Diseño de la implementación de un Centro de Operaciones de Seguridad (SOC) basado en ITIL

Antonio Díaz Pérez
Grado de Ingeniería Informática
Gestión de Proyectos

Joan Gallifa Roca
Atanasi Daradoumis Haralabus

Junio de 2021

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Diseño de la implementación de un Centro de Operaciones de Seguridad (SOC) basado en ITIL*
Nombre del autor:	*Antonio Díaz Pérez*
Nombre del consultor/a:	*Joan Gallifa Roca*
Nombre del PRA:	*Atanasi Daradoumis Haralabus*
Fecha de entrega (mm/aaaa):	06/2021
Titulación:	*Grado de Ingeniería Informática*
Área del Trabajo Final:	*Gestión de Proyectos*
Idioma del trabajo:	*Español*
Palabras clave	*SOC, ITIL*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados y conclusiones del trabajo.*

En la actualidad, la información se ha convertido en el activo principal de las organizaciones. El auge y el desarrollo de los sistemas informáticos ha permitido crear mecanismos que facilitan el acceso a los datos de manera más ágil. Asimismo, a medida que se ha extendido la transformación digital en las organizaciones, también ha aumentado el compromiso de la información. Como resultado, los sistemas informáticos se han expuesto a amenazas constantes, por lo que han necesitado la adaptación continua de soluciones para garantizar su seguridad.

Debido a esto, la seguridad de la información y de los sistemas se considera un pilar clave para todas las organizaciones. Se hace necesario garantizar sistemas seguros que permitan identificar y enfrentar las posibles amenazas a tiempo, por lo que muchas organizaciones han optado por la implementación de un Centro de Operaciones de Seguridad (SOC), que es una unidad centralizada que se dedica a los aspectos tácticos y operativos asociados con la ciberseguridad.

Asimismo, ITIL constituye la biblioteca de recursos más extendida a nivel de administración de tecnologías de la información. En consecuencia, en este trabajo, se propone desarrollar una guía que diseñe la implementación de un SOC basado en ITIL, que, además, tendrá en cuenta elementos de metodologías ágiles. Con este fin, se pretende ofrecer un documento que guíe la implementación de un SOC que establezca la forma más eficiente de administrar las actividades de seguridad de la información de las organizaciones.

Abstract (in English, 250 words or less):

Nowadays, information has become the main asset of organisations. The rise and development of IT systems has enabled the creation of mechanisms that facilitate access to data in a more agile way. Moreover, as the digital transformation of organisations has become more widespread, so has the engagement of information. As a result, IT systems have been exposed to constant threats, necessitating the continuous adaptation of solutions to ensure their security.

As a result, information and systems security is considered a key pillar to all organisations. It is necessary to ensure secure systems that can identify and address potential threats in a timely manner, which is why many organisations have opted for the implementation of a Security Operations Centre (SOC), which is a centralised unit dedicated to the tactical and operational aspects associated with cyber security.

ITIL is also the most extensive library of resources for IT management. In consequence, this project proposes to develop a guide to design the implementation of a SOC based on ITIL, which will also take into account elements of agile methodologies. With this intent, the aim is to provide a document that guides the implementation of a SOC that establishes the most efficient way to manage the information security activities of organisations.

Índice

Lista de ilustraciones

Lista de tablas

1. Introducción

1.1 Contexto y justificación del Trabajo

Antes del surgimiento y difusión del uso de los sistemas informáticos, la información de valor empresarial se gestionaba y archivaba en medios físicos como papel, cintas de vídeo y fotografías, entre otros. Por tanto, se obtenía como resultado el almacenamiento de grandes volúmenes de material ubicado en un lugar físico y único, que concluía con que el acceso, el almacenamiento y el procesamiento de los datos importantes suponían un coste muy elevado para las organizaciones.

Con la aparición de los sistemas informáticos se facilitó la digitalización de la información, que repercutió directamente en la generación de mecanismos de procesamiento más rápido y fácil acceso a los datos. De hecho, en la actualidad, cada vez son más las organizaciones que hacen uso de la tecnología digital, que crean, transportan y almacenan sus datos, su información y su conocimiento mediante sistemas digitales y que, incluso, se encuentran sumidas en procesos de transformación digital. Debido a esto, la información se convierte en el activo más valioso e importante de toda entidad y, por consiguiente, su protección pasa a ser una necesidad primaria.

Asimismo, dado que cada vez se cuenta con un mayor uso de tecnologías y sistemas de información digitales, también se ha detectado un aumento de los ataques informáticos en busca de explotar las vulnerabilidades existentes en las infraestructuras corporativas. Por tanto, las amenazas a las que se han visto expuestos los sistemas informáticos han ido evolucionando en la misma medida en la que lo ha hecho el desarrollo de las tecnologías.

Debido a esto, se ha requerido una adaptación continua con nuevas medidas que den solución a estas vulnerabilidades y los problemas técnicos detectados. Además, las nuevas condiciones han estado determinadas por la sofisticación de los ataques y las amenazas a la seguridad de los sistemas, por lo que también ha aumentado la complejidad de sus soluciones.

Dadas a estas ideas, la seguridad de la información, de los sistemas, las aplicaciones y las comunicaciones se considera uno de los elementos fundamentales a tener en cuenta en toda organización. De hecho, cada vez más, estas entidades trabajan en minimizar y gestionar los riesgos de seguridad y garantizar sistemas seguros que permitan identificar las posibles amenazas, con el fin de respaldar el uso adecuado de sus bienes y recursos con los que desarrolla sus actividades diarias.

Por este motivo, el Centro Criptológico Nacional (CCN), con el fin de cercar conceptos, define la Seguridad de la Información como la protección de la confidencialidad, la integridad y la disponibilidad de la información, así como de otras características como son la autenticidad, la responsabilidad, la fiabilidad y

la precaución del repudio. Concepto descrito de forma similar en la norma establecida UNE-EN ISO/IEC 27001 (2013).

En consecuencia, las organizaciones, comúnmente, interpretan este concepto como la suma de las acciones de carácter técnico, legítimo, organizativo y corporativo con las que se asegura la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de los sistemas de información. Además, demandan un servicio que vele por estas cinco dimensiones de la seguridad de la información y que, en caso de desastre, establezca mecanismos adecuados para la recuperación de datos en el menor tiempo y con la menor afectación y daño posible a sus actividades y negocio.

Debido a estas necesidades, diferentes organizaciones han optado por la implementación de un Centro de Operaciones de Seguridad (SOC - *Security Operations Center*, por sus siglas en inglés), que permita contar con una unidad centralizada y dedicada a los aspectos tácticos y operativos asociados con la ciberseguridad. A consecuencia de esto, un SOC realiza labores orientadas a la monitorización, protección y defensa de los activos de información en tiempo real, a través de equipos tecnológicos y personal especializado y centralizado, y se encarga de los servicios de detección y reacción ante incidentes de seguridad en la organización.

Por tanto, el diseño de la implementación de un Centro de Operaciones de Seguridad debe guiarse por metodologías que aseguren su adecuada implementación. Entre las más utilizadas, se destaca ITIL, que, actualmente, constituye la biblioteca de recursos más extendida a nivel de administración de tecnologías de la información. Por otra parte, las metodologías ágiles establecen la forma más eficiente de administrar las actividades de las organizaciones en entornos de incertidumbre.

Por este motivo, se hace posible combinar elementos de estas metodologías, con el fin de obtener resultados eficaces y eficientes a nivel tecnológico. No obstante, será necesario realizar un análisis de los criterios a los que se puede ajustar la aplicación de combinar las diferentes metodologías.

En función de los elementos indicados, como propuesta de Trabajo de Final de Grado, se propone elaborar el diseño de la implementación de un SOC mediante las buenas prácticas propuestas por ITIL y las metodologías ágiles. De esta forma, se ofrece un servicio de ciberseguridad que permita a las organizaciones centralizar los eventos e incidentes de seguridad de la información, de los sistemas, de las aplicaciones y de las comunicaciones y aportar una solución a los problemas que se identifiquen en este ámbito.

1.2 Objetivos del Trabajo

En los últimos años, se ha detectado un aumento de los ataques informáticos a escala mundial, hasta el punto de comprometer a organizaciones públicas y privadas y repercutir en sus actividades diarias y su negocio. Por tanto, el

objetivo principal de este trabajo es diseñar un documento guía para la implementación de un Centro de Operaciones de Seguridad (SOC), a partir de la combinación de las buenas prácticas propuestas por ITIL y las metodologías ágiles, con el fin de facilitar su puesta en marcha para que proteja la seguridad de la información en la organización que lo requiera. Este documento se incluirá en el Anexo 1 de este documento.

Por consiguiente, para alcanzar este objetivo principal, a continuación, se describen los hitos específicos que darán lugar al éxito del proyecto:

1.2.1 Análisis de criterios por la combinación de metodologías

Se trata de un análisis de los criterios que se pueden ajustar en la aplicación de una combinación de metodologías ágiles y de las buenas prácticas de ITIL para la confección de una guía para la implementación de un Centro de Operaciones de Seguridad (SOC). De hecho, el uso de metodologías asegura la adecuada implementación de un servicio de esta magnitud.

En la actualidad, se destaca el uso de ITIL a niveles administrativos en el ámbito de las tecnologías de la información y el uso de las metodologías ágiles como vía eficiente de administración de las actividades de los servicios en las organizaciones. Por tanto, este objetivo pretende que, en el documento guía para la implementación de un SOC, quede reflejada la combinación de los criterios de ITIL y de las metodologías ágiles que se ajustan a este diseño, con el fin de obtener resultados eficaces y eficientes a nivel tecnológico.

1.2.2 Definición de tipos de servicio

Se trata de la definición de los tipos de servicios que formarán parte del Centro de Operaciones de Seguridad (SOC). Este servicio de seguridad informática, se ocupa de prevenir, monitorear y controlar la seguridad en los sistemas, redes y aplicaciones de las organizaciones. Por tanto, independientemente de las características de las organizaciones que decidan implementar un SOC, existe una serie de servicios básicos de los que se debe encargar el servicio y que abarcan desde el diagnóstico de vulnerabilidades hasta la recuperación del negocio en caso de desastre. En consecuencia, este objetivo propone definir dichos servicios para que puedan ser reflejados como parte del documento guía para la implementación de un SOC.

1.2.3 Identificación de los requisitos de cada servicio

Se trata de la identificación de los requisitos exigibles y específicos de cada uno de los servicios que integrarán el Centro de Operaciones de Seguridad (SOC). De esta forma, para cada uno de los servicios definidos en el objetivo anterior, que son los que formarán parte del servicio, se hace necesario establecer una serie de requisitos que permitan guiar la implementación de cada uno de estos servicios, así como medir su alcance. En consecuencia, este

objetivo se enfoca en desarrollar los servicios que formarán parte del SOC y reflejar los requisitos exigibles y requisitos específicos en el documento final.

1.2.4 Definición de los roles de cada servicio

Se trata de la definición de los roles encargados de gestionar la demanda y la entrega de cada uno de los servicios que integrarán el SOC. Es decir, definir la función, el papel de cada uno de los servicios.

El personal de un Centro de Operaciones de Seguridad se caracteriza por estar compuesto por un equipo de analistas y técnicos de ciberseguridad altamente experimentados y especializados en este ámbito. Por esta razón, un SOC se divide en diferentes niveles, que se corresponden con el grado de especialización de los analistas. De esta manera, el servicio podrá contar con diferentes perfiles en la materia. Desde analistas que se encarguen de monitorizar continuamente las alertas que recibe el SOC hasta profesionales altamente capacitados que se encarguen de dar solución a los incidentes y problemas en busca de prevención. Por tanto, este objetivo se centra en definir cada uno de los roles asociados a los niveles de especialización del personal encargado de operar el SOC.

1.2.5 Propuesta de un Plan de implementación de un SOC

Se trata de la propuesta de un Plan de implementación del Centro de Operaciones de Seguridad (SOC). Una vez desarrollados los objetivos anteriores, se elaborará una propuesta de donde se expresen las diferentes etapas que debe atravesar el proceso de implementación de un Centro de Operaciones de Seguridad. Por tanto, mediante este hito, se reflejarán los objetivos de cada una de las etapas y las fechas estimadas para su consecución.

Finalmente, tal y como se ha indicado, una vez abarcados todos los hitos planteados, se procederá a la elaboración del documento guía para la implementación de un Centro de Operaciones de Seguridad (SOC); el objetivo principal del proyecto (Anexo 1).

1.3 Enfoque y método seguido

Dada la naturaleza del proyecto, marcada por el diseño de la implementación de un servicio, se decide hacer uso de buenas prácticas, metodologías, paradigmas y procedimientos de trabajo basados en estándares de reconocimiento internacional. En este punto, se estudiarán las buenas prácticas de las versiones 3 y 4 de ITIL (*Information Technology Infrastructure Library*) y los conceptos de las metodologías ágiles como DevOps, Extreme Programming (XP), SCRUM y Kanban para valorar el papel que pueden jugar en el diseño de implementación de un SOC.

Debido a esto, a continuación, se definen estos estándares de reconocimiento y prestigio en el mundo de la gestión de proyectos y de las Tecnologías de la Información (TI):

1.3.1 ITIL

Se define como una biblioteca, un marco de referencia, que contiene la descripción de un conjunto de recomendaciones y buenas prácticas para la administración de servicios de TI. Además, aunque ITIL no es una metodología, permite que los acuerdos de calidad del servicio mejoren la relación con el cliente. Por ello, se orienta a la estructura de la organización de TI, se centra en los objetivos corporativos y se esfuerza en incluir información sobre los objetivos a alcanzar, las actividades generales, las entradas y las salidas de los procesos que se pueden incorporar a las diferentes áreas de TI.

Por tanto, su objetivo principal trata de generar valor en la entrega de servicios mediante la provisión de las buenas prácticas para la Gestión de Servicios. Asimismo, las dos versiones de ITIL más extendidas en la actualidad son las siguientes:

1.3.1.1 ITIL versión 3

Versión de ITIL que tiene como meta la creación de valor a través de servicios de TI y, por lo tanto, de los procesos y funciones del Ciclo de Vida del Servicio de TI.

1.3.1.2 ITIL versión 4

Versión de ITIL que tiene como meta la co-creación de valor conjuntamente y de manera continua entre el proveedor del servicio y su consumidor y, por consiguiente, de sus prácticas definidas en los Principios Guía y los conceptos de Sistema de Valor del Servicio y de Cadena de Valor del Servicio.

1.3.2 DevOps

Se define como una filosofía colaborativa, una cultura, para la creación de productos y servicios ajustados a las necesidades de tiempo de los clientes, que une principios tanto de Lean como de metodologías ágiles y tiene como objetivo unificar las funciones de desarrollo de software (Dev) y de producción/operación (Ops) en un proceso único, integrado y continuo.

Además, su ciclo de vida busca la innovación, la monitorización y la mejora continua, por lo que no debe de haber pausas ni retrasos entre iteraciones o entregas y el desglose de tareas debe de estar automatizado. Por ello, su ciclo de vida se basa en la gestión continua y entrega continua con las siguientes etapas: desarrollo, prueba, integración, despliegue y monitorización.

1.3.5 Kanban

Se define como una metodología ágil que incide en la productividad y eficiencia del equipo de trabajo mediante la definición, gestión y mejora de los servicios que derivan en la entrega de conocimiento. Además, se fundamenta en los pilares de transparencia y eficiencia a través de la elaboración de un cuadro o diagrama en donde se refleja el estado de las tareas: pendientes, en proceso y terminadas, entre otras. De esta manera, se señalan los hitos de trabajo del equipo y, por tanto, se agilizan las prioridades, se mejoran la comunicación y la colaboración de las acciones, se genera mayor independencia, se facilita el entendimiento de los objetivos y se acerca más a la estrategia del negocio.

Por otra parte, Kanban cuenta con tres principios directores que se centran en los requisitos de la organización y suponen llamadas a la acción que se basan en las necesidades de la organización:

1. El principio director de Sostenibilidad, que se focaliza en conseguir un ritmo sostenible y se enfoca en la mejora.
2. El principio director de Orientación al Servicio, que se orienta en alcanzar el rendimiento para la satisfacción del cliente.
3. El principio director de Supervivencia, que se centra en la competitividad y adaptabilidad.

1.3.3 Extreme Programming (XP)

Se define como una metodología de desarrollo ágil que se orienta hacia la mejora de la producción de software de la mejor calidad de forma constante en el tiempo mientras se promueve la mejor calidad de vida para los desarrolladores. Por tanto, se encarga de potenciar las relaciones personales y profesionales mediante el trabajo en equipo. Por otra parte, su aplicación requiere entender los valores, los principios y las prácticas que lo componen.

1.3.4 Scrum

Se define como una metodología de desarrollo ágil que se caracteriza por:

- Planificar una estrategia de desarrollo iterativo basado en ciclos de feedback rápido, en vez de una para la ejecución completa del resultado final. Esto implica que cualquier ciclo de desarrollo del producto y/o servicio, se desglosa en pequeños proyectos ejecutados en las distintas etapas de análisis, desarrollo y prueba.
- Centrar la calidad del producto y la solución en el conocimiento implícito del personal en equipos que se organizan a sí mismos, en vez de la calidad de los procedimientos utilizados.
- Enlazar las diferentes fases del desarrollo, en vez de ejecutarlas de forma secuencial.

1.3.6 Estrategia metodológica

Por consiguiente, desde el punto de vista estratégico y con el fin de conseguir los objetivos del proyecto, se valoran las diferentes opciones elegidas para realizar este diseño:

1. Trabajar bajo las buenas prácticas de la versión 3 de ITIL y darle un enfoque orientado, prácticamente, al servicio.
2. Trabajar a partir de los conceptos y prácticas de la versión 4 de ITIL y darle un enfoque orientado al valor.
3. Trabajar a partir de los conceptos de las metodologías ágiles, que se ocupan de satisfacer al cliente a través de la entrega temprana y continua de valor, aceptar la modificación de los requisitos y ser flexibles con las etapas de desarrollo de los servicios y productos.

En conclusión, tras tener en cuenta que, tras la última actualización de ITIL a la versión 4, en donde se incluye la colaboración creada por las iniciativas de Agile y DevOps y la mejora de la calidad impulsada por Lean, todos estos modelos comparten fundamentos similares destinados a mejorar la sinergia y la eficiencia. De esta manera, esta última versión de ITIL sugiere el impulso de la automatización para mejorar la eficiencia del servicio y complementar a las metodologías ágiles en las entregas que realizan a los clientes mediante la propia automatización.

Por tanto, con el fin de lograr una gestión óptima, se escoge trabajar bajo las buenas prácticas de la gestión de servicios propuestas por la versión 4 de ITIL y los conceptos de las metodologías ágiles. Esto quiere decir que al mismo tiempo que se fundamenta el diseño de la implementación de un SOC en ITIL, se gestionarán los aspectos operacionales y de apoyo a los servicios de las metodologías agiles.

Asimismo, debido a la importancia que tiene el uso de estas metodologías en el proyecto, se decide dedicar un posterior epígrafe a su análisis en profundidad, en donde se determinará el uso y funciones de cada metodología. De esta forma, se logrará una visión más clara de la aplicación y repercusión que tendrá en el diseño de la guía de implementación de un Centro de Operaciones de Seguridad (SOC) a partir de las buenas prácticas y metodologías propuestas.

1.4 Planificación del Trabajo

Este trabajo se inicia el día 26 de febrero de 2021, tras la propuesta de proyecto, y finaliza el día 21 de junio de 2021, con el la defensa del trabajo final de grado ante el Tribunal. Por tanto, a continuación, se definen los hitos principales del proyecto y sus tareas más importante, así como los tiempos previstos para su solución:

1.4.1 Hito 1: Plan de trabajo (PEC1)

El hito 1 de este Trabajo Final de Grado consiste en la realización del Plan de trabajo del proyecto y se sustenta en las siguientes tareas parciales:

1	Lectura del Plan de estudios y documentación del TFG.
2	Definición del proyecto.
3	Descripción del contexto y justificación del Trabajo.
4	Definir objetivos del trabajo.
5	Establecer el enfoque y método seguido.
6	Descripción de los capítulos de la memoria.
7	Redacción y revisión del entregable.

Tabla 1 - Tareas parciales del hito 1.

Por tanto, se establece la siguiente planificación temporal para este hito:

	Fecha de inicio	Duración (horas)	Fecha de entrega
Hito 1: Plan de Trabajo (PEC1)	**26/02/2021**	**64**	**12/03/2021**
Lectura del plan de estudios y documentación del TFG	26/02/2021	20	02/03/2021
Definición del proyecto	02/03/2021	11	05/03/2021
Descripción del contexto y justificación del Trabajo	05/03/2021	7	07/03/2021
Definir objetivos del trabajo	07/03/2021	8	09/03/2021
Establecer el enfoque y método seguido	09/03/2021	5	10/03/2021
Descripción de los capítulos de la memoria	10/03/2021	5	11/03/2021
Redacción y revisión del entregable	11/03/2021	8	12/03/2021

Tabla 2 - Planificación temporal del hito 1.

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

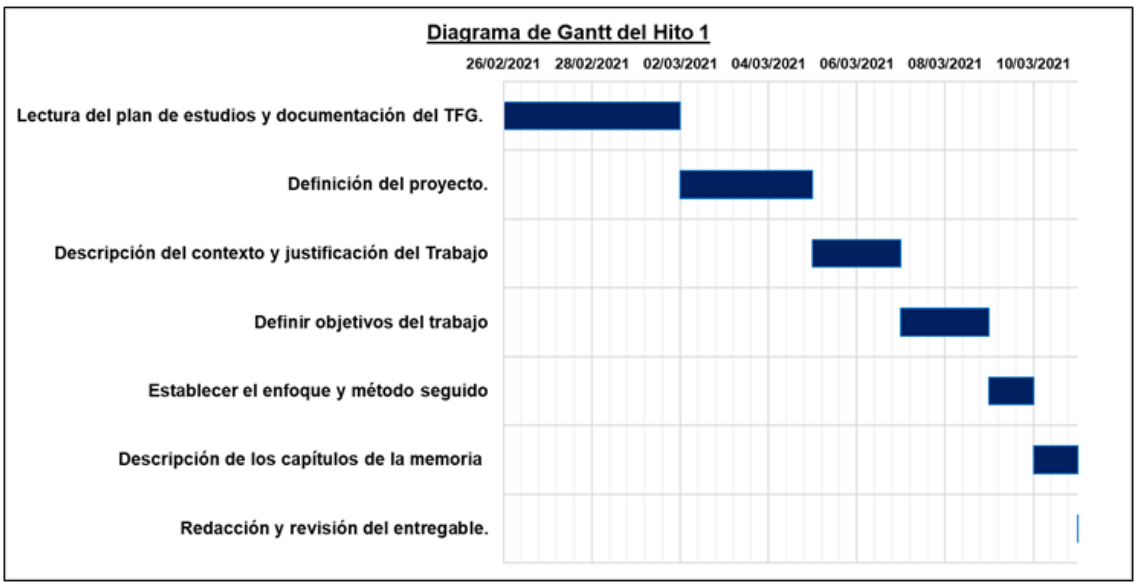

Ilustración 1 - Diagrama de Gantt del Hito 1.

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

El hito 2 de este Trabajo se corresponde con la etapa inicial de la ejecución del Plan de trabajo y se respalda en las siguientes tareas parciales:

1	Investigación y análisis de ITIL y metodologías agiles.
2	Análisis comparativo de ITIL y metodologías agiles.
3	Redacción de los aportes básicos.
4	Revisión bibliográfica sobre los servicios que formarán el SOC.
5	Definir los tipos de servicios que formarán el SOC.
6	Análisis de los riesgos.
7	Redacción y revisión del entregable.

Tabla 3 - Tareas parciales del hito 2.

Por tanto, se determina la siguiente planificación temporal para este hito:

	Fecha de inicio	Duración (horas)	Fecha de entrega
Hito 2: Primera fase de ejecución del plan de trabajo (PEC2)	**13/03/2021**	**88**	**09/04/2021**
Investigación y análisis de ITIL y metodologías agiles	13/03/2021	20	20/03/2021
Análisis comparativo de ITIL y metodologías agiles	20/03/2021	14	25/03/2021
Redacción de los aportes básicos	25/03/2021	8	28/03/2021
Revisión bibliográfica sobre los servicios que formarán el SOC	28/03/2021	12	02/04/2021
Definir los tipos de servicios que formarán el SOC	02/04/2021	14	06/04/2021
Análisis de los riesgos.	06/04/2021	6	07/04/2021
Redacción y revisión del entregable	07/04/2021	14	09/04/2021

Tabla 4 - Planificación temporal del hito 2.

Adicionalmente, se indica que, durante esta etapa del desarrollo de la investigación, el contenido se encuentra prácticamente orientado a un análisis en profundidad de los postulados teóricos de las diferentes metodologías. Debido a esto, se ha previsto un tiempo adecuado para poder desarrollar su análisis comparativo.

Por tanto, se concibe como posible riesgo derivado de esta etapa, la necesidad de hacer una redefinición de los servicios identificados como parte del SOC, en donde se establecerían vínculos directos con los aportes realizados por las metodologías analizadas. En definitiva, se considera importante que en esta etapa queden claros los procesos concebidos y su relación con la metodología guía, ya que este aspecto influirá en el posterior desarrollo del trabajo y su calidad.

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	Poca profundidad en la conceptualización de las metodologías escogidas para el proyecto.	Revisión de bibliografía actualizada
		Revisión de bibliografía en diferentes idiomas
		Reajuste de las horas dedicadas a la planificación de las tareas a cumplir.
2	Reformulación de los objetivos del proyecto.	Ajuste del alance del proyecto
		Reformulación teórica de los objetivos
3	Dificultad en la definición de los servicios identificados como parte del SOC.	Vinculación de las metodologías propuestas con los servicios identificados como parte del SOC
		Aclaración de los valores aportados por cada una de las metodologías
		Definición de los procesos que implica cada uno de los servicios identificados como parte del SOC.

Tabla 5 - Riegos del hito 2.

Seguidamente, también se presenta su diagrama de Gantt:

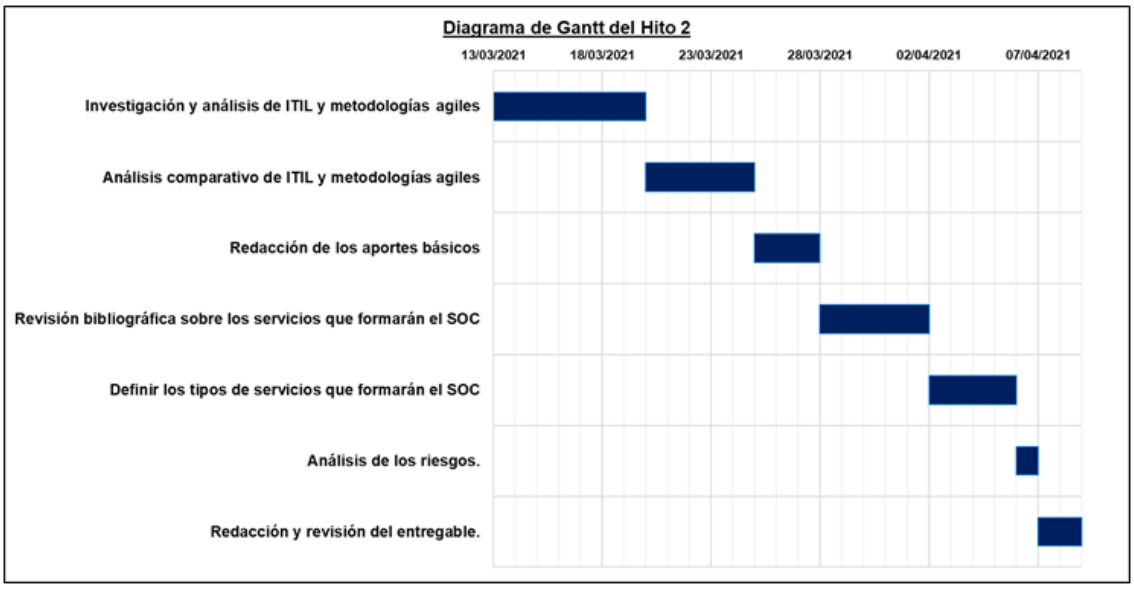

Ilustración 2 - Diagrama de Gantt del Hito 2.

1.4.3 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 las siguientes tareas parciales:

1	Definición de requisitos exigibles específicos para cada uno de los servicios
2	Análisis de métricas a aplicar a cada uno de los requisitos.
3	Identificación de los flujos de trabajo en cada tipo de servicio.
4	Definición de los roles encargados de gestionar la demanda y la entrega para cada uno de los servicios.
5	Elaboración del Plan de implementación para el SOC.
6	Análisis de los riesgos.
7	Redacción y revisión del entregable.

Tabla 6 - Tareas parciales del hito 3.

Por tanto, se fija la siguiente planificación temporal para este tercer hito:

	Fecha de inicio	Duración (Horas)	Fecha de entrega
Hito 3:Segunda fase de ejecución del plan de trabajo (PEC3)	**10/04/2021**	**92**	**07/05/2021**
Definición de requisitos exigibles específicos para cada uno de los servicios	10/04/2021	20	15/04/2021
Análisis de métricas a aplicar a cada uno de los requisitos	15/04/2021	12	20/04/2021
Identificación de los flujos de trabajo en cada tipo de servicio	20/04/2021	12	24/04/2021
Definición de los roles encargados de gestionar la demanda y la entrega para cada uno de los servicios	24/04/2021	12	28/04/2021
Elaboración del Plan de implementación para el SOC (Anexo 1)	28/04/2021	16	03/05/2021
Análisis de los riesgos	03/05/2021	6	05/05/2021
Redacción y revisión del entregable	05/05/2021	14	07/05/2021

Tabla 7 - Planificación temporal del hito 3.

De igual forma que en el punto anterior, en esta etapa del trabajo, que contiene una fuerte carga de elaboración y análisis, se pueden identificar diferentes riesgos que pueden obstaculizar el cumplimiento del plan de trabajo propuesto:

- Por una parte, se pueden encontrar demoras en las definiciones técnicas asociadas a cada uno de los tipos de servicios concebidos para el SOC, ya que, aunque se han establecido tiempos holgados para estas definiciones, se trata de un proceso que requiere alto nivel de atención a los detalles.
- Por otra parte, la elaboración del Plan de Implementación de un SOC, constituye el producto final del trabajo, por lo que puede verse afectado en el tiempo por la necesidad de más horas para su elaboración y para

su modificación en base a las indicaciones y sugerencias propuestos tras su revisión.

Por consiguiente, también 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 las definiciones técnicas asociadas a cada uno de los tipos de servicios concebidos para el SOC.	Cumplimiento de los tiempos establecidos para cada tarea.
		Consulta de artículos especializados.
		Atención a los detalles.
		Descripción detallada de cada uno de los requisitos y procesos presentados para cada uno de los servicios.
2	Incumplimiento del tiempo establecido para la elaboración del Plan de Implementación de un SOC.	Reajuste de las horas dedicadas a esta actividad.
		Solucionar los señalamientos que se hagan en tiempo, evitando las demoras.
		Reformulación de los tiempos dedicados a la tarea.

Tabla 8 - Riegos del hito 3.

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

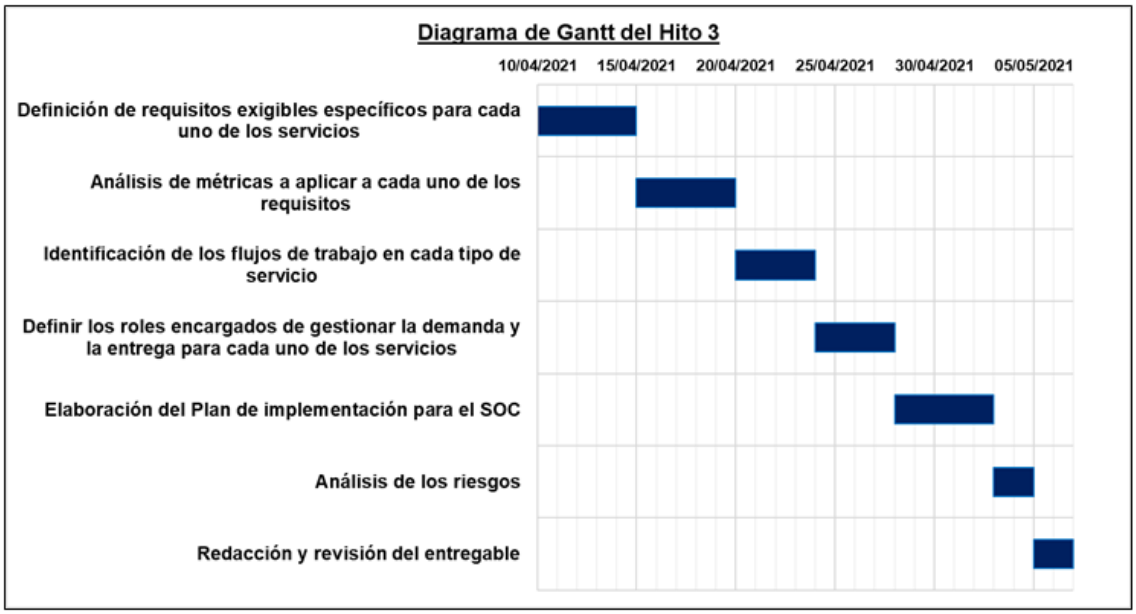

Ilustración 3 - Diagrama de Gantt del Hito 3.

1.4.4 Hito 4: Entrega del Trabajo, de la memoria y su presentación

El hito 4 de este Trabajo se basa en la entrega del Trabajo Final de Grado y su memoria, junto a su presentación y se fundamenta en las siguientes tareas parciales:

1	Corrección de la memoria del Trabajo.
2	Revisión final de la memoria del trabajo.
3	Preparación de la defensa
4	Realizar la presentación virtual de la defensa.
5	Realizar el informe de autoevaluación.

Tabla 9 - Tareas parciales del hito 4.

Por tanto, se determina la siguiente programación temporal para este hito:

	Fecha de inicio	Duración (horas)	Fecha de entrega
Hito 4: Entrega final del trabajo, memoria y presentación.	**08/05/2021**	**72**	**06/06/2021**
Corrección de la memoria del trabajo.	08/05/2021	22	16/05/2021
Revisión final de la memoria del trabajo.	16/05/2021	12	24/05/2021
Preparación de la defensa	24/05/2021	24	02/06/2021
Realizar la presentación virtual de la defensa	02/06/2021	12	04/06/2021
Realizar el informe de autoevaluación.	04/06/2021	2	06/06/2021

Tabla 10 - Planificación temporal del hito 4.

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

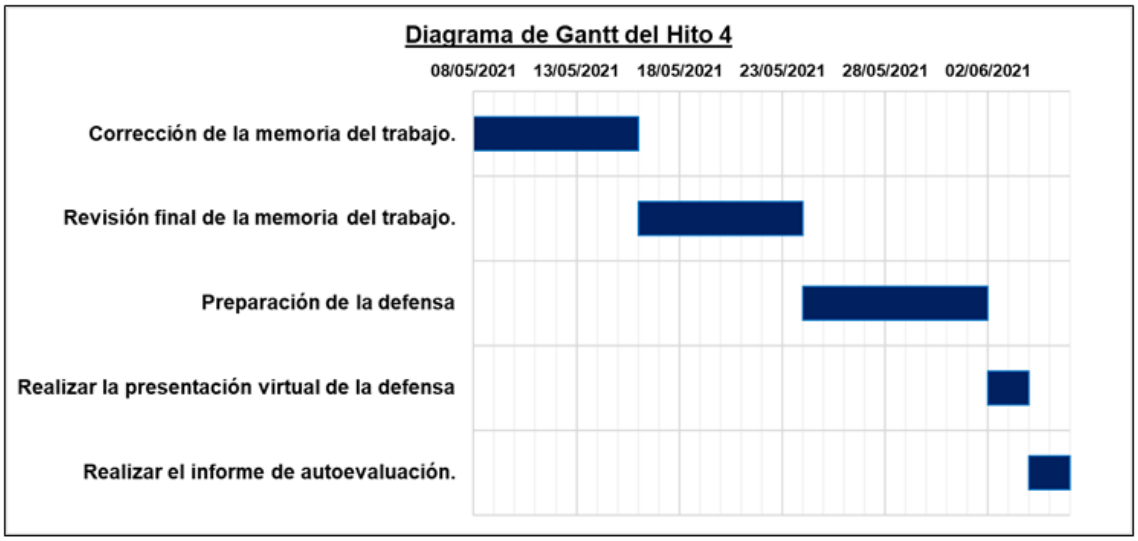

Ilustración 4 - Diagrama de Gantt del Hito 4.

1.4.5 Hito 5: Defensa virtual

El hito 5 de este Trabajo consiste en la defensa virtual del Trabajo Final de Grado ante el Tribunal:

1	Defensa virtual del TFG ante el Tribunal.

Tabla 11 - Tareas parciales del hito 5.

Por tanto, se estipula la siguiente programación temporal:

	Fecha de inicio	Duración (horas)	Fecha de entrega
Hito 5: Defensa virtual	**19/06/2021**	**4**	**21/06/2021**
Realizar la defensa ante el tribunal	19/06/2021	4	21/06/2021

Tabla 12 - Planificación temporal del hito 5.

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

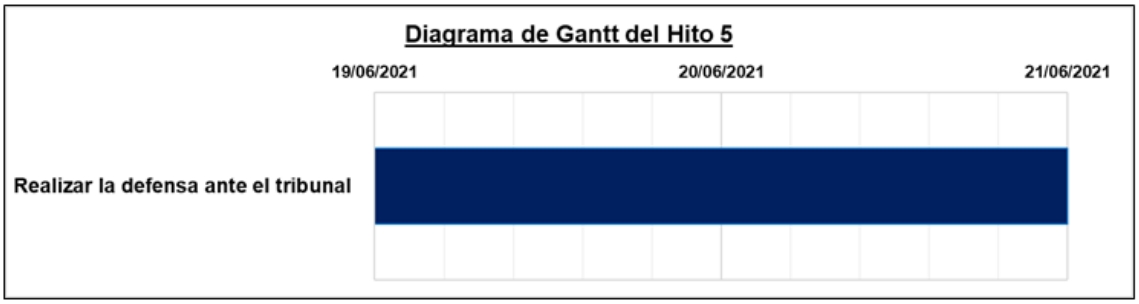

Ilustración 5 - Diagrama de Gantt del Hito 5.

1.4.6 Diagrama de Gantt completo del Trabajo Final de Grado

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

Ilustración 6 - Diagrama de Gantt del TFG.

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

	Fecha de inicio	Duración (horas)	Fecha de entrega
TFG: Diseño de la implementación de un SOC basado en ITIL.	**26/02/2021**	**320**	**21/06/2021**
Hito 1: Plan de Trabajo (PEC1)	26/02/2021	64	12/03/2021
Hito 2: Primera fase de ejecución del plan de trabajo (PEC2)	13/03/2021	88	09/04/2021
Hito 3:Segunda fase de ejecución del plan de trabajo (PEC3)	10/04/2021	92	07/05/2021
Hito 4: Entrega final del trabajo, memoria y presentación.	08/05/2021	72	06/06/2021
Hito 5: Defensa virtual	19/06/2021	4	21/06/2021

Tabla 13 - Planificación temporal del TFG.

1.5 Breve sumario de productos obtenidos

El producto final que se pretende conseguir con este proyecto es el diseño de una guía de implementación para un Centro de Operaciones de Seguridad (SOC) a partir de las buenas prácticas propuestas por ITIL y las metodologías ágiles. Por tanto, los diferentes entregables que se proporcionarán en este trabajo son los siguientes:

- Memoria del trabajo:
  - Análisis de criterios propuestos por la metodología ITIL y las metodologías ágiles ajustados a la implementación de un SOC.
  - Portafolio de Servicios que integran un SOC.
  - Plan de implementación de un SOC (Anexo 1).
- Presentación del trabajo.
- Informe de autoevaluación.

1.6 Breve descripción de los otros capítulos de la memoria

A continuación, se hace una breve descripción de alto nivel de los demás capítulos en los que se desarrolla el proyecto:

1.6.1 Capítulo 2: Análisis de ITIL y metodologías ágiles

En este capítulo se hará un estudio en profundidad de cada una de estos modelos de referencia y metodologías y sus aportes y beneficios para el diseño de una guía de implementación para un Centro de Operaciones de Seguridad (SOC).

1.6.2 Capítulo 3: Centro de Operaciones de Seguridad (SOC)

En este capítulo se tendrán en cuenta los diferentes servicios que brindan los Centros de Operaciones de Seguridad y se establecerán los diferentes indicadores operativos como los requisitos, los roles, el alcance y el flujo de trabajo, entre otros.

1.6.3 Capítulo 4: Conclusiones

En este capítulo se recoge una descripción de las conclusiones del proyecto. Para ello, se indican las lecciones se han aprendido, una reflexión crítica sobre el logro de los objetivos planteados desde el inicio, un análisis crítico del seguimiento de la planificación y metodología y una descripción de las líneas de trabajo abiertas a futuro.

1.6.4 Capítulo 5: Glosario

En este capítulo se recoge la definición de los términos y acrónimos más relevantes utilizados dentro de la Memoria del trabajo.

1.6.5 Capítulo 6: Bibliografía

En este capítulo se engloba el conjunto de referencias bibliográficas utilizado a modo de consulta para el desarrollo del proyecto.

1.6.6 Capítulo 7: Anexos

En este capítulo se congrega el producto resultante de este trabajo, así como el listado de apartados que tienen un carácter autocontenido:

1.6.6.1 Anexo 1: Guía de implementación de un Centro de Operaciones de Seguridad (SOC)

En este anexo se dará respuesta al objetivo general marcado con la entrega de una guía de implementación para el Centro de Operaciones de Seguridad (SOC) a partir de la aplicación de las buenas prácticas ITIL y las metodologías ágiles.

1.6.6.2 Anexo 2: Seguimiento de la PEC2 del TFG

En este anexo se realizará una revisión de los objetivos, el alcance, la planificación, los riesgos del proyecto, así como una valoración del trabajo realizado hasta el momento.

1.6.6.3 Anexo 3: Seguimiento de la PEC3 del TFG

En este anexo se realizará una revisión de los objetivos, el alcance, la planificación, los riesgos del proyecto, así como una valoración del trabajo realizado hasta el momento.

2. Análisis de ITIL y metodologías ágiles

La gestión de servicios de Tecnologías de la Información (TI) centrada en la obtención de la mayor la calidad de los servicios, se apoya en el marco facilitado por ITIL, que le permite implementar mejores prácticas en sus procesos y asegurar entregas de alta calidad. No obstante, en el mercado actual, el enfoque centrado en la satisfacción al cliente requiere velocidad de reacción rápida y eficiente, por lo que los estrictos métodos de ITIL no resultan suficientes para alcanzar los niveles necesarios de competitividad. Ante este contexto, la metodología Agile se considera la solución para agilizar la toma de decisiones y le permite alcanzar mayor precisión y aumentar la productividad en la gestión de servicios TI.

En un principio, ITIL y Agile pueden resultar formas de gestión con principios enfrentados: ITIL ofrece prácticas específicas que permiten optimizar los procesos en busca de la máxima calidad, mientras que Agile flexibiliza los procesos y los adapta a las necesidades de los clientes. No obstante, la combinación de estas metodologías y buenas prácticas puede ser la solución óptima y equilibrada que permita alcanzar la satisfacción del cliente mediante la agilidad en el servicio y sin afectar a su calidad.

2.1 ITIL

Los servicios de Tecnologías de la Información (TI) establecen la relación entre la tecnología, las personas y los procesos de una organización. Desde este enfoque, la gestión de servicios se encarga de concebir a la organización como un sistema interrelacionado de prácticas y recursos organizativos con la finalidad de incrementar la satisfacción del cliente. En consecuencia, se va desde una organización orientada a los productos (en la que existen procesos no coordinados ni administrados) hacia una organización en donde los proveedores de servicios son libres de diseñar procesos a medida para que funcionen en su organización y se apoyen en la mejora continua para generar siempre valor.

Además, la gestión de servicios se encarga de determinar qué procesos necesitan ser mejorados o rediseñados y de establecer sus prioridades. También se ocupa de proveer un ambiente para comenzar y mantener los planes de mejora, en función de los objetivos a alcanzar, y de facilitar la comprensión de la dinámica de los procesos de negocio, bajo el conocimiento de sus fortalezas y debilidades.

ITIL es una biblioteca, un marco de referencia, que contiene la descripción de un conjunto de recomendaciones y buenas prácticas para la administración de servicios de TI. Además, este modelo incluye información sobre los objetivos a alcanzar, las actividades generales, las entradas y las salidas de los procesos que se pueden incorporar a las áreas de TI. Igualmente, el objetivo principal de

ITIL es generar valor en la entrega de servicios mediante la provisión de las buenas prácticas para la Gestión de Servicios de TI.

La siguiente figura muestra el modelo de Sistema de Valor del Servicio propuesto por ITIL:

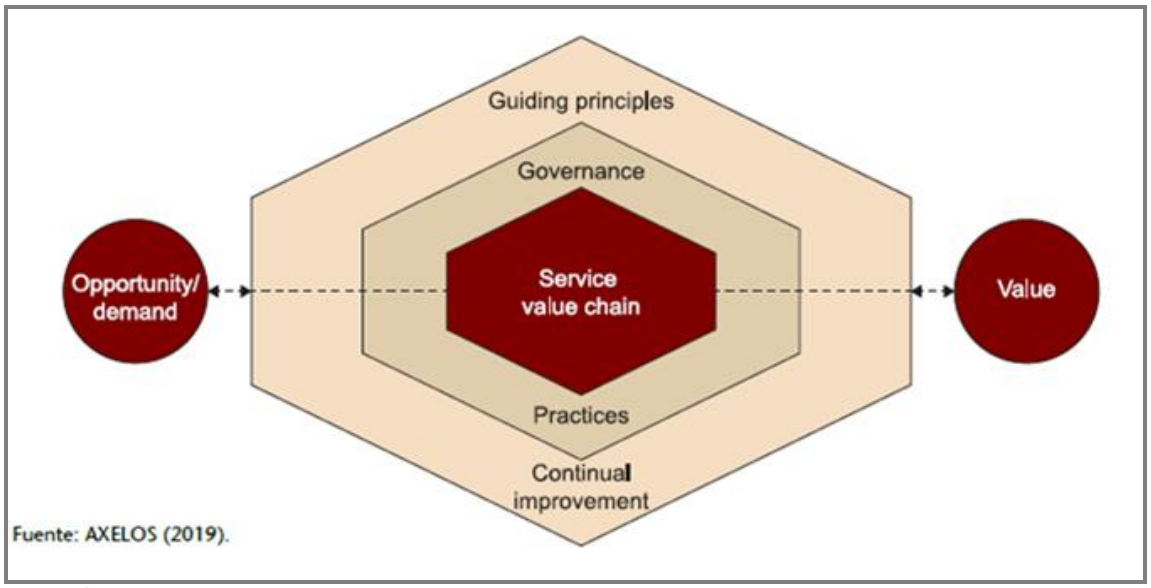

Ilustración 7 - Sistema de Valor del Servicio de ITIL (SVS).

ITIL implica un proceso de cambio organizacional. Por tanto, se requiere énfasis en los siguientes aspectos:

- Compromiso de la alta dirección: Sin el apoyo gerencial sólo se lograrán resultados parciales y no una mejora sostenida a largo plazo.
- Visión de un proyecto formal: Con este punto se hace referencia a la necesidad de asignar recursos materiales, humanos y económicos para poder realizar tareas que implican:
  - Administración del proyecto.
  - Actualización de la documentación de los procesos actuales.
  - Revisión y análisis de los procesos para alinearlos a ITIL.
  - Establecimiento y seguimiento del plan de comunicación interna del proyecto.
- Capacitación empresarial: Todos los niveles de empresa deben recibir formación en relación con lo que es ITIL.
- Participación a todos los niveles: Se trata de un proceso de cambio organizacional, por lo que todos los trabajadores que sean parte de este cambio, deben estar informados e involucrados.

Por consiguiente, con el fin de implementar con éxito el nuevo marco de trabajo, se deben gestionar los servicios de forma holística mientras se considera el contexto estratégico. Para ello, ITIL define un conjunto de prácticas o recursos organizativos diseñados para llevar a cabo la

implementación en la empresa y alcanzar los objetivos fijados. Estas prácticas se agrupan en tres grandes grupos:

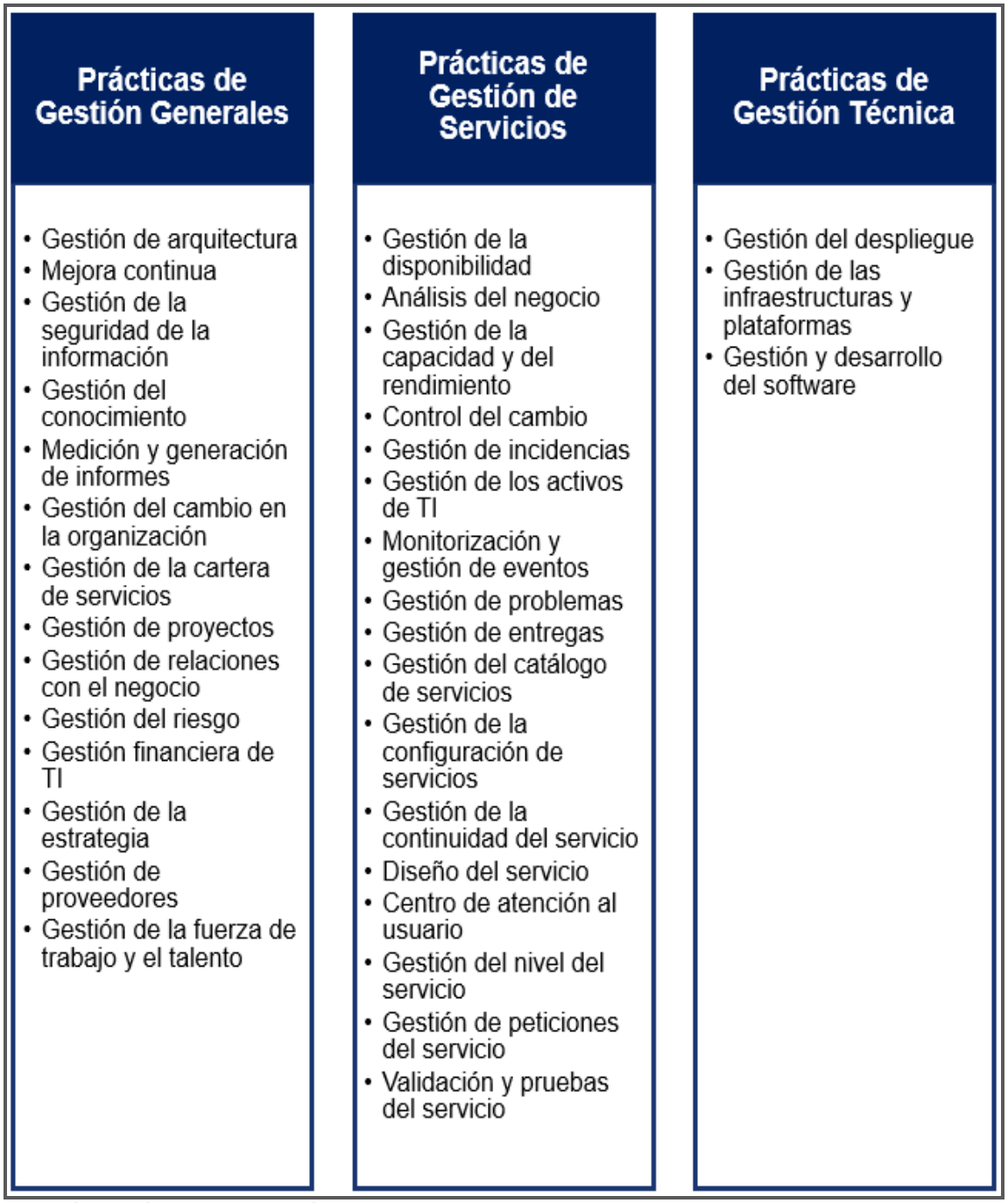

Ilustración 8 - Prácticas de ITIL versión 4.

Asimismo, se debe tener en cuenta que cada una de estas prácticas está basada en cuatro dimensiones, que, a su vez, se ven afectadas por diferentes factores legales, ambientales, económicos, tecnológicos, sociales y políticos. Además, estas dimensiones críticas son los espacios donde se definen los servicios que agregan valor.

Por tanto, el esquema propuesto por ITIL para las cuatro dimensiones de la Gestión del Servicio es el siguiente:

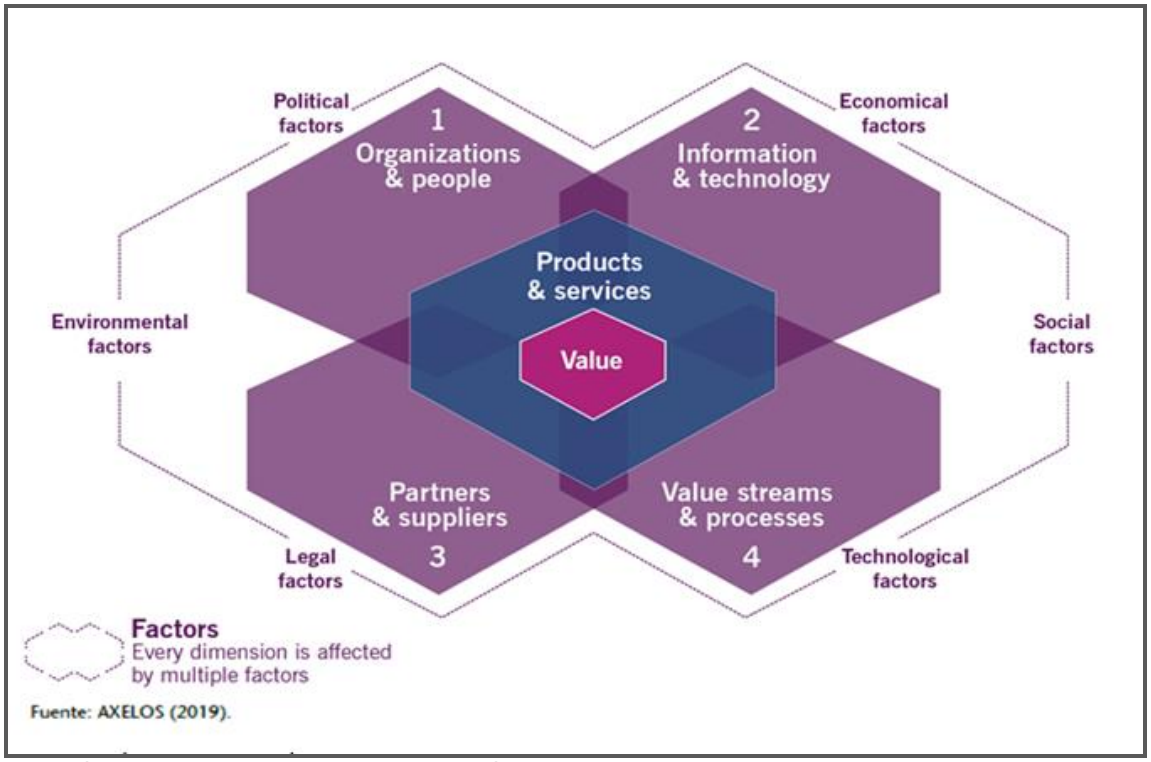

Ilustración 9 - Las cuatro dimensiones de ITIL versión 4.

2.1.1 Aplicación de ITIL en este trabajo

Tras realizar un estudio exhaustivo sobre el valor que otorga ITIL a este proyecto, se establece que esta biblioteca de buenas prácticas se aplique en el diseño del documento guía para la implementación de un Centro de Operaciones de Seguridad (SOC).

Por tanto, los beneficios asociados a la implementación de ITIL son, entre otros, los siguientes:

- Fortalece la comunicación: ofrece un lenguaje común y consistente en función de términos detalladamente definidos y aceptados por las diferentes áreas de la empresa.
- Proporciona un modelo de Gobernabilidad de TI: facilita la obtención de información a través de controles y estructuras que aseguran que el departamento de TI apoye las estrategias empresariales. Además, integra los objetivos del negocio y genera confianza en los indicadores y controles.
- Reduce los costes de TI y mejora de la calidad del Servicio: aquellos procesos de TI con mayor madurez generan mayor productividad y reduzcan los costes.
- Permite implementar procesos integrados en toda el área de TI: define un modelo de procesos sustentados por roles y responsabilidades, los

que generan una nueva forma de trabajo interno de la organización basada en las responsabilidades puntuales.

- Mejora la Integración de TI con el Negocio: el enfoque de Gestión de Servicios de TI permite alinear los servicios TI a los procesos de Negocio.
- Cumple eficientemente con las regulaciones: cumple con la necesidad de las regulaciones locales e internacionales, tales como Sabanes-Oxley (SOX), Base II, regulaciones gubernamentales, ISO/IEC 27001, ISO/IEC 38500 e ISO/IEC 20000, entre otras.
- Mejora la Gestión de proveedores: esclarece los niveles de servicio que se deben solicitar a los clientes.

De manera general, se puede decir que la implementación de ITIL está enfocada para incrementar la satisfacción del cliente, ya que está diseñada para enfocarse a sus necesidades mediante el provecho de la experiencia de los usuarios. De esta manera, aumentar la satisfacción del cliente es lo que genera más valor a la empresa y crea una relación de confianza por cada una de las dimensiones de ITIL indicadas anteriormente:

- Organizaciones y personas.
- Información y tecnología.
- Socios y proveedores.
- Flujos de valores y procesos.

Por tanto, proponer este conjunto de estándares conlleva que los proveedores de servicios puedan entregar los servicios y productos, a la vez que se cumple con los Acuerdos de Nivel de Servicio. Además, se garantiza su verificación por parte de los equipos de soporte para que se puedan restaurar de forma rápida y ágil, a la vez que se minimiza el tiempo en el que haya pérdida de servicio. De esta forma, se garantiza cumplir con las condiciones estipuladas y se puede actuar adecuadamente ante el surgimiento de cualquier inconveniente.

ITIL ofrece oportunidades que permiten la simplificación y estandarización, provee los procesos y modelos que ayudan a los proveedores y facilita la toma de buenas decisiones ante oportunidades de inversión. Por otra parte, la adopción del cambio para el negocio y de la gestión continua de las prácticas de servicio también permiten a la empresa centrar sus objetivos en la entrega de valor al cliente. Asimismo, la definición de los portafolios de servicios permite alcanzar un crecimiento significativo y genera una mayor ventaja competitiva.

En conclusión, los beneficios principales de usar ITIL en el diseño del documento guía para la implementación de un SOC, se resumen en:

- Reducción de los costes de soporte.

- Aumento de la resolución de incidentes a partir de la primera toma de contacto.
- Aumento del valor del catálogo de servicios y reducción de sus costes y riesgos.
- Reducción del tiempo del ciclo de vida de los cambios y proyectos de la organización.
- Aumento de la tasa de éxito de los cambios organizativos y de servicios y productos.
- Reducción del riesgo de cambios no previstos y tardíos.

2.2 Metodologías Ágiles

Las metodologías agiles se sustentan en el desarrollo incremental e iterativo y se caracterizan por tener una planificación adaptativa, un desarrollo iterativo y evolutivo y por dar respuesta rápida a los cambios. Se utilizan para conseguir el servicio, producto o software más funcional posible en el mínimo tiempo, a la vez que se disminuyen los riesgos y permiten, a cualquier proyecto, adaptarse a los cambios rápidamente.

Asimismo, existen diferentes metodologías Ágiles, por lo que, en este análisis se abordarán en profundidad las indicadas en el enfoque y método que se planificó en este proyecto: DevOps, Kanban, Extreme Programming (XP) y SCRUM. Además, también se hace referencia a los criterios por los que estas metodologías se ajustan a la implementación de un Centro de Operaciones de Seguridad y se aplican o se descartan para este fin.

2.2.1 DevOps

DevOps surge de la combinación de las palabras “desarrollo” y “operaciones” en inglés: “*Development* (*Dev*) *& Operations* (*Ops*)”. Este dato sirve como punto de partida para comprender que su significado hace referencia a un conjunto de técnicas, pensamientos y modelos de trabajo de diferentes ámbitos de la gestión de los proyectos.

Por tanto, se puede definir a DevOps como una cultura o como una filosofía colaborativa para la creación de productos y servicios que une principios tanto de Lean como de metodologías ágiles, que se ajusta a las planificaciones y requisitos temporales de los clientes y tiene como objetivo unificar las funciones de desarrollo de software (Dev) y de producción/operación (Ops) en un proceso único, integrado y continuo. Se trata de una dinámica de trabajo que incluye procesos de dos ámbitos entrelazados, pero muy separados hasta el momento.

Además, su ciclo de vida busca la innovación, la monitorización y la mejora continua, por lo que no debe de haber pausas ni retrasos entre iteraciones o

entregas y el desglose de tareas debe de estar automatizado. Su ciclo de vida se basa en la gestión continua y entrega continua con las siguientes etapas:

1. Desarrollo
2. Prueba
3. Integración
4. Despliegue
5. Monitorización

Patrick Debois, uno de los gurús de DevOps, en el año 2012 postuló cuatro ámbitos fundamentales para revelar los aspectos principales de DevOps (Jiménez, 2016):

- Ámbito 1: Propagar la entrega a producción, en donde los equipos de desarrollo y operaciones cooperan con el fin de optimizar la entrega de un proyecto en el entorno de explotación.
- Ámbito 2: Propagar la respuesta del sistema y la información de interés de las operaciones de producción del proyecto en el equipo de desarrollo.
- Ámbito 3: Transmitir la información, el conocimiento y la responsabilidad de los resultados finales del proyecto en el equipo de operaciones.
- Ámbito 4: Involucrar al equipo de operaciones en el comienzo del proyecto para incorporar su experiencia en el equipo de desarrollo.

Debido a esto, Gartner define DevOps como un método para el desarrollo de un producto o software que facilita la comunicación, colaboración e integración entre el equipo de desarrolladores y el equipo de operaciones de una estructura de TI.

Entre los principios del proceso de desarrollo ágil se destaca entregar un producto o software en incrementos pequeños y frecuentes en contraposición con el enfoque "*Big Bang*" del método en cascada (*waterfall*). El objetivo es tener al final de cada sprint un producto o código potencialmente entregable. Esto puede conducir a que, a final de cada sprint, exista un ratio de entrega muy elevado en el despliegue, lo que provoca que surja un cuello de botella en la parte de Operaciones.

De esta forma, Agile constituye un instrumento ideal para recuperar la confianza en el desarrollo de productos y de software, pero relega a un segundo plano la parte de operaciones. Por consiguiente, DevOps nace con la idea de igualar ambos equipos para que esa confianza sea extensible a toda la estructura de TI. Además, modifica el flujo de trabajo entre ambos equipos (desarrollo y operaciones) para facilitar la implantación y despliegue del nuevo producto o código. De esta forma, el uso de prácticas de DevOps contribuye a una mejor eficiencia organizativa.

Esta dinámica de trabajo también repercute en el alcance de beneficios tangibles y permite perseguir objetivos de mayor alcance. DevOps se entiende como una cultura organizativa y no únicamente como un conjunto de herramientas o procesos. Asimismo, su aplicación permite atender elementos relacionados con el trabajo diario, como pueden ser la mejora en la documentación de procesos, la intercomunicación y colaboración entre equipos, el reparto de responsabilidades, etc. Las empresas tecnológicas que aplican prácticas de DevOps obtienen mejoras notables en su rendimiento.

2.2.1.1 Aplicación de DevOps en este trabajo

Es frecuente que las empresas se enfrenten a un problema de desajuste entre los departamentos de desarrollo y operaciones. Por lo general, los equipos de desarrollo de software construyen código a un ritmo acelerado, pero no se responsabilizan del proceso de despliegue, del que se encarga el equipo de operaciones. Como resultado, se obtiene un gran cúmulo de trabajo donde el equipo de operaciones se atasca debido a la cantidad de productos a desplegar.

DevOps propone el uso de prácticas para resolver estas diferencias. Estas prácticas constituyen el valor fundamental por el que se ha decidido tener en cuenta su aplicación en la implementación de un Centro de Operaciones de Seguridad. A continuación, se definen los aportes que ofrece DevOps y por el que se ha escogido como metodología para el desarrollo de este proyecto:

- DevOps ofrece una fuerte estructura de TI que constituye una ventaja competitiva: Las empresas con una estructura organizativa avanzada tienen más probabilidades de aumentar su rendimiento y cuota de mercado, por lo que les permite alcanzar objetivos más ambiciosos.
- DevOps utiliza prácticas que mejoran el rendimiento en TI: Las técnicas de gestión, como son el uso de herramientas para control de versiones o la entrega continua, mejoran el rendimiento de la empresa.
- DevOps otorga importancia a la organización cultural de las empresas: El núcleo central de DevOps apuesta por la adecuada trasmisión de información, la colaboración participativa entre distintos equipos, las responsabilidades compartidas, la interiorización practica de aprender de los errores y dar paso a nuevas ideas. Este tipo de prácticas asegura que la empresa tenga más garantías y posibilidades de obtener buenos resultados, por lo que se considera que la organización cultural es uno de los activos más sólidos a nivel de rendimiento de TI y del rendimiento global de la empresa.
- DevOps propone que la satisfacción en equipos de TI es el principal predictor en una estructura organizativa: Se ha de tener en cuenta que, cuando la satisfacción en el trabajo es alta, los trabajadores dan el máximo de sí mismos, por lo que influye en el grado de compromiso con la empresa, así como en la creatividad y la productividad de su trabajo.

2.2.2 Kanban

Kanban proviene de una palabra japonesa donde “Kan” se traduce como “visual” y “Ban” se corresponde con “tarjeta”, por lo que su significado se asocia con “tarjetas visuales”. De hecho, se trata de una metodología de trabajo muy fácil de utilizar, actualizar y asumir por parte del equipo y en donde su objetivo se fundamenta en la gestión generalizada de la manera en la que se completan las tareas. Además, se destaca que es una técnica de gestión de las tareas muy visual, ya que permite representar el estado de los proyectos y poner pautas en el desarrollo del trabajo de manera efectiva.

Asimismo, esta metodología se sustenta en una serie de principios que la caracterizan y la distinguen del resto de metodologías ágiles:

- Calidad garantizada: Todo lo que se hace, debe salir bien a la primera; no hay margen de error. Es una metodología enfocada en la calidad final de las tareas realizadas.
- Reducción del desperdicio: Kanban propone hacer solamente lo justo y necesario, pero hacerlo bien en base al principio YAGNI, que supone la reducción de todo aquello que es superficial o secundario.
- Mejora continua: Kanban se entiende como un sistema de mejora en el desarrollo de proyectos, en función de los objetivos a alcanzar.
- Flexibilidad: La siguiente actividad a realizar se decide del *backlog* (tareas pendientes acumuladas), que otorgan prioridad según las necesidades del momento. Esto hace de Kanban una metodología capaz de dar respuesta a tareas imprevistas.

La aplicación de la metodología Kanban implica la generación de un tablero de actividades que permitirá mejorar el flujo de trabajo y lograr un ritmo sostenible. Por ello, para implementar esta metodología es necesario tener en cuenta los siguientes aspectos:

- Definir el flujo de trabajo de los proyectos: Para esto es necesario crear un tablero visible y accesible a todos los miembros del equipo. El tablero debe contar con diferentes columnas que se corresponderán con el estado concreto del flujo de tareas.
- Visualizar las fases del ciclo de producción: Kanban se basa en el principio de desarrollo incremental, lo que implica dividir el trabajo en distintas partes, por lo que se agiliza el proceso de producción. El objetivo de la visualización se basa en clarificar al máximo el trabajo a realizar y las tareas asignadas a cada equipo de trabajo, así como definir las prioridades y la meta establecida.
- *Stop starting*, *start finishing*: Kanban prioriza el trabajo que está en curso antes de empezar nuevas tareas. Por esta razón, el trabajo en curso debe estar limitado, por lo que debe existir un número máximo de tareas a realizar en cada fase. No es posible abrir una nueva tarea sin finalizar otra.

- Control del flujo: Kanban mezcla tareas y proyectos, manteniendo a los trabajadores con un flujo de trabajo constante. Se desarrollan las tareas más importantes en cola y se brinda un seguimiento pasivo para no tener que interrumpir al trabajador en cada momento.

2.2.2.1 Aplicación de Kanban en este trabajo

Kanban se basa en el desarrollo incremental, por lo que divide el trabajo en partes. Además, utiliza técnicas visuales para ver la situación de cada tarea, que se representan en tableros de *post-its*. Por otra parte, estos *post-its* pueden tener información variada donde se abarque la descripción y la estimación de la duración de la tarea. Por tanto, la aplicación de Kanban en la implantación de un SOC en cualquier organización puede ser útil para la definición de cada una de las tareas a desarrollar.

Esta metodología permite realizar entregas en cualquier momento, cambiar prioridades y la visualizar el flujo de trabajo. El método Kanban se considera el más indicado para las organizaciones que requieran de flexibilidad en la entrada de tareas, en su seguimiento, en su priorización, en la supervisión del equipo de trabajo y en los informes de dedicación.

Visualizar el flujo de trabajo permite mostrar los logros y problemas del proceso, identificar los diferentes riesgos o problemas que pueden generar cuellos de botellas en el flujo de ejecución (Salvay, s.f.). Es un enfoque para catalizar el cambio en una organización. Utiliza la limitación del “Trabajo en Curso” o “*Work In Progress* (WIP)”, como mecanismo de control para demostrar cuantas actividades por estado pueden ser trabajadas y, de esta forma, incentivar las discusiones de cambio.

El proceso del equipo para el desarrollo de software y productos y la administración de proyectos siempre será único, adaptado a la medida del equipo y optimizado para darle valor al flujo de trabajo. Este proceso implica medición de riesgo, capacidades y habilidades del equipo, demanda del cliente, identificación, corrección de los cuellos de botella y variaciones que pueden afectar al equipo y a sus miembros.

2.2.3 Unión de DevOps y Kanban

Como se ha analizado hasta este punto, DevOps y Kanban constituyen dos metodologías agiles que no se consideran excluyentes, por lo que se tendrá en consideración el valor de cada una ellas en el plan de implementación de un Centro de Operaciones de Seguridad. Por consiguiente, entre los principales beneficios de usar Kanban junto a DevOps, se destaca que Kanban permite combinar múltiples flujos en uno, decir <<no>> a ciertas tareas y mejorar la comunicación visual del flujo de trabajo del equipo.

Asimismo, Kanban determina cuando se alcanzan los límites del WIP (no se puede hacer más tareas, sin sacrificar la productividad), ya que un equipo de

DevOps trabaja, por lo general, en varios proyectos importantes a la vez y puede resultar fácil que algunas tareas se atasquen. Además, Kanban predica el tipo de actitud de “una vez comenzado, debe completarse”, lo que permite que los miembros del equipo identifiquen un problema y trabajen juntos en la finalización de cada tarea para la mejora tanto del flujo como de la comunicación del equipo.

Por último, se destaca que Kanban resulta muy valioso para un equipo de DevOps, desde el punto de vista de la gestión de proyectos y procesos, ya que se considera infinitamente flexible y puede abordar los problemas centrales del equipo de manera cómoda, ligera y discreta. Además, DevOps acerca la transformación cultural y facilita la creación de servicios y productos adaptados a las necesidades cambiantes de los clientes mientras busca agilizar las entregas a los clientes a través de la agilidad y la automatización.

2.2.4 Extreme Programming (XP)

Extreme Programming (XP) se define como un marco de desarrollo de software ágil que tiene como objetivo producir software de calidad a la vez que se da la mayor calidad de vida al equipo de desarrollo. XP se considera el más específico de los marcos ágiles, en relación a las prácticas de ingeniería adecuadas para el desarrollo de software.

Asimismo, según se observa en Agile Alliance (s.f.), XP resulta apropiado para:

- Requisitos de software que cambian dinámicamente.
- Riesgos provocados por proyectos de tiempo fijo que utilizan nueva tecnología.
- Equipo de desarrollo extendido pequeño y co-ubicado.
- La tecnología que está utilizando permite realizar pruebas funcionales y unitarias automatizadas

Debido a la especificidad de XP cuando se trata de su conjunto completo de prácticas de ingeniería de software, existen varias situaciones en las que es posible que no desee practicar completamente XP. De hecho, los cinco valores de XP son:

1. Comunicación: El desarrollo de software es inherentemente a la práctica en equipo, se basa en la comunicación para transferir conocimientos de un miembro del equipo a todos los demás en el equipo. Además, esta metodología enfatiza la importancia del tipo apropiado de comunicación: discusión cara a cara con la ayuda de una pizarra u otro mecanismo de dibujo.
2. Sencillez: El propósito es evitar el desperdicio y hacer solo las cosas absolutamente necesarias, como mantener el diseño del sistema lo más simple posible para que sea más fácil de mantener, respaldar y revisar.

La simplicidad también significa abordar solo los requisitos que se conocen, no intentar predecir el futuro.

3. Realimentación: Mediante la retroalimentación constante sobre sus esfuerzos anteriores, los equipos pueden identificar áreas de mejora y revisar sus prácticas. La retroalimentación también admite un diseño simple. El equipo realiza una tarea, genera comentarios sobre su diseño e implementación y, finalmente, adapta su producto en el futuro.
4. Coraje: Necesita coraje para plantear problemas organizativos que reducen la eficacia de su equipo, para dejar de hacer algo que no funciona e intentar otra cosa y para aceptar los comentarios y actuar sobre ellos, incluso cuando sea difícil de aceptar.
5. Respeto: Los miembros de su equipo deben respetarse entre sí para comunicarse entre sí, proporcionar y aceptar comentarios que honren su relación y trabajar juntos para identificar diseños y soluciones simples.

El eje de XP se basa en la interconexión del conjunto de las prácticas de desarrollo de software. Si bien es posible realizar estas prácticas de forma aislada, muchos equipos han descubierto que algunas prácticas refuerzan a las demás y deben realizarse en conjunto para eliminar por completo los riesgos a los que se enfrenta a menudo en el desarrollo de software. Además, se trata de una metodología con reglas simples que se fundamentan en valores y bases sólidas:

- Planificación: en la etapa de planificación se escriben historias de usuarios, que se utilizan para crear estimaciones de tiempo para la reunión de planificación de lanzamientos. En esta etapa, los desarrolladores suelen lanzar pequeñas versiones iterativas del sistema a los clientes. Además, el proyecto se divide en iteraciones y las iteraciones están programadas entre una y tres semanas de duración.
- Gestión: esta regla requiere que el espacio de trabajo esté abierto y que se eliminen las barreras, como los cubículos que dividen a las personas. Se entiende que establecer el ritmo es tener el software más completo y listo para producción en cada iteración, por lo que requiere que las personas se muevan para evitar una pérdida grave de conocimientos y cuellos de botella de codificación. Además, se sacrifica una gran cantidad de tiempo del desarrollador para obtener una cantidad trivial de comunicación.
- Diseño: esta regla requiere que el diseño de un modelo sea simple. Un modelo simple siempre tarda menos en terminar que uno complejo.
- Codificación: esta regla requiere que el cliente siempre esté disponible, no sólo para ayudar al equipo de desarrollo, sino también para ser parte de él. Esta regla también requiere que el código se escriba según los estándares acordados.
- Pruebas: todo el código debe someterse a pruebas unitarias, que son las piedras angulares de los proyectos. Cuando se encuentra un error, se crean pruebas para evitar que vuelva a aparecer. Además, las pruebas

de aceptación se crean a partir de historias de usuarios. Durante la iteración, las historias de usuario seleccionadas durante la reunión de planificación de la iteración se traducirán en pruebas de aceptación.

2.2.4.1 Descarte de Extreme Programming (XP) de este trabajo

Aunque es cierto que con grupos de más de una treintena de programadores ha tenido éxito en algunos proyectos, Extreme Programming (XP) se considera una metodología ideada para grupos más reducidos y que comprendan entre dos y doce desarrolladores. Por tanto, no se recomienda usar esta metodología en proyectos con gran cantidad de personal. Además, debe tenerse en cuenta que, en proyectos con requerimientos cambiantes, dinámicos y de gran riesgo, se debe tener en cuenta la posibilidad de que un equipo reducido de programadores que usen la metodología XP sea más efectivo que un equipo grande de todos modos.

Por otra parte, XP requiere de un equipo de desarrollo extendido, que no sólo incluya a los desarrolladores, sino también a todas las partes interesadas, como son la dirección y a los clientes, para que trabajen en conjunto. Esto es debido a que acciones como hacer preguntas, negociar el alcance y los cronogramas y crear pruebas funcionales requiere algo más que la mera participación de los desarrolladores en la producción del software.

Asimismo, este método de gestión de proyectos debe poder crear pruebas unitarias y funcionales automatizadas, por lo que requiere obtener experiencia a través de pruebas en algunos entornos. Además, debido a que el objetivo real se basa en entregar el software que se necesita cuando se necesita, se posibilita el cambio del diseño en el sistema de trabajo para facilitar estas pruebas.

Extreme Programming se centra en el desarrollo de software con énfasis los procesos adaptables por encima de la previsión de incidentes. Por ello, los defensores de XP exponen que los accidentes, fallos o inconvenientes que acontecen durante un proyecto son elementos naturales. Se debe saber adaptar el proceso antes que hacer por suspenderlo y por poner en riesgo sus resultados.

En conclusión, a pesar de las ventajas que puede aportar esta metodología de trabajo en la implantación de un SOC, se destaca que XP se enfoca en el desarrollo de software y no en la integración de otros servicios, por lo que queda fuera del ámbito de este proyecto. Debido a esto, se descarta el uso de esta metodología en el desarrollo del trabajo.

2.2.5 Scrum

Scrum se define como un marco de proceso que se utiliza para gestionar el desarrollo de productos y otros trabajos de conocimiento. Además, resulta empírico, ya que proporciona un medio para que los equipos establezcan una

hipótesis de cómo creen que funciona algo, lo prueben, reflexionen sobre la experiencia adquirida y realicen los ajustes necesarios. Scrum está estructurado de manera que permite a los equipos incorporar prácticas de otras metodologías, donde tengan sentido para el contexto del equipo.

Esta metodología se considera la más adecuada cuando un equipo multifuncional esté trabajando en un entorno de desarrollo de productos donde se localiza gran cantidad de trabajo sustancial, que puede concluir en dos o más iteraciones de entre 2 a 4 semanas. Además, según se observa en Agile Alliance (s.f.), se espera que los equipos que siguen a SCRUM aprendan y exploren los siguientes valores:

- Compromiso: Cada integrante del equipo se compromete por sí mismo a conseguir los objetivos del equipo.
- Coraje: Los integrantes del equipo asumen los problemas difíciles en busca de su solución.
- Enfoque: Los integrantes del equipo se centran en las tareas definidas para el sprint y para los objetivos del equipo.
- Franqueza: Los integrantes del equipo y todas las partes interesadas (*stakeholders*, en inglés) se encuentran receptivos ante todas las tareas y aquellos retos que afronta el equipo.
- Respeto: Los integrantes del equipo se honran como iguales entre sí, con el fin de sentirse competentes e autónomas.

Por otra parte, los siguientes principios sustentan la naturaleza empírica de esta metodología:

- Transparencia: Se debe trabajar en un entorno en donde todos los integrantes del equipo tengan conocimiento de los problemas a los que se enfrentan sus compañeros.
- Inspección: Se deben realizar inspecciones periódicas dentro del marco de trabajo para permitir al equipo que analice el funcionamiento de los procesos. Entre otros, se deben incluir reuniones diarias y reuniones de revisión de cada *sprint*.
- Adaptación: Se debe plantear en todo momento el estado y la situación de los hitos y revisar las tareas que se puedan desecharse.

Scrum fracciona el desarrollo de los productos en *sprints*. De hecho, un *sprint* es un periodo de tiempo de aproximadamente algo menos de un mes en el que el equipo produce un incremento viable del producto resultante. Un equipo comienza un *sprint* con una discusión en la que se determinan los elementos de la cartera de productos con los se trabajará y finaliza, como resultado final de la planificación del sprint, con el *Sprint Backlog*.

La planificación de *sprint*, generalmente, ocurre en dos segmentos. En un primer segmento, se acuerdan, entre el dueño del producto y todos los

miembros del equipo, los elementos del portfolio que se incluirán en el *sprint*. En un segundo segmento, el equipo establece la manera en la que se entregarán los elementos del portfolio que se determinen como un incremento del producto que se considere preparado. Por consiguiente, los elementos del portfolio que se estipulen para la entrega con éxito componen el *Sprint Backlog*.

Por tanto, el dueño del producto y todos los miembros del equipo determinan el alcance del *sprint*, que se define en los epígrafes de la lista de tareas pendientes del producto de forma cerrada, por lo que no se permite añadir más elementos al *Sprint Backlog*. Gracias a esta medida, se protege al equipo de realizar cambios en el alcance del propio *sprint*.

Scrum determina el rol de dueño del producto con el fin de afrontar los retos a los que se enfrentaban los equipos de desarrollo de productos que tienen diferentes directrices o no tienen ninguna en relación con el desarrollo de los objetivos. Por otra parte, el equipo de desarrollo se compone por los técnicos que facilitan el incremento del producto en un sprint. Por esta razón, su principal responsabilidad se centra en la entrega del incremento que da valor en cada sprint.

Este marco de trabajo, además, da flexibilidad a los equipos de desarrollo para dar respuesta ante los cambios. Además, dispone de diferentes puntos de control con los que se garantice la correcta alineación del equipo con los objetivos deseados, así como con la identificación de los problemas, con el fin de dales solución, y la adaptación del proceso para que se ejecute en la fase de esfuerzo. En definitiva, todos los trabajos necesarios para el desarrollo del producto se dividen en diferentes *sprints* como subconjuntos del propio producto final.

2.2.5.1 Descarte de Scrum en este trabajo

La contribución más importante de Scrum en el ámbito del desarrollo de software se enfoca en la simplicidad y la efectividad de la gestión del trabajo de un equipo colaborativo diseñado para el desarrollo de productos. Además, proporciona un marco de trabajo y un conjunto de reglas que facilitan una planificación adecuada, un control del trabajo y el reconocimiento, la mitigación y la resolución de riesgos y problemas.

Asimismo, aunque Scrum se define como una metodología de trabajo para el desarrollo ágil de software, otros sectores han empezado a implantar este método de trabajo en sus modelos de organización para aprovecharse de sus beneficios. También resulta útil para los proyectos en donde sea necesario intervenir en el proceso porque, entre otras, los equipos muestran índices de rendimiento bajo, la calidad del producto resultante sea inferior al deseado, se obtengan altos costes o las entregas de los productos finales se prolonguen en el tiempo más de lo deseado.

Sin embargo, pese a los beneficios que pueda aportar esta metodología de trabajo en la implantación de un SOC, se destaca que, sobre todo, tiene un

mejor rendimiento con equipos reducidos, se tienen que definir los hitos y su planificación con exactitud y los miembros de los equipos deben tener un nivel formativo alto sobre su funcionamiento. Por tanto, dado que las iteraciones son la esencia de esta metodología, las grandes organizaciones deben estar divididas en sectores con objetivos concretos y la implantación de este servicio requiere de expertos en ciberseguridad y no en la gestión de proyectos bajo este método de trabajo, no se obtendrán los resultados deseados si se necesita realizar un reajuste entre los procesos de Scrum y el proyecto.

Como consecuencia de lo indicado anteriormente y que se considera muy probable tener la necesidad de realizar reajustes entre los procesos del marco de trabajo y el propio proyecto, se descarta el uso de esta metodología en la implantación del SOC. Debido a esto, se excluye Scrum en el desarrollo del trabajo.

3. Centro de Operaciones de Seguridad (SOC)

Un Centro de Operaciones de Seguridad (SOC - *Security Operations Center*, por sus siglas en inglés) se define como un equipo de trabajo centralizado que se dedica a los aspectos tácticos y operativos asociados con la ciberseguridad de una organización. Debido a esto, esta unidad técnica realiza labores orientadas a la monitorización, protección y defensa de los activos de información en tiempo real, a través de equipos tecnológicos y de personal especializado y centralizado, y se encarga de los servicios de detección y reacción ante incidentes de seguridad en la entidad en la que trabaje.

Asimismo, el diseño de la guía de implementación de un SOC indicado en este trabajo, se ha guiar en base a las buenas prácticas ITIL, para asegurar su adecuada implementación. Esto supone un modelo de procesos que depende del ciclo de vida de los sistemas y de los servicios relacionados con las Tecnologías de Información. Por consiguiente, los pasos a seguir para el proceso de implementación de ITIL son:

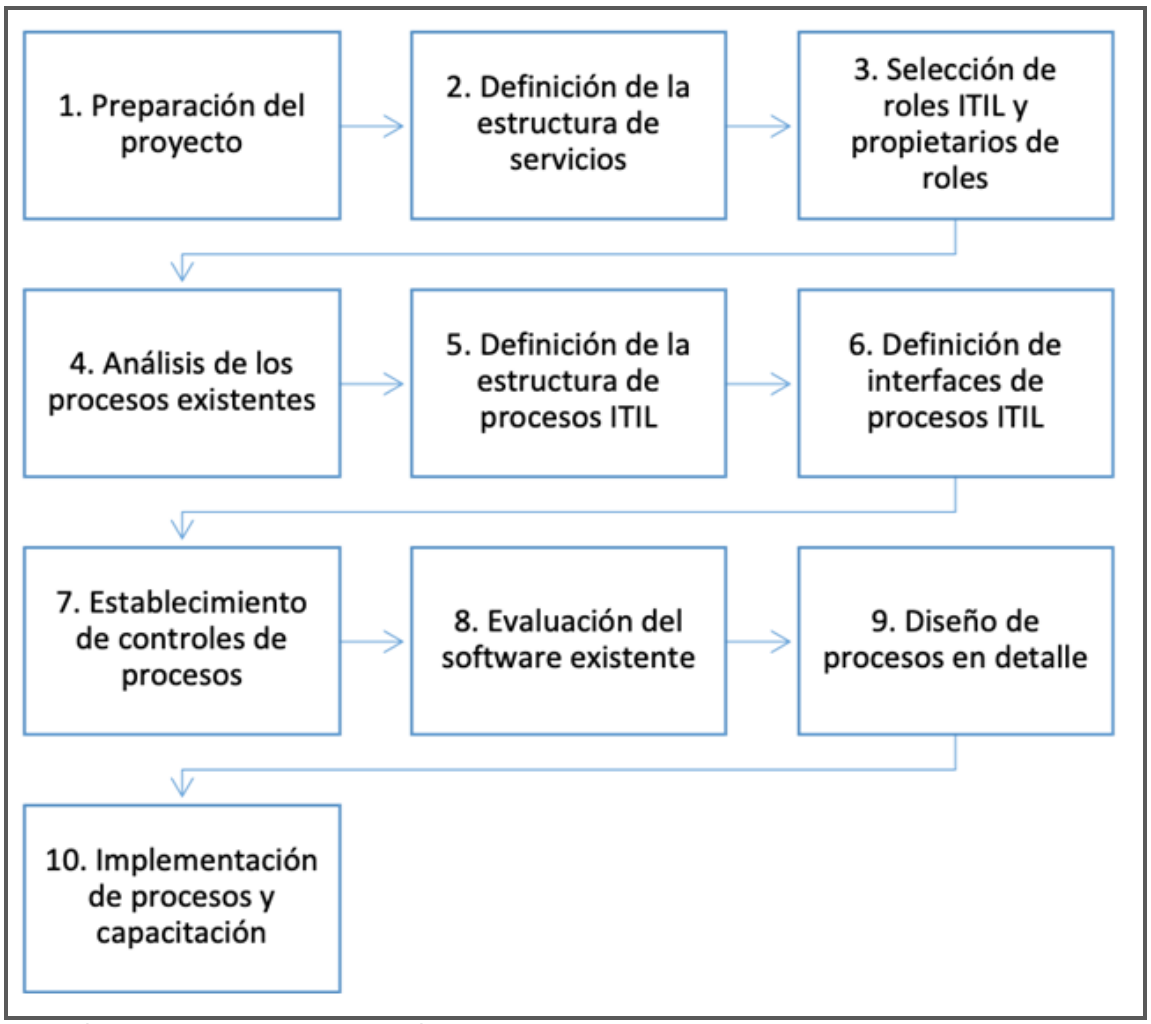

Ilustración 10 - Pasos para la implementación de ITIL en el SOC.

Por otra parte, dada su naturaleza y fin, el SOC se debe de encargar de los siguientes aspectos:

- Monitorización, análisis, alerta y respuesta ante incidentes de ciberseguridad, mediante la utilización de las tecnologías existentes en la organización y de la incorporación de las capacidades necesarias.
- Administración de las tecnologías de ciberseguridad, en donde se delegan las tareas de monitorización continua, actualización y mantenimiento de sus configuraciones óptimas en el personal de los Centros de Operaciones con el nivel de conocimiento adecuado.
- Gestión de la seguridad de la información de los puestos de trabajo y de los entornos de servidores.
- Servicios de respuesta ante incidentes de seguridad informática que se realicen por el equipo de ciberseguridad especializado en la contención, remediación y análisis de situaciones críticas de este ámbito.
- Gestión de vulnerabilidades, en donde se debe ser capaz de minimizar la ventana de exposición de los sistemas informáticos y permitir la detección de aquellos elementos que tienen vulnerabilidades y que podrían ser explotables por un atacante.

Se destaca que todo Centro de Operaciones de Seguridad debe cumplir con los requerimientos legales nacionales, así como con los estándares internacionales. Además, debe respetar las políticas y reglas de negocio determinadas por la Alta Dirección de la organización para la que trabaje. De hecho, la normativa interna o externa, nacional o internacional, debe regir la implementación de procesos y procedimientos que regulen las actividades del personal.

La estandarización de los procesos busca reducir y eliminar la variabilidad del resultado de las actividades llevadas a cabo, por lo que permite que el producto o servicio que entregan los procesos sea siempre el mismo. Además, resulta importante resaltar que este proceso de estandarización implica la realización del análisis de la situación actual, de la identificación de las herramientas y personas involucradas y del consenso de las actividades y su secuenciación, por lo que permite la elaboración de un documento formal. Debido a esto, la documentación obtenida permite realizar procesos de mejora continua a través de la medición y el análisis de diferentes indicadores.

A continuación, se presentan los procesos que se han definido como parte de la gestión del SOC. Se resalta que, a menudo, las organizaciones no documentan todos los procesos que identifican los especialistas de ciberseguridad. No obstante, su identificación resulta útil para ilustrar las tareas y operaciones que se pueden realizar en este servicio.

Por consiguiente, la exposición de servicios que brinda el Centro de Operaciones de Seguridad permite a la organización trabajar de forma organizada. Así, en atención a esta demanda, se definen los siguientes servicios y procesos que se contemplan para el SOC:

3.1 Servicio de Gestión de eventos e incidentes

El servicio de gestión de eventos e incidentes de seguridad se nutrirá fundamentalmente de la información proveniente de las herramientas de seguridad implantadas en la organización. Asimismo, se empleará la información suministrada directamente por el cliente y los usuarios de la organización.

La sofisticación de los ataques no ha parado de crecer en los últimos años. A las diversas técnicas de explotación y ataque, se le unen técnicas de ocultación que dificultan la detección de los incidentes, de manera que pueden pasar inadvertidos durante más tiempo. Por tanto, para contrarrestar esta dinámica, se deberán implantar estrategias de análisis basadas en la cadena *Cyber Kill Chain*, que descompone los ataques en las siete etapas que un atacante debe seguir sucesivamente para poder tener éxito:

Ilustración 11 - Etapas del atacante según la cadena Cyber Kill Chain según Lockheed Martin.

Para ello, el SOC deberá llevar a cabo acciones de detección y respuesta para posibilitar la detección de los ataques en varias de estas etapas. Esta estrategia, a la vez que mejora el nivel de detección y reduce el impacto, limita la posibilidad de que el atacante retome la actividad en otra etapa de la cadena de ataque. Por tanto, el SOC se deberá valer del análisis e identificación de patrones de ataque para identificar y prevenir modos de actuación en el futuro.

La implantación de las nuevas reglas de correlación seguirá un proceso ordenado de gestión en espiral, de modo que se obtengan resultados lo antes posible, a la vez que se adaptan y mejoran los casos a la situación de la infraestructura. Este modelo proporciona una gestión eficaz de los paquetes de correlación, al mismo tiempo que disminuye la ocurrencia de falsos positivos.

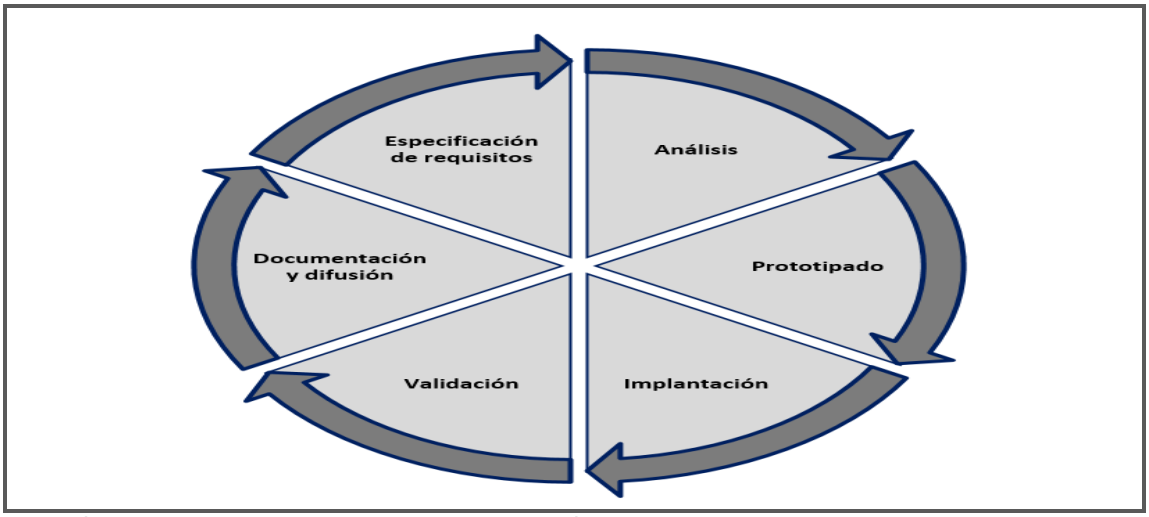

Ilustración 12 - Proceso de desarrollo de reglas de correlación.

Asimismo, los procesos de este servicio se definirán asegurando que la transición entre las distintas tareas se presenta de modo que, especialmente, en caso de un incidente informático real, todo el personal del SOC sepa cuál es su responsabilidad y cómo encaja en el proceso de principio a fin, siguiendo las metodologías presentadas en puntos anteriores. Asimismo, se definirán las actividades periódicas a realizar, así como *checklists* y los modelos de informe necesarios, para la correcta ejecución de los procesos siguiendo las directrices del cliente. Para ello, el SOC empleará las herramientas dispuestas por el cliente a lo largo de todo el ciclo de vida del incidente, por lo que será necesario proporcionar acceso a todos sus miembros a las herramientas y consolas necesarias de la organización.

Los procesos previstos para el servicio de gestión de eventos e incidentes de seguridad son los siguientes:

Servicio de gestión de eventos e incidentes	Monitorización de eventos
	Clasificación y triaje de eventos
	Investigación
	Registro de incidentes
	Escalado interno de incidentes
	Escalado externo de incidentes
	Recogida de muestras y evidencias
	Respuesta ante incidentes
	Notificación de incidentes
	Seguimiento de incidentes
	Análisis post-incidente

Ilustración 13 - Procesos del servicio de gestión de eventos e incidentes de seguridad.

Tal y como se ha comentado, el servicio se llevará a cabo en base a los procedimientos de gestión de eventos e incidentes de seguridad ya implantados por la organización y mediante la articulación y supervisión de las medidas necesarias entre los distintos grupos responsables de los activos afectados. Por ello, en relación a la gestión de incidentes, se propone un modelo de trabajo ampliamente extendido en otras organizaciones de similares características. Las actividades del SOC se deberán distribuir en base a un proceso de detección, priorización y resolución de incidentes mediante una organización multi-nivel compuesta por la siguiente estructura:

- Nivel 1: Equipo técnico de analistas de seguridad que realicen las siguientes acciones:
    - Registro y triaje de eventos.
    - Remediación ágil y rápida a través de procedimientos definidos y aprobados.
    - Escalado, en su caso, al nivel 2.
- Nivel 2: Equipo técnico de especialistas de seguridad con capacidad para el tratamiento y resolución de incidencias más complejas y, en su caso, escalado al nivel 3.

- Nivel 3: Equipo de técnico de ingenieros de seguridad que se encargue de:
    - Análisis avanzado.
    - *Threathunting* proactivo.
    - Forense avanzado (análisis detallado de los medios digitales de manera válida a efectos legales, con el objetivo de identificar, preservar y analizar artefactos en dichos medios y de presentar conclusiones acerca de la información digital que contenga).
    - Escalado, en su caso, al nivel 4.
- Nivel 4: Jefe del SOC (CISO), que se encarga de la gestión, responsabilidades y dirección del servicio y de enlace con la alta dirección de la organización.

Este modelo de trabajo permite priorizar aquellas amenazas que, por su relevancia o naturaleza, puedan impactar en mayor grado en la organización, al tiempo que optimiza el uso de los recursos humanos disponibles. Se trata de una estructura prácticamente piramidal en cuanto a responsabilidades.

Asimismo, la respuesta ante incidentes se considera una de las tareas más reconocida y visible del SOC. Su realización consistente y efectiva demanda procesos y procedimientos. De hecho, el proceso de gestión de incidentes de seguridad guarda relación con el proceso de gestión de incidentes de TI, por lo que se consideran las actividades de detección, investigación, contención y recuperación, encaminadas a minimizar el impacto y asegurar la continuidad operativa.

En este caso, los procedimientos de investigación son dependientes del proceso de gestión de incidentes de seguridad, a partir de los cuales se establecen los pasos que los analistas deben efectuar en dependencia del tipo de incidente que se trate. Los procedimientos deben ser redactados una vez que se hayan podido modelar los tipos de incidentes, con el fin de identificar la mejor respuesta.

Por consiguiente, pueden darse casos en que los incidentes que son detectados, no son casos de uso previamente configurados por el personal del SOC, por lo que se puede confeccionar un proceso de retroalimentación con el objetivo de actualizar la base de datos de conocimiento de los casos de uso, las alertas, etc., que permita detectar a futuro las situaciones previamente no detectadas. De esta forma, se pueden reconfigurar y optimizar los dispositivos de detección existentes.

Para definir un procedimiento ágil en la gestión y respuesta ante incidentes de seguridad, se hace necesario establecer los puntos que serán utilizados ante un caso de incidente. Por tanto, algunas herramientas y recursos para la gestión de eventos e incidentes son las siguientes:

3.1.1 Herramientas para manejar las comunicaciones durante la gestión de eventos e incidentes

Estas herramientas determinan los medios que serán utilizados para establecer la comunicación durante la gestión del evento o incidente en los diferentes grupos de trabajo. Algunos ejemplos de estas herramientas son:

- Información de la asignación y escalada a las diferentes áreas de la organización.
- Mecanismos de reporte de la presencia de un incidente a las personas involucradas (correo electrónico, vía telefónica, sistema gestor de incidentes, etc.).
- Herramienta de seguimiento de tickets relacionados con el incidente.
- Instalaciones de almacenamiento de seguridad para salvaguardar la información sensible y las evidencias de seguridad obtenidas del proceso de esta gestión.

3.1.2 Herramientas de hardware y software para analizar los eventos e incidentes

Se trata de todas las herramientas tecnológicas que sean necesarias para la gestión de los incidentes. Algunos ejemplos de estas herramientas son:

- Hardware necesario (equipos de sobremesa, portátiles, impresoras, servidores, *tablets*, dispositivos de red, dispositivos de almacenamiento extraíble, estaciones de trabajo especializadas, etc.)
- Herramientas informáticas para el análisis de protocolos de comunicación.
- Herramientas forenses digitales para el análisis de discos y otras actividades.

3.1.3 Recursos de información para el análisis de eventos e incidentes

Se trata de recursos destinadas a la compilación de información actualizada y legible para la revisión durante la gestión del incidente. Algunos ejemplos de estos recursos son:

- Documentación de sistemas operativos, aplicaciones, detección de intrusos y protocolos antivirus.
- Listado de activos críticos.
- Diagrama de red de la empresa.
- Líneas de las configuraciones actualizadas de los Sistemas Operativos, dispositivos de red, aplicaciones, etc.

Asimismo, para que el proceso de gestión de incidentes sea eficaz, se hace necesario priorizar todos los casos trabajados. Por tanto, se recomienda que, como parte de su gestión, se registren en una base de conocimientos. De esta manera, se posibilita tener en cuenta los siguientes elementos:

- Impacto funcional: se refiere a la influencia del incidente en las funciones del negocio y el impacto que tendría en el caso de no ser solucionado de forma rápida.
- Impacto sobre la información: se refiere a la influencia del incidente en la información organizacional a nivel de clientes, empleados y empresa en general. Se relaciona con la información crítica que se compromete.
- Recuperación: se refiere al tamaño del incidente y los recursos afectados. Se debe determinar el tiempo, el esfuerzo que requerirá la recuperación ante los daños y el costo de este proceso.

3.2 Servicio de Alerta Temprana

El servicio se integrará con los procedimientos de gestión de vulnerabilidades ya implantados por la organización y a partir de los principios de priorización, prontitud, eficacia y máxima utilidad. Para ello, la información de interés seguirá un proceso de análisis y priorización, de forma que se aporte información enriquecida antes de que se produzca.

El servicio de alerta temprana se deberá alimentar de múltiples fuentes de información, tanto de carácter público como privado, para recibir alertas e información de interés. Las principales fuentes, con reconocimiento mundial y según cada caso, son las indicadas a continuación:

Catálogo MITRE (CVSS)	Canada CERT Public Safety
National Vulnerability Database	ICS CERT
CCN-CERT	NCSC-FI (Finlandia)
INCIBE Cert	Packetstorm
CERT-EU	SANS (Internet Storm Center Diary)
US CERT	McAfee Critical Infrastructure Protection
Open Source Vulnerability Database	ThreatPost
Trend Micro Security Intelligence	Zscaler Alerts
Hipasec	Google Security Blogs
Microsoft Security Advisories	Kaspersky Daily
StormShield Security Watch	Sophos Naked Security
Cisco Security Advisories	Symantec Security Focus
Microsoft Security Bulletins	Carnegie Mellon University CERT
NCSA (National CyberSecurity Alliance)	FireEye TaoSecurity

Tabla 14 - Fuentes propuestas para el servicio de Alerta Temprana.

Respecto a las tecnologías aplicables en cada momento, el equipo de trabajo del servicio será responsable de consensuar un listado de activos, tanto software como hardware, con el cliente. Para el levantamiento del inventario se pueden utilizar procedimientos manuales (creación de un listado detallado) o automático (utilización de herramientas de descubrimiento). El servicio será más o menos eficaz, en la medida en que sea posible obtener con precisión el detalle de las versiones desplegadas en cada momento en el parque de la organización. Para ello, el cliente deberá suministrar a los miembros del SOC el acceso a la información o a las herramientas que permitan determinar dicha información.

El inventario debe ser una buena fuente de información puesto que el análisis se ciñe a los activos contenidos en la lista, y cargados en el sistema. Todos aquellos activos no existentes en el inventario no serán contemplados en el análisis de alerta temprana. Las tecnologías en el alcance se podrán ver incrementadas a medida que se vayan adoptando por la organización. En cualquier caso, y para la correcta gestión de los cambios tecnológicos y su incorporación al sistema de alerta temprana, será necesario la notificación a los miembros del SOC por lo que, al margen del uso de herramientas de descubrimiento (manual o automático), se sugiere la inclusión de un representante del SOC en aquellos comités o procesos de cambio relacionados.

El servicio de alerta temprana se prestará de manera continua con una periodicidad diaria durante una franja de la jornada laboral, según el calendario laboral y las necesidades de la seguridad. Para ello, el Coordinador del SOC designará diariamente a un miembro del equipo como gestor de la alerta temprana, que realizará los procesos de identificación, validación, clasificación, triaje, registro y notificación al equipo técnico responsable de las nuevas vulnerabilidades que afecten a la infraestructura corporativa. Así mismo, el gestor designado realizará la depuración y envío de noticias e información de interés, guías técnicas e informes relacionados con la actualidad de la ciberseguridad, bajo las directrices del Coordinador del SOC. Sin perjuicio de dichas directrices, en cualquier momento el cliente podrá priorizar las tecnologías y/o sistemas sobre los que deban reportarse vulnerabilidades.

Por otro lado, el gestor de la alerta temprana realizará el seguimiento del estado de las vulnerabilidades pendientes, reflejando dicho estado en un informe de seguimiento semanal. Para ello, el SOC mantendrá un registro del estado de las vulnerabilidades notificadas. Esto, además, mantiene la continuidad de las tareas asociadas a la gestión de la alerta entre distintos turnos, especialmente útil para aquellas alertas que se encuentren bajo análisis, por su mayor volumen de análisis o por la incertidumbre sobre su aplicabilidad real, y que puedan requerir más de una franja diaria para su completa gestión.

Los procesos previstos para el servicio de Alerta Temprana son los siguientes:

Servicio de alerta temprana.	Identificación y validación de alertas
	Clasificación y triaje de alertas
	Registro y notificación de alertas
	Actualización de alertas
	Seguimiento de alertas

Ilustración 14 - Procesos del servicio de Alerta Temprana.

Asimismo, los procesos de este servicio se definirán asegurando que la transición entre las distintas tareas se presenta de modo que todo el personal del SOC sepa cuál es su responsabilidad y cómo encaja en el proceso de principio a fin, siguiendo las metodologías presentadas en puntos anteriores. Asimismo, se definirán las actividades periódicas a realizar, así como *checklists* y los modelos de informe necesarios, para la correcta ejecución de los procesos siguiendo las directrices del cliente.

En referencia a las nuevas vulnerabilidades sobre las tecnologías desplegadas en el parque de la organización, se seguirá el siguiente flujo orientativo:

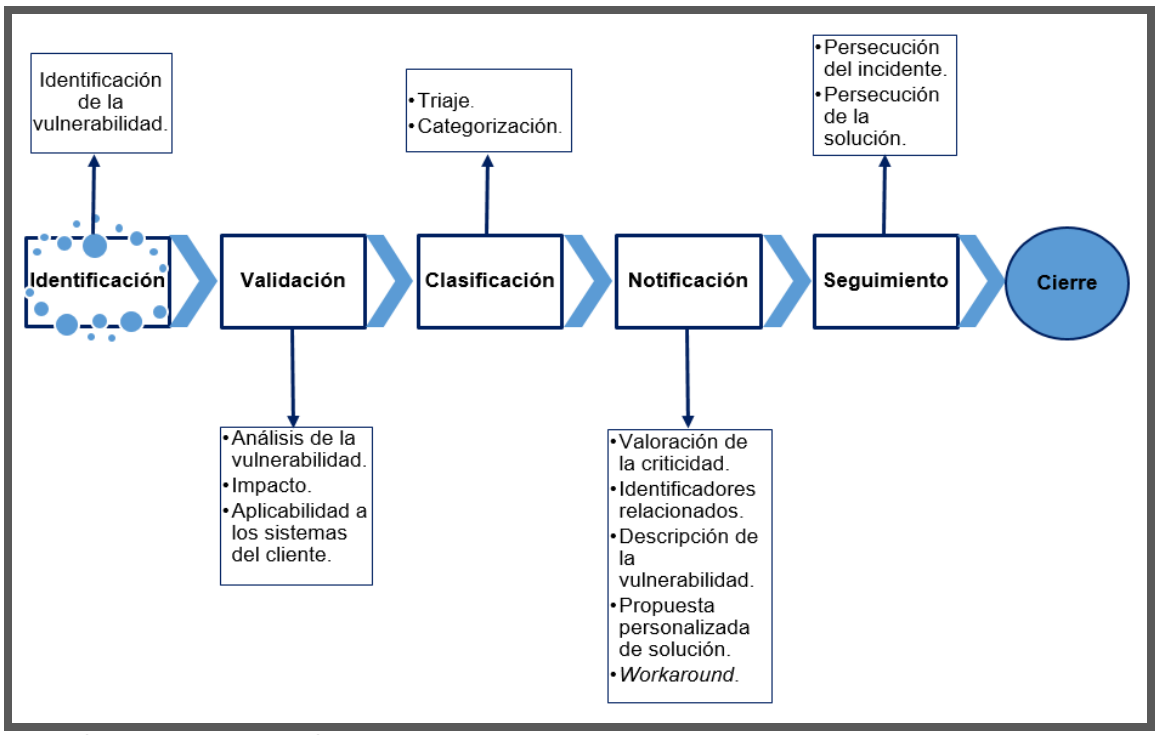

Ilustración 15 - Proceso de gestión de alertas (vulnerabilidades).

Para el servicio de alerta temprana, los miembros del SOC usarán las herramientas de registro y notificación de vulnerabilidades dispuestas por el cliente para tal fin. Además, el servicio SOC se apoyará en un sistema que ofrezca soporte a la ingesta y priorización de los contenidos relacionados con la alerta temprana, y, que finalmente, se convertirán en las alertas que se envíen.

Por otra parte, una alerta de seguridad puede ser detectada a través de diferentes mecanismos, como pueden ser, entre otros, el uso de herramientas automatizadas, antivirus, monitoreo de *logs* o manualmente, mediante los reportes de problemas que hacen los usuarios de la empresa. Por lo general, el volumen de señales de posibles alertas es muy alto, por lo que se requiere de un personal con conocimientos especializados y experimentado en la realización de análisis eficaces de la información relacionada con el incidente.

Debido a esto, entre las fuentes utilizadas para la detección de las posibles alertas de seguridad se pueden encontrar:

3.2.1 Herramientas automatizadas de alertas

Las herramientas automatizadas de alertas tienen funcionalidades de seguridad encargadas de generar alarmas ante actividades sospechosas en la red, los sistemas y las aplicaciones de la infraestructura corporativa. De hecho, algunos ejemplos de estas herramientas son:

3.2.1.1 IDPS (*Intrusion Detection and Prevention System*)

Por una parte, se tienen los sistemas de prevención de intrusos (IPS, por sus siglas en inglés) y, por otra parte, los sistemas de detección de intrusos (IDS, también por sus siglas en inglés). Sistemas que se complementan y que ayudan a alertar de las posibles amenazas en la infraestructura corporativa.

De hecho, los IPS son herramientas software que monitorizan el tráfico de una red informática, con el fin de proteger sus sistemas tecnológicos de ataques cibernéticos. Estos sistemas se consideran como una prolongación de los sistemas de detección de intrusos (IDS), pero en realidad es otro tipo de control del tráfico de red, más semejante a los cortafuegos, ya que resuelven las ambigüedades detectadas en la monitorización pasiva del tráfico de tramas de red y bloquean lo que considera no legítimo. Sin embargo, los IPS se diferencian de los cortafuegos tradicionales en que toman decisiones basadas en los contenidos del tráfico de red monitorizado, más allá de las tramas básicas de red.

3.2.1.2 SIEM (*Security Information and Event Manager*)

Por una parte, se tienen los sistemas de gestión de información de seguridad (SIM, por sus siglas en inglés) y, por otra parte, los sistemas de gestión de eventos de seguridad (SEM, por sus siglas también en inglés), cuya unión se

denomina sistemas de gestión de información y eventos de seguridad (SIEM, como en anteriores ocasiones, también por sus siglas en inglés).

De hecho, los SIEM son herramientas que unifican e interpretan todos los datos relacionados con la seguridad de la información detectados en diferentes eventos obtenidos de múltiples fuentes, con el fin de facilitar un análisis completo de las relaciones de una misma posible amenaza en diferentes puntos de la infraestructura corporativa. Debido a esto, desde un mismo panel centralizado se pueden detectar patrones y tendencias no habituales en la red, por lo que se pueden detectar las posibles amenazas en la red.

Además, los SIEM se alimentan de múltiples fuentes que recogen los eventos de seguridad y se encarga del almacenamiento a largo plazo, del análisis y la comunicación de los datos de seguridad y de la monitorización en tiempo real, correlación de eventos, notificaciones y vistas de la consola de la información de seguridad.

3.2.1.3 Software de Antivirus y Antispam

Por una parte, el software antivirus es el encargado de evitar que las estaciones de trabajo, los servidores y otros dispositivos se contagien de malware. Esta herramienta utiliza una base de datos de virus para comparar con los archivos de cada uno de los equipos, lo que requiere de actualizaciones constantes. Por otra parte, la herramienta antispam permite evitar que los usuarios de la infraestructura corporativa reciban correos no deseados y/o que puedan contener archivos con amenazas para sus sistemas.

3.2.1.4 Software validador de Integridad de archivos

Se trata de una herramienta que detecta los cambios en los archivos dentro de los diferentes equipos informáticos, mediante el uso de algoritmos criptográficos para la obtención de un HASH (o *checksum*) para cada uno de los archivos. De existir alteraciones en ese HASH, existe la posibilidad de que el archivo haya sido alterado de forma maliciosa, por lo que se alertará de la posible amenaza.

3.2.2 Registros de *logs* de eventos y actividades

Los registros de *logs* de los eventos y las actividades de los diferentes equipos de la red hacen referencia a archivos de auditoría donde quedan registradas las actividades y los eventos que son ejecutados sobre un sistema operativo, un equipo, un dispositivo, una base de datos o cualquier otro recurso. Además, pueden facilitar información relevante respecto a la solución de una alerta de seguridad e, incluso, de un evento o incidente. Por ello, se destacan los ejemplos:

3.2.2.1 Registros de *logs* de Sistemas Operativos, Servicios y Aplicaciones

Los registros de *logs* de Sistemas Operativos, servicios y aplicaciones almacenan el estado y las operaciones realizadas de manera cronológica en estos sistemas y tienen como función salvaguardar todo aquello que sucede durante su ejecución. Por tanto, la revisión de estos registros se debe establecer como una de las acciones principales para la identificación de una alerta. Por otra parte, estos registros también pueden ser utilizados como herramienta de correlación durante la fase de validación de la alerta temprana.

3.2.2.2 Registros de *logs* de Dispositivos de Red

En este caso, se hace referencia a cortafuegos o *rourters* como forma de proveer información de naturaleza sospechosa y tienen como función almacenar toda la información de lo que sucede durante su ejecución. Por tanto, también en este caso, la revisión de estos registros se debe establecer como una de las acciones principales para la identificación de una alerta. Además, también estos registros pueden ser utilizados como herramienta de correlación durante la fase de validación de la alerta temprana.

3.2.3 Información pública disponible y del personal

Tal y como se obtiene de la tabla 15 de este documento, la detección de las posibles alertas de seguridad también se puede encontrar a través de las diferentes fuentes públicas. Esta fuente de detección se relaciona con el carácter investigativo del personal del SOC y se refiere a la preparación para detectar y analizar los posibles incidentes a partir del conocimiento de vulnerabilidades recientes.

Por otra parte, la detección de las posibles alertas de seguridad también se puede obtener a través de información del personal corporativo, de los clientes y de los proveedores, que informan de vulnerabilidades internas en las funcionalidades de los servicios de la organización. Son los usuarios de las herramientas y los que detectan de primera mano sus posibles fallos.

3.3 Servicio de Cibervigilancia

El Servicio de Cibervigilancia se nutrirá de la información relativa a exfiltraciones proporcionada por el CCN-CERT en sus comunicados públicos y de información generada por el SOC en base a muestreos regulares para identificar de manera proactiva la exposición de información corporativa expuesta en Internet. Una vez detectadas, las exfiltraciones entrarán en el circuito de gestión de incidentes mediante el correspondiente registro y clasificación como incidente en el sistema de registro de eventos e incidentes de seguridad.

Asimismo, este servicio se prestará de manera continua con una periodicidad semanal durante una franja de la jornada laboral, según el calendario laboral y las necesidades de la seguridad. Por otra parte, el servicio será proporcionado por el nivel 3 del SOC debido a la experiencia de sus analistas. Además, se apoya fundamentalmente en las herramientas de extracción de metadatos y motores de búsqueda de distinta naturaleza.

Los procesos previstos para el servicio de Cibervigilancia son los siguientes:

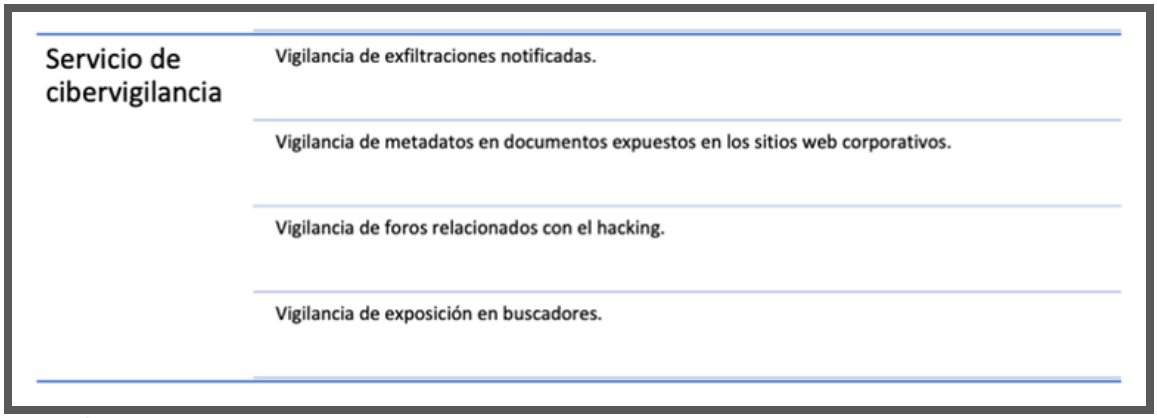

Ilustración 16 - Procesos del servicio de Cibervigilancia.

Por otra parte, existen diferentes tipos de herramientas que pueden ser útiles para la gestión de este servicio, entre las que se destacan las herramientas de inteligencia y orientación que permiten evaluar lo que ocurre en el mundo de las amenazas informáticas:

3.3.1 Herramientas de Inventarios de Activos

La gestión de activos implica el manejo de gran cantidad de datos. Por tanto, la automatización juega un papel importante en la captación, catalogación, gestión, análisis y reporte de datos de los activos. Gracias a esto, los sistemas de gestión de activos se consideran elementos esenciales para establecer la toma de decisiones y escalonar los procesos de operaciones en un conjunto de activos de gran tamaño. De hecho, algunos ejemplos de estas herramientas son:

JIRA Service Management	InvGate Assets
Freshservice	N-central
NinjaRMM	Miradore Management Suite
Netwrix Auditor	OTRS

Tabla 15 - Ejemplos de Herramientas de Inventarios de Activos para Cibervigilancia.

3.3.2 Herramientas de monitorización de seguridad

La selección correcta de herramientas tipo SIEM depende de los requisitos de la organización. Por tanto, en base a esto, se puede seleccionar la herramienta más adecuada para su capacidad de cumplimiento o de detección de amenazas. Además, se deben considerar factores como las capacidades de inteligencia de amenazas, las capacidades de análisis forense de la red, las funcionalidades para el estudio y análisis de datos, las capacidades de respuesta automatizada y su calidad, el soporte nativo para las fuentes de registro. Por ello, algunos ejemplos de estas herramientas son:

SolarWinds SIEM	Micro Focus ArcSight
Datadog	LogRhythm
Splunk Enterprise SIEM	AlienVault USM
McAfee ESM	RSA NetWitness
QRadar	Securonix
FortiSIEM	Rapid7

Tabla 16 - Ejemplos de Herramientas de monitorización de seguridad para Cibervigilancia.

3.3.3 Herramientas de inteligencia de amenazas

Las herramientas de inteligencia informática se utilizan para, de manera automática, identificar información de interés de cara a la organización, detectar datos sensibles que puedan haber sido exfiltrados, localizar y/o identificar a posibles atacantes, detractores de marcas (*haters*, en inglés) o alertar para prevenir un posible incidente cibernético, entre otras. De aquí que algunos ejemplos de estas herramientas son:

IBM XForce Exchange	Anomali ThreatStream
Palo Alto Network AutoFocus	RSA NetWitness Suite

Tabla 17 - Ejemplos de Herramientas de inteligencia de amenazas para Cibervigilancia.

3.3.4 Sistemas de Detección y Prevención de Intrusos (IDPS)

Tal y como se ha señalado anteriormente, los sistemas de detección de intrusos (IDS, por sus siglas en inglés) muestran las posibles amenazas en base a las actividades sospechosas detectadas en todos los dispositivos de red de una organización y los sistemas de prevención de intrusos (IPS, por sus siglas en inglés) realizan acciones para prevenir las posibles amenazas detectadas en las actividades sospechosas detectadas en todos los dispositivos de red de una organización. Se trata de dos tecnologías complementarias que descubren, localizan y señalan o bloquean todas las amenazas de la red corporativa de manera automática, con el fin de ofrecer

una seguridad informática más sólida y con más grado de éxito que los cortafuegos. Por ello, algunos ejemplos de estas herramientas son:

McAfee NSP	AT&T Cybersecurity
Darktrace	Palo Alto Networks
Trend Micro Tipping Point	NSFocus
Darktrace	Trend Micro Deep Discovery Inspector
Cisco Firepower NGIPS	

Tabla 18 - Ejemplos de Sistemas de Detección y Prevención de Intrusos (IDPS) para Cibervigilancia.

3.3.5 Analizador de flujos de red

Los analizadores de flujos de red se definen como herramientas que permiten monitorizar el tráfico de una red corporativa, mediante chequeos automatizados de amenazas especificadas con anterioridad. Algunos ejemplos de estas herramientas son:

Nagios	ntpdump
ntop	nmap
nfdump	Whireshark

Tabla 19 - Ejemplos de Analizador de flujos de red para Cibervigilancia.

3.3.6 Escáneres de vulnerabilidades

Los escáneres de vulnerabilidades se definen como herramientas que favorecen la ejecución de auditorías automatizadas sobre un conjunto de sistemas, redes o aplicaciones dentro de la infraestructura corporativa de una organización, con el fin de obtener información acerca de las posibles vulnerabilidades de los equipos analizados. Algunos ejemplos de estas herramientas son:

F-Secure Radar	Nessus
Qualys Guard	Nmap
Caín y Abel	DB-scan
Metasploit	SQLmap
Andspoilt	Pompem

Tabla 20 - Ejemplos de herramientas de Escáneres de vulnerabilidades para Cibervigilancia.

3.3.7 Proxys Web

Los Proxys Web son herramientas que se encargan de registrar las conexiones web realizadas en una infraestructura corporativa y redirigir el tráfico hacia los servicios finales, por lo que permite filtrar las posibles amenazas de manera automatizada. Algunos ejemplos de estas herramientas son:

Squid Proxy	WAF Imperva
IPFire	Fortiweb
Mod_proxy de Apache	

Tabla 21 - Ejemplos de Proxys Web para Cibervigilancia.

3.4 Servicio de Supervisión de indicadores de seguridad

La definición de nuevos indicadores se hará siguiendo el método GQM (*goal-questionmetrics*). Tanto el proceso de vigilancia de los indicadores existentes en la organización como el de propuesta e implantación de nuevos indicadores seguirá un ciclo de Deming, tal y como recomienda ITIL, como el siguiente:

Ilustración 17 - Ciclo de control y propuesta de nuevos indicadores de seguridad.

El servicio se nutrirá a partir de la información presente en los sistemas y herramientas de gestión de eventos e incidentes de seguridad, así como en los dispositivos de seguridad con los que cuente la organización. Además, en dependencia de la evolución del servicio, las prioridades definidas con el cliente y de la dispersión de los diferentes indicadores que puedan existir, se sugerirá desarrollar una aplicación de cuadro de mandos que integre todos los KPI necesarios para este fin.

El servicio se llevará a cabo a través de tareas de control periódicas distribuidas entre los miembros del SOC y reportarán al Coordinador del servicio y al cliente. Por otra parte, los procesos previstos para el servicio de Supervisión de indicadores de seguridad son los siguientes:

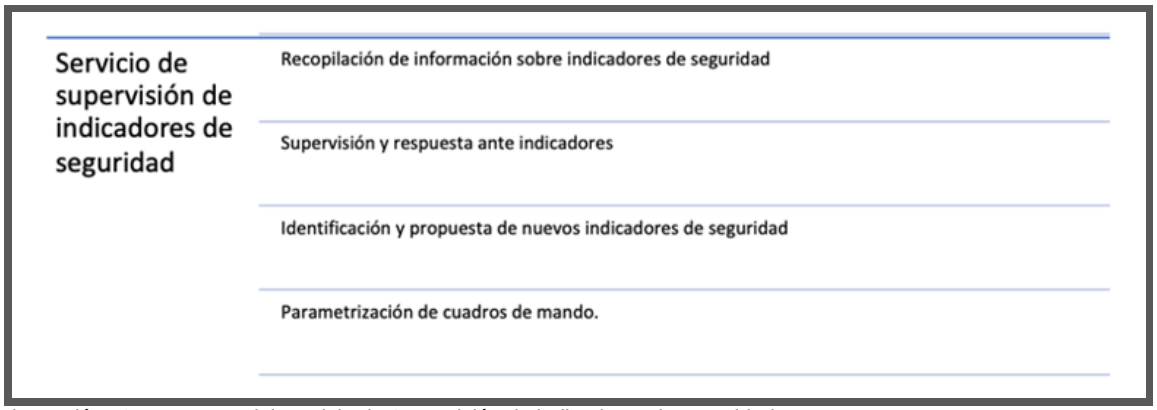

Ilustración 18 - Procesos del servicio de Supervisión de indicadores de seguridad.

Dichos procesos se definirán con la firmeza de que la transición entre las distintas tareas se presenta claramente de modo que todo el personal del SOC sepa cuál es su responsabilidad y cómo encaja en el proceso de principio a fin. Asimismo, se definirán las actividades periódicas a realizar, así como *checklists* y los modelos de informe necesarios, para la correcta ejecución de los procesos, según las directrices del cliente.

Las formas de evaluación de la gestión de los incidentes de seguridad pueden ser variadas. Debido a esto, se propone el establecimiento de una serie de indicadores que deben ser medidos de forma periódica para poder evaluar el desempeño de cada área al finalizar el rango de tiempo deseado: mes, trimestre, semestre, año, etc. Por tanto, la siguiente tabla muestra una propuesta de estos indicadores:

Indicador	Definición	Fórmula	Rango temporal
Cantidad de Incidentes	Total de los incidentes registrados en el período evaluado.	Total Incidentes	Mensual
Repetición de Incidentes	Porcentaje de incidentes que se repiten en el período evaluado.	% Incidentes Repetidos (Incidentes Repetidos / Total Incidentes)	Trimestral
Solución de Incidentes	Porcentaje de incidentes que se solucionan en el período evaluado.	% Incidentes Solucionados (Incidentes Solucionados / Total Incidentes)	Mensual

Solución de Incidentes Críticos	Porcentaje de incidentes críticos que se solucionan en el período evaluado.	% Incidentes Críticos Solucionados (Incidentes Críticos Solucionados / Total Incidentes Críticos)	Mensual
Incidentes pendientes	Porcentaje de incidentes que quedan pendientes en el período evaluado.	% Incidentes pendientes (Incidentes pendientes / Total Incidentes)	Mensual
Incidentes críticos pendientes	Porcentaje de incidentes críticos que quedan pendientes en el período evaluado.	% Incidentes críticos pendientes (Incidentes críticos pendientes / Total Incidentes)	Mensual
Tiempo medio de solución de Incidentes	Tiempo promedio de solución de un incidente en el período evaluado.	Tiempo medio (Sumatorio de tiempo de solución de Incidentes Solucionados / Incidentes Solucionados)	Mensual

Tabla 22 - Conjunto de indicadores para el servicio de Supervisión de indicadores de seguridad.

3.5 Definición de los Roles

En función del tamaño y de las necesidades de cada una de las organizaciones, el conjunto de roles que implica un SOC puede verse afectado. No obstante, tal y como indica la plataforma de automatización y orquestación de seguridad, Rapid7 Komand (2016), disponer de un equipo de seguridad efectivo y balanceado, en el que cada rol sirva de complemento y apoyo a todo el equipo, resulta necesario.

Asimismo, aunque su relación con el resto de áreas de una organización es estrictamente necesario, un Centro de Operaciones de Seguridad debe ser un servicio totalmente independiente del resto de equipos de dicha organización, ya que se deben de abstraer de la prioridad que requiere la funcionalidad de los servicios para poder visibilizar y garantizar el correcto análisis en base a su seguridad. Además, este servicio debe monitorizar y supervisar el resto de equipos de la organización, por lo que su separación se considera imprescindible para evitar los posibles conflictos internos.

Debido a esto, se propone la siguiente relación de roles, imprescindibles en un SOC, de forma genérica, a todas las organizaciones:

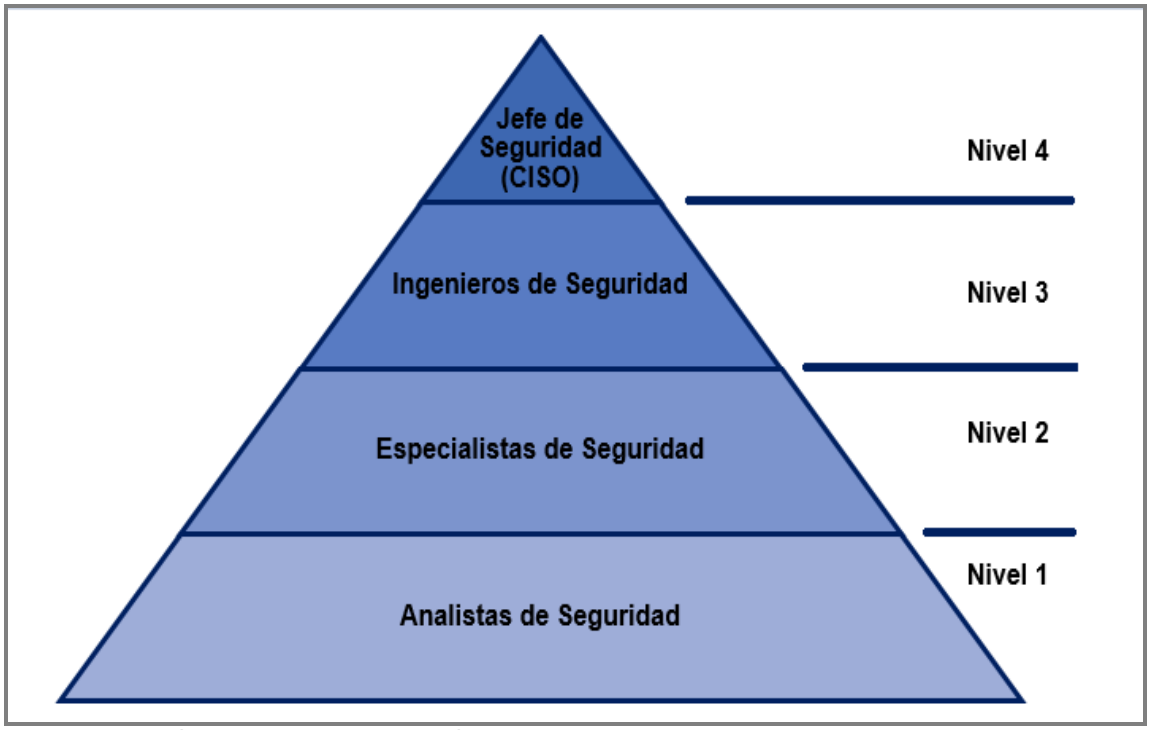

Ilustración 19 - Roles de Seguridad básicos en un SOC.

Por tanto, se propone que las funciones y competencias de cada uno de los roles de seguridad de un SOC se dividan en diferentes niveles de una estructura piramidal:

3.5.1 Nivel 1: Analistas de Seguridad de la Información

Los analistas de seguridad constituyen el rol técnico más básico de un SOC. Se trata de personal técnico encargado de registrar, detectar, responder, investigar y realizar el triaje de los eventos e incidentes de seguridad informática presentados en la organización. Además, se deben responsabilizar de la monitorización, la gestión de las herramientas proporcionadas para la ejecución de sus actividades y de la remediación ágil y rápida, a través de procedimientos definidos y aprobados.

De forma generalizada, todas las organizaciones procesan un alto volumen de datos, por lo que el personal destinado a este rol necesita tener una distribución balanceada de las actividades que realiza, como la monitorización, revisión y procesado de la información de la organización. Debido a esto, las habilidades, conocimientos, funciones y responsabilidades que debe tener un analista de Seguridad de la Información, entre otros, son las siguientes:

Habilidades (*skills*) y conocimientos del nivel 1	
Administrador de sistemas operativos.	Conocimientos de los lenguajes de programación.
Administrador de redes de ordenadores.	Conocimientos de herramientas de análisis y *debbug*.
Conocimientos de seguridad informática.	Comprensión del negocio y de la seguridad de la información.
Capacidad analítica y curiosidad.	Capacidad de trabajo en equipo.
Capacidad de trabajo bajo presión.	Capacidad de comprensión y aprendizaje.

Tabla 23 - Habilidades y conocimientos de los Analistas de Seguridad.

Funciones y competencias del nivel 1	
Gestión del servicio de eventos e incidentes de seguridad.	Notificación de las vulnerabilidades en el servicio de Alerta Temprana.
Monitorización y remediación de las alertas de seguridad de la información.	Análisis y respuesta ante eventos e incidentes de seguridad.
Diseño y desarrollo de las alertas de monitorización.	Seguimiento, estudio y análisis de eventos e incidentes de seguridad.
Categorización y priorización de los eventos e incidentes de seguridad informática.	Gestión de procesos de inteligencia ante amenazas de seguridad a través de la alerta temprana.
Registro de los eventos e incidentes de seguridad.	Desarrollo y aplicación de medidas de seguridad.
Gestión y uso de las herramientas de seguridad.	Revisión periódica de los riesgos de seguridad.

Tabla 24 - Funciones y competencias de los Analistas de Seguridad.

3.5.1 Nivel 2: Especialistas de Seguridad de la Información

Los Especialistas de Seguridad de la Información son las figuras técnicas expertas, en el campo de la seguridad informática, con capacidad para el tratamiento y resolución de incidencias complejas y con conocimientos para el escaneo de vulnerabilidades y la realización de pruebas de penetración en los sistemas y las aplicaciones.

Además, este grupo de técnicos debe de asumir todos aquellos eventos e incidentes de seguridad y resto de tareas que no son capaces de solucionarse o realizarse desde el Nivel 1 del servicio. Debido a esto, las habilidades, conocimientos, funciones y responsabilidades que debe tener un especialista de Seguridad de la Información, entre otros, son las siguientes:

Habilidades (*skills*) y conocimientos del nivel 2	
Implicación y constancia.	Capacidad de mejora continua
Iniciativa y proactividad.	Experto en la explotación de vulnerabilidades de los lenguajes de programación.
Administrador experto de sistemas, aplicaciones y redes de ordenadores.	Experto en la realización de pruebas de penetración de sistemas y aplicaciones.
Experto en seguridad informática.	Comprensión del negocio y de la seguridad de la información.
Capacidad analítica y curiosidad.	Capacidad de trabajo en equipo.
Capacidad de trabajo bajo presión.	Capacidad de comprensión y aprendizaje.
Capacidad de correlación de eventos.	Capacidades comunicativas y de enseñanza.

Tabla 25 - Habilidades y conocimientos de los Especialistas de Seguridad.

Funciones y competencias del nivel 2	
Gestión del servicio de eventos e incidentes de seguridad.	Gestión del servicio de Alerta Temprana.
Notificación de los resultados del servicio de Cibervigilancia.	Ayuda y enseñanza a los técnicos del nivel 1 del servicio.
Remediación de las alertas complejas de seguridad de la información.	Análisis y respuesta ante eventos e incidentes complejos de seguridad.
Validación y supervisión del diseño y desarrollo de las alertas de monitorización.	Supervisión, estudio y análisis de eventos e incidentes de seguridad.
Planificación y ejecución de escaneos periódicos de vulnerabilidades de los sistemas corporativos.	Administración de los procesos de inteligencia ante las amenazas de seguridad.
Planificación y ejecución de pruebas periódicas de penetración en los sistemas corporativos.	Automatizar y generar documentación de las actividades diarias comunes.
Generación de informes semanales y mensuales de los escaneos de vulnerabilidades, testeos y pruebas de penetración realizadas.	Planificación y desarrollo de medidas para minimizar los riesgos de seguridad.

Tabla 26 - Funciones y competencias de los Especialistas de Seguridad.

3.5.1 Nivel 3: Ingenieros de Seguridad de la Información

Los Ingenieros de Seguridad de la Información son las figuras técnicas y de gestión que desempeñan sus funciones en base a la ingeniería y arquitectura de los sistemas de seguridad de la información. Este grupo, además, se encarga de la documentación de los requisitos y procedimientos necesarios para el servicio, así como del cumplimiento de los protocolos, del correcto uso de las herramientas y del diseño de las medidas de seguridad.

Por otra parte, los ingenieros de seguridad, nivel 3 del SOC, también pueden colaborar con los desarrolladores de la organización y sus proveedores, con el fin de conseguir productos seguros y que cumplan con las políticas de la organización y de las normas de seguridad internacionales. Asimismo, esta parte del equipo debe de asumir todos aquellos eventos e incidentes de seguridad y resto de tareas que no son capaces de solucionarse o realizarse desde el Nivel 2 del servicio.

Debido a esto, las habilidades, conocimientos, funciones y responsabilidades que debe tener un ingeniero de Seguridad de la Información, entre otros, son las siguientes:

Habilidades (*skills*) y conocimientos del nivel 3	
Liderazgo.	Meticulosidad en el trabajo.
Implicación y constancia.	Capacidad de mejora continua.
Iniciativa y proactividad.	Ingeniero y arquitecto de seguridad de la información.
Ingeniero de sistemas y redes de ordenadores.	Ingeniero y arquitecto de software.
Capacidad analítica y seriedad.	Comprensión del negocio y de la seguridad de la información.
Capacidad de gestión del tiempo y los recursos.	Capacidad de gestión de equipos y de trabajo en equipo.
Capacidad de trabajo bajo presión.	Capacidad de comprensión y aprendizaje.
Capacidad de resolución ante problemas.	Capacidades comunicativas y de enseñanza.

Tabla 27 - Habilidades y conocimientos de los Ingenieros de Seguridad.

Funciones y competencias del nivel 3	
Gestión del servicio de eventos e incidentes de seguridad.	Gestión del servicio de Alerta Temprana.
Gestión del servicio de Cibervigilancia.	Gestión del servicio de supervisión de indicadores de seguridad.
Diseño de contramedidas ante las alertas irresolubles de seguridad.	Soporte y enseñanza a los técnicos del nivel 2 del servicio.

Enlace de comunicación entre el Jefe del SOC (CISO) y el resto del equipo.	Generación de estadísticas e informes del trabajo diario del equipo para el reporte al Jefe del SOC (CISO).
Crear y diseñar los requisitos de seguridad de la información en base a lo requerido por el Jefe del SOC y el negocio.	Documentar y formar al resto del servicio sobre los procedimientos y protocolos de los diferentes servicios que presta el SOC.
Soporte de seguridad informática al resto de equipos de la organización.	Documentar los Planes diseñados por el Jefe del SOC (CISO).
Soporte al Jefe del SOC (CISO) en todo lo relacionado con el trabajo diario del SOC.	Velar y supervisar por el cumplimiento de la seguridad de la información de todas las áreas de la infraestructura corporativa (internas y de proveedores).

Tabla 28 - Funciones y competencias de los Ingenieros de Seguridad.

3.5.4 Nivel 4: Rol de Jefe de Seguridad de la Información (CISO)

El Jefe de Seguridad de la información (CISO) es el máximo responsable jerárquico de la seguridad informática de una organización. Por ello, bajo sus directrices se establecen las líneas de negocio relacionadas con la seguridad de la información y de los sistemas, así como las estrategias, políticas, procesos, procedimientos y actividades relacionadas con la seguridad informática de los recursos físicos, personales y digitales de una organización.

Además, esta figura se encarga de coordinar y gestionar el equipo de trabajo del Centro de Operaciones de Seguridad y de sus diferentes niveles jerárquicos. Por otra parte, se considera el enlace entre el equipo y la alta dirección de la organización, a la que tiene que dar respuestas.

Debido a esto, las habilidades, conocimientos, funciones y competencias que debe tener un Jefe de Seguridad de la Información, entre otros, son las siguientes:

Habilidades (*skills*) y conocimientos del CISO (nivel 4)	
Liderazgo y dotes de mando.	Conocimientos técnicos del servicio.
Experiencia en la gestión de equipos.	Arquetipo y seriedad.
Iniciativa y templanza.	Inteligencia emocional.
Capacidad comunicativa.	Experiencia en la seguridad informática.
Capacidad de manipulación.	Comprensión del negocio y de la seguridad de la información.

Tabla 29 – Habilidades y conocimientos del Jefe de Seguridad (CISO).

Funciones y competencias del CISO (nivel 4)	
Revisar el programa de seguridad informática.	Fiscalizar las tareas del equipo de trabajo.
Crear las estrategias de seguridad informática.	Proporcionar las estrategias de seguridad informática al equipo de trabajo.
Fomentar la criticidad de la seguridad informática corporativa.	Entrevistar y contratar al personal de seguridad informática para el servicio.
Equiparar los objetivos del negocio con los de la seguridad de la información.	Crear y delegar el Plan de Respuesta ante Vulnerabilidades.
Planificar y controlar el cumplimiento de las certificaciones de seguridad informática de la organización.	Crear y delegar el Plan de gestión de notificaciones de Alerta Temprana.
Crear y delegar el Plan de gestión de notificaciones de Cibervigilancia.	Crear y delegar el Plan de la supervisión de los indicadores de seguridad.
Crear y gestionar el Plan de Continuidad del Negocio.	Crear y delegar el Plan de Respuesta ante eventos e incidentes de seguridad informática.
Crear el Plan de Seguridad de la Información y los sistemas corporativos.	Crear los procedimientos y diseñar las alertas de seguridad.
Gestión del presupuesto destinado a la seguridad de la información.	Desarrollar y visibilizar los flujos de trabajo.
Crear el Plan de Comunicación del servicio.	Generar informes para la auditoría y control de los indicadores de seguridad informática.

Tabla 30 – Funciones y competencias del Jefe de Seguridad (CISO).

3.6 Valoración económica de la implementación de un SOC

Dado que este proyecto, en donde se describe el diseño de la planificación de un Centro de Operaciones de Seguridad, es genérico y no atiende a una organización concreta, no se puede especificar una valoración económica exacta. Esto es debido a que el presupuesto que una organización debe destinar a la implementación de un SOC depende de múltiples factores, entre los que se destacan el hardware (puestos de usuario, cortafuegos, SIEM, IDPS…), el software (antivirus, proxys web, gestores de contraseñas…) y el gasto en personal (trabajadores, formación, certificaciones…).

Por tanto, debido al desconocimiento del posible software y hardware que puede tener o requerir una organización para implementar un SOC, se puede intentar crear una estimación de la valoración económica que puede requerir sólo para el personal, en el caso de que no lo tenga ya en plantilla. Igualmente, puede servir para entender mejor el número de trabajadores que necesita para realizar una buena implementación.

Según los datos de la encuesta *Common and Best Practices forSecurity Operations Centers: 2019 Survey* del SANS Institute, la gran mayoría de las organizaciones destinan alrededor del 3% de su personal, a personal de TI; y, a su vez, alrededor del 3% del personal de TI, al personal de seguridad de TI. Debido a esto, el dimensionamiento más frecuente de un SOC, en función del tamaño de la organización, es el siguiente:

Tamaño de la plantilla en una organización	Número más común de técnicos destinados al SOC de una organización
< 10.000 trabajadores	2 - 5 técnicos
10.000 - 15.000 trabajadores	6 - 10 técnicos
15.001 – 100.000	11 - 25 técnicos
> 100.000	26 - 100 técnicos

Tabla 31 - Número frecuente de técnicos en un SOC según SANS Institute.

Equivalentemente, dada la regla indicada anteriormente, en donde el 3% del 3% (0,0009) se destina a personal de seguridad de TI, el dimensionamiento más exacto de un SOC, en función del tamaño de la organización, debería ser el siguiente:

Tamaño de la plantilla en una organización	Número recomendado de técnicos destinados al SOC de una organización
< 10.000 trabajadores	< 8 técnicos + 1 Jefe del SOC
10.001 - 15.000 trabajadores	≈ 8 - 14 técnicos + 1 Jefe del SOC
15.001 – 100.000	≈ 14 - 90 técnicos + 1 Jefe del SOC
> 100.000	> 90 técnicos + 1 Jefe del SOC

Tabla 32 - Número recomendado de técnicos en un SOC.

Por otra parte, los costes salariales también pueden variar según el emplazamiento que tenga una organización u otra y según el precio que haya en el mercado. Por tanto, en base a los datos encontrados en las diferentes ofertas de empleo encontradas en los portales de búsqueda de empleo Infojobs y Tecnoempleo entre los años 2020 y 2021, las organizaciones pueden estimar la siguiente valoración económica que puede costarle cada miembro del personal de un SOC:

Tipo de trabajador en un SOC (Nivel en el SOC)	Salario unitario mínimo orientativo en España
Analista de Seguridad Informática (Nivel 1)	≈ 30 000 €/año.
Especialista de Seguridad Informática (Nivel 2)	≈ 38 000 €/año.
Ingeniero de Seguridad Informática (Nivel 3)	≈ 45 000 €/año.
Jefe de Seguridad Informática (CISO) (Nivel 4)	≈ 60 000 €/año.

Tabla 33 - Valoración económica anual estimada del personal de un SOC.

Indistintamente a estos datos, siempre se debe de considerar viable invertir en seguridad informática para garantizar (o, a lo sumo, aminorar los daños) que el negocio no se ve envuelto en un problema de filtración de datos corporativos o en un problema de cifrado de sus datos. Dos de los problemas de seguridad informática más comunes en la actualidad.

Además, en España se aprobó el Real Decreto-Ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos en el BOE, que regula la cuantía de las multas y el procedimiento sancionador. De hecho, las sanciones en este Real Decreto-Ley se establecen según si son leves, graves o muy graves:

- Sanciones para infracciones Leves: multa de hasta 40.000 €, como, por ejemplo:
  - Incumplimiento de la obligación de informar al afectado de la rectificación, supresión o limitación del tratamiento de datos por parte de un destinatario.
  - Incumplimiento de los deberes de responsabilidad del tratamiento de datos.
- Sanciones para infracciones Graves: multa de 40.001 € a 300.000 €, como, por ejemplo:
  - Tratamiento de datos de menores de edad sin consentimiento de padres o tutores legales.
  - Abandono o desamparo de medidas de carácter organizativo y técnico para la protección de datos desde el diseño.
- Sanciones para infracciones Muy Graves: multa entre 300.001 € a 20.000.000 €, como, por ejemplo:
  - Uso los datos personales recabados con una finalidad diferente a la de su consentimiento.
  - Infringir el deber de confidencialidad.

4. Conclusiones

Este proyecto se basa en la importancia que, en la actualidad, tiene la seguridad de la información, de los sistemas, de las aplicaciones y de las comunicaciones para todas las organizaciones. Cada vez más se trabaja en minimizar y gestionar los riesgos de seguridad informática, mediante sistemas seguros que permitan identificar las posibles amenazas, con el fin de respaldar el uso adecuado de sus bienes y recursos con los que desarrolla sus actividades diarias.

Asimismo, diversas organizaciones han optado por la implementación de un Centro de Operaciones de Seguridad, lo que implica tener una unidad centralizada y dedicada a los aspectos tácticos y operativos asociados con la ciberseguridad. El Centro de Operaciones de Seguridad se define como el equipo de TI que se encarga de realizar labores orientadas a la monitorización, protección y defensa de los activos de información en tiempo real, a través de equipos tecnológicos y personal especializado y centralizado. Por otra parte, juega un papel fundamental en la detección y reacción ante incidentes de seguridad en la organización.

Además, se ha realizado un análisis de aquellos elementos derivados de la implementación de las buenas prácticas propuestas por ITIL y de determinadas metodologías agiles que pueden resultar beneficiosas en la puesta en marcha de un SOC. ITIL actualmente constituye la biblioteca de recursos más extendida a nivel de administración de tecnologías de la información, por lo que se considera una garantía de seguro internacional de buenas prácticas. Por otra parte, las metodologías ágiles establecen la forma más eficiente de administrar las actividades de las organizaciones en entornos de incertidumbre.

La combinación de estos elementos metodológicos permite obtener resultados eficaces y eficientes a nivel tecnológico. Por tanto, en el presente Trabajo de Final de Grado se ha propuesto elaborar el diseño de la implementación de un Centro de Operaciones de Seguridad (SOC) mediante las buenas prácticas propuestas por ITIL y las metodologías ágiles DevOps y Kanban.

Esta combinación tiene como esencia la necesidad de ofrecer un servicio de ciberseguridad que permita a las organizaciones centralizar los eventos e incidentes de seguridad de la información, de los sistemas, de las aplicaciones y de las comunicaciones y aportar una solución a los problemas que se identifiquen en el negocio desde el punto de vista de este ámbito. El resultado del estudio realizado ha permitido obtener un documento que pretende ser una guía general para aquellas organizaciones que decidan incorporar las actividades desarrolladas por un Centro de Operaciones de Seguridad a su gestión.

Al mismo tiempo, se ha estudiado y descartado incluir a esta combinación de metodologías a Extreme Programming (XP) y Scrum. Por una parte, Extreme Programming se centra en el desarrollo de software con énfasis los procesos

adaptables por encima de la previsión de incidentes. Por ello, los defensores de XP exponen que los accidentes, fallos o inconvenientes que acontecen durante un proyecto son elementos naturales.

Por otra parte, Scrum se define como una metodología de trabajo resulta útil para los proyectos en donde sea necesario intervenir en el proceso porque, entre otras, los equipos muestran índices de rendimiento bajo, la calidad del producto resultante sea inferior al deseado, se obtengan altos costes o las entregas de los productos finales se prolonguen en el tiempo más de lo deseado. Debido a esto, en resumen, XP se enfoca en el desarrollo de software y no en la integración de otros servicios, por lo que queda fuera del ámbito de este proyecto. Además, dado que se considera muy probable tener la necesidad de realizar reajustes entre los procesos del marco de trabajo y el propio proyecto, también se excluye Scrum del dominio de este trabajo.

El documento guía resultante expresa los principales resultados del análisis realizado, expone los beneficios y ventajas de la aplicación de las metodologías mencionadas y define los principales servicios y roles que se asocian a un SOC. Se resalta que, entre los servicios que se deben prestar, se encuentran:

- Servicio de gestión de eventos e incidentes de seguridad.
- Servicio de Alerta Temprana.
- Servicio de Cibervigilancia.
- Servicio de Supervisión de indicadores de seguridad.

De igual forma, se considera importante destacar que estos servicios constituyen una propuesta, por lo que cada una de las organizaciones debe ser capaz de adaptarlo a sus particularidades. Además, cada Centro de Operaciones de Seguridad debe cumplir con los requerimientos legales nacionales, así como con los estándares internacionales, respetar las políticas y reglas de negocio determinadas por la Alta Dirección.

La memoria del trabajo ofrece un documento “Guía de Implementación del SOC” donde quedan recogidas las diferentes características y etapas que deben tenerse en cuenta en este proceso. La elaboración de este documento es el resultado de un análisis profundo de la bibliografía disponible. No obstante, resulta oportuno anotar que el campo de la seguridad es amplio, por lo que este trabajo constituye un primer acercamiento y caracterización de algunos de los elementos que lo componen.

De manera personal, tras la redacción de la memoria, queda la intención de poner en práctica los postulados teóricos recogidos mediante la propuesta a diferentes organizaciones reales. Además, se considera que la implementación práctica de esta propuesta puede enriquecer el contenido de la memoria haciéndolo más congruente con la realidad que acontece en las organizaciones.

El trabajo realizado ha sido, ante todo, un entrenamiento para abordar cuestiones técnicas desde una posición académica y profesional. Su seguimiento y planificación constituyeron la clave y guía fundamental en el proceso de elaboración. A modo de evaluación personal, se considera que el establecimiento de los tiempos de dedicación, así como los hitos a alcanzar en cada etapa fueron los determinantes para poder alcanzar los objetivos planteados inicialmente. En un principio el estudio podía entenderse como pretencioso en su alcance, pero el trabajo y revisión constante permitió concretar y definir mejor las metas planteadas, lo que facilitó el desarrollo de los contenidos abordados.

La memoria resultante de este proyecto constituye una evidencia del proceso de investigación que se ha desarrollado durante este semestre. Su elaboración abarca fundamentalmente elementos teóricos relacionados con la implementación de Centro de Operaciones de Seguridad, por lo que se deja la posibilidad de complementarlo mediante futuras investigaciones y con los elementos prácticos asociados a su ejecución. En definitiva, la evaluación de la efectividad de la “Guía de Implementación de un SOC” puede constituir el motivo de desarrollo de futuras investigaciones.

5. Glosario

- **ACTIVO**: Recurso de una organización necesario para el desempeño de las funciones diarias que, en caso de indisponibilidad o fallo, supone un problema o coste para el negocio.
- **ALERTA**: Notificación de la posible interrupción de un servicio, de la reducción en su calidad o de un evento que puede tener un impacto negativo en los activos, las operaciones u objetivos del negocio de una organización.
- **AMENAZA**: Situación adversa que puede tener consecuencias negativas en los activos de información de una organización y afectar a su disponibilidad, integridad, confidencialidad, autenticidad y/o trazabilidad.
- **ANTIVIRUS**: Programa informático creado para detectar, bloquear y eliminar posibles programas dañinos y proteger los sistemas de una organización.
- **AUTENTICIDAD**: Propiedad de la información que garantiza la identidad de su suministrador.
- **BOE**: Boletín Oficial del Estado: Diario oficial nacional español destinado a la publicación de las leyes, disposiciones y actos de inclusión obligatoria.
- **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 ante Incidentes de Seguridad de la Información del Centro Criptológico Nacional.
- **CENTRO DE OPERACIONES DE SEGURIDAD (SOC)**: *Security Operations Center* o SOC, por sus siglas en inglés: Equipo de trabajo centralizado que se dedica a los aspectos tácticos y operativos asociados con la ciberseguridad de una organización.
- **CERT**: Equipo de Respuesta ante Emergencias Informáticas (*Computer Emergency Response Team*, por sus siglas en inglés).
- **CHECKLISTS**: Lista de control usada para reducir las fallos y olvidos en las tareas repetitivas y garantizar la coherencia y la integridad de una tarea.
- **CIBERSEGURIDAD**: Seguridad informática relacionada con la protección de los activos de información mediante el procesado de las amenazas que puedan poner en riesgo la información de una organización.

- **CIFRADO**: Proceso usado para convertir datos legibles en ilegibles, por lo que se puede proteger la lectura de la información contra usuarios no deseados (tanto desde el punto de vista de la seguridad, cuando se realiza por un usuario legítimo, como de un incidente de seguridad cuando se realiza por un usuario no legítimo).
- **CISO**: *Chief Information Security Officer*, por sus siglas en inglés: Responsable máximo de la seguridad de la información de una organización.
- **CONFIDENCIALIDAD**: Propiedad de la información que garantiza el acceso sólo al personal autorizado.
- **CORTAFUEGOS**: Sistemas de seguridad de la información (también conocidos como *firewalls*, en inglés) que se sitúan en los puntos fronterizos de las redes corporativas y tienen como función el permitir o bloquear el tráfico de red entre los diferentes puntos de dicha frontera en la que se encuentra.
- **DIAGRAMA DE GANTT**: Diagrama que muestra la línea cronológica de las tareas que se ejecutan en un proyecto.
- **DISPONIBILIDAD**: Propiedad de un recurso o dato de ser accesible y utilizable sólo por el proceso o personal autorizado.
- **Extreme Programming (XP)**: Metodología de desarrollo ágil que se orienta hacia la mejora de la producción de software de la mejor calidad de forma constante en el tiempo mientras se promueve la mejor calidad de vida para los desarrolladores.
- **EFICACIA**: Capacidad para conseguir las metas y objetivos propuestos.
- **EFICIENCIA**: Relación entre los recursos usados y los objetivos logrados.
- **EVENTO DE SEGURIDAD**: Circunstancia que expone los niveles de riesgo de un activo o servicio relacionado con la seguridad de la información de una organización, pero sin afección a las operaciones u objetivos del negocio.
- **EXFILTRACIÓN**: Movimiento, salida o paso de la información de una organización de una zona de la infraestructura interna a otra o al exterior de la organización
- **FALSO POSITIVO**: Alerta informática que no responde a ninguna amenaza de seguridad y que no debería de aparecer como amenaza.
- **IDS**: Sistemas de detección de intrusos (*Intrusion Detection System*, en inglés) muestran las posibles amenazas en base a las actividades sospechosas detectadas en todos los dispositivos de red de una organización.
- **IMPACTO**: Cambio desfavorable en el grado de cumplimiento de los objetivos del negocio.

- **INCIDENTE (INCIDENCIA)**: Interrupción no planificada de un activo o servicio de una organización, que tiene afección en las operaciones u objetivos del negocio.
- **INCIDENTE DE SEGURIDAD**: Interrupción no planificada de un activo o servicio relacionado con la seguridad de la información de una organización, que tiene afección a las operaciones u objetivos del negocio.
- **INFORMACIÓN**: Conjunto de datos procesados y relacionados que pueden ser entendidos e interpretados por la organización.
- **INTEGRIDAD**: Propiedad de la información que garantiza la veracidad de los datos y respalda que no hayan sido modificados en ninguna de sus formas.
- **IPS**: Sistemas de prevención de intrusos (*Intrusion Prevention System*, en inglés) realizan acciones para prevenir las posibles amenazas detectadas en las actividades sospechosas detectadas en todos los dispositivos de red de una organización.
- **ISO**: Organización Internacional de Normalización (*International Organization for Standardization* en inglés): Organización centralizada que se encarga de crear estándares internacionales y se compone de varias organizaciones nacionales de normalización.
- **ITIL**: Biblioteca, un marco de referencia, que contiene la descripción de un conjunto de recomendaciones y buenas prácticas para la administración de servicios de TI.
- **KANBAN**: Metodología ágil que incide en la productividad y eficiencia del equipo de trabajo mediante la definición, gestión y mejora de los servicios que derivan en la entrega de conocimiento.
- **LOG**: Fichero que almacena la actividad realizada y los eventos registrados por un activo de forma cronológica.
- **MALWARE**: Tipo de amenaza informática que tiene como objetivo vulnerar los sistemas de información de una organización (por ejemplo: virus, troyanos, *spywares*, gusanos, etc.).
- **METADATOS**: Datos que identifican a otros datos de manera única.
- **METODOLOGÍA**: Grupo de métodos, mecanismos y procedimientos empleados para el éxito de los objetivos de una actividad o proyecto.
- **METODOLOGÍA ÁGIL**: Método de desarrollo de proyectos, generalmente de software, que se caracterizan por crear pequeños incrementos de las actividades de un proyecto para darles rapidez, flexibilidad en su desarrollo y suministrar pequeñas entregas que muestren su avance.
- **MONITORIZACIÓN**: Supervisión y análisis del estado y rendimiento del funcionamiento de los activos de una organización con el fin de notificar y reaccionar ante una anomalía determinada.

- **PARTES INTERESADAS**: *Stakeholders*, en inglés: Conjunto de personas u organizaciones involucradas que influyen y tienen intereses en actividades, proyectos o negocios corporativos de la organización.
- **PENETRACIÓN**: Técnica de intrusión y explotación de vulnerabilidades de los activos de una organización.
- **PROCESO DE NEGOCIO**: Conjunto de tareas y actividades estructuradas que producen un servicio o producto esencial para el negocio de una organización.
- **PROXY WEB**: Sistema web que centraliza las redirecciones web de una organización y bloquea el acceso al contenido no permitido.
- **SCRUM**: Metodología de desarrollo ágil que planifica una estrategia de desarrollo iterativo basado en ciclos de feedback rápido, centra la calidad del producto y la solución en el conocimiento implícito del personal en equipos que se organizan a sí mismos, en vez de la calidad de los procedimientos utilizados, y enlaza las diferentes fases del desarrollo, en vez de ejecutarlas de forma secuencial.
- **SEGURIDAD DE LA INFORMACIÓN**: Seguridad informática relacionada con la protección de los activos de información mediante el procesado de las amenazas que puedan poner en riesgo la información de una organización.
- **SISTEMA DE INFORMACIÓN (SI)**: Conjunto de datos que interactúan entre sí con un fin común.
- **SPRINT**: Intervalo de tiempo predefinido en el que se crea un incremento de un producto utilizable y potencialmente entregable.
- **TECNOLOGÍA DE LA INFORMACIÓN (TI)**: Conjunto de sistemas, infraestructuras, aplicaciones y resto de activos relacionados con el almacén, la recuperación, la transmisión y la manipulación de los datos en base a los Sistemas de Información (SI).
- **TRAZABILIDAD**: Propiedad de la información que garantiza su histórico, ubicación y trayectoria desde su origen hasta su destino.
- **TRIAJE**: Protocolo de intervención o método de selección y clasificación de eventos, incidentes y alertas de seguridad de la información.
- **VULNERABILIDAD**: Deficiencia, debilidad o fallo de un activo informático que puede generar una amenaza en los sistemas de información de una organización.

6. Bibliografía

- Anderson, David J.; Carmichael, Andy (2016, abril). “Essential Kanban Condensed”. Versión 28. Edición 1. Seattle, Washington: Lean Kanban University Press.
- Andrade De la Cruz, Nilton C. y Capcha, Walter E. (2013, junio). “Diseño e implementación de la gestión de servicios TI, basados en ITIL V.3 para la empresa virtual ITExpert” [artículo en línea]. Escobar Urueña, Marcela. Proyecto Profesional para acceder al Título de Ingeniero de Sistemas de información. Lima, Perú [Fecha de consulta: 15 de marzo de 2021]. <http://repositorioacademico.upc.edu.pe/upc/handle/10757/322266>
- Agile Alliance (s.f.). “Extreme Programming (XP)” [artículo en línea]. Agile Alliance [Fecha de consulta: 29 de marzo de 2021]. <https://www.agilealliance.org/glossary/xp/>
- Agile Alliance (s.f.). “Scrum” [artículo en línea]. Agile Alliance [Fecha de consulta: 29 de marzo de 2021]. <https://www.agilealliance.org/glossary/scrum/>
- Bernal, Aurea y del Moral, Guillermo (2015). “Razones que soportan una implementación ITIL y su relación con el éxito o fracaso de la misma” [artículo en línea]. Ramos, M. y Solares, P.(eds.). Universidad Iberoamericana. Ciencias de la Tecnología de la Información ECORFAN, Ciudad de México D.F. [Fecha de consulta: 15 de marzo de 2021]. <http://www.ecorfan.org/proceedings/CTI_II/7.pdf>
- BOE (2018, julio). “Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos” [artículo en línea]. Agencia Estatal Boletín Oficial del Estado [Fecha de consulta: 28 de abril de 2021]. <https://www.boe.es/buscar/doc.php?id=BOE-A-2018-10751>
- Carrasco, E. A., y Ascue, M. A. (2007). “Aplicación del modelo ITIL en la gestión de servicios de Tecnologías de Información y comunicaciones para Electro Sur Este S.A.A” [artículo en línea]. Palomino, Emilio. Tesis de Grado para el Título Profesional de Ingeniero Informático y de Sistemas. Universidad Nacional San Antonio Abad. Cusco, Perú [Fecha de consulta: 16 de marzo de 2021]. <https://www.academia.edu/27183536/APLICACI%C3%93N_DEL_MODELO_ITIL_ELECTRO?auto=download>
- Corbelli, Óscar A. (2019, marzo). “ITIL 4 Fundamentos”. Versión 1.1. Edición 4. (rev. Díaz Pereira, Isabel). Madrid: Tecnofor Ibérica.
- Crowley, Chris & Pescatore, John (2019, julio). “Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey” [artículo en línea]. SANS Institute [Fecha de consulta: 01 de mayo de 2021]. <https://www.sans.org/media/analyst-program/common-practices-security-operations-centers-results-2019-soc-survey-39060.pdf>

- EAE Business School (2018, agosto). “Usos y limitaciones de la metodología Scrum” [artículo en línea]. EAE Business School [Fecha de consulta: 27 de marzo de 2021]. <https://retos-directivos.eae.es/usos-y-limitaciones-de-la-metodologia-scrum/>
- Gartner (2021). “Glosario IT de Gartner” [artículo en línea]. DevOps. Gartner [Fecha de consulta: 20 de marzo de 2021]. <https://www.gartner.com/en/information-technology/glossary/devops>
- Infojobs (2021). “Portal Infojobs” [página en línea]. Adevinta Spain [Fechas de consulta: febrero - mayo de 2021]. <https://www.infojobs.net/>
- Jiménez, Guillermo (2016). “DevOps, la nueva tendencia en el desarrollo de sistemas TI, un caso práctico en el análisis de incidencias de software” [artículo en línea]. Sorroche, Alberto. Proyecto final de carrera de Ingeniería de Telecomunicaciones. Universitat Politécnica de Catalunya junto con Everis [Fecha de consulta: 29 de marzo de 2021]. <https://upcommons.upc.edu/bitstream/handle/2117/85074/Análisis%20de%20incidentes%20en%20el%20ámbito%20TIC%20con%20DevOps.pdf>
- Lachapelle, Eric (2005). “ISO/IEC 27001 Lead Implementer”. Versión 4.7. Guía de Consulta. PECB.
- Lockheed Martin (2015). “Gaining the Advantage” [artículo en línea]. Applying Cyber Kill Chain® Methodology to Network Defense. Lockheed Martin. [Fecha de consulta: 30 de marzo de 2021]. <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf>
- López, Dídac (2020, febrero). “DevOps y la gestión de servicios de SI/TI” [artículo en línea]. FUOC - Fundación para la Universitat Oberta de Catalunya (coord. Guitart, Isabel) [Fecha de consulta: 3 de marzo de 2021]. <http://materials.cv.uoc.edu/daisy/Materials/PID_00270737/pdf/PID_00270737.pdf>
- Mañas, José Antonio (2015, agosto). “Guía de Seguridad (CCN-STIC-401) - Glosario y Abreviaturas” [artículo en línea]. CCN [Fecha de consulta: 1 de marzo de 2021]. <https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=index.html>
- Martí Tassier, Martí (2020, febrero). “ITIL 4: una introducción” [artículo en línea]. FUOC - Fundación para la Universitat Oberta de Catalunya [Fecha de consulta: 3 de marzo de 2021]. <http://materials.cv.uoc.edu/daisy/Materials/PID_00272898/pdf/PID_00272898.pdf>
- Menzinsky, Alexander; López, Gertrudis; Palacio, Juan (2016, julio). “Guía de Scrum Manager”. Versión 2.6. Lubaris Info 4 Media.

- Molina Rodríguez, Marlon; Corbelli, Óscar A. (2016, enero). “ITIL 3 Fundamentos”. Edición 4.4.1. (col. Díaz Pereira, Isabel). Madrid: Tecnofor Ibérica.
- Nanou, Electra (2021, marzo). “The 9 Best Intrusion Detection and Prevention Systems to Boost Your Cyber Security” [Artículo en línea]. Makeuseof [Fecha de consulta: 18 de abril de 2021]. <https://www.makeuseof.com/best-intrusion-detection-and-prevention-systems/>
- Navarro Cadavid, Andrés; Fernández Martínez, Juan Daniel; Morales Vélez, Jonathan (2013, septiembre). “Revisión de metodologías ágiles para el desarrollo de software” [artículo en línea]. Universidad Autónoma del Caribe [Fecha de consulta: 5 de marzo de 2021]. <https://dialnet.unirioja.es/descarga/articulo/4752083.pdf>
- Rapid7 Komand (2016, agosto). “How to hire a strong and effective security team” [artículo en línea]. Rapid7 Komand [Fecha de consulta: 15 de abril de 2021]. <https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-komand-hire-strong-effective-security-team-whitepaper.pdf>
- 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. <https://reunir.unir.net/bitstream/handle/123456789/8169/ROMAN%20TORRES%2C%20MARIA%20JOSE.pdf?sequence=1&isAllowed=y>
- Salvay, Javer E. (s.f.). “Kanban y Scrumban orientados a Proyectos de Tecnología de la Información” [artículo en línea]. Versión 3.9 del Proyecto de Grado de Ingeniería en Sistemas. Instituto Universitario Aeronáutico [Fecha de consulta: 31 de marzo de 2021]. <https://rdu.iua.edu.ar/bitstream/123456789/880/1/Proyecto%20de%20Grado%20-%20Kanban%20y%20Scrumban%20-%20Javier%20Salvay.pdf>
- Sharma, Sanjeev (2014). “DevOps para Dummies, IBM Limited Edition”. Hoboken, New Jersey: John Wiley & Sons, Inc.
- Software Testing Help (2021, marzo). “Top 11 Best SIEM Tools In 2021 For Real-Time Incident Response And Security” [Artículo en línea]. Software Testing Help [Fecha de consulta: 18 de abril de 2021]. <https://www.softwaretestinghelp.com/siem-tools/>
- Tecnoempleo (2021). “Portal de empleo especializado en informática y telecomunicaciones” [página en línea]. Tecnoempleo [Fechas de consulta: febrero - mayo de 2021]. <https://www.tecnoempleo.com/>

- Vite Cevallos, Harry; Montero, Kelvin; Cuesta, Jefferson (2018). “Metodologías ágiles frente a las tradicionales en el proceso de desarrollo de software” [artículo en línea]. Espirales: Revista Multidisciplinaria de Investigación. [Fecha de consulta: 5 de marzo de 2021]. <https://www.researchgate.net/publication/327537074_Metodologias_agiles_frente_a_las_tradicionales_en_el_proceso_de_desarrollo_de_software>
- Zimmerman, Carson (2014). “MITRE Corporation. (2014). Ten strategies of a World-Class Cybersecurity Operations Center” [Artículo en línea]. The MITRE Corporation. ISBN: 978-0-692-24310-7. Estados Unidos [Fecha de consulta: 20 de abril de 2021]. <https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf>

7. Anexos

7.1 Anexo 1: Guía de implementación de un Centro de Operaciones de Seguridad (SOC)

Universitat Oberta de Catalunya
uoc.edu

Guía de implementación de un Centro de Operaciones de Seguridad (SOC)

Antonio Díaz Pérez
Grado de Ingeniería Informática
Gestión de Proyectos

Joan Gallifa Roca
Atanasi Daradoumis Haralabus

Junio de 2021

Índice

1. Introducción

A continuación, se propone una guía genérica, que resume la información abordada en los epígrafes de este Trabajo Final de Grado, para la implementación de un SOC. Asimismo, este documento pretende servir de orientación para las organizaciones que se planteen la incorporación de este servicio a su funcionamiento empresarial.

Ilustración 20 - Guía de implementación de un Centro de Operaciones de Seguridad (SOC).

7.1.1 Alineación de los objetivos de gestión de la organización y los objetivos para la tecnología de la información

2. Alineación de los objetivos de gestión de la organización y los objetivos para la tecnología de la información

Inicialmente, para la implementación de un SOC se hace imprescindible la evaluación de capacidades de los procesos, de las personas y de las tecnologías en base a los objetivos que se desean alcanzar. Esta medición implica hacer una revisión de la situación actual y contrarrestarla con el estado que se desea alcanzar. Además, este paso resulta imprescindible porque permitirá definir la estrategia a seguir y concebir una hoja de ruta que guíe el proceso.

La evaluación de capacidades debe ser desarrollada por personal con experiencia en la materia. Además, en la realización de esta tarea, se debe tener en cuenta la aplicación del enfoque metodológico previamente definido. Para este caso, se resaltan las ventajas de la implementación de tecnologías ágiles.

Para su adecuada realización, se considera necesario que los objetivos de la organización y los objetivos de TI se encuentren alineados. En función de este

proceso, se identifican las capacidades que se esperan obtener a partir de la implementación de un SOC en la organización. Posteriormente, se recogerá información referente a las personas, los procesos y las tecnologías existentes para analizar las brechas entre lo que es y lo que debe ser, mientras se expresan los resultados formalmente a través de un informe final.

Además, este informe se describe como un punto medular en cualquier puesta en marcha que se desee hacer de un Centro de Operaciones de Seguridad, ya que la madurez del servicio y la evaluación de su funcionamiento dependerá del alineamiento y correspondencia que tengan sus objetivos con los objetivos de la organización. Debido a esto, se considera necesario que siempre participen juntos, en la creación de este tipo de informes, un responsable de TI y un responsable del negocio, con el fin de garantizar esta correcta alineación de objetivos.

Asimismo, cabe la posibilidad de que existan casos en donde los objetivos no se encuentren correctamente definidos, por lo que habría que recurrir a personas clave expertas en la materia y obtener sus opiniones y visiones sobre la tecnología en seguridad de la información. En esta situación, se hace imprescindible tener en cuenta la visión del personal de diferentes áreas y niveles jerárquicos de la propia organización para tener una mejor valoración de conjunto y conocimiento de sus necesidades.

A través del uso de ITIL como marco de referencia, se posibilita la asociación de los objetivos de las tecnologías de la información con elementos de gestión financieros, cuestiones asociadas al cliente, aspectos internos de la organización, crecimiento y aprendizaje. Los beneficios asociados a la implementación de ITIL son los siguientes:

- Fortalece la comunicación: ofrece un lenguaje común y consistente en función de términos detalladamente definidos y aceptados por las diferentes áreas de la empresa.
- Proporciona un modelo de Gobernabilidad de TI: facilita la obtención de información a través de controles y estructuras que aseguran que el departamento de TI apoye las estrategias empresariales. Además, integra los objetivos del negocio y genera confianza en los indicadores y controles.
- Reduce los costes de TI y mejora de la calidad del Servicio: aquellos procesos de TI con mayor madurez generan mayor productividad y reduzcan los costes.
- Permite implementar procesos integrados en toda el área de TI: define un modelo de procesos sustentados por roles y responsabilidades, los que generan una nueva forma de trabajo interno de la organización basada en las responsabilidades puntuales.

- Mejora la Integración de TI con el Negocio: el enfoque de Gestión de Servicios de TI permite alinear los servicios TI a los procesos de Negocio.
- Cumple eficientemente con las regulaciones: cumple con la necesidad de las regulaciones locales e internacionales, tales como Sabanes-Oxley (SOX), Base II, regulaciones gubernamentales, ISO/IEC 27001, ISO/IEC 38500 e ISO/IEC 20000, entre otras.
- Mejora la Gestión de proveedores: esclarece los niveles de servicio que se deben solicitar a los clientes.

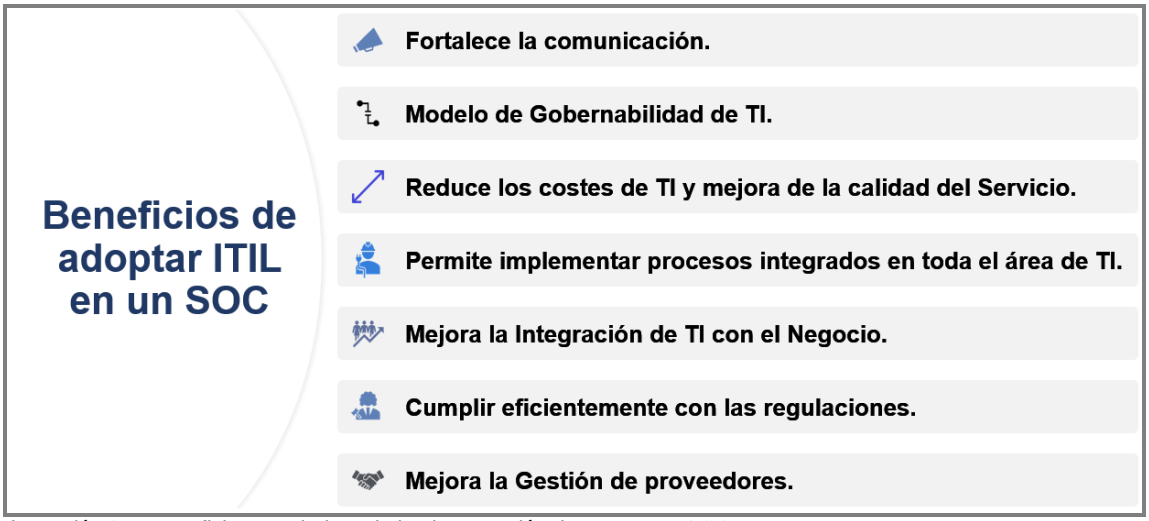

Ilustración 21 - Beneficios asociados a la implementación de ITIL en un SOC.

Al concluir esta primera etapa, la organización debe contar con una lista de objetivos corporativos asociados a los objetivos de tecnologías de la información. A partir de estas metas, se posibilita la realización de una identificación de los procesos necesarios que permitan dar cumplimiento a los objetivos de TI y, a su vez, a los objetivos de la empresa.

7.1.2 Identificación de las capacidades requeridas para dar cumplimiento a los objetivos de TI

3. Identificación de las capacidades requeridas para dar cumplimiento a los objetivos de TI

En este punto de la guía, se tiene en cuenta que los objetivos responden a la ejecución de procesos, por lo que cada uno de los servicios debe ser definido junto a sus capacidades. Por tanto, la evaluación de capacidades debe implicar los procesos, las personas y las tecnologías.

7.1.2.1 Procesos

3.1 Procesos

Los procesos son los encargados de ordenar las actividades y articular las operaciones. Se considera necesario que se encuentren adecuadamente documentados y con las métricas establecidas para medir su implementación. Entre los principales procesos, el SOC se encarga de evaluar la gestión de incidentes y la gestión de vulnerabilidades.

Los procesos que se plantean a continuación, pueden ser tomados como referencia y adaptarse a las particularidades de cada una de las organizaciones, por lo que pueden ser profundizados, simplificados o removidos en función del nivel de especialización que se pretenda lograr. Para este momento, se propone el análisis y ajuste de los siguientes servicios y procesos como parte del proceso de implementación del SOC:

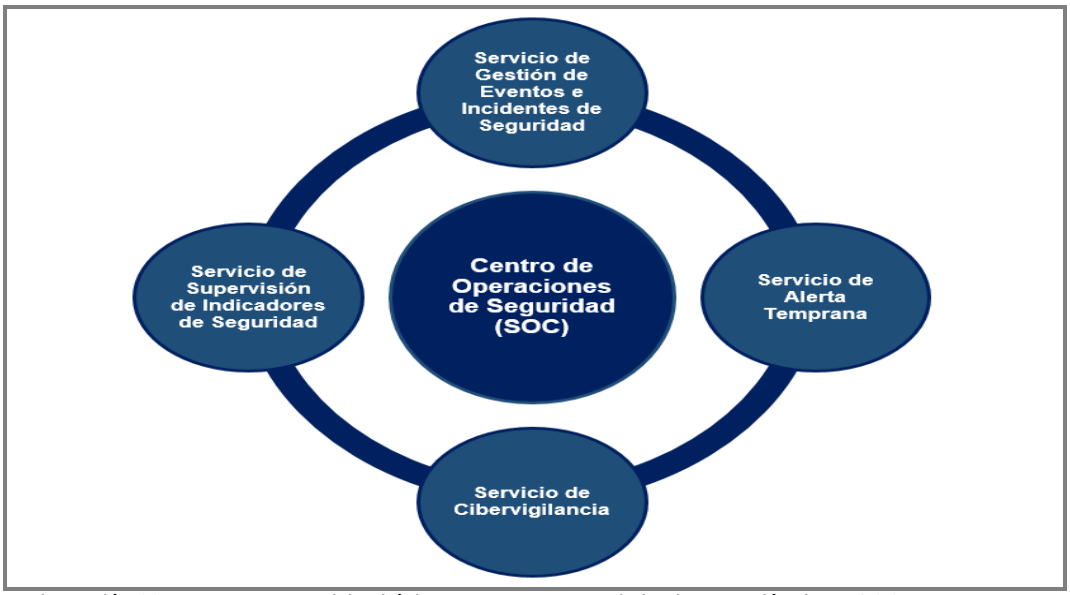

Ilustración 22 - Procesos y servicios básicos propuestos para la implementación de un SOC.

7.1.2.1.1 Servicio de gestión de eventos e incidentes

3.1.1 Servicio de gestión de eventos e incidentes

Las actividades del Servicio de gestión de eventos e incidentes que se proponen son, entre otras, las siguientes:

- Monitorización de eventos.
- Clasificación y triaje de eventos.

- Investigación.
- Registro de incidentes.
- Escalado interno de incidentes.
- Escalado externo de incidentes.
- Recogida de muestras y evidencias.
- Respuesta ante incidentes.
- Notificación de incidentes.
- Seguimiento de incidentes.
- Análisis post-incidente.

7.1.2.1.2 Servicio de Alerta Temprana

3.1.2 Servicio de Alerta Temprana

Las actividades del Servicio de Alerta Temprana que se proponen son, entre otras, las siguientes:

- Identificación y validación de alertas.
- Clasificación y triaje de alertas.
- Registro y notificación de alertas.
- Actualización de alertas.
- Seguimiento de alertas.

7.1.2.1.3 Servicio de Cibervigilancia

3.1.3 Servicio de Cibervigilancia

Las actividades del Servicio de Cibervigilancia que se proponen son, entre otras, las siguientes:

- Vigilancia de exfiltraciones notificadas.
- Vigilancia de metadatos en documentos expuestos en los sitios web corporativos.
- Vigilancia de foros relacionados con el hacking.
- Vigilancia de exposición en buscadores.

7.1.2.1.4 Servicio de Supervisión de indicadores de seguridad

3.1.4 Servicio de Supervisión de indicadores de seguridad

Las actividades del Servicio de Supervisión de indicadores de seguridad que se proponen son, entre otras, las siguientes:

- Recopilación de información sobre indicadores de seguridad
- Supervisión y respuesta ante indicadores
- Identificación y propuesta de nuevos indicadores de seguridad
- Parametrización de cuadros de mando.

7.1.2.2 Roles (personal)

3.2 Roles (personal)

Se considera necesario determinar las capacidades esperadas del personal del SOC. Por ello, resulta imprescindible que exista entendimiento e involucramiento por parte de la Alta Dirección en las funciones y servicios brindados por SOC, en donde se deben establecer los niveles de seguimiento, atención y apoyo que se le brinda.

Además, se debe tener en cuenta una estructura para la conformación del SOC, a partir de la experiencia de las personas, de su capacidad para trabajar bajo presión y de su capacitación técnica para afrontar las tareas. A continuación, se representa la estructura de roles piramidal que se sugiere para el SOC:

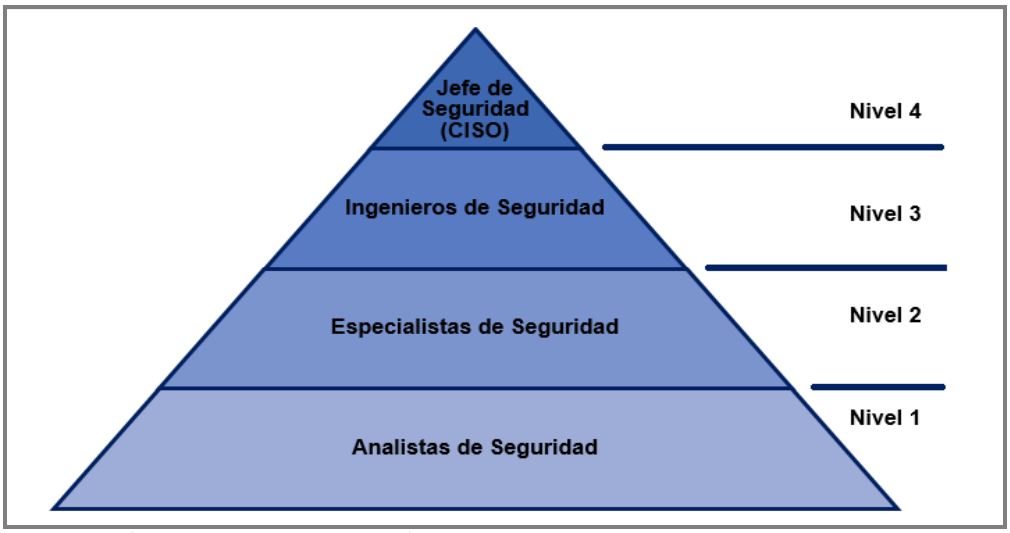

Ilustración 23 - Roles de Seguridad básicos en un SOC.

Página 6

Por tanto, tal y como se observa en la ilustración anterior, la estructura queda de la siguiente manera:

- Nivel 1: Analistas de Seguridad de la Información.
- Nivel 2: Especialistas de Seguridad de la Información.
- Nivel 3: Ingenieros de Seguridad de la Información.
- Nivel 4: Jefe de Seguridad de la Información (CISO).

7.1.2.3 Tecnología

3.3 Tecnología

Se debe realizar un análisis referente a la tecnología de la que dispone la organización, su estado de implementación y configuración y los niveles de atención. Resulta importante lograr identificar las tecnologías necesarias para que el SOC pueda ofrecer los servicios esperados a partir de los requisitos de la Alta Dirección. Además, se deben evaluar las redes de datos, los procesos de administración de registros de auditoria, la gestión de eventos e información de seguridad, la monitorización y detección de amenazas y el descubrimiento de vulnerabilidades, entre otros.

7.1.3 Elaboración de informe a partir de la recolección de la información

4. Elaboración de informe a partir de la recolección de la información

Una vez se disponga de los objetivos corporativos, de su materialización en objetivos de tecnologías de la información y de los servicios de TI que los sustentan, así como de un panorama general de las capacidades necesarias para la implementación del SOC y de las capacidades reales implementadas hasta este momento, se puede proceder a la elaboración de un informe que refleje estos resultados. Se trata del informe que explica la situación actual y la situación deseada.

Asimismo, en este proceso deben participar especialistas de diferentes ámbitos, de forma que pueda enriquecerse el documento y evitar conflictos futuros provocados por desconocimiento en el tema analizado. Por ello, el informe puede verse reforzado por documentos complementarios como:

- Inventario de activos y dependencias.

- Mapas de la red de ordenadores.
- Documentación de seguridad corporativa.
- Archivos de configuración y registros de *logs*.
- Procesos y procedimientos.
- Relación de controles de seguridad activos.

El informe, como objetivo básico, debe reflejar el estado actual del SOC. Además, debe contemplar la relación entre los objetivos corporativos y los objetivos de las tecnologías de la información. Por tanto, se destaca que el informe debe reflejar la visión y estrategia empresarial, a la misma vez que explica cómo la inclusión de la seguridad informática puede beneficiar a la organización.

Del mismo modo, en el desarrollo del informe pueden incluirse los hallazgos de la evaluación realizada representados a través de información resumida y estructurada. Por otra parte, en el caso de experimentar algún incidente, también debe quedar reflejado en este informe.

Ilustración 24 - Elaboración de informe de situaciones AS-IS y TO-BE para la implementación de un SOC.

7.1.4 Implementación de las metodologías agiles

5. Implementación de las metodologías agiles

Una vez se han establecido los objetivos y la comparativa entre el estado actual y el deseado para el SOC, se debe tener en cuenta que la

implementación de un Centro de Operaciones de Seguridad produce cambios en las organizaciones, por lo que, frecuentemente, se pueden encontrar resistencias en las diferentes áreas o en personas concretas implicadas en los cambios de la organización. En base a esta condición, se hace necesario preparar, junto a la alta dirección, al personal que pueda verse afectado para minimizar los problemas en este aspecto. Aquí es donde también juegan un papel importante las metodologías ágiles.

Las metodologías agiles se sustentan en el desarrollo incremental e iterativo y se caracterizan por tener una planificación adaptativa, un desarrollo iterativo y evolutivo y por dar respuesta rápida a los cambios. Se utilizan para conseguir el servicio, producto o software más funcional posible en el mínimo tiempo, a la vez que se disminuyen los riesgos y permiten, a cualquier proyecto, adaptarse a los cambios rápidamente. También desde el punto de vista del personal. Por tanto, se proponen las siguientes metodologías ágiles para la implementación de un SOC:

7.1.4.1 DevOps

5.1 DevOps

En relación con el sistema metodológico, se recomienda la aplicación de DevOps para estos tipos de procesos. Frecuentemente, las empresas se enfrenten a un problema de desajuste entre los departamentos de desarrollo y operaciones. Por lo general, los equipos de desarrollo de software construyen código a un ritmo acelerado, pero no se responsabilizan del proceso de despliegue, del que se encarga el equipo de operaciones. Como resultado, se obtiene un gran cúmulo de trabajo donde el equipo de operaciones se atasca debido a la cantidad de productos a desplegar. En un SOC, por ejemplo, se unificarían los procesos de desarrollo de escaneo de vulnerabilidades y las operaciones del proceso. Hecho que tendería a agilizar el proceso.

DevOps propone el uso de prácticas para resolver estas diferencias. Estas prácticas constituyen el valor fundamental por el que se ha decidido tener en cuenta su aplicación en la implementación de un Centro de Operaciones de Seguridad. A continuación, se definen los aportes que ofrece DevOps y por el que se ha escogido como metodología para el desarrollo de este proyecto:

- DevOps ofrece una fuerte estructura de TI que constituye una ventaja competitiva: Las empresas con una estructura organizativa avanzada tienen más probabilidades de aumentar su rendimiento y cuota de mercado, por lo que les permite alcanzar objetivos más ambiciosos.
- DevOps utiliza prácticas que mejoran el rendimiento en TI: Las técnicas de gestión, como son el uso de herramientas para control de versiones o la entrega continua, mejoran el rendimiento de la empresa.

- DevOps otorga importancia a la organización cultural de las empresas: El núcleo central de DevOps apuesta por la adecuada trasmisión de información, la colaboración participativa entre distintos equipos, las responsabilidades compartidas, la interiorización practica de aprender de los errores y dar paso a nuevas ideas. Este tipo de prácticas asegura que la empresa tenga más garantías y posibilidades de obtener buenos resultados, por lo que se considera que la organización cultural es uno de los activos más sólidos a nivel de rendimiento de TI y del rendimiento global de la empresa.
- DevOps propone que la satisfacción en equipos de TI es el principal elemento en una estructura organizativa: Se ha de tener en cuenta que, cuando la satisfacción en el trabajo es alta, los trabajadores dan el máximo de sí mismos, por lo que influye en el grado de compromiso con la empresa, así como en la creatividad y la productividad de su trabajo.

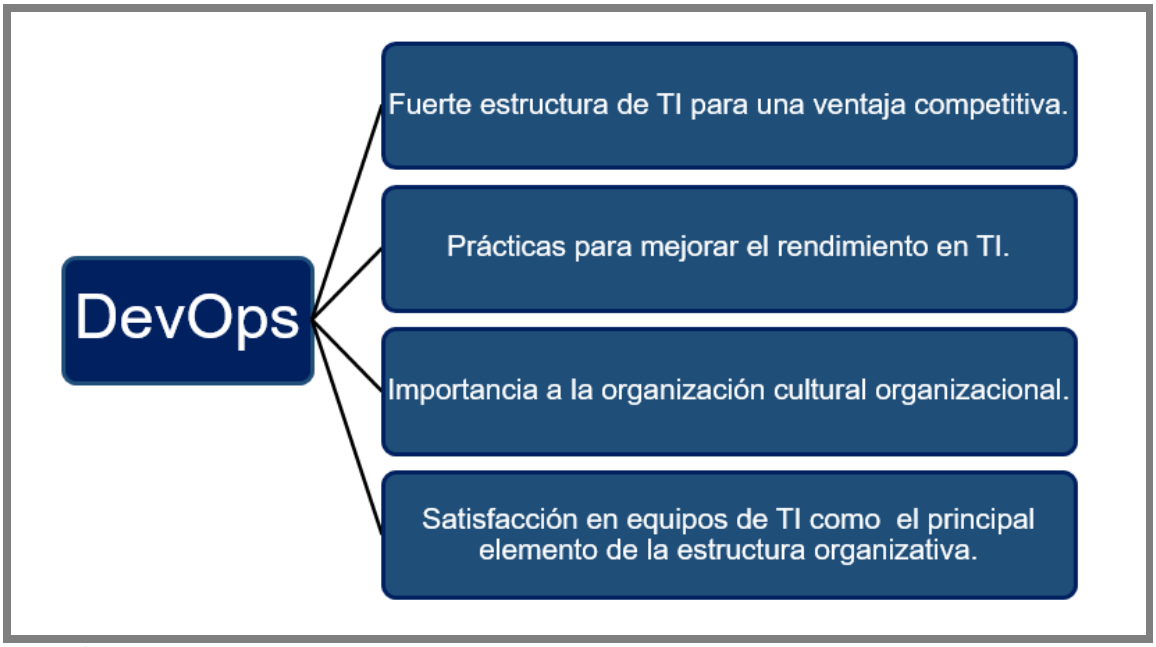

Ilustración 25 - Aportes que ofrece DevOps al desarrollo del proyecto.

7.1.4.2 Kanban

5.2 Kanban

Kanban se basa en el desarrollo incremental, por lo que divide el trabajo en partes. Además, utiliza técnicas visuales para ver la situación de cada tarea, que se representan en tableros de *post-its*. Por otra parte, estos *post-its* pueden tener información variada donde se abarque la descripción y la estimación de la duración de la tarea. Por tanto, la aplicación de Kanban en la implantación de

un SOC en cualquier organización puede ser útil para la definición de cada una de las tareas a desarrollar.

Esta metodología permite realizar entregas en cualquier momento, cambiar prioridades y la visualizar el flujo de trabajo. El método Kanban se considera el más indicado para las organizaciones que requieran de flexibilidad en la entrada de tareas, en su seguimiento, en su priorización, en la supervisión del equipo de trabajo y en los informes de dedicación.

Visualizar el flujo de trabajo permite mostrar los logros y problemas del proceso, identificar los diferentes riesgos o problemas que pueden generar cuellos de botellas en el flujo de ejecución (Salvay, s.f.). Es un enfoque para catalizar el cambio en una organización. Utiliza la limitación del "Trabajo en Proceso" o "*Work In Progress* (WIP)", como mecanismo de control para demostrar cuantas actividades por estado pueden ser trabajadas y, de esta forma, incentivar las discusiones de cambio.

Ilustración 26 – Ejemplo de tablero Kanban con mecanismos de control de actividades.

El proceso del equipo para el desarrollo de software y productos y la administración de proyectos siempre será único, adaptado a la medida del equipo y optimizado para darle valor al flujo de trabajo. Este proceso implica medición de riesgo, capacidades y habilidades del equipo, demanda del cliente, identificación, corrección de los cuellos de botella y variaciones que pueden afectar al equipo y a sus miembros.

La aplicación de la metodología Kanban implica la generación de un tablero de actividades que permitirá mejorar el flujo de trabajo y lograr un ritmo sostenible. Por ello, para implementar esta metodología es necesario tener en cuenta los siguientes aspectos:

- Definir el flujo de trabajo de los proyectos: Para esto es necesario crear un tablero visible y accesible a todos los miembros del equipo. El tablero debe contar con diferentes columnas que se corresponderán con el estado concreto del flujo de tareas.

- Visualizar las fases del ciclo de producción: Kanban se basa en el principio de desarrollo incremental, lo que implica dividir el trabajo en distintas partes, por lo que se agiliza el proceso de producción. El objetivo de la visualización se basa en clarificar al máximo el trabajo a realizar y las tareas asignadas a cada equipo de trabajo, así como definir las prioridades y la meta establecida.
- *Stop starting*, *start finishing*: Kanban prioriza el trabajo que está en curso antes de empezar nuevas tareas. Por esta razón, el trabajo en curso debe estar limitado, por lo que debe existir un número máximo de tareas a realizar en cada fase. No es posible abrir una nueva tarea sin finalizar otra.
- Control del flujo: Kanban mezcla tareas y proyectos, manteniendo a los trabajadores con un flujo de trabajo constante. Se desarrollan las tareas más importantes en cola y se brinda un seguimiento pasivo para no tener que interrumpir al trabajador en cada momento.

7.1.4.3 Unión de DevOps y Kanban

5.3 Unión de DevOps y Kanban

DevOps y Kanban constituyen dos metodologías agiles que no se consideran excluyentes, por lo que se tendrá en consideración el valor de cada una ellas en el plan de implementación de un Centro de Operaciones de Seguridad. Por consiguiente, entre los principales beneficios de usar Kanban junto a DevOps, se destaca que Kanban permite combinar múltiples flujos en uno, decir <<no>> a ciertas tareas y mejorar la comunicación visual del flujo de trabajo del equipo.

Asimismo, Kanban determina cuando se alcanzan los límites del WIP (no se puede hacer más tareas, sin sacrificar la productividad), ya que un equipo de DevOps trabaja, por lo general, en varios proyectos importantes a la vez y puede resultar fácil que algunas tareas se atasquen. Además, Kanban predica el tipo de actitud de “una vez comenzado, debe completarse”, lo que permite que los miembros del equipo identifiquen un problema y trabajen juntos en la finalización de cada tarea para la mejora tanto del flujo como de la comunicación del equipo.

Por último, se destaca que Kanban resulta muy valioso para un equipo de DevOps, desde el punto de vista de la gestión de proyectos y procesos, ya que se considera infinitamente flexible y puede abordar los problemas centrales del equipo de manera cómoda, ligera y discreta. Además, DevOps acerca la transformación cultural y facilita la creación de servicios y productos adaptados a las necesidades cambiantes de los clientes mientras busca agilizar las entregas a los clientes a través de la agilidad y la automatización.

7.1.5 Hoja de ruta

6. Hoja de ruta

La implementación de un SOC implica el diseño de una hoja de ruta donde se ubiquen, en el tiempo, la evolución del SOC en base a los servicios incorporados, la adopción y puesta en práctica de nuevas tecnologías, los cambios en la estructura y los restantes elementos que conlleven a la consecución de los objetivos. MITRE Corporation (2014) definió cuatro etapas que estiman el tiempo que transcurre entre la puesta en marcha y el pleno funcionamiento del Centro de Operaciones de Seguridad. Por tanto, en este trabajo se toman estas estimaciones como referencia para la confección de la hoja de ruta:

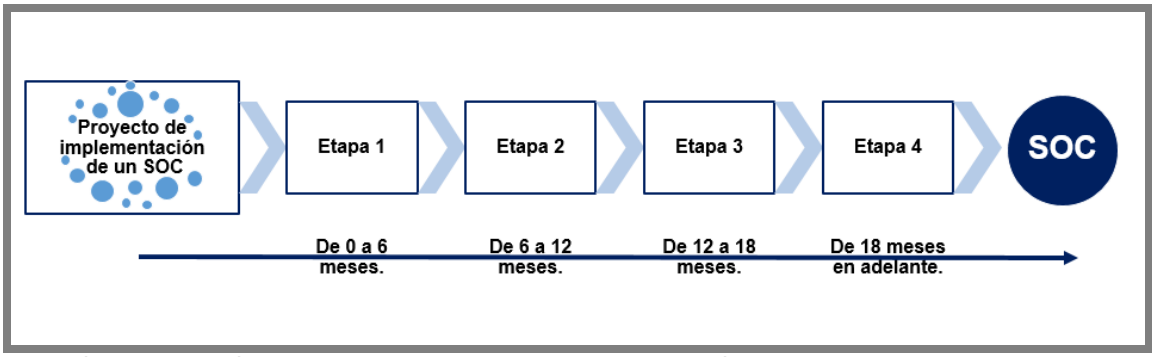

Ilustración 27 - Estimación temporal de la hoja de ruta para la implementación de un SOC.

7.1.5.1 Etapa 1

6.1 Etapa 1

La primera etapa de la implementación de un SOC abarca desde su fundación hasta, prácticamente, los primeros seis meses de su transcurso. Por ello, durante esta etapa se considera necesario atender a lo siguiente:

- Obtener la confirmación de las partes interesadas y las autoridades respecto a la misión, las funciones, las responsabilidades, delimitación del alcance del proceso de implementación.
- Formación del personal y su ubicación en el espacio físico integrado.
- Despliegue de las tecnologías.
- Identificación de los procesos críticos.

Además, se considera importante tener en cuenta aquellos elementos que se encuentran implementados para otorgarles valor y aprovecharlos en el contexto de la seguridad de la información.

7.1.5.2 Etapa 2

6.2 Etapa 2

La segunda etapa de la implementación de un SOC abarca desde los seis meses de transcurso del servicio hasta el primer año. Se trata del periodo en el SOC comienza a operar y brindar servicios. Por tanto, se considera importante atender los siguientes aspectos:

- Se debe establecer contacto con centros de respuesta a emergencias y otros Centros de Operaciones de Seguridad para permitir recibir información sobre inteligencia de seguridad y nutrirse de conocimiento.
- Se deben establecer los requisitos de compra de nuevas tecnologías que no están disponibles en este momento, así como la toma de responsabilidad de las tecnologías existentes por la organización.
- Se debe obtener experiencia en el uso y monitorización de las herramientas existentes.

Además, se considera el momento de iniciar y potenciar, en mayor volumen, el proceso de reclutamiento y formación de personal para alcanzar un mínimo del 50% del personal deseado.

7.1.5.3 Etapa 3

6.3 Etapa 3

La tercera fase de la implementación de un SOC abarca desde los 12 hasta los 18 meses. En este momento, se debe disponer de un local físico acomodado a la estructura del SOC y de las contrataciones y formación del personal deben girar alrededor del 90% de la plantilla. Por ello, en este momento se deben cumplir las siguientes actividades:

- Despliegue y formación de la nueva tecnología y formación y práctica de la tecnología existente en la organización.
- Activación de los procesos de monitorización continuo.
- Activación de los procesos de registro de eventos, incidentes y alertas de seguridad.

Además, en esta etapa, se recomienda también la interacción con otras áreas de la organización para ganar en visibilidad y ofrecer colaboración a sus servicios desde el punto de vista de la seguridad informática.

7.1.5.4 Etapa 4

6.4 Etapa 4

La cuarta y última fase de la implementación de un SOC se concibe a partir de los 18 meses. En este momento, el SOC debe funcionar a pleno rendimiento y cumplir con el alcance establecido para su cometido. Además, resulta necesario detectar y responder a las necesidades de crecimiento profesional del personal y al desarrollo organizacional. Por tanto, se deben atender los siguientes elementos:

- Los procesos deben alcanzar altos niveles de madurez.
- Los servicios de monitorización creados deben evolucionar para ganar madurez.
- Se deben refinar las técnicas de recolección de datos y análisis.

Asimismo, el SOC debe alcanzar al usuario final mediante campañas de concienciación y debe convertirse en el responsable de la información corporativa mediante las técnicas de calidad y de inteligencia de seguridad informática.

7.2 Anexo 2: Seguimiento de la PEC2 del TFG

7.2.1 Revisión de los objetivos y alcance del proyecto

Los objetivos del proyecto, tanto el principal como los parciales, se mantienen, tal y como se planificó desde el principio. 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.

7.2.2 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	Duración (horas)	Fecha de entrega	Verificación
Hito 2: Primera fase de ejecución del plan de trabajo (PEC2)	**13/03/2021**	**84**	**09/04/2021**	✓
Investigación y análisis de ITIL y metodologías agiles	13/03/2021	20	20/03/2021	✓
Análisis comparativo de ITIL y metodologías agiles	20/03/2021	14	25/03/2021	✓
Redacción de los aportes básicos	25/03/2021	8	28/03/2021	✓
Revisión bibliográfica sobre los servicios que formarán el SOC	28/03/2021	12	02/04/2021	✓
Definir los tipos de servicios que formarán el SOC	02/04/2021	14	06/04/2021	✓
Análisis de los riesgos.	06/04/2021	6	07/04/2021	✓
Redacción y revisión del entregable	07/04/2021	14	09/04/2021	✓

Tabla 34 - Planificación cumplida en el hito 2.

7.2.3 Revisión de los riesgos

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

7.2.4 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.

7.3 Anexo 3: Seguimiento de la PEC3 del TFG

7.3.1 Revisión de los objetivos y alcance del proyecto

Los objetivos del proyecto, tanto el principal como los parciales, se han cumplido, tal y como se concibió desde el principio del trabajo. Además, se ha planteado una justificación por la que no se desarrolla una planificación económica exacta y, únicamente, se dan valores orientativos para el coste en personal.

7.3.2 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	Duración (horas)	Fecha de entrega	Verificación
Hito 3:Segunda fase de ejecución del plan de trabajo (PEC3)	**10/04/2021**	**92**	**07/05/2021**	✓
Definición de requisitos exigibles específicos para cada uno de los servicios	10/04/2021	20	15/04/2021	✓
Análisis de métricas a aplicar a cada uno de los requisitos	15/04/2021	12	20/04/2021	✓
Identificación de los flujos de trabajo en cada tipo de servicio	20/04/2021	12	24/04/2021	✓
Definición de los roles encargados de gestionar la demanda y la entrega para cada uno de los servicios	24/04/2021	12	28/04/2021	✓
Elaboración del Plan de implementación para el SOC (Anexo 1)	28/04/2021	16	03/05/2021	✓
Análisis de los riesgos	03/05/2021	6	05/05/2021	✓
Redacción y revisión del entregable	05/05/2021	14	07/05/2021	✓

Tabla 35 - Planificación cumplida en el hito 3.

7.3.3 Revisión de los riesgos

No se han detectado ninguno de los riesgos en pronóstico ni se han detectado riesgos imprevistos en esta entrega.

7.3.4 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 el desarrollo del proyecto y se han culminado con la entrega del producto deseado.