punto 7.2.14.1 del Anexo 2 para más información sobre el RFC 2350.

#	Acciones	Descripción
1	**Análisis de los servicios del SOC**	Realizar un estudio de los servicios incluidos en la definición del SOC y catalogarlos en las áreas centrales de servicios [49] para especificar sus procesos y describir sus flujos de trabajo.
2	**Descripción de los procesos del SOC**	Crear un documento formal con cada uno de los procesos[50] que conforman los diferentes servicios incluidos en el SOC y su definición detallada con su descripción, su responsable, su propósito, su disparador o activador, su prestación en los servicios en los que actúe, sus directrices y sus actividades, entre otros.
3	**Diseño de los flujos de trabajo de los procesos del SOC**	Incluir en el documento formal de la descripción de los procesos del SOC, un diagrama por cada proceso que describa gráficamente el funcionamiento de las actividades que realizan junto a sus disparadores o activadores y camino a seguir.
4	**Redacción del catálogo de servicios del SOC**	Crear un documento formal con el conjunto de servicios que se desean ofrecer desde el SOC, su descripción, sus características, sus procesos y flujos de trabajo.

Tabla 7 - Servicios del SOC y sus procesos y flujos de trabajo.

2.2.3 Plan de formación del SOC

Tras la redacción del catálogo de servicios que ofrece el SOC y su selección del intervalo de actividad en la fase de Preparación, se recomienda que se diseñe y establezca un Plan de formación inicial de las actividades que debe realizar el SOC. De esta manera, si el intervalo de actividad se basa en un 24x7, siempre será el personal del SOC el que realiza las actividades relacionadas con la ciberseguridad y necesita conocer cómo actuar internamente en la organización en la que presta el nuevo servicio. Sin embargo, si se basa en 8x5, el resto del tiempo en el que el personal del SOC no presta servicio, posiblemente, se encargue de atender la recepción del evento o incidente de ciberseguridad, un operador o alguien relacionado con las operaciones funcionales de la organización que no tiene por qué conocer cómo actuar en esos casos. Por tanto, se aconseja que se realicen las siguientes acciones:

#	Acciones	Descripción
1	**Planificación de la formación inicial del SOC**	Organizar y estructurar un Plan de formación inicial con diferentes seminarios, talleres, laboratorios y cursos que cubran las actividades operativas y técnicas que debe realizar el SOC, así como sus disposiciones legales, sus normativas de cooperación y de orientación sobre los servicios y sus procesos, flujos de trabajo y metodologías.

[49] Ver el punto 2.8 para más información sobre las Áreas centrales de servicios de un SOC.
[50] Ver el punto 7.3.1 del Anexo 3 para más información sobre los Procesos de un SOC.

2	**Planificación de la formación para el desarrollo de habilidades**	Organizar y estructurar un Plan de formación para el desarrollo de habilidades necesarias para el personal del SOC y su crecimiento interno en el área, como pueden ser las competencias profesionales (gestión de conflictos, pensamiento crítico, comunicación, protección de datos, control de procesos…) y las competencias de liderazgo (gestión del personal, gestión de proyectos, planificación estratégica…).

Tabla 8 - Plan de formación del SOC.

2.2.4 Instalaciones del SOC

Una vez establecido el Plan de formación que debe realizar el SOC, se tienen que diseñar unas instalaciones para la prestación de los servicios que ofrece el SOC con espacios de trabajo separados y con reglamentos y normativas claras para el correcto funcionamiento del SOC. Por tanto, se aconsejan las siguientes actividades:

#	Acciones	Descripción
1	**Preparación de las instalaciones del SOC**	Acondicionar las instalaciones para la prestación de servicios del SOC que incluya, como mínimo, una sala para el procesamiento de datos de las tecnologías, una sala de oficinas para el trabajo diario del personal del SOC y una sala para las reuniones y recepción de los invitados.
2	**Adecuación de la seguridad física de las instalaciones del SOC**	Reformar las políticas de seguridad física de las instalaciones del SOC para garantizar un control de acceso, una supervisión, una evaluación de riesgos y un impacto sostenible adecuados, así como un entorno laboral cómodo y apropiado para el funcionamiento diario del personal del SOC.

Tabla 9 - Instalaciones del SOC.

2.2.5 Plan de buenas prácticas para la tecnología del SOC

Tras el acondicionamiento del SOC y la preparación de las políticas para su seguridad física, se deben diseñar y planificar las acciones necesarias para mejorar su funcionamiento tecnológico, por lo que se sugieren las siguientes actividades para intentar garantizar mejor el éxito de sus procesos:

#	Acciones	Descripción
1	**Creación de la alta disponibilidad tecnológica**	Implantar e integrar dispositivos redundantes en alta disponibilidad en la organización para facilitar el restablecimiento del servicio automático en caso de desastre.

2	**Provisión de copias de seguridad de la información**	Automatizar el almacenamiento de copias de seguridad de la información crítica para facilitar su recuperación y disponibilidad temprana en caso de desastre.
3	**Segmentación de la red de la organización**	Dividir las redes de la organización en diferentes áreas (producción, DMZ, pruebas…) protegidas por cortafuegos[51] para dar mayor seguridad al acceso a los servicios y sistemas de información.
4	**Selección de la ubicación de servicios del SOC**	Elegir correctamente los servicios que se prestan desde las instalaciones físicas de la organización y desde la nube a través del estudio y valoración de los riesgos en contra de la disponibilidad y sus costes para garantizar lo máximo posible la seguridad de la información confidencial, secreta o privada.
5	**Automatización de los procesos**	Automatizar todos los posibles procesos de gestión tecnológica para mejorar la eficiencia de la prestación de servicios del SOC, entre los que se recomiendan encarecidamente los de los gestión de *ticketing*[52], los de gestión de información y eventos de seguridad[53] para correlacionar y centralizar la información y los de publicación de alertas y vulnerabilidades[54].

Tabla 10 - Plan de buenas prácticas para la tecnología del SOC.

2.2.6 Plan de buenas prácticas para la protección de la organización

Tras la planificación de las buenas prácticas para la mejora del funcionamiento tecnológico del SOC, se deben diseñar y planificar las actividades y buenas prácticas para la mejora de la protección de la organización. Por tanto, se aconsejan las siguientes actividades de diseño:

#	Acciones	Descripción
1	**Gestión de los desafíos y riesgos[55]**	Diseñar un programa para realizar una gestión de los riesgos a la ciberseguridad de la organización, basado en sus diferentes fases[56], y combatir los desafíos a los que se enfrente la implementación del SOC, con el fin de minimizar sus amenazas.

[51] Ver el punto 7.3.2.1 del Anexo 3 para más información sobre Cortafuegos (*Firewall)*.
[52] Ver el punto 7.3.2.11 del Anexo 3 para más información sobre herramientas de gestión de *ticketing*.
[53] Ver el punto 7.3.2.4 del Anexo 3 para más información sobre los sistemas de gestión de información y eventos de seguridad (SIEM).
[54] Ver el punto 7.3.2.12 del Anexo 3 para más información sobre gestores de vulnerabilidades.
[55] Ver el punto 2.6 para más información sobre los desafíos y riesgos de un SOC.
[56] Ver el punto 7.1.2.2.1 del Anexo 1 para más información sobre las fases de la Gestión de Riesgos.

2	**Creación de alianzas de colaboración**	Firmar acuerdos de colaboración para compartir información sobre vulnerabilidades y amenazas de ciberseguridad con otros SOC y equipos de respuesta ante incidentes de ciberseguridad y diseñar los procedimientos y protocolos de cooperación para unificar conocimientos y combatir juntos contra los atacantes de la seguridad de los activos de información.
3	**Implantación de un SGSI[57]**	Diseñar la implementación de un Sistema de Gestión de la Seguridad de la información (SGSI) en la organización para que adopte una postura favorable ante las tareas en materia de ciberseguridad que debe realizar un SOC. En el caso de que se encuentre ya implementado, se recomienda que se realice una evaluación y se compare con las buenas prácticas y directrices indicados en la norma ISO/IEC 27001[58].

Tabla 11 - Plan de buenas prácticas para la protección de la organización.

2.3 Fase 3: Aplicación

Se trata de la etapa que se centra en la elaboración y estructura del equipo de trabajo del SOC y su asignación de roles, en la implantación de su tecnología de trabajo, en la creación de los procesos que debe seguir y en el establecimiento de los servicios que se desean ofrecer desde el SOC, entre otros factores importantes. Normalmente, esta fase dura un periodo entre 3 y 12 meses y requiere de las siguientes actividades:

2.3.1 Aprobación de los Planes diseñados para la creación del SOC

Una vez realizadas las actividades de la fase de diseño, se deben aprobar todos los Planes trazados para su aplicación e implantación en el SOC. Por tanto, se recomienda que se realicen las siguientes actividades:

#	Acciones	Descripción
1	**Aprobación de la estructura del SOC**	Aprobar y aplicar la estructura organizativa diseñada para el SOC y definir los diferentes puestos y roles de su personal.
2	**Aprobación de las instalaciones del SOC**	Aprobar y fundar las instalaciones diseñadas y acondicionadas para el SOC y difundir internamente y controlar sus políticas de seguridad física.
3	**Aplicación de los procesos y flujos de trabajo**	Aprobar y aplicar los documentos formales de cada uno de los procesos y flujos de trabajo para formalizar la prestación de servicios del SOC.

[57] Ver el punto 7.1.1.5 del Anexo 1 para más información sobre los sistemas de Gestión de la Seguridad de la información (SGSI).
[58] Ver el punto 7.2.1.2 del Anexo 2 para más información sobre la normativa ISO/IEC 27001 en su última versión.

4	**Aprobación de la documentación del SGSI**	Aprobar, aplicar y ejecutar la implementación del Sistema de Gestión de la Seguridad de la información (SGSI) diseñado para la organización o, en su caso, aprobar y ejecutar los resultados de su evaluación, así como la ejecución y capacitación de sus procedimientos de gestión detallados.
5	**Aprobación del Plan de formación**	Aprobar y ejecutar el Plan de formación diseñado para el aprendizaje de conocimientos teórico-prácticos del personal del SOC y para el desarrollo de las habilidades necesarias para el cumplimiento de sus funciones.
6	**Aprobación de los protocolos para las alianzas de colaboración**	Aprobar, difundir y capacitar internamente los procedimientos y protocolos de cooperación diseñados para compartir los conocimientos relacionados con las amenazas de ciberseguridad y combatir en conjunto a sus atacantes.
7	**Aprobación de la gestión de los riesgos**	Aprobar y ejecutar el programa para de gestión de los riesgos a la ciberseguridad de la organización diseñado para proteger a la organización mediante la prevención temprana de las amenazas que pueda sufrir.

Tabla 12 - Aprobación de los Planes diseñados para la creación del SOC.

2.3.2 Cubrimiento de las carencias para la aplicación del SOC

Una vez aprobados los Planes diseñados para la aplicación e implantación del SOC, se deben cubrir las carencias de personal y tecnologías para el correcto funcionamiento de los servicios diseñados y aprobados que presta el SOC. Por tanto, se aconseja que se realicen las siguientes actividades:

#	Acciones	Descripción
1	**Nombramiento del personal del SOC y asignación de roles**	Cubrir todos los puestos de trabajo diseñados y aprobados para la estructura organizativa del SOC, mediante el personal cualificado que se tiene en la organización y mediante la contratación de nuevo personal con conocimientos y experiencia en la materia que se desee cubrir, así como asignar los roles y responsabilidades en base a los niveles del SOC que se hayan estructurado[59].
2	**Implantación de nueva tecnología**	Implantar e integrar nueva tecnología en la organización para cubrir todas las necesidades de automatización de procesos de gestión tecnológica diseñados.

Tabla 13 - Cubrimiento de las carencias para la aplicación del SOC.

[59] Ver el punto 7.3.3 del Anexo 3 para más información sobre Personal y estructura de roles de un SOC.

2.3.3 Batería de pruebas y puesta en funcionamiento inicial del SOC

Tras cubrir las carencias de diseño tecnológico y personal del SOC, se deben realizar las pruebas necesarias para comprobar su correcto funcionamiento y poner en marcha los servicios que debe prestar el SOC a modo de aprendizaje y evaluación, por lo que se recomienda que se ejecuten las siguientes acciones:

#	Acciones	Descripción
1	**Ejecución de una batería de pruebas**	Ejecutar una batería de pruebas del funcionamiento del SOC resultante para notificar las deficiencias de sus tecnologías, procesos y flujos de trabajo, con el fin de verificar sus carencias y realizar los ajustes necesarios para su integración en la organización.
2	**Implantación de nueva tecnología**	Implantar e integrar nueva tecnología en la organización para cubrir todas las necesidades de automatización de procesos tecnológicos diseñados.
3	**Puesta en funcionamiento inicial del SOC**	Poner en funcionamiento los servicios que debe prestar el SOC durante un tiempo limitado, a modo de aprendizaje y de evaluación, con el fin de garantizar su correcto dimensionamiento tecnológico y humano y la adecuada ejecución de sus operaciones y actividades diarias.

Tabla 14 - Batería de pruebas y puesta en funcionamiento inicial del SOC.

2.4 Fase 4: Operaciones

Se trata de la etapa que se centra en la prestación de los servicios de ciberseguridad por parte del SOC a la organización, a través de los procesos creados que ejecuta su equipo de trabajo y mediante las herramientas funcionales integradas, entre otros factores importantes. Normalmente, esta fase comienza entre 12 y 18 meses después del comienzo de la fase de preparación y requiere de las siguientes actividades:

2.4.1 Puesta en funcionamiento formal del SOC

Una vez realizadas todas las actividades de la fase de diseño y de la de aplicación, el SOC debe empezar su funcionamiento de manera formal. Tras la batería de pruebas y la puesta en funcionamiento inicial en la fase de aplicación, se debe empezar a prestar el servicio de ciberseguridad de manera operativa y rigurosa. Por tanto, se recomienda que se ejecuten las siguientes acciones:

#	Acciones	Descripción
1	**Formalización del funcionamiento del SOC**	Inaugurar y comunicar formalmente la puesta en funcionamiento del SOC para ejecutar sus operaciones y actividades diarias.

2	**Cubrimiento de las carencias residuales**	Contratar el personal e integrar la tecnología necesaria aún no cubierta para completar la ejecución de los procesos, los flujos de trabajo y la prestación de los servicios diseñados para el SOC y aceptados por la organización.

Tabla 15 - Puesta en funcionamiento formal del SOC.

2.4.2 Seguimiento del funcionamiento del SOC

Tras poner en funcionamiento el SOC de manera formal y empezar a prestar los servicios a la organización, se debe realizar un seguimiento de su funcionamiento para comprobar que se realizan y completan todas las actividades y se cumplen los diferentes acuerdos de nivel de servicio (ANS). Por tanto, se aconseja que se realicen las siguientes tareas:

#	Acciones	Descripción
1	**Gestión de la calidad**	Realizar una verificación y seguimiento del rendimiento general del SOC y de los acuerdos de nivel de servicio (ANS) para gestionar la calidad de las operaciones y del servicio prestado a la organización, mediante mediciones mensuales de los indicadores clave de rendimiento (KPI)[60] que se asocian a los procesos y flujos de trabajo y al cumplimiento de los objetivos de los servicios, de los análisis estadísticos y de las acciones para la mejora de su calidad.
2	**Gestión del rendimiento del personal**	Realizar una verificación y seguimiento del rendimiento individual del personal del SOC para identificar sus casos de éxito y sus aspectos de mejora, con el fin de maximizar su rendimiento individual y generalizado.
3	**Gestión del rendimiento tecnológico**	Realizar una verificación y seguimiento del rendimiento de los procesos, flujos de trabajo, KPI, sistemas, herramientas y automatización en materia de ciberseguridad que utiliza el SOC en su funcionamiento diario para identificar sus aspectos de mejora y buscarles solución.
4	**Gestión de la satisfacción**	Realizar una verificación y seguimiento de la subsanación de las necesidades de las partes intervinientes del SOC y la alta dirección de la organización, con el fin de valorar sus expectativas e identificar aspectos de mejora.
5	**Cálculo de los costes para el presupuesto**	Identificar todos aquellos recursos que provocan un coste para el cálculo del presupuesto anual relacionado con el funcionamiento diario del SOC en la organización, en concordancia con las normativas legales y propias de la organización.

[60] https://es.wikipedia.org/wiki/Indicador_clave_de_rendimiento

6	**Documento de iniciativas de mejoras anuales**	Crear un documento formal en una tabla con las iniciativas de mejora a valorar cada año con su descripción y justificación, a partir del estudio de la satisfacción de las partes intervinientes del SOC y la alta dirección de la organización, las actividades y operaciones del equipo de trabajo, los procesos y la tecnología utilizada, con el fin de presentarlo cuando se active la fase de Mejora continua en el desarrollo continuo del SOC.

Tabla 16 - Seguimiento del funcionamiento del SOC.

2.5 Fase 5: Mejora continua

Se trata de la etapa que se centra en el seguimiento y la revisión del funcionamiento del SOC para su crecimiento y mejora, a través de estudios de rendimiento, iniciativas de mejora y aprobación de nuevo presupuesto para volver a la fase de Diseño (fase 2) de manera cíclica, entre otros factores importantes. Esta fase, normalmente, se activa tras un año en la fase de Operaciones (fase 4), mientras ésta continúa su actividad y funcionamiento, y requiere de las siguientes actividades:

2.5.1 Iniciativas de mejora para el SOC

Finalmente, como último paso antes de retomar el ciclo en la fase de Diseño nuevamente, una vez activada la fase de Mejora continua en la implementación del SOC, se deben seleccionar las iniciativas de mejora del documento de iniciativas de mejoras anuales realizado en la etapa de Operaciones y aprobar todas aquellas que se consideren correctamente justificadas para devolverlas a las fases de Diseño, Aplicación y Operaciones. Por tanto, se recomienda que se realicen las siguientes acciones:

#	Acciones	Descripción
1	**Selección y aprobación de las iniciativas de mejora**	Realizar un estudio de las iniciativas de mejora presentadas en la fase de Operaciones, en base a sus necesidades y justificación, para generar un listado con las iniciativas aprobadas.
2	**Preparación de los planes de las iniciativas de mejora**	Realizar un documento formal con la planificación de las iniciativas de mejora aprobadas para enviarlas a la fase de Diseño, con toda la información de relevancia, como su justificación, sus objetivos, sus expectativas, su asignación de tiempo y de recursos y sus procedimientos, entre otros.
3	**Cálculo de los costes para el presupuesto de mejoras**	Identificar todos aquellos recursos que provocan un coste para el cálculo del presupuesto relacionado con el listado de mejoras del SOC en la organización, ya sea por procesos, personal, tecnología o cualquier otro recurso como pueden ser las instalaciones, los contratos con proveedores, los acuerdos con otras organizaciones o la formación, entre otros.

Tabla 17 - Iniciativas de mejora para el SOC.

4. Conclusiones y trabajos futuros

4.1 Consecución de objetivos y conclusiones

El establecimiento de un SOC en una organización se considera un trabajo continuo y complejo, que requiere de un proceso previo bien estructurado para encauzar su implementación, del apoyo de su alta dirección y de sus partes interesadas y de una planificación ágil a largo plazo para guiar su desarrollo y enderezarlo hacia sus intereses estratégicos en materia de ciberseguridad. Esto significa que se identifica con facilidad la linealidad de su fase inicial, en donde se comprenden y justifican las necesidades de la organización y se aportan los beneficios de un SOC para convencer a la alta dirección y a los intervinientes, pero que las siguientes fases entran en un ciclo de diseño, aplicación, operatividad y mejora continua para perfeccionar sus servicios, ofrecer mayor eficiencia y alinear los procesos estratégicos de la organización con la transversalidad de la ciberseguridad.

Asimismo, la realización de una guía simple para la implementación de un SOC se debe basar en diferentes análisis y estudios de investigación relacionados con la organización y la ciberseguridad, con el fin de obtener los resultados y objetivos deseados. Por este motivo, en este trabajo, se han analizado los conceptos para la comprensión de la gestión de la Seguridad de la Información y de la ciberseguridad, se han examinado los estándares, normativas, metodologías internacionales y las disposiciones legales vigentes más relevantes, se han investigado los procesos, las tecnologías, el personal y los roles en los que se fundamentan los servicios mínimos que debe de prestar el SOC y los conceptos y particularidades necesarias para su implementación, por lo que se han obtenido los resultados que se esperaban y se han alcanzado todos los objetivos planteados, tanto el principal como los específicos.

Por tanto, del estudio de la implementación de un SOC en una organización, de los diferentes análisis realizados en este trabajo y de los resultados conseguidos se obtienen, entre otras, las siguientes conclusiones:

- Todas las organizaciones necesitan un área que se responsabilice y gestione su ciberseguridad, que vele por su cumplimiento legal y normativo en esta área, que capacite a todas las partes intervinientes y que responda ante los incidentes y brechas de seguridad en sus activos de información interconectados.
- La implementación de un SOC mejora las capacidades en materia de ciberseguridad de una organización, fortalece sus estructuras y procesos de negocio, refuerza, gestiona y potencia el talento y maximiza sus capacidades de protección, prevención, detección y respuesta ante incidentes.
- La integración de un SOC en una organización proporciona reducción de costes a largo plazo, agiliza la resolución de incidentes de ciberseguridad, mejora el valor del catálogo de servicios, aumenta la tasa de éxito en la protección de los ataques y amenazas de ciberseguridad y minimiza sus riesgos.
- Todo SOC necesita colaborar y cooperar con otras entidades para maximizar sus capacidades de protección en la organización en la que opera, así como capacitar en materia de ciberseguridad a todas sus partes intervinientes para mejorar su cultura, enseñar sus buenas prácticas y garantizar el apoyo de la parte directiva.

- Las organizaciones que deseen implementar un SOC necesitan de una guía que les asista y les oriente para realizar un diseño y una integración de éxito, pero requieren de la implicación de todas las partes interesadas para alinear sus procesos de negocio con los de ciberseguridad y cubrir todas las necesidades de protección de sus activos de información.

4.2 Seguimiento de la planificación, la metodología y el impacto ético-social, de sostenibilidad y de diversidad

Una vez finalizado el Trabajo Final de Máster, dado que se ha cumplido con el cronograma de hitos planificado y se han utilizado las guías y buenas prácticas de las metodologías de investigación exploratoria-descriptiva y de la combinación de DevOps y Kanban sin necesidad de introducir cambios significativos, se considera que el trabajo realizado ha sido el adecuado y se ha organizado y estructurado correctamente. Por tanto, se le ha otorgado direccionalidad a su investigación y desarrollo y se han alcanzado todos los propósitos específicos y su objetivo principal, la guía simple de implementación de un SOC.

Asimismo, el trabajo realizado y la implementación de un SOC en una organización se alinean con los Objetivos de Desarrollo Sostenible y con las tres dimensiones que definen las Competencias de Compromiso Ético y Global (CCEG). Por tanto, su estudio y desarrollo se realiza sobre principios éticos, íntegros, sostenibles, sensatos, responsables, plurales y respetuosos con las personas, la sociedad y el medio ambiente y se enfoca en la guía simple de un proyecto de implantación y seguimiento tecnológico basado en buenas prácticas globales que impacta directa o indirectamente en lo siguiente:

- Protección de los sistemas de información de infraestructuras críticas, que velan por los intereses de los objetivos de alto nivel relacionados con la sostenibilidad del negocio de esas infraestructuras.
- Protección de la información personal, sensible, intelectual y de valor de los individuos y organizaciones en sociedad, que, entre otros, favorece el crecimiento económico, aumenta el empleo sostenido e inclusivo, impulsa el progreso, fortalece a las entidades e instituciones, vela por los requerimientos legales, facilita tranquilidad a las personas y se alinea con los propósitos de reducción de la desigualdad y la distinción de género.

4.3 Trabajos futuros

A pesar de que las organizaciones que deseen implementar un SOC requieran de la implicación de la alta dirección y de los intervinientes para alinear sus procesos de negocio con los de ciberseguridad y cubrir sus necesidades de protección de sus activos de información, necesitan un documento guía que les asista y oriente para garantizar el éxito en la implementación e integración del SOC. Sin embargo, las instituciones deberían de plantearse la creación de una normativa internacional que cubra esta necesidad y que estandarice su diseño e implantación. Por tanto, un posible trabajo a futuro puede ser el impulso de esta normativa, que implicaría diferentes líneas de trabajo, como, entre otras, las implementaciones reales de SOC en diferentes organizaciones a partir de la guía simple creada para adquirir experiencia y mejorar la propia guía, definir los diferentes escenarios de incidentes y brechas de ciberseguridad para mejorar su operatividad y crear un catálogo de servicios de ciberseguridad estándar, que mejore su calidad y funcionamiento real.

5. Glosario

- **ACTIVO DE INFORMACIÓN**: Recurso con un valor potencial en la información y los datos que procesa para el funcionamiento diario de una organización.

- **ALERTA DE CIBERSEGURIDAD**: Notificación de un posible suceso anómalo, no deseado o con impacto negativo en la Seguridad de la Información interconectada digitalmente de los servicios de una organización o en sus activos de información, sus operaciones o sus objetivos del negocio.

- **AMENAZA DE CIBERSEGURIDAD (CIBERAMENAZA)**: Situación adversa para la seguridad de la información interconectada digitalmente que puede tener un impacto negativo en los activos de información de una organización y en cualquiera de las propiedades de la información.

- **ANONIMATO**: Propiedad de la seguridad de la información que protege del reconocimiento de un sujeto en cualquier acción que realice sobre la información para de salvaguardar su identidad.

- **ANTIMALWARE**: Programa software de ciberseguridad creado para detectar, proteger y eliminar software malicioso en puntos finales en tiempo real.

- **AUDITABILIDAD o RESPONSABILIDAD**: Propiedad de la seguridad de la información que garantiza el registro y la monitorización del uso de la información por parte de usuarios, aplicaciones o procesos conectados y autorizados.

- **AUTENTICIDAD**: Propiedad de la seguridad de la información que garantiza la identidad del suministrador de la información; es decir, que certifica que el autor de la comunicación de la información es quien dice ser.

- **BOE (BOLETIN OFICIAL DEL ESTADO)**: Diario oficial del Estado español dedicado a la publicación de las normativas legales, como Leyes, Reales Decretos y Reglamentos, entre otros.

- **CCN (CENTRO CRIPTOLÓGICO NACIONAL)**: Organismo oficial nacional español que se responsabiliza de coordinar la acción de los diferentes organismos de la Administración Pública para garantizar la seguridad de las Tecnologías de la Información, coordinar la obtención de material Criptológico e instruir al personal técnico de TI de la Administración.

- **CCN-CERT**: Equipo de Respuesta de Emergencias Informáticas e Incidentes de Seguridad de la Información del Centro Criptológico Nacional.

- **CENTRO DE OPERACIONES DE SEGURIDAD (SOC)**: Equipo o área centralizada para las operaciones tácticas, técnicas y procedimentales relacionados con la ciberseguridad de una organización.

- **CERT/CSIRT**: Equipo de Respuesta ante Emergencias Informáticas e Incidentes de Seguridad de la Información.

- **CHECKLISTS**: Lista de control de tareas de una actividad que reduce los olvidos y errores de coherencia e integridad en su realización.

- **CIBERSEGURIDAD**: Práctica de protección de la información que se encuentra en formato digital y se ubica en los activos de información interconectados de una organización con medidas preventivas, defensivas y ofensivas.

- **CIFRADO**: Proceso que transforma datos legibles en ilegibles para proteger la lectura no deseada de su información.

- **CISO**: Máximo responsable de la Seguridad de la Información de una organización.
- **CONFIDENCIALIDAD**: Propiedad de la seguridad de la información que protege a la información para que sólo sea accesible por quien tiene autorización (lo tiene permitido), ya sea persona, entidad, aplicación o proceso.
- **CONFIABILIDAD**: Propiedad de la seguridad de la información que garantiza el correcto cumplimiento de todas las propiedades de la información.
- **DIAGRAMA DE GANTT**: Estructura gráfica que muestra el cronograma de las tareas que se planifican para la ejecución de un proyecto.
- **DIGITALIZACIÓN**: Proceso que transforma datos físicos o analógicos en digitales.
- **DISPONIBILIDAD**: Propiedad de la seguridad de la información que respalda que la información se encuentra a disposición de quien tenga autorización cuando la necesite; es decir, que siempre esté dispuesta para el autorizado que la requiera.
- **EFICACIA**: Facultad para lograr los objetivos y metas propuestas sin importar los recursos usados.
- **EFICIENCIA**: Facultad para lograr los objetivos y metas propuestas con los mínimos recursos posibles.
- **EVENTO DE CIBERSEGURIDAD**: Suceso que supone un riesgo de ciberseguridad para un activo de información de una organización, pero sin perjuicio en los objetivos ni las operaciones del negocio.
- **EXFILTRACIÓN**: Robo, movimiento o publicación de información confidencial, secreta o privada de una organización para usarse sin autorización de su propietario.
- **FALSO POSITIVO**: Alerta de ciberseguridad que, tras su análisis, no debería notificarse como amenaza de ciberseguridad, ya que no se corresponde con ninguna o se ha ejecutado a conciencia por el área de ciberseguridad para prevenir o detectar vulnerabilidades o errores de ciberseguridad.
- **IMPACTO**: Consecuencia de que una amenaza de ciberseguridad se materialice sobre un activo de información con la explotación de una vulnerabilidad.
- **INCIDENTE DE CIBERSEGURIDAD (CIBERINCIDENTE)**: Materialización de una amenaza con o sin impacto sobre cualquiera de los activos de información de una organización.
- **INFORMACIÓN**: Conjunto de datos asociados y procesados que, en un contexto determinado, tienen significado y se comprenden e interpretan.
- **ISO (ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN**: Organización centralizada y formada por diferentes entidades nacionales de normalización y que se responsabiliza de la creación y mantenimiento de los estándares internacionales.
- **INTEGRIDAD**: Propiedad de la seguridad de la información que ampara a la información para que no pueda ser alterada en ninguna de sus formas y que asegura la veracidad de sus datos.
- **REGISTRO LOG**: Fichero que almacena los sucesos, las actividades ejecutadas y los eventos detectados que se producen de manera cronológica en un activo tecnológico de información.
- **MALWARE**: Software o artefacto malicioso que se instala en un sistema objetivo sin consentimiento del propietario para realizar acciones dañinas sobre sus datos, su propietario o su propiedad intelectual de manera intencionada.
- **METADATOS**: Datos que identifican y aportan información única de otros datos.

- **METODOLOGÍA**: Conjunto de definiciones, conocimientos, métodos, procedimientos y mecanismos que se utilizan para garantizar el éxito de la ejecución de una actividad o proyecto, así como de sus objetivos.

- **METODOLOGÍA ÁGIL**: Método para el desarrollo de proyectos que se desarrollan a través de la creación de pequeños incrementos de actividades para facilitar su flexibilidad y rapidez y del suministro entregas parciales que muestren su evolución.

- **MONITORIZACIÓN**: Supervisión y análisis en tiempo real del rendimiento, la situación y el estado de los activos de información de una organización para alertar y responder ante los sucesos anómalos o no deseados.

- **NO REPUDIO**: Propiedad de la seguridad de la información que avala que el ejecutor de una acción no pueda negar que la ha realizado.

- **PARTES INTERESADAS o INTERVINIENTES**: Conjunto de recursos humanos, internos y externos, o de organizaciones que intervienen, influyen y se interesan por las actividades de proyectos y negocios de una organización.

- **PENETRACIÓN**: Ataque de ciberseguridad que consiste en la intrusión y explotación de las vulnerabilidades de los activos tecnológicos de información de una organización.

- **PRIVACIDAD**: Propiedad de la seguridad de la información que protege al sujeto que realiza acciones sobre la información de ser observado y de tener restricciones sobre su propia identidad.

- **PROCESO DE NEGOCIO**: Conjunto de actividades y operaciones estructuradas sucesivamente que producen un producto o servicio vital para el negocio de una organización.

- **RIESGO DE CIBERSEGURIDAD**: Probabilidad de que se materialice una amenaza de ciberseguridad en cualquiera de los activos tecnológicos de una organización y pueda causar un incidente de ciberseguridad.

- **SEGURIDAD DE LA INFORMACIÓN**: Práctica de protección de la información que se encuentra en cualquiera de sus formatos y estados y se ubica en los activos de información interconectados o no de una organización con medidas preventivas, defensivas y ofensivas. Además, se considera un súper conjunto de la Seguridad Informática y la Ciberseguridad.

- **SEGURIDAD INFORMÁTICA**: Práctica de protección de la información que se encuentra en formato digital y se ubica contenida en los activos de información digital de una organización con medidas preventivas y defensivas.

- **SISTEMA DE INFORMACIÓN (SI)**: Conjunto ordenado de componentes y datos que interactúan entre sí con un fin común.

- **TECNOLOGÍA DE LA INFORMACIÓN (TI)**: Conjunto ordenado de sistemas, herramientas, aplicaciones, infraestructuras y resto de activos relacionados con el aprovisionamiento, el tratamiento y la transferencia de los componentes y datos de los Sistemas de Información (SI).

- **TRAZABILIDAD**: Propiedad de la seguridad de la información que asegura el histórico, la ubicación y la trayectoria de origen a destino de la información.

- **TRIAJE**: Protocolo o método de selección, verificación, priorización y clasificación de las alertas, los eventos y los incidentes de ciberseguridad.

- **VULNERABILIDAD**: Debilidad, fallo o deficiencia en cualquiera de los activos tecnológicos de una organización que se puede convertir en un incidente de ciberseguridad con o sin impacto.

6. Bibliografía

- **Aarons, Michelle** (2020, febrero). “Colorful cybersecurity: Know what red, blue, and yellow mean” [artículo en línea]. Medium [Fecha de consulta: 21 de noviembre de 2022]. <https://ww1.medium.com/colorful-cybersecurity-know-what-red-blue-and-yellow-mean-6a895865fd5>

- **Acosta, David** (2018, agosto). “¿Qué es PCI DSS?” [artículo en línea]. PCI Hispano [Fecha de consulta: 15 de octubre de 2022]. <https://www.pcihispano.com/que-es-pci-dss/>

- **AFS Informática** (s.f.). “Tácticas, Técnicas y Procedimientos (TTP)” [artículo en línea]. AFS Informática [Fecha de consulta: 15 de octubre de 2022]. <https://www.afsinformatica.com/tacticas-tecnicas-y-procedimientos-ttp/>

- **Agencia Española de Protección de Datos** (2019, octubre). “Guía de Privacidad desde el Diseño” [artículo en línea]. AEPD [Fecha de consulta: 28 de octubre de 2022]. <https://www.aepd.es/es/documento/guia-privacidad-desde-diseno.pdf>

- **Agencia Estatal Boletín Oficial del Estado** (s.f.). <<Todas las Leyes, Leyes Orgánicas, Reales Decretos, Reales Decretos Ley y Reglamentos indicados en este documento>>. [artículos en línea]. Agencia Estatal del Boletín Oficial del Estado. Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática. Gobierno de España [Fecha de consulta: 9 de octubre de 2022]. <https://www.boe.es/buscar/>

- **Anomali** (s.f.). “¿Qué son STIX y TAXII?” [artículo en línea]. Anomali [Fecha de consulta: 12 de octubre de 2022]. <https://www.anomali.com/es/resources/what-are-stix-taxii>

- **Asociación Española de Normalización** (2017, mayo). “Norma Española UNE-EN ISO/IEC 27002” [artículo en línea]. Publicado por AENOR Internacional, S.A.U. bajo licencia de la Asociación Española de Normalización (UNE). Obtenido en la biblioteca de Universitat Oberta de Catalunya (UOC). Asociación Española de Normalización (UNE) [Fecha de consulta: 10 de octubre de 2022]. <https://ra.biblioteca.uoc.edu/prestatgeries/articles/protegits/B2627/027002NEII100_ES.pdf>

- **Briskinfosec** (junio, 2022). “Red vs Blue vs Purple vs Orange vs Yellow vs Green vs White Cybersecurity Team” [artículo en línea]. Briskinfosec [Fecha de consulta: 1 de noviembre de 2022]. <https://www.briskinfosec.com/blogs/blogsdetail/Red-vs-Blue-vs-Purple-vs-Orange-vs-Yellow-vs-Green-vs-White-Cybersecurity-Team>

- **Brownlee, N. & Guttman, E.** (1998, junio). “Expectations for Computer Security Incident Response” [artículo en línea]. IETF [Fecha de consulta: 18 de octubre de 2022]. <https://datatracker.ietf.org/doc/html/rfc2350>

- **Candau, Javier** (2021, septiembre). “Ciberseguridad. Evolución y tendencias” [artículo en línea]. Instituto Español de Estudios Estratégicos [Fecha de consulta: 10 de octubre de 2022]. <https://www.ieee.es/Galerias/fichero/docs_marco/2021/DIEEEM11_2021_JAVCAND_Ciberseguridad.pdf>

- **CCN** (2019, marzo). “Guía de seguridad (CCN-STIC-801). Esquema Nacional de Seguridad. Responsabilidades Y Funciones” [artículo en línea]. Fundació Universitat Oberta de Catalunya (FUOC). UOC [Fecha de consulta: 24 de septiembre de 2022]. <https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/801-Responsabilidades_en_el_ENS/801_ENS-responsabilidades_feb-11.pdf>

- **CCN** (2020, abril). “Guía de Seguridad de las TIC CCN-STIC 817. Esquema Nacional de Seguridad. Gestión de ciberincidentes” [artículo en línea]. CCN-Cert. Centro Criptológico Nacional (CCN) [Fecha de consulta: 4 de junio de 2022]. <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html>

- **CCN** (s.f.). “ENS” [artículo en línea]. CCN [Fecha de consulta: 17 de octubre de 2022]. <https://ens.ccn.cni.es/es/esquema-nacional-de-seguridad-ens>

- **Ciberseguridad** (s.f.). “QUÉ ES EL MARCO MITRE ATT&CK Y CÓMO IMPLEMENTARLO” [artículo en línea]. Ciberseguridad [Fecha de consulta: 15 de octubre de 2022]. <https://ciberseguridad.com/herramientas/marco-mitre-att-ck/>

- **Comité Europeo de Protección de Datos** (2020, enero). “Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de vídeo” [artículo en línea]. Versión 2. EDPB. [Fecha de consulta: 9 de octubre de 2022]. <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_es.pdf>

- **Cruz Allende, Daniel & Tortajada Gallego, Arsenio & Segovia Henares, Antonio José** (2020, septiembre). “Planes de continuidad de negocio” [artículo en línea]. Fundació Universitat Oberta de Catalunya (FUOC). UOC [Fecha de consulta: 4 de diciembre de 2021]. <https://materials.campus.uoc.edu/daisy/Materials/PID_00275347/pdf/PID_00275347.pdf>

- **CSIRT-KIT** (s.f.). “CSIRT TOOLS KIT” [artículo en línea]. CSIRT-KIT [Fecha de consulta: 28 de marzo de 2022]. <https://csirt-kit.org/#services>

- **Diario Oficial de la Unión Europea** (2016, abril). “Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)” [artículo en línea]. Publicado en el BOE. Parlamento Europeo y Consejo de la Unión Europea [Fecha de consulta: 1 de octubre de 2021]. <https://www.boe.es/doue/2016/119/L00001-00088.pdf>

- **Díaz Pérez, Antonio** (2021, junio). “Diseño de la implementación de un Centro de Operaciones de Seguridad (SOC) basado en ITIL” [artículo en línea]. Gallifa Roca, Joan & Daradoumis Haralabus, Atanasi. Trabajo Final de Grado de Ingeniería Informática. UOC. [Fecha de consulta: 15 de diciembre de 2022]. <https://openaccess.uoc.edu/bitstream/10609/132246/6/antoniodTFG0621memoria.pdf>

- **ENISA** (s.f.). “Acerca de la ENISA - Agencia de la Unión Europea para la Ciberseguridad” [artículo en línea]. ENISA [Fecha de consulta: 30 de octubre de 2022]. <https://www.enisa.europa.eu/about-enisa/about/es>

- **ENISA** (2020, diciembre). “How to set up CSIRT and SOC” [artículo en línea]. ENISA [Fecha de consulta: 01 de octubre de 2022]. <https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc>

- **Estevan de Quesada, Rafael** (2022, febrero). “Auditoría técnica de seguridad de sistemas de información y comunicaciones” [artículo en línea]. Coordinador: Garrigues Olivella, Carles. Fundació Universitat Oberta de Catalunya (FUOC). UOC [Fecha de consulta: 14 de octubre de 2022]. <https://materials.campus.uoc.edu/daisy/Materials/PID_00285945/pdf/PID_00285945.pdf>

- **Filipkowski**, Ben (s.f.). “What is the difference between MDR, XDR, and EDR?” [artículo en línea]. Field Effect [Fecha de consulta: 21 de noviembre de 2022]. <https://fieldeffect.com/blog/mdr-xdr-edr/>

- **Flores Terrón, Miguel Ángel** (2022, febrero). “Fundamentos de DevSecOps” [artículo en línea]. Coordinador: Jorba Esteve, Josep. Fundació Universitat Oberta de Catalunya (FUOC). UOC [Fecha de consulta: 20 de octubre de 2022]. <https://materials.campus.uoc.edu/daisy/Materials/PID_00286171/pdf/PID_00286171.pdf>

- **Fouz, Carlos** (2021, febrero). “Introducción a las vulnerabilidades” [artículo en línea]. Coord: Rifà Pous, Helena. Fundació Universitat Oberta de Catalunya (FUOC). UOC [Fecha de consulta: 29 de septiembre de 2022]. <https://materials.campus.uoc.edu/daisy/Materials/PID_00274038/pdf/PID_00274038.pdf>

- **Frayssinet, Maurice** (2022, febrero). “Implementación del Centro de operaciones de seguridad (SOC)” [multimedia en línea]. Youtube [Fecha de consulta: 15 de diciembre de 2022]. <https://www.youtube.com/watch?v=QyEGELTFkvU>

- **Garre Gui, Silvia & Segovia Henares, Antonio José & Tortajada Gallego, Arsenio** (2020, septiembre). “Implantación de un sistema de gestión de la seguridad de la información (SGSI)” [artículo en línea]. Fundació Universitat Oberta de Catalunya (FUOC). UOC [Fecha de consulta: 7 de noviembre de 2022]. <https://materials.campus.uoc.edu/daisy/Materials/PID_00275348/pdf/PID_00275348.pdf>

- **Garre Gui, Silvia & Segovia Henares, Antonio José & Tortajada Gallego, Arsenio** (2020, septiembre). “Introducción a la seguridad de la información” [artículo en línea]. Fundació Universitat Oberta de Catalunya (FUOC). UOC [Fecha de consulta: 30 de septiembre de 2022]. <https://materials.campus.uoc.edu/daisy/Materials/PID_00275350/pdf/PID_00275350.pdf>

- **Grupo Atico34** (s.f.). “Los 10 mejores Firewall o cortafuegos para Windows” [artículo en línea]. Grupo Atico34 [Fecha de consulta: 21 de noviembre de 2022]. <https://protecciondatos-lopd.com/empresas/mejores-firewall-windows/>

- **Guijarro Olivares, Jordi** (2022, febrero). “Introducción a la seguridad en *cloud computing*” [artículo en línea]. Coordinador: Jorba Esteve, Josep. Fundació Universitat Oberta de Catalunya (FUOC). UOC [Fecha de consulta: 01 de marzo de 2022]. <https://materials.campus.uoc.edu/daisy/Materials/PID_00285949/pdf/PID_00285949.pdf>

- **Hartmans, Avery** (2022, marzo). “5 de los ciberataques más comunes, desde las inyecciones de código a los de fuerza bruta, y cómo han sido usados en conflictos anteriores” [artículo en línea]. Business Insider [Fecha de consulta: 21 de noviembre de 2022]. <https://www.businessinsider.es/5-ciberataques-comunes-han-visto-otros-conflictos-1024341>

- **INCIBE** (2016, noviembre). “CEO, CISO, CIO… ¿Roles en ciberseguridad?” [artículo en línea]. INCIBE [Fecha de consulta: 17 de septiembre de 2021]. <https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad>

- **INGERTEC** (s.f.). “Nueva Versión ISO 27001:2022” [artículo en línea]. INGERTEC [Fecha de consulta: 30 de octubre de 2022]. <https://ingertec.com/nueva-version-iso-27001-2022/>

- **Infofive** (2021, marzo). “Cuál es la diferencia entre seguridad informática y ciberseguridad en una empresa” [artículo en línea]. Infofive [Fecha de consulta: 3 de octubre de 2022]. <https://infofive.com/cual-es-la-diferencia-entre-seguridad-informatica-y-ciberseguridad-en-una-empresa/>

- **InvGate** (2021, mayo). “Gestión de seguridad de la información en un mundo ITIL 4” [artículo en línea]. InvGate [Fecha de consulta: 15 de octubre de 2022]. <https://blog.invgate.com/es/gesti%C3%B3n-de-seguridad-de-la-informaci%C3%B3n-en-un-mundo-itil-4>

- **ISO Tools** (2022, junio). “ISO/IEC 27002:2022 Controles Organizacionales. Todo lo que necesita saber” [artículo en línea]. ISO Tools [Fecha de consulta: 30 de octubre de 2022]. https://www.isotools.org/2022/07/29/iso-iec-270022022-controles-organizacionales-todo-lo-que-necesitas-saber/

- **ISO Tools** (2022, septiembre). “Transición a ISO/IEC 27001:2022. Requisitos” [artículo en línea]. ISO Tools [Fecha de consulta: 30 de octubre de 2022]. <https://www.isotools.org/2022/09/09/transicion-a-iso-iec-270012022-requisitos/>

- **Kaspersky** (s.f.). “Las 7 principales ciberamenazas a las que hay que prestar atención” [artículo en línea]. Kaspersky [Fecha de consulta: 21 de noviembre de 2022]. <https://www.kaspersky.es/resource-center/threats/top-7-cyberthreats>

- **KeepCoding** (2022, agosto). “¿Qué es un vector de ataque en ciberseguridad?” [artículo en línea]. KeepCoding [Fecha de consulta: 8 de octubre de 2022]. <https://keepcoding.io/blog/que-es-un-vector-de-ataque-en-ciberseguridad/>

- **LISA Institute** (2021, marzo). “Diferencia entre Ciberseguridad, Seguridad Informática y Seguridad de la Información” [artículo en línea]. LISA Institute [Fecha de consulta: 3 de octubre de 2022]. <https://www.lisainstitute.com/blogs/blog/diferencia-ciberseguridad-seguridad-informatica-seguridad-informacion>

- **Mahn, Amy & Marron, Jeffrey & Quinn, Stephen & Topper, Daniel** (2021, agosto). “Primeros pasos de NIST. Marco de ciberseguridad: Guía de inicio rápido” [artículo en línea]. NIST [Fecha de consulta: 12 de octubre de 2022]. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271es.pdf>

- **Martínez Gómez, Mònica** (2021, septiembre). “Implementación de un centro de operaciones de seguridad (SOC) de código abierto con elementos de red para sistemas industriales.” [artículo en línea]. López Patiño, José Enrique. Trabajo Final de Grado de Ingeniería de Tecnologías y Servicios de Telecomunicación. Escuela Técnica Superior de Ingeniería de Telecomunicación. Universitat Politècnica de València. [Fecha de consulta: 15 de diciembre de 2022]. <https://riunet.upv.es/bitstream/handle/10251/174344/Martinez%20-%20Implementacion%20de%20un%20centro%20de%20operaciones%20de%20seguridad%20SOC%20de%20codigo%20abierto%20con%20elem....pdf>

- **Martínez, Roger & Fouz, Carlos** (2021, febrero). “Introducción a las ciberamenazas” [artículo en línea]. Coord: Rifà Pous, Helena. Fundació Universitat Oberta de Catalunya (FUOC). UOC [Fecha de consulta: 30 de septiembre de 2022]. <https://materials.campus.uoc.edu/daisy/Materials/PID_00274039/pdf/PID_00274039.pdf>

- **Mir Rubio, Joan** (2020, septiembre). “Riesgos, vulnerabilidades y amenazas” [artículo en línea]. Coord: Rifà Pous, Helena. Fundació Universitat Oberta de Catalunya (FUOC). UOC [Fecha de consulta: 29 de septiembre de 2022]. <https://materials.campus.uoc.edu/daisy/Materials/PID_00276303/pdf/PID_00276303.pdf>

- **Mir Rubio, Joan** (2020, septiembre). “Ataques” [artículo en línea]. Coord: Rifà Pous, Helena. Fundació Universitat Oberta de Catalunya (FUOC). UOC [Fecha de consulta: 15 de noviembre de 2022]. <https://materials.campus.uoc.edu/daisy/Materials/PID_00276300/pdf/PID_00276300.pdf>

- **Mir Rubio, Joan** (2020, septiembre). “Sistemas de protección, prevención y detección” [artículo en línea]. Coord: Rifà Pous, Helena. Fundació Universitat Oberta de Catalunya (FUOC). UOC [Fecha de consulta: 16 de noviembre de 2022]. <https://materials.campus.uoc.edu/daisy/Materials/PID_00276302/pdf/PID_00276302.pdf>

- **Mitre** (2022, abril). “Enterprise Matrix” [artículo en línea]. Mitre [Fecha de consulta: 12 de octubre de 2022]. <https://attack.mitre.org/matrices/enterprise/>

- **Molina Caza, Christian Rubén** (2020, diciembre). “Desarrollo e implementación de un SOC en el Consejo de Aseguramiento de la Calidad de la Educación Superior.” [artículo en línea]. Brande Hernández, Daniel & García Font, Víctor. Trabajo Final de Máster de Seguridad de las Tecnologías de la Información y las Comunicaciones. UOC. [Fecha de consulta: 15 de diciembre de 2022]. <https://openaccess.uoc.edu/bitstream/10609/126988/7/cmolinacazTFM220memoria.pdf>

- **Naciones Unidas** (s.f.). “17 objetivos para transformar nuestro mundo” [artículo en línea]. Naciones Unidas [Fecha de consulta: 29 de septiembre de 2022]. <https://www.un.org/sustainabledevelopment/es/infrastructure/>

- **Naciones Unidas** (s.f.). “La Agenda para el Desarrollo Sostenible” [artículo en línea]. Naciones Unidas [Fecha de consulta: 29 de septiembre de 2022]. <https://www.un.org/sustainabledevelopment/es/development-agenda/>

- **NIST** (s.f.). “CYBERSECURITY FRAMEWORK” [artículo en línea]. NIST [Fecha de consulta: 12 de octubre de 2022]. <https://www.nist.gov/cyberframework>

- **Noticias Tech** (2022, enero). “Actualízate: 4 desafíos para el SOC en el futuro” [artículo en línea]. Noticias Tech [Fecha de consulta: 17 de octubre de 2022]. <https://intelectoweb.com/web/tech/2022/01/24/actualizate-4-desafios-para-el-soc-en-el-futuro/>

- **Oodrive** (2021, marzo). “Los 10 principales tipos de ciberataques” [artículo en línea]. Oodrive [Fecha de consulta: 7 de octubre de 2022]. <https://www.oodrive.com/es/blog/seguridad/top-10-principales-tipos-de-ciberataques/>

- **Peña Juárez, Juan** (2021, junio). “Desarrollo e implementación de un SOC en una organización” [artículo en línea]. Brande Hernández, Daniel & García Font, Víctor. Trabajo Final de Máster de Seguridad de las Tecnologías de la Información y las Comunicaciones. UOC, URV y UAB. [Fecha de consulta: 15 de diciembre de 2022]. <https://openaccess.uoc.edu/bitstream/10609/133128/6/juapejuaTFM0621memoria.pdf>

- **PMG SSI** (2017, febrero). “¿Cómo realizar un inventario de activos de información?” [artículo en línea]. PMG SSI [Fecha de consulta: 24 de septiembre de 2021]. <https://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/>

- **Privasec** (2021, junio). “Red, Blue, Purple, White, Black & Gold Team” [artículo en línea]. Privasec [Fecha de consulta: 1 de noviembre de 2022]. <https://privasec.com/blog/coloredteams/>

- **QuestionPro** (s.f.). “¿Qué es la Investigación Exploratoria?” [artículo en línea]. QuestionPro [Fecha de consulta: 30 de septiembre de 2022]. <https://www.questionpro.com/blog/es/investigacion-exploratoria/>

- **QuestionPro** (s.f.). “¿Qué es la investigación descriptiva?” [artículo en línea]. QuestionPro [Fecha de consulta: 30 de septiembre de 2022]. <https://www.questionpro.com/blog/es/investigacion-descriptiva/>

- **Román Torres, María José** (2019, enero). “Proceso para definir y establecer un Centro de Operaciones de Seguridad (SOC) en una organización financiera” [artículo en línea]. Rubio Blanco, José Antonio. Trabajo Final de Máster. Universidad Internacional de la Rioja. Guayaquil. [Fecha de consulta: 17 de noviembre de 2022]. <https://reunir.unir.net/bitstream/handle/123456789/8169/ROMAN%20TORRES%2C%20MARIA%20JOSE.pdf?sequence=1&isAllowed=y>

- **Rodríguez, José Ramón** (s.f.). “La gestión de proyectos. Conceptos básicos.” [artículo en línea]. Coordinador: Jorba Esteve, Josep. Fundació Universitat Oberta de Catalunya (FUOC). UOC [Fecha de consulta: 02 de diciembre de 2022]. <http://cv.uoc.edu/annotation/ebc1adfc61836d7205ad7dde343367b5/603266/PID_00153570/PID_00153570.html>

- **Salas Piñón, Julián** (2020, septiembre). “Introducción a la privacidad” [artículo en línea]. Coordinadora: Pérez Solà, Cristina. Fundació Universitat Oberta de Catalunya (FUOC). UOC [Fecha de consulta: 25 de febrero de 2022]. <http://cvapp.uoc.edu/autors/MostraPDFMaterialAction.do?id=274691>

- **Smartekh** (2021, julio). “¿Qué es SOAR y qué beneficios tiene para tu organización?” [artículo en línea]. Smartekh [Fecha de consulta: 21 de noviembre de 2022]. <https://blog.smartekh.com/que-es-soar-y-que-beneficios-tiene-para-tu-organizacion>

- **TI América** (2022, marzo). “Conoce los 5 tipos de firewall más importantes que existen” [artículo en línea]. TI América [Fecha de consulta: 27 de octubre de 2022]. <https://www.ti-america.com/tipos-de-firewall-que-pueden-integrar-en-su-arquitectura-de-ti/>

- **Toledo, Rogelio** (s.f.). “Características de un SOC de ciberseguridad completo” [artículo en línea]. Cibernos [Fecha de consulta: 30 de octubre de 2022]. <https://www.grupocibernos.com/blog/caracteristicas-de-un-soc-de-ciberseguridad-completo>

- **UOC** (2022, septiembre). “Guía transversal para el estudiantado de TF de los Estudios de Informática, Multimedia y Telecomunicación. ¿Cómo incorporar la competencia "Comportamiento ético y global" al Trabajo Final (TF)?” [artículo en línea]. FUOC - Fundación para la Universitat Oberta de Catalunya [Fecha de consulta: 10 de octubre de 2022]. <https://campus.uoc.edu/webapps/classroom/download.do?nav=activitats&sub-nav=descarregar-adjunt&id=904645&serial=false&s=203d94519019eaf71b70501c051dcff94a7605044654ff4d7693f7afc566f2d824a0e0a040d6a88085c23834e1022ce1ed13a8227f300824d6f543402dcab1bd&domainId=896030&proposedFilename=04.+Guia+transversal+sobre+la+CCEG+dirigida+a+estudiantado+de+TFx-EIMT_vPublicada.pdf&idLang=&javascriptDisabled=false&subjectId=896030&domainCode=221_m1_887_01&classroomId=901115>

7. Anexos

7.1 Anexo 1: Análisis del marco preliminar y conceptual de un SOC

Con el fin de comprender las nociones necesarias para la gestión de la Seguridad de la Información, la gestión de la ciberseguridad y, por consiguiente, los criterios para la implantación y funcionamiento diario de un SOC, a continuación, se resume el análisis y estudio de los conceptos más importantes de la Seguridad de la Información relacionados con esta área y que se han estudiado y repasado en las diferentes asignaturas del máster universitario de Ciberseguridad y Privacidad de la UOC.

7.1.1 Seguridad de la Información

7.1.1.1 Definición y objetivos de la Seguridad de la Información

La **Seguridad de la Información**, tal y como se ha indicado en la introducción de este documento, se define como el conjunto de medidas de protección de la información en todas sus formas, como puede ser la oral, la electrónica o la escrita, entre otras, y en todas las fases de su ciclo de vida, como, por ejemplo, en su creación, distribución, uso o almacenamiento. Además, debido a que la información se considera uno de los activos más importantes, a nivel empresarial, su seguridad se describe como un proceso de negocio que se debe incorporar en el funcionamiento diario de toda organización para gestionarlo y complementarlo con los demás procesos de alto nivel.

Asimismo, tal y como se indicaba en la Introducción, se recalca que la Seguridad de la Información no debe confundirse ni con la Seguridad Informática ni con la Ciberseguridad, ya que se concibe como un conjunto global que protege la información en todos sus estados y engloba a estas otras dos disciplinas. De hecho, se recuerda que la Seguridad Informática se encarga de proteger la información contenida sólo en los activos de información digital mediante medidas de prevención y de protección y la Ciberseguridad se encarga de proteger la información en formato digital de los activos de información interconectados, pero con medidas tanto preventivas como ofensivas para su protección.

Por otra parte, el **objetivo principal** de esta disciplina, como proceso de negocio de una organización, se basa en la protección de la información en todas sus propiedades y de todos sus activos de las posibles amenazas que puedan afectar de alguna manera a las operaciones de negocio de la propia organización. Igualmente, con el fin de lograr el éxito en este objetivo principal, se requiere de, entre otros, los diferentes propósitos específicos:

- Garantizar el uso responsable de los activos de información de la organización.
- Gestionar y minimizar los posibles riesgos en los procesos de negocio de la organización.
- Identificar, prevenir y combatir las amenazas a la Seguridad de la Información.
- Gestionar los eventos e incidentes de seguridad detectados en la organización.

- Asegurar la continuidad del negocio y la recuperación inmediata de las operaciones.
- Cumplir con los requerimientos, normativas y disposiciones legales aplicables a la organización.

7.1.1.2 Propiedades de la información

La Seguridad de la Información se resume como la defensa continuada de las propiedades fundamentales y básicas de los datos que componen la información y que guían a sus políticas de seguridad en las organizaciones. Se trata del resguardo de la confidencialidad, de la integridad y de la disponibilidad, como pilares fundamentales que se conocen como Triada de la información, y de la autenticidad, del no repudio, de la trazabilidad, de la responsabilidad o auditabilidad, de la confiabilidad, del anonimato y de la privacidad, como cualidades importantes incluidas en la legislación vigente, pero que no siempre se requieren. A continuación, se define cada una de estas propiedades:

- **Confidencialidad**: Se trata de la propiedad de la seguridad de la información que protege a la información para que sólo sea accesible por quien tiene autorización, ya sea persona, entidad, aplicación o proceso; es decir, que no sea accesible por quien no lo tenga permitido.
- **Integridad**: Se trata de la propiedad de la seguridad de la información que ampara a la información para que no pueda ser alterada en ninguna de sus formas y que asegura la veracidad de sus datos.
- **Disponibilidad**: Se trata de la propiedad de la seguridad de la información que respalda que la información se encuentra a disposición de quien tenga autorización a ella cuando la necesite; es decir, que siempre esté dispuesta para la persona, entidad, aplicación o proceso autorizado que la requiera.
- **Autenticidad**: Se trata de la propiedad de la seguridad de la información que garantiza la identidad del suministrador de la información; es decir, que certifica que el autor de la comunicación de la información es quien dice ser.
- **No repudio**: Se trata de la propiedad de la seguridad de la información que avala que el ejecutor de una determinada acción sobre la información no pueda negar que la ha realizado.
- **Trazabilidad**: Se trata de la propiedad de la seguridad de la información que asegura el histórico, la ubicación y la trayectoria de la información desde su origen hasta su destino.
- **Responsabilidad** o **auditabilidad**: Se trata de la propiedad de la seguridad de la información que garantiza el registro y la monitorización del uso de la información por parte de usuarios, aplicaciones o procesos conectados y autorizados.
- **Confiabilidad**: Se trata de la propiedad de la seguridad de la información que garantiza el correcto cumplimiento de todas las propiedades de la información.
- **Anonimato**: Se trata de la propiedad de la seguridad de la información que protege del reconocimiento de un sujeto en cualquier acción que realice sobre la información para de salvaguardar su identidad.
- **Privacidad**: Se trata de la propiedad de la seguridad de la información que protege al sujeto que realiza acciones sobre la información de ser observado y de tener restricciones sobre su propia identidad.

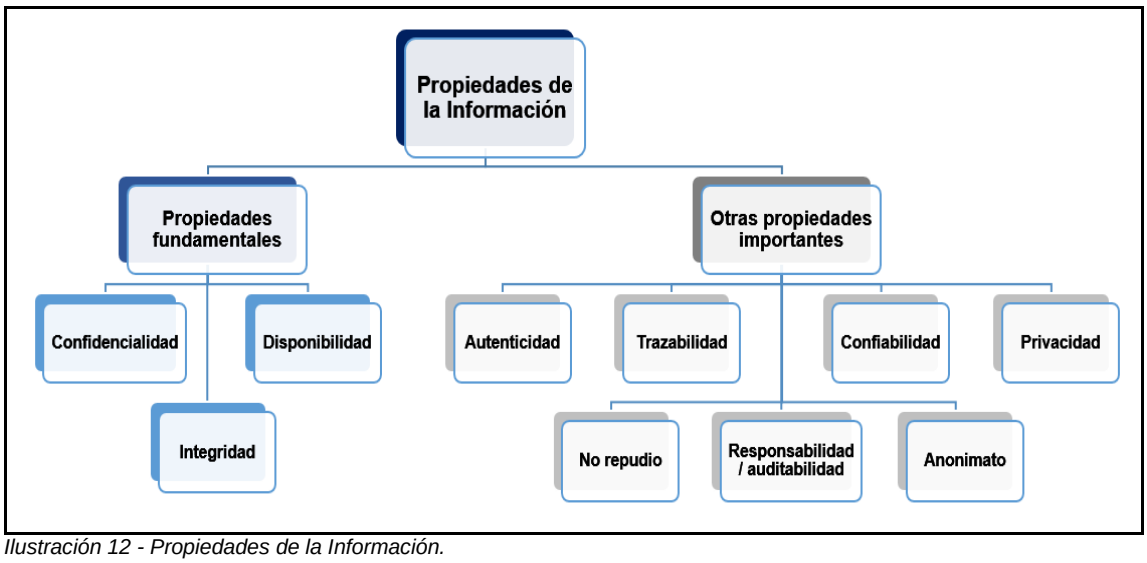

Ilustración 12 - Propiedades de la Información.

7.1.1.3 Gestión de la Seguridad de la información

La Gestión de la Seguridad de la Información se define como la aplicación del conjunto de actividades que protegen los datos que constituyen la información de cualquier posible amenaza. Se trata del proceso continuo que engloba todas las tareas necesarias para proporcionar seguridad a la información y que tiene como objetivo la salvaguarda de sus propiedades mediante el establecimiento y mantenimiento de actividades, métodos y documentos, como pueden ser los siguientes:

- **Políticas de Seguridad de la Información**: Se trata del grupo de documentos que explica las actividades y los controles necesarios para determinar que la información de una organización se considera segura. De hecho, en su conjunto, explican lo que se quiere proteger, contra quién se quiere realizar esa protección y cómo se va a llevar a cabo.
- **Controles de Seguridad**: Se trata del grupo de actividades que forman la protección global de la información, mediante buenas prácticas, para reducir el nivel de riesgo y mitigar los posibles ataques.
- **Procedimientos de Seguridad**: Se trata del conjunto de documentos que indican las acciones que se deben realizar y cómo realizarlas para proteger la información y sus activos.

Asimismo, las actividades necesarias para conseguir los objetivos de la Seguridad de la Información se pueden organizar desde diferentes perspectivas:

- **Según su naturaleza**: Se trata de las actividades y controles humanos, organizativos, técnicos o legales:
    - **Controles humanos**: Actividades que engloban todos los recursos humanos de la organización para facilitar capacitación, asignar responsabilidades y revisar los controles, con el fin de proteger la información.
    - **Controles organizativos**: Actividades que engloban todos los recursos de la entidad para definir e instaurar la Política de Seguridad y los diferentes planes, como el de Contingencia, con el fin de proteger la información y alinear su seguridad con el negocio.

    - **Controles técnicos**: Actividades que engloban todos los recursos digitales para instaurar sistemas seguros, con el fin de proteger la información y todos sus activos.
    - **Controles legales**: Actividades que engloban todos los recursos normativos y legales, con el fin de proteger la información y el cumplimiento de cláusulas, normativas y leyes.

- **Según su actuación**: Se trata de las actividades y controles que aplican sobre la reducción del impacto o de su probabilidad:
    - **Controles que reducen el impacto**: Actividades que engloban todos los recursos para minimizar el impacto en el negocio si se materializa una amenaza, con el fin de proteger la información.
    - **Controles que reducen su probabilidad**: Actividades que engloban todos los recursos para minimizar la probabilidad de la materialización de una amenaza, con el fin de proteger la información.

- **Según su finalidad**: Se trata de las actividades y controles que actúan en base al ciclo de vida de un posible incidente de seguridad:
    - **Controles de prevención**: Actividades que engloban todos los recursos que minimizan la ocurrencia de un riesgo para que no se materialice, con el fin de proteger la información.
    - **Controles de monitorización**: Actividades que engloban todos los recursos que visualizan eventos para evidenciar y rastrear anomalías, con el fin de proteger la información.
    - **Controles de detección**: Actividades que engloban todos los recursos que localizan los posibles incidentes de seguridad con celeridad.
    - **Controles de corrección**: Actividades que engloban todos los recursos que reducen la afección y recuperan la estabilidad tras un incidente.

7.1.1.4 Modelos de Gestión de la Seguridad de la información

La Seguridad de la información se puede gestionar en base a diferentes modelos, totalmente válidos en dependencia del tipo de organización, que se dividen en tres enfoques diferentes: los modelos de gestión interna, los modelos de gestión externalizada y los modelos mixtos. A continuación, se presentan los puntos a favor y en contra de cada modelo de gestión, así como la comparación de cada uno de ellos:

- **Gestión interna de la seguridad de la información**: Este modelo permite formar al personal de otras empresas y organizaciones especializado en Seguridad de la Información, así como gestionar de forma externa su seguridad. Además, también permite aportar el conocimiento del modelo de negocios de la organización para las empresas de gestión de seguridad externas, lo que se ejecuta también en el modelo de gestión mixto. Entre otras, algunas ventajas y desventajas pueden ser:
    - **Ventajas**:
        - Se utiliza personal interno de las organizaciones para los procesos de gestión de la seguridad de la información.
        - Se contrata personal especializado en el área de seguridad de la información.
        - Se capacita al personal de la organización en seguridad de la información.
        - Se tiene el conocimiento del dominio del modelo de negocio y de sus procesos.

        - Se involucra al personal en todos los procesos.
        - Se conforma un equipo para la seguridad de la información con un responsable y con dimensiones acordes con el tamaño de la organización.
    - **Inconvenientes**:
        - Se puede realizar una vulneración de la seguridad de la información por parte del personal interno.
        - Se elevan los gastos de la organización en la contratación de personal especializado interno.
        - Se incurre en costes extra por la capacitación del personal en seguridad de la información.
        - Se detecta poca flexibilidad para dimensionar los equipos de trabajo en relación con las necesidades de seguridad de la información de las organizaciones.

- **Gestión externalizada de la seguridad de la información**: Este modelo fortalece la seguridad con la combinación de la experiencia de la especialización del personal de gestión externo con el conocimiento del negocio de los equipos de gestión de la seguridad interna. Además, la fortaleza de la **implementación de un SOC** favorece la gestión interna de la seguridad. Ambas características son aportes para el modelo de gestión mixto. Entre otras, algunas ventajas y desventajas pueden ser:
    - **Ventajas**:
        - Se contrata empresas externas especializadas en seguridad de la información, que puede trabajar físicamente en la organización o vía remota, según los acuerdos de contratación de los servicios.
        - Se trabaja con personal altamente especializado, calificado y con gran experiencia en seguridad de la información.
        - Se define un contrato y un acuerdo de nivel de servicios con la empresa externa para que se establezcan todas responsabilidades de todas las partes involucradas.
        - Se define el SOC para centralizar las operaciones externas de seguridad de la información, como el uso de herramientas de gestión y monitorización.
        - Se centralizan las herramientas de gestión de incidentes de seguridad de la información.
    - **Inconvenientes**:
        - Se debe tener en cuenta la credibilidad de la empresa a subcontratar para las labores de seguridad de la información, con el fin de no incurrir en problemas de confidencialidad a futuro.
        - Se carece de los conocimientos requeridos de los procesos de negocio de la organización, dado que el personal responsable de la seguridad de la información es externo.
        - Se puede carecer de confianza en la relación con el personal interno de la organización.

- **Gestión mixta de la seguridad de la información**: En este modelo se eliminan las debilidades de los modelos de gestión interna y externa y se combinan sus fortalezas, por lo que se trata de un modelo que contiene todas las ventajas de los modelos anteriores:

- **Ventajas**:
  - Se orienta en la organización del equipo interno de seguridad de la información y en la colaboración de un equipo externo especializado.
  - Se enfoca en los puntos fuertes de los modelos de la gestión de seguridad interna y de la gestión de seguridad externa.
  - Se posee el conocimiento y competencias de los procesos de negocio de la organización por parte del personal interno.
  - Se posee el conocimiento y competencias de la parte técnica especializada de los procesos de seguridad de la información por parte del personal externo.
- **Inconvenientes**:
  - Se pueden generar conflictos de interés si no se establecen bien las responsabilidades de todas las partes involucradas.
  - Se requiere de equipos altamente coordinados por ambas partes, tanto de la organización como del equipo de apoyo externo.

7.1.1.5 Sistema de Gestión de la Seguridad de la información (SGSI)

Un **Sistema de Gestión de Seguridad de la Información** (SGSI) se define como un sistema o herramienta que contiene el conjunto de políticas, procedimientos y directrices que, en conjunto con los recursos y actividades relacionadas, son gestionados por la organización para proteger sus datos, información, conocimiento y activos de información necesarios para conseguir sus objetivos de negocio. Se trata del conjunto de normativas y documentos que facilitan el gobierno de la protección de la información y de todas sus propiedades para minimizar los riesgos en los diferentes procesos de negocio de una organización.

Asimismo, la norma internacional **ISO/IEC 27001**[61], desde su versión de 2013, determina las disposiciones necesarias para crear y gestionar un SGSI bajo el proceso iterativo de calidad llamado Ciclo de Deming[62] o ciclo PDCA (PHVA, por sus siglas en español), que consta de cuatro fases:

- **Fase de Planificación (*Plan*)**: Fase que determina los objetivos y procesos esenciales para alcanzar los resultados deseados. Consta de las siguientes etapas:
  - PI. Definición de la política de la seguridad de la información.
  - PII. Estudio del contexto de la organización.
  - PIII. Estructura de la organización.
  - PIV. Definición de las políticas de alto nivel.
  - PV. Definición de los objetivos de seguridad.
  - PVI. Identificación de los riesgos.
  - PVII. Selección de las salvaguardas.
- **Fase de Hacer (*Do*)**: Fase que implanta los nuevos procesos. Consta de las siguientes etapas:
  - DI. Implantación del plan de gestión de riesgos.
  - DII. Selección e implantación de los indicadores con los que medir la eficacia.

[61] https://normaiso27001.es/
[62] https://www.unir.net/ingenieria/revista/ciclo-de-deming-pdca/

- **Fase de Verificar (*Check*)**: Fase que cuantifica los nuevos procesos y contrasta los resultados obtenidos con los deseados. Consta de las siguientes etapas:
    - CI. Desarrollo de los procedimientos de monitorización.
    - CII. Revisión regular del SGSI.
    - C.III. Auditoría interna del SGSI.
- **Fase de Actuar (*Act*)**: Fase que estudia las diferencias entre los resultados esperados y los obtenidos, con el fin de comprender las causas y proponer mejoras. Consta de las siguientes etapas:
    - AI. Implanta las mejoras y las acciones correctivas y preventivas.
    - AII. Mantenimiento de los registros y gestión de las evidencias.

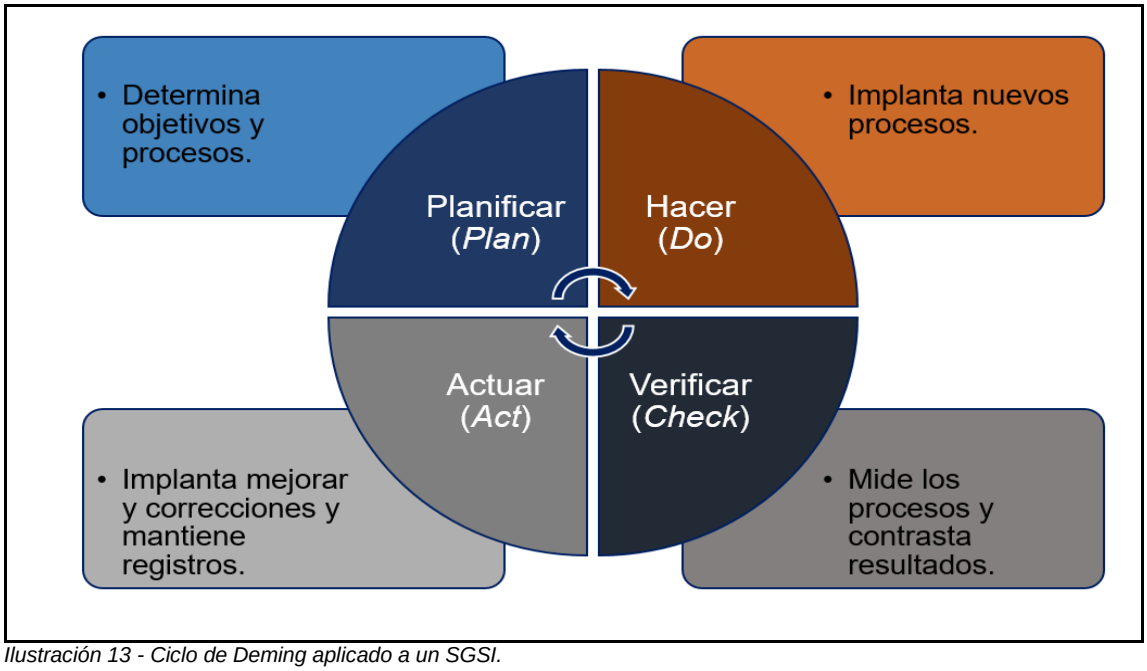

Ilustración 13 - Ciclo de Deming aplicado a un SGSI.

7.1.1.6 Equipos de Seguridad de la Información

Dentro del ámbito de la Seguridad de la Información y, en concreto, de la ciberseguridad, se han definido diferentes equipos que han seguido líneas o contextos de este ámbito diferentes. Mientras unos se han dedicado a defender las amenazas a la Seguridad de la Información, otros se han dedicado a buscar vectores de ataque para encontrar debilidades o maneras de vulnerar los sistemas de información. Por tanto, a raíz de un estudio sobre la inclusión de los equipos de desarrollo en el área de ciberseguridad por la *hacker* April C. Wright[63] y su correspondiente publicación presentada en el BlackHat USA 2017[64], la visión de la ciberseguridad se ha ampliado y se han formado diferentes equipos bajo la asignación de los colores primarios y sus combinaciones:

[63] https://www.blackhat.com/us-17/speakers/April-C-Wright.html
[64] https://www.blackhat.com/us-17/briefings.html#orange-is-the-new-purple-how-and-why-to-integrate-development-teams-with-red-blue-teams-to-build-more-secure-software

- **Equipo Azul (*Blue Team*)**: Se trata del equipo o grupo responsable de la ciberseguridad defensiva en tiempo real. Se denomina "*The Defenders*" y se encarga de la administración diaria y su fortalecimiento, bastionado [65], monitorización y mantenimiento de la ciberseguridad de los activos de información de una organización, así como de su protección, prevención, detección y respuesta ante incidentes y brechas de seguridad.
- **Equipo Rojo (*Red Team*)**: Se trata del equipo o grupo responsable de la ciberseguridad ofensiva en tiempo real. Se denomina "*The Breakers*", se comporta como un atacante real y se encarga de hacking ético, la detección y explotación de vulnerabilidades, las pruebas de penetración[66] y caja negra (*black box*), la ingeniería social y el escaneo de aplicaciones web para detectar todas las posibles debilidades y brechas de seguridad de los activos de información de una organización.
- **Equipo Amarillo (*Yellow Team*)**: Se trata del equipo o grupo responsable de la ciberseguridad del software. Se denomina "*The Builders*" y se encarga de diseñar aplicaciones y programas sin fallos ni brechas de seguridad, se nutren de la información sobre vulnerabilidades y errores de ciberseguridad de los equipos Azul (*Blue Team*) y Rojo (*Red Team*) y colaboran con los equipos de I+D+i para mejorar la Seguridad de la Información de la organización.
- **Equipo Púrpura (*Purple Team*)**: Se trata del equipo o grupo mixto que une los equipos Azul (*Blue Team*) y Rojo (*Red Team*) y que se responsabiliza de alinear la ciberseguridad defensiva y la ofensiva en tiempo real. Se encarga de perfeccionar las capacidades de los mecanismos de protección, prevención, detección y respuesta ante ciberincidentes, optimizar las capacidades de los equipos Azul y Rojo, de mejorar el rendimiento y funcionamiento de los ciberataques y su defensa y de maximizar sus objetivos a través de la integración de controles y tácticas del equipo defensivo con la detección de vulnerabilidades y amenazas por parte del equipo ofensivo. Además, en caso de ausencia de los equipos Azul y Rojo, se encarga de todas sus funciones.
- **Equipo Naranja (*Orange Team*)**: Se trata del equipo o grupo mixto que une los equipos Rojo (*Red Team*) y Amarillo (*Yellow Team*) y que se responsabiliza de alinear la ciberseguridad ofensiva y el desarrollo de aplicaciones y programas seguros en tiempo real. Se encarga de perfeccionar el diseño de código seguro, protegido y sin errores ni debilidades, gracias a la perspectiva de los posibles atacantes, optimizar las capacidades de los equipos Rojo y Amarillo y capacitar al equipo Amarillo en la construcción de código a través de la información en tiempo real que recibe del equipo Rojo. Además, en caso de ausencia de los equipos que lo forman, se encarga de todas sus funciones.
- **Equipo Verde (*Green Team*)**: Se trata del equipo o grupo mixto que une los equipos Azul (*Blue Team*) y Amarillo (*Yellow Team*) y que se responsabiliza de alinear la ciberseguridad defensiva y el desarrollo de aplicaciones y programas seguros en tiempo real. Se encarga de perfeccionar la automatización de la ciberseguridad con el diseño de código seguro, optimizar las capacidades de los equipos Azul y Amarillo y capacitar al equipo Amarillo en la construcción de código a través de la información en tiempo real que recibe del equipo Azul. Además, en caso de ausencia de los equipos que lo forman, se encarga de todas sus funciones.

[65] https://protecciondatos-lopd.com/empresas/bastionado-de-sistemas/

[66] Ver el punto 7.1.4.2.1 del Anexo 1 para más información sobre las Principales medidas de prevención, como las pruebas de penetración.

- **Equipo Blanco (*White Team*)**: Se trata del equipo o grupo responsable de mediar las acciones realizadas entre los equipos Azul (*Blue Team*) y Rojo (*Red Team*) en el uso de sus funciones para alinearlos con las estrategias de negocio de la organización. Por tanto, se encarga del control de las acciones realizadas por ambos equipos, de la evaluación y documentación de los resultados de esas acciones, de la seguridad operacional y del cumplimiento normativo y logístico la ciberseguridad de una organización.

Asimismo, en la actualidad, también se comienzan a nombrar otros equipos como pueden ser, por ejemplo, el **Equipo Negro (*Black Team*)**, que se encarga de las mismas labores que el Equipo Rojo, pero con atacantes físicos y no sólo a la ciberseguridad, sino a la Seguridad de la Información de una organización, o el **Equipo Dorado (*Gold Team*)**, que se encarga de la simulación de escenarios de riesgos y crisis de ciberseguridad para la capacitación y mejora de la defensa y continuidad del negocio de una organización. Además, aunque sea fuera de una paleta de colores o incluya personal de los diferentes equipos indicados anteriormente, entre los equipos más importantes de la Seguridad de la Información se encuentra el **Equipo de Auditores**, que se encarga de realizar una revisión de los controles, procedimientos y funcionamiento del SGSI de una organización en base a su principio de independencia, sobre el que se sostienen la objetividad e imparcialidad de los resultados de una auditoría y garantizan unas conclusiones íntegras.

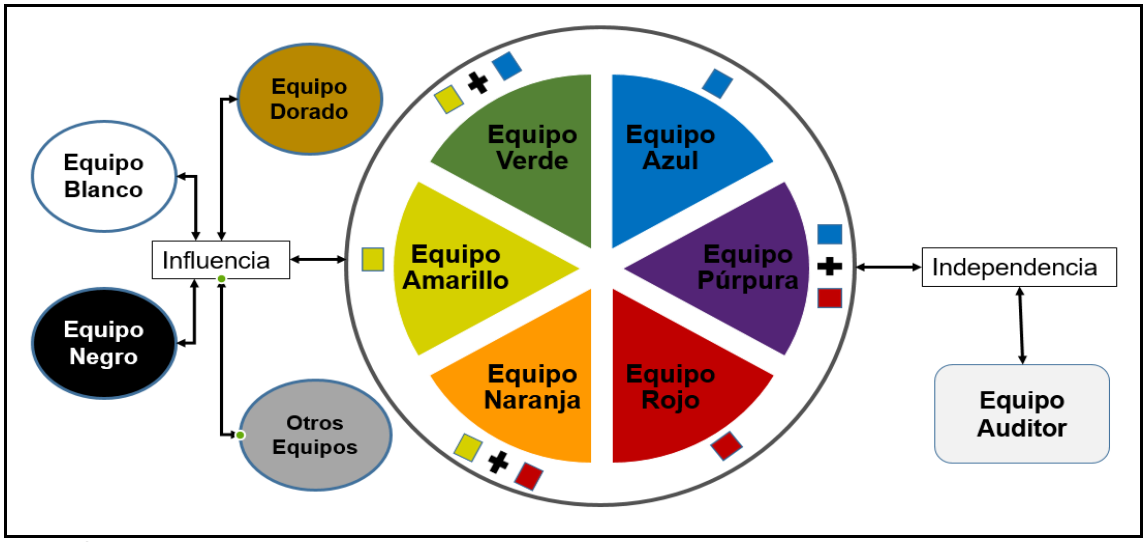

Ilustración 14 - Equipos de Ciberseguridad.

7.1.2 Gestión de riesgos, de vulnerabilidades y de amenazas

La gestión de riesgos, de vulnerabilidades y de amenazas son tres procesos importantes que se deben tramitar en todo Sistema de Gestión de Seguridad de la Información. A continuación, se explican con algo más de detalle:

7.1.2.1 Definición de conceptos y su relación

Con el fin de entender mejor las nociones y relaciones más importantes de las gestiones de riesgos, vulnerabilidades y amenazas, seguidamente, se establecen algunos de sus conceptos:

- **Riesgo**: Probabilidad de que se materialice una amenaza en cualquiera de los activos tecnológicos de una organización y pueda causar un incidente de seguridad.
- **Amenaza**: Acción que aprovecha una vulnerabilidad para producir acciones negativas sobre los activos de una organización.
- **Ciberamenaza**: Amenaza que se produce en un entorno digital e interconectado.
- **Vulnerabilidad**: Debilidad, fallo o deficiencia en cualquiera de los activos tecnológicos de una organización que se puede convertir en un incidente de seguridad con o sin impacto.
- **Impacto**: Consecuencia de que una amenaza se materialice sobre un activo de información con la explotación de una vulnerabilidad.

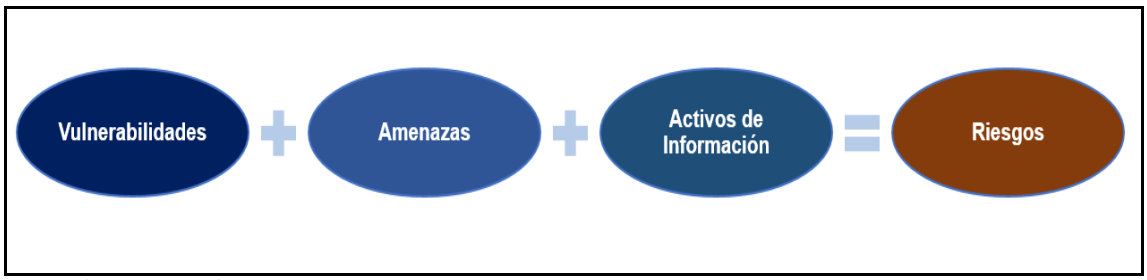

Ilustración 15 - Relación lineal entre conceptos relacionados con el Riesgo.

7.1.2.2 Gestión de Riesgos

La **gestión de riesgos** se define como un proceso continuo del negocio que se encarga de reconocer, medir, analizar y tratar todos los riesgos que afecten a la Seguridad de la Información de una organización, a través de la ejecución rigurosa de procedimientos, actividades y políticas en sus procesos de negocio para minimizar los riesgos en sus activos. Se trata de uno de los macro procesos más importantes en la Gestión de la Seguridad de la Información de una organización.

7.1.2.2.1 Fases de la Gestión de Riesgos

La gestión de riesgos, dada su criticidad y amplitud como proceso de negocio en la Seguridad de la Información de una organización, se divide en las diferentes fases:

- **Identificación de riesgos**: Etapa en donde se reconoce y califica cada uno de los riesgos significativos en los procesos de negocio de la organización y se determinan sus criticidades y urgencias. Su proceso más importante es el análisis de riesgos.
- **Evaluación de riesgos**: Etapa en donde se analizan cada uno de los riesgos en los procesos de negocio de la organización, se determinan sus amenazas y salvaguardas y se estima el impacto que pueden ocasionar.
- **Tratamiento de riesgos**: Etapa en donde se tratan los sistemas de información para protegerlos de los riesgos mediante la transferencia del riesgo a otro activo, la reducción del riesgo heredado (se acepta un riesgo menor), la ampliación del riesgo heredado (se acepta un riesgo mayor) o la erradicación del propio riesgo, entre otros.

- **Seguimiento de los riesgos**: Etapa en donde se monitorizan de manera continua todos los activos de información que tengan riesgos para detectar anomalías significativas en su tratamiento.
- **Revisión de riesgos**: Etapa en donde se examinan continuamente los riesgos para verificar su estado y evolución en los activos de información de una organización.

7.1.2.2.2 Análisis de Riesgos

Al margen de las diferentes etapas de la gestión de riesgos, su proceso más destacable se considera el **análisis de riesgos**, que se encuentra linealmente en la etapa de identificación y se encarga de identificar los riesgos, determinar su alcance y determinar sus áreas afectadas. Se trata del proceso que se ocupa de reconocer a los activos de información con mayor probabilidad de que ocurra un incidente de seguridad. Además, entre las razones más importantes para realizar este proceso, se encuentran las siguientes:

- Facilita la identificación de los diferentes riesgos de seguridad de la información en el funcionamiento de los diferentes procesos de negocio de una organización.
- Posibilita la elección de las protecciones necesarias para tratar los riesgos de la organización que puedan afectar a sus procesos de negocio.
- Permite la creación e implantación de los planes de contingencias de una organización.
- Favorece la creación de un Sistema de Gestión de la Seguridad de la Información (SGSI) y del conocimiento del contexto para la implantación de normativas de Seguridad y su posible certificación.

Por otra parte, en base a los propósitos que se requieran y a la perspectiva utilizada en un análisis de riesgo, se pueden realizar dos tipos de análisis de riesgos:

- **Análisis de riesgos intrínseco**: Se trata del estudio de los riesgos que no tiene en cuenta las protecciones de seguridad ya implantadas en una organización y que obtiene un riesgo intrínseco como resultado.
- **Análisis de riesgos residual**: Se trata del estudio de los riesgos que sí tiene en cuenta las protecciones de seguridad ya implantadas en una organización y que obtiene un riesgo real como resultado.

7.1.2.3 Gestión de vulnerabilidades

La **gestión de vulnerabilidades** se define como un proceso continuo del negocio que se responsabiliza de reconocer, valorar, tratar y notificar las debilidades de seguridad de los sistemas de información de una organización para prevenir las posibles amenazas a su seguridad de la información y minimizar su posible impacto. Se trata de uno de los procesos más importantes para la gestión de riesgos de una organización y, entre otras actividades, analiza el motivo por el que se produce una vulnerabilidad, hace uso de repositorios estandarizados a nivel mundial para su análisis y las clasifica para su gestión.

7.1.2.3.1 Posibles motivos de una vulnerabilidad

La gestión de vulnerabilidades se realiza desde diferentes perspectivas, por lo que se producen por diferentes motivos, como pueden ser los siguientes:

- **Errores de configuración (*misconfigurations*)**: Se trata de implementaciones insuficientes o fallidas en los controles de seguridad de un activo que le provoca una debilidad.
- **Ausencia de configuración (*default installation*)**: Se trata del establecimiento de la configuración inicial, conocida públicamente y por defecto en un sistema o activo de información que le provoca una debilidad, ya que, por lo general, sólo se incluyen las medidas de protección mínimas para facilitar su funcionalidad.
- **Desbordamiento de memoria (*buffer overflow*)**: Se trata de un error de software en donde se intentan gestionar más datos de los permitidos sobre un área de memoria reservada, lo que provoca una debilidad en los activos de información afectados.
- **Ausencia de actualizaciones (*missing patches*)**: Se trata de la falta de correcciones de funcionalidad y seguridad de un sistema o activo de información, lo que provoca una debilidad.
- **Errores de diseño (*design flaws*)**: Se trata de errores o fallos en la lógica de la funcionalidad intrínseca al diseño de un sistema o activo de información que le provoca una debilidad.
- **Errores del sistema operativo (*operating system flaws*)**: Se trata de defectos o implementaciones erróneas en los controles de seguridad del programa que gestiona y enlaza los recursos hardware y software de un sistema o activo de información, lo que le provoca una debilidad.
- **Ausencia de contraseña o inclusión por defecto (*default passwords*)**: Se trata de la ausencia del establecimiento de una contraseña o la configuración de la contraseña por defecto en un sistema o activo de información, que suele ser débil y conocida y documentada públicamente, lo que le provoca una debilidad.

7.1.2.3.2 Repositorios de información de vulnerabilidades

Con el fin de estandarizar, controlar y compartir las vulnerabilidades, se han desarrollado diferentes **repositorios** de información a nivel mundial que facilitan su gestión. Por tanto, a continuación, se indican los más destacados y usados internacionalmente:

- ***National Vulnerability Database* (NVD)**: Se trata de la base de datos de vulnerabilidades del Gobierno de Estados Unidos, que permite la automatización del tratamiento y la protección de las vulnerabilidades para su cumplimiento normativo. Se basa en un estándar del Protocolo de automatización de contenido de seguridad (SCAP) y contiene información sobre listas de seguridad, errores de software, fallos de configuración y métricas relacionadas con el impacto de los diferentes productos afectados.

- ***Common Vulnerability Scoring System* (CVSS)**: Se trata de la base de datos de vulnerabilidades creada para normalizar la puntuación de la gravedad de las vulnerabilidades a nivel internacional y que indica las principales características y debilidades técnicas de los activos y productos de información. Además, este estándar se compone de tres conjuntos de métricas:
    - **Puntuación base**: Puntuación de entre 0 y 10 que representa las características técnicas, objetivas, constantes e intrínsecas de una vulnerabilidad a través de las siguientes métricas:
        - **Métricas de explotabilidad**: Medidas donde se encuentran las propias características del componente vulnerable:
            - Vector de acceso.
            - Complejidad del acceso.
            - Privilegios de acceso requeridos.
            - Interacción del usuario.
        - **Métrica de alcance**: Medida que valora los límites del ataque sobre el componente vulnerable en el entorno de computación:
            - Alcance.
        - **Métricas de impacto**: Medidas que verifican la forma en la que se altera la seguridad:
            - Integridad.
            - Confidencialidad.
            - Disponibilidad.
    - **Puntuación temporal**: Puntuación de entre 0 y 10 que representa las características propias de una vulnerabilidad que se pueden desarrollar con el paso del tiempo, como actualizaciones o soluciones temporales, a través de las siguientes métricas:
        - **Métricas de Temporalidad**: Medidas donde se analizan únicamente las características propias del desarrollo temporal:
            - Madurez del código de explotación.
            - Confianza.
            - Remedio a la vulnerabilidad.
    - **Puntuación del entorno**: Puntuación de entre 0 y 10 que representa las características de una vulnerabilidad en base a la criticidad del activo de información de la organización que pueda verse afectado, a través de las siguientes métricas:
        - Mismas métricas que en la Puntuación base.
        - Requisitos de confidencialidad, disponibilidad e integridad.
- ***Common Vulnerabilities and Exposures* (CVE)**: Se trata de un listado de datos de las vulnerabilidades conocidas con una codificación única (número identificativo, descripción y referencia) para cada vulnerabilidad conocida. Además, se gestiona por MITRE Corporation[67], previene de duplicidades en su registro y facilita el intercambio de su información entre las bases de datos de vulnerabilidades y sus herramientas de gestión.
- ***Common Weakness Enumeration* (CWE)**: Se trata de un listado de datos que estandariza las referencias de las vulnerabilidades, su prevención y su mitigación entre los diferentes fabricantes de software y hardware.
- ***Common Platform Enumeration* (CPE)**: Se trata de un esquema estructurado de datos de plataformas con vulnerabilidades que les añade un nombre formal, un método para verificarlos y una descripción formateada.

[67] https://www.mitre.org/

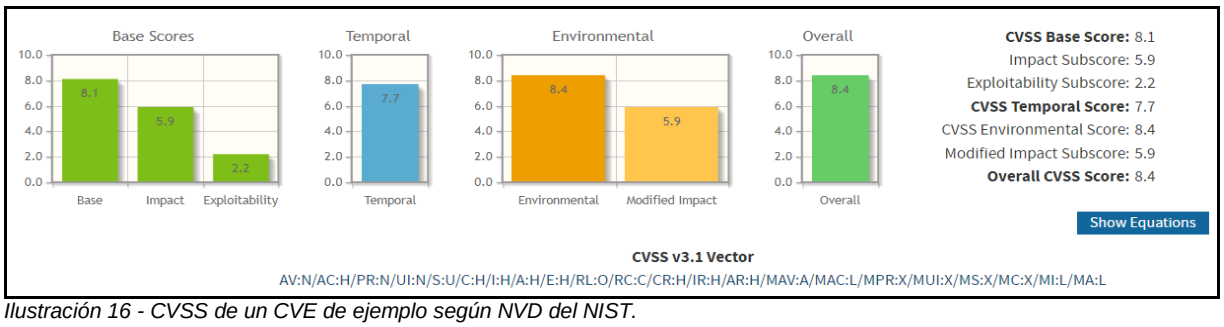

Ilustración 16 - CVSS de un CVE de ejemplo según NVD del NIST.

7.1.2.3.3 Clasificación de vulnerabilidades

La gestión de vulnerabilidades requiere de un proceso que clasifique las vulnerabilidades para poder priorizarlas y tratarlas. Por tanto, a continuación, se exponen algunas de las diferentes formas de realizar esta tarea:

- **Conocimiento de las vulnerabilidades**:
  - **Vulnerabilidades no conocidas**: Se trata de aquellas vulnerabilidades desconocidas para todos los intervinientes en sus detecciones y análisis, como pueden ser los propios fabricantes, los CERT[68] o los servicios de Ciberseguridad. También suelen llamarse como vulnerabilidades de día cero (o *zero day*).
  - **Vulnerabilidades conocidas**: Se trata de aquellas vulnerabilidades registradas a nivel internacional con un código que puede ser, por ejemplo, un CVE.
- **Tipo de sistema afectado por la vulnerabilidad**:
  - **Sistemas Informáticos**: Se trata de aquellas vulnerabilidades que afectan a los protocolos y elementos de red, al hardware o al sistema operativo.
  - **Aplicaciones**: Se trata de aquellas vulnerabilidades que afectan a todo tipo de aplicaciones, como pueden ser las webs, las de escritorio, las móviles o cualquier otra.
  - **Gestión de información**: Se trata de aquellas vulnerabilidades que afectan a los sistemas de información por la gestión de procedimientos y protocolos no seguros o por personal no capacitado ni formado en seguridad de la información.
- **Tipo de activo que provoca la vulnerabilidad**:
  - **Vulnerabilidades humanas**: Se trata de aquellas vulnerabilidades producidas por deficiencias en la capacitación y concienciación del personal en la seguridad de la información.
  - **Vulnerabilidades físicas**: Se trata de aquellas vulnerabilidades producidas por debilidades en el acceso físico a los sistemas de una organización.
  - **Vulnerabilidades naturales**: Se trata de aquellas vulnerabilidades producidas por deficiencias en los controles de seguridad ante desastres naturales.

[68] https://es.wikipedia.org/wiki/Equipo_de_Respuesta_ante_Emergencias_Inform%C3%A1ticas

- **Vulnerabilidades de hardware**: Se trata de aquellas vulnerabilidades producidas por debilidades en los componentes físicos de los sistemas de una organización.
- **Vulnerabilidades de software**: Se trata de aquellas vulnerabilidades producidas por deficiencias en programas o aplicaciones de una organización.
- **Vulnerabilidades de red**: Se trata de aquellas vulnerabilidades producidas por debilidades en los protocolos y elementos de red de una organización.

7.1.2.4 Gestión de las ciberamenazas

La **gestión de ciberamenazas** se define como un proceso continuo del negocio que se encarga de tratar el ciclo temporal de vida de una ciberamenaza para localizarla, analizarla y dar respuesta los más rápido posible para evitar o minimizar un incidente de seguridad o una acción negativa sobre un activo de información. Se trata de otro de los procesos más importantes en la gestión de riesgos de una organización.

7.1.2.4.1 Clasificación de las ciberamenazas

El CCN-CERT, con el fin de comprender la finalidad y el posible impacto que pueden tener las ciberamenazas, las clasifica y define en base a la motivación que pueden tener los diferentes tipos de agentes atacantes. Por este motivo, se puede describir el siguiente catálogo de amenazas informáticas:

- **Ciberespionaje**: Acciones cibernéticas que tienen el objetivo de conseguir secretos de Estado o información de carácter personal, sensible o de propiedad intelectual sin el consentimiento del propietario de la información.
- **Cibercrimen** o **ciberdelito**: Actividad que emplea actos ilegales a través del espacio digital para, generalmente, obtener un retorno económico.
- **Ciberactivismo**: Conjunto de acciones a través de Internet para impulsar una causa de carácter social o político.
- **Ciberterrorismo**: Actividad digital orientada a causar miedo y pánico de un conjunto de la población civil.
- **Ciberguerra** o **ciberconflicto**: Acciones militares de un Estado para desequilibrar a otros Estados y concentrar a la población civil.
- **Amenazas por actores internos** o ***insiders***: Actividad perjudicial para las organizaciones originada por su propio personal de manera intencionada o negligente.

Por otra parte, la metodología MAGERIT[69], tipifica las ciberamenazas en cuatro tipos, en base a su origen:

- **De origen natural**: Amenaza causada por accidentes naturales, como terremotos, que afectan a activos de información de una organización.
- **De origen industrial**: Amenaza causada por accidentes en el entorno, como fallos eléctricos, que afectan a activos de información de una organización.

69 https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

- **Causadas por las personas de manera accidental**: Amenaza causada por errores no deliberados de personas con acceso a los activos de información de una organización.
- **Causadas por las personas de manera deliberada**: Amenaza causada por acciones deliberados de personas con acceso a los activos de información de una organización para obtener un beneficio no corporativo.

7.1.2.4.2 Ejemplos de ciberamenazas

La extensión del uso de información digital por las organizaciones a nivel mundial ha traído consigo el aumento del número de amenazas hacia la Seguridad de la Información. Por tanto, a continuación, se presentan algunos tipos de ciberamenazas:

- **Violación de datos**: Se trata de una amenaza muy conocida, que se extiende por todos los ámbitos y contextos, como puede ser el financiero con los datos económicos. Su impacto puede ocasionar pérdidas innumerables en las organizaciones, pero no sólo económicas, sino también relacionadas con su reputación y posible existencia.
- **Configuración incorrecta y control inadecuado de los cambios**: Se trata de una amenaza muy latente, ya que los clientes suelen ser quienes hacen sus configuraciones y quienes llevan un control de cambio que suele ser muy poco adecuado. Por tanto, puede repercutir en malas configuraciones accidentales que pueden violar la seguridad de la información e, incluso, su pérdida.
- **Falta de arquitectura y estrategia de seguridad en la nube**: Se trata de una amenaza ocasionada por la ausencia de consideración, un estudio incorrecto de la arquitectura para sus servicios de negocio o un contrato de infraestructuras inadecuado, por lo que puede ocasionar altos riesgos en la seguridad de sus sistemas.
- **Identidad insuficiente, credencial, acceso y gestión de claves**: Se trata de una amenaza relacionada con la falta de identidad que poseen las organizaciones cuando establecen la conexión con los servicios internos y externos, por lo que cabe la posibilidad de que tengan una administración y seguridad inadecuadas para este cambio de escenario.
- **Secuestro de cuentas**: Se trata de una amenaza donde un atacante obtiene las credenciales de acceso de cuentas que no le pertenecen de manera no legítima. De hecho, debido a la frecuencia de los intentos de *phishing* cada vez más preparados, entre otros casos, un atacante se puede apoderar de las credenciales de acceso de otros clientes y obtener privilegios donde acceder a la información.
- **Amenazas internas**: Se trata de amenazas donde su origen son empleados de las propias empresas (*insiders*), que, entre otras acciones, o bien, no fortalecen sus claves de acceso o las comparten por desconocimiento o inocencia o bien, tienen algún tipo de resentimiento y atacan a la propia empresa, lo que pone en riesgo los servicios corporativos.
- **Plano de control débil**: Se trata de una amenaza que se da cuando hay debilidad en los procesos de duplicación de datos, almacenamiento o migración de los mismos. Esta situación se produce cuando hay personal humano que no tienen la suficiente capacidad de controlar la lógica, la seguridad y la infraestructura de los datos de la empresa.

- **Fallos en la metaestructura y la estructura de aplicaciones**: Se trata de amenazas provocadas por las vulnerabilidades y/o la mala implementación de las API con las que se obtiene la información de las metaestructuras. De hecho, éstas poseen toda la información de seguridad de cómo se deben proteger los datos y se consume a través de las API para, entre otras, detectar accesos no autorizados.
- **Abuso y mal uso de los servicios públicos**: Se trata de amenazas donde los atacantes utilizan los propios servicios públicos de una organización para realizar sus ataques o alojar sus artefactos maliciosos con los que atacar. Así, como los servicios de alojamiento público resultan de utilidad para las organizaciones responsables y productivas, también lo resultan para los atacantes, que, sin que los proveedores de servicio conozcan sus intenciones, hagan un abuso del servicio y planifiquen sus acciones delictivas desde este tipo de infraestructuras.

7.1.3 Ataques informáticos e incidentes de seguridad

Toda organización conectada a Internet está expuesta a ser atacada informáticamente y a sufrir incidentes de seguridad de mayor o menor criticidad. Por ello, un **ataque informático** o **ciberataque** se define como cualquier acción ofensiva sobre un activo de información de una organización para acceder, exhibir, modificar, perturbar o eliminar sus datos sin autorización de su responsable. Debido a ello, el concepto de **incidente de seguridad** o **ciberincidente** se amplía y se define como la materialización de una amenaza con o sin impacto sobre cualquiera de los activos de una organización. Además, todo ciberataque y la gestión de cualquier incidente de seguridad recorre diferentes fases, tal y como se revela gracias al concepto de la ***Cyber Kill Chain***[70], que se describe como una cadena de procesos dirigidos hacia un activo objetivo para conseguir obtener un resultado deseado sin autorización.

7.1.3.1 Fases de un ataque informático y de la gestión de un incidente de seguridad

Realizar un ataque informático, desde el punto de vista ofensivo, o gestionar un incidente de seguridad, desde el punto de vista defensivo, pueden ser complicados, pero se pueden describir como el paso y progreso por las diferentes fases indicadas en la *Cyber Kill Chain*:

1. **Reconocimiento (*reconnaissance*)**: Fase en la que se recolecta información sobre el objetivo que se desea atacar. Las técnicas son variadas, pero, en su mayoría, hay de dos tipos:
    - Reconocimiento pasivo, donde no tenemos contacto directo con el blanco
    - Reconocimiento activo, que implica un contacto directo y más intrusivo y, por tanto, aumenta el riesgo de detección.
2. **Armamentización (*weaponization*)**: Fase en la que se analiza la información obtenida en el reconocimiento para desarrollar y planificar el arma para usarla en el vector de ataque al objetivo.

[70] https://www.incibe-cert.es/blog/cyber-kill-chain-sistemas-control-industrial

3. **Entrega (*delivery*)**: Fase en la que se entrega el arma desarrollada en la fase de armamentización a través de un vector de ataque como puede ser un fichero adjunto en un correo o un dispositivo USB.
4. **Explotación o acceso inicial (*exploitation*)**: Fase en la que se utilizan diferentes técnicas, como phishing o la explotación de vulnerabilidades, a través de los diferentes vectores de ataque, para conseguir acceso inicial al objetivo e intentar crear persistencia.
5. **Instalación o ejecución (*installation*)**: Fase en la que se garantiza el acceso persistente al objetivo, mediante una puerta trasera, la creación de una cuenta de administración o el acceso remoto, por ejemplo.
6. **Dominio y control (*command and control*)**: Fase en la que se obtiene el acceso persistente al objetivo y se intentan conseguir todos los privilegios necesarios para tener su control.
7. **Acciones para el objetivo (*actions on objective*)**: Fase en la que, tras garantizar los privilegios y la persistencia, se ejecuta el ataque sobre el objetivo.

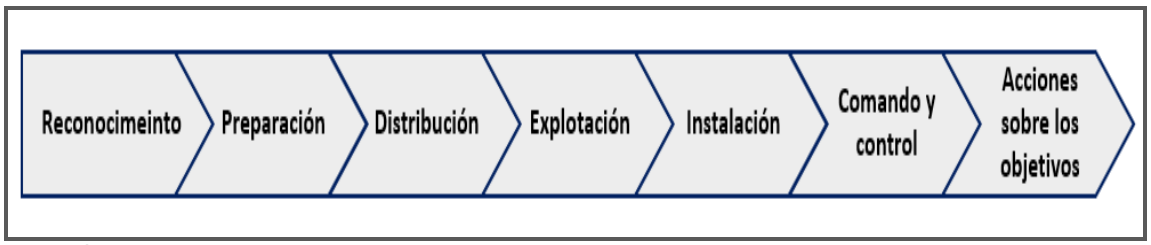

Ilustración 17 - Etapas de la cadena Cyber Kill Chain (Lockheed Martin).

7.1.3.2 Taxonomía de incidentes de seguridad o ciberincidentes

Tal y como define la guía STIC 817[71], sobre la gestión de ciberincidentes, del CCN-CERT, los incidentes de seguridad se pueden clasificar y tipificar de la siguiente manera:

Clasificación	Tipo de incidente	Descripción
Contenido abusivo	Spam	Correo electrónico no deseado y masivo.
	Delito de odio	Contenido acosador, discriminatorio o difamatorio.
	Pornografía infantil, contenido sexual o violento inadecuado	Contenido inadecuado o ilegal.
Contenido dañino	Sistema infectado	Activo tecnológico infectado con malware.
	Servidor C&C (Mando y Control)	Conexiones con sistemas de Mando y Control (C&C) por infección de activo tecnológico.
	Distribución de malware	Uso de recursos para distribuir malware.
	Configuración de malware	Alojamiento de ficheros de configuración de malware.

[71] https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

Obtención de información	Escaneo de redes (*scanning*)	Conexiones para el descubrimiento de posibles debilidades y recolección de información.
	Análisis de paquetes (*sniffing*)	Captura y estudio del tráfico de redes.
	Ingeniería social	Recolección de información sin el uso de la tecnología.
Intento de intrusión	Explotación de vulnerabilidades conocidas	Intento de comprometer o interrumpir el servicio de un activo tecnológico por la explotación de vulnerabilidades conocidas.
	Intento de acceso con vulneración de credenciales	Intento reiterado de descubrir credenciales.
	Ataque desconocido	Cualquier ataque que use métodos o herramientas desconocidas.
Intrusión	Compromiso de cuenta con privilegios	Compromiso de un activo tecnológico con credenciales con privilegios obtenidos por el atacante.
	Compromiso de cuenta sin privilegios	Compromiso de un activo tecnológico con credenciales sin privilegios.
	Compromiso de aplicaciones	Compromiso de una aplicación mediante un ataque hacia su software.
	Robo	Sustracción de un activo físico sin acceso autorizado.
Disponibilidad	DoS (Denegación de servicio)	Ataque de denegación de servicio.
	DDoS (Denegación distribuida de servicio)	Ataque de denegación de servicio distribuido.
	Mala configuración	Indisponibilidad por configuración errónea un servicio.
	Sabotaje	Indisponibilidad por sabotaje físico.
	Interrupciones	Indisponibilidad por interrupciones ajenas a la organización.
Compromiso de la información	Acceso no autorizado a información	Acceso a la información sin autorización.
	Modificación no autorizada de información	Modificación de información sin autorización.
	Pérdida de datos	Pérdida de información.

Fraude	Uso no autorizado de recursos	Uso inadecuado de los recursos para propósitos no legítimos.
	Derechos de autor	Uso de programas o material sin licencia o sin derechos de autor.
	Suplantación	Usurpación de una persona o entidad para obtener provechos no legítimos.
	Phishing	Usurpación de una persona o entidad para obtener credenciales privadas ajenas.
Vulnerable	Criptografía débil	Servicios con criptografía débil.
	Amplificador DDoS	Servicios que permitan reflexión o amplificación de ataques DDoS.
	Servicios con acceso potencial no deseado	Servicios que permiten accesos no deseados.
	Revelación de información	Servicios que muestren información sensible sin autorización.
	Sistema vulnerable	Sistema que presenta vulnerabilidades.
Otros	Otros	Todo incidente que no ajuste a ninguna otra categoría.
	APT	Incidente producido por un ataque dirigido contra una organización concreta con artefactos sofisticados y anonimato, ocultación y persistencia.

Tabla 22 - Taxonomía de incidentes de la guía STIC 817 del CCN-CERT.

7.1.3.3 Ciberataques más comunes

Al margen de su motivación, los ciberataques más comunes, trascendentales y preocupantes de los últimos años y que han causado un mayor impacto en los incidentes de seguridad a las entidades atacadas, se relacionan con los siguientes conceptos:

- **Programa malicioso (*malware*)**: Software o artefacto malicioso que se instala en un sistema objetivo sin consentimiento del propietario para realizar acciones dañinas sobre sus datos, su propietario o su propiedad intelectual de manera intencionada y produce, entre otros, incidentes de seguridad de tipo “Sistema infectado” (categoría “Contenido dañino”). Entre otros tipos, se destacan los dos siguientes:
    - **Ransomware**: Tipo de *malware* que se emplea para limitar el acceso a la información de un sistema objetivo y secuestrarla con técnicas de cifrado para solicitar un rescate económico. Por tanto, además de incidentes de seguridad de tipo “Sistema infectado”, también puede producir incidentes de seguridad por “Interrupciones” de la categoría “Disponibilidad” o “Modificación no autorizada de información” (categoría “Compromiso de la información”).

    - **Spyware**: Tipo de *malware* que se emplea para robar información confidencial, secreta o privada de un sistema y de su propietario sin su consentimiento y con fines maliciosos. Por tanto, además de incidentes de seguridad de tipo “Sistema infectado”, también puede producir incidentes de seguridad “Acceso no autorizado a información” (categoría “Compromiso de la información”).

- **Denegación de servicio distribuido (DDoS)**: Ataque que consiste en el envío de peticiones de tráfico repartido entre múltiples orígenes con el objetivo de saturar un recurso objetivo y afectar a su disponibilidad y produce, entre otros, incidentes de seguridad de tipo “DDoS” (categoría “Disponibilidad”).
- **Vulnerabilidades**: Debilidades o fallos de un sistema digital que pueden suponer una amenaza y un riesgo para su seguridad y la de una organización y produce, entre otros, incidentes de seguridad de tipo “Sistema vulnerable” (categoría “Vulnerable”).
- **Filtración de información (exfiltración)**: Robo o publicación de información confidencial, secreta o privada de una organización para usarse sin autorización de su propietario y produce, entre otros, incidentes de seguridad “Acceso no autorizado a información” (categoría “Compromiso de la información”).

7.1.4 Sistemas de protección, prevención y detección y respuesta

La gestión de la Seguridad de la Información requiere de diversas actividades de protección, prevención y detección y respuesta o corrección para garantizar un nivel de seguridad adecuado. Por ello, se considera sumamente importante utilizar mecanismos que faciliten estas actividades.

7.1.4.1 Mecanismos de protección

Los mecanismos de protección se definen como los sistemas o soluciones que se usan para proteger los activos de información de una organización frente a los ciberataques. Por ello, las organizaciones deben configurar sus componentes de seguridad de la información, sus activos y su arquitectura bajo las premisas de protección necesarias.

7.1.4.1.1 Principales medidas de protección

Entre las principales medidas de protección que puede implementar una organización, se pueden encontrar las siguientes:

- **Protección a nivel físico**: Protección que garantiza que un atacante no pueda interferir en los dispositivos de comunicación ni de transmisión.
- **Protección a nivel de enlace**: Protección que garantiza que las tramas de comunicación de bajo nivel no se puedan interceptar ni modificar.
- **Protección a nivel de red**: Protección que garantiza que los datos propagados a través de los protocolos de red y los enviados a los protocolos de nivel de transporte se transmiten protegidos.

- **Protección a nivel de transporte**: Protección que garantiza que la comunicación se establece de manera protegida a través de los protocolos de transporte y mediante la configuración o actualización de los nodos extremos de la comunicación.
- **Protección a nivel de aplicación**: Protección que garantiza que la información se encuentra protegida y es legítima, tanto en su transmisión como en su almacenamiento.

7.1.4.1.2 Ejemplos de medidas de protección

Algunos ejemplos reales de medidas de protección en las organizaciones pueden ser:

- **Protección de las zonas perimetrales de la red**: Se trata del principal mecanismo de protección de una organización y se basa en la defensa de su perímetro para crear una zona de seguridad con unos requisitos específicos de protección, como pueden ser la distinción de las diferentes zonas de red con interfaces diferentes a las que se les aplique una política de seguridad. Además, entre las zonas de seguridad se pueden distinguir la zona controlada, la zona no controlada y la zona restringida y su principal tecnología puede ser un *firewall* o cortafuegos[72].
- **Protección de redes inalámbricas**: Se trata de una protección a nivel de enlace y se basa en la defensa de las comunicaciones inalámbricas para evitar que puedan ser interceptadas o accedidas sin autorización.
- **Protección mediante criptografía**[73]: Se trata de una protección en diferentes niveles que se basa en la defensa de los datos mediante métodos matemáticos que los ofuscan o esconden.
- **Protección mediante sistemas de autenticación**: Se trata de una protección en diferentes niveles que se basa en la defensa de los datos mediante la verificación de su legitimidad, así como los de su origen y su identidad.
- **Protección mediante VPN**: Se trata de una protección en diferentes niveles que se basa en la defensa de las comunicaciones y los datos mediante la conexión de un sistema a una red privada, que no puede ser interceptada, y virtual, que no se existe físicamente.

7.1.4.2 Mecanismos de prevención

Los mecanismos de prevención se definen como el conjunto de sistemas o soluciones que se usan para proteger los activos de información de una organización de los ciberataques antes de que éstos ocurran o lleguen a su objetivo. Por ello, las organizaciones deben instaurar políticas de seguridad, incluir sistemas trampa y realizar pruebas de penetración para verificar el estado de seguridad de sus activos de información y prevenir las posibles debilidades que supongan una amenaza y un posterior ataque.

[72] Ver el punto 7.3.2.1 del Anexo 3 para más información sobre Cortafuegos (*Firewall).*
[73] https://www.tecnologia-informatica.com/que-es-la-criptografia/

7.1.4.2.1 Principales medidas de prevención

Entre las principales medidas de prevención que puede aplicar una organización, se pueden encontrar las siguientes:

- **Uso de leyes y estándares**: Se trata del mecanismo de prevención que consiste en aplicar la legislación vigente, los procedimientos internos, los controles de seguridad y los estándares de buenas prácticas a la gestión de los sistemas de información de una organización para anticipase a posibles ataques.
- **Uso de sistemas trampa**: Se trata del mecanismo de prevención que consiste en incluir sistemas, como pueden ser los *honeypots*[74], que simulan servicios con fallos de seguridad para engañar a un atacante y hacerle pensar que se puede aprovechar de una vulnerabilidad cuando realmente se registra toda su actividad para mitigarla o bloquearla antes de que consiga realizar un incidente de seguridad.
- **Uso de pruebas de penetración**: Se trata del mecanismo de prevención que consiste en evaluar la seguridad de un servicio o un activo de información mediante un ciberataque simulado y controlado en donde no sólo se verifica una vulnerabilidad, sino que también se intenta explotar para mitigarlo o bloquearlo antes de que se pueda producir un incidente de seguridad real. Asimismo, este tipo de pruebas, usadas en auditorías, pueden ser de diferentes tipos:
    - **Pruebas de caja negra (*black box*)**: Pruebas de penetración que consiste en, a penas, conocer información sobre la organización, tal y como lo realizaría un posible atacante real, por lo que se descubren debilidades en la arquitectura que se pueden prevenir con medidas de mitigación o bloqueo.
    - **Pruebas de caja blanca (*white box*)**: Pruebas de penetración que consiste en analizar íntegramente toda la infraestructura con toda la información disponible de la organización, por lo que se realizan todas las pruebas de penetración posibles y se descubren las debilidades en la arquitectura y en los servicios y configuraciones internas de la organización, que se pueden prevenir con medidas de mitigación o bloqueo o reconfiguración de los servicios, entre otros.
    - **Pruebas de caja gris (*grey box*)**: Pruebas de penetración más equilibrada, que mezcla las pruebas de caja blanca y caja negra y se basa en conocer algo de información específica de la organización para detectar debilidades en sus servicios, tal y como lo realizaría un atacante que hubiese vulnerado y estudiado su arquitectura y perímetro, por lo que, aunque requeriría tiempo y recursos, se descubren debilidades, que se pueden prevenir con medidas de mitigación o bloqueo o reconfiguración de los servicios, entre otros.

7.1.4.3 Mecanismos de detección y respuesta

Los mecanismos de detección y respuesta se definen como los sistemas y componentes de seguridad de una organización que se encargan de localizar y notificar cualquier actividad sospechosa de ser maliciosa en la red corporativa y de reaccionar ante ese evento para evitar impacto en el posible ataque y su correspondiente incidente de seguridad. Por ello, las organizaciones deben instaurar

[74] https://latam.kaspersky.com/resource-center/threats/what-is-a-honeypot

equipos de seguridad, como puede ser un SOC, junto a herramientas de seguridad, como puede ser un SIEM, para predecir, detectar, estudiar, responder y restablecer los servicios y activos de información ante los posibles incidentes de seguridad.

7.1.4.3.1 Principales herramientas de detección y respuesta

Aunque este tipo de tecnologías viene definido en el apartado 7.3.2 del Anexo 3[75], entre los principales sistemas de detección y respuesta que se pueden implantar en una organización, se encuentran los siguientes:

- **Sistema de gestión de eventos e información de seguridad (SIEM)**: Se trata de una herramienta que identifica, realiza seguimiento, registra, agrupa y analiza los eventos de seguridad dentro de un entorno de red en tiempo real, mediante la recepción de registros de logs de diferentes fuentes, para detectar posibles incidentes de seguridad.
- **Sistema de detección y respuesta de puntos finales (EDR)**: Se trata de una herramienta que detecta y combate las amenazas y ataques más avanzadas de los puntos finales de la red de una organización, como los equipos de usuario o los servidores, para responder a los incidentes de seguridad resultantes.
- **Sistema de orquestación, automatización y respuesta de seguridad (SOAR)**: Se trata de una herramienta que recolecta y agrupa datos de los diferentes eventos de seguridad que se detecten en los registros de *logs* que se reciban de las diferentes fuentes, para dar respuesta automática a las posibles amenazas e incidentes de seguridad sin interacción humana.
- **Sistema de detección de intrusiones (IDS)**: Se trata de una herramienta que supervisa las comunicaciones de red de una organización para detectar movimientos sospechosos, actividades maliciosas o vulneraciones en sus políticas de seguridad.

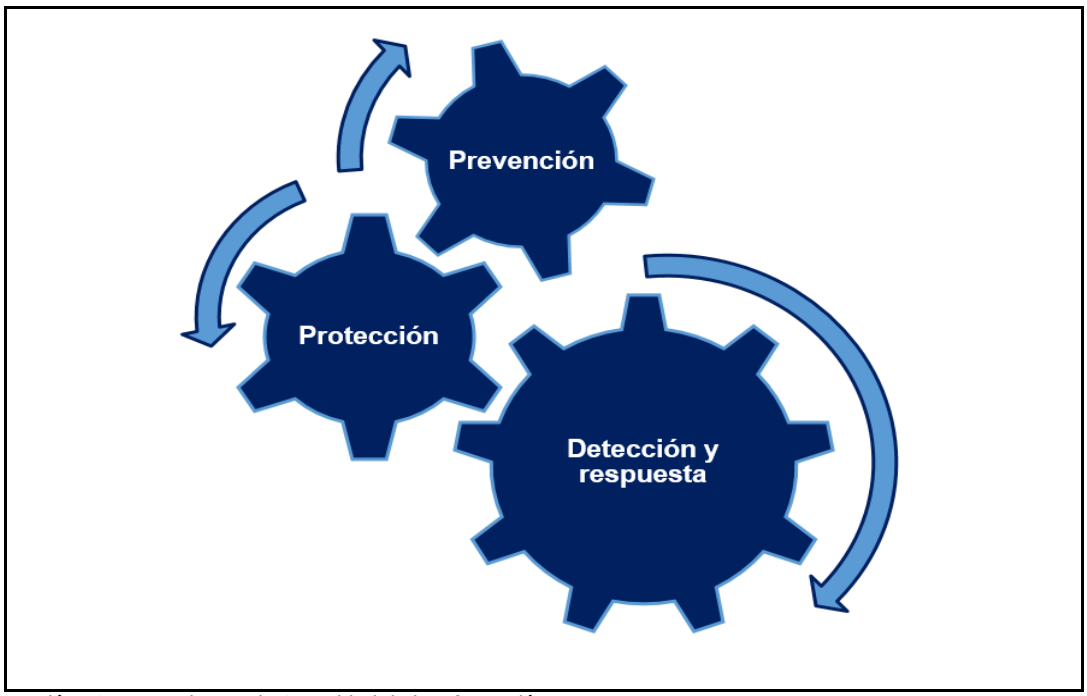

Ilustración 18 - Mecanismos de Seguridad de la Información.

[75] Ver el punto 7.3.2 del Anexo 3 para más información sobre las Tecnologías de un SOC.

7.2 Anexo 2: Análisis del marco metodológico y legal de un SOC

Con el fin de comprender el marco metodológico y las diferentes disposiciones legales que aplican a la gestión de la Seguridad de la Información y, por su interconexión en la red, también a la gestión de la Ciberseguridad, a continuación, se resume el análisis y estudio de algunos de los estándares, normativas y metodologías internacionales más importantes y relevantes, así como de las disposiciones legales vigentes que se aplican a este equipo de seguridad y a su implementación, tal y como se han estudiado en diferentes asignaturas del máster universitario de Ciberseguridad y Privacidad de la UOC.

En la actualidad, existen diferentes documentos guías y de buenas prácticas para la implementación de un CSIRT[76] o un SOC[77], como el publicado por ENISA (Agencia de la Unión Europea para la Ciberseguridad), pero no existe un estándar, normativa o marco metodológico propio para la gestión y funcionamiento de un SOC. Sin embargo, existen diferentes guías, estándares, normativas, buenas prácticas, metodologías internacionales y disposiciones legales relacionadas con la Seguridad de la Información, la Gestión de Proyectos, las Tecnologías de la Información en las organizaciones y el uso y tratamiento de la información que, por extensión, pueden ser aplicables a un SOC y favorecer su correcta administración, desempeño y organización. Por tanto, a continuación, se describen algunos de los más relevantes:

7.2.1 Normativas ISO

Las normativas ISO se definen como el conjunto de modelos de referencia con reconocimiento internacional creados para facilitar y homogeneizar la implementación, gestión, desarrollo de productos y prestación de servicios en las organizaciones.

Ilustración 19 - Logo ISO (https://www.iso.org/)

Por ello, en relación con la Seguridad de la Información, la Ciberseguridad y el funcionamiento de un SOC, se destacan las siguientes normas:

[76] https://es.wikipedia.org/wiki/Equipo_de_Respuesta_ante_Emergencias_Inform%C3%A1ticas
[77] https://www.enisa.europa.eu/publications/csirt-setting-up-guide

7.2.1.1 ISO/IEC 27000

Las normas ISO/IEC 27000 se definen como un conjunto estándares de Seguridad de la Información publicados por la Organización Internacional para la Estandarización y la Comisión Electrotécnica Internacional que facilitan las mejores experiencias para la implantación, el seguimiento y la gestión de los Sistemas de Gestión de Seguridad de la Información (SGSI). Asimismo, su principal objetivo se basa en disponer de los términos y conceptos que se utilizan en toda la serie 27000 y en garantizar la seguridad, las mejoras continuas y la reducción de los posibles riesgos en estos Sistemas de Gestión.

7.2.1.2 ISO/IEC 27001 e ISO/IEC 27002

Entre las normas más importantes de la familia de la ISO/IEC 27000 se encuentran las normativas ISO/IEC 27001 y la ISO/IEC 27002 que se describen a continuación:

- **ISO/IEC 27001**: Normativa principal de la serie 27000 que determina los requerimientos necesarios para la implantación y gestión de un SGSI que se basa en asegurar las propiedades de la información de una organización, sus tecnologías y los activos que la gestionan. Además, se trata de una norma certificable y se estructura desde su versión de 2013 de la siguiente forma:
    1. **Alcance y objeto de aplicación**: Guía acerca de su utilidad, finalidad y aplicación de la norma.
    2. **Terminología**: Define los conceptos y términos de la norma.
    3. **Referencias Normativas**: Menciona y relaciona otras normas y documentos necesarios para aplicar esta norma.
    4. **Contexto organizativo**: Estudia la organización, su entorno, necesidades, aspiraciones y alcance de un SGSI.
    5. **Liderazgo**: Indica que la alta dirección debe mostrar liderazgo en el compromiso de la norma y crear una política de seguridad, capacitar a toda la organización y establecer responsabilidades, roles y autoridades, ya que ésta necesita de todos los activos humanos de la organización para su funcionamiento.
    6. **Planificación**: Determina la necesidad de gestionar los riesgos y las oportunidades y de establecer los objetivos y su forma de lograrlos.
    7. **Soporte**: Manifiesta la necesidad de usar recursos, documentación, capacitación y competencias para el funcionamiento de un SGSI basado en la norma.
    8. **Operación**: Establece la necesidad de realizar la planificación, implementación y control de los procesos de negocio de la organización y valorar y tratar sus riesgos.
    9. **Desempeño**: Determina la manera de realizar el seguimiento, evaluar, analizar, ponderar, auditar y revisar un SGSI en base a la planificación realizada según la norma.
    10. **Mejora**: Determina la importancia de la mejora continua de la eficacia, el beneficio y la conveniencia de un SGSI.

  Igualmente, en su nueva versión de 2022, tras casi una década de diferencia entre versiones, la norma se actualiza a los nuevos cambios y necesidades de

vida y de los negocios ocasionados, por ejemplo, por la pandemia de la COVID-19 o el avance de las tecnologías, en donde el teletrabajo y el uso de recursos en la nube obtienen mayor relevancia y generan nuevos riesgos que se deben considerar en un SGSI. De hecho, aunque no se encuentran demasiados cambios significativos, se pueden encontrar los siguientes:

- Se reestructura la numeración con mayor visión de alto nivel.
- Se referencian y describen los controles del Anexo A en ISO/IEC 27002:2022.
- Se sustituye los objetivos de control por los "atributos" y "propósitos" de los controles.
- Se cambia la definición de "control de seguridad de la información" por "control" (cláusula 1.3 c).
- Se definen los procesos junto con sus interacciones para alinearlo con las buenas prácticas (cláusula 4.4).
- Se manifiesta la importancia de informar los roles en seguridad de la información en toda la organización (cláusula 5.3).
- Se expresa la importancia de la monitorización de los objetivos de Seguridad de la Información (cláusula 6.2).
- Se indica la necesidad de planificar y controlar los cambios del SGSI y documentar sus pasos y formas de implementación (cláusula 6.3).
- Se reitera la importancia de gestionar por procesos el SGSI y de establecer pautas para definir criterios y aplicar sus controles (sección 8 y cláusula 8.1).

- **ISO/IEC 27002**: Normativa que establece las buenas prácticas y experiencias para la implantación y gestión de un SGSI, que, en su versión de 2013, se basaba en 114 controles que se estructuraban en 14 dominios de seguridad y, en su nueva versión de 2022, se basa en 93 controles (37 organizativos, 8 de personal, 14 físicos y 34 tecnológicos) que se estructuran en 4 cláusulas o grupos. De hecho, en la nueva versión, se unifican 24 controles con controles existentes de la versión anterior, se actualizan 58 controles existentes y se incluyen 11 nuevos:
  - Inteligencia de ciberamenazas.
  - Seguridad de la Información para servicios en la nube.
  - Adecuación de la continuidad de negocio a los activos de información.
  - Análisis en tiempo real de la seguridad física.
  - Gestión de la configuración.
  - Eliminación de la información.
  - Encubrimiento de los datos.
  - Prevención de la filtración de datos.
  - Análisis en tiempo real de las actividades.
  - Filtrado web.
  - Control de la codificación segura.

Asimismo, su estructura de controles se realiza mediante atributos, utiliza conceptos más relevantes y actuales como los tipos de control, mayor número de propiedades de Seguridad de la Información y términos de ciberseguridad, entre otros. Además, también orienta su perspectiva hacia mecanismos de prevención contra los posibles incidentes de seguridad que surjan en las organizaciones.

7.2.1.3 Resto de normativas de la familia ISO/IEC 27000

A continuación, se cita el resto de normas de la familia ISO/IEC 27000 con mayor relevancia para la Seguridad de los Sistemas de Información:

- **ISO/IEC 27003**: Normativa que proporciona las pautas para la implantación de un SGSI enfocada en las características importantes para el éxito del proceso y que se basa en facilitar esas directrices para la implantación de un SGSI.
- **ISO/IEC 27004**: Normativa que proporciona las pautas, métricas y técnicas para evaluar el rendimiento de los SGSI y que se basa en facilitar esas directrices y controles para valorar el funcionamiento y la utilidad de un SGSI.
- **ISO/IEC 27005**: Normativa que facilita las diferentes directrices y recomendaciones para la gestión de riesgos de la seguridad de la información de una organización y que da soporte para aplicar de forma satisfactoria un SGSI basado en el enfoque de la gestión de riesgos.
- **ISO/IEC 27006**: Normativa que indica los requerimientos necesarios para la acreditación de entidades que proporcionan la certificación de un SGSI y que se centra en proporcionar esos requisitos para acreditar a las entidades certificadoras de un SGSI. Además, se trata de una norma certificable.
- **ISO/IEC 27007**: Normativa que indica las pautas necesarias para auditar un SGSI en su proceso de certificación de la implementación del estándar ISO/IEC 27001 en una organización y que se basa en la guía para auditar los SGSI.
- **ISO/IEC TS 27008**: Normativa que rige la auditoría de los controles seleccionados en el marco de implantación de un SGSI y que se basa en la guía para auditar dichos controles.
- **ISO/IEC 27009**: Normativa que indica los requerimientos para crear estándares concretos para ampliar la norma ISO/IEC 27001 y completan o rectifican la ISO/IEC 27002 para proteger un ámbito determinado y que se centra en complementar y corregir los requisitos y controles a las normas ISO/IEC 27001 y ISO/IEC 27002.
- **ISO/IEC 27010**: Normativa que aconseja sobre la gestión de la seguridad de la información en el intercambio de información relativa a los riesgos, controles, problemas e incidentes relacionados con la seguridad de la información y que se centra en la gestión de las comunicaciones relacionados con la seguridad de la información entre sectores.
- **ISO/IEC 27011**: Normativa que proporciona las directrices para la implantación y gestión de un SGSI en organizaciones del sector de las telecomunicaciones y que se basa en las indicaciones acerca de cómo implantar controles de seguridad de la información de manera eficiente para este sector.

- **ISO/IEC 27013**: Normativa que facilita las directrices para la integración de las normas ISO/IEC 27001 (SGSI) e ISO/IEC 20000-1 (Sistema de Gestión de Servicios o SGS) de forma conjunta y que se centra en guiar la implementación integrada de ambas ISO.
- **ISO/IEC 27014**: Normativa que facilita las directrices y principios para gobernar la seguridad de la información y que se centra en que las organizaciones puedan evaluar, controlar e informar las actividades relacionadas con la seguridad de la información.
- **ISO/IEC TR 27016**: Normativa que proporciona la orientación para el análisis económico y financiero de los sistemas y procedimientos de la seguridad de la información y que se basa en facilitar la toma de decisiones económicas relacionadas con los SGSI.
- **ISO/IEC 27017**: Normativa que indica los requerimientos para crear una guía para los controles de seguridad de la información que se atribuyen al suministro y aplicación de servicios en la nube y que se centra en facilitar la implementación de nuevos controles y de los controles relevantes de la ISO/IEC 27002 para la puesta en marcha de los servicios en la nube. Además, se trata de una norma certificable, pero como ampliación y en conjunto con la ISO/IEC 27001.
- **ISO/IEC 27018**: Normativa que indica los requerimientos para para poner en funcionamiento acciones para salvaguardar la información de identificación personal (PII) en base a los principios de privacidad de la normativa ISO/IEC 29100 en entornos de computación en la nube pública. Además, se trata de una norma certificable, pero como ampliación y en conjunto con la ISO/IEC 27001.
- **ISO/IEC 27019**: Normativa que indica los requerimientos para crear un estándar para gobernar y monitorizar el tratamiento y conservación de la energía eléctrica, el gas, el petróleo y el calor de los sistemas de control de procesos usados por la industria de servicios públicos de energía y sus procesos de soporte.
- **ISO/IEC 27021**: Normativa que indica los requerimientos para establecer la atribución de los profesionales de ISMS que establecen, implementan, mantienen y mejoran de forma continua los procesos del sistema de gestión de seguridad de la información indicados en la norma ISO/IEC 27001.
- **ISO/IEC 27022**: Normativa que indica los requerimientos para establecer un modelo de referencia para los procesos (PRM) de dominio de la gestión de la seguridad de la información.
- **ISO/IEC 27023**: Normativa que indica los requerimientos para migrar de las versiones de 2005 a 2013 de las normas ISO/IEC 27001 e ISO/IEC 27002.
- **ISO/IEC 27031**: Normativa que establece los requisitos para la creación de un plan de Continuidad de las tecnologías de la información y comunicaciones y que se enfoca en guiar las bases para generar continuidad de negocio en las organizaciones de TIC.
- **ISO/IEC 27032**: Normativa que establece las directrices para fortalecer el estado de la ciberseguridad de las organizaciones en base a la seguridad de la información, así como de las redes, de las Infraestructuras Críticas para la Información y en internet y que se basa en proporcionar una guía sobre ciberseguridad para las organizaciones.

- **ISO/IEC 27033**: Normativa parcialmente desarrollada, pero con partes publicadas, que establece las directrices para fortalecer el estado de la seguridad de las redes de comunicaciones de las organizaciones.
- **ISO/IEC 27034**: Normativa parcialmente desarrollada, pero con partes publicadas, que establece las directrices para fortalecer el estado de la seguridad de las aplicaciones informáticas de las organizaciones.
- **ISO/IEC 27035**: Normativa que establece las buenas prácticas para la gestión de incidentes de seguridad de la información y que se focaliza en proporcionar las directrices necesarias para ejecutar un plan de gestión de incidentes estratégico que tenga en cuenta la respuesta ante incidentes de seguridad de la información.
- **ISO/IEC 27036**: Normativa que establece las directrices para fortalecer el estado de la seguridad de las relaciones con proveedores de las organizaciones.
- **ISO/IEC 27037**: Normativa que establece las guías para el reconocimiento, recolección, la adquisición y la preservación de pruebas digitales que se pueden utilizar con valor probatorio y en el intercambio entre las diferentes jurisdicciones
- **ISO/IEC 27038**: Normativa que establece las guías para la seguridad en la redacción digital de documentos.
- **ISO/IEC 27039**: Normativa que establece las directrices para la elección, despliegue y tratamiento operativo de sistemas de detección (IDS) y prevención de intrusiones (IPS).
- **ISO/IEC 27040**: Normativa que establece las directrices para la seguridad de los dispositivos de almacenamiento.
- **ISO/IEC 27041**: Normativa que establece las directrices para la certificar la adecuación y conveniencia de los métodos de investigación.
- **ISO/IEC 27042**: Normativa que establece las bases y los procesos de investigación de incidentes relacionados con la recolección de evidencias digitales.
- **ISO/IEC 27050**: Normativa que establece los conceptos, las buenas prácticas y las directrices para identificar, preservar, recolectar, procesar, revisar, analizar y gestionar la información recogida en dispositivos electrónicos.
- **ISO/IEC 27100**: Normativa que establece una definición del concepto de ciberseguridad y su contexto en diferencia con la seguridad de la información.
- **ISO/IEC 27102**: Normativa que establece los requerimientos para valorar la contratación de un ciberseguro como opción para el tratamiento de los riesgos y la gestión del impacto de un ciberincidente en una organización.
- **ISO/IEC TR 27103**: Normativa que facilita una guía sobre la manera de utilizar las normativas existentes en el ámbito de la ciberseguridad.
- **ISO/IEC TS 27110**: Normativa que establece los conceptos básicos del ámbito de la ciberseguridad para el desarrollo de marcos de ciberseguridad.
- **ISO/IEC TR 27550**: Normativa que establece conceptos del ámbito de la privacidad en ingeniería de Sistemas de Tecnologías de la Información y Comunicaciones.

- **ISO/IEC TR 27555**: Normativa que establece las directrices para el desarrollo y establecimiento de políticas y procedimientos para la eliminación de PII en una organización.
- **ISO/IEC TS 27570**: Normativa que establece las guías sobre la privacidad de los ciudadanos para el desarrollo de ecosistemas para las *smart cities* (ciudades inteligentes).
- **ISO/IEC 27701**: Normativa que establece los requerimientos y las guías para el tratamiento continuo de Sistemas de gestión de información de privacidad (PIMS) dentro del contexto de una organización y como ampliación de las normas ISO/IEC 27001 e ISO/IEC 27002.

7.2.1.4 ISO 22301

Se trata de una normativa de **Continuidad del Negocio** que establece los requisitos para la creación de un Sistema de Gestión de la Continuidad de negocio en donde se establecen las directrices, los procesos y los conceptos necesarios para su gestión. Su alcance es mucho mayor que la seguridad de la información, pero tiene relación con este ámbito y su objetivo principal se enfoca en guiar las bases para generar la continuidad de negocio en cualquier organización.

7.2.1.5 ISO 31000

Se trata de una normativa de **Gestión de Riesgos** que determina las bases, el ámbito y un proceso para la gestión de cualquier tipo de riesgo. Su alcance también es mucho mayor que la seguridad de la información, pero tiene relación con este ámbito. Además, su objetivo principal se basa en facilitar los principios y directrices para la gestión de riesgos a nivel estratégico y operativo en las organizaciones.

7.2.2 CobIT

Se trata de una normativa que establece una lista de controles y buenas prácticas para la dirección y gestión de la información y de sistemas empresariales. Además, facilita un marco de referencia para que las organizaciones lo ajusten a sus objetivos de negocio y determinen la manera de obtener la información, la forma de conseguir sus objetivos del negocio a través de las tecnologías de información, el modo de gestionar sus riesgos, proteger sus recursos y medir sus controles. Asimismo, su nombre proviene de las siglas de **C***ontrol* ***ob****jectives for* ***I****nformation and related* ***T****echnology*, su última versión se define como Cobit 2019 y bajo esta norma se definen cinco áreas de trabajo:

- La alineación estratégica.
- La entrega de valor.
- La gestión de los riesgos.
- La gestión de los recursos.
- El cómputo del desempeño.

Por tanto, CobIT puede facilitar el análisis de los controles que se implanten en un SOC con la inclusión de métricas y valoraciones obtenidas, según su Modelo de Madurez, y la incorporación de diagramas, flujos y gráficas que guíen a los procesos internos para la gestión de las diferentes áreas y la toma de decisiones en la implantación de un SOC y en el tratamiento de los eventos e incidentes de seguridad que se produzcan.

Ilustración 20 - Logo de CobIT 2019 (https://www.isaca.org/)

7.2.3 PCI DSS

Se trata de una normativa de seguridad de datos para la industria de las tarjetas de pago de débito y de crédito, en donde su principal objetivo se centra en la seguridad de la información sensible de estas tarjetas, a través de una guía para procesar, almacenar, transmitir y asegurar los datos de los titulares de las tarjetas y sus transacciones, con el fin de impedir los posibles casos de fraude que puedan recibir. Se desarrolló por una junta formada por personal de las empresas de tarjetas de pago más importantes y su nombre proviene de las siglas de ***P**ayment **C**ard **I**ndustry **S**ecurity **S**tandards **C**ouncil*. Además, su última versión, la 4.0, establece 12 requisitos o controles, que se organizan en 6 objetivos de control, que se pueden utilizar de guía en la implementación de un SOC aplicado a una organización empresarial con negocio en las tarjetas de pago y en su gestión de los eventos e incidentes de seguridad. Sus objetivos de control y requisitos se muestran a continuación:

1. **Diseño y gestión de una red segura**:
    - **Control 1**: Instalación, configuración y gestión de un cortafuegos.
    - **Control 2**: Uso de contraseñas complejas y parámetros de seguridad seguros.
2. **Protección de los datos de los propietarios de las tarjetas**:
    - **Control 3**: Salvaguarda de los datos guardados de los titulares de las tarjetas.
    - **Control 4**: Cifrado de datos e información confidencial de los titulares de las tarjetas que se transmiten por redes públicas abiertas.
3. **Mantenimiento de programas para gestionar las vulnerabilidades**:
    - **Control 5**: Uso y actualización continua de software antivirus.
    - **Control 6**: Desarrollo y gestión de sistemas y aplicaciones seguras.
4. **Implementación de medidas robustas del control de acceso**:
    - **Control 7**: Restricción de acceso a los datos de los propietarios de las tarjetas y de los componentes del sistema para fines comerciales.
    - **Control 8**: Asignación de un identificador único a cada persona para uso digital.
    - **Control 9**: Restricción del acceso físico a los datos de los titulares de las tarjetas.

5. **Monitorización y comprobación regular de las redes**:
    - **Control 10**: Monitorización y rastreo de los accesos a los recursos de red y de datos de los titulares de las tarjetas.
    - **Control 11**: Comprobación regular de los sistemas y sus procesos de seguridad.
6. **Mantenimiento de una Política de Seguridad de la Información**:
    - **Control 12**: Mantenimiento de una política que respalde de la Seguridad de la Información de la organización.

Ilustración 21 - Logo de PCI-DSS (https://www.pcisecuritystandards.org/)

7.2.4 CMM

Se trata de un modelo que proporciona las directrices para el desarrollo de procesos eficientes y de calidad en las organizaciones, que se desarrolló, en sus comienzos, para los procesos de desarrollo de software, pero que se ha ampliado al resto de procesos de negocio, por lo que su objetivo se focaliza en la mejora de los procesos. Además, su nombre proviene de ***C**apability **M**aturity **M**odel* (Modelo de Madurez de Capacidades, en español) y determina una serie procesos clave o buenas prácticas que se agrupan en **KPA** (*Key Process Area* o Áreas Clave de Procesos, en español) y se caracterizan por definirse en procesos documentados, proveer a la organización de formación y medios, ejecutarse sistemática, uniforme y universalmente y medirse y verificarse.

Asimismo, este modelo puede facilitar la medición de métricas de los diferentes servicios y procesos de un SOC a través de las KPA indicadas, que se congregan en cinco niveles de madurez:

1. **Inicial**: No se dispone de estabilidad ni planificación.
2. **Repetible**: Se dispone de prácticas de gestión de proyectos, métricas básicas y seguimiento de la calidad.
3. **Definido**: Se dispone de una buena gestión de proyectos y buenas métricas, técnicas de ingeniería, procedimientos de coordinación y formación del personal.
4. **Gestionado**: Se dispone de métricas significativas de productividad y calidad para la gestión de riesgos y la toma de decisiones.
5. **Optimizado**: Se utilizan métricas, se tratan procesos de innovación y se centra en la mejora continua de los procesos.

7.2.5 SSE-CMM

Se trata de un modelo, derivado del CMM, que describe las principales características de los procesos necesarios para garantizar la creación y el desarrollo seguro de los sistemas de las organizaciones, por lo que, además de medir los diferentes procesos y servicios de un SOC, también puede describir el estado de madurez de sus controles y de los controles de Seguridad de la Información de la organización para la que trabaja. Su nombre proviene de ***S**ystem **S**ecurity **E**ngineering **C**apability **M**aturity **M**odel* (Modelo de Madurez de Capacidades en la Ingeniería de Seguridad de Sistemas, en español) y fue desarrollado por la organización sin ánimo de lucro *International Systems Security Engineering Association* (ISSEA). Asimismo, este modelo define 22 áreas, 11 de procesos de ingeniería y otras 11 de procesos de organización y gestión de proyectos, que se miden y cuantifican con los niveles de madurez del modelo CMM y según las denominadas Características Comunes:

1. Responsabilidad de ejecución.
2. Suficiencia para la ejecución.
3. Tareas ejecutadas.
4. Métricas, estudio y análisis.
5. Comprobación de la puesta en funcionamiento.

7.2.6 ITIL

Los servicios de Sistemas y Tecnologías de la Información determinan la relación entre las personas, las tecnologías y los procesos en una organización. Por tanto, la **gestión de servicios** entiende a la organización como un sistema interconectado de recursos organizativos y prácticas con el objetivo de mejorar y maximizar la satisfacción del cliente. Esto tiene como consecuencia que se recorra la organización desde su perspectiva en los productos, donde no haya procesos coordinados ni administrados, hacia una perspectiva donde prime la libertad en el diseño de los procesos a medida y su mejora continua, por parte de los proveedores de servicios, para que se desempeñen en su organización y generen siempre valor.

La gestión de servicios se ocupa de establecer los procesos que se deben mejorar, rediseñar y priorizar. Además, también se encarga de facilitar un ambiente para crear y gestionar planes de mejora, en base a los objetivos establecidos, y de favorecer el entendimiento de la mecánica de los procesos de negocio, bajo el razonamiento de sus fortalezas y debilidades.

ITIL se define como una biblioteca, un marco de referencia, que contiene una serie de recomendaciones y buenas prácticas descritas para la administración y gestión de servicios de Tecnologías de la Información. Asimismo, este modelo contiene la información necesaria de los objetivos y propósitos a alcanzar, de las actividades y tareas generales y de las entradas y salidas de los procesos que se pueden añadir a las áreas de las Tecnologías de la Información. Además, su objetivo principal se centra en generar valor en la entrega de servicios mediante la provisión de las mejores prácticas para la Gestión de Servicios de Tecnologías de la Información. De hecho, a continuación, se muestra el modelo de Sistema de Valor del Servicio propuesto por ITIL:

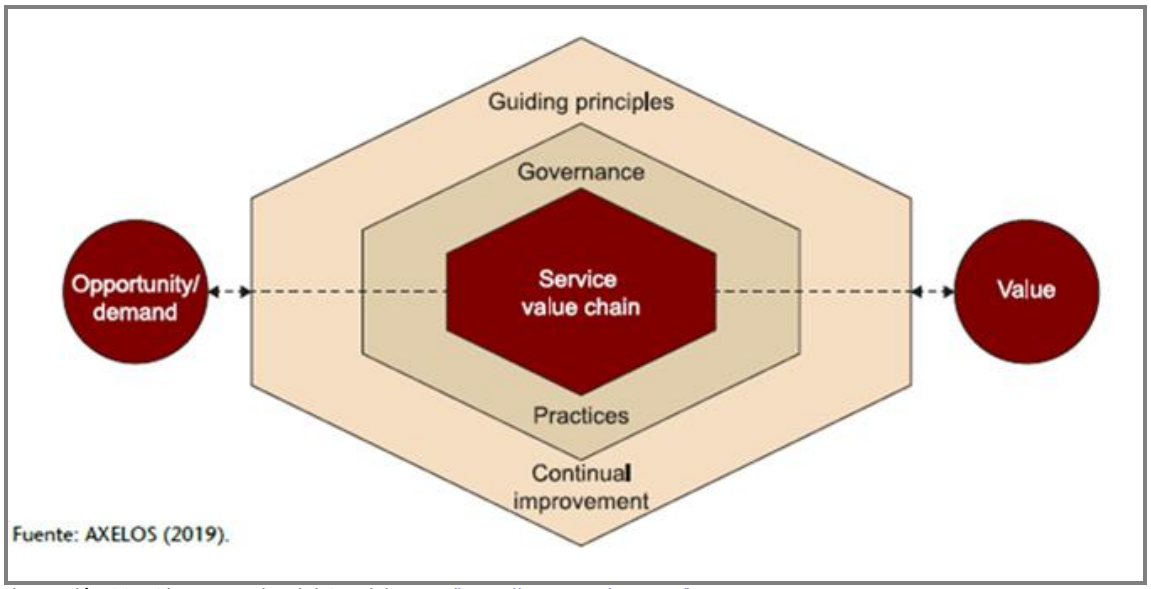

Ilustración 22 - Sistema Valor del Servicio ITIL (https://www.axelos.com/).

Por otra parte, ITIL también conlleva un proceso de cambio en la organización si se desea aplicar a un proyecto de implementación de un servicio, como puede ser un SOC. Por tanto, se enfatizan los siguientes aspectos:

- **Responsabilidad de la alta dirección**: Sin el apoyo de la dirección no se lograrán los objetivos ni las mejoras continuadas en el tiempo, sino sólo propósitos y resultados parciales.
- **Formalidad del proyecto**: Se necesitan asignar recursos económicos, materiales y humanos para poder realizar tareas que impliquen administrar el proyecto, actualizar la documentación de los procesos, analizar y revisar la alineación de la guía con los procesos de negocio y establecer el plan de comunicación del proyecto en la organización, entre otros.
- **Formación del negocio**: Todo el personal de la organización debe estar instruido en la relación de ITIL con el negocio.
- **Participación de todos los intervinientes**: Se requiere que todas los niveles y partes involucradas en este cambio organizativo, se encuentren informados de todo el proceso.

En consecuencia, se deben gestionar los servicios de forma global mientras se atiende al contexto estratégico. Debido a este motivo, ITIL define una serie de recursos organizativos, llamados prácticas, que se han diseñado para su implementación en las organizaciones para alcanzar los objetivos fijados. Estas prácticas se asocian en tres grandes conjuntos:

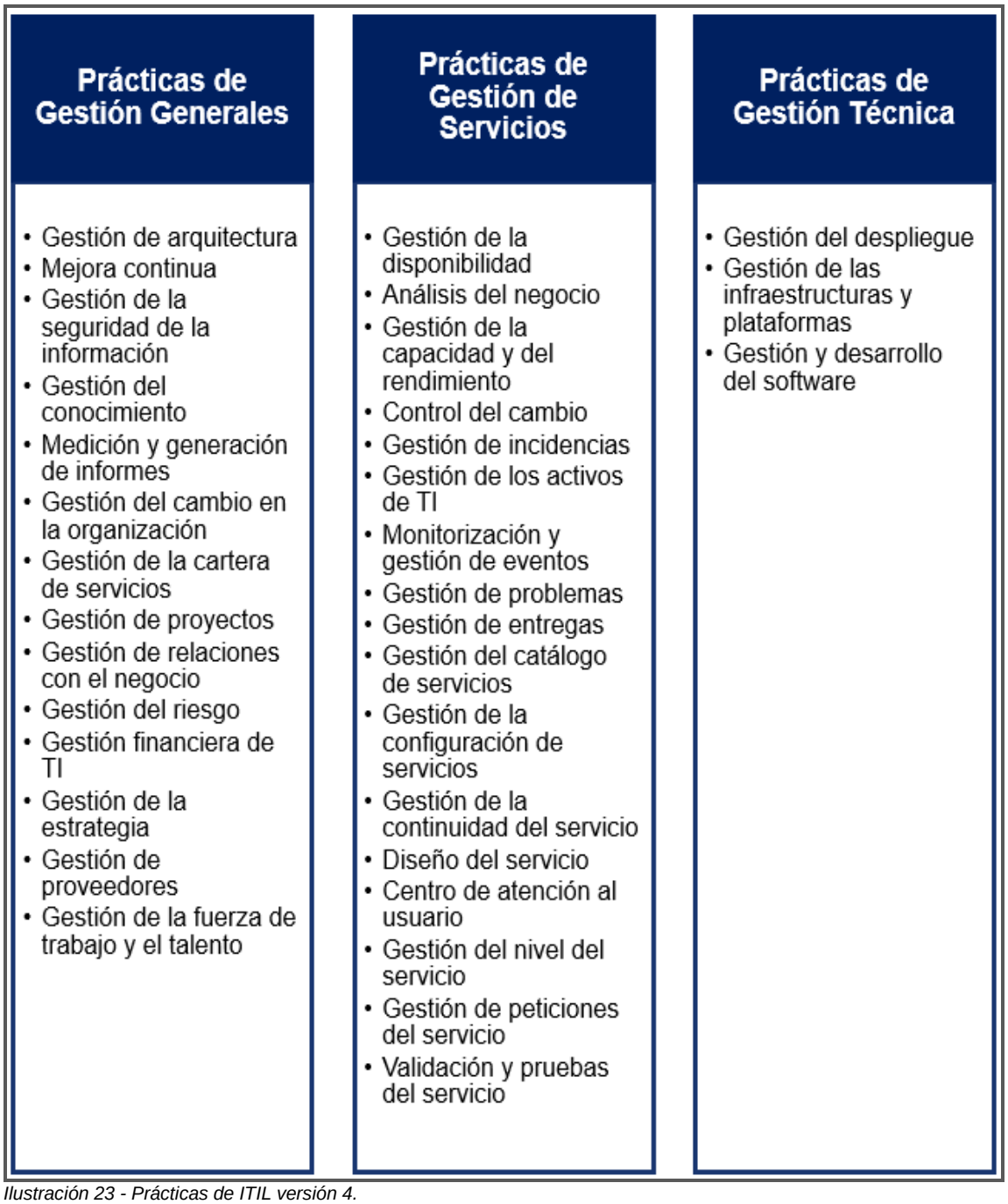

Ilustración 23 - Prácticas de ITIL versión 4.

Asimismo, estas prácticas o recursos organizativos se encuentran afectados por factores del tipo legal, ambiental, económico, tecnológico, social y políticos, entre otros, por lo que se basan en cuatro espacios, llamados dimensiones, donde se definen los servicios que finalmente agregan valor. Por tanto, el esquema propuesto por ITIL para estas cuatro dimensiones de la Gestión del Servicio se expresa como sigue a continuación:

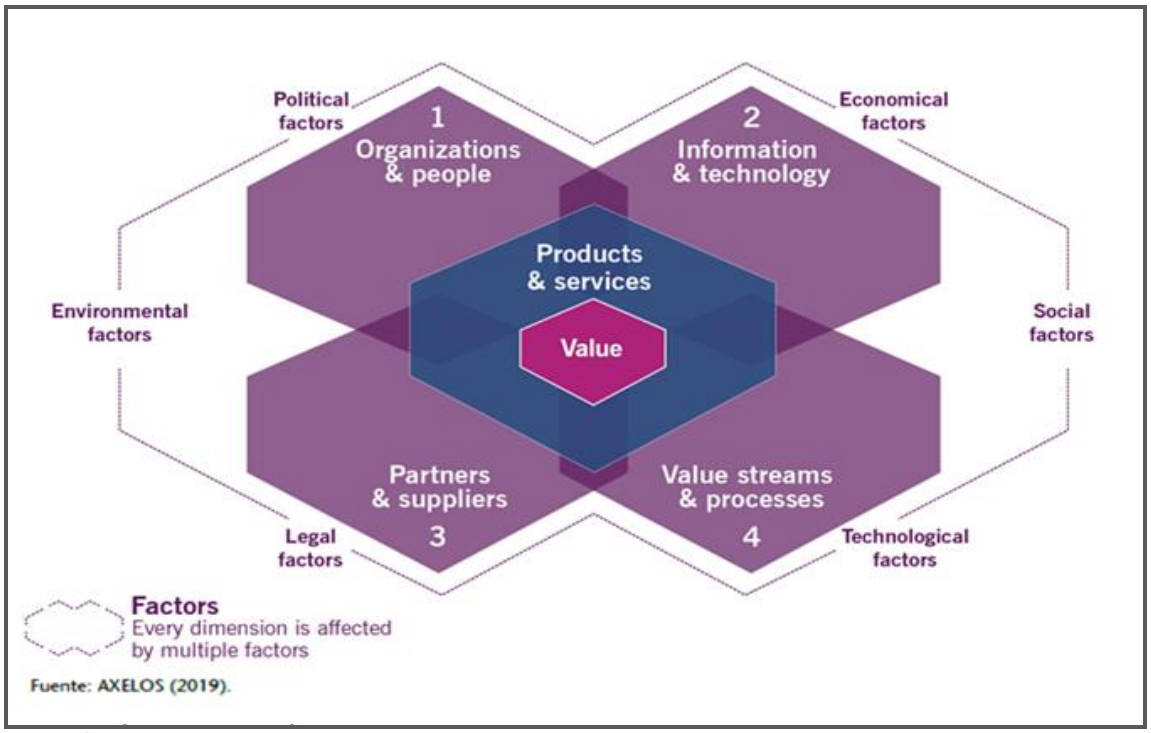

Ilustración 24 - Cuatro dimensiones de ITIL v.4 (https://www.axelos.com/).

De esta manera, ITIL entrega valor a un proyecto de implementación de un SOC a través de los siguientes beneficios:

- **Favorece la comunicación**: Garantiza un lenguaje común para todas las áreas de una organización.
- **Suministra un modelo de dirección de TI**: Implementa objetivos de negocio con los que genera confianza y provee de estructuras y controles de información para garantizar el apoyo de las estrategias de negocio por el departamento de TI.
- **Minimiza los costes de TI y maximiza la calidad del Servicio**: Genera más productividad y reduce los gastos con procesos de TI maduros.
- **Implementa e integra procesos en el área de TI**: Describe un modelo de procesos con responsabilidades y roles que mejora la manera de trabajar en una organización.
- **Intensifica la Integración del Negocio con el área de TI**: Alinea los servicios de TI con los procesos de negocio, mediante el ideal de la Gestión de Servicios de TI.
- **Respeta las regulaciones**: cumple con las regulaciones y normativas legales, como pueden ser Base II, la ISO/IEC 27001, la ISO/IEC 38500 y Sabanes-Oxley (SOX), entre otras.
- **Optimiza la Gestión de proveedores**: Recoge los diferentes niveles de servicio para con los clientes y establece Acuerdos de Nivel de Servicio (ANS).
- **Entrega valor**: Crea una relación de confianza con el cliente y aumenta su satisfacción.

7.2.7 DevSecOps

DevOps se describe como una cultura o filosofía colaborativa basada en los principios de Lean y de las metodologías ágiles para la generación de servicios y productos que se adaptan a las necesidades y plazos de los clientes. Sin embargo, dado que la Seguridad de la Información se considera un factor que se debe tener en cuenta como un elemento integral y automatizable en todos los procesos del ciclo de vida de un producto, debe considerar la Seguridad como un proceso de la misma importancia que el Desarrollo y las Operaciones para romper con la barrera que los separa. Por ello, su responsabilidad se debe encontrar distribuida por todos sus equipos y se necesitan incorporar herramientas de seguridad en cada uno de los procesos de su pipeline de principio a fin. Por tanto, a partir de la seguridad en DevOps, se ha establecido el concepto de **DevSecOps**,

DevSecOps se define como un enfoque o filosofía de gestión que integra la automatización de la seguridad en todas las fases del ciclo de desarrollo y de la entrega continua de DevOps. Debido a esto, integrar esta cultura en la implementación y funcionamiento de un SOC puede mejorar su puesta en funcionamiento, su gestión y la calidad en la entrega de los servicios. Además, su integración se segmenta en diferentes prácticas que se requieren para garantizar la seguridad del pipeline de DevOps en las siguientes cuatro etapas:

1. **Análisis**: Se trata de la etapa de DevSecOps, incluida dentro de la fase de Planificar de DevOps, en donde se detectan y priorizan las vulnerabilidades y amenazas y se estudian y planifican los riesgos actuales. De hecho, en esta etapa se incluye la participación, el debate, la comprobación y la planificación de la estrategia del análisis de seguridad y la creación del Plan detallado de las pruebas de seguridad.
2. **Securización**: Se trata de la etapa de DevSecOps, incluida dentro de la fase de Codificar de DevOps, en donde se determinan las estrategias de seguridad y se establecen las medidas de protección para minimizar los riesgos detectados en la etapa de Análisis. Además, se marcan las directrices para establecer la seguridad al desarrollo deseado y se ejecutan las prácticas para el control del código en desarrollo, así como de sus librerías o funcionalidades, y de los cambios y la configuración.
3. **Verificación**: Se trata de la etapa de DevSecOps, incluida dentro de la fase de Verificar de DevOps, en donde se constatan y validan las medidas de protección tomadas en la etapa de Securización y se identifican las vulnerabilidades de código fuente mediante su análisis estático (SAST) y dinámico (DAST) y *pentesting* (pruebas de penetración) al artefacto resultante y sus componentes. De hecho, en esta etapa se ejecutan todas las pruebas para identificar los errores de codificación y construcción antes de la entrega.
4. **Defensa**: Se trata de la etapa de DevSecOps, incluida dentro de la fase de Monitorizar de DevOps, en donde se verifica activamente el comportamiento de la ejecución del entregable y se detectan sus comportamientos irregulares y los ataques que recibe. De hecho, en esta etapa se realizan los chequeos en tiempo de ejecución, mediante la automatización de controles y bucles de supervisión de seguridad.

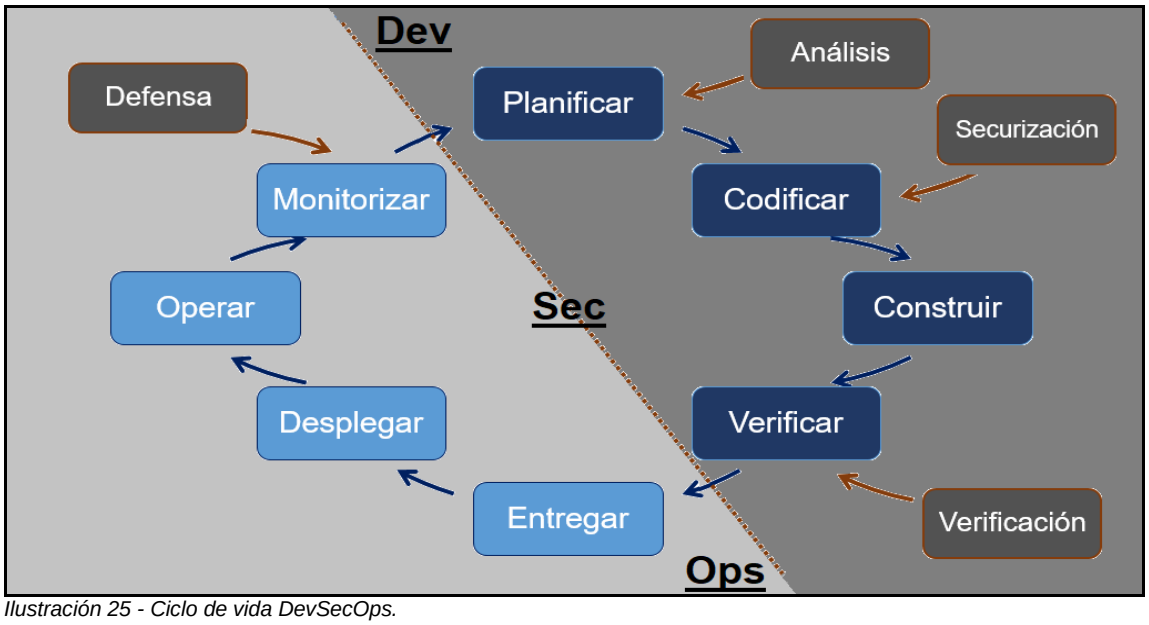

Ilustración 25 - Ciclo de vida DevSecOps.

7.2.8 Marco de Ciberseguridad del NIST

El Marco de Ciberseguridad (*Cybersecurity Framework*) del NIST se define como el conjunto de normas, directrices y requerimientos propuestos por el Instituto Nacional de Estándares y Tecnología para ayudar a definir las guías, los procedimientos, los procesos y las políticas relacionadas con la ciberseguridad en las organizaciones. Se encuentra en la versión 1.1 y, entre otras características, se constituye de prácticas efectivas, impulsa la comunicación entre intervinientes internos y externos, incorpora una gestión de riesgos que alinea la ciberseguridad con el negocio y se estructura en cinco procesos fundamentales que determinan una perspectiva completa del ciclo de vida de la gestión del riesgo en materia de ciberseguridad y del funcionamiento de un SOC:

1. **Identificación**: Proceso que proporciona un entendimiento de la organización para la gestión del riesgo de la información y sus activos en materia de ciberseguridad y comprende, entre otras las siguientes actividades:
    - Reconocimiento de procesos y activos críticos del negocio.
    - Aplicación de flujos de información documentada.
    - Gestión del inventario de los activos de información.
    - Creación de políticas, roles y responsabilidades para la ciberseguridad.
    - Detección de vulnerabilidades, amenazas y riesgos en los activos de información.
2. **Protección**: Proceso que desarrolla y pone en funcionamiento las salvaguardas adecuadas para asegurar la entrega de servicios y que, entre otras, incluye algunas de las siguientes actividades:
    - Administración del acceso a la información y sus activos.
    - Protección de la información sensible.
    - Realizar copias de seguridad con regularidad.
    - Protección de los dispositivos.
    - Gestión de las vulnerabilidades.
    - Formación al personal.

3. **Detección**: Proceso que desarrolla y pone en funcionamiento las tareas necesarias para reconocer y tratar los incidentes de ciberseguridad. Engloba, entre otras, algunas de las siguientes actividades:
    - Verificación y actualización de los procesos de detección.
    - Mantenimiento y monitorización de los registros de *logs*.
    - Conocimiento de los flujos de datos de la organización.
    - Comprensión de las consecuencias de los incidentes de ciberseguridad.
4. **Respuesta**: Proceso que desarrolla y pone en funcionamiento las tareas convenientes para actuar ante un incidente de ciberseguridad detectado. Además, abarca, entre otras, algunas de las siguientes actividades:
    - Comprobación de los planes de respuesta.
    - Actualización de los planes de respuesta.
    - Coordinación de los intervinientes internos y externos.
5. **Recuperación**: Proceso que desarrolla y pone en funcionamiento las tareas oportunas para preservar los planes de resiliencia y subsanar los servicios afectados por un incidente de ciberseguridad. Asimismo, incorpora, entre otras, algunas de las siguientes actividades:
    - Comunicación entre intervinientes internos y externos.
    - Actualización de los planes de recuperación.
    - Gestión de la reputación y las relaciones públicas de las organizaciones.

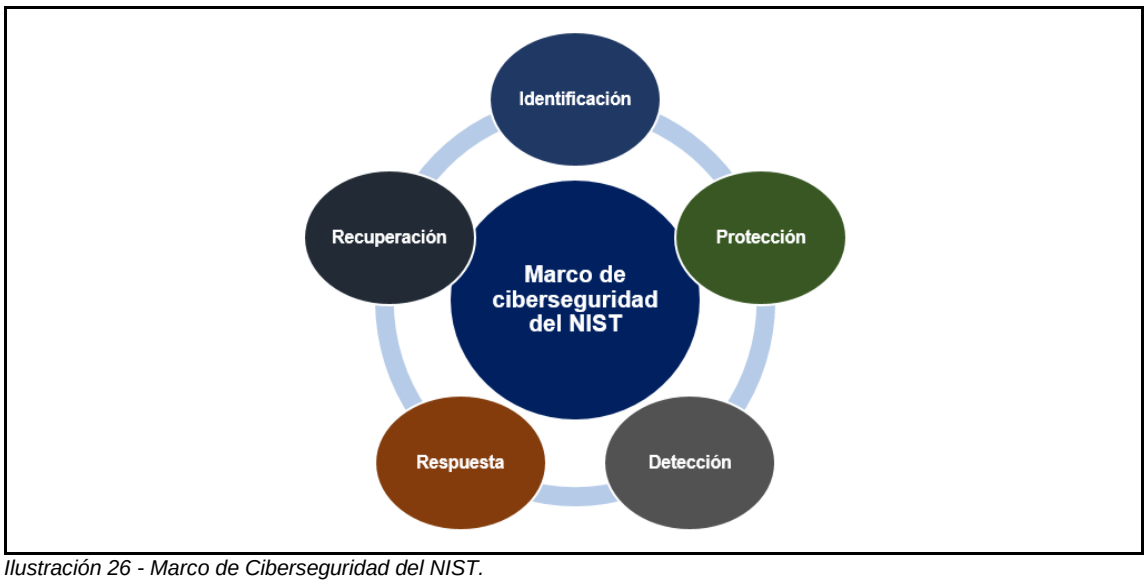

Ilustración 26 - Marco de Ciberseguridad del NIST.

7.2.9 Marco de MITRE ATT&CK

El marco de **MITRE ATT&CK** (MITRE *Adversarial Tactics, Techniques, and Common Knowledge*) se define como una base de datos o modelo de conocimiento y comportamiento de las fases del ciclo de vida de los diferentes ciberataques en las diversas plataformas conocidas. Se describe a partir de matrices que se clasifican por fases de ataque de principio a fin y, tal y como indica su propio nombre, se compone de tácticas, que contienen técnicas y se desarrollan con conocimiento común expresado en procedimientos (**TTP**[78]):

[78] https://www.afsinformatica.com/tacticas-tecnicas-y-procedimientos-ttp/

- **Táctica**: Se trata del método que se centra en el objetivo táctico o vector de ataque de un atacante para desarrollar su actividad y conseguir sus objetivos. Actualmente, existen las siguientes 14 tácticas:
  - Reconocimiento.
  - Desarrollo de recursos.
  - Acceso inicial.
  - Ejecución.
  - Persistencia.
  - Escalada de privilegios.
  - Evasión de defensa.
  - Acceso a Credenciales.
  - Descubrimiento.
  - Movimiento lateral.
  - Recopilación.
  - Comando y control.
  - Exfiltración.
  - Impacto.
- **Técnica**: Se trata de la acción o destreza que explica la manera con la que un atacante realiza una táctica para desarrollar su actividad y conseguir sus objetivos. Actualmente, el número de técnicas se corresponde con 224 y se engloban de la siguiente forma:
  - 10 técnicas para la táctica de Reconocimiento.
  - 7 técnicas para la táctica de Desarrollo de recursos.
  - 9 técnicas para la táctica de Acceso inicial.
  - 13 técnicas para la táctica de Ejecución.
  - 19 técnicas para la táctica de Persistencia.
  - 13 técnicas para la táctica de Escalada de privilegios.
  - 42 técnicas para la táctica de Evasión de defensa.
  - 17 técnicas para la táctica de Acceso a Credenciales.
  - 30 técnicas para la táctica de Descubrimiento.
  - 9 técnicas para la táctica de Movimiento lateral.
  - 17 técnicas para la táctica de Recopilación.
  - 16 técnicas para la táctica de Comando y control.
  - 9 técnicas para la táctica de Exfiltración.
  - 13 técnicas para la táctica de Impacto.
- **Procedimiento**: Se trata la documentación del conocimiento común de las acciones y pasos que realizan los ciberatacantes para ejecutar las técnicas con las que buscan desarrollar su actividad y conseguir sus objetivos.

Por tanto, este marco de trabajo puede mejorar la inteligencia en el funcionamiento de un SOC a partir de la identificación y clasificación de las anomalías e incidentes de seguridad detectados. Además, dado que se trata de una norma usada internacionalmente, facilita un lenguaje común con las diferentes organizaciones ante los atacantes comunes.

Ilustración 27 - Logo MITRE ATT&CK (https://attack.mitre.org/).

7.2.10 Estrategia Nacional de Ciberseguridad de ENISA

La **Estrategia Nacional de Ciberseguridad** (NCSS o *National Cybersecurity Strategies*, en inglés) de **ENISA** consiste en una guía de buenas prácticas, pasos y objetivos para orientar una estrategia común de ciberseguridad para los funcionarios públicos y su personal político de la Unión Europea y del área EFTA[79]. Además, facilita información de interés para los intervinientes en el ciclo de vida de esta estrategia común y las partes interesadas externas a través de 6 directrices para realizar su diseño y desarrollo y 15 objetivos para su implementación:

- Las **directrices** para su diseño y desarrollo se exponen a continuación:
    1. Determinar la perspectiva, alcance, prioridades y objetivos.
    2. Evaluar los riesgos.
    3. Analizar las regulaciones y las políticas.
    4. Implementar una estructura de dirección sólida.
    5. Reconocer e implicar a los intervinientes interesados.
    6. Determinar procedimientos y procesos de compartición de información.
- Los **propósitos** para su implementación se muestran a continuación:
    1. Desarrollo de planes de contingencia en materia de ciberseguridad.
    2. Protección de las infraestructuras críticas.
    3. Planificación de ejercicios de ciberseguridad.
    4. Establecimiento de medidas y controles de ciberseguridad.
    5. Establecimiento de herramientas y procedimientos de reporte de incidentes de seguridad.
    6. Concienciación a los usuarios.
    7. Uso de herramientas de educación y capacitación.
    8. Establecimiento de procesos de respuesta ante incidentes de seguridad.
    9. Tratamiento de ciberdelitos.
    10. Participación y cooperación internacional.
    11. Establecimiento de asociación de intervinientes.
    12. Fortalecimiento de la privacidad en la seguridad de la información.
    13. Cooperación entre instituciones públicas.
    14. Fortalecimiento del I+D+i.
    15. Facilitar ayudas para fomentar la inversión del sector privado en materia de ciberseguridad.

Ilustración 28 - Logo de ENISA (https://www.enisa.europa.eu/).

[79] https://es.wikipedia.org/wiki/Asociaci%C3%B3n_Europea_de_Libre_Comercio

7.2.11 MAGERIT

Tal y como su propio nombre indica, se trata de una **M**etodología de **a**nálisis y **ge**stión de **ri**esgos de las **t**ecnologías de información) que se define como el método o instrumento con el que analizar y gestionar los riesgos ocasionados por el uso y la implantación de Sistemas y Tecnologías de la Información, con el fin de eliminarlos o minimizarlos todo lo posible. Además, se compone de las siguientes diez fases:

1. **Toma de datos y procesos de información**: Se trata de la fase donde se define el alcance y la granularidad de lo que se desea analizar. Además, también es la fase donde se evalúan todos los procesos organizacionales, dado que sus posibles riesgos puedan afectar en los procesos críticos del negocio.
2. **Dimensionamiento y establecimiento de parámetros**: Se trata de la fase donde se determina el valor de los parámetros que se deben identificar y usar durante todo el proceso de aplicación de la metodología, que son el valor de los activos, las vulnerabilidades, el impacto y la efectividad del control de seguridad. Además, debido a su importancia, se deben utilizar en todo el proceso sin modificarse para evitar que el análisis de riesgos proporcione resultados equivocados.
3. **Análisis de activos**: Se trata de la fase donde se identifican y valoran todos los activos de la organización que se encuentren dentro del alcance del análisis de riesgos, es decir, los elementos necesarios físicos, lógicos, humanos e intangibles que se requieren para el desarrollo del negocio y que abarcan el alcance fijado. Asimismo, con el fin de poder hacer el análisis de activos correcto, se requiere que la organización proporcione unos rangos de valoración para cada activo en donde tenga en cuenta la reposición, la configuración o puesta a punto, el uso del activo y la pérdida de oportunidad, entre otros.
4. **Análisis de amenazas**: Se trata de la fase donde se estudian las posibles amenazas, que son las circunstancias que puedan desembocar en un problema para la organización. Además, aunque las amenazas se analizan individualmente, se clasifican en cuatro grupos para un mejor entendimiento sobre su afección a los activos: accidentes, errores, amenazas intencionales presenciales y amenazas intencionales remotas.
5. **Establecimiento de las vulnerabilidades**: Se trata de la fase donde se estudian y clasifican las vulnerabilidades de los activos que pueden permitir que una amenaza pueda ocasionar un problema en la organización.
6. **Valoración de impactos**: Se trata de la fase donde se evalúa el efecto que se produce cuando una amenaza aprovecha una vulnerabilidad y afecta a un activo de la organización. Se deben tener en cuenta el resultado de una amenaza, la consecuencia sobre los activos, el valor económico de las pérdidas, sean cuantitativas o cualitativas.
7. **Análisis de riesgos intrínsecos**: Se trata de la fase donde se valoran los riesgos actuales de la organización sin tener en cuenta ninguna medida de seguridad y se obtiene de la multiplicación del valor del activo por el valor de su vulnerabilidad y por el de su impacto; datos obtenidos en las fases anteriores.
8. **Influencia de las salvaguardas**: Se trata de la fase donde se selecciona la solución más adecuada para prevenir o reducir los riesgos y solventar sus consecuencias, ya sea de forma preventiva o correctiva.

9. **Análisis de riesgos efectivos**: Se trata de la fase donde se valoran los riesgos reales de la organización tras aplicar las medidas de seguridad; es decir, donde se estudia cómo las salvaguardas pueden minimizar significativamente los riesgos. Por ello, estos valores se obtienen de la multiplicación del valor del riesgo intrínseco por el porcentaje de disminución de la vulnerabilidad y por el porcentaje de disminución del impacto.
10. **Evaluación de riesgos**: Se trata de la última fase donde, finalmente, se deciden las medidas de seguridad para minimizar los riesgos intrínsecos, donde se toman las decisiones más adecuadas para su gestión (reducirlos, transferirlos o aceptarlos) y donde se establece el plan de acción con sus prioridades, estudio del coste sobre el beneficio, la elección de los controles, la atribución de las responsabilidades y la instauración de los controles elegidos.

7.2.12 Esquema Nacional de Seguridad (ENS)

El **ENS** se define como una normativa que tiene el objetivo principal de garantizar la seguridad en el uso de medios electrónicos para que sea correcta, apropiada y homóloga en todo el Estado español y para que los datos y servicios usados en todos los trámites efectuados con las Administraciones Públicas sean seguros, sea cual sea el organismo que los trate o que preste el servicio. Además, se constituye por requisitos y principios mínimos que aportan un lenguaje común entre entidades y se considera de obligado cumplimiento para, prácticamente, todo el sector público en España. De hecho, establece la política de seguridad para el resguardo de la información y los servicios gestionados mediante un programa común formado por 7 principios básicos, 15 requisitos mínimos, 73 medidas de seguridad estructuradas en 3 bloques planeados para el ámbito público y sus proveedores tecnológicos con los que puede facilitar la gestión de controles y el funcionamiento de un SOC:

- **Principios básicos**:
    1. Seguridad íntegra.
    2. Gestión de riesgos.
    3. Prevención, detección, defensa y recuperación.
    4. Planificación de la defensa.
    5. Monitorización continua.
    6. Revisión continua.
    7. Diferenciación de roles y responsabilidades.
- **Requisitos mínimos**:
    1. Gestión de procesos de seguridad.
    2. Estudio y tratamiento de los riesgos.
    3. Gestión de personal.
    4. Profesionalidad.
    5. Regulación y verificación de permisos de acceso.
    6. Salvaguarda del perímetro físico.
    7. Compra de productos.
    8. Seguridad por defecto.
    9. Actualización e integridad de los sistemas.
    10. Salvaguarda de la información en todos sus estados.
    11. Prevención y precaución con sistemas de información externos interconectados.
    12. Rastreo de actividad.
    13. Incidentes de seguridad.
    14. Continuidad del negocio y de la actividad.
    15. Mejora continua de los procesos de seguridad.

- **Medidas de seguridad**: se estructuran en 3 marcos:
    - **Marco Organizativo**: Marco que se constituye por medidas relacionadas con la organización global de la seguridad.
    - **Marco Operacional**: Marco que se constituye por medidas para proteger las operaciones de los sistemas globales.
    - **Medidas de protección**: Marco que se constituye por medidas para proteger los activos de información según su naturaleza y criticidad.

Asimismo, se regula en el Real Decreto 311/2022, de 3 de mayo, donde se cumple lo previsto en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y tras evolucionar desde su primer desarrollo con el Real Decreto 3/2010, de 8 de enero, su modificación con el Real Decreto 951/2015, de 23 de octubre, y su aprobación del Reglamento de actuación en el Real Decreto 203/2021, de 30 de marzo. Además, se originó gracias al trabajo coordinado, primero por el Ministerio de la Presidencia y, posteriormente, por el Ministerio de Política Territorial y Administración Pública (Real Decreto 1366/2010) y con el apoyo y la participación del Centro Criptológico Nacional (CCN) y de todas las administraciones públicas, incluidas las universidades públicas (CRUE). Por ello, entre su ámbito de aplicación, se destacan, entre otras, las entidades que se corresponden con:

- La Administración General del Estado.
- La Administración de la Comunidades Autónomas.
- Las entidades de la Administración Local.
- El sector público institucional.

Todo este trabajo, a su vez, se ha realizado a través de los órganos colegiados con competencias en materia de administración electrónica. De hecho, entre estos órganos, se encuentran el Consejo Superior de Administración Electrónica, el Comité Sectorial de Administración Electrónica y la Comisión Nacional de Administración Local, e incluye todos los informes preceptivos del Ministerio de Política Territorial, del Ministerio de la Presidencia, de la Agencia Española de Protección de Datos y del Consejo de Estado, donde también se tiene presente la opinión de las asociaciones de la Industria del sector TIC y su colaboración, tras la publicación de su borrador en la web del Consejo Superior de Administración Electrónica.

Ilustración 29 - Logo ENS (https://ens.ccn.cni.es/es/).

7.2.13 STIX y TAXII

STIX y TAXII son dos estándares creados para facilitar la prevención y defensa de los ciberataques:

- **STIX** (***S****tructured* ***T****hreat* ***I****nformation e****X****pression*): Se define como un lenguaje común estandarizado que se desarrolló por MITRE y el CTI de OASIS[80] para facilitar la recopilación, el intercambio, el análisis, el uso y la automatización de la información de las amenazas a la Seguridad de la Información y que se estructura para describir la ciberamenaza según los siguientes criterios:
  - Motivaciones.
  - Habilidades.
  - Capacidades.
  - Respuesta.
- **TAXII** (***T****rusted* ***A****utomated e****X****change of* ***I****ndicator* ***I****nformation*): Se define como un estándar que define los servicios y mensajes con los que se intercambia la información sobre las ciberamenazas y que admite el estándar STIX como fuente. Además, entre sus modelos principales se encuentran:
  - **Hub and Spoke**: Se trata de un almacén de información
  - **Fuente/suscriptor**: Se trata una fuente única para la entrada de información.
  - **Peer-to-peer**: Se trata de un conjunto de equipos que intercambian información.

  Asimismo, este estándar describe cuatro servicios:
  - Descubrimiento de los servicios admitidos.
  - Gestión de recopilación de la información.
  - Bandeja de entrada para recibir la información.
  - Encuesta para solicitar la información.

Por tanto, mientras STIX determina las características de la inteligencia contra amenazas, TAXII define la manera como se difunde esas características o información. Además, ambos se encuentran en su versión 2.1 y su objetivo común consiste en mejorar las medidas de seguridad con actividades como:

- Mejora del proceso de intercambio de inteligencia contra ciberamenazas.
- Mejora la respuesta proactiva ante una detección.
- Mejora la perspectiva global de la inteligencia contra ciberamenazas.

Ilustración 30 - Logos de STIX y TAXII (https://www.oasis-open.org).

[80] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

7.2.14 RFC

Los **RFC** (*Request for Comments*) se definen como un conjunto de estándares o documentos numerados y gestionados por IETF[81], que definen, explican y exponen comentarios de los diferentes conceptos, aspectos de funcionamiento, características, métodos y protocolos de Internet, entre otras propiedades de las redes de computadores y los sistemas interconectados. Por tanto, aunque no existe un RFC concreto para la descripción y funcionamiento de un SOC, existe el RFC 2350, que define un CSIRT y puede ser un buen punto de partida para un SOC y el RFC 3227, que recoge los criterios para el almacenamiento y recogida de evidencias ante incidentes de seguridad, entre otros.

7.2.14.1 RFC 2350

El **RFC 2350** se define como el estándar que describe las diferentes características para la respuesta ante incidentes de Seguridad de la Información, que puede aprovecharse para definir el SOC que se desea implementar y consta de 7 puntos específicos para su presentación:

1. Información del documento y su difusión.
2. Información del contacto.
3. Información de su constitución junto con su misión, alcance y autoridad.
4. Políticas junto con los tipos de incidentes y la comunicación, entre otros.
5. Servicios del equipo de respuesta.
6. Notificación de incidentes.
7. Descargo de responsabilidad.

7.2.14.2 RFC 3227

El **RFC 3227** se define como el estándar que describe los diferentes criterios para almacenar y recopilar la información en forma de evidencias encontradas en los eventos e incidentes de seguridad. Además, consta de 4 puntos importantes que contienen los diferentes procesos:

1. Principios de recolección de evidencias.
   1.1. Orden de volatilidad.
   1.2. Acciones a evitar.
   1.3. Observaciones sobre la privacidad.
2. Procedimiento de recolección.
   2.1. Transparencia.
   2.2. Diferentes pasos.
3. El procedimiento de almacenamiento.
   3.1. Cadena de custodia.
   3.2. Lugar y forma de almacenarlo.
4. Herramientas necesarias.

[81] https://es.wikipedia.org/wiki/Grupo_de_Trabajo_de_Ingenier%C3%ADa_de_Internet

7.2.15 Disposiciones legales para un SOC en el Estado español

Las principales leyes y normativas legales que regulan la gestión y el tratamiento de la información y de sus activos y, por extensión, la implementación, coordinación y funcionamiento de un equipo de ciberseguridad, como puede ser un SOC, se describen a continuación:

7.2.15.1 Ley de Seguridad Nacional

La "**Ley 36/2015, de 28 de septiembre, de Seguridad Nacional**"[82] se define como el instrumento legal español con el que se regulan los principios, componentes, órganos, autoridades, sistemas que gestionan las crisis y los recursos que contribuyan en la Seguridad Nacional. Además, se aplica, sobre todo, a organizaciones que trabajan en el ámbito gubernamental, ya que busca proteger los secretos de Estado de posibles amenazas como pueden ser los programas software destinados al espionaje (*spyware*).

7.2.15.2 Ley de Secretos Oficiales

La "**Ley 9/1968, de 5 de abril, sobre secretos oficiales**"[83] se define como el instrumento legal español con el que se regula la información sensible que no debe conocerse públicamente porque supondría un riesgo para la seguridad y conservación del estado español. Además, se aplica a todos los sectores empresariales y personales, ya que siempre se trata información confidencial.

7.2.15.3 Ley de Secretos Empresariales (LSE)

La "**Ley 1/2019, de 20 de febrero, de Secretos Empresariales (LSE)**"[84] se define como la norma legal española con el que se regula la protección contra la adquisición, el uso y la divulgación ilícita de la información técnica y empresarial considerada como secreta para una organización. Además, se aplica, entre otros, a las empresas privadas, por el uso de servidores que almacenan información y a los proveedores y personas, por el manejo de documentación e información, ya que se debe garantizar en todo momento su confidencialidad en base a las cláusulas firmados en los contratos acordes a su legalidad.

7.2.15.4 Leyes de Protección de Infraestructuras Críticas (LPIC)

La "**Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (LPIC)**"[85] se define como el instrumento legal español con el que se regula el establecimiento de las estrategias para identificar, designar y coordinar las actuaciones en materia de protección y mejorar su prevención, defensa y respuesta frente a amenazas e incidentes de seguridad que afecten a las infraestructuras de información crítica. Además, se aplica a todas las empresas, caracterizadas como críticas, que puedan sufrir un ciberataque a sus infraestructuras y sistemas de información, así como a todo proveedor o persona que conozca su información y características.

---

[82] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10389
[83] https://www.boe.es/buscar/act.php?id=BOE-A-1968-444
[84] https://www.boe.es/buscar/doc.php?id=BOE-A-2019-2364
[85] https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630

7.2.15.5 Leyes de Seguridad de las redes y sistemas de información

El "**Real Decreto Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información**"[86] y el "**Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información**"[87] se definen como el instrumento legal español con el que se regulan las acciones para asegurar la protección de las redes y sistemas de información en la Unión (NIS), así como su información clasificada, la gestión del orden público y la investigación, localización y seguimiento de delitos aplicados a los servicios esenciales que dependen de redes y sistemas de información, de zonas estratégicas y servicios digitales. Además, se deben generar políticas de seguridad que contemplen los riesgos, las medidas de seguridad y los planes de recuperación tanto internos como para proveedores de servicios.

7.2.15.6 Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE)

La "**Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSICE)**"[88] se define como el instrumento legal español con el que se regulan las obligaciones y el régimen sancionador de los prestadores de servicios y sus intermediarios relacionados con la gestión de la información, la contratación electrónica y sus condiciones y la difusión de contenido a través de redes de telecomunicaciones, entre otros. Por tanto, se aplica a los proveedores de servicios a distancia y prestadores de servicio, que brindan acceso a la información, lo que conlleva, a su vez, el deber de colaborar con las autoridades, en caso de investigación por incidente de seguridad o actividad delictiva.

7.2.15.7 Leyes de Telecomunicaciones

Por una parte, la "**Ley 11/2022, de 28 de junio, General de Telecomunicaciones**"[89] se define como el instrumento legal español con el que se regula la instalación, explotación, prestación de servicios, recursos, servicios asociados y terminales de telecomunicaciones, así como los dispositivos radioeléctricos. Por otra parte, la "**Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones**"[90] se define como el instrumento legal español con el que se regula la obligación de conservación de los datos gestionados en la prestación de servicios de las telecomunicaciones y de su entrega a los agentes facultativos, siempre que exista autorización judicial, para detectar, investigar y enjuiciar los delitos oportunos. Asimismo, estas leyes se aplican a cualquier entidad, con el fin de garantizar la protección de las redes y las telecomunicaciones y de colaborar con las autoridades, en caso de investigación por incidente de seguridad.

[86] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257
[87] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-1192
[88] https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758
[89] https://www.boe.es/buscar/doc.php?id=BOE-A-2022-10757
[90] https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243

7.2.15.8 Ley del Esquema Nacional de Seguridad (ENS)

El "**Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS)**"[91] se define como el instrumento legal español con el que se regula el propio ENS. Además, consta de principios básicos, requisitos mínimos y medidas de seguridad ordenadas en 3 bloques, para otorgar seguridad a la información tratada y a los servicios prestados. Además, se aplica, principalmente, a las organizaciones y administraciones públicas, por lo que los organismos deben cumplir esta normativa para garantizar la seguridad de la información. Asimismo, también se aplica a las empresas privadas y proveedoras de servicios, que suministran servicios a las administraciones públicas y que manejan información confidencial y sensible, como mecanismo para garantizar la seguridad de sus sistemas de información.

7.2.15.9 Ley de Firma electrónica

La "**Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza**"[92] se define como el instrumento legal español con el que se regula el tratamiento de la firma electrónica, su actividad jurídica, su valor de certificación y diferentes características de los servicios electrónicos de confianza, que se complementa con el Reglamento (UE) número 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. Además, se aplica a los prestadores de servicios electrónicos de confianza establecidos en España, ya sean públicos o privados.

7.2.15.10 Leyes de Protección de Datos Personales (RGPD y LOPDGDD)

Por una parte, el "**Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD)**"[93] se define como el instrumento legal europeo que regula el tratamiento y la gestión de los datos personales relacionados con personas en la Unión Europea (UE) por parte de las entidades, organizaciones y personas. Por otra parte, la "**Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)**"[94] se define como el instrumento legal español que regula el ordenamiento jurídico español para que se adapte a la RGPD europea, asegurar el derecho digital de las personas y completar sus disposiciones. Por tanto, ambos recursos legales se aplican a todos los intervinientes del tratamiento de datos personales, con el fin de determinar su responsabilidad y de garantizar los derechos de las personas físicas y su actividad, aunque, en el caso de proveedores de servicios, no se encuentren dentro de la Unión Europea.

---

91 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191
92 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-14046
93 https://www.boe.es/doue/2016/119/L00001-00088.pdf
94 https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

7.2.15.11 Ley de Propiedad Intelectual (TRLPI)

El "**Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia**"[95] se define como el instrumento legal español con el que se regula la protección del derecho de autor y derechos conexos en España. Además, se aplica a toda obra científica, artística o literaria que ya ha sido creada, por lo que se le atribuye a su autor la total disposición y exclusividad para su explotación.

[95] https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930

7.3 Anexo 3: Análisis del marco característico de un SOC

Con el fin de comprender el marco característico utilizado para la guía de implementación de un SOC y los dominios principales en los que se basa para su estructura y funcionamiento diario, a continuación, se resume el análisis y estudio de los procesos, de las tecnologías y del personal y sus roles, con el que se construyen los servicios mínimos que debe de prestar esta área de ciberseguridad para la protección y prevención de los activos de información de una organización y para la detección y respuesta ante sus incidentes y brechas de ciberseguridad.

7.3.1 Procesos de un SOC

De manera general, las organizaciones buscan instaurar procesos estandarizados para reducir e, incluso, eliminar la variación de los resultados obtenidos de las actividades realizadas, por lo que les permite entregar un producto o servicio con la misma calidad en todo momento y con mejoras incrementales. Debido a esto, con el fin de establecer esta estandarización, se debe realizar un documento formal que indique el análisis de la situación actual y de la tendencia hacia la que se dirigen los servicios, la organización de los intervinientes en sus actividades, el establecimiento de las tecnologías y herramientas necesarias, el despliegue de tareas junto a su periodicidad y la medición de los diferentes indicadores para establecer una mejora continua a los procesos estandarizados.

Asimismo, como el primero de los tres dominios principales definidos en los que se fundamenta un SOC, se enfoca en el detalle de los procedimientos y protocolos que se deben ejecutar para proteger, prevenir, detectar y reaccionar ante los incidentes de ciberseguridad. Por tanto, a continuación, se presentan los procesos mínimos que forman parte de sus actividades y tareas diarias:

Procesos mínimos	Descripción
Recolección de los registros *logs*	Se trata de la recopilación y centralización de los registros que generan las actividades que realizan las diferentes fuentes provenientes de las tecnologías de Seguridad de la Información de una organización.
Almacenamiento y custodia de los registros *logs*	Se trata de la salvaguarda y retención en el tiempo de los registros que generan las actividades que realizan las diferentes fuentes provenientes de las tecnologías de Seguridad de la Información de una organización.
Análisis de los registros *logs*	Se trata del estudio e interpretación de la información, que se obtiene de los registros *logs*, para obtener resultados ordenados, medidos y comprensibles que faciliten el entendimiento de los diferentes eventos e incidentes de ciberseguridad.
Monitorización de estados de los activos de información	Se trata de la verificación continua de los diferentes servicios implantados en una organización, así como de la notificación de alertas ante los sucesos negativos que les puedan ocurrir.

Integración de dispositivos fuente emisores de registros *logs*	Se trata de la incorporación de todas las tecnologías de Seguridad de la Información de la organización posibles en el envío de sus registros *logs* para su recolección, almacenamiento, custodia y análisis.
Monitorización de eventos de ciberseguridad	Se trata de la verificación continua de los diferentes sucesos no deseados en una organización, a través de los registros *logs* de las actividades que realizan las diferentes fuentes provenientes de las tecnologías de Seguridad de la Información de una organización.
Correlación de eventos de ciberseguridad	Se trata de la unificación de la sucesión de eventos de ciberseguridad relacionados entre sí que se han registrado a través de los diferentes registros logs obtenidos y almacenados.
Clasificación de eventos e incidentes de ciberseguridad	Se trata de la categorización de los eventos e incidentes de ciberseguridad que se detecten en una organización.
Triaje de eventos e incidentes de ciberseguridad	Se trata del diagnóstico inicial de los eventos e incidentes de ciberseguridad que se detecten en una organización.
Identificación de ciberamenazas e incidentes de ciberseguridad	Se trata del reconocimiento de amenazas de ciberseguridad que se detecten en la correlación de los registros *logs* de los activos de información de una organización.
Investigación de eventos e incidentes de ciberseguridad	Se trata del análisis y estudio en profundidad de los eventos e incidentes de ciberseguridad que se detecten en una organización, una vez se haya realizado el diagnóstico inicial y aún sigan activos.
Registro de los incidentes de ciberseguridad	Se trata de la anotación de los incidentes de ciberseguridad que se detecten en una organización y de todas sus consecuencias, actividades, vías de entrada y problemas causados.
Tratamiento y escalado de los incidentes de ciberseguridad	Se trata de la gestión y el escalado de los incidentes de ciberseguridad que se detecten en una organización.
Recogida de evidencias de las ciberamenazas	Se trata de la recopilación de las muestras e indicadores de compromiso (*IoC*) de las amenazas relacionadas con los incidentes de ciberseguridad.
Reacción ante ciberamenazas e incidentes de ciberseguridad	Se trata de la respuesta que se dé ante las amenazas e incidentes de ciberseguridad que se identifiquen entre los registros *logs* de los activos de información de una organización que se hayan correlacionado.
Notificación de los incidentes de ciberseguridad	Se trata de la comunicación de los incidentes de ciberseguridad que se detecten en una organización y de todas sus consecuencias, actividades, vías de entrada y problemas causados.

Seguimiento de los incidentes de ciberseguridad	Se trata del rastreo y persecución de las acciones y soluciones aplicadas a los incidentes de ciberseguridad que se detecten en una organización.
Análisis posterior a los incidentes de ciberseguridad	Se trata del análisis y estudio en profundidad de los incidentes de ciberseguridad que se detecten en una organización y de sus soluciones aplicadas, una vez se hayan resuelto, para realizar una mejora continua de sus procesos y tratamiento.
Desarrollo de flujos de trabajo ante eventos e incidentes de ciberseguridad	Se trata de la creación de reglas de correlación y de protocolos de reacción ante sucesos no deseados para detectar y responder ante eventos e incidentes de ciberseguridad.
Identificación de alertas de ciberseguridad y vulnerabilidades de activos	Se trata del reconocimiento y la validación de las alertas de ciberseguridad y vulnerabilidades de activos de información que se detecten en una organización y/o se notifiquen por entidades externas, como pueden ser las de los fabricantes de esos activos o las de los investigadores otros Equipos de ciberseguridad.
Validación de alertas de ciberseguridad y vulnerabilidades de activos	Se trata del análisis y estudio en profundidad de las alertas de ciberseguridad y vulnerabilidades de activos de información que se identifiquen tras su detección o notificación prematura.
Clasificación de alertas de ciberseguridad y vulnerabilidades de activos	Se trata de la categorización de las alertas de ciberseguridad y vulnerabilidades de activos de información que se identifiquen y validen por alguno de los Equipos de ciberseguridad de una organización.
Triaje de alertas de ciberseguridad y vulnerabilidades de activos	Se trata del diagnóstico inicial de las alertas de ciberseguridad y vulnerabilidades de activos de información que se identifiquen, validen y clasifiquen en las infraestructuras de una organización.
Registro de alertas de ciberseguridad y vulnerabilidades de activos	Se trata de la anotación de las alertas de ciberseguridad y vulnerabilidades de activos de información que se diagnostiquen y validen en las infraestructuras de una organización.
Tratamiento y escalado de alertas de ciberseguridad y vulnerabilidades de activos	Se trata de la gestión y el escalado de las alertas de ciberseguridad y vulnerabilidades de activos de información que se registren en las infraestructuras de una organización.
Notificación de alertas de ciberseguridad y vulnerabilidades de activos	Se trata de la comunicación de la información de las alertas de ciberseguridad y de las vulnerabilidades de activos de información que se traten y registren en una organización.

Reacción ante alertas de ciberseguridad y vulnerabilidades de activos	Se trata de la respuesta que se dé ante las alertas de ciberseguridad y vulnerabilidades de activos de información que se traten, registren y notifiquen en una organización.
Actualización de alertas de ciberseguridad y vulnerabilidades de activos	Se trata del refresco y renovación de la información de las alertas de ciberseguridad y de las vulnerabilidades de activos de información que se traten, registren y notifiquen en una organización.
Seguimiento de alertas de ciberseguridad y vulnerabilidades de activos	Se trata del rastreo y persecución de las acciones y soluciones aplicadas a las alertas de ciberseguridad y vulnerabilidades de activos de información que se traten, registren y notifiquen en una organización.
Vigilancia de filtraciones de información corporativa	Se trata del rastreo y detección del robo o publicación de la información confidencial, secreta o privada de una organización para usarse sin su autorización.
Vigilancia de exposición de metadatos de documentación corporativa	Se trata del rastreo y detección de la publicación de documentos corporativos con información confidencial, secreta o privada en sus metadatos, que pueden ser utilizados para obtener información corporativa.
Vigilancia de foros relacionados con la ciberseguridad.	Se trata del rastreo y detección de la publicación de información sobre brechas de seguridad y compromiso de la información de una organización en foros relacionados con la ciberseguridad.
Vigilancia de registros de dominios semejantes a los corporativos	Se trata del rastreo y detección de los registros de dominios que, por su parecido a los dominios propios de una organización, pueden ser usados para la suplantación de su identidad corporativa.
Recopilación de información sobre indicadores de ciberseguridad	Se trata de la recolección de la información que proviene de los indicadores de ciberseguridad de los diferentes activos de información de una organización para comprender su estado actual y poder emprender acciones de mejora.
Monitorización de los indicadores de ciberseguridad	Se trata de la verificación continua de los indicadores de ciberseguridad de los diferentes activos de información de una organización para detectar sus anomalías.
Reacción ante los indicadores de ciberseguridad no deseados	Se trata de la respuesta que se dé ante los indicadores de ciberseguridad de los diferentes activos de información de una organización que no se encuentren dentro de los parámetros deseados y acordados en los acuerdos de nivel de servicio (SLA).

Identificación y propuesta de nuevos indicadores de ciberseguridad	Se trata del reconocimiento, la validación y la propuesta de nuevos indicadores de ciberseguridad en una organización para monitorizar más datos de sus diferentes activos de información.
Desarrollo de cuadros de mando de ciberseguridad	Se trata de la creación y parametrización de cuadros de mando con información sobre los indicadores de ciberseguridad de los diferentes activos de información de una organización.
Comunicación de información de ciberseguridad	Se trata de la notificación y el comunicado de los diferentes informes ejecutivos, técnicos y funcionales relacionados con la ciberseguridad de una organización, sus ciberincidentes más críticos y el funcionamiento de los diferentes Equipos de Seguridad de la Información, como pueden ser el propio SOC.

Tabla 23 - Procesos mínimos de un SOC.

7.3.2 Tecnologías necesarias para un SOC

La tecnología, como el segundo de los tres dominios principales en los que se cimienta un SOC, se enfoca en los recursos y herramientas informáticas que utiliza su personal en su funcionamiento diario. Su integración y desarrollo cubren las necesidades básicas en materia de ciberseguridad en una organización y sus funcionalidades proporcionan las opciones principales para personalizar la protección de todos sus procesos de negocio. Sin embargo, para ello, requieren de una buena elección de los sistemas y sus herramientas con los que obtener la seguridad integral de todos sus activos de información, ya que existen múltiples soluciones tecnológicas y no todos tienen las capacidades necesarias para integrarse correctamente en cualquier entidad.

Asimismo, con el fin de obtener el máximo valor de los recursos tecnológicos de ciberseguridad integrados, las organizaciones deben coordinar sus esfuerzos de personal con sus responsabilidades y roles y alinear sus iniciativas estratégicas con sus funcionalidades, procesos y servicios. Además, deben proveer visibilidad de todas las alertas de eventos, incidentes, brechas y sucesos no deseados relacionados con la ciberseguridad y facilitar interoperabilidad[96] con el resto de sus activos. Por tanto, a continuación, se presentan las tecnologías más importantes para cubrir todos los procesos que realizan los servicios que prestan los SOC para la protección, prevención, detección y defensa de una organización:

7.3.2.1 Cortafuegos (Firewall)

Un **Cortafuegos** (o *firewall*, en inglés) se define como un sistema de seguridad de red, que puede ser hardware o software y que monitoriza y analiza el tráfico de paquetes de datos que circulan por él en el intercambio de información de pares de dispositivos que se sitúan en diferentes segmentos de red, en el que, al menos, uno de ellos se encuentra internamente en la organización. Se trata de la tecnología que funciona mediante la lectura y ejecución secuencial de reglas restrictivas que permiten o deniegan las peticiones de conexión de red de los diferentes elementos interconectados en la organización o interconectados con ella desde Internet u otras redes, con el fin de proporcionar redes internas controladas y seguras.

[96] https://tfig.itcilo.org/SP/contents/interoperability.htm

Asimismo, dada su evolución y en base a sus necesidades del momento, existen diferentes tipos de cortafuegos, entre los que se destacan los siguientes:

Tipos de cortafuegos	Descripción
Cortafuegos de filtrado de paquetes	Se trata del *firewall* que toma decisiones de procesamiento mediante una verificación simple de los paquetes de datos, sin inspeccionar su contenido, y con base en los protocolos, puertos y direcciones de red para permitir o denegar el tráfico. Por ello y dadas sus limitaciones, se trata de una solución poco segura para las amenazas de ciberseguridad de hoy en día.
Cortafuegos a nivel de circuito	Se trata del *firewall* que toma decisiones de procesamiento mediante la verificación de permisos de conexiones en la capa de transporte de los modelos de referencia de Internet (OSI[97]), que se compara con la tabla de conexiones que, previamente, define los circuitos permitidos. Por tanto, dado que verifica que la sesión sea legítima, pero no inspecciona los paquetes, se trata de una solución poco segura para las amenazas de ciberseguridad de hoy en día.
Cortafuegos de inspección con estado	Se trata del *firewall* que toma decisiones de procesamiento mediante la combinación de la verificación de permisos de conexiones en la capa de transporte del modelo OSI y la inspección de paquetes, por lo que permite el seguimiento del estado de la conexión. Sin embargo, aunque se trata de una solución segura, consume demasiados recursos y ralentiza demasiado el tráfico de red y la transferencia de paquetes.
Cortafuegos proxy	Se trata del *firewall* que toma decisiones de procesamiento mediante la conexión con el origen del tráfico, en la capa de aplicación del modelo OSI, para inspeccionar el paquete de datos entrante y permitir o denegar los accesos a partir de las definiciones de la aplicación. Se trata de una solución bastante segura, ya que crea una nueva capa de protección entre el origen y el destino, pero puede ralentizar mucho el tráfico de red y la transferencia de paquetes.
Cortafuegos de próxima generación (NGFW)	Se trata del *firewall* que toma decisiones de procesamiento mediante la inspección del contenido real y completo del paquete de datos, la inspección a nivel de superficie y la comprobación de la sesión del protocolo de enlace TCP. Además, también incluye otras tecnologías, como puede ser un sistema de prevención de intrusiones (IPS[98]), por lo que se considera de las soluciones más actuales y completas ante las ciberamenazas de la actualidad.

[97] https://es.wikipedia.org/wiki/Modelo_OSI
[98] Ver el punto 7.3.2.3 del Anexo 3 para más información sobre IPS.

Cortafuegos de software	Se trata del *firewall* que se instala en un dispositivo en local y toma decisiones de procesamiento en base a las necesidades de protección en profundidad de los puntos finales ubicados en diferentes segmentos de red. Se trata de una solución costosa de mantener por su gestión aislada en los puntos finales y que no siempre favorece la interoperabilidad entre los diferentes activos de una organización.
Cortafuegos de hardware	Se trata del *firewall* que se integra en la red organizativa como un dispositivo más y toma decisiones de procesamiento de la misma manera que un enrutador de tráfico de red para interponerse en los paquetes de datos y las solicitudes de tráfico enviadas entre dos puntos finales o activos de una organización.
Cortafuegos en la nube	Se trata del *firewall* que se sitúa en la nube y toma decisiones de procesamiento al igual que un firewall de tipo proxy, dado que su funcionamiento suele ser idéntico. Igualmente, dada su naturaleza, se integran con facilidad en las organizaciones, aunque delegan todo el tráfico de red perimetral fuera de sus sistemas.

Tabla 24 - Tipos de firewalls.

En la actualidad, los cortafuegos más utilizados por las grandes organizaciones son los cortafuegos de próxima generación. Además, en el mercado existen grandes empresas que se dedican a la fabricación de estos cortafuegos y lideran su venta de productos, por lo que, a continuación, se presentan algunos de los mejores para que las organizaciones los valoren y decidan sobre su integración e interoperabilidad:

Fabricante	Modelos de ejemplo
Fortinet[99]	• FortiGate Series.
Palo Alto Networks[100]	• PA-7000 Series. • PA-5400 Series. • PA-5200 Series.
Check Point[101]	• Quantum Lightspeed Series.
Cisco[102]	• Firepower Series. • Meraki series MX.
Forcepoint[103]	• 3400 Series. • 2200 Series. • 1100 Series.
Sophos[104]	• XG Series. • XGS Series.

Tabla 25 - Ejemplos de modelos firewalls.

99 https://www.fortinet.com/lat/products/next-generation-firewall
100 https://www.paloaltonetworks.es/network-security/next-generation-firewall-hardware
101 https://resources.checkpoint.com/next-generation-firewall/quantum-security-appliance-brochure
102 https://www.cisco.com/c/es_es/products/security/firewalls/index.html
103 https://www.forcepoint.com/es/appliance/forcepoint-ngfw-appliances
104 https://www.sophos.com/es-es/products/next-gen-firewall/tech-specs#Overview

7.3.2.2 Sistemas de detección de intrusos (IDS)

Un **Sistema de detección de intrusos** (**IDS** o *Intrusion Detection System*, en inglés) se define como la herramienta de detección y notificación de accesos no autorizados y sucesos anómalos no deseados de una organización, que se basa en la monitorización y análisis de los eventos que ocurren en su red y los compara con una serie de reglas establecidas, que indican si se ha detectado una amenaza de seguridad, con el fin de enviar una notificación de alerta de ciberseguridad. Por tanto, tal y como se aprecia, este sistema sólo alerta de las posibles amenazas que detecten sin realizar ninguna acción para solucionarla o mitigarla.

Asimismo, los IDS pueden ser de tipo hardware, que se instalan entre las comunicaciones de red de las organizaciones, o tipo software, que se incluyen como módulos o sensores en otras soluciones de seguridad, como pueden ser los cortafuegos NGFW o antivirus. Además, en base a su arquitectura de red, estos sistemas pueden ser de diferentes tipos:

Tipos de IDS	Descripción
IDS basado en equipos (HIDS)	Se trata del IDS que monitoriza el tráfico de red entrante y saliente de un punto final, como puede ser un equipo (*Host IDS*, en inglés) y notifica las alertas que detecte al respecto.
IDS basado en redes (NIDS)	Se trata del IDS que monitoriza todo el tráfico entrante y saliente de un segmento de red (*Network IDS*, en inglés) y notifica las alertas que detecte al respecto.
IDS basado en firmas (SBIDS)	Se trata del IDS que monitoriza todo el tráfico entrante y saliente de un segmento de red y lo compara con un conjunto de firmas predefinidas (*Signature-based IDS*, en inglés) y notifica las alertas que detecte al respecto.
IDS basado en anomalías (ABIDS)	Se trata del IDS que monitoriza todo el tráfico entrante y saliente de un segmento de red y lo compara con una línea base predefinida para detectar conductas extrañas (*Anomaly-based IDS*, en inglés) y notifica las alertas que detecte al respecto.

Tabla 26 - Tipos de IDS.

Por otra parte, en el mercado existen diferentes modelos de IDS, por lo que, para su valoración y decisión de integración e interoperabilidad en la organización que lo requiera, a continuación, se presentan algunos de los más utilizados:

Fabricante	Modelos de ejemplo
SolarWinds[105]	• SolarWinds Security Event Manager.
Snort[106]	• Snort 3.
Suricata[107]	• Suricata IDS.

[105] https://www.solarwinds.com/security-event-manager/use-cases/intrusion-detection-software?CMP=BIZ-RVW-SWTH-SEM
[106] https://www.snort.org/
[107] https://suricata.io/

Trend Micro[108]	• Trend Micro DDI.
Wazuh[109]	• Wazuh.
OSSEC[110]	• OSSEC.

Tabla 27 - Ejemplos de modelos de IDS.

7.3.2.3 Sistemas de prevención de intrusos (IPS)

Un **Sistema de prevención de intrusos** (**IPS** o *Intrusion Prevention System*, inglés) se define como la herramienta de detección, prevención, protección y notificación de accesos no autorizados y sucesos anómalos no deseados de una organización, que se basa en la monitorización y análisis de los eventos que ocurren en su red y los compara con una serie de reglas establecidas, que indican si se ha detectado una amenaza de seguridad, para bloquearlos y enviar una notificación de la alerta de ciberseguridad y su acción realizada para resolverla. Por tanto, tal y como se aprecia, a diferencia de los IDS, este sistema alerta de las posibles amenazas que se detecten y realiza una acción para solucionarla o mitigarla.

Asimismo, los IPS pueden ser de tipo hardware, que se suelen instalar tras los cortafuegos para bloquear todo tráfico no legítimo entrante y saliente de la red de las organizaciones, o tipo software, que se incluyen como módulos o sensores en otras soluciones de seguridad, como pueden ser los propios cortafuegos NGFW o los antivirus. Además, estos sistemas se consideran como una prolongación de los IDS, pero realizan un tipo de control del tráfico de red diferente y se asemejan más a los cortafuegos, ya que monitorizan el tráfico de red y lo permiten o lo bloquean.

Por otra parte, en base a su arquitectura de red, estos sistemas pueden ser de diferentes tipos:

Tipos de IPS	Descripción
IPS basado en equipos (HIPS)	Se trata del IPS que monitoriza el tráfico de red entrante y saliente de un punto final, como puede ser un equipo (*Host IPS*, en inglés), reacciona ante los sucesos no deseados y notifica las alertas que detecte y las acciones realizadas para su remediación.
IPS basado en redes LAN (NIPS)	Se trata del IPS que monitoriza todo el tráfico entrante y saliente de un segmento de red LAN (*Network IPS*, en inglés), reacciona ante los sucesos no deseados y notifica las alertas que detecte y las acciones realizadas para su remediación.
IPS basado en redes wireless (WIPS)	Se trata del IPS que monitoriza todo el tráfico entrante y saliente de una red inalámbrica (*Wireless IPS*, en inglés), reacciona ante los sucesos no deseados y notifica las alertas que detecte y las acciones realizadas para su remediación.

[108] https://www.trendmicro.com/es_es/business/products/network/advanced-threat-protection/inspector.html
[109] https://wazuh.com/
[110] https://www.ossec.net/

IPS basado en análisis de comportamiento (NBA)	Se trata del IPS que monitoriza todo el tráfico entrante y saliente de un segmento de red y lo compara con una línea base predefinida para detectar anomalías o conductas extrañas (*Network Behaviour Analysis*, en inglés), reacciona ante los sucesos no deseados y notifica las alertas que detecte y las acciones realizadas para su remediación.
IPS de próxima generación (NGIPS)	Se trata del IPS que, además de realizar las propias labores de detección, prevención, protección y notificación de las amenazas localizadas en la red de una organización, ofrece inteligencia avanzada en su funcionamiento y proporciona mayor visibilidad.

Tabla 28 - Tipos de IPS.

De la misma forma que las demás tecnologías, en el mercado existen diferentes modelos de IPS, por lo que, para su valoración y decisión de integración e interoperabilidad en una organización, a continuación, se muestran algunos de los más usados:

Fabricante	Modelos de ejemplo
Palo Alto Networks[111]	• Módulo IPS en sus NGFW.
Fortinet[112]	• Módulo IPS en sus Fortigate Series.
McAfee[113]	• McAfee Network Security Platform.
Trend Micro[114]	• Trend Micro TippingPoint (NGIPS).
Cisco[115]	• Cisco Firepower (NGIPS).

Tabla 29 - Ejemplos de modelos de IPS.

7.3.2.4 Sistemas de gestión de información y eventos de seguridad (SIEM)

Un **Sistema de gestión de información y eventos de seguridad** (**SIEM** o *Security Information and Event Management*, en inglés) se define como un sistema de detección y protección de las ciberamenazas en tiempo real que afecten a una organización, mediante la correlación, centralización e interpretación de los datos relativos a la ciberseguridad y la reacción y respuesta a los eventos obtenidos de diferentes fuentes de datos sobre una misma amenaza, con el fin de notificar sus acciones y análisis completo en una única alerta de seguridad. Por tanto, proporciona la visibilidad y la detección de los patrones y sucesos anómalos de una ciberamenaza desde un único panel centralizado y facilita una respuesta ágil, rápida y concreta para esa detección y su reacción y respuesta.

111 https://www.paloaltonetworks.es/network-security/next-generation-firewall-hardware
112 https://www.fortinet.com/lat/products/next-generation-firewall
113 https://www.mcafee.com/enterprise/es-es/assets/data-sheets/ds-virtual-network-security-platform.pdf
114 https://www.trendmicro.com/es_es/business/products/network/intrusion-prevention/tipping-point-threat-protection-system.html
115 https://www.cisco.com/c/en/us/products/security/ngips/index.html

Asimismo, se trata de la herramienta central del ecosistema tecnológico de la ciberseguridad de una organización y del funcionamiento de todo SOC, ya que proporciona la recopilación, agregación y análisis de múltiples datos en tiempo real, agiliza sus flujos de trabajo y favorece sus capacidades operativas sobre gestión de incidentes y generación de informes, entre otros. Además, los SIEM son el resultado de la conjunción de dos tecnologías diferentes que se complementan:

- **Sistema de gestión de eventos de seguridad** (**SEM** o *Security Event Management*, en inglés): Sistema que correlaciona, centraliza, procesa y monitoriza los eventos de seguridad en tiempo real para notificar las alertas de amenazas de ciberseguridad.
- **Sistema de gestión de información de seguridad** (**SIM** o *Security Information Management*, en inglés): Sistema que almacena los registros *logs* recibidos y los eventos de seguridad correlacionados para mantener un histórico, permitir el análisis forense de los eventos e incidentes de ciberseguridad y generar conocimiento sobre los ciberataques.

Por otra parte, en el mercado existen diferentes herramientas o modelos SIEM con el que mejorar las capacidades de los procesos de negocio de una organización en materia de ciberseguridad y la agilidad de reacción de los SOC ante las ciberamenazas detectadas, por lo que, para su valoración y decisión de integración e interoperabilidad en una organización, a continuación, se muestran algunos de los más usados a nivel empresarial:

Fabricante	Modelos de ejemplo
Fortinet[116]	• FortiSIEM.
IBM[117]	• IBM Security QRadar.
McAfee[118]	• McAfee Enterprise Security Manager.
LogRhythm[119]	• LogRhythm SIEM.
Splunk[120]	• Splunk Enterprise Security.
Alien Vault[121]	• Alien Vault OSSIM.

Tabla 30 - Ejemplos de modelos SIEM.

116 https://www.fortinet.com/lat/products/siem/fortisiem
117 https://www.ibm.com/products/qradar-siem
118 https://www.mcafee.com/enterprise/es-mx/assets/data-sheets/ds-enterprise-security-manager.pdf
119 https://logrhythm.com/products/logrhythm-siem/
120 https://www.splunk.com/en_us/products/enterprise-security.html?301=/en_us/cyber-security/siem.html
121 https://cybersecurity.att.com/products/ossim

7.3.2.5 Sistemas de orquestación, automatización y respuesta de seguridad (SOAR)

Un **Sistema de orquestación, automatización y respuesta de seguridad** (**SOAR** o *Security Orchestration Automation and Response*, en inglés) se define como un sistema de ciberseguridad que, en base a la definición de métricas y flujos de trabajo y la información obtenida de múltiples fuentes, realiza labores y toma decisiones para la gestión de ciberamenazas y de vulnerabilidades, la reacción y respuesta ante incidentes de ciberseguridad y la automatización de las operaciones de detección, prevención y protección de los activos de información de una organización. Tal y como indica su propio nombre, esta herramienta dispone de tres capacidades que, en conjunto, mejoran tanto la reactividad como la proactividad de la ciberseguridad de una organización:

- **Orquestación de la ciberseguridad**: Capacidad para integrar y correlacionar diferentes herramientas de seguridad y automatizar sus procesos para mejorar la eficiencia de las operaciones de ciberseguridad de una organización.
- **Automatización de la ciberseguridad**: Capacidad para disminuir la interacción participación humana en las labores de detección, priorización y remediación de amenazas de ciberseguridad de una organización.
- **Respuesta de ciberseguridad**: Capacidad para gestionar, planificar, controlar y notificar las reacciones ante amenazas e incidentes de ciberseguridad de una organización.

Asimismo, los sistemas SOAR proporcionan una rápida y mejor comprensión del contexto de las amenazas e incidentes de ciberseguridad y facilita a los SOC las herramientas para realizar una mejora continua de los procedimientos y flujos de trabajo de la Seguridad de la Información en las organizaciones. Además, proporcionan múltiples beneficios, entre los que se destacan:

- **Mejora de los tiempos de respuesta**: Reacciona de manera instantánea gracias a la automatización.
- **Minimiza el impacto de las ciberamenazas**: Detecta con mayor agilidad y responde instantáneamente.
- **Mejora de la inteligencia de ciberamenazas**: Incorpora y correlaciona la información de diferentes fuentes para actualizar su inteligencia.
- **Aumenta la perspectiva de ciberseguridad**: Facilita a los equipos de ciberseguridad, como los SOC, comprensión del alcance y la naturaleza de las ciberamenazas más allá de sólo su definición.
- **Optimiza sus operaciones**: Facilita la automatización de la correlación de los datos, del manejo de las ciberamenazas y de las respuestas a los ciberincidentes.
- **Perfecciona el rendimiento y la productividad**: Facilita la clasificación y priorización de las tareas y la agilidad de las respuestas a más incidentes de ciberseguridad en tiempos más reducidos.
- **Minimiza los costes**: Agiliza y simplifica el tratamiento de las ciberamenazas de manera automatizada, por lo que reduce los costes de reacción por impactos y recursos de personal.

Por otra parte, en el mercado existen diferentes modelos de SOAR que pueden facilitar las operaciones de seguridad de los SOC y demás equipos de ciberseguridad de las organizaciones, por lo que, a continuación, se presentan algunos de los más publicitados a nivel empresarial, con el fin de que se pueda valorar de cara a su integración e interoperabilidad:

Fabricante	Modelos de ejemplo
Palo Alto Networks[122]	• Cortex XSOAR.
IBM[123]	• IBM Security QRadar SOAR.
Rapid7[124]	• Rapid7 Insightconnect.
Fortinet[125]	• FortiSOAR.
Splunk[126]	• Splunk Security Orchestration, Automation and Response (SOAR).

Tabla 31 - Ejemplos de modelos SOAR.

7.3.2.6 Herramientas de protección de puntos finales (EEP)

Una **Herramienta de protección de puntos finales** (**EPP** o *Endpoint Protection*, en inglés) se define como un software de ciberseguridad que detecta, protege y elimina software malicioso en puntos finales en tiempo real, como pueden ser equipos de usuario o servidores, entre otros. Se trata de una solución que proporciona detección de ciberamenazas y protección y desinfección de malware en los equipos finales, en base a una serie de firmas precargadas (uso de listas negras[127]) en los activos finales de información de una organización y a sus comportamientos anómalos. Además, se puede considerar como la evolución de los antivirus y los *antimalwares* clásicos, ya que permiten realizar las siguientes acciones:

- Incluir módulos de ciberseguridad, como los HIPS o reputación de accesos web.
- Salvaguardar la información personal de los usuarios y servicios.
- Realizar análisis de software en base a listas negras.
- Analizar el comportamiento sospechoso de las ejecuciones en los sistemas.
- Reportar información sobre los análisis realizados y recomendar acciones de prevención y protección.

Por otra parte, en el mercado existen diferentes soluciones para la protección de los puntos finales, por lo que, a continuación, se presentan algunos de los más utilizados a nivel empresarial para su valoración por parte de las organizaciones:

122 https://www.paloaltonetworks.es/cortex/cortex-xsoar
123 https://www.ibm.com/es-es/products/qradar-soar
124 https://www.rapid7.com/products/insightconnect/
125 https://www.fortinet.com/lat/products/fortisoar
126 https://www.splunk.com/en_us/products/splunk-security-orchestration-and-automation.html
127 https://es.wikipedia.org/wiki/Lista_negra_(inform%C3%A1tica)

Fabricante	Modelos de ejemplo
Trend Micro[128]	• Trend Micro Apex One.
Kaspersky[129]	• Endpoint Security for Business.
G Data[130]	• Endpoint Security Solution.
Avast[131]	• Avast Business.
ESET[132]	• ESET Endpoint Security.
Bitdefender[133]	• Bitdefender Endpoint Security.
Check Point[134]	• Check Point Endpoint Security.

Tabla 32 - Ejemplos de modelos EPP.

7.3.2.7 Herramientas de detección y respuesta

Una **Herramienta de detección y respuesta** (*Detection and Response*, en inglés) se define como un software de ciberseguridad que monitoriza, recopila los registros sobre las acciones realizadas en los activos de información para conocer su funcionamiento y detectar y responder ante los sucesos anómalos y las amenazas e incidentes de ciberseguridad en tiempo real. Se trata de una solución que proporciona el aprendizaje del funcionamiento normal de un sistema para detectar comportamientos anómalos (uso de listas blancas[135]), como pueden ser la ejecución de un proceso no conocido o de una ciberamenaza, y protegerlo ante todo suceso no conocido.

Asimismo, en base a su destino y funcionalidad, estos sistemas pueden ser de diferentes tipos:

Tipos de Sistemas de detección y respuesta	Descripción
Sistema de detección y respuesta en puntos finales	Se trata del Sistema software de detección y respuesta que se encarga de proteger los dispositivos de puntos finales de ciberamenazas y comportamientos anómalos (EDR o *Endpoint Detection and Response*, en inglés).
Sistema de detección y respuesta en segmentos de red	Se trata del Sistema software de detección y respuesta que se encarga de proteger los segmentos de red de ciberamenazas y comportamientos anómalos (NDR o *Network Detection and Response*, en inglés).

128 https://www.trendmicro.com/es_es/business/products/user-protection/sps/endpoint.html
129 https://www.kaspersky.es/small-to-medium-business-security/endpoint-select
130 https://www.gdatasoftware.com/business/endpoint-security
131 https://www.avast.com/es-es/business#pc
132 https://www.eset.com/es/empresas/proteccion-de-endpoints/
133 https://www.bitdefender.com/business/solutions/endpoint-security.html
134 https://www.checkpoint.com/es/solutions/endpoint-security/
135 https://esgeeks.com/que-es-lista-blanca/

Sistema de detección y respuesta extendida	Se trata del Sistema software de detección y respuesta que se encarga de proteger toda la infraestructura de una organización de ciberamenazas y comportamientos anómalos (XDR o *eXtended Detection and Response*, en inglés).
Sistema de detección y respuesta gestionada	Se trata del Sistema de detección y respuesta que se administra como servicio por un proveedor externo experimentado, gracias a la ayuda de cualquiera de los sistemas software de detección y respuesta nombrados anteriormente (EDR, NDR y/o XDR), para proteger la parte de la organización contratada en los acuerdos de nivel de servicio (SLA) de ciberamenazas y comportamientos anómalos (MDR o *Manage Detection and Response*, en inglés).

Tabla 33 - Tipos de Sistemas de detección y respuesta.

Por otra parte, en el mercado existen diferentes soluciones de detección y respuesta, por lo que, a continuación, se indican algunos de los más nombrados a nivel empresarial para su posible valoración por parte de las organizaciones:

Fabricante	Modelos de ejemplo
Trend Micro[136]	• Trend Micro Vision One (XDR).
Cynet[137]	• Cynet 360 AutoXDR.
WatchGuard[138]	• WatchGuard EDR.
Palo Alto Networks[139]	• Cortex XDR Prevent. • Cortex XDR Pro (posibilidad de MDR).
Fortinet[140]	• FortiEDR.

Tabla 34 - Ejemplos de Sistemas de detección y respuesta.

7.3.2.8 Cortafuegos de Aplicaciones web (WAF)

Un **Cortafuegos de aplicaciones web** (**WAF** o *Web Application Firewall*, en inglés) se define como un sistema de seguridad, software o hardware, que protege a los servidores de aplicaciones web de los ataques de ciberseguridad, a través del análisis y la inspección de los paquetes de las peticiones HTTP y HTTPS y de los diferentes modelos de tráfico web. Se trata de una solución a nivel de aplicación del modelo OSI, que revisa el cumplimiento de todas las reglas predefinidas sobre el permiso o denegación de tráfico de todas las peticiones que se envían a los servidores de aplicaciones, antes de que les lleguen. Además, suelen tener las siguientes capacidades:

- Reconocimiento de firmas de ataque.
- Análisis de patrones para el tráfico web.

136 https://www.trendmicro.com/es_es/business/products/detection-response.html
137 https://www.cynet.com/platform/
138 https://www.watchguard.com/es/wgrd-products/watchguard-endpoint-edr
139 https://www.paloaltonetworks.com/cortex/cortex-xdr
140 https://www.fortinet.com/lat/products/endpoint-security/fortiedr

- Inteligencia artificial y aprendizaje automático.
- Creación de diferentes perfiles de actuación.
- Motor de reglas personalizables.
- Motor de correlación
- Protección contra los DDoS[141].
- Red de entrega de contenido (CDN[142]).

Asimismo, los WAF se pueden implementar de diferentes maneras en la infraestructura web de una organización. Entre estos tipos, se destacan:

Tipos de implementación de WAF	Descripción
Puente transparente (*Transparent bridge*)	Las peticiones web se envían directamente al servidor de aplicaciones web a través del WAF.
Proxy inverso transparente (*Transparent reverse proxy*)	Las peticiones web se envían al WAF, que, sin modificar nada de la petición, como puede ser el enmascaramiento de la IP, la reenvía al servidor de aplicaciones web.
Proxy inverso (*Reverse proxy*)	Las peticiones web se envían al WAF, que filtra la petición con, por ejemplo, el enmascaramiento de la IP, y la reenvía al servidor de aplicaciones web modificada.

Tabla 35 - Tipos de implementación de WAF.

Por otra parte, a continuación, se presentan algunos de los cortafuegos de aplicaciones web más competitivos para su evaluación por parte de las organizaciones:

Fabricante	Modelos de ejemplo
Fortinet[143]	• Fortiweb.
Imperva[144]	• Imperva SecureSphere.
Barracuda[145]	• Barracuda Networks WAF.
Monitorapp[146]	• Monitorapp AIWAF.
F5[147]	• Advanced Web Application Firewall

Tabla 36 - Ejemplos de WAF.

141 Ver el punto 7.1.3.3 del Anexo 1 para más información sobre DDoS y los Ciberataques más comunes.
142 https://es.wikipedia.org/wiki/Red_de_distribuci%C3%B3n_de_contenidos
143 https://www.fortinet.com/lat/products/web-application-firewall/fortiweb
144 https://www.imperva.com/products/web-application-firewall-waf/
145 https://www.barracuda.com/products/webapplicationfirewall
146 https://www.monitorapp.com/waf/
147 https://www.f5.com/es_es/products/security/advanced-waf

7.3.2.9 Sistemas de protección del correo electrónico

Un **Sistema de protección del correo electrónico** se define como un sistema de ciberseguridad que protege las cuentas y comunicaciones de correo electrónico de las ciberamenazas por intrusión, pérdida, fraude y accesos no legítimos a los buzones de correo de una organización. Se basa en la protección, prevención, detección y respuesta ante amenazas e incidentes de ciberseguridad relacionados con el correo no deseado, el engaño o suplantación de remitentes, el *phishing* y la infección por malware de los buzones de correo electrónico y los dispositivos en los que se utiliza el propio servicio.

Asimismo, las herramientas de ciberseguridad del correo electrónico de una organización proporcionan protección en todos sus vectores de ataque de forma centralizada, por lo que, además del uso de cifrados y firma digital, de protocolos como SPF[148], DKIM[149] y DMARC[150] y antimalware, se consideran una muy buena solución para proteger a la organización, tanto a nivel de reputación como de sistemas y personal. Igualmente, existen diferentes soluciones de protección del correo electrónico que engloban una protección holística del correo electrónico, por lo que, a continuación, se indican algunos de los más utilizados a nivel empresarial para su posible valoración por parte de las organizaciones:

Fabricante	Modelos de ejemplo
Trend Micro[151]	• InterScan Messaging Security (IMS). • Deep Discovery Email Inspector (DDEI).
Sophos[152]	• Sophos Email.
Barracuda[153]	• Barracuda Email Protection.
Cisco[154]	• Cisco Email Security Appliance (ESA).
Fortinet[155]	• FortiMail.

Tabla 37 - Ejemplos de Sistemas de protección del correo electrónico.

7.3.2.10 Herramientas de inventario de activos de información

Una **Herramienta de inventario de activos de información** se define como una herramienta de ciberseguridad que proporciona control, catalogación, administración, tratamiento, análisis y reporte de los datos y la información de la que se componen los activos de información de una organización. De hecho, estos sistemas se consideran esenciales, dado que tratan una gran cantidad de información con la que determinar una toma de decisiones ante sucesos no deseados en estos activos. Además, tal y como se indica en la norma ISO/IEC 27001, se considera fundamental disponer de una herramienta en la organización que inventaríe los activos de información. De esta manera, los SOC siempre podrán entender la gravedad de las amenazas e incidentes de ciberseguridad.

148 https://www.mdirector.com/blog/que-es-el-spf/
149 https://www.dmarcanalyzer.com/es/dkim-3/
150 https://www.dmarcanalyzer.com/es/dmarc-3/
151 https://www.trendmicro.com/es_es/business/products/user-protection/sps/email-and-collaboration.html
152 https://www.sophos.com/en-us/products/sophos-email
153 https://www.barracuda.com/products/email-protection
154 https://www.cisco.com/c/m/es_es/products/security/email-security/setup-guide.html
155 https://www.fortinet.com/lat/products/email-security

Por otra parte, algunos de las herramientas de inventario de activos de información pueden ser:

Fabricante	Modelos de ejemplo
Atlassian[156]	• JIRA Service Management.
GLPI[157]	• GLPI.
OTRS[158]	• OTRS.
OCS[159]	• OCS Inventory.
InvGate[160]	• InvGate Assets.

Tabla 38 - Ejemplos de Sistemas de inventario de activos.

7.3.2.11 Herramientas de gestión de ticketing

Una **Herramienta de gestión de ticketing** se define como un sistema o herramienta que permite el histórico y seguimiento de los incidentes de ciberseguridad, las solicitudes y reclamaciones de los usuarios y clientes y las actividades y tareas realizadas por los diferentes equipos de ciberseguridad, como puede ser un SOC, de manera organizada y detallada. Se trata de la herramienta en donde se anotan todos los detalles y las acciones realizadas ante cualquier ciberamenaza o solicitud.

Además, entre los sistemas de seguimiento de *tickets*, algunos de las herramientas más famosas, al igual que para el inventario de activos de información, se pueden encontrar, entre otras, las siguientes:

Fabricante	Modelos de ejemplo
Atlassian[161]	• JIRA Service Management.
GLPI[162]	• GLPI.
OTRS[163]	• OTRS.
BMC Software[164]	• BMC Remedy ITSM.

Tabla 39 - Ejemplos de Sistemas de inventario de activos.

156 https://www.atlassian.com/software/jira/service-management
157 https://glpi-project.org/es/
158 https://otrs.com/es/home/
159 https://ocsinventory-ng.org/?lang=en
160 https://invgate.com/assets/
161 https://www.atlassian.com/software/jira/service-management
162 https://glpi-project.org/es/
163 https://otrs.com/es/home/
164 https://www.bmcsoftware.es/it-solutions/remedy-itsm.html

7.3.2.12 Sistemas de gestión de vulnerabilidades

Un **Sistema de gestión de vulnerabilidades** se define como la herramienta de ciberseguridad que se responsabiliza de reconocer, valorar, tratar y notificar las debilidades de seguridad de los sistemas de información de una organización, con el fin de prevenir las posibles ciberamenazas y minimizar su posible impacto. Se trata de uno de los sistemas más importantes para la gestión de riesgos de una organización y, entre otras actividades, analiza el motivo por el que se produce esa debilidad, utiliza repositorios estandarizados a nivel mundial para su análisis y la clasifica para su gestión, así como también favorece la ejecución de auditorías automatizadas en los activos de información de una organización.

Además, en el mercado se pueden encontrar múltiples herramientas de análisis de vulnerabilidades, por lo que, a continuación, se presentan las más conocidas para su valoración de cara a su posible implementación:

Fabricante	Modelos de ejemplo
Tenable[165]	• Nessus.
Qualys[166]	• Qualys VMDR.
GFI[167]	• GFI LanGuard.
Greenbone[168]	• OpenVas.
CIR[169]	• Nikto2.
Beyond Trust[170]	• Retina CS. • Retina Network Security Scanner.

Tabla 40 - Ejemplos de Sistemas de gestión de vulnerabilidades.

7.3.2.13 Herramientas de monitorización de disponibilidad

Una **Herramienta de monitorización de disponibilidad** se define como un sistema o herramienta que vigila y verifica el estado de los activos de información y sus servicios y avisa y notifica de cualquier suceso o cambio de estado que les ocurra. Se trata de las herramientas que monitorizan el tráfico de red de una organización, mediante chequeos automatizados de amenazas precargados, y que informan de la pérdida de disponibilidad total o parcial de un proceso o servicio que ofrece una organización prácticamente en tiempo real, por lo que permite una rápida reacción ante este tipo de sucesos.

Asimismo, se destacan las siguientes herramientas de monitorización de la disponibilidad para su valoración por parte de las organizaciones:

165 https://es-la.tenable.com/products/nessus?tns_redirect=true
166 https://www.qualys.com/apps/vulnerability-management-detection-response/
167 https://www.gfi.com/products-and-solutions/network-security-solutions/languard
168 https://www.openvas.org/
169 https://cirt.net/Nikto2
170 https://www.beyondtrust.com/vulnerability-management

Fabricante	Modelos de ejemplo
Nagios[171]	• Nagios.
Pandora FMS[172]	• Pandora FMS.
Solucions IM[173]	• ITRS OP5 Monitor.
Paessler[174]	• Paessler PRTG.

Tabla 41 - Ejemplos de Sistemas de monitorización de disponibilidad.

7.3.2.14 Otras tecnologías de interés para un SOC

Además de los sistemas y herramientas indicados anteriormente, la evolución de la ciberseguridad en las organizaciones y la madurez de los SOC, demandan otras tecnologías de interés que, con su gestión, incrementan los principios de protección, prevención, detección y respuesta de este ámbito, como pueden ser, entre otras, las siguientes:

Otras tecnologías	Descripción
Herramientas de auditorías e integridad de archivos	Se definen como las herramientas software de ciberseguridad que comprueban la integridad de los archivos de los diferentes equipos informáticos, mediante algoritmos criptográficos para la obtención de un HASH (o *checksum*) para cada uno de ellos.
Sistemas VPN (Red privada virtual)	Se definen como los sistemas que cifran el tráfico de red de una conexión para enmascarar su identidad en línea y establecer la protección necesaria que dificulte el seguimiento de sus acciones.
Herramientas *sandbox*	Se definen como entorno de pruebas aislado para ejecutar ficheros o programas potencialmente maliciosos sin afectar a los recursos propios de la organización ni generar incidentes de ciberseguridad y poder analizarlos, estudiarlos y obtener su información.
Herramientas de proxy web	Se definen como las herramientas que se registran las conexiones web realizadas a la infraestructura de una organización, analizan y filtran los paquetes de sus peticiones web y redirigen el tráfico que se considere libre de amenazas hacia los servicios de aplicaciones finales de manera automatizada.
Herramientas de inteligencia de amenazas	Se definen como las herramientas de ciberseguridad que proporcionan información sobre las ciberamenazas que pueden surgir en los activos de información de una organización, mediante la obtención, identificación, centralización y rastreo de los indicadores de compromiso (*IoC*) de las posibles amenazas de ciberseguridad que se detectan en la red interna y que se publican y comparten por agentes externos en sus organizaciones.

171 https://www.nagios.org/
172 https://pandorafms.com/es/
173 https://www.solucions-im.com/es/op5-monitor
174 https://www.paessler.com/es/prtg

Herramientas de análisis forense	Se definen como las herramientas de ciberseguridad que identifican, recuperan y estudian los datos de los activos de información de una organización para obtener algún tipo de información desconocida, dañada, perdida o que haya podido haber constituido algún tipo de delito, con el fin de proporcionar información y evidencias de esos activos.
Sistemas de copias y respaldo de seguridad	Se definen como los sistemas que almacenan la información de los activos de información de una organización de manera periódica para tener un respaldo que restaurar en caso de pérdida de información.
Sistemas trampa o de señuelo	Se definen como los sistemas que simulan ser un servicio vulnerable para registrar los intentos de intrusión que reciban, con el fin de obtener información sobre los ataques y adquirir inteligencia sobre las ciberamenazas.
Sistemas PKI	Se definen como los sistemas de infraestructura de clave pública que permiten la creación, gestión, distribución, uso, almacenaje y revocación de certificados digitales y cifrado de clave pública, mediante la conjunción de roles, procedimientos y políticas.
Sistemas HSM	Se definen como los sistemas que almacenan, custodian y protegen las claves privadas de los certificados digitales y el cifrado de la clave pública, mediante criptografía.
Herramientas MDM	Se definen como las herramientas de ciberseguridad de dispositivos móviles que protege sus datos, los de sus aplicaciones, almacenamiento en la nube, movimiento de redes corporativas y repositorios de almacenamiento.
Herramientas de inteligencia de fuentes abiertas (OSINT)	Se definen como las herramientas de inteligencia de datos con las que obtener información útil a partir de la recolección, procesamiento, análisis y toma de decisiones de los datos obtenidos de diferentes fuentes públicas.

Tabla 42 - Más tecnologías de interés para un SOC.

7.3.2.15 Herramientas más recomendadas

Asimismo, una vez instalados los sistemas de ciberseguridad, entre los que se destaca el SIEM, entre las herramientas más recomendadas para todo SOC, tal y como se observa en la web de CSIRT KIT[175] (s.f.), se pueden localizar las siguientes:

Herramientas recomendadas	Descripción
MISP[176]	Herramienta software de inteligencia de amenazas que facilita el intercambio y la centralización de información de amenazas y de indicadores de compromiso.

[175] https://csirt-kit.org/#services
[176] https://www.misp-project.org/

IntelMQ[177]	Herramienta software de manejo de incidentes de seguridad mediante la recopilación y el procesamiento de fuentes de seguridad abiertas y registros de *logs* obtenidos a partir del protocolo de cola de mensajes.
The Hive[178]	Herramienta software de respuesta a incidentes de ciberseguridad que centraliza las alertas provenientes de diferentes fuentes.
Cortex[179]	Herramienta software de consulta y análisis de muestras para la respuesta ante incidentes de ciberseguridad.
Nfsen[180]	Herramienta software de análisis forense de la red que permite ejecución de comandos y facilita descripciones gráficas de los flujos de red de la organización.
Elastic[181]	Herramienta software de inteligencia operativa para localizar, verificar, visualizar y analizar los datos de los activos de información a través de la recepción de sus registros *logs*.
Wazuh[182]	Herramienta software de monitorización de ciberseguridad para detectar amenazas, verificar continuamente la integridad de los sistemas, reaccionar ante los ciberincidentes y verificar el cumplimiento.
Packetbeat[183]	Herramienta software de análisis de paquetes de datos de red que se integra con servidores Elastic.
Graylog[184]	Herramienta software de gestión de registros que facilita la combinación, correlación, centralización y visualización de información útil sobre ciberseguridad, las aplicaciones, los activos y la infraestructura de una organización.
N8N[185]	Herramienta software de automatización de flujos de trabajo que moviliza y transforma los datos de las bases de datos y de las aplicaciones.

Tabla 43 - Herramientas recomendadas para un SOC (CSIRT-KIT).

7.3.3 Personal y roles de un SOC

Las personas, como el tercero de los tres dominios principales en los que se establece un SOC, se enfoca en el talento humano que debe ejecutar los procesos del SOC mediante el uso de sus tecnologías, así como de definir sus competencias, conocimiento y experiencia requerida. Además, en base al tamaño y las necesidades de cada organización, los roles y las responsabilidades del personal requeridas para un SOC se ven modificadas y varían. No obstante, resulta necesario disponer de un área, equipo o departamento de ciberseguridad efectivo y balanceado para su correcto funcionamiento.

177 https://github.com/certtools/intelmq
178 https://thehive-project.org/
179 https://thehive-project.org/
180 https://nfsen.sourceforge.net/
181 https://www.elastic.co/es/
182 https://wazuh.com/
183 https://www.elastic.co/es/beats/packetbeat
184 https://www.graylog.org/
185 https://n8n.io/

Asimismo, toda organización debe entender que un SOC debe ser un servicio o equipo independiente del resto de áreas de la organización, con el fin de separarse y aislarse de los aspectos más funcionales de los servicios para centrarse plenamente en su protección y seguridad. Igualmente, la relación con el resto de equipos y departamentos de su organización se considera necesaria y fundamental para el cumplimiento de sus funciones, ya que, entre otras se encuentra la de supervisar y monitorizar la actividad de estas otras áreas en materia de ciberseguridad. Por tanto, a continuación, se propone la siguiente relación de roles que, de forma genérica, se consideran imprescindibles dentro de todo SOC en una organización:

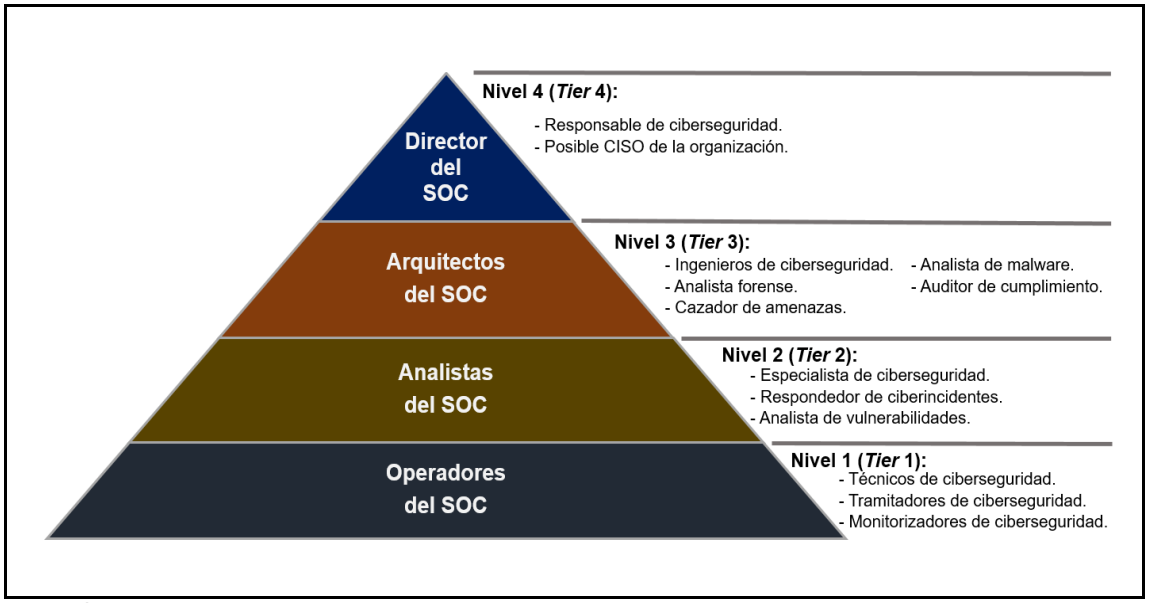

Ilustración 31 - Roles del personal del SOC.

7.3.3.1 Nivel 1: Operadores del SOC

Los operadores del SOC componen el rol técnico inicial y más básico de la ciberseguridad en una organización. Se trata de personal técnico del SOC que se responsabiliza de registrar los eventos e incidentes de ciberseguridad en *tickets*, de tramitar, clasificar y realizar el triaje de las amenazas y vulnerabilidades de ciberseguridad detectadas y de monitorizar los activos de información de la organización. Además, se encargan de la gestión de las tecnologías suministradas para el uso de sus funciones y de la remediación ágil y rápida de los incidentes de ciberseguridad que cuenten con un procedimiento definido, verificado y aprobado.

Las organizaciones, por lo general, procesan un volumen de datos muy elevado, por lo que los operadores del SOC se encargan de realizar una distribución balanceada de las actividades destinadas para su rol, como son la verificación continua, el escrutinio y el procesado de la información de la organización. Por tanto, entre los conocimientos y las habilidades que debe tener un técnico de ciberseguridad asignado al Nivel 1 del SOC (*Tier* 1) se pueden encontrar los siguientes:

Conocimientos y habilidades (*skills*) del nivel 1	
Conocimientos para administrar sistemas operativos.	Conocimientos de diferentes lenguajes de programación.
Conocimientos para administrar redes de comunicaciones.	Conocimientos de diferentes herramientas de análisis y *debugger*.
Conocimientos de ciberseguridad.	Capacidad analítica e inquietud para la investigación.
Capacidad de comprensión, capacitación y aprendizaje.	Comprensión y conocimiento del negocio y de su relación con la ciberseguridad.
Capacidad de trabajo bajo presión.	Capacidad de trabajo en equipo.

Tabla 44 - Habilidades y conocimientos de los operadores del SOC.

Asimismo, entre las funciones y responsabilidades que debe asumir este rol, se pueden encontrar las siguientes:

Competencias y funciones del nivel 1	
Gestión de la primera atención de los incidentes de ciberseguridad.	Notificación de las vulnerabilidades de los activos tecnológicos de información asociadas a un CVE[186].
Monitorización y remediación de las alertas de ciberseguridad asociadas a procedimientos aprobados.	Análisis básico y primera respuesta ante los eventos y los incidentes de ciberseguridad.
Diseño, desarrollo e implementación de las alertas de monitorización de ciberseguridad.	Control y seguimiento de los incidentes de ciberseguridad tramitados.
Triaje, catalogación y priorización de los eventos, alertas e incidentes de seguridad informática.	Gestión de procesos de inteligencia ante amenazas de ciberseguridad asociadas a procedimientos escritos.
Registro de *tickets* de los eventos e incidentes de seguridad.	Desarrollo y aplicación de medidas de primera respuesta de ciberseguridad.
Gestión, mantenimiento y uso de las herramientas de ciberseguridad.	Revisión y seguimiento continuo de los riesgos de ciberseguridad.

Tabla 45 - Funciones y competencias de los operadores del SOC.

7.3.3.2 Nivel 2: Analistas del SOC

Los analistas del SOC componen el rol técnico avanzado y especialista de la ciberseguridad en una organización. Se trata del personal con capacidades para el tratamiento, gestión y resolución de las incidencias más complejas de ciberseguridad y con conocimientos para la verificación de las vulnerabilidades y la ejecución de pruebas de penetración en los activos tecnológicos de información de la organización. Además, se encargan de la gestión de todos aquellas tareas, eventos, alertas e incidentes de ciberseguridad que no cuentan con un procedimiento asociado y no se solucionan desde el Nivel 1 del SOC. Por tanto, entre los conocimientos y las habilidades que debe tener un especialista de ciberseguridad asignado al Nivel 2 del SOC (*Tier* 2) se pueden encontrar los siguientes:

[186] Ver el punto 7.1.2.3.2 del Anexo 1 para más información sobre Repositorios de información de vulnerabilidades y definición de CVE.

Conocimientos y habilidades (*skills*) del nivel 2	
Constancia y proactividad.	Capacidad de mejora continua.
Iniciativa e implicación.	Conocimientos expertos en ciberseguridad.
Experiencia para administrar activos tecnológicos de información.	Experiencia en la ejecución de pruebas de penetración en los activos tecnológicos de información.
Experiencia en la explotación de vulnerabilidades de activos tecnológicos de información.	Comprensión y conocimiento del negocio y de su relación con la ciberseguridad.
Capacidad analítica e inquietud para la investigación.	Capacidad de trabajo en equipo.
Capacidad de trabajo bajo presión.	Capacidad de comprensión, capacitación y aprendizaje.
Capacidad y experiencia en la correlación de eventos.	Capacidades comunicativas y de síntesis de información.

Tabla 46 - Habilidades y conocimientos de los Analistas del SOC.

Asimismo, entre las funciones y responsabilidades que debe asumir este rol, se pueden encontrar las siguientes:

Competencias y funciones del nivel 2	
Gestión de la atención y respuesta avanzada de las alertas y los incidentes de ciberseguridad.	Gestión de la detección y respuesta de las vulnerabilidades en los activos tecnológicos de información.
Análisis de los eventos e incidentes complejos de ciberseguridad.	Apoyo y formación a los técnicos del nivel 1 del SOC.
Supervisión y aprobación del diseño, desarrollo e implementación de las alertas de monitorización.	Supervisión y seguimiento de los eventos e incidentes de ciberseguridad complejos.
Planificación, preparación y ejecución periódica de los escaneos de vulnerabilidades de los activos tecnológicos de información.	Planificación, preparación y ejecución periódica de pruebas de penetración en los activos tecnológicos de información.
Gestión de los procesos de inteligencia ante amenazas de ciberseguridad.	Generar documentación y automatizar las actividades diarias comunes.
Desarrollo de informes periódicos de los escaneos de vulnerabilidades y pruebas de penetración realizadas.	Planificación, preparación y desarrollo de actividades y medidas para disminuir los riesgos de ciberseguridad.

Tabla 47 - Funciones y competencias de los Analistas del SOC.

7.3.3.3 Nivel 3: Arquitectos del SOC

Los arquitectos del SOC componen los roles de ingeniería y arquitectura de la ciberseguridad en una organización. Se trata del personal con capacidades para la documentación de los procedimientos, necesidades y requisitos para el correcto y la mejora continua del servicio que presta el SOC, así como del cumplimiento normativo y de los protocolos, del uso adecuado y correcto de los activos tecnológicos de ciberseguridad y del diseño y la implementación de las medidas y controles de ciberseguridad de la organización y del propio SOC. Además, se encargan de colaborar con los desarrolladores y proveedores de Seguridad de la Información de la organización para la protección de sus activos de información y la consecución de productos seguros que se adaptan a sus normativas y políticas de negocio.

Asimismo, este grupo de ingenieros de ciberseguridad se encarga y asume las tareas, eventos, alertas, vulnerabilidades e incidentes de ciberseguridad que no se solucionan desde el Nivel 2 del SOC. Por tanto, entre los conocimientos y las habilidades que debe tener un arquitecto de ciberseguridad asignado al Nivel 3 del SOC (*Tier* 3) se pueden encontrar los siguientes:

Conocimientos y habilidades (*skills*) del nivel 3	
Liderazgo e iniciativa.	Minuciosidad en la realización de actividades y tareas.
Arquetipo y constancia.	Capacidad de mejora continua.
Proactividad e implicación.	Conocimiento experto en ingeniería y arquitectura de ciberseguridad.
Conocimiento en ingeniería de los activos tecnológicos de información.	Conocimiento en ingeniería, ciencia y arquitectura de software.
Capacidad analítica, seriedad e inquietud para la investigación avanzada.	Comprensión y conocimiento del negocio y de su relación con la ciberseguridad.
Capacidad para gestionar con efectividad el tiempo y los recursos.	Capacidad para gestionar equipos con efectividad.
Capacidad de trabajo en equipo y bajo presión.	Capacidad de comprensión, capacitación y aprendizaje.
Capacidad y experiencia para la resolución de problemas de ciberseguridad.	Capacidades comunicativas, de síntesis de información y de enseñanza.

Tabla 48 - Habilidades y conocimientos de los Arquitectos del SOC.

Por otra parte, entre las funciones y responsabilidades que debe asumir este rol, se pueden encontrar las siguientes:

Competencias y funciones del nivel 3	
Gestión de la atención y respuesta experta de las alertas y los incidentes de ciberseguridad.	Monitorización y tratamiento de los indicadores de ciberseguridad.
Gestión de la vigilancia y exposición de filtraciones de información corporativa.	Análisis de los eventos e incidentes complejos de ciberseguridad sin resolución.

Gestión de la caza e inteligencia de amenazas a la ciberseguridad.	Gestión del análisis de malware y el análisis forense de los incidentes de ciberseguridad.
Diseño, desarrollo e implementación de respuesta ante las alertas y problemas de ciberseguridad sin resolución.	Apoyo y formación a los analistas del nivel 2 del SOC.
Enlace y conexión de comunicación entre el Director (posible CISO) y el resto del SOC.	Generación de estadísticas e informes de los ANS y de las funciones diarias del SOC para el reporte al Director (posible CISO).
Creación y diseño de los requisitos de ciberseguridad indicados Director del SOC (posible CISO) y los procesos de negocio de la organización.	Documentar y capacitar al resto del equipo sobre los procesos y las tecnologías usadas para los servicios que presta el SOC.
Soporte y asistencia en materia de ciberseguridad a la dirección y responsables técnicos de la organización.	Documentar y poner en funcionamiento los Planes diseñados por el Director del SOC (posible CISO).
Soporte al Director (posible CISO) en todo lo relacionado con el funcionamiento diario del SOC.	Auditar y supervisar el cumplimiento de la ciberseguridad en todas las áreas de organización (tanto internas como externas y de proveedores).

Tabla 49 - Funciones y competencias de los Arquitectos del SOC.

7.3.3.4 Nivel 4: Director del SOC

El director del SOC constituye la máxima responsabilidad jerárquica de la ciberseguridad en una organización. Si no se trata del propio CISO[187], responsable de Seguridad de la Información, se encuentra jerárquicamente justo por debajo y le justifica sus labores y decisiones. Por ello, bajo sus criterios se establecen los procesos de negocio relacionadas con la ciberseguridad de los activos tecnológicos de información, así como los planes directores, las políticas, las estrategias y las actividades relacionadas con el ámbito de la ciberseguridad de la organización.

Asimismo, se encarga de dirigir, coordinar y alinear el equipo de trabajo del SOC y de sus niveles jerárquicos, por lo que se considera el enlace entre todas las partes del área de ciberseguridad, en donde entra el SOC, y la alta dirección de la organización. Debido a esto, en el caso de ser el propio CISO, tiene que dar respuestas al CEO[188]; en caso de no serlo, debe dar respuestas al CISO. Por tanto, entre los conocimientos y las habilidades que debe tener un Director de ciberseguridad asignado al Nivel 4 del SOC (*Tier* 4) se pueden encontrar los siguientes:

Conocimientos y habilidades (*skills*) del nivel 4	
Dotes de mando y liderazgo.	Experiencia en ciberseguridad.
Experiencia en la gestión de equipos.	Arquetipo y seriedad.
Templanza e iniciativa.	Proactividad e implicación.

187 https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad
188 https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad

Capacidad comunicativa, de comprensión, capacitación y aprendizaje.	Comprensión y conocimiento del negocio y de su relación con la ciberseguridad.
Capacidad de manipulación e inteligencia emocional.	Conocimientos técnicos y de análisis, ingeniería y arquitectura de ciberseguridad.

Tabla 50 - Habilidades y conocimientos del Director del SOC.

Por otra parte, entre las funciones y responsabilidades que debe asumir este rol, se pueden encontrar las siguientes:

Competencias y funciones del nivel 4	
Creación, verificación y actualización continua del programa de ciberseguridad.	Supervisión y fiscalización de las funciones y actividades del SOC.
Creación y seguimiento de las estrategias de ciberseguridad.	Diseño y capacitación de las estrategias de ciberseguridad al equipo del SOC.
Fomento la criticidad e importancia de la ciberseguridad.	Realización de entrevistas y contratos del personal del SOC y la ciberseguridad.
Alineación de los objetivos de negocio con la ciberseguridad.	Creación y dirección del Plan de respuesta ante vulnerabilidades e incidentes y brechas de ciberseguridad.
Planificación y control del cumplimiento de las certificaciones de ciberseguridad de la organización y su personal.	Creación y dirección del Plan de gestión de notificaciones ágiles y tempranas.
Creación y dirección del Plan de gestión de notificaciones de vigilancia de filtraciones y fugas de información.	Creación y dirección del Plan de supervisión de los indicadores de seguridad.
Creación, dirección y gestión del Plan de Continuidad del Negocio.	Creación y dirección del Plan de ciberseguridad.
Creación y dirección del Plan de Comunicación del SOC y la ciberseguridad.	Crear los procedimientos y diseñar las alertas de seguridad.
Gestión y control del presupuesto destinado a la ciberseguridad.	Desarrollo y visualización de los flujos de trabajo del SOC.
Generación informes de ciberseguridad para la alta dirección y el CISO, en caso de no serlo.	Generación informes de control y auditoría de indicadores de ciberseguridad.

Tabla 51 - Funciones y competencias del Director del SOC.

7.3.3.5 Estimación económica del personal del SOC

Debido a que la implementación de un SOC puede considerarse un proyecto genérico y depende de múltiples factores, como el tamaño y las necesidades tecnológicas de hardware (cortafuegos, SIEM, IPS…) y de software (protección de puntos finales, de detección y respuesta, gestores de *ticketing*…) y de personal de la organización (sueldos, formación, certificaciones…), no se puede indicar una valoración económica específica. Sin embargo, se puede intentar crear una estimación de la valoración económica que puede requerir la contratación y el mantenimiento del personal del SOC, que, además, puede valer para comprender y planificar el número de trabajadores que se requieren para su implementación.

Asimismo, aunque los costes en salario de personal pueden variar en dependencia del emplazamiento en el que se encuentre la organización y en base a los cambios de demanda del mercado, en las diferentes ofertas de trabajo localizadas en diferentes portales de búsqueda de empleo entre los años 2020 y 2022 (tras la pandemia por la COVID-19), las organizaciones estiman, de media, la siguiente valoración económica para cada miembro del personal del SOC:

Tipo de trabajador en un SOC (Nivel en el SOC)	Salario unitario mínimo orientativo en España
Operador del SOC (Nivel 1)	≈ 30 000 €/año.
Analista del SOC (Nivel 2)	≈ 38 000 €/año.
Arquitecto del SOC (Nivel 3)	≈ 45 000 €/año.
Director del SOC (posible CISO) (Nivel 4)	≈ 60 000 €/año.

Tabla 52 - Valoración económica anual estimada del personal de un SOC.

Además, aunque se pueden realizar múltiples interpretaciones, no hay una respuesta genérica exacta y la asignación de roles depende de las necesidades de cada entidad, las organizaciones pueden estimar que, de manera generalizada, necesitan más personal para los niveles más bajos en número que para los más altos, por lo que se propone la siguiente cantidad de personal para su implementación:

- 1 director de ciberseguridad.
- X arquitectos de ciberseguridad.
- el doble de analistas (Y) de ciberseguridad que de arquitectos (Y = 2X).
- el doble de operadores (Z) de ciberseguridad que de analistas (Z = 2Y).

7.3.4 Servicios de ejemplo para un SOC

Todo SOC debe prestar una serie de servicios mínimos, con los que alinear los procesos, las tecnologías y los roles en la organización para la que trabaja. De esta manera, protege y previene sus activos de información y detecta y responde ante sus incidentes y brechas de ciberseguridad. Por tanto, se deben definir todos los servicios que se consideren necesarios, en dependencia del dimensionamiento del SOC, para cumplir con los objetivos de ciberseguridad de la organización. Debido a esto, como ejemplos, a continuación, se definen dos servicios que se podrían proponer para la implementación de un SOC funcional:

7.3.4.1 Servicio de Gestión de Incidentes de Ciberseguridad

El **Servicio de Gestión de Incidentes de Ciberseguridad**, como su propio nombre indica, se define como el servicio en el que se gestionan todos los incidentes de ciberseguridad de una organización, independientemente de si han tenido o no impacto sobre alguno de sus activos de información. Se trata del ejercicio en el que se deben tratar las amenazas que se consigan explotar contra la organización y que se sitúa dentro del área central de servicios de la gestión de eventos de ciberseguridad.

El avance y la complejidad de los ataques de ciberseguridad no ha dejado de aumentar en los últimos años. Sobre todo, tras la pandemia por la COVID-19, en donde la vida empresarial sufrió un cambio de paradigma en relación con la ubicación de los trabajadores. Por ello, a las diferentes tácticas, técnicas y procedimientos para la explotación de estos ataques, mejoran la ocultación y evasión de los atacantes, que complican la detección de los incidentes de ciberseguridad y les permiten pasar mucho más tiempo inadvertidos. Debido a esto, para contener estas acciones, las organizaciones deben instaurar estrategias de protección, prevención y detección basadas en la cadena *Cyber Kill Chain* [189], que segmenta los ataques de ciberseguridad en diferentes fases con las que un atacante busca tener éxito.

El SOC, como encargado de la ciberseguridad de la organización, debe implementar y ejecutar los mecanismos de detección de ataques y amenazas, que posibiliten su localización y situación en las diferentes etapas de la cadena. Esta estrategia, mientras maximiza el grado de detección, minimiza el impacto y la probabilidad de que un atacante reanude la actividad maliciosa en otra de esas etapas. Por tanto, esta área de ciberseguridad debe realizar el análisis y reconocimiento de los patrones e indicadores de compromiso (*IoC*) de estos desafíos para identificar y prevenir los sucesos no deseados en el futuro.

Por consiguiente, la integración de reglas de correlación nuevas se debe considerar una constante que sigue un proceso de gestión ordenado y circular con el que se maximizan y agilizan los resultados, mientras se adecúan y mejoran los casos al escenario actual de la organización y se minimiza la ocurrencia de los falsos positivos. Visualmente, a continuación, se ofrece una ilustración con la que se observa el ciclo de desarrollo de reglas de correlación:

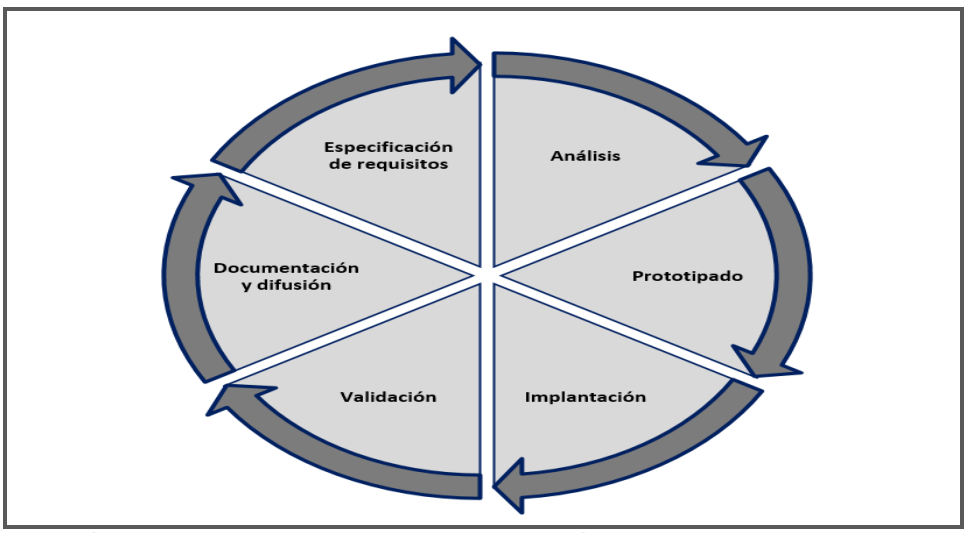

Ilustración 32 - Proceso de desarrollo de reglas de correlación.

[189] Ver el punto 7.1.3.1 del Anexo 1 para más información sobre las fases de un ataque informático y de la cadena Cyber Kill Chain.

Asimismo, este servicio debe definir sus actividades en base a la premisa de que, en caso de incidente de ciberseguridad real con impacto en alguno de los activos de información de la organización, el personal del SOC conozca sus responsabilidades y atribuciones en todo momento para reaccionar adecuadamente y bajo las políticas y metodologías implantadas por la organización. Además, por una parte, se deben definir tareas programadas periódicamente con sus *checklists*[190] y sus modelos de informes, entre otros, para garantizar los acuerdos a nivel de servicio y las reacciones rápidas del personal; y, por otra, se deben utilizar las herramientas y sistemas aprovisionadas por el cliente durante el ciclo de vida del incidente de ciberseguridad, por lo que deben proporcionar los accesos y permisos para todos los miembros del SOC.

La gestión de incidentes de ciberseguridad se trata de una de las principales tareas con mayor reconocimiento y visibilidad en un SOC. Además, esta gestión guarda especial relación con las actividades de gestión de incidentes de TI y con sus procesos de detección, investigación, contención y recuperación, que tienen el objetivo de reducir el impacto y asegurar la continuidad de las funciones operativas. Por tanto, este servicio se debe implementar y llevar a cabo según los protocolos, procedimientos y políticas indicados por la organización y por los responsables de los activos de información que puedan verse afectados. En consecuencia, se debe proponer un modelo de trabajo para el SOC que se centre en la distribución de actividades para la preparación, la detección y el análisis, el triaje y la clasificación, la contención, la erradicación y la recuperación y, finalmente, las medidas post-incidente de los incidentes de ciberseguridad mediante una organización multinivel.

La definición de un procedimiento para la ágil gestión y respuesta ante incidentes de ciberseguridad, requiere que se determinen las acciones que se deben realizar. Además, aunque se nutra principalmente de la información proveniente de las herramientas de ciberseguridad implantadas en la organización, debe tenerse en cuenta que no siempre son detectados por la tecnología, sino que, en ocasiones, son detectados por los usuarios, que informan de problemas o sucesos sospechosos, por lo que se debe implementar un proceso de retroalimentación que actualice la gestión del conocimiento y el aprendizaje del personal el SOC para mejorar y optimizar los mecanismos de prevención. Por esta razón, con el fin de que el servicio de gestión de ciberincidentes se considere lo más eficiente y eficaz posible, se requiere que se registren todos los casos abiertos de su cola de trabajo en diferentes *tickets* y los priorice en base a los criterios que se consideren.

Finalmente, los dominios en los que se basa este servicio se definen a continuación:

[190] https://www.isotools.org/2018/03/08/que-es-un-checklist-y-como-se-debe-utilizar/

Dominios del servicio de gestión de ciberincidentes	Descripción
Procesos principales del servicio	• Monitorización de eventos de ciberseguridad. • Correlación de eventos de ciberseguridad. • Clasificación de eventos y ciberincidentes. • Triaje de eventos e incidentes de ciberseguridad. • Identificación de ciberamenazas y ciberincidentes. • Investigación de eventos y ciberincidentes. • Registro de los ciberincidentes. • Tratamiento y escalado de los y ciberincidentes. • Recogida de evidencias de las ciberamenazas. • Reacción ante ciberamenazas y ciberincidentes. • Notificación de los ciberincidentes. • Seguimiento de los ciberincidentes. • Análisis posterior a los ciberincidentes • Desarrollo de flujos de trabajo ante ciberincidentes.
Tecnologías principales para la gestión del servicio	• Sistemas de gestión de información y eventos de seguridad (SIEM). • Sistemas de orquestación, automatización y respuesta de seguridad (SOAR). • Herramientas de gestión de *ticketing*. • Herramientas de inteligencia de amenazas. • Herramientas de análisis forense.
Tecnologías secundarias para la gestión del servicio	• Cortafuegos (Firewall). • Sistemas de detección de intrusos (IDS). • Sistemas de prevención de intrusos (IPS). • Herramientas de protección de puntos finales (EEP). • Herramientas de detección y respuesta. • Cortafuegos de Aplicaciones web (WAF). • Sistemas de protección del correo electrónico. • Herramientas de inventario de activos de información. • Herramientas de monitorización de disponibilidad.

Personas y roles	• **Nivel 1**: Equipo técnico de operadores del SOC que realizan, entre otras, las siguientes acciones:
	  ○ Registro y triaje de eventos e incidentes.
	  ○ Remediación ágil y rápida a través de procedimientos definidos y aprobados.
	  ○ Asignación y escalado, en su caso, al nivel 2.
	• **Nivel 2**: Equipo técnico de analistas del SOC que realizan, entre otras, las siguientes acciones:
	  ○ Tratamiento y resolución de incidencias más complejas.
	  ○ Asignación y escalado, en su caso, al nivel 3.
	• **Nivel 3**: Equipo de arquitectos del SOC que se encargan de, entre otras, las siguientes actividades:
	  ○ Análisis avanzado de amenazas e incidentes.
	  ○ Cazadores de amenazas proactivos.
	  ○ Análisis forense avanzado.
	  ○ Control del cumplimiento normativo del servicio.
	• **Nivel 4**: Director del SOC (posible CISO), que se encarga de la dirección y las responsabilidades del servicio y de su alineación con la alta dirección de la organización.

Tabla 53 - Dominios del Servicio de Gestión de Ciberincidentes.

7.3.5.2 Servicio de Alerta Temprana

El **Servicio de Alerta Temprana** se define como el servicio en el que se gestionan la detección, notificación y reacción ante las vulnerabilidades de los activos tecnológicos de información de una organización. Se trata del ejercicio en el que se deben tratar las debilidades de los sistemas de una organización y que se sitúa dentro del área central de servicios de la gestión de riesgos y vulnerabilidades.

Este servicio se debe implementar en base a los principios de prontitud, priorización, criticidad y utilidad de los activos tecnológicos y se debe integrar junto a los procedimientos y protocolos de gestión de vulnerabilidades que ya se encuentren implantados en la organización. Por tanto, se debe realizar un proceso de análisis de la información de la vulnerabilidad y del impacto que puede tener en la organización antes de que pueda ocurrir para aportar información enriquecida para su protección y prevención. Además, este servicio se debe alimentar de diferentes fuentes de información, tanto internas (Inteligencia de amenazas y pruebas de penetración) como externas (información de diferentes CERT o CSIRT), para recibir las alertas de las debilidades y su información de interés para analizarlo en la infraestructura de la organización.

En relación con las tecnologías aplicables en cada momento, el personal del SOC debe consensuar un listado de activos tecnológicos de información, tanto software como hardware, con el cliente para definir un alcance. Por ello, para el descubrimiento del inventario se recomienda utilizar herramientas de inventario de activos de información, aunque, en dependencia del tamaño de la organización, también se pueden utilizar procedimientos manuales para la creación de un listado detallado. Además, en base a la posibilidad de obtener con precisión las versiones desplegadas en cada activo de información de la infraestructura de la organización, el SOC actuará con mayor eficacia, pero, para ello, el cliente y los responsables de estos activos deben suministrar los accesos y permisos al personal del SOC y a las herramientas de inventario para poder disponer de la información requerida.

Asimismo, el análisis se debe ajustar a los activos de información contenidos en el inventario obtenido y que se encuentren operativos en la organización, por lo que este listado debe ser la raíz única de la información. Por tanto, todos los activos que no se encuentren en el inventario no se verificarán y notificarán a través del análisis de la alerta temprana. Además, el alcance de las tecnologías puede verse afectado, en incremento o decremento, en base a las medidas de altas y bajas de activos que requiera la organización. Igualmente, aunque estas altas y bajas deban requerir de un proceso de notificación de cambio, para su inclusión en el Servicio de Alerta Temprana, debe ser necesaria una solicitud de incorporación al servicio enviada al SOC para su estudio y valoración. De hecho, una posible solución para que esta solicitud y comunicación siempre se produzca consiste en incluir al Director o un representante del SOC en todos aquellos comités y reuniones en los que se traten los cambios y la configuración tecnológica de la organización.

Por otra parte, este servicio debe prestarse diariamente en las franjas laborales que requiera la organización, según la periodicidad de cambios en los activos de información que realice y a la publicación de las nuevas vulnerabilidades descubiertas. Por tanto, el Director del SOC asignará periódicamente un analista del SOC (o, a lo sumo, un operador) como gestor de este servicio para que realice los procesos para identificar, validar, clasificar, realizar el triaje, registrar y notificar las debilidades de los activos tecnológicos, para depurar la información para comunicar la actualidad de la

ciberseguridad y de las vulnerabilidades y para realizar un seguimiento de las vulnerabilidades activas.
El flujo de trabajo ante una nueva vulnerabilidad en alguno de los activos de información tecnológicos de información se define, como ejemplo, a continuación:

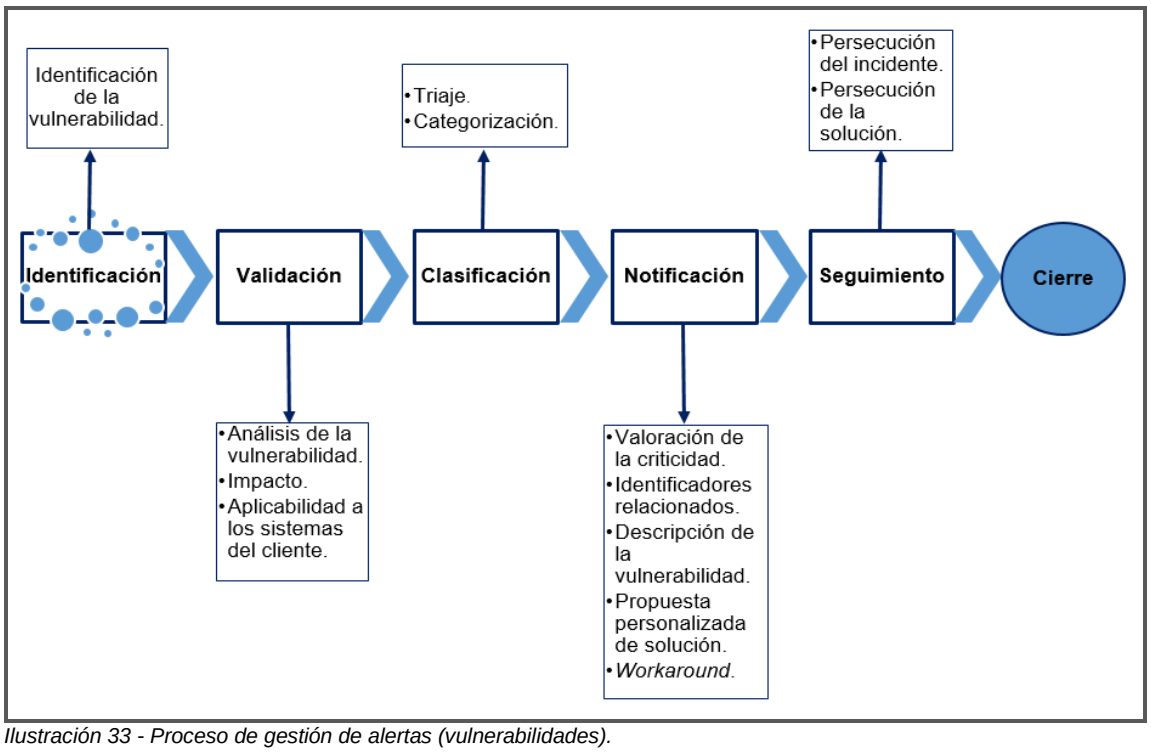

Ilustración 33 - Proceso de gestión de alertas (vulnerabilidades).

Al mismo tiempo, este servicio debe definir sus actividades con la idea de permitir la transición de las actividades en diferentes horarios y turnos, por lo que el personal del SOC debe conocer sus responsabilidades y atribuciones en todo momento para reaccionar adecuadamente y bajo las políticas y metodologías implantadas por la organización. Además, por una parte, se deben definir tareas programadas periódicamente con sus *checklists* y sus modelos de informes, entre otros, para garantizar los acuerdos a nivel de servicio y las reacciones rápidas del personal; y, por otra, se deben utilizar las herramientas y sistemas aprovisionadas por el cliente durante el ciclo de vida de las vulnerabilidades, por lo que deben proporcionar los accesos a los activos tecnológicos de información, junto a sus permisos, para todo el personal del SOC.

Una alerta de ciberseguridad se puede detectar a través de diferentes mecanismos de detección, como pueden ser, entre otros, el uso de herramientas automatizadas o los gestores de vulnerabilidades, o a través de medios manuales, mediante los reportes de problemas que hacen los usuarios de la organización en la gestión de ticketing. Por lo general, el volumen de registros sobre alertas suele ser elevado, por lo que se requiere de personal con habilidades y conocimientos avanzados y especializados en el análisis de las vulnerabilidades.

Finalmente, los dominios en los que se basa este servicio se definen a continuación:

Dominios del Servicio de Alerta Temprana	Descripción
Procesos principales del servicio	• Identificación de alertas y vulnerabilidades. • Validación de alertas y vulnerabilidades. • Clasificación de alertas y vulnerabilidades. • Triaje de alertas y vulnerabilidades. • Registro de alertas y vulnerabilidades. • Tratamiento y escalado de alertas y vulnerabilidades. • Notificación de alertas y vulnerabilidades. • Reacción ante alertas y vulnerabilidades. • Actualización de alertas y vulnerabilidades. • Seguimiento de alertas y vulnerabilidades.
Tecnologías principales para la gestión del servicio	• Sistemas de gestión de vulnerabilidades. • Herramientas de inventario de activos de información. • Sistemas de gestión de información y eventos de seguridad (SIEM). • Sistemas de orquestación, automatización y respuesta de seguridad (SOAR). • Herramientas de gestión de *ticketing*.
Tecnologías secundarias para la gestión del servicio	• Cortafuegos (Firewall). • Sistemas de detección de intrusos (IDS). • Sistemas de prevención de intrusos (IPS). • Herramientas de protección de puntos finales (EEP). • Herramientas de detección y respuesta. • Cortafuegos de Aplicaciones web (WAF). • Sistemas de protección del correo electrónico. • Herramientas de monitorización de disponibilidad.

Personas y roles	• **Nivel 1**: Equipo técnico de operadores del SOC que realizan, entre otras, las siguientes acciones:
	  ○ Notificación y alerta de las vulnerabilidades en base a la información recibida del Nivel 2.
	  ○ Remediación ágil y rápida a través de procedimientos definidos y aprobados.
	• **Nivel 2**: Equipo técnico de analistas del SOC que realizan, entre otras, las siguientes acciones:
	  ○ Análisis, tratamiento y resolución de las vulnerabilidades detectadas.
	  ○ Realización de pruebas de penetración en los activos tecnológicos de información.
	  ○ Asignación de la notificación al nivel 1.
	  ○ Asignación y escalado, en su caso, al nivel 3.
	• **Nivel 3**: Equipo de arquitectos del SOC que se encargan de, entre otras, las siguientes actividades:
	  ○ Verificación de las alertas y vulnerabilidades complejas.
	  ○ Reporte, en su caso, al nivel 4.
	• **Nivel 4**: Director del SOC (posible CISO), que se encarga de la dirección y asignación de responsabilidades al personal del servicio y de enlazarlo con la alta dirección de la organización.

Tabla 54 - Dominios del Servicio de Alerta Temprana.

7.4 Anexo 4: Seguimiento de la PEC2 del TFM

7.4.1 Revisión de los objetivos y alcance del proyecto

Los objetivos del TFM, tanto el principal como los parciales, se mantienen, tal y como han sido planificados. No obstante, se destaca que se ha necesitado describir con más detalle el alcance del proyecto, mediante una definición más clara y concreta de los objetivos parciales.

7.4.2 Revisión de la planificación

Una vez finalizado este hito, se verifica que se ha cumplido con la planificación establecida y, por tanto, se han conseguido los hitos planteados:

	Fecha de inicio	Fecha de entrega	Ejecución
Hito 2: Primera fase de ejecución del Plan de Trabajo (PEC2).	**12/10/2022**	**08/11/2022**	✓
Análisis del marco preliminar para un SOC.	12/10/2022	15/10/2022	✓
Estudio de Riesgos, Amenazas y Vulnerabilidades.	15/10/2022	19/10/2022	✓
Análisis del marco conceptual de un SOC.	19/10/2022	22/10/2022	✓
Sistemas de protección, prevención y detección.	22/10/2022	24/10/2022	✓
Estudio de los ataques y los incidentes de seguridad.	24/10/2022	26/10/2022	✓
Análisis del marco metodológico, estándares y buenas prácticas para un SOC.	26/10/2022	31/10/2022	✓
Reunión de seguimiento con el tutor del TFM (I).	27/10/2022	27/10/2022	✓
Definición de un SOC y justificación de su necesidad.	31/10/2022	03/11/2022	✓
Análisis de las normativas legales para un SOC.	03/11/2022	05/11/2022	✓
Análisis de los riesgos de este hito.	05/11/2022	06/11/2022	✓
Redacción y revisión de este entregable.	06/11/2022	08/11/2022	✓

Tabla 55 - Planificación cumplida en el hito 2.

7.4.3 Revisión de los riesgos

No se han manifestado ninguno de los riesgos previstos ni se han detectado riesgos inesperados en esta entrega.

7.4.4 Valoración del trabajo realizado hasta el momento

Se considera que el trabajo realizado hasta el momento ha sido el adecuado, ya que se ha cumplido fielmente el cronograma planificado y se han alcanzado los objetivos planteados. Por tanto, estas acciones han permitido que se realice una revisión en profundidad de los conceptos y temas estudiados, por lo que se le otorga direccionalidad al proyecto.

7.5 Anexo 5: Seguimiento de la PEC3 del TFM

7.5.1 Revisión de los objetivos y alcance del proyecto

Los objetivos del TFM, tanto el principal como los parciales, se han cumplido, tal y como se planteó desde el comienzo del trabajo. Además, se mantiene el alcance y el objetivo principal del proyecto.

7.5.2 Revisión de la planificación

Una vez finalizado este hito, se verifica que se ha cumplido con la planificación establecida y, por tanto, se han conseguido los hitos planteados:

	Fecha de inicio	Fecha de entrega	Ejecución
Hito 3: Segunda fase de ejecución del Plan de Trabajo (PEC3).	**12/10/2022**	**08/11/2022**	✓
Análisis del marco teórico y requisitos de un SOC.	09/11/2022	13/11/2022	✓
Definición de tipos de servicios y procesos de un SOC.	13/11/2022	18/11/2022	✓
Análisis de los requisitos de cada servicio.	18/11/2022	21/11/2022	✓
Análisis de las métricas para cada proceso.	21/11/2022	24/11/2022	✓
Definición de los flujos de trabajo de cada servicio.	24/11/2022	27/11/2022	✓
Análisis de las tecnologías necesarias para un SOC.	27/11/2022	30/11/2022	✓
Reunión de seguimiento con el tutor del TFM (II).	29/11/2022	29/11/2022	✓
Análisis de los roles que gestionan un SOC.	30/11/2022	03/12/2022	✓
Análisis de los riesgos de este hito.	03/12/2022	04/12/2022	✓
Redacción y revisión de este entregable.	04/12/2022	06/12/2022	✓

Tabla 56 - Planificación cumplida en el hito 3.

7.5.3 Revisión de los riesgos

No se han detectado ninguno de los riesgos anunciados ni se han detectado riesgos no previstos en esta entrega.

7.5.4 Valoración del trabajo realizado hasta el momento

Se considera que el trabajo realizado ha sido el adecuado, ya que, en este caso, también se ha cumplido con el cronograma planteado y se han alcanzado todos los objetivos planteados. Por tanto, se ha realizado un desarrollo adecuado del TFM, que se culminará con la entrega del producto deseado.