ARQUITECTURA Y MODELO DE GESTIÓN COMO PRINCIPALES REQUERIMIENTOS DE IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD

SEBASTIAN CABALLERO BARRAGAN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CALI
2022

ARQUITECTURA Y MODELO DE GESTIÓN COMO PRINCIPALES REQUERIMIENTOS DE IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD

SEBASTIAN CABALLERO BARRAGAN

Monografía presentada para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMÁTICA

JOEL CARROLL
Director de trabajo de grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CALI
2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

TABLA DE CONTENIDO

LISTA DE CUADROS

Pag.

LISTA DE IMAGENES

Pág.

GLOSARIO

Amenaza: Puede describirse como cualquier actividad que busque sacar provecho de una vulnerabilidad, con el objetivo de afectar la seguridad de un sistema informático[1].

Analista del SOC. Es el grupo de personal encargado del monitoreo continuo de los eventos que aparecen en la red monitoreada. Estos pueden dividirse en diferentes niveles, según su nivel de experticia y responsabilidad frente a las acciones del SOC[2]

Ataque: Intento de destruir de alguna manera un activo, también puede asociarse con el robo de accesos para acceder de forma no autorizada a un sistema de información[3].

Centro de operaciones de seguridad: Puede definirse como un conjunto de personas, procesos y tecnología que tienen como objetivo proteger los sistemas de información de las organizaciones mediante la utilización de sistemas de monitoreo, detección de estados no deseados y reducción de efectos asociados a eventos no deseados[4].

Confidencialidad[5]: Característica que hace que la información no pueda ser accedida por personal no autorizado.

Coordinador del SOC[6]: Es el líder del centro de operaciones, normalmente actúa como gerente del SOC, gestionando tanto los recursos tecnológicos como los humanos y financieros del mismo.

---

[1] INCIBE. “Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?”. {En línea}. {15 de abril de 2022} disponible en: (https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian).

[2] LELAND, Michael. & VALENZUELA, Ismael. “SOCwise: A Security Operation Center (SOC) Resource to Bookmark”. {En línea}. {15 de abril de 2022} disponible en: (https://www.mcafee.com/blogs/enterprise/security-operations/socwise-a-security-operation-center-soc-resource-to-bookmark/).

[3] NETWORK WORKING GROUP. “RFC4949. Internet Security Glosary, version 2”. {En línea}. {15 de abril de 2022} disponible en: (https://datatracker.ietf.org/doc/html/rfc4949).

[4] COMPTIA. “What Is a Security Operations Center?”. {En línea}. {5 de febrero de 2022} disponible en: (https://www.comptia.org/content/articles/what-is-a-security-operations-center).

[5] INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Visión general y vocabulario. Bogotá. ICONTEC. 2017.

[6] VEERAPPA, Babbu. “Security Operations Centre (SOC) in Utility Organizations”. {En línea}. {6 de marzo de 2022} disponible en: (https://sansorg.egnyte.com/dl/gtxpv0pW5T/?).

Disponibilidad[7]: Característica que hace que la información pueda ser accedida en el momento en que es requerida por aquellos que tienen acceso a ella.

Incidente de seguridad[8]: Son eventos que de alguna manera pueden llegar a afectar algunas de las características de la triada de la seguridad de la información, confidencialidad, integridad o disponibilidad

Integridad[9]: Característica que garantiza la exactitud y completitud de la información.

LOG[10]: Es un tipo de registro de acciones ejecutadas en diferentes sistemas o equipos informáticos, los cuales permiten detectar tanto errores, malos funcionamientos, fallos, así como intentos fallidos de acceso, accesos no autorizados, intentos de acceso exitosos, entre otros eventos. La monitorización de estos de forma manual o mediante el uso de herramientas especializadas, permite generar alertas de seguridad que pueden ser interpretadas para evitar la materialización de un incidente de seguridad.

Riesgo[11]: Un riesgo de seguridad informática se entiende como la probabilidad de que una amenaza explote una vulnerabi¨ ˙ad, logrando de alguna manera tener un impacto negativo en el funcionamiento del sistema informático afectado.

SIEM[12]: Es una herramienta tecnológica especializada en la recolección de logs, alertas de seguridad, y eventos, en una consola central, la cual puede proporcionar análisis en tiempo real de lo que puede estar sucediendo en una red.

Vulnerabilidad[13]: Una vulnerabilidad podría describirse como una debilidad propia de un sistema informático, la cual podría poner en riesgo la seguridad de este, facilitando que un ciberdelincuente pueda afectar los pilares de la seguridad de la información.

---

[7] INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Visión general y vocabulario. Bogotá. ICONTEC. 2017.

[8] Ibid.

[9] Ibid.

[10] INCIBE. “Gestión de logs: Políticas de seguridad para la Pyme”. {En línea}. {15 de abril de 2022} disponible en: (https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/gestion-logs.pdf).

[11] PINZÓN, Iralda. Gestión del riesgo en Seguridad Informática. Bogotá, 2018. pp 3 – 5. Trabajo de grado (Especialista en Seguridad Informática). Universidad Piloto De Colombia. Facultad de ingeniería

[12] GAST, Kelsey. “What is SIEM? And How Does It Work?”. {En línea}. {15 de abril de 2022} disponible en: (https://logrhythm.com/what-is-siem/).

[13] INCIBE. “Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?”. {En línea}. {15 de abril de 2022} disponible en: (https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian).

RESUMEN

Es bien conocido que, en la actualidad, la gran mayoría de la información de una compañía se encuentra digitalizada. Dicha información digital, se convierte entonces en uno de los activos más valiosos tanto para la compañía como para los ciberdelincuentes que quieren apoderarse de ella.

Surge entonces la necesidad de contar con diferentes mecanismos que permitan a las organizaciones velar por la seguridad de dichos activos; los centros de operaciones de seguridad o SOC por sus siglas en inglés (Security Operation Center), son uno de estos mecanismos, los cuales combinan herramientas tecnológicas, procedimientos de operación, conocimiento y habilidades de personas, buscando proteger los activos informáticos de una compañía.

La investigación por desarrollar busca presentar una guía documental para el definir la arquitectura y el modelo de gestión al momento de implementar un Centro de Operaciones de Seguridad. Para ello, se plantea realizar el estudio de diferentes modelos y arquitecturas de centros de operaciones de seguridad existentes, así como de diferentes marcos de trabajo para la operación de los mismos.

Al finalizar el documento se espera contar con un estudio base que permita guiar a líderes del área de seguridad informática o ciberseguridad en la creación de un Centro de Operaciones de Seguridad partiendo de la definición de dos requerimientos importantes para su implementación, el modelo de gestión y su arquitectura.

Palabras claves: Arquitectura, Ciberseguridad, Ciberdefensa, Gestión, Implementación, SOC, Seguridad, Tecnología.

ABSTRACT

It is well known that, today, the vast majority of a company's information is digitized. This digital information then becomes one of the most valuable assets both for the company and for the cybercriminals who want to seize it.

The need arises then to have different mechanisms that allow organizations to ensure the security of said assets; the security operations centers or SOC for its acronym in English (Security Operation Center), are one of these mechanisms, which combine technological tools, operating procedures, knowledge and skills of people, seeking to protect the computer assets of a company.

The research to be developed seeks to present a documentary guide to define the architecture and the management model when implementing a security operations center. To do this, it is proposed to study different models and architectures of existing security operations centers, as well as different frameworks for their operation.

At the end of the document, it is expected to have a base study that will allow to guide leaders in the area of computer security or cybersecurity in the creation of a security operations center based on the definition of two of the most important requirements for its implementation, the management model and its architecture.

Keywords: Architecture, Cybersecurity, Cyber-defense, Implementation, Management, SOC, Security, Technology.

INTRODUCCIÓN

La ciberseguridad se ha vuelto uno de los principales retos de la gran mayoría de organizaciones alrededor del mundo, la expansión acelerada del uso de la tecnología como soporte para la mayoría de los procesos de las empresas, ha hecho que las superficies de ataque sean cada vez más amplias, llamando la atención de más grupos de ciberdelincuentes. Esto ha hecho que no sea tarea sencilla proteger la información de usuarios, de la organización, de clientes y proveedores; son múltiples las herramientas de seguridad que pueden implementar las organizaciones para intentar mantener a raya a los atacantes, estas pueden ir desde firewalls, IDS/IPS, antivirus, NAC, herramientas de prevención de fugas de información, WAF, entre otras.

Esta basta cantidad de herramientas, en algunas ocasiones pueden llegar a ser difíciles de administrar y podrían incluso presentarse situaciones en que la gran cantidad de información recibida desde cada herramienta disminuya la visibilidad de los eventos realmente relevantes para la red.

Existen herramientas que pueden ayudar a solventar el inconveniente que podría llegar a causar el uso excesivo de herramientas y aplicaciones de seguridad, una de las más populares son los SIEM, por sus siglas en inglés, *Security Informatión and Event Manager.* Dichas herramientas permiten recolectar en una sola consola central los eventos de mayor relevancia generados por otras herramientas de seguridad y encontrando la relación existente entre cada uno de ellos.

Los SIEM se convierten entonces en una herramienta de gran utilidad para gestionar de forma centralizada la seguridad de una organización, sin embargo, por si solos los SIEM no realizan todo el trabajo, es necesario que se cuente con personal experto capaz de analizar y gestionar las alertas que se puedan identificar en la herramientas, dicha necesidad puede ser cubierta por los Centros de Operaciones de Seguridad, los cuales pueden proporcionar la experticia para realizar el análisis adecuado de dichas alertas (personas), así como tener la capacidad de gestionar los eventos detectados de manera adecuada (procesos) y contar con otras herramientas que podrían ayudar a cerrar cualquier tipo de brecha de seguridad identificada durante el monitoreo (tecnologías).

En este documento se busca realizar un acercamiento a los Centros de Operaciones de seguridad como una pieza fundamental en las compañías frente a las amenazas de ciberseguridad a las que pueden estar expuestas, dicho acercamiento se realizará desde el estudio de la arquitectura y modelo de gestión de los SOC como unos de los requerimientos de implementación más relevantes; para ello se plantea la evaluación de centros de operaciones de seguridad ya implementados, el estudio de marcos de trabajo de ciberseguridad, seguridad informática o seguridad de la información como base para la definición del modelo de gestión y por último la

selección de herramientas y estimación del presupuesto de implementación de un Centro de Operaciones de Seguridad.

El trabajo realizado busca convertirse en una guía de consulta para los líderes de seguridad de diferentes compañías a nivel nacional, de manera que sirva como base para el inicio de la implementación de un Centro de Operaciones de Seguridad, aportando al mejoramiento de la ciberseguridad.

1. DEFINICIÓN DEL PROBLEMA

1.1. ANTECEDENTES DEL PROBLEMA

Un Centro de Operaciones de Seguridad[14] es una herramienta de gestión que permite a las compañías y organizaciones, centralizar el problema de la ciberseguridad en un solo equipo, de esta manera, se logran cubrir varios aspectos relevantes como la seguridad perimetral, el análisis de eventos, el análisis de intentos de intrusión, la contaminación por malware, la fuga de información, los accesos no autorizados y demás amenazas a las que se ve expuesta una compañía, desde un único punto central de gestión.

Normalmente los centros de operaciones de seguridad suelen ser equipos conformados por grupos de expertos en inteligencia y cacería de ciber amenazas, los cuales se pueden dividir en diferentes niveles jerárquicos dentro del equipo, según su nivel de experticia, las actividades que ejecutan e incluso su nivel de atención a clientes tanto internos como externos de la compañía dueña del SOC.

Adicionalmente, los centros de operaciones de seguridad complementan su operación con el uso de diferentes herramientas tecnológicas que permiten realizar un análisis más completo de la situación de seguridad que vive la red de una organización, dichas herramientas pueden ir desde software para correlación de eventos, herramientas para el análisis de vulnerabilidades, software para la detección de intrusos, hasta las mismas herramientas de los diferentes sistemas operativos, las cuales permiten enviar logs o registros a una consola de análisis central.

Los dos componentes anteriormente mencionados se articulan mediante los diferentes procedimientos del Centro de Operaciones de Seguridad, los cuales pueden estar enfocados en la gestión de eventos e incidentes, la ejecución de las labores de cacería de amenazas, gestión de vulnerabilidades, generación de alertas o boletines de seguridad, entre otros. Dichos procedimientos permiten completar la tríada personas, tecnologías y procesos, la cual es base del funcionamiento de los centros de operaciones de seguridad.

Las organizaciones privadas y públicas del país no se ven exentas de recibir un buen número de ataques por año, esto se ve reflejado en la cantidad de noticias asociadas a seguridad informática y ciberseguridad que presentan los diferentes medios de comunicación en los últimos años. Esta situación ha ido empeorando tanto en Latinoamérica como en el país, el cual ocupó el tercer lugar en el top de

[14] COMPTIA. “What Is a Security Operations Center?”. {En línea}. {5 de febrero de 2022} disponible en: (https://www.comptia.org/content/articles/what-is-a-security-operations-center).

países con más fraudes asociados a cibercrimen en la región en el año 2020, esto según lo presenta la revista Semana[15] en una de sus publicaciones web.

Sin duda alguna, la pandemia del Covid-19 y la nueva realidad laboral que trajo consigo, ha sido uno de los cambios tecnológicos más grandes que hemos tenido en los últimos años, la gran mayoría de las compañías se han volcado a la virtualidad y esto ha hecho que el cibercrimen aumente debido a la expansión de la superficie de ataque, esto según lo expuesto por la INTERPOL[16]. Dichos aumentos hablan de cifras cercanas al 569% para el aumento en la creación de dominios maliciosos.

Por lo anteriormente expuesto, es que se puede apreciar que existe una mayor preocupación en cuando a la adecuada preparación de mecanismos de ciberdefensa tanto para organizaciones públicas como privadas, dichos esfuerzos se ven reflejados en diferentes propuestas, tal como la que presenta en su trabajo de grado, “Centro de operaciones de seguridad. Estrategia, diseño y gestión”, Biggeri Patricio[17], en esta hace un acercamiento a los SOC, desde el enfoque de estos como solución al problema de gestión de la ciberdefensa, demostrando como la triada personas, procesos y tecnología, juegan un rol de suma importancia en la implementación y puesta en marcha de un Centro de Operaciones de Seguridad.

Dentro del país, se presentan propuestas como el trabajo realizado por Cuellar Jorge y Pompeyo Daniel[18], en el cual presentan el “Diseño del Esquema de implementación de un Centro de Operaciones de Seguridad (SOC) de la información en la empresa KPMG en la sede de Bogotá D.C. – Colombia”. En este, enfocan su análisis inicial en el estudio de las mejores prácticas asociadas a ciberseguridad, para relacionarlas con la triada personas, procesos y tecnologías, con el objetivo de definir las necesidades de implementación del SOC en la Compañía seleccionada por los autores. En su propuesta logran mostrar como el diseño propuesto puede brindar las bases para mejorar la seguridad de la información de la compañía.

---

[15] SEMANA. “Colombia ocupó el tercer lugar en el ‘ranking’ de cibercrimen en América Latina”. {En línea}. {23 de febrero de 2022} disponible en: (https://www.semana.com/tecnologia/articulo/colombia-ocupo-el-tercer-lugar-en-el-ranking-de-cibercrimen-en-america-latina/202117/).

[16] INTERPOL. “Ciberdelincuencia: Efector de la COVID-19”. {En línea}. {3 de febrero de 2022} disponible en: (https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19).

[17] BIGGERI HERNAN, Patricio. Centro de operaciones de seguridad. Estrategia, diseño y gestión. Buenos Aires, 2018, pp 34-69. Trabajo de grado (Maestría en Gestión Estratégica de Sistemas y Tecnologías de la Información). Facultad de Ciencias Económicas.

[18] CUELLAR RODRIGUEZ, Jorge. POMPEYO, Daniel. Diseño del esquema de implementación de un centro de operaciones de seguridad (SOC) de la información en la empresa KPMG en la sede de Bogotá D.C. – Colombia. Bogotá, 2021. pp 35 – 89. Proyecto de grado (Especialista en Seguridad Informática). Universidad Piloto De Colombia. Facultad de ingeniería.

De la misma manera, en su trabajo “Diseño y planificación de un Centro de Operaciones de Seguridad informática aplicado como servicio por la organización A3SEC bajo marcos de trabajo propuestos por SANS, ISACA y NIST”, Bonilla Billy y Rojas Anthony[19], realizan un acercamiento al diseño de un SOC, basado en marcos de trabajo propuestos por tres de las organizaciones de seguridad informática más conocidas a nivel mundial.

El contexto anterior lleva a pensar en lo importante que pueden llegar a ser los centros de operaciones de seguridad como mecanismos de defensa frente a las diferentes amenazas a las que se puede ver expuesta una compañía, además de ello es claramente observable que la definición adecuada de la arquitectura y modelo de gestión de un Centro de Operaciones de Seguridad es parte fundamental de su puesta en operación. Surge entonces la siguiente pregunta problema:

1.2. FORMULACIÓN DEL PROBLEMA

¿De qué manera definir la arquitectura y el modelo de gestión necesario para poner en operación un Centro de Operaciones de Seguridad?

[19] BONILLA BLANCO, Billy Mauricio. ROJAS PATERNINA, Anthony. Diseño y planificación de un centro de operaciones de seguridad informática aplicado como servicio por la organización A3SEC bajo marcos de trabajo propuestos por SANS, ISACA Y NIST. Bogotá, 2019. pp 70 -100. Trabajo de grado (Especialista en Seguridad Informática). Universidad Piloto de Colombia. Facultad de Ingeniería.

2. JUSTIFICACIÓN

En el año 2020, Colombia tuvo entre marzo y noviembre, alrededor de 32 mil reportes asociados a casos de ciber amenazas, los cuales fueron reportados ante la fiscalía general de la nación[20]. Claramente, este número de amenazas reportadas están directamente relacionadas con el volcamiento hacia la virtualidad, que trajo consigo la actual pandemia del COVID-19. Sin embargo, en años pre-pandemia, y se había evidenciado un crecimiento en los ataques informáticos, no solo en Colombia, sino en la región, Latinoamérica, donde en el año 2019, se observaba que ocurrían alrededor de 6,4 ataques asociados a malware en dispositivos móviles por segundo[21].

Lo anterior permite tener una perspectiva inicial del panorama de ciberseguridad que se vive en el país, lo que da muestra del nivel de exposición que tienen las diferentes compañías del país. Sin lugar a duda, las auditorías o monitoreos de seguridad, buscando generar alertas tempranas, serán unas de las estrategias más valiosas a la hora de hacer frente a este la mayoría de las amenazas a las que estamos expuestos[22].

Una de las herramientas de gestión y auditoría de seguridad informática que pueden ayudar a las empresas son los centros de operaciones de seguridad, los cuales son equipos conformados por personas, procesos y tecnología, los cuales permiten identificar amenazas antes de que logren afectar la red de una compañía, mediante la generación de alertas tempranas. Estos equipos también tienen el nivel de preparación para contener y erradicar las posibles amenazas que logren colarse dentro de la red de una organización.

La propuesta de monografía presentada busca realizar un estudio de las diferentes arquitecturas y modelos de gestión utilizados por algunos centros de operaciones de seguridad, apuntando a definir una base documental, que pueda ser utilizada como guía para el diseño, creación y puesta en marcha de un SOC en las compañías del país, de manera que estas puedan gestionar de una manera más adecuada sus defensas frente a las diferentes ciber amenazas a las cuales puede estar expuestas.

---

[20] CCIT. “Cifras de ciberseguridad en Colombia prenden alarmas al cierre del 2020”. {En línea}. {14 de mayo de 2022} disponible en: (https://www.ccit.org.co/noticias/cifras-de-ciberseguridad-en-colombia-prenden-alarmas-al-cierre-del-2020/).

[21] TECNÓSFERA. “El cibercrimen no descansa, estas son las proyecciones para el 2020”. {En línea}. {6 de marzo de 2022} disponible en: (https://www.eltiempo.com/tecnosfera/dispositivos/cifras-de-ciberataques-de-2019-y-tendencias-para-el-2020-435508).

[22] HOYOS BUITRON, Victor Antonio. ¿Qué tal esta Colombia en cuestión de Ciberseguridad?. Bogotá, 2015. pp 10-15. Proyecto de grado (Especialización En Administración De La Seguridad). Universidad Militar Nueva Granada. Facultad De Relaciones Internacionales, Estrategia Y Seguridad.

3. OBJETIVOS

3.1. OBJETIVOS GENERAL

Proponer una arquitectura y modelo de gestión adecuado para la implementación de un Centro de Operaciones de Seguridad.

3.2. OBJETIVOS ESPECÍFICOS

Evaluar el diseño de al menos dos centros de operaciones de seguridad implementados en pequeñas empresas o en empresas de tamaño superior.

Comparar como mínimo dos marcos de trabajo enfocados en ciberseguridad, seguridad informática o seguridad de la información que puedan ser utilizados para la definición del modelo de gestión de un Centro de Operaciones de Seguridad.

Seleccionar las principales herramientas que hacen parte de la arquitectura de un Centro de Operaciones de Seguridad.

Estimar los posibles costos asociados a la implementación de un Centro de Operaciones de Seguridad.

4. MARCO REFERENCIAL

4.1. MARCO TEÓRICO

Dentro de los referentes bibliográficos abordados para la elaboración de esta monografía, se tuvieron en cuenta aquellos que pudieran aportar al estudio de las diferentes metodologías, marcos de trabajo, estrategias y modelos de gestión asociados a Centro de Operaciones de Seguridad, los mecanismos para su implementación y las herramientas que pudieran ser utilizadas para ello. A continuación, se presentan algunos referentes que se estudiaron para el desarrollo de la investigación.

En su trabajo de grado, “Centro de operaciones de seguridad. Estrategia, diseño y gestión”, Biggeri Patricio[23], hace un acercamiento a los SOC, desde el enfoque de estos como solución al problema de gestión de la ciberdefensa. Demostrando como la triada persona, procesos y tecnología, juegan un rol de suma importancia en la implementación y puesta en marcha de un Centro de Operaciones de Seguridad.

También se incluye como base de estudio, el trabajo realizado por Cuellar Jorge y Pompeyo Daniel[24], en el cual presentan el “Diseño del Esquema de implementación de un Centro de Operaciones de Seguridad (SOC) de la información en la empresa KPMG en la sede de Bogotá D.C. – Colombia”. En este, enfocan su análisis inicial en el estudio de las mejores prácticas asociadas a ciberseguridad, para relacionarlas con la triada persona, procesos y tecnologías, con el objetivo de definir las necesidades de implementación del SOC en la Compañía seleccionada por los autores. En su propuesta logran mostrar como el diseño propuesto puede brindar las bases para mejorar la seguridad de la información de la compañía.

En el trabajo “Diseño y planificación de un Centro de Operaciones de Seguridad informática aplicado como servicio por la organización A3SEC bajo marcos de trabajo propuestos por SANS, ISACA y NIST”, Bonilla Billy y Rojas Anthony[25], realizan un acercamiento al diseño de un SOC, basado en marcos de trabajo propuestos por tres de las organizaciones de seguridad informática más conocidas

[23] BIGGERI HERNAN, Patricio. Centro de operaciones de seguridad. Estrategia, diseño y gestión. Buenos Aires, 2018, pp 34-69. Trabajo de grado (Maestría en Gestión Estratégica de Sistemas y Tecnologías de la Información). Facultad de Ciencias Económicas.

[24] CUELLAR RODRIGUEZ, Jorge. POMPEYO, Daniel. Diseño del esquema de implementación de un centro de operaciones de seguridad (SOC) de la información en la empresa KPMG en la sede de Bogotá D.C. – Colombia. Bogotá, 2021. pp 35 – 89. Proyecto de grado (Especialista en Seguridad Informática). Universidad Piloto De Colombia. Facultad de ingeniería.

[25] BONILLA BLANCO, Billy Mauricio. ROJAS PATERNINA, Anthony. Diseño y planificación de un centro de operaciones de seguridad informática aplicado como servicio por la organización A3SEC bajo marcos de trabajo propuestos por SANS, ISACA Y NIST. Bogotá, 2019. pp 70 -100. Trabajo de grado (Especialista en Seguridad Informática). Universidad Piloto de Colombia. Facultad de Ingeniería.

a nivel mundial, lo cual entrega a la investigación, los puntos de partida para realizar el análisis de los diferentes marcos de trabajo para la implementación de un Centro de Operaciones de Seguridad.

4.1.1. Conceptos clave. La base teórica analizada en este documento se centra en elementos de seguridad informática y ciberseguridad, para ello, a continuación, se presentan los conceptos claves para el entendimiento de la monografía desarrollada:

4.1.2. Centro de operaciones de seguridad. *Puede definirse como un conjunto de personas, procesos y tecnología que tienen como objetivo proteger los sistemas de información de las organizaciones mediante la utilización de sistemas de monitoreo, detección de estados no deseados y reducción de efectos asociados a eventos no deseados, esto según lo descrito por el CompTIA en su publicación "What is a Security Operation Center"*[26]***.***

4.1.3. Analista del SOC. *Es el grupo de personal encargado del monitoreo continuo de los eventos que aparecen en la red monitoreada. Estos pueden dividirse en diferentes niveles, según su nivel de experticia y responsabilidad frente a las acciones del SOC*[27]***.***

4.1.4. Coordinador del SOC. *Es el líder del centro de operaciones, normalmente actúa como gerente del SOC, gestionando tanto los recursos tecnológicos como los humanos y financieros del mismo*[28]***.***

4.1.5. LOG. Tal como describe INCIBE[29] en su documento "Gestión de logs: Políticas de seguridad para la pyme", los logs son registros de acciones ejecutadas en diferentes sistemas o equipos informáticos, los cuales permiten detectar tanto errores, malos funcionamientos, fallos, así como intentos fallidos de acceso, accesos no autorizados, intentos de acceso exitosos, entre otros eventos. La monitorización de estos de forma manual o mediante el uso de herramientas especializadas, permite generar alertas de seguridad que pueden ser interpretadas para evitar la materialización de un incidente de seguridad.

4.1.6. SIEM. Es una herramienta tecnológica especializada en la recolección de logs, alertas de seguridad, y eventos, en una consola central, la cual puede proporcionar análisis en tiempo real de lo que puede estar sucediendo en una red.

---

[26] COMPTIA. "What Is a Security Operations Center?". {En línea}. {5 de febrero de 2022} disponible en: (https://www.comptia.org/content/articles/what-is-a-security-operations-center).
[27] MCAFEE COMMUNITY. (2020). Creating and Maintaining a SOC
[28] VEERAPPA, Babbu. "Security Operations Centre (SOC) in Utility Organizations". {En línea}. {6 de marzo de 2022} disponible en: (https://sansorg.egnyte.com/dl/gtxpv0pW5T/?).
[29] INCIBE. "Gestión de logs: Políticas de seguridad para la Pyme". {En línea}. {15 de abril de 2022} disponible en: (https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/gestion-logs.pdf).

Tal como describe Gast K.[30] de LogRythm, un SIEM puede traer grandes ventajas para un Centro de Operaciones de Seguridad, entre ellas se destacan la visibilidad en tiempo real de lo que sucede en el ambiente monitoreado, la gestión centralizada de logs y alertas, la reducción de alertas asociadas a falsos positivos, la reducción de los tiempos de detección y respuesta, entre otros.

Incidente de seguridad. Según lo descrito en la norma técnica ISO/IEC[31] 27035, son eventos que de alguna manera pueden llegar a afectar algunas de las características de la triada de la seguridad de la información, confidencialidad, integridad o disponibilidad.

Fases de la respuesta a incidentes. Según lo descrito en el libro "Security Operations Center Building, Operating and Maintaining Your SOC" de Muniz, McIntyre y Alfardan32, una de las actividades fundamentales de un Centro de Operaciones de Seguridad es la de gestionar incidentes, dicha actividad cuenta con las siguientes fases: Preparación, detección, clasificación y respuesta inicial, recolección y análisis de datos, reporte y actividades post-incidente.

Riesgo. Un riesgo de seguridad informática se entiende como la probabilidad de que una amenaza explote una vulnerabilidad, logrando de alguna manera tener un impacto negativo en el funcionamiento del sistema informático afectado. Esto según lo descrito por Pinzon[33] en "Gestión del riesgo en Seguridad informática".

Vulnerabilidades y amenazas. Tal como lo describe el INCIBE[34], una vulnerabilidad podría describirse como una debilidad propia de un sistema informático, la cual podría poner en riesgo la seguridad de este, facilitando que un ciberdelincuente pueda afectar los pilares de la seguridad de la información en este. Una amenaza, puede describirse como cualquier actividad que busque sacar provecho de una vulnerabilidad, con el objetivo de afectar la seguridad del sistema informático.

[30] GAST, Kelsey. "What is SIEM? And How Does It Work?". {En línea}. {15 de abril de 2022} disponible en: (https://logrhythm.com/what-is-siem/).
[31] INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Técnicas de seguridad. Gestión de incidentes de seguridad de la información. Bogotá. ICONTECT. 2016.
[32] MUNIZ, Joseph. MCINTYRE, Gary. ALFARDAN, Nadhem. Security Operations Center: Building, Operating, and Maintaining Your Soc. Hoboken: Cisco Press, 2015, pp 45 – 60.
[33] PINZÓN, Iralda. Gestión del riesgo en Seguridad Informática. Bogotá, 2018. pp 3 – 5. Trabajo de grado (Especialista en Seguridad Informática). Universidad Piloto De Colombia. Facultad de ingeniería.
[34] INCIBE. "Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?". {En línea}. {15 de abril de 2022} disponible en: (https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian).

4.1.7. Estudios referenciales de la monografía. Como herramientas adicionales para la construcción de este documento, también se realiza un estudio de diferentes artículos asociados a la gestión de centros de operaciones de seguridad. Estos se enfocan en lo siguiente:

4.1.7.1. Clasificación de los centros de operaciones de seguridad. El artículo presentado por Pierre Jacobs, Alapan Arnab y Barry Irwin[35], presenta un modelo para medir la madurez y capacidad de un SOC, permitiendo encontrar algunas características claves a la hora de realizar la implementación de un Centro de Operaciones de Seguridad.

4.1.7.2. Estado del arte de los SOC. En su artículo "Security Operations Center: A Systematic Study and Open Challenges" Manfred Vielberth et al[36], presentan una recopilación bibliográfica que permite tener un acercamiento con el estado del arte de los centros de operaciones de seguridad, esta herramienta permitirá tener un acercamiento a las metodologías y estrategias usadas por los SOC actuales, así como la estructura de composición de estos.

4.1.7.3. Analistas de un SOC. En el artículo "Towards a Framework for Measuring the Performance of a Security Operations Center Analyst", Enoch Agyepong et al[37], presentan una serie de herramientas documentales que permiten medir o probar el rendimiento de un analista de SOC.

4.1.7.4. Principales implicaciones de seguridad a tener en cuenta por un SOC. En el artículo "Security concerns towards Security Operations centers", Janos y Dai[38] presentan los principales puntos a tener en cuenta cuando se implementa un Centro de Operaciones de Seguridad que quiere ser efectivo, este documento ayudará a tener una visión más cercana a las actividades que debe ejecutar un SOC.

4.1.7.5. Gestión de incidentes. Miloslavskaya[39], presenta en su artículo "Security Operations Centers for Information Security Incident Management", como los centros de operaciones de seguridad realizan las tareas de gestión de incidentes,

---

[35] JACOBS, Pierre. ARNAB, Alapan. IRWIN, Barry. Classification of Security Operation Centers. En: Information Security for South Africa, 2013, pp 1-7.

[36] VIELBERTH, Manfred. BOHM, Fabian. FICHTINGER, Ines. PERNUL, Gunter. Security Operations Center: A Systematic Study and Open Challenges. En: IEEE Access, vol. 8, 2020, pp. 227756-227779.

[37] AGYEPONG, Enoch. CHERDANTSEVA, Yulia. REINECKE, Phillip. BURNAP, Pete. Towards a Framework for Measuring the Performance of a Security Operations Center Analyst. En: International Conference on Cyber Security and Protection of Digital Services (2020); pp. 1-8

[38] JÁNOS, Fecher David. PHUOC DAI, Nguyen. Security concerns towards Security Operations centers. En: IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI), vol 12, 2018, pp. 273-278.

[39] MILOSLAVSKAYA, Natalia. Security Operations Centers for Information Security Incident Management. En: IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), vol 4, 2016, pp. 131-136.

mostrando como esta puede ser automatizada o mejorada con la implementación de un SOC efectivo.

4.1.7.6. Uso de herramientas en los centros de operaciones de seguridad. Anikó Szarvák y Valéria Póser[40], presentan en su artículo "Review of using Open Source Software for SOC for education purposes – a case study" un análisis de las tareas realizadas por un SOC y la relación de algunas herramientas de uso libre que pueden ayudar a ejecutarlas.

4.2. MARCO CONCEPTUAL

Un Centro de Operaciones de Seguridad normalmente se ha descrito como un lugar físico en el cual un grupo de expertos en seguridad monitorean una compañía garantizando que esta puede funcionar de forma segura. Sin embargo, tal como lo presenta CompTia[41] en su artículo *What Is a Security Operations Center?,* el Covid-19 ha conseguido que incluso esta definición se vea modificada, actualmente los analistas de un SOC pueden estar trabajando activamente desde sus *home-office,* sin que esto disminuya la efectividad de un SOC como herramienta de ciberdefensa.

Tal como es mencionado por Pierre Jacobs et al[42], el objetivo principal de un Centro de Operaciones de Seguridad es el de mejorar la postura de seguridad de una organización, detectando y respondiendo ante posibles ataques de manera temprana, evitando que estos tengan un impacto critico en la compañía.

4.2.1. Principales actividades de los Centros de Operaciones de Seguridad.

Las principales actividades de un SOC[43] son las siguientes:

[40] SZARVÁK, Aniko. PÓSER, Valeria. Review of using Open Source Software for SOC for education purposes – a case study. EN: IEEE 25th International Conference on Intelligent Engineering Systems (INES), vol 25, 2012, pp 209-214.
[41] COMPTIA. "What Is a Security Operations Center?". {En línea}. {5 de febrero de 2022} disponible en: (https://www.comptia.org/content/articles/what-is-a-security-operations-center).
[42] JACOBS, Pierre. ARNAB, Alapan. IRWIN, Barry. Classification of Security Operation Centers. En: Information Security for South Africa, 2013, pp 1-7.
[43] VIELBERTH, Manfred. BOHM, Fabian. FICHTINGER, Ines. PERNUL, Gunter. Security Operations Center: A Systematic Study and Open Challenges. En: IEEE Access, vol. 8, 2020, pp. 227756-227779.

4.2.1.1. Monitoreo proactivo. Esta actividad se refiere al análisis de diferentes fuentes de información asociadas a la seguridad de la organización, esto puede ir desde logs entregados por Endpoints hasta información entregada por dispositivos de red, firewalls, IDS/IPS y otras aplicaciones que puedan entregar información valiosa para detectar de manera temprana situaciones que puedan afectar la seguridad de la organización.

4.2.1.2. Responder y gestionar eventos e incidentes de seguridad. Basado en la información que se logra obtener del monitoreo proactivo realizado por el SOC, es posible que los miembros del equipo de monitoreo deban responder a los eventos detectados, coordinando las actividades necesarias para detener y reducir el impacto causado por el evento o incidente materializado. Estas actividades están ligadas de manera completa a un plan de gestión de incidentes, el cual podría estar basado en guías técnicas como la descrita por la norma ISO 27005.

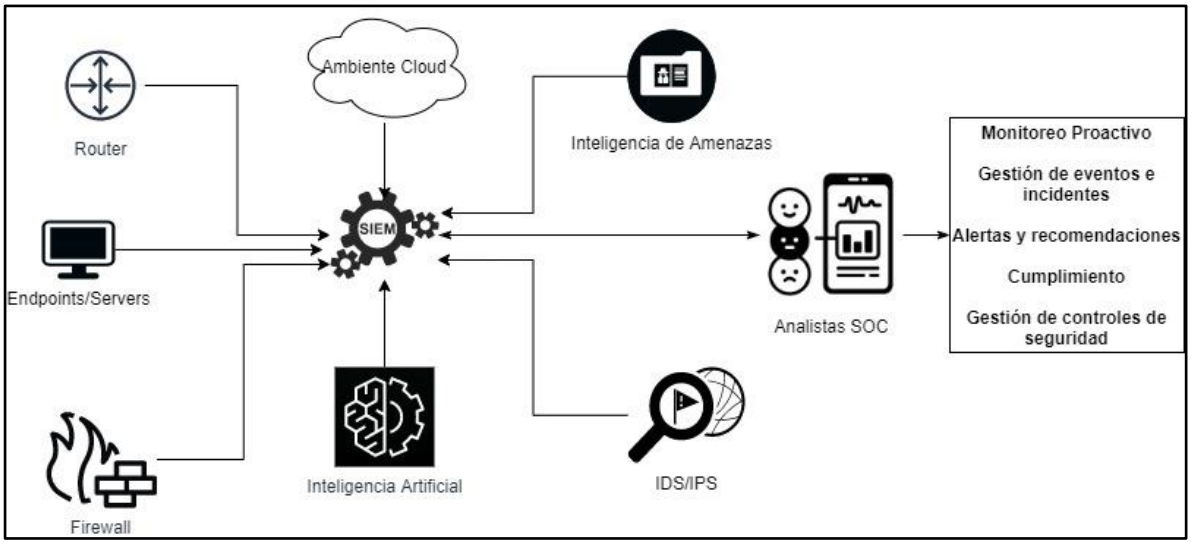
4.2.1.3. Brindar alertas y recomendaciones de seguridad. La capacidad técnica de los centros de operaciones de seguridad permiten que estos tengan la capacidad de detectar de manera temprana posibles fallas en la configuración de los diferentes equipos de la red, de esta manera, se convierte en una tarea continua el entregar las recomendaciones necesarias para ajustar las configuraciones de dichos dispositivos de acuerdo con las mejores prácticas de seguridad actuales, basados en inteligencia de amenazas y en la información liberada por diferentes fabricantes.

4.2.1.4. Gestionar los diferentes controles de seguridad. Dentro del SOC, esta tarea se enfoca en garantizar el correcto funcionamiento de los diferentes controles de seguridad que existan en la organización, estos pueden estar enfocados en medios tecnológicos o procedimentales.

4.2.1.5. Apoyar el cumplimiento de estándares y marcos de trabajo de seguridad. Una de las tareas complementarias de los Centros de Operaciones de Seguridad, es la de apoyar el cumplimiento de frameworks como el de NIST, normas o estándares como ISO 27001 y reglamentaciones, normas o leyes, como por ejemplo en Colombia la Ley 1581 de protección de datos personales.

Las actividades anteriormente mencionadas se basan en las fuentes de información que alimentan el Centro de Operaciones de Seguridad, un analista de SOC debería estar en la capacidad de interpretar, analizar y filtrar la información que recibe desde diferentes herramientas. A continuación, se presenta un esquema que pretende mostrar el funcionamiento básico de un SOC:

Figura 1. Esquema básico de operación de un SOC.



Fuente: Autor. Basado en: COMPTIA. (2020). What Is a Security Operations Center | Cybersecurity | CompTIA. Default. Recuperado de: https://www.comptia.org/content/articles/what-is-a-security-operations-center

4.2.2. Organización interna de los Centros de Operaciones de Seguridad.

La organización interna de un Centro de Operaciones de Seguridad está basada en la especialidad técnica y experiencia de los miembros de su equipo, de manera básica, un SOC está conformado[44] por los siguientes miembros:

4.2.2.1. Analista de seguridad Junior. Normalmente este es el rol encargado de monitorear de manera continua los diferentes eventos enviados desde las fuentes de información del SOC.

4.2.2.2. Analista de seguridad Senior. Ejecutan actividades similares a las de los analistas de nivel junior, sin embargo, tienen la experiencia necesaria para atender situaciones de un mayor nivel de complejidad. Este rol puede estar directamente ligado a la gestión de eventos e incidentes de seguridad.

4.2.2.3. Cazador de amenazas. Se encarga de analizar la información especializada recolectada de diferentes herramientas para lograr detectar de

[44] BIGGERI HERNAN, Patricio. Centro de operaciones de seguridad. Estrategia, diseño y gestión. Buenos Aires, 2018, pp 34-69. Trabajo de grado (Maestría en Gestión Estratégica de Sistemas y Tecnologías de la Información). Facultad de Ciencias Económicas.

manera temprana posibles ataques de seguridad, anticipando la acción de estos en la organización.

4.2.2.4. Especialista en ciber inteligencia de amenazas. Este es un profesional especializado en la gestión de las fuentes de inteligencia disponibles para alertar y prevenir a la organización frente a amenazas de seguridad, estos únicamente tienen como objetivo la información proveniente de estas fuentes de inteligencia.

4.2.2.5. Coordinador o gerente del SOC. Es el responsable de gestionar a los miembros del equipo SOC, las tecnologías y recursos del equipo, de esta manera garantiza que todo funcione de acuerdo con lo esperado y que el Centro de Operaciones de Seguridad cumpla con sus objetivos.

4.2.3. Pasos para construir un centro de operaciones de Seguridad. Según lo descrito por Muniz[45] et al en su libro Security Operations Center: Building, Operating, and Maintaining your SOC, los principales pasos para construir y operar un Centro de Operaciones de Seguridad son:

4.2.3.1. Planeación del SOC. Este inicia con la evaluación de las capacidades de seguridad existentes en la organización, enfocándose en personas, procesos y tecnologías, esto permite establecer la línea base de los objetivos del SOC.

4.2.3.2. Diseño y construcción del SOC. Esta etapa está estrictamente ligada con la selección de tecnología para el centro de operaciones, enfocada inicialmente en la manera en que se recolectará la información de las diferentes fuentes, lo cual normalmente es realizado con herramientas tipo SIEM, según lo expuesto por Muniz y sus colegas.

4.2.3.3. Operación del SOC. En esta etapa el Centro de Operaciones de Seguridad entrará a realizar sus actividades, es importante que antes de iniciar operaciones, se logre lo siguiente apoyo ejecutivo de la compañía. En el proceso de operación no debe descuidarse la triada personas, procesos y tecnologías, en esta etapa es importante tener presente que las personas deben mantenerse en constante capacitación o entrenamiento, los procesos deben ser actualizados acorde con la realidad de la organización y las tecnologías deben estar siento verificadas para que funcionen de acuerdo con lo esperado.

4.2.3.4. Revisión del SOC. En esta última etapa, se realiza la medición sobre qué tan efectiva es la operación del SOC, buscando encontrar las posibles mejoras que podrían ser aplicadas a este en cualquiera de sus pilares fundamentales, personas, procesos y tecnologías. En esta etapa se podrían llevar a cabo las siguientes actividades que permiten tener una medición adecuada del comportamiento del SOC: Determinar el alcance de la revisión del centro de operaciones, determinar los

[45] MUNIZ, Joseph. MCINTYRE, Gary. ALFARDAN, Nadhem. Security Operations Center: Building, Operating, and Maintaining Your Soc. Hoboken: Cisco Press, 2015, pp 45 – 60.

participantes en la revisión, establecer una metodología de auditoría, definir qué tan seguido se harán revisiones al SOC y priorizar las actividades de mejora según lo encontrado en las revisiones.

4.3. ANTECEDENTES Y ESTADO ACTUAL

Son muchos los desafíos a los cuales se exponen las empresas cuando se habla de seguridad informática; para todos es bastante claro que se ha percibido un aumento en lo que se refiere al uso de tecnologías de la información por parte de la población en general, esto hace que las superficies de ataque sean cada vez más y más grandes, facilitando que un tercero malintencionado, pueda de alguna manera afectar la disponibilidad, integridad o confidencialidad de la información de las organizaciones.

4.3.1. Guías MSPI del MINTIC en Colombia. En Colombia, el gobierno nacional ha realizado esfuerzos para mejorar la seguridad de la información que manejan las diferentes entidades gubernamentales, para ello, ha publicado guías como el MSPI o Modelo de Seguridad y Privacidad de la información, las cuales, si bien solo son obligatorias para entidades públicas, de una u otra manera pueden servir como referente para las organizaciones privadas que desean de alguna manera mejorar la gestión de su seguridad de la información. La guía o modelo planteado por el Ministerio de las TIC[46] en el País, pretende proporcionar lineamientos e instructivos para adoptar el modelo, ayudar en el desarrollo de una estrategia de seguridad digital y contribuir mediante esto al desarrollo de las Entidades.

El MSPI presentado por el gobierno nacional, cuenta con 21 guías de implementación y está sustentado jurídicamente en la política nacional de seguridad digital, la cual se presentó en el CONPES 3854[47], dicha política, enfoca sus esfuerzos en contrarrestar el aumento de las amenazas del ciberespacio, apuntando a la defensa nacional y a la reducción de los cibercrímenes. La política del CONPES 3854, se vuelve entonces una línea guía para definir el rumbo de la ciberseguridad en Colombia, sirviendo de apoyo tanto a las entidades públicas como a las organizaciones privadas.

Si bien, no todas las guías presentadas en el MSPI podrían asociarse al frente de ciberdefensa que cubriría un Centro de Operaciones de Seguridad, a continuación, se destacan algunas de las guías que podrían ser de interés a la hora de implementar un SOC:

[46] MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES DE COLOMBIA. Modelo de Seguridad y Privacidad de la Información. Bogotá. MINTIC. 2021.
[47] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL REPÚBLICA DE COLOMBIA DEPARTAMENTO NACIONAL DE PLANEACIÓN. Política nacional de seguridad digital. Bogotá. DNP. 2016.

4.3.1.1. Gestión Clasificación de Activos. Presenta los lineamientos para definir la criticidad de los activos de información de una organización, lo cual permitiría tener plena identificación de los activos que deberían tener cierto nivel de prioridad[48.]

4.3.1.2. Gestión de Riesgos. Permite definir los riesgos a los que se enfrenta una organización, basado en el insumo de dado por la clasificación de los activos de información. Una adecuada gestión de riesgos podría ser insumo inicial para priorizar el monitoreo y alertas de un Centro de Operaciones de Seguridad[49].

4.3.1.3. Seguridad en la Nube. Presenta los lineamientos para definir un mecanismo de protección de los activos de información que se encuentran en la nube. La gran mayoría de organizaciones, cuentan de alguna manera con algún tipo de despliegue en la nube, por lo cual esta guía brinda información que podría ser clave a la hora de definir las estrategias de monitoreo de los activos que se encuentran en este tipo de despliegues[50].

4.3.1.4. Gestión de Incidentes. Entrega los lineamientos para realizar la adecuada gestión de los eventos e incidentes de seguridad que podrían presentarse en una organización[51].

4.3.2. CSIRTs y SOCs en Colombia. Los referentes anteriores han marcado el camino de inicio para la preparación en ciberdefensa para las diferentes compañías del país, esto se ha visto reflejado en el registro de CSIRTs o Equipo de Respuesta a Incidentes de Seguridad Informática, los cuales a su vez algunos incluyen Centros de Operaciones de Seguridad. A continuación, se presentan los datos asociados a los SOC pertenecientes a CSIRTs registrados ante FIRST[52], la cual es la comunidad internacional que agrupa los equipos de respuesta a incidentes a nivel mundial y que tiene como objetivo compartir procedimientos, ideas y guías de acción frente a incidentes de seguridad:

4.3.2.1. BS-CSIRT. Cyber Security Operation Center de la compañía B-SECURE, el cual tiene como objetivo prevenir, detectar, analizar, contener y remediar los incidentes de seguridad que puedan impactar a sus clientes.

---

[48] MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES DE COLOMBIA. Guía para la Gestión y Clasificación de activos de Información. Bogotá. MINTIC. 2016.
[49] MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES DE COLOMBIA. Guía de gestión de riesgos. Bogotá. MINTIC. 2016.
[50] MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES DE COLOMBIA. Seguridad en la Nube. Bogotá. MINTIC. 2016.
[51] MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES DE COLOMBIA. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Bogotá. MINTIC. 2016.
[52] FIRST. “FIRST Members around the world”. {En línea}. {4 de junio de 2022} disponible en: (https://www.first.org/members/map).

4.3.2.2. CSIRT-MOC Newnet. Centro de Operaciones de Ciberseguridad de la Compañía Newnet S.A. Este tiene como objetivo monitorear e identificar las amenazas avanzadas y riesgos de seguridad que podrían afectar a sus clientes.

4.3.2.3. SOC ETEK. Centro de Operaciones de Seguridad de la Compañía ETEK, tiene como objetivo monitorear los servicios de sus clientes desde la perspectiva de la seguridad informática.

4.3.2.4. Gamma CSOC-CSIRT. SOC de la Compañía Gamma Ingenieros. Este es un Centro de Operaciones de Seguridad enfocado en brindar servicios de seguridad a clientes externos.

4.3.2.5. ITSSOC-CSIRT. SOC de la compañía ITSS. Este funciona como un Centro de Operaciones de Seguridad como servicio, el cual brinda apoyo en seguridad a clientes de la Compañía.

4.3.2.6. SOC Team Claro Colombia. Centro de Operaciones de Seguridad de la Compañía Claro en Colombia. Presta servicio a sus clientes internos y externos.

4.3.2.7. SOC-CCOC. Centro de Operaciones de Seguridad del Comando Conjunto Cibernético de las Fuerzas Armadas de Colombia. Este presta servicios al Ejército Nacional y aquellos entes públicos que tienen acuerdos con dicha Entidad. Sus objetivos apuntan a la protección de la infraestructura critica Nacional.

En Colombia se tienen registrados ante FIRST dieciocho CSIRTs, sin embargo, los siete equipos mencionados anteriormente poseen específicamente un SOC; lo anterior es un claro indicativo del crecimiento que han tenido los esfuerzos en ciberseguridad a nivel país.

4.4. MARCO LEGAL

En el país existen un grupo de leyes asociados a la ciberseguridad, seguridad de la información y seguridad informática, como aporte significativo y dato a tener presente en la guía documental que busca ser este documento, a continuación, se presentan las leyes encontradas como más significativas en lo que respecta al eje central de la monográfica, la ciberseguridad:

Ley 1273 de 2009[53]. “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

[53] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1273 de 2009. Diario Oficial No. 47.223 de 5 de enero de 2009, 2015). Bogotá. 2015.

Circular externa 007 de 2018 de la Super Intendencia Financiera de Colombia[54]. “Imparte instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad”.

Circular externa 008 de 2018 de la Super Intendencia Financiera de Colombia[55]. “Imparte instrucciones en materia de requerimientos mínimos de seguridad y calidad para la realización de operaciones”.

CONPES 3701 de 2011[56]. Lineamientos de política para ciberseguridad y ciberdefensa.

CONPES 3854 de 2016[57]. Política Nacional de Seguridad Digital.

[54] SUPER INTENDENCIA FINANCIERA DE COLOMBIA. Circular Externa 007 de 2018. Bogotá. SFC. 2018.
[55] SUPER INTENDENCIA FINANCIERA DE COLOMBIA. Circular Externa 008 de 2018. Bogotá. SFC. 2018.
[56] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL REPÚBLICA DE COLOMBIA DEPARTAMENTO NACIONAL DE PLANEACIÓN. Política nacional de seguridad digital. Bogotá. DNP. 2016.
[57] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL REPÚBLICA DE COLOMBIA DEPARTAMENTO NACIONAL DE PLANEACIÓN. Lineamientos de política para ciberseguridad y ciberdefensa. Bogotá. DNP. 2011.

5. DESARROLLO DE LOS OBJETIVOS

5.1. EVALUACIÓN DEL DISEÑO DE CENTROS DE OPERACIONES DE SEGURIDAD YA IMPLEMENTADOS

Tal como se ha mencionado anteriormente en este documento, los Centros de Operaciones de Seguridad sustentan sus operaciones en tres pilares fundamentales, personas, procesos y tecnologías, por tal razón, es desde dichos pilares desde donde partirá la evaluación a realizar a los diferentes centros de operaciones de seguridad a analizar en esta sección.

Se iniciará la evaluación desde los propuesto por Biggeri Patricio[58], Pompeyo Daniel[59], Bonilla Billy y Rojas Anthony[60] en sus trabajos asociados al diseño e implementación de Centros de Operaciones de Seguridad.

5.1.1. Personas. Como primer pilar de la triada de formación de un Centro de Operaciones de Seguridad, se tiene a las personas, quienes se encargarán de ejecutar las actividades de monitoreo y análisis de información, base de la operación del SOC. Estos como principal herramienta de inteligencia frente a amenazas, deberán contar con experticia técnica en seguridad que les permita ejecutar de la mejor manera sus actividades.

Los estudios, formación y experiencia son factores claves para el recurso humano que hará parte del centro de operaciones; se debe tener en cuenta las labores a ejecutar por el personal, las cuales podrían llegar a ser repetitivas en algunas ocasiones y de gran nivel de presión y estrés en otras.

Teniendo en cuenta la definición anterior, a continuación, se presenta los principales aspectos asociados al diseño del pilar “personas” en los diferentes SOC analizados.

Biggeri[61] plantea que, para lograr estructurar el recurso humano necesario para el SOC, se debe abordar su diseño desde los siguientes aspectos:

---

[58] BIGGERI HERNAN, Patricio. Centro de operaciones de seguridad. Estrategia, diseño y gestión. Buenos Aires, 2018, pp 34-69. Trabajo de grado (Maestría en Gestión Estratégica de Sistemas y Tecnologías de la Información). Facultad de Ciencias Económicas.

[59] CUELLAR RODRIGUEZ, Jorge. POMPEYO, Daniel. Diseño del esquema de implementación de un centro de operaciones de seguridad (SOC) de la información en la empresa KPMG en la sede de Bogotá D.C. – Colombia. Bogotá, 2021. pp 35 – 89. Proyecto de grado (Especialista en Seguridad Informática). Universidad Piloto De Colombia. Facultad de ingeniería.

[60] BONILLA BLANCO, Billy Mauricio. ROJAS PATERNINA, Anthony. Diseño y planificación de un centro de operaciones de seguridad informática aplicado como servicio por la organización A3SEC bajo marcos de trabajo propuestos por SANS, ISACA Y NIST. Bogotá, 2019. pp 70 -100. Trabajo de grado (Especialista en Seguridad Informática). Universidad Piloto de Colombia. Facultad de Ingeniería.

[61] Ibid.

5.1.1.1. Roles. Son el grupo de aptitudes que debería cumplir el personal del SOC para cumplir con los objetivos propuestos en la organización. Estos pueden dividirse en roles de liderazgo, roles analíticos y roles operativos. El autor propone que estos roles no sean específicamente buscados fuera de la organización que desea implementar un Centro de Operaciones de Seguridad, sino que estos pueden ser encontrados en otras áreas de la compañía.

5.1.1.1.1. Los roles de liderazgo. Son aquellos asociados a la coordinación del Centro de Operaciones de Seguridad, por lo cual podrían ser definidos como gerentes o directores del SOC, estos tendrían la tarea de ordenar el equipo de trabajo y definir el enfoque de estos para lograr alcanzar los objetivos propuestos, es común que se cuente con un único líder del centro de operaciones, pero esto puede depender del tipo y tamaño de organización, así como de la cantidad de recursos económicos con los que se cuente para su implementación.

5.1.1.1.2. Los roles analíticos. Son aquellos en los cuales se concentra el grupo principal de recursos humanos que se encargarán de cumplir los objetivos propuestos por el SOC, estos roles pueden diferenciarse según diferentes niveles, lo cual determinará el tipo de tareas que deberían ejecutar y con qué nivel de experticia se espera que la ejecuten, los analistas del SOC, quienes ocupan este rol, deberían contar con las habilidades asociadas a todos los servicios cubiertos por el centro de operaciones, las cuales pueden ser, según Biggeri, gestión de incidentes, análisis y detección de vulnerabilidades, monitoreo continuo, inteligencia de amenazas, investigación forense, entre otras.

5.1.1.1.3. Los roles operativos. Son un grupo de recurso humano que, según el autor, deberían estar enfocados en el mantenimiento de la tecnología que sustenta las actividades del SOC, estos pueden llegar a ser el mismo personal de soporte del área de TI de la organización. Este grupo de personas podría tener la necesidad de escalar casos especializados para el mantenimiento y soporte de las herramientas especializadas del SOC, por lo cual, podrían llegar a tener apoyo de proveedores externos especializados en dichas tareas.

5.1.2. Funciones y estructura del SOC. Biggeri también propone que las funciones de los centros de operaciones de seguridad podrían agruparse en cuatro líneas generales, las cuales se describen a continuación.

5.1.2.1. Función de operación. En esta línea se presentan las principales actividades que brindará el SOC, las cuales incluyen el monitoreo continuo de la seguridad de la organización, la investigación, análisis y gestión de incidentes, descubrimiento y gestión de vulnerabilidades, detección y prevención de ataques.

5.1.2.2. Función de ingeniería de servicios. Esta puede verse como el conjunto de actividades que se encargan de la operación, configuración y administración de las herramientas de seguridad ya existentes en una organización. Dentro de estas podrían ser incluidos los firewalls, sistemas antivirus, herramientas antispam, herramientas de prevención de fugas de información, Network Access Control, entre otras. Dentro de estas funciones podrían incluirse incluso aquellas asociadas a la gestión de las herramientas propias para la ejecución de actividades del SOC.

5.1.2.3. Funciones de inteligencia de seguridad. Esta también es conocida como inteligencia de amenazas y se encarga de monitorear amenazas externas, trabajando como puente entre la organización y las diferentes fuentes de grupos especializados externos, los cuales brindan información de amenazas existentes, de esta manera se logra que el SOC pueda dar reportes y alertas de valor que permitan la identificación temprana de posibles brechas de seguridad.

5.1.2.4. Funciones de soporte. Esta incluye las actividades que son la base para el funcionamiento de SOC, normalmente son comunes en grandes centros de operaciones de seguridad y pueden ir desde el soporte técnico, gestores de proyectos, de recursos humanos y auditores, esto puede verse de tal manera como se ven los procesos de soporte de las grandes compañías, comparando el SOC con una organización como cualquier otra, claramente esto variará según el tamaño del SOC, tal como se mencionó anteriormente, las diferentes funciones y roles necesarios para operar, podrían ser ofrecidos por otras áreas de la organización que desea implementar el centro de operaciones.

5.1.3. Dimensionamiento. Dentro del pilar personas, el dimensionamiento es clave, puesto que permite estimar cual será la cantidad necesaria de recursos humanos para implementar según lo esperado el Centro de Operaciones de Seguridad, dentro de la estimación, según lo expuesto por Biggeri[62], se podrían considerar los siguientes aspectos: Horario de servicio, condiciones laborales (días de descanso, horas máximas de trabajo, horas extra, etc.), cantidad de eventos a gestionar, tiempos de respuesta a solicitudes y atención de eventos. Con los datos anteriores es posible realizar una estimación de los recursos necesarios para la implementación de un SOC, sin embargo, estos pueden variar dependiendo de la realidad de cada organización.

5.1.4. Aprovisionamiento de personal. En esta actividad, se debe pensar en la manera en que se suplirán las necesidades de recurso humano dentro del Centro de Operaciones de Seguridad, el cual, según lo definido podría ser externo, interno o subcontratado.

Los aprovisionamientos externos se refieren a la contratación de personal nuevo que supla las funciones del SOC, lo cual implica dos frentes de acción, la

[62] Ibid. P 46 – 47.

contratación de personal experimentado, el cual cuenta con la ventaja de tener experiencia, sin embargo podría llegar a ser de un costo elevado en el mercado laboral, o la contratación de personal sin experiencia que podría llegar a ser entrenado en el tema de la ciberseguridad, este tiene la ventaja de ser de bajo costo en el mercado laboral, sin embargo, al adquirir experiencia suficiente podría llegar a abandonar la organización.

El aprovisionamiento interno se basa en la asignación de tareas específicas del SOC a colaboradores ya pertenecientes a la organización, los cuales de alguna manera ya tienen un conocimiento avanzado sobre la compañía, brindando una ventaja respecto a este punto.

La subcontratación es el mecanismo mediante el cual se busca suplir algunos de los roles del Centro de Operaciones mediante profesionales de otras compañías, las cuales pueden ser firmas consultoras o prestadores de servicios, estos tienen la ventaja de que pueden ser ocupados únicamente cuando se les requiere, permitiendo mantener un adecuado nivel de gastos, sin embargo, el desconocimiento de la operación propia de la compañía podría ser una gran desventaja a la hora de definir este como mecanismo de acción para el aprovisionamiento.

Según lo expuesto por Biggeri, no existe un frente de acción de aprovisionamiento ideal, este va a depender de las necesidades de la compañía que implementa el SOC, por lo cual podría ser incluso una mezcla de los tres mecanismos aquel que pueda solucionar de mejor manera el aprovisionamiento de recursos humanos para una compañía.

5.1.5. Procesos. Cuando se habla de procesos en un SOC, se está hablando de la manera como se gestionarán las operaciones del mismo, de tal manera que se logren definir cuáles son las actividades a ejecutar y de qué manera se mantendrá en ejecución y constante mejora el servicio ofrecido. Dentro de lo denominado como procesos del SOC, se pueden incluir políticas, procedimientos, instructivos, y otras herramientas que logren garantizar que desde el centro de operaciones se cumplen con los objetivos propuestos por la organización, dando valor a la misma de una u otra manera. En ultimas, estos procedimientos, políticas e instructivos definen y de alguna manera reglan la manera en que se ejecutan las actividades del SOC.

Según lo expuesto por Cuellar & Pompeyo[63], al pensar en la definición de los procesos del Centro de Operaciones de Seguridad debería tenerse en cuenta los siguientes aspectos:

[63] CUELLAR RODRIGUEZ, Jorge. POMPEYO, Daniel. Diseño del esquema de implementación de un centro de operaciones de seguridad (SOC) de la información en la empresa KPMG en la sede de Bogotá D.C. – Colombia. Bogotá, 2021. pp 35 – 89. Proyecto de grado (Especialista en Seguridad Informática). Universidad Piloto De Colombia. Facultad de ingeniería.

Identificación y definición de las entradas, acciones y salidas que conforman el funcionamiento del SOC.

Selección y definición de las áreas de la organización que tendrán relación con los flujos de operación del SOC.

Análisis de las variables que intervienen en el cambio de las condiciones del flujo de acción asociado a los eventos de seguridad, identificando de qué manera deberían ser estos atendidos.

Tener en cuenta las actividades o acciones que harán que, dentro del flujo de operaciones del SOC, se requiera un escalamiento de reportes o eventos, de manera que este pueda ser tratado por quienes realmente tienen la capacidad de hacerlo.

En complemento de lo anterior, se identifica que, para el pilar asociado a los procesos, Bonilla & Rojas[64], hacen una recomendación enfocada específicamente en la creación de casos de usos para definir los procesos del Centro de Operaciones de Seguridad. Este concepto hace referencia a la definición de las actividades que se deben seguir para identificar eventos o incidentes en una organización, en general, estos pretender ayudar a los centros de operaciones a tener una guía estructurada sobre las acciones que se deberían tomar para determinados tipos de eventos o incidentes. Estos tienen como importancia la detección temprana de actividades sospechosas, sin embargo, su rango de acción puede ser limitado al estar definido para un evento determinado. Tal como lo exponen los autores, para ello se deberían tomar en cuenta los siguientes aspectos:

[64] BONILLA BLANCO, Billy Mauricio. ROJAS PATERNINA, Anthony. Diseño y planificación de un centro de operaciones de seguridad informática aplicado como servicio por la organización A3SEC bajo marcos de trabajo propuestos por SANS, ISACA Y NIST. Bogotá, 2019. pp 70 -100. Trabajo de grado (Especialista en Seguridad Informática). Universidad Piloto de Colombia. Facultad de Ingeniería.

5.1.6. Definición de las amenazas. Específica a que se encuentra expuesta la organización o de que debería defenderse.

5.1.6.1. Definición de partes involucradas. En este punto, se definen quienes serán los encargados de ejecutar acciones previamente definidas en caso de presentarse el caso de uso analizado.

5.1.6.2. Fuente de información. Debe definirse cuál es la fuente de información que permitirá definir si se está presentando un evento asociado al caso de uso analizado.

5.1.6.3. Pruebas del caso de uso. Debería probarse el evento, los registros, las acciones y respuestas asociadas al caso de uso, de manera que este realmente sea efectivo cuando ocurra realmente y deba ser detectado y gestionado por el personal del Centro de Operaciones de Seguridad.

5.1.6.4. Definición de prioridades. Al crear varios casos de usos para el SOC, es importante definir las prioridades de los mismos según el análisis de impacto asociado a este en caso de materializarse, así se podrán definir cuales eventos serán atendidos con prioridad, en caso de que aparezcan varios al tiempo.

5.1.6.5. Salidas. En este último ítem, se definen cuáles serán los informes o reportes para entregar una vez se detecta y gestiona el evento asociado al caso de uso, esto se refiere a lo que se debe presentar, a quien se debe presentar y cuando se debe presentar.

Mediante lo anterior, se define un caso de uso para un SOC, el cual tiene como objetivo determinar el evento que lo ocasiona, las entradas asociadas, las actividades y las salidas del mismo, esto, en ultimas hace referencia a la definición de procedimientos específicos para cada tipo de evento definido en el centro de operaciones como crítico.

Biggeri, a su vez expone que, dentro de los procesos de un SOC, se pueden considerar como recomendados los siguientes:

5.1.6.6. Gestión de servicios corporativos. Dentro de estos se encuentran algunos procesos que de alguna manera podrían ya estar definidos en las áreas de TI de las organizaciones, estos podrían ser el procedimiento de gestión de eventos e incidentes, el procedimiento de gestión de vulnerabilidades y en algunas ocasiones, podrían incluirse procedimientos como el de gestión de cambios y/o gestión de configuraciones.

5.1.6.7. Gestión de servicios de seguridad. En este grupo de procesos se pueden encontrar aquellos que están estrechamente relacionados con la seguridad de la información y que podrían ser ligados a un SGSI o Sistema de Gestión de Seguridad de la Información; dentro de estos se pueden encontrar procesos como gestión de indicadores o métricas, mejora continua, procesos de auditoría y cumplimiento, procesos de continuidad de operación y recuperación a desastres, procesos de capacitación en seguridad de la información, gestión de proveedores, entre otros.

5.1.7. Operación de los servicios de seguridad. Dentro de este grupo de procesos se identifican aquellos que apoyan el mantenimiento a las herramientas e información utilizada por el centro de operaciones para su correcto funcionamiento; dentro de este se mencionan procesos como el de monitoreo de licencias, procesos de monitoreo de herramientas, procesos de gestión del SOC, y todos aquellos procesos que permiten la puesta en producción del Centro de Operaciones de Seguridad.

5.1.7.1. Monitoreo de seguridad. Este sin duda alguna es el grupo de procesos que conforma el Core del SOC, incluye procesos para la gestión y reporte de eventos e incidentes, proceso de monitoreo y escalamiento de eventos de seguridad, proceso de gestión de casos, gestión de alertas desde fuentes externas y gestión del conocimiento.

5.1.7.2. Investigación y respuesta a incidentes. Dentro de los SOC, esta es una de las actividades más conocidas, incluye la detección, investigación, contención y recuperación frente a la aparición de un incidente de seguridad. Dentro de este se pueden encontrar procesos como el de análisis de software malicioso y el proceso de gestión y atención de eventos e incidentes, tanto de TI como de seguridad.

5.1.7.3. Gestión de vulnerabilidades. En general el SOC no será responsable de la aplicación de parches o la remediación de vulnerabilidades, sin embargo, si se incluyen en este apartado la definición de procesos de descubrimiento de vulnerabilidades, los cuales se basan en técnicas o herramientas de escaneo de vulnerabilidades, así como la coordinación y seguimiento a las actividades asociadas a su cierre. También se incluyen en este grupo los procesos asociados al análisis de reportes de vulnerabilidades desde fuentes externas, como por ejemplo los proveedores y fabricantes de software y hardware.

5.1.8. Inteligencia de seguridad. En este se incluyen los procesos asociados a la recepción, análisis y consumo de información de fuentes de inteligencia en ciberamenazas y darle valor según el contexto propio de la organización. Dentro de estos están la identificación de amenazas y la instrucción y notificación sobre las mismas.

5.1.8.1. Gestión de reportes de seguridad. Estos procesos están enfocados en definir la manera en que se debe reportar la información consolidada por el SOC, estos pueden ser producidos para usuarios de la organización, para autoridades y para el mismo personal del centro de operaciones.

5.1.9. Tecnología. Este pilar se encarga de complementar los dos anteriores, de manera que las personas del SOC utilizan la tecnología para llevar a cabo los procesos del mismo. La información procesada por un SOC en general pasa por algún tipo de herramienta tecnológica, no es posible concebir un SOC con un déficit en alguno de los pilares del servicio, sin embargo, la falta de tecnología haría casi imposible la ejecución de actividades del centro de operaciones.

Bonilla & Rojas, proponen que para lograr definir de manera adecuada las tecnologías del SOC, estas deben estar pensadas en cumplir con las siguientes premisas:

Entender la importancia del uso de las herramientas tecnológicas para lograr alcanzar de manera adecuada la meta de brindar seguridad a una organización.

Identificar cuáles serán las herramientas claves que permitirán el desarrollo de las actividades del SOC y la suma de valor a los recursos del mismos (personas).

Utilizar de manera adecuada las fuentes de información de amenazas e inteligencia externas para la correlación de eventos de seguridad, de manera que se pueda prever la ocurrencia de un evento o incidente de seguridad.

Biggeri identifica que dentro de la definición de las tecnologías para la implementación de un Centro de Operaciones de Seguridad se deberían tener en cuenta lo siguiente:

5.1.9.1. Redes de comunicaciones. Este es un aspecto fundamental de la tecnología base del SOC, ya que es el principal foco de monitoreo del mismo, así como el lugar donde este existe, sin red de comunicación no se podría implementar un SOC, a la vez que, sin esta, el Centro de Operaciones de Seguridad no tendría un objetivo.

5.1.9.2. Seguridad de la red. Dentro de la implementación de un Centro de Operaciones de Seguridad, es necesario que se tenga en cuenta las limitaciones que debería tener la red para mantenerse segura, esto incluye el control de acceso a la red mediante ACL o el uso de firewalls para restringir el acceso a ciertos puertos y direcciones en la red. Además de firewalls, dentro de una red, existen múltiples herramientas que podrían ayudar en la mejora de su seguridad, esto incluye más no se limita a IDS/IP, filtros de contenido, antivirus, VPN, entre otros. Todas estas herramientas de seguridad para la red, en ultimas se convertirán en una fuente de información para la herramienta principal de correlación de eventos del SOC.

5.1.9.3. Plataformas especializadas de seguridad informática dentro de un SOC. Estas incluyen las principales herramientas tecnológicas que se podrían encontrar en un Centro de Operaciones de Seguridad de la información, como: SIEM, Firewall, enrutadores, switches, NAC, Proxy, IDS/IPS, herramientas antispam, WAF, Suscripción a feeds de amenazas, antivirus, sandbox, honeypots, herramientas de prevención de fugas de información, herramientas de análisis de vulnerabilidades, software y hardware de investigación forense.

Con el objetivo de mostrar un resumen de lo definido por cada autor analizado en lo asociado a la implementación de una arquitectura de SOC basada en los pilares, personas, tecnologías y procesos, se presentan a continuación, tres tablas que compilan lo propuesto por cada uno de los autores estudiados.

Cuadro 1. Resumen de lo propuesto por Bonilla & Rojas en su trabajo "Diseño y planificación de un centro de operaciones de seguridad informática aplicado como servicio por la organización A3SEC bajo marcos de trabajo propuestos por SANS, ISACA y NIST."

Personas	**Procesos**	**Tecnologías**
• Analista de alertas (Nivel 1) • Analista de respuesta a incidentes (Nivel 2) • Cazador (Nivel 3) • Gerente del SOC	• Definición de casos de uso (Seguimiento de autenticación, validación de alertas IDS/IPS, Trafico excesivo de entrada y salida, conexión no autorizada, etc.) • Ciclo de vida y gestión de eventos e incidentes de seguridad	• SIEM • Firewall • IDS/IPS • DLP (Data Loss Prevention) Prevención de fugas de información. • Análisis de vulnerabilidades • Monitoreo de bases de datos • Software de cifrado • Sniffers • Herramientas forenses
Elaboración propia basada en lo expuesto por Bonilla & Rojas[65].		

[65] Ibid.

Cuadro 2. Resumen de lo propuesto por Cuellar y Pompeyo en su trabajo “Diseño del esquema de implementación de un centro de operaciones de seguridad (soc) de la información en la empresa KPMG en la sede de Bogota D.C.”

Personas	**Procesos**	**Tecnologías**
• Analista SOC Nivel I • Analista SOC Nivel II • Especialista de seguridad del SOC • Gerente del SOC	• Gestión de eventos e incidentes de seguridad • Atención de casos generados vía mesa de ayuda • Atención de casos generados por los analistas SOC • Atención de • casos generados por herramienta SIEM	• SIEM • Fuentes de inteligencia de amenazas • Fuentes de información (firewall, antivirus, servidores de archivos, máquinas virtuales, servidores Windows y Linux). • WAF
Elaboración propia basada en lo expuesto por Cuellar & Pompeyo[66].		

Cuadro 3. Resumen de lo propuesto por Biggeri en su trabajo “Centro de Operaciones de Seguridad. Estrategia, Diseño y Gestión”

Personas	**Procesos**	**Tecnologías**
• Analistas Iniciales • Analistas Intermedios • Operadores • Analistas Avanzados • Gerente o director del SOC.	• Gestión de eventos e incidentes de seguridad • Gestión de vulnerabilidades • Gestión de cambios • Gestión de configuraciones • Gestión de indicadores o métricas • Gestión de auditorias	• Red de comunicaciones • SIEM • Firewall • NAC • Proxy • IDS/IPS • Herramientas antispam • WAF • Suscripción a feeds de amenazas

[66] CUELLAR RODRIGUEZ, Jorge. POMPEYO, Daniel. Diseño del esquema de implementación de un centro de operaciones de seguridad (SOC) de la información en la empresa KPMG en la sede de Bogotá D.C. – Colombia. Bogotá, 2021. pp 35 – 89. Proyecto de grado (Especialista en Seguridad Informática). Universidad Piloto De Colombia. Facultad de ingeniería.

	• Gestión de continuidad y recuperación a desastres • Gestión de monitoreo • Gestión de inteligencia de amenazas • Gestión de reportes de seguridad	• Antivirus • Sandbox • Honeypots • Herramientas de prevención de fugas de información, herramientas de análisis de vulnerabilidades, software y hardware de investigación forense
Elaboración propia basada en lo expuesto por Biggeri[67].		

5.2. MARCOS DE TRABAJO DE SEGURIDAD PARA LA DEFINICIÓN DEL MODELO DE GESTIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD.

En el capítulo anterior se ha abordado el análisis de diferentes implementaciones de centros de operaciones de seguridad, enfocando su diseño en los pilares de personas, procesos y tecnologías. En este capítulo, se partirá de dicho análisis para ir avanzando en la comparación de los diferentes marcos de trabajo que podrían aportar a la consolidación del modelo de gestión de un SOC. Teniendo presente lo ya descrito, a continuación, se inicia dicho análisis partiendo por la discusión de marcos de trabajo que podrían aportar en la definición de la gestión de recursos humanos del centro de operaciones.

Como ya se ha discutido anteriormente en el documento, el capital humano es base fundamental para el cumplimiento de los objetivos de un Centro de Operaciones de Seguridad; por tal razón, la adecuada gestión del recurso humano del SOC será de suma importancia. Dentro de los marcos de trabajo que enfocan parte de sus esfuerzos en la gestión del recurso humano, se encuentra ITIL, el cual es un marco de trabajo enfocado en los servicios de TI, a continuación, se presenta una descripción breve de este *framework.*

5.2.1. ITIL (Information Technology Infrastructure Library). Según lo descrito por Hiberus[68], en su blog “ITIL® 4, todas las novedades de ITIL en 2019”. ITIL es un compendio de buenas prácticas asociadas con la adecuada gestión de servicios de TI, presentando la manera que estos pueden relacionarse con los procesos de la organización. Este es un marco de trabajo que tiene como fases de implementación

[67] BIGGERI HERNAN, Patricio. Centro de operaciones de seguridad. Estrategia, diseño y gestión. Buenos Aires, 2018, pp 34-69. Trabajo de grado (Maestría en Gestión Estratégica de Sistemas y Tecnologías de la Información). Facultad de Ciencias Económicas.

[68] HIBERUS. “ITIL® 4, todas las novedades de ITIL en 2019”. {En línea}. {15 de abril de 2022} disponible en: (https://www.hiberus.com/crecemos-contigo/novedades-itil-v4/).

la definición de la gestión de servicios como algo estratégico, el diseño de los servicios TI a ofrecer, ejecutar la transición entre lo diseñado a la realidad operativa de los servicios, la ejecución de los servicios diseñados y por último la evaluación de los mismos para garantizar la mejora continua.

El marco de trabajo ITIL, en su versión 4, incluye 34 practicas, las cuales reúnen un grupo de recursos que pueden ayudar a las organizaciones a ejecutar sus actividades y/o alcanzar sus metas en lo que a servicios de TI respecta.

Las prácticas de ITIL 4 se dividen en los siguientes tres grupos: Prácticas de gestión general, prácticas de gestión de servicios y prácticas de gestión técnica. Cada una de estas prácticas a su vez se ven relacionadas con cuatro dimensiones presentadas en el marco de trabajo, organizaciones y personas, información y tecnología, partners y proveedores y flujos de valor y procesos.

Dentro de las practicas definidas por ITIL 4, se han identificado aquellas que podrían estar relacionadas con la gestión del personal del centro de operaciones, estas se presentan a continuación:

5.2.1.1. Gestión del conocimiento. Según lo descrito en Knowledgehut[69], el propósito de esta práctica se enfoca en asegurar y mejorar el conocimiento de la organización, de forma que pueda ser utilizado de manera efectiva por toda la compañía. La creación de bases de datos de conocimiento se convierte en un aliado en la gestión del recurso humano pues permite ser más eficiente a la hora de adaptar nuevo personal a las actividades del centro de operaciones; un ejemplo de esto podría estar asociado a la gestión del conocimiento derivado de la atención de eventos e incidentes, de manera que la información consolidada de dichos eventos pueda ser estudiada por cualquier colaborador del SOC, haciendo más simple su adaptación a las actividades.

5.2.2.2. Métricas y reportes. El propósito de la gestión de métricas y reportes es el de mostrar cual es el estado de comportamiento del servicio ofrecido, esto ayudaría en la toma de decisiones y en la mejora de servicios. Esta medición se asocia al talento humano pues este es uno de los aspectos que deberían ser medidos, buscando mejorar su rendimiento y trabajar en la creación de conocimiento o experticia en aquellas áreas en las cuales se encuentre un déficit al analizar los indicadores. Específicamente, la medición y los reportes apunta a la mejora del servicio, en este caso se puede ver como la mejora asociada a las actividades de los colaboradores del Centro de Operaciones de Seguridad.

5.2.2.3. Gestión de cambios organizacionales. Según lo descrito en Knowledgehut[70], esta práctica tiene como objetivo asegurar la gestión de los

[69] KNOWLEDGEHUT. “ITIL®4 Management Practices”. {En línea}. {21 de mayo de 2022} disponible en: (https://www.knowledgehut.com/tutorials/itil4-tutorial/itil-management-practices-processes).
[70] Ibid.

recursos humanos al realizar cambios en los servicios ofrecidos, garantizando la correcta implementación de estos a través de una gestión efectiva de cambios. En general, las personas serán el centro de los cambios organizacionales, esto relacionado estrechamente con lo que respecta a comportamientos y cultura organizacional. Se debe contar con un modelo para la gestión del cambio que permita que estos sean precisos y se adopten de la mejor manera en la compañía.

5.2.2.4. Gestión de talento y fuerza de trabajo. Sin duda alguna esta práctica es la más relevante en el pilar de las personas en cuanto a lo que respecta a la gestión de un Centro de Operaciones de Seguridad, este se enfoca en asegurar que la organización cuenta con las personas adecuadas para la ejecución de sus responsabilidades, contando con habilidades, conocimiento y capacidades para ello. La adecuada gestión de la fuerza de trabajo y el talento humano debe incluir: Gestión de la fuerza de trabajo, reclutamiento, medición del comportamiento, desarrollo personal, aprendizaje y desarrollo y mentoría y planeación de logros.

Dentro de lo analizado en el marco de trabajo de ITIL en lo relacionado con la gestión del pilar "Personas", según lo mostrado por BMC Software[71] en su blog "ITIL & ITSM Roles and Responsibilities", los roles en las organizaciones que prestan servicios de TI, como por ejemplo un SOC, van a verse totalmente influenciadas por el tamaño de la compañía. Lo anterior se presenta en el siguiente cuadro.

Cuadro 4. Roles en las organizaciones según su tamaño

Compañías de TI de gran tamaño	**Compañías de TI de pequeño tamaño**
Se cuenta con diferentes roles que ejecutan actividades separadas	Es posible que un mismo rol ejecute más de una actividad principal
La segregación de funciones tiene un nivel de madurez elevado	Se tiene una pobre segregación de funciones
Las habilidades tienen un factor de especialidad elevado, de manera que algunos roles pueden ejecutar actividades bastante específicas.	Las habilidades son generalizadas debido al tamaño de la organización, sin embargo, puede existir cierto grado de especialidad.
La complejidad en la gestión de los roles y funciones tiende a ser elevada debido a la cantidad de funciones que podrían ser asociadas a diferentes roles.	La complejidad de la gestión de roles y funciones no es tan elevada, debido a que existen pocos roles con muchas funciones asociadas a ellos.
Elaboración del autor, basada en lo presentado por BMC[72]	

[71] BMC. "ITIL & ITSM Roles and Responsibilities". {En línea}. {14 de mayo de 2022} disponible en: (https://www.bmc.com/blogs/itil-itsm-roles-responsibilities/#:~:text=In%20fact%2C%20the%204%20Ps%20of%20ITIL%20%C2%AE,quality%20IT%20services%20to%20users%20and%20customer%20alike).

[72] Ibid

Lo anterior debería ser tenido en cuenta a la hora de realizar las labores de búsqueda de colaboradores para un Centro de Operaciones de Seguridad a implementar, el tamaño esperado del SOC en general, en comparación con la organización a la cual prestará sus servicios, debería ser un factor clave para definir la cantidad de roles, funciones y responsabilidades del mismo.

5.3. ISO/IEC 27001:2013

Si bien la norma ISO 27001 es una norma enfocada en sistemas de gestión de seguridad de la información, presenta en sus requisitos y controles aspectos claves que podrían llegar a ser de utilidad en la definición de la gestión de los recursos humanos de un Centro de Operaciones de Seguridad, esto sin mencionar que en general los procesos de un SOC podrían estar certificados en esta norma, por lo cual es totalmente acertado pensar en llevar lo que la norma dicta en cuestión de talento humano a la gestión de un centro de operaciones.

Tal como con ITIL, inicialmente se dará una breve descripción de lo que es este marco de trabajo. La norma ISO 27001, según lo presentado por ICONTEC[73], es un estándar de seguridad que presenta los requisitos para implementar un Sistema de Gestión de Seguridad de la Información o SGSI. Dichos requisitos se encuentran descritos en la norma, específicamente en los siguientes numerales:

5.3.1. Contexto de la organización. Numeral 4 de la norma, este busca definir las necesidades de la organización en lo que se refiere al contexto interno y externo de la misma, en este requisito de la norma se define el alcance del SGSI a implementar, esto según el análisis de las necesidades y expectativas analizadas en el contexto de la compañía.

5.3.2. Liderazgo. Este corresponde al numeral 5 de la norma, se enfoca en la definición de la importancia de la alta dirección y su compromiso con el SGSI, definiendo los roles y funciones de los colaboradores de la organización, las políticas y los recursos que se utilizarán para la implementación de este.

5.3.3. Planificación. En este requisito, el cual corresponde al numeral 6 de la norma, se busca que la organización defina la manera como evaluará y tratará sus riesgos de seguridad de la información.

5.3.4. Soporte. Este corresponde al numeral 7 de la norma y se enfoca en la definición de los recursos de la organización, la competencia del personal, la creación de conciencia en seguridad de la información, la comunicación dentro de la organización y la necesidad de mantener la información documentada.

[73] INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. Bogotá. ICONTEC. 2013.

5.3.5. Operación. El numeral 8 de la norma presenta la manera en cómo deben ser planificadas, implementadas y controladas las operaciones de una organización, incluyendo lo relacionado con la gestión de riegos definida en el numeral 6.

5.3.6. Evaluación y desempeño. Este numeral, el cual corresponde al 9 de la norma, habla de la importancia de realizar un adecuado seguimiento y evaluación al SGSI, incluyendo auditorías internas y revisión por la dirección para su adecuado funcionamiento.

5.3.7. Mejora. Este último numeral, especifica cómo deberían ser tratadas las no conformidades derivadas de la evaluación y desempeño. En general estas son, acciones correctivas de no conformidades y mejora continua del Sistema de Gestión.

La norma ISO/IEC 27001:2013, también incluye un anexo en el cual se presentan en total 114 controles, los cuales se agrupan en 14 objetivos de control que van desde el A.5 hasta el A.18. Entre estos controles, el objetivo A.7. Seguridad de los recursos humanos, es el que incluye todo lo relacionado con la gestión del talento humano desde la perspectiva de la seguridad de la información. A continuación, se realiza una ampliación de los aspectos asociados con la gestión del recurso humano desde el punto de vista de la norma, tanto para requisitos como para controles.

5.3.7.1. Gestión de recursos. Tal como se muestra en la norma transcrita por ICONTEC74, Las organizaciones deberían poder definir y asignar los recursos para el establecimiento y mantenimiento del SGSI. Este requerimiento podría ser extrapolado a lo relacionado con la implementación de un Centro de Operaciones de Seguridad de la información, de esta manera, podría decirse que, de la misma manera, la organización debería poder definir y asignar los recursos para implementar el SOC.

5.3.7.2. Competencia. Las personas que hacen parte del equipo que trabajo de la organización y que de alguna manera se ven relacionadas con el SGSI, en este caso con el SOC, deberían contar con las competencias adecuadas para el desarrollo de sus actividades. Estas competencias podrían ser medidas en relación con la educación, formación y experiencia del colaborador. De la misma manera, la norma menciona que en casos en los cuales sea necesario, debería pensarse en las acciones a realizar para que la competencia necesaria sea adquirida por los colaboradores, esto trae al frente el tema de la capacitación constante.

5.3.7.3. Comunicación. En lo referente al recurso humano, también se encuentra como prioridad la definición clara de un esquema de comunicaciones, de manera que se exponga de manera precisa que se va a comunicar, cuando, a quien, el responsable de comunicar y la manera en que se realizará la comunicación. Lo

[74] Ibid

anterior permite que exista una clara comprensión de objetivos, en este caso extrapolados a lo referente al SOC.

5.3.7.4. Información documentada. Al igual que con la implementación de un SGSI, para la implementación de un SOC, será de gran importancia el definir y documentar aquellos procesos o información necesaria para ejecutar de manera eficaz las tareas del Centro de Operaciones de Seguridad.

De manera similar a como lo mencionaba la práctica de “Gestión de talento y fuerza de trabajo” de ITIL, la norma ISO 27001, también presenta una serie de recomendaciones, en forma de controles, para los procesos asociados a la gestión del talento humano, estos se presentan a continuación.

5.3.7.5. Selección de personal. Los candidatos a colaboradores de la organización, específicamente del Centro de Operaciones de Seguridad, deberían pasar por un proceso de verificación de antecedentes y requisitos legales, esto aplica totalmente a la implementación de un SOC, ya que el personal del mismo tendrá acceso a información confidencial tanto de clientes como de la misma compañía dueña del SOC.

5.3.7.6. Definición de los términos y condiciones del empleo. Las organizaciones deberían dejar claros los acuerdos a nivel contractual que regirán entre colaboradores y empresa, esto quiere decir, que debe existir un contrato o acuerdo legal firmado donde queden claras las condiciones de trabajo y las responsabilidades del colaborador.

5.3.7.7. Proceso disciplinario. Debería ser claro cuáles podrían ser las consecuencias y el proceso formal que puede llevarse a cabo en caso de existir una violación al cumplimiento de las responsabilidades del colaborador; esto podría llevarse a la implementación del SOC, asociado a las condiciones que se especifican en la contratación y en las reglas internas del Centro de Operaciones de Seguridad.

A continuación, se presenta de manera resumida aquellos aspectos de gestión del pilar “Personas” que se cubren desde la perspectiva de los dos marcos de trabajo analizados.

Cuadro 5. Aspectos de gestión del talento humano desde la perspectiva de ITIL v4 e ISO/IEC 27001:2013

Característica	**ITIL v4**	**ISO/IEC 27001:2013**
Aspectos de gestión del conocimiento	Lo incluye de manera directa en una de sus prácticas.	Puede ser asociado a lo relacionado con la información documentada (procedimientos bien definidos)
Métricas y reportes	Se incluye de manera directa en una de sus prácticas.	Podría estar incluido en la definición de indicadores de gestión.
Gestión de cambios organizacionales	Se incluye de manera directa en una de sus prácticas.	Se incluye en lo asociado a la información documentada y las operaciones.
Gestión del recurso humano	Incluido en sus prácticas documentadas.	Se presenta tanto en la definición de requisitos como en las recomendaciones (controles).
Gestión de competencias (educación, formación y experiencia)	Se incluye en la práctica de gestión de la fuerza de trabajo y talento.	Se incluye en el requisito de competencias de la norma.
Comunicación	No se incluye de manera explícita.	Se incluye como requisito de la norma.
Información documentada	Podría verse asociado con la práctica de mantener una adecuada gestión del conocimiento.	Se incluye como requisito de la norma.
Aspectos para la selección de nuevos colaboradores	Se incluye en la práctica de gestión de la fuerza de trabajo y talento.	Se incluye como controles para la gestión del recurso humano.
Definición de acuerdos contractuales	Se incluye en la práctica de gestión de la fuerza de trabajo y talento.	Se incluye como controles para la gestión del recurso humano.
Aspectos disciplinarios	No se incluye de manera explícita.	Se incluye como controles para la gestión del recurso humano.
Relación entre definición de roles y tamaño de la organización.	Se presenta una relación entre estos en lo definido por las practicas del marco de trabajo.	No se incluye de manera explícita. Los requisitos de la norma están pensados para cualquier

Característica	ITIL v4	ISO/IEC 27001:2013
		tamaño y tipo de organización.
Elaboración del autor		

Habiendo analizado un par de marcos de trabajo asociados al pilar del factor humano para la implementación de un SOC, a continuación, se presenta lo propio para el pilar de los procesos, para ello, se tendrá en cuenta el proceso que se considera central en los Centro de Operaciones de Seguridad, esto basado en el análisis realizado en el primer capítulo, donde se encontró que cada uno de los autores investigados, incluyó la gestión de eventos e incidentes de seguridad como uno de los principales procesos del SOC.

En lo que se refiere a gestión de eventos e incidentes de seguridad, existen dos referentes en lo que respecta a marcos de trabajo, estos son, la guía para la gestión de incidentes de seguridad del NIST (NIST Special Publication 800-61)[75] y la norma técnica ISO/IEC 27035:2012[76]. Ambos marcos de trabajo se enfocan en presentar una serie de recomendaciones para llevar una adecuada gestión de eventos e incidentes de seguridad de la información.

5.3.8. Guía para la gestión de incidentes de seguridad del NIST. La guía presentada por el NIST es una herramienta para los líderes de las áreas de TI que buscan establecer un mecanismo eficiente y efectivo para atender eventos e incidentes de seguridad, la cual puede ser aplicada a cualquier tipo de organización sin importar el tipo de hardware, software, aplicaciones y/o sistemas operativos que posea.

En esta guía, el NIST deja claro que las organizaciones deberían definir que es para ellos un incidente, de manera que, para todas las personas relacionadas con la gestión de incidentes, se tenga claridad sobre de lo que se está hablando y cuáles son las acciones relacionadas con su atención. En lo que respecta a la implementación de un Centro de Operaciones de Seguridad, esto no es ajeno, para el SOC debería ser claro lo que representa un evento y un incidente de seguridad, dentro del contexto de la organización a la cual brinda sus servicios.

Según lo descrito en este marco de trabajo, los componentes principales de el plan, política y procedimientos para la gestión de incidentes deberían incluir lo siguiente.

5.3.8.1. Política de gestión de incidentes. Debería incluir Propósito y objetivos de la política, alcance, definición de los roles y responsabilidades en lo referente a la

[75] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Computer Security Incident Handling Guide. NIST Special Publication 800-61 (Revision 2). Washington D.C. NIST. 2012.
[76] INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Técnicas de seguridad. Gestión de incidentes de seguridad de la información. Bogotá. ICONTECT. 2012.

gestión de incidentes, rangos de priorización de incidentes, mecanismos de reporte y contacto.

5.3.8.2. Plan de gestión de incidentes. Debería incluir la misión, los objetivos y estrategias para cumplirlos, aprobación de los lideres o gerentes, mecanismos de comunicación entre el equipo de gestión de incidentes y otros grupos de la organización, métricas de evaluación de la gestión de incidentes y el roadmap que muestre la manera como se mejorará la gestión.

5.3.8.3. Procedimientos de gestión de incidentes. Estos deberían estar basados en el plan y la política de gestión de incidentes; delimitan la manera en que se abordarán los incidentes desde el punto de vista técnico, estos deberían ser evaluados y luego socializados con todos los miembros del equipo, de manera que todos conozcan lo que deberían hacer, en relación con su rol dentro del proceso.

El enfoque dado por NIST para la gestión de incidentes de seguridad se divide por fases, estas son:

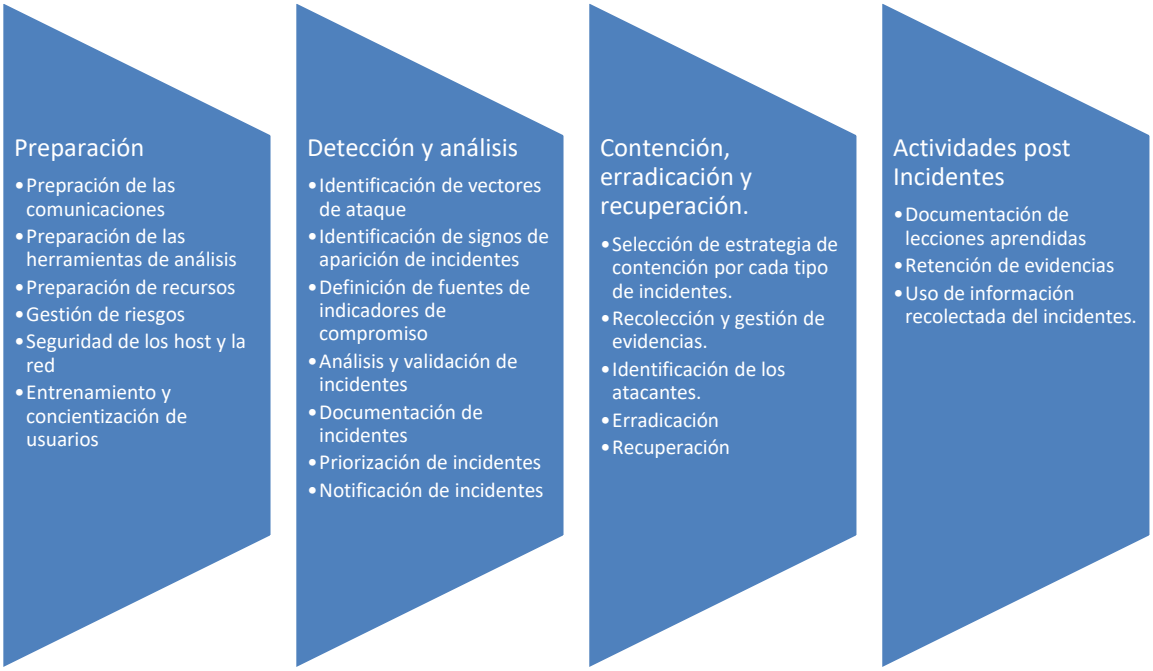
5.3.8.3.1. Fase de preparación. En esta fase se llevan a cabo las actividades que permitan establecer las capacidades de respuesta a incidentes de la organización, así como el asegurarse de que los sistemas tecnológicos son seguros. Estas actividades son claramente definidas como preparación y prevención. Dentro de la preparación se encuentran acciones como la preparación de las comunicaciones y el sitio de trabajo, preparación de las herramientas de análisis de hardware y software, preparación de los recursos de análisis y preparación de software para la mitigación. En lo que respecta a la prevención, se incluyen la gestión de riesgos de seguridad, la seguridad de los hosts, la seguridad de la red, la prevención contra malware y el entrenamiento y concientización de usuarios.

5.3.8.3.2. Fase de detección y análisis. En esta fase se llevan a cabo diferentes tareas enfocadas en la identificación de los diferentes tipos de vectores de ataque (web, email, suplantación, uso no apropiado de equipos, robo o pérdida de equipos, entre otros), identificación de las signos de aparición de un incidente, definición de las fuentes de indicadores de compromiso (generalmente sistemas SIEM, IDS/IPS, herramientas de seguridad, logs de sistemas operativos, reportes de personal de la organización, entre otros), análisis y validación de la aparición de un incidente (comparación del comportamiento normal de los sistemas y las redes, ejecutar análisis de correlación de eventos, sincronización de eventos en el tiempo, uso de las bases de datos de conocimiento, filtrado de datos, análisis de paquetes de red, entre otros), documentación del incidente, priorización del incidente y notificación del incidente.

5.3.8.3.3. Fase de contención, erradicación y recuperación. En esta fase se incluye la selección de una estrategia adecuada para la contención de incidentes, la cual podría incidir en las decisiones a tomar al momento de materializarse un incidente (apagar los dispositivos, desconectar el segmento de red, inhabilitar algunos servicios o funciones, entre otros), normalmente estas estrategias y decisiones se definen según el tipo de incidente ocurrido, dentro de los criterios para definir la estrategia de contención más apropiada se encuentran el análisis del daño potencial del incidente, la necesidad de preservar evidencias, la necesidad de tener algunos servicios disponibles, los recursos necesarios para su implementación y la duración de la solución. También se encuentra dentro de esta fase la recolección y gestión de evidencias las cuales podrían llegar a ser necesarias por cuestiones legales. La identificación de los atacantes es otra de las actividades de esta fase, en esta se incluye la validación de las direcciones IP desde las cuales sale el ataque, la investigación de estas, el uso de bases de datos públicas de incidentes y el monitoreo de los posibles canales de comunicación de los atacantes. Las últimas actividades de esta fase son las de erradicación y recuperación, las cuales incluyen la eliminación de archivos y programas maliciosos, la eliminación de cuentas de usuario comprometidas, remediación de vulnerabilidades explotadas, recuperación de sistemas operativos completos o recuperación a estados “limpios” mediante la instalación de imágenes de backups.

5.3.8.3.4. Fase de actividades post-incidente. En esta fase se incluye la documentación de lecciones aprendidas, las cuales pretender guardar un registro de lo ocurrido durante el incidente, las acciones necesarias para atender el incidente, las posibles mejoras que podrían haber evitado la materialización del incidente y aquellas recomendaciones para estar mejor preparados frente a este tipo de situaciones. En esta fase también se presentan como actividades post-incidentes la retención de evidencias y el uso de la información recolectada para mejora de la capacidad de gestión.

Imagen 1. Resumen de las fases de gestión de incidentes propuestas por NIST



Elaboración propia. Basado en la información expuesta por NIST[77] en la Guía de gestión de eventos de seguridad.

5.4. ISO/IEC 27035:2021

La guía de la ISO presenta un enfoque que apunta a la definición e implementación de una adecuada gestión de incidentes de seguridad, la cual, desde el punto de vista de la guía, incluye también la gestión de vulnerabilidades. Esta brinda un enfoque para: Detectar, reportar y evaluar incidentes de seguridad de la información, responder a estos y gestionarlos, así como para detectar, evaluar y gestionar vulnerabilidades. En general esta guía puede utilizarse para organizaciones de cualquier tamaño, aunque los recursos a utilizar pueden por los diferentes tipos de organizaciones podrían variar según sus necesidades propias.

Según la guía de la ISO, la relación existente entre los diferentes objetos relacionados en la cadena de un incidente de seguridad es la siguiente: Inicialmente, las amenazas causan acciones no deseadas, las cuales aprovechas las vulnerabilidades de los sistemas, generando la ocurrencia de un evento de seguridad de la información, el cual puede llegar a ser clasificado como un incidente de seguridad de la información, el cual a su vez trae implicaciones para la seguridad

[77] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Computer Security Incident Handling Guide. NIST Special Publication 800-61 (Revision 2). Washington D.C. NIST. 2012.

de la información (confidencialidad, integridad y disponibilidad) de los activos de información.

Esta guía propone que la gestión de incidentes de seguridad de la información consta de cinco fases, estas se describen a continuación.

5.4.1. Fase de planificación y preparación. Esta fase incluye actividades como formulación y creación de política de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información, documentación de formularios, procedimientos, elementos y herramientas utilizadas para la gestión y el reporte de incidentes, creación de un grupo de respuesta a incidentes, definición de las relaciones y conexiones con organismos internos y externos, definición de programas de formación y toma de conciencia en gestión de eventos e incidentes de seguridad de la información y ejecución de pruebas al esquema de gestión de incidentes definido.

5.4.2. Fase de detección y reporte. Las actividades claves dentro de esta fase incluyen, detección y reporte de eventos, esto se puede apoyar en el uso de herramientas tipo IDS/IPS, antivirus, herramientas de correlación, análisis de logs, reportes de usuarios, notificaciones de terceros, entre otras. También se incluye en esta fase la recolección de información asociada al evento o incidente de seguridad de la información, registro de las actividades de análisis, recolección de evidencia de forma adecuada de manera que esta sea posible de utilizar en caso que se requiera por razones legales o disciplinarias, escalamiento de atención de eventos en caso de ser necesario y registro de lo evidenciado en sistemas especializados para la gestión de eventos e incidentes de seguridad de la información.

5.4.3. Fase de evaluación y decisión. Para esta fase las actividades clave se centran en la evaluación y determinación de si un evento es o no un incidente de seguridad de la información, sus necesidades de escalamiento, dentro de estas definiciones deberán tenerse en cuenta escalas para la clasificación de eventos e incidentes, teniendo en cuenta el tipo de impacto generado por estos (físico o digital), activos de información, procesos, servicios, herramientas, aplicaciones, infraestructura, información y/o cualquier otro elemento que se pueda ver afectado por el evento. La definición de la manera en que debería ser abordado un incidente de seguridad de la información y por quien, se incluye en esta fase, de la misma manera se debe incluir la definición de la urgencia para su atención.

5.4.4. Fase de respuestas. En esta fase se incluye la definición de la respuesta requerida según el tipo de situación presentada, las cuales podrían ir desde la respuesta inmediata para iniciar la activación de una contingencia, hasta la generación de un comunicado informativo a colaboradores involucrados con el evento o incidente de seguridad, normalmente las respuestas inmediatas incluirán la interrupción o apagado de un sistema, la desconexión de una red o segmento de red, la implementación de controles adicionales, entre otros. Las respuestas

posteriores que deberían ejecutar desde un proceso de gestión de incidentes, según lo presentado por la guía, debería incluir la restauración de un sistema, servicio o red, la aplicación de parches y remediación de vulnerabilidades, desactivación de servicios y/o el cambio de contraseñas de los sistemas afectados. Esta fase incluye también la asignación de recursos para dar respuesta al incidente, la ejecución de análisis forenses si son necesarios, escalamiento del incidente en caso de que se encuentre necesario y distribución de las actividades para la gestión del incidente.

5.4.5. Fase de lecciones aprendidas. En esta se deben incluir la identificación de las lecciones aprendidas y las vulnerabilidades detectadas, identificar y ejecutar acciones de mejora a los controles de seguridad de la información, en lo posible, debería incluirse la inclusión de mejoras en el análisis de riesgos de la organización, actualización de las bases de datos de conocimiento de eventos e incidentes de seguridad, ejecutar acciones enfocadas en la comunicación y socialización de los resultados asociados a los eventos e incidentes de seguridad sucedidos.

Cuadro 6. Comparación de los marcos de trabajo para la gestión de eventos e incidentes de seguridad del NIST Special Publication 800-61 y la ISO 27035.

Fases	NIST Special Publication 800-61	ISO 27035
Fase de preparación	Incluye la preparación y prevención para estar preparado frente a la materialización de un evento o incidente de seguridad.	
Fase de detección y análisis	Incluye las actividades relacionadas con la identificación de eventos e incidentes de seguridad y su clasificación para posterior respuesta.	En ISO 27035, esta fase se divide en dos, una que incluye la detección del evento o incidente, en conjunto con el reporte del mismo y otra en la cual se realiza la evaluación y decisión sobre las acciones a seguir según el tipo de evento o incidente.
Fase de contención erradicación y recuperación	Hace referencia a las actividades que se deberían llevar a cabo para lograr detener el impacto causado por la materialización del incidente	
Fase de actividades post incidentes	Incluye las actividades que se realizan una vez se ha dado cierre al incidente de seguridad, recopilando información para la base de datos de conocimientos que será de ayuda para evitar la materialización de un evento o incidente similar en el futuro.	
Elaboración propia del autor		

Si bien, las dos guías o marcos de trabajo estudiados presentan grandes similitudes en las actividades de cada una de sus fases, el enfoque para ambos puede llegar a ser algo distinto, la presentada por NIST, puede que esté mayoritariamente enfocada a incidentes de seguridad informática y a su enfoque técnico para la gestión y respuesta de la misma, mientras que por otro lado el enfoque de la norma ISO 27035 es más de un sistema de gestión y puede llegar a verse más ligado a un SGSI que a un Centro de Operaciones de Seguridad. Sin embargo, se debe resaltar que ambos presentan un núcleo común que lo hace de suma importancia para definir el proceso central de un SOC a implementar.

5.4.6. Aspectos de ITIL para la gestión de infraestructura tecnológica enfocada a SOCs. En lo que respecta a la al pilar de las tecnologías, no se presentan marcos de trabajo específicamente pensados para ello, sin embargo, ITIL, incluye en sus prácticas algunas relacionadas con la gestión de tecnología desde el punto de vista de la gobernanza de TI, la cual podría aplicar totalmente a la implementación de un Centro de Operaciones de Seguridad. Entre estas prácticas se destacan las siguientes:

5.4.6.1. Gestión de la capacidad y rendimiento. En esta práctica se busca garantizar que se cuenta con la suficiente capacidad para brindar los servicios ofrecidos por la organización, a los niveles de rendimiento esperados. En lo que respecta a un Centro de Operaciones de Seguridad, el análisis de la capacidad se podría enfocar a las necesidades de funcionamiento de las diferentes herramientas a utilizar en el SOC, pensando en sus tiempos de carga o respuesta, así como los tiempos de espera durante los análisis o la generación de reportes. La meta fundamental de una adecuada gestión de la capacidad es la de garantizar la capacidad suficiente para prestar el servicio ofreció, teniendo en cuenta esto, las organizaciones deberían investigar, analizar y presupuestar los requerimientos de capacidad de su servicio, planear e implementar dicha capacidad e identificar las posibles mejoras que beneficien la misma.

5.4.6.2. Gestión de los activos de TI. En ITIL se define a un activo como cualquier componente del servicio que tiene un valor y contribuye a entregar de manera adecuada el servicio ofrecido, en este orden de ideas, las herramientas de monitoreo, equipos de cómputo, de red y servidores utilizados por el Centro de Operaciones de Seguridad hacen parte de los activos de TI. La adecuada gestión de activos busca asegurar el obtener el máximo valor de los activos, permitir una toma de decisiones acertada en lo concerniente a adquisición o retiro de activos, así como poder gestionar de manera adecuada los riesgos asociados a estos.

5.4.6.3. Gestión de despliegue. Esta práctica se enfoca en asegurar un adecuado despliegue de los procesos, hardware o software nuevos para la organización al ambiente productivo, dependerá del tipo de compañía el definir el tipo de despliegue que tendrá para sus componentes de servicios, estos podrían hacerse uno a uno, todos a la vez, por fases, de forma automatizada o manual. En lo que respecta a un

SOC, esta práctica podría ser tenida en consideración al momento de ir adicionando nuevo software o herramientas al pull de servicios ofrecidos, garantizando una transición adecuada del ambiente de pruebas al de producción.

5.4.6.4. Gestión de infraestructura y plataforma. El escenario de gestión de la infraestructura y plataforma se enfoca en garantizar que se tenga una visibilidad de la plataforma tecnológica de la organización, de manera se pueda mantener a la misma en monitoreo continuo y garantizar el funcionamiento las soluciones tecnológicas utilizadas para la prestación del servicio. Esta práctica hace la recomendación de incluir todos los proveedores de servicios en la nube, herramientas, aplicaciones, software como servicio, infraestructura como servicio, herramientas de inteligencia artificial y en general todas las que sustentan los servicios que ofrece la organización. La gestión de la infraestructura tendrá una relación estrecha con otros aspectos de gestión como el financiero, de proveedores, de la capacidad, de incidentes, de control de cambios y de despliegue.

5.5. SELECCIÓN DE HERRAMIENTAS QUE HACEN PARTE DE LA ARQUITECTURA DE UN CENTRO DE OPERACIONES DE SEGURIDAD

Tal como se ha mencionado en capítulos anteriores de este documento, las herramientas tecnológicas son parte fundamental de los centros de operaciones de seguridad, ya se ha mencionado en los análisis realizados a trabajos de implementación de SOC que existen algunas herramientas en las cuales los autores concuerdan de manera clara, estos son los siguientes: SIEM, IDS/IPS, herramientas de gestión de vulnerabilidades, Sandbox y herramientas de inteligencia de amenazas.

Si bien existen otras herramientas adicionales mencionadas por los autores de las implementaciones de Centros de Operaciones de Seguridad analizados, estas se no se incluyen en lo que se considera como herramientas de un SOC, debido a que no son propias de estos, sino que se podrían llegar a considerar como herramientas de seguridad que normalmente se encuentran en las diferentes compañías, por ejemplo, Firewalls, antivirus, WAF, herramientas de control de acceso, entre otros, las cuales incluso podrían llegar a verse como fuentes de información de herramientas como los SIEM.

A continuación, se hará un despliegue más completo de cada una de las herramientas tecnológicas que se han considerado para hacer parte de la arquitectura de un centro de operaciones de seguridad.

5.5.1. SIEM. Ya se ha hablado de estos como parte fundamental de un SOC, esto debido a que son estas herramientas las que se encargan de analizar, correlacionar y generar alertas mediante la recopilación de eventos de seguridad proveniente de múltiples fuentes. Esta herramienta de análisis y correlación de eventos se vuelve casi el núcleo de un centro de operaciones de seguridad puesto que es mediante

ella como se los analistas logran percibir la realidad de operación de la seguridad de una compañía.

Estos dispositivos traen consigo una gran capacidad de aumentar la visibilidad en tiempo real de lo que ocurre con los dispositivos de la red, sin embargo, esta gran cantidad de información podría llegar a convertirse en algo tedioso de analizar si no se cuentan con dashboards claros que presenten la información de una manera adecuada a los analistas u operadores del SOC.

Como ya se ha mencionado antes, los SIEM recopilan datos de diferentes fuentes de información de una red, entre los cuales se pueden encontrar: enrutadores, Access points, controladores WiFi, switches, servidores de correo, servidores de archivos, servidores web, herramientas de prevención y detección de intrusiones, firewalls, gestores antivirus, herramientas de filtrado de contenido y en general cualquier tipo de software[78].

La recopilación de registros de eventos en los SIEM se lleva a cabo mediante diferentes mecanismos y protocolos, en los cuales se destaca el uso de agentes de monitoreo, los cuales se instalan en los equipos a monitorear y estos se encargan de redirigir todos los eventos generados en el activo monitoreado al servidor central de monitoreo. Sin embargo, este no es el único mecanismo utilizado por los SIEM para recopilar información, en los casos donde no es posible instalar ningún tipo de agente, se puede llegar a hacer recolección de LOGs mediante la función de log forwarding o reenvío de logs, la cual lo que normalmente hace es que los servidores, aplicaciones, herramientas y otros dispositivos configuren el servidor central de monitoreo como su servidor de almacenamiento de registros de eventos.

Dentro del análisis realizado por este tipo de herramientas en cada uno de los eventos que recopila, se destacan algunos atributos que son normalmente tenidos en consideración, los cuales son: las direcciones IP relacionadas con el evento, el tipo de evento, la fecha y hora del evento, los usuarios relacionados, la aplicación relacionada, puertos o servicios asociados al evento, entre otros. Las funciones de un SIEM no se quedan únicamente en recopilar los eventos y analizar algunos atributos de estos, normalmente estas herramientas cuentan con algún tipo de módulo de inteligencia que mediante unas reglas de correlación puede llegar a discernir cuando un evento o una serie de estos pueden estar relacionados con situaciones maliciosas para la red, lo cual llevará a activar un indicador de posible compromiso y a generar una alerta para los analistas del SOC.

Los SIEM normalmente almacenan los registros de eventos durante un tiempo determinado que puede ir desde los días hasta meses o años, según la capacidad

[78] SPLUNK. “What is a SIEM?”. {En línea}. {6 de marzo de 2022} disponible en: (https://www.splunk.com/en_us/data-insider/what-is-siem.html).

de almacenamiento del equipo donde corra la herramienta, esto permite mantener evidencias en caso de investigaciones futuras de incidentes de seguridad.

Las herramientas tipo SIEM pueden ser encontradas con licencias gratuitas y de pago, lo cual puede hacer mucho más sencilla su implementación en compañías que no cuentan con un gran presupuesto para inversión en herramientas especializadas en seguridad.

Según lo descrito por Gartner en su cuadrante mágico para este tipo de herramientas en el año 2021, existen un grupo de fabricantes lideres entre los cuales se destacan:

- Exabeam
- Securonix
- IBM
- Splunk
- Rapid7
- LogRythim

A estos fabricantes anteriormente mencionados los siguen de cerca los denominados visionarios en los cuales aparecen:

- Microsoft
- Fortinet
- Gurucul
- Sumo Logic

Cabe destacar que estas soluciones SIEM mencionadas son de licencia de pago. A continuación, se presenta el cuadrante mágico de gartners para herramientas SIEM en el año 2021:

Imagen 2. Cuadrante mágico de Gartner para SIEM a corte de 2021

Tomado de lo presentado por Exabeam[79]

En cuanto herramientas SIEM gratuitas, entre las más conocidas, según lo descrito por DNSStuff[80], se encuentran:

- AlientVault OSSIM
- OSSEC
- Wazuh
- Apache Metron.

5.5.2. IDS/IPS. Los IDS/IPS son herramientas que se encargan de analizar y comparar paquetes de red frente a firmas de amenazas de seguridad de redes ya conocidas, de manera que puedan identificar si alguna de dichas herramientas se encuentra en la red monitoreada. Según el tipo de dispositivo, si es un IDS (Intrusion Detection System) o un IPS (Intrusion Prevention System), este podría tener una serie de características que lo diferencia.

[79] EXABEAM. “Cuadrante mágico de gartner para SIEM”. {En línea}. {21 de junio de 2022} disponible en: (https://www.exabeam.com/wp-content/uploads/GartnerMQ-2021-Figure1-2.png)
[80] DNSSTUFF. “10 Best Free and Open-Source SIEM Tools”. {En línea}. {18 de junio de 2022} disponible en: (https://www.dnsstuff.com/free-siem-tools).

Un IDS puro, podría considerarse una herramienta de monitoreo de red que indicará si existe un paquete que tenga patrones similares a alguno asociado a una amenaza ya identificada de forma previa, esta indicación generará una alerta en los analistas del centro de operaciones, de manera que podrán tomar cartas en el asunto según la veracidad de la alerta generada y la criticidad de la situación.

Los IPS por otro lado, además de generar este tipo de alertas, están en la capacidad de tomar acciones automáticas frente a las amenazas que detectan, funcionando de una manera similar a como lo hacen los firewalls, de manera que estos podrían incluso llegar a hacer un descarte de paquetes que consideran maliciosos.

Este tipo de herramientas normalmente son incluidos como módulos en los Firewall, específicamente en Firewalls de nueva generación (NGFW); si bien podría pensarse en los IDS/IPS como una fuente más de información para los SIEM, estos se convierten en una herramienta de importante despliegue de los SOC ya que puede generar alertas de monitoreo por sí sola, e incluso tomar acciones que ayuden a evitar la materialización de un evento o incidente de seguridad.

Si bien se ha mencionado que los IDS/IPS utilizan métodos de comparación de firmas para detectar amenazas en la red, algunos fabricantes incluyen módulos de inteligencia artificial y machine learning que utilizan para detectar amenazas más sofisticadas y complejas, logrando detectar comportamientos maliciosos de manera orgánica y no basados en eventos sucedidos con anterioridad, lo que ayuda a detectar ataques nuevos que de momento no tengan una firma comparable para identificarlos[81].

Para el año 2018, Gartner[82], incluyo en su cuadrante mágico de líderes en este tipo de herramientas a los siguientes fabricantes:

- Cisco
- TrendMicro
- McAfee

[81] KEARY, Tim. “Comparitech. IDS vs IPS”. {En línea}. {15 de abril de 2022} disponible en: (https://www.comparitech.com/net-admin/ids-vs-ips/).
[82] GARTNER. “Gartner Magic Quadrant for Intrusion Detection and Prevention Systems”. {En línea}. {15 de junio de 2022} disponible en: (https://www.gartner.com/en/documents/3844163/magic-quadrant-for-intrusion-detection-and-prevention-sy).

Imagen 3. Cuadrante mágico de Gartner para IDS/IPS en el año 2018

Tomado de Gartner.

Este tipo de herramientas también pueden ser implementados mediante soluciones de tipo gratuito, entre los cuales, según el blog de seguridad UpGuard[83], entre estas se destacan:

- Snort
- Suricata
- OpenWigs-ng
- Security Onion

5.5.3. Herramientas de gestión de vulnerabilidades. Estas herramientas de tipo software tienen como función principal ayudar a los analistas de monitoreo a tener una visión completa de los dispositivos que podrían ser vulnerables y que requieren de una actividad de remediación o de lo contrario podrían verse expuestas a que una amenaza las explotara.

La gestión y análisis de vulnerabilidades se basa en la identificación, análisis y remediación de las debilidades de los sistemas de información críticos de una

[83] SEN Kaushik. “Top 6 Free Network Intrusion Detection Systems (NIDS) Software in 2022”. {En línea}. {2 de junio de 2022} disponible en: (https://www.upguard.com/blog/top-free-network-based-intrusion-detection-systems-ids-for-the-enterprise).

compañía, esta actividad debe ser realizada de manera periódica, de forma que se logre tener un cubrimiento de las vulnerabilidades que van surgiendo con el día a día.

Una adecuada gestión de vulnerabilidades es un ciclo continuo que incluye las siguientes fases[84]: Inventario de activos o sistemas, en esta fase se identifican cuáles serán los sistemas de información, equipos de cómputo, servidores, dispositivos de red, entre otros dispositivos que serán parte del alcance de la prueba o análisis de vulnerabilidades, luego se realiza la planeación del análisis de vulnerabilidades, fase en la cual se determinan los tipos de análisis a realizar, el cronograma de pruebas y posibilidades de afectación de las mismas, se continua con la ejecución del análisis de vulnerabilidades, la cual es la fase en la que se lleva a cabo todo el descubrimiento de las debilidades de los activos que hacen parte del alcance, una vez tenidos los resultados del análisis, se priorización de vulnerabilidades encontradas, dando prioridad al cierre de aquella con mayor nivel de severidad, por último, se ejecuta la remediación de las vulnerabilidades encontradas para luego realizar validación de cierre de las mismas, esto podría hacerse con una segunda corrida del análisis.

Si bien no se tiene un benchark corporativo como el ofrecido por el cuadro mágico de Gartner para este tipo de herramientas, existen algunas que se destacan por su trayectoria en el mercado de la gestión y análisis de vulnerabilidades, entre las cuales se tiene:

- Nessus
- Qualys
- Rapid7
- Tenable.IO
- Acunetix

También es posible encontrar herramientas para la gestión de vulnerabilidades de licenciamiento gratuito, entre las cuales se encuentran:

- OpenVAS
- OWASP ZAP
- Nmap
- Uniscan

5.5.4. Sandbox. Las herramientas conocidas como Sandbox son aquellas que se utilizan para generar ambientes aislados en los cuales se pueden realizar pruebas sobre archivos, aplicaciones y/o cualquier otro tipo de software del cual se sospecha

[84] A2SECURE. “Herramientas para la gestión y análisis de Vulnerabilidades”. {En línea}. {13 de mayo de 2022} disponible en: (https://www.a2secure.com/blog/herramientas-para-la-gestion-y-analisis-de-vulnerabilidades/).

que podría incluir algún tipo de amenaza estas herramientas podrían ser de tipo software e incluso hardware dedicado.

Existen tres mecanismos principales de despliegue de este tipo de herramientas, una asociada a la emulación completa del sistema, en la cual se simula el hardware físico, la memoria y CPU del dispositivo, de manera que se tiene una comprensión completa de los efectos del malware sobre el sistema. El segundo mecanismo es la emulación únicamente del sistema operativo, en este caso la herramienta no emula el hardware, memoria o CPU, dando así una precisión que podría considerarse un poco menor a la del primer mecanismo. Por último, se tiene el mecanismo de menor precisión, el de virtualización o uso de contenedores, en este ejemplo el sistema solo se utiliza para correr el software a evaluar, de manera que la confianza en estos puede ser bastante limitada ya que no se emula de forma completa el impacto del posible malware en el sistema ni en el hardware asociado al mismo[85].

Las principales características de estas herramientas están enfocadas en el análisis de malware, incluyendo apoyo en el análisis de amenazas, filtrado de amenazas, detección temprana de amenazas, reporte y automatización de análisis. Este tipo de herramientas sin duda alguna es un apoyo a las actividades de monitoreo de los analistas de un SOC ya que les permite identificar si algún archivo, software, paquete o dato sospechoso podría llegar a ser o no malicioso, de esta manera se logra influir positivamente en la capacidad de prevención y detención del centro de operaciones de seguridad.

Un Sandbox debería ser capaz de analizar gran cantidad de tipos de objetos de diferentes formatos como, por ejemplo, PDFs, Microsoft office, librerías, archivos JAVA y Flash, así como elemento de código HTML o JavaScript que podrían ser maliciosos.

Existen gran cantidad de fabricantes de herramientas Sandbox con licencia comercial como gratuita, a continuación, se presentan algunos de estos fabricantes de herramientas Sandbox licenciadas:

- Crowdstrike: Falcon Sandbox
- Fortinet: FortiSandbox
- McAfee: Advance Threat Defense
- Zscaler: Cloud Sandbox

[85] HYSOLATE. “Sandboxing Security: A Practical Guide”. {En línea}. {21 de junio de 2022} disponible en: (https://www.hysolate.com/learn/sandboxing/sandboxing-security-a-practical-guide/).

En cuanto a herramientas Sandbox de uso libre, se cuenta con los siguientes referentes:

- VirusTotal
- Shade Sandbox
- Máquinas virtuales especialmente configuradas en VMware o VirtualBox.
- Cameyo

5.5.5. Herramientas de inteligencia de amenazas. Este tipo de herramientas son fundamentales en lo que respecta a la preparación, prevención e identificación de amenazas de seguridad para la red. La inteligencia de amenazas se ocupa de la recolección, procesamiento y análisis para comprender todo el contexto de las amenazas, desde sus actores, motivaciones y comportamiento de ataques relacionados. Este tipo de herramientas brindan la posibilidad de acceder a fuentes de información de amenazas los cuales traerán entre otros beneficios los siguientes, descubrimiento de amenazas desconocidas para la red, entendimiento de los ataques que suceden a nivel local o global y que podrían afectar a la red de una compañía y facilita la toma de decisiones y planteamiento de estrategias de seguridad de forma efectiva[86].

Las plataformas o herramientas de inteligencia de amenazas aportan gran cantidad de información asociada a indicadores de compromiso, presentando recomendaciones necesarias para evitar ser víctima de algún tipo ataque. Dentro de los indicadores de compromiso que se pueden encontrar en estas plataformas se encuentran, direcciones IP asociadas a amenazas, correos electrónicos maliciosos, dominios asociados a amenazas, enlaces o archivos adjuntos asociados a actividades maliciosas, firmas o hashes, archivos de librerías y registros, entre otros. Algunas de estas plataformas están asociadas a otros dispositivos y herramientas de seguridad, como por ejemplo las plataformas de inteligencia asociadas a Firewalls de diferentes fabricantes.

La inteligencia artificial y el machine learning también juegan un papel importante en este tipo de herramientas, esto debido a la gran cantidad de información que se debe tratar en la actualidad, estas características permiten que las herramientas puedan reconocer patrones y predecir posibles ataques.

A continuación, se listan algunas plataformas de inteligencia de amenazas licenciadas que pueden encontrarse en el mercado:

- CrowdStrike Falcon X
- AlienVault Unified Security Management

[86] BAKER, Kurt. “What is cyber threat intelligence?”. {En línea}. {23 de junio de 2022} disponible en: (https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/)

- Avira Threat Intelligence
- EclecticIQ Platform

Dentro de este tipo de plataformas también se encuentran algunas de uso libre, entre las cuales se destacan las siguientes:

- IBM X-Force
- Cisco Talos
- Metadefender
- VirusTotal
- The Hive Project

Con lo anterior se ha dado un repaso por las herramientas tecnológicas que juegan un papel importante para la implementación de un SOC, a continuación, se hará la selección de dos herramientas para cada uno de los tipos descritos, una de uso libre y una licenciada, esto para incluir ambas opciones en el análisis presupuestal del siguiente capítulo de este documento.

- SIEM licenciado: Splunk
- SIEM de uso libre: Wazuh
- IDS/IPS licenciado: Cisco NGIPS
- IDS/IPS de uso libre: Suricata
- Herramienta de gestión de vulnerabilidades licenciada: Nessus
- Herramienta de gestión de vulnerabilidades licenciada: OpenVAS
- Sandbox licenciado: Crowdstrike: Falcon Sandbox
- Sandbox de uso libre: VirusTotal
- Herramienta de inteligencia de amenazas licenciada: AlienVault Unified Security Management
- Herramienta de inteligencia de amenazas de uso libre: Cisco Talos

5.6. COSTOS ASOCIADOS A LA IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD.

En los anteriores capítulos de este documento se ha realizado una revisión de todos los aspectos necesarios para implementar un SOC desde el punto de vista de tres aristas fundamentales: Personas, Procesos y Tecnologías.

En este capítulo final del documento se propone realizar un acercamiento presupuestas a los diferentes costos asociados que se pueden tener al implementar un centro de operaciones de seguridad, teniendo en consideración los elementos que se han definido en cada uno de los capítulos anteriores.

Empezando por el pilar de las personas, se deberán definir los roles y/o perfiles de cargo que harán parte del Centro de Operaciones de Seguridad de la información; teniendo en consideración aquello analizado en el primer capítulo de esta

monografía, se ha identificado que normalmente los centros de operaciones de seguridad se componen de los siguientes roles principales:

- Analista de nivel 1
- Analista de nivel 2
- Analista especializado en cacería de amenazas y/o atención de incidentes
- Director o gerente del SOC

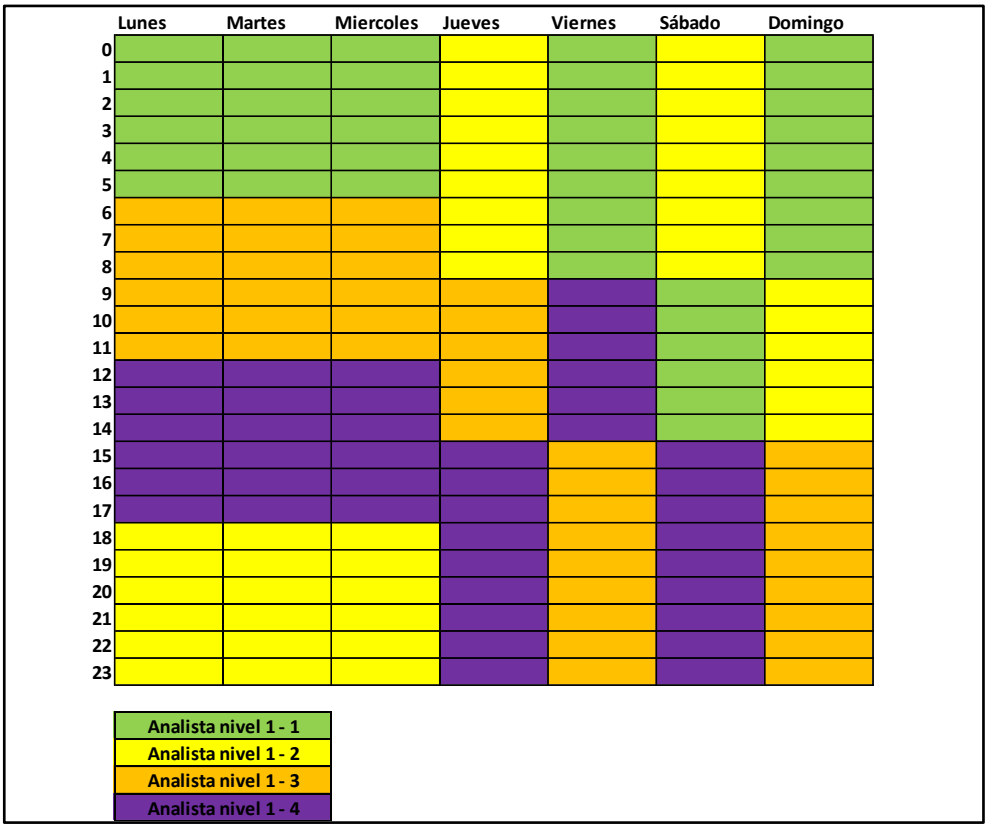
Teniendo identificados los roles que hacen parte comúnmente de los SOC, es importante definir la cantidad de personas que ocuparan los roles presentados, esta cantidad normalmente se logra definir teniendo en cuenta el horario de servicio del Centro de Operaciones de Seguridad, los cuales en su gran mayoría funcionan en modalidad 7x24.

Según el Código Sustantivo del Trabajo de Colombia, la jornada máxima de trabajo diario no debe ser superior a las 9 horas y semanalmente no debe superar las 42 horas, teniendo siempre un día de descanso semanal[87], esto implica que para lograr cubrir los 7 días de la semana en sus 24 horas, lo cual representa un total de 168 horas, se deberían tener mínimo 4 analistas de nivel 1 que cubran cada uno 42 horas, de esta manera se logra el total de horas requeridas cumpliendo con la normatividad laboral del país.

Con el objetivo de mostrar la manera en que se podría distribuir el horario de trabajo de cada analista, se presenta a continuación un cronograma u horario laboral propuesto para los analistas de nivel 1, quienes realizan la labor de monitoreo constante de las fuentes de información de amenazas, logs de sistemas, vulnerabilidades, alertas, entre otras:

[87] REPUBLICA DE COLOMBIA. (2022). Código Sustantivo del Trabajo. Decreto 2663 de 1950. Diario Oficial No. 51945. Bogotá. 1951.

Imagen 4. Cronograma de trabajo propuesto para Analistas de nivel 1



Elaboración propia del autor

De la misma manera, para cubrir la disponibilidad de los analistas de nivel 2 durante las jornadas de 7x24 horas que deben garantizarse en el SOC, deberían existir como mínimo dos analistas de nivel dos que laboren 6 días a la semana por 7 horas (en diferentes jornadas), cada uno con un día de descanso diferente al del otro analista de nivel 2.

Por último, tanto el analista especializado en solución de incidentes de seguridad como el director del SOC deberían tener jornadas de 6 días por 7 horas cada una con un día de descanso, sin embargo, estos cargos deberán ser tratados como cargos de confianza, los cuales según el artículo 162 Código Sustantivo del Trabajo de Colombia[88], pueden tener jornadas que superen las máximas establecidas, es decir que podrían superar las 42 horas máximas a la semana, lo que permitiría que ambos roles puedan reaccionar frente a situaciones que no pueden ser atendidas por los analistas de nivel 1 y/o nivel 2.

[88] Ibid

Una vez identificada la cantidad de personas requeridas para ejercer la labor de cada rol, se precede a realizar la identificación de los posibles costos asociados a la contratación de cada uno de ellos, para hacer un análisis más simple, se tendrán en consideración únicamente los costos asociados a salarios, más no los asociados a aportes fiscales, documentación, afiliaciones u otros aportes administrativos que deriven de la contratación de un trabajador.

Para lograr definir un valor salarial aproximado para los diferentes roles que podrían hacer parte de un SOC, se realizó una revisión de diferentes propuestas de trabajo asociadas a dichos roles, de manera que se pudiera definir un perfil aproximado con el cual buscar información de costos salariales asociados.

Inicialmente se analizó el rol de analista de nivel 1 mediante la plataforma LinkedIn[89], en la cual, con ayuda del buscador de empleos se encontró lo siguiente respecto a la experiencia o perfil del cargo:

- Mínimo un año de experiencia como analista de red o de seguridad.
- Conocimiento en gestión de redes.
- Conocimiento en utilización de herramientas especializadas de seguridad.
- Conocimiento en normativas de seguridad.

Con el objetivo de encontrar valores referenciales para este tipo de cargos, se realizó una búsqueda en la herramienta Computrabajo.com[90]. En la cual se encontró que, para cargos con requerimientos de experiencia y formación similares, los salarios oscilan entre el $1.500.000 y los $2.500.000, esto permite definir un rango medio de aproximadamente $2.000.000.

De la misma manera, utilizando LinkedIn[91], se logró encontrar que para el rol de analista nivel 2, la experiencia o perfil de cargo asociado apunta a lo siguiente:

- Mínimo dos años de experiencia como analista de red o seguridad.
- Conocimiento avanzado de herramientas de red y servidores
- Conocimiento avanzado de herramientas de seguridad

Según lo encontrado en CompuTrabajo[92] para perfiles similares al mencionado para el cargo de analista de nivel 2 para el SOC, los valores referenciales de salarios se

[89] LINKEDIN. “Buscador de empleos LinkedIn”. {En línea}. {7 de junio de 2022} disponible en: (https://www.linkedin.com/).
[90] COMPUTRABAJO. “Ingeniero de redes”. {En línea}. {7 de junio de 2022} disponible en: (https://www.computrabajo.com.co/trabajo-de-ingeniero-de-redes).
[91] Ibid
[92] COMPUTRABAJO. “Ingeniero de soporte nivel 2”. {En línea}. {7 de junio de 2022} disponible en: (https://www.computrabajo.com.co/trabajo-de-soporte-nivel-2).

encuentran entre los $2.300.000 y $3.200.000, esto permite definir un rango medio aproximado de $2.750.000.

Los roles de analista especialista en solución de incidentes y Director SOC fueron buscados de la misma manera, utilizando la ayuda del buscador de la red social LinkedIn y la página para búsqueda de empleo denominada “ElEmpleo”. Las búsquedas arrojaron los siguientes valores para cargos de similar experiencia y perfil.

Salario promedio para cargos similares al de analista especialista en solución de incidentes de seguridad: $4.000.000 a $4.500.000[93].

Salario promedio para cargos similares al de Director SOC: $4.500.000 a $5.500.000[94].

Cuadro 7. Revisión de costos de contratación de personal para el SOC

Rol	**Cantidad de personas requeridas**	**Salario mensual por persona**	**Costo mensual total**
Analista nivel 1	4	$2.000.000	$8.000.000
Analista nivel 2	2	$2.750.000	$5.500.000
Analista especialista en solución de incidentes de seguridad	1	$4.250.000	$4.250.000
Director del SOC	1	$5.000.000	$5.000.000
		Total	**$22.750.000**
Elaboración propia del autor			

Según el análisis realizado, los costos salariales aproximados para la planta de recursos del pilar “Personas” serían de $22.750.000 mensuales.

El siguiente pilar del servicio de Centro de Operaciones de Seguridad que implica un gasto monetario es el de las “Tecnologías”, el cual incluye tanto el hardware necesario para la operación, como el software especializado que podría necesitar el SOC para funcionar.

[93] ELEMPLEO. “Senior Incident Response specialist”. {En línea}. {7 de junio de 2022} disponible en: (https://www.elempleo.com/co/ofertas-trabajo/senior-incident-response-specialist/1885124212?trabajo=respuesta%20a%20incidentes).

[94] ELEMPLEO. “Director del SOC”. {En línea}. {7 de junio de 2022} disponible en: (https://www.elempleo.com/co/ofertas-trabajo/director-del-soc/1881089727).

Inicialmente se hará el análisis de aquellos elementos básicos de funcionamiento, se obviarán equipos de red como routers, firewalls o switches, pues se considera en el estudio realizado que se implementará el SOC en una Compañía que ya cuenta con dichos equipos, en este análisis de costos solo se incluirán los equipos de cómputo del personal del SOC y los monitores o pantallas extra que son típicas de los centros de monitoreo.

Se definirán a continuación, tres gamas de equipos de cómputo para los diferentes roles del SOC, una gama inicial más enfocada a actividades administrativas y de gestión, como las desarrolladas por el Director del SOC; una gama intermedia será pensada para los analistas tanto de nivel 1 como de nivel 2; por último, se relaciona una última gama especializada de equipo de cómputo pensada para el especialista en solución de incidentes de seguridad.

Características equipo de gama inicial:

Memoria RAM de 12 GB
Disco duro de 250 GB tipo SSD
Sistema Operativo Dual: Windows 10/Ubuntu
Procesador Intel Core I3 o AMD Ryzen 3

Características equipo de gama intermedia:

Memoria RAM de 16 GB
Disco duro de 500 GB tipo SSD
Sistema Operativo Dual: Windows 10/Ubuntu
Procesador Intel Core I5 o AMD Ryzen 5

Características equipo de gama especializada:

Memoria RAM de 32 GB
Disco duro de 1TB tipo SSD
Sistema Operativo Dual: Kali Linux
Procesador Intel Core I7 o AMD Ryzen 7

A continuación, se presenta la tabla de costos para los equipos de cómputo y los monitores extra para el Centro de Operaciones de Seguridad:

Cuadro 8. Revisión de costos de adquisición de equipos de cómputo y monitores para el SOC

Tipo de Dispositivo	**Cantidad de dispositivos**	**Valor unitario**	**Costo total**
Equipo de gama inicial	1	$1.890.500[95]	$1.890.500
Equipo de gama intermedia	6	$2.314.914[96]	$13.889.484
Equipo de gama especializada	1	$5.849.900[97]	$5.849.900
Monitor extra de 24”	8	$710.000[98]	$5.680.000
		Total	**$27.309.884**
Elaboración propia del autor			

Según el análisis y recopilación de costos realizada, el costo para la adquisición de equipos de cómputo es de $27.309.884, este valor podría dividirse en 3 años, para determinar el costo anual de la adquisición, teniendo en consideración la renovación de los equipos al finalizar los tres años, esto supone un costo anual de $9.103.295, de esta manera se podrán llevar a cabo la totalización de costos anuales de implementación del Centro de Operaciones de Seguridad.

Para terminar, ahora es necesario realizar el análisis y recopilación de costos de las herramientas seleccionadas en el capítulo anterior, se debe tener en cuenta que se

[95] MERCADOLIBRE. “Consulta Computador Portatil”.{En línea}. {7 de junio de 2022} disponible en: (https://articulo.mercadolibre.com.co/MCO-867337790-portatil-asus-x515-core-i3-1005g1-ssd-256gb-12gb-ram-obs-win-_JM?searchVariation=174280574915#searchVariation=174280574915&position=18&search_layout=stack&type=item&tracking_id=4e48132d-3753-49d6-b00e-916ef8deaa8f).

[96] MERCADOLIBRE. “Consulta Computador Portatil”. {En línea}. {7 de junio de 2022} disponible en: (https://www.mercadolibre.com.co/laptop-dell-inspiron-3505-gris-156-amd-ryzen-5-3450u-16gb-de-ram-256gb-ssd-amd-radeon-rx-vega-8-60-hz-1366x768px-windows-10-home/p/MCO16999018?pdp_filters=category:MCO1652#searchVariation=MCO16999018&position=1&search_layout=stack&type=product&tracking_id=17d1b815-3446-4125-9559-14cdd0d77ceb).

[97] MERCADOLIBRE. “Consulta Computador Portatil”. {En línea}. {7 de junio de 2022} disponible en: (https://articulo.mercadolibre.com.co/MCO-820678334-portatil-msi-core-i7-10750h-ram-32gb-dd-1tb-ssd-156-fhd-_JM?searchVariation=173803746208#searchVariation=173803746208&position=5&search_layout=stack&type=item&tracking_id=1831e60a-723a-4b44-b2ba-383a6d56058d).

[98] MERCADOLIBRE. “Consulta Computador Portatil”. {En línea}. {7 de junio de 2022} disponible en: (https://www.mercadolibre.com.co/monitor-gamer-samsung-f24t35-led-24-azul-y-gris-oscuro-100v240v/p/MCO17360590?pdp_filters=category:MCO1656#searchVariation=MCO17360590&position=1&search_layout=stack&type=product&tracking_id=a99baa65-bbba-424b-90e9-04fc939e2fca).

hará el análisis para las herramientas licenciadas, debido a que son estas aquellas que tendrán un costo para la compañía.

Para el análisis de los costos asociados a las herramientas de tipo software, se deberá tener en consideración la necesidad de adquirir servidores (físicos o en la nube) que permitan ejecutar las herramientas cuando así se requiera pues estos valores no se incluyen en el análisis realizado. A continuación, se hace un recuento de las herramientas licenciadas seleccionadas en el capítulo anterior:

- SIEM licenciado: Splunk
- IDS/IPS licenciado: Cisco NGIPS
- Herramienta de gestión de vulnerabilidades licenciada: Nessus
- Sandbox licenciado: Crowdstrike: Falcon Sandbox
- Herramienta de inteligencia de amenazas licenciada: AlienVault Unified Security Management

5.6.1. Splunk. Iniciando por la herramienta Splunk, es importante saber que esta tiene varios modelos de licenciamiento, los cuales podrían estar asociados al tipo de licencia que se adquiere, ya sea tipo Cloud o Enterprise. Según la guía de precios de Splunk, en su versión Cloud, el costo por equipo de cómputo empieza en $40 USD por mes[99]. Teniendo en cuenta el valor promedio del dólar para el año 2021 en Colombia, el cual está fijado en $3.743[100], este valor equivaldría a un total de $149.720 por mes, lo que a su vez se puede llevar a un valor de 1.796.640 por año por cada equipo monitoreado. Para efectos prácticos se supone una red en la cual se deba monitorear un máximo de 30 equipos, lo cual daría un costo total aproximado anual para la herramienta Splunk de $53.899.200, es importante tener en cuenta que este es un valor que podría modificarse según los acuerdos entre proveedores y clientes según los diferentes niveles de partnering o los volúmenes de compra. Esta herramienta al ser de despliegue en la nube no requiere la adquisición de un equipo de tipo servidor adicional.

5.6.2. NGIPS de CISCO. Continuando con el análisis aproximado del costo de la implementación de las herramientas seleccionada, el NGIPS de Cisco en su versión para sistemas virtualizados con licencia de un año, tiene un costo de aproximadamente $9.895 USD[101], esto representa un total anual de $37.036.985. Para esta herramienta, si es necesario tener un servidor de virtualización en el cual implementarla, específicamente uno con licencia de VMWare.

---

[99] SPLUNK. “Splunk Pricing”. {En línea}. {8 de junio de 2022} disponible en: (https://www.splunk.com/en_us/software/pricing.html).

[100] DOLARHOY. “Precio del dólar en el año 2021”. {En línea}. {23 de junio de 2022} disponible en: (https://www.dolarhoy.co/ano/2021).

[101] ITPRICE. “Cisco FP-VMW-IPS-K9”. {En línea}. {8 de junio de 2022} disponible en: (https://itprice.com/cisco/fp-vmw-ips-k9.html).

5.6.3. Nessus Professional. La herramienta de análisis de vulnerabilidades Nessus Professional, según la página web oficial, tiene un costo anual de $16.802.191[102]. Para esta herramienta es importante que se debe tener un equipo de cómputo o servidor en el cual implementarla.

5.6.4. Crowdstrike: Falcon Sandbox. Esta herramienta tiene un valor aproximado de $6.000[103] USD para una capacidad de hasta 250 archivos por mes. Esto equivale a un total de $22.458.000 anuales. Es importante considerar para esta herramienta que el despliegue se hace en una nube privada, lo que podría aumentar los costos de despliegue de la misma.

5.6.5. AlienVault Unified Security Management. Por último, la herramienta de inteligencia de amenazas de AlienVault tiene un valor mensual de $1.695 USD[104], lo que se traduce en un aproximado de $20.340 USD al año, lo que es igual a $76.132.620. Con esta última herramienta es importante tener en consideración que esta podría reemplazar tanto al NGIPS, al SIEM y al escáner de vulnerabilidades. Razón por la cual se evaluará de manera individual.

Habiendo realizado un acercamiento presupuestal para todas las posibles herramientas a utilizar en la implementación del SOC, a continuación, se presenta el resumen de costos del rubro asociado al software necesario para la implementación:

Cuadro 9. Análisis y recopilación de costo anual de herramientas tipo software para la implementación del SOC

Software	**Costo**
SIEM Spluk	$53.899.200
NGIPS Virtual Cisco	$37.036.985
Nessus Professional	$16.802.191
Clowdstrike Falcon Sandbox	$22.458.000
Total	**$130.196.376**
Elaboración propia del autor	

Como se observa en la tabla 9, la implementación de las herramientas de software en el SOC puede llegar a ser lo más costoso, es por esta razón que en el capítulo anterior también se presentaron algunas opciones de herramientas de uso libre, las

[102] NESSUS. “Nessus Professional Price”. {En línea}. {7 de junio de 2022} disponible en: (https://es-la.tenable.com/products/nessus/nessus-professional)
[103] CYBERSECURITYPRICING. “Crowdstrike Pricing”. {En línea}. {23 de junio de 2022} disponible en: (https://cybersecuritypricing.org/tag/crowdstrike-pricing/).
[104] AT&T. “USM Pricing”. {En línea}. {23 de junio de 2022} disponible en: (https://cybersecurity.att.com/pricing).

cuales pueden ser utilizadas según la necesidad de implementación, reduciendo costos de acuerdo con el presupuesto de cada compañía.

A continuación, se presenta el análisis final de costos en el cual se incluyen los tres aspectos analizados en este capítulo:

Cuadro 10. Costo total aproximado de implementación del SOC utilizando herramientas licenciadas.

Rubro del gasto	**Costo total anual**
Gastos en personal	$273.000.000
Gasto en herramientas tipo hardware	$9.103.295
Gasto en herramienta tipo software	$130.196.376
Total	**$412.299.671**
Elaboración propia del autor.	

Tal como se presenta en la tabla 10, el costo total aproximado para la implementación de un SOC con 8 colaboradores y servicio de atención 7x24 es de $412.299.671 por año. Es importante tener en consideración que este costo puede ser disminuido si se opta por utilizar herramientas libres, lo que reduciría los gastos en un aproximado de 130 millones de pesos, lo que daría un total de gastos anuales cercanos a los $282.103.295

6. CONCLUSIONES

La información recopilada en este documento ha permitido no solo tener un acercamiento a la arquitectura base de un centro de operaciones de seguridad, sino también a su modelo de gestión y operación, identificando, desde la evaluación de centros de operaciones de seguridad ya implementados, que existen tres pilares fundamentales a la hora de implementar un SOC, estos son las personas, los procesos y las tecnologías, en los cuales se destacan respectivamente los analistas del SOC, los procesos de gestión de eventos e incidentes de seguridad y las herramientas tipo SIEM, cada uno de estos elementos constituye los principales de cada pilar, base fundamental para la implementación de un centro de operaciones de seguridad.

Como se expuso anteriormente, el pilar de las personas es crítico en la implementación de un centro de operaciones de seguridad y a la vez en la definición de su modelo de gestión, ITIL se encuentra como un referente a seguir para la definición de dicho modelo, no solo por las buenas prácticas en gestión de tecnología que incluye, sino que también propone dentro de su guía el apoyo a la adecuada gestión del talento humano (los analistas del SOC), desde el enfoque de la gestión del conocimiento, gestión del recurso humano y gestión de competencias. Al comparar este marco de referencia ITIL con la norma ISO/IEC 27001:2013, en lo que respecta a gestión de talento humano, es notable el enfoque que se da desde cada uno de los marcos de referencia, destacando a ITIL como uno más adecuado para la gestión de talento humano en servicios tecnológicos como lo es un SOC, principalmente por la facilidad de incluir en el modelo de gestión del SOC aspectos adicionales de ITIL que son relevantes para la implementación del servicio, como lo son la gestión de la capacidad y rendimiento, gestión de activos, gestión de despliegues y gestión de plataformas.

En el análisis de implementaciones de SOC se encontró como proceso principal de estos la gestión de eventos e incidentes de seguridad, razón por la cual se consideró fundamental incluir la gestión de este proceso en modelo de gestión principal del SOC; los marcos de referencia para la gestión de eventos e incidentes de seguridad comparados, NIST e ISO/IEC 27035, resultaron ser similares en cuanto las etapas o fases que incluye cada uno de ellos, sin embargo el enfoque más técnico de NIST lo pone por encima del enfoque procedimental de ISO para la gestión de eventos e incidentes que podría realizar un centro de operaciones de seguridad.

Según lo evaluado en el capítulo 5.1 de este documento, las tecnologías o herramientas principalmente usadas para la implementación de un centro de operaciones de seguridad incluyen los SIEM, sistemas IDS/IPS, herramientas de gestión de vulnerabilidades, Sandbox y herramientas de inteligencia de amenazas. Herramientas como el cuadrante mágico de Gartner presentan información de gran valor para la selección de líderes en cada una de las tecnologías en lo que a

tecnologías licenciadas se refiere, de esta manera se logró seleccionar herramientas como Splunk SIEM, CISCO NGIPS, Nessus, Falcon Sandbox y AlienVault USM. De la misma manera, el estudio referencial de fuentes de información tecnológica permite la selección de las principales herramientas libres para cada una de las categorías descritas como Wazuh, Suricata, OpenVAS, VirusTotal y Cisco Talos. Estas herramientas, tanto licenciadas como de uso libre, permiten la implementación de un centro de operaciones de seguridad que permita realizar el principal proceso encontrado para estos, la gestión de eventos e incidentes de seguridad de la información.

El análisis presupuestal realizado, el cual incluyó principalmente aquello concerniente al pilar de personas y tecnologías, mostró que existe una diferencia de aproximadamente 130 millones de pesos entre un camino de implementación del SOC y otro, el primero, utilizando herramientas licenciadas tendría un costo anual aproximado de COP $412.299.671; mientras que, en su versión con herramientas de uso libre, esta implementación podría reducir su costo anual a un total aproximado de COP $282.103.295. De manera contundente se encuentra que el principal gasto de implementación que podría tener un centro de operaciones de seguridad es el asociado a su pilar de personas el cual podría llegar a tener un valor cercano a los COP $273.000.000.

7. RECOMENDACIONES

El análisis realizado en este documento presenta un enfoque inicial para la implementación de un centro de operaciones de seguridad, sin embargo, se encuentra relevante que en estudios futuros relacionados al tema se incluyan análisis enfocados en el mantenimiento de un SOC, los ajustes asociados a los tres pilares del servicio, personas, procesos y tecnologías, así como a lo que se refiere a gastos económicos que podrían adicionarse o deducirse durante la operación.

El modelo de gestión propuesto para la implementación de un centro de operaciones de seguridad se basó en la gestión del pilar de personas y el proceso de gestión de eventos e incidentes, este análisis podría ampliarse en trabajos futuros, para incluir el estudio de un modelo de gestión más amplio, que cubra mayor cantidad de procesos e incluso la gestión de las herramientas tecnológicas.

En el escenario propuesto para la implementación de un centro de operaciones de seguridad, se definieron dos caminos a seguir en lo que respecta al pilar de las tecnologías, uno mediante el uso de herramientas licenciadas y otro mediante uso de herramientas de uso libre, estos no son los únicos caminos posibles en la implementación de un SOC, dependiendo de las necesidades y posibilidades de una compañía, se podría optar por elegir algunas herramientas de uso libre y otras licenciadas según sea de menor o mayor conveniencia para la organización. Este punto podría incluirse en un estudio futuro relacionado, el cual presente un análisis más avanzado de las posibles características que podrían cubrir o dejar de cubrir cada tipo de herramienta según su licenciamiento y soporte.

Dentro del análisis presupuestal realizado no se tuvieron en consideración gastos asociados a herramientas tecnológicas como routers, firewalls, equipos de red y servicios de conectividad necesarios para la operación del SOC, esto debido a que se consideró la implementación del mismo en un escenario que ya contara con dichos elementos, razón por la cual quienes se basen en esta guía de implementación deberán tener en cuenta la posibilidad de aparición de estos gastos dependiendo de las condiciones de arranque del proyecto de implementación.

BIBLIOGRAFÍA

A2SECURE. “Herramientas para la gestión y análisis de Vulnerabilidades”. {En línea}. {13 de mayo de 2022} disponible en: (https://www.a2secure.com/blog/herramientas-para-la-gestion-y-analisis-de-vulnerabilidades/).

AGYEPONG, Enoch. CHERDANTSEVA, Yulia. REINECKE, Phillip. BURNAP, Pete. Towards a Framework for Measuring the Performance of a Security Operations Center Analyst. En: International Conference on Cyber Security and Protection of Digital Services (2020); pp. 1-8

AT&T. “USM Pricing”. {En línea}. {23 de junio de 2022} disponible en: (https://cybersecurity.att.com/pricing).

BAKER, Kurt. “What is cyber threat intelligence?”. {En línea}. {23 de junio de 2022} disponible en: (https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/)

BIGGERI HERNAN, Patricio. Centro de operaciones de seguridad. Estrategia, diseño y gestión. Buenos Aires, 2018, pp 34-69. Trabajo de grado (Maestría en Gestión Estratégica de Sistemas y Tecnologías de la Información). Facultad de Ciencias Económicas.

BMC. “ITIL & ITSM Roles and Responsibilities”. {En línea}. {14 de mayo de 2022} disponible en: (https://www.bmc.com/blogs/itil-itsm-roles-responsibilities/#:~:text=In%20fact%2C%20the%204%20Ps%20of%20ITIL%20%C2%AE,quality%20IT%20services%20to%20users%20and%20customer%20alike).

BONILLA BLANCO, Billy Mauricio. ROJAS PATERNINA, Anthony. Diseño y planificación de un centro de operaciones de seguridad informática aplicado como servicio por la organización A3SEC bajo marcos de trabajo propuestos por SANS, ISACA Y NIST. Bogotá, 2019. pp 70 -100. Trabajo de grado (Especialista en Seguridad Informática). Universidad Piloto de Colombia. Facultad de Ingeniería.

CCIT. “Cifras de ciberseguridad en Colombia prenden alarmas al cierre del 2020”. {En línea}. {14 de mayo de 2022} disponible en: (https://www.ccit.org.co/noticias/cifras-de-ciberseguridad-en-colombia-prenden-alarmas-al-cierre-del-2020/).

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1273 de 2009. Diario Oficial No. 47.223 de 5 de enero de 2009, 2015). Bogotá. 2015.

COMPTIA. “What Is a Security Operations Center?”. {En línea}. {5 de febrero de 2022} disponible en: (https://www.comptia.org/content/articles/what-is-a-security-operations-center).

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL REPÚBLICA DE COLOMBIA DEPARTAMENTO NACIONAL DE PLANEACIÓN. Lineamientos de política para ciberseguridad y ciberdefensa. Bogotá. DNP. 2011.

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL REPÚBLICA DE COLOMBIA DEPARTAMENTO NACIONAL DE PLANEACIÓN. Política nacional de seguridad digital. Bogotá. DNP. 2016.

CYBERSECURITYPRICING. “Crowdstrike Pricing”. {En línea}. {23 de junio de 2022} disponible en: (https://cybersecuritypricing.org/tag/crowdstrike-pricing/).

CUELLAR RODRIGUEZ, Jorge. POMPEYO, Daniel. Diseño del esquema de implementación de un centro de operaciones de seguridad (SOC) de la información en la empresa KPMG en la sede de Bogotá D.C. – Colombia. Bogotá, 2021. pp 35 – 89. Proyecto de grado (Especialista en Seguridad Informática). Universidad Piloto De Colombia. Facultad de ingeniería.

DNSSTUFF. “10 Best Free and Open-Source SIEM Tools”. {En línea}. {18 de junio de 2022} disponible en: (https://www.dnsstuff.com/free-siem-tools).

DOLARHOY. “Precio del dólar en el año 2021”. {En línea}. {23 de junio de 2022} disponible en: (https://www.dolarhoy.co/ano/2021).

EXABEAM. “Cuadrante mágico de gartner para SIEM”. {En línea}. {21 de junio de 2022} disponible en: (https://www.exabeam.com/wp-content/uploads/GartnerMQ-2021-Figure1-2.png)

FIRST. “FIRST Members around the world”. {En línea}. {4 de junio de 2022} disponible en: (https://www.first.org/members/map).

GARTNER. “Gartner Magic Quadrant for Intrusion Detection and Prevention Systems”. {En línea}. {15 de junio de 2022} disponible en: (https://www.gartner.com/en/documents/3844163/magic-quadrant-for-intrusion-detection-and-prevention-sy).

GAST, Kelsey. “What is SIEM? And How Does It Work?”. {En línea}. {15 de abril de 2022} disponible en: (https://logrhythm.com/what-is-siem/).

HIBERUS. “ITIL® 4, todas las novedades de ITIL en 2019”. {En línea}. {15 de abril de 2022} disponible en: (https://www.hiberus.com/crecemos-contigo/novedades-itil-v4/).

HOYOS BUITRON, Victor Antonio. ¿Qué tal esta Colombia en cuestión de Ciberseguridad?. Bogotá, 2015. pp 10-15. Proyecto de grado (Especialización En Administración De La Seguridad). Universidad Militar Nueva Granada. Facultad De Relaciones Internacionales, Estrategia Y Seguridad.

HYSOLATE. “Sandboxing Security: A Practical Guide”. {En línea}. {21 de junio de 2022} disponible en: (https://www.hysolate.com/learn/sandboxing/sandboxing-security-a-practical-guide/).

INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Técnicas de seguridad. Gestión de incidentes de seguridad de la información. Bogotá. ICONTECT. 2012.

INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. Bogotá. ICONTEC. 2013.

INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Visión general y vocabulario. Bogotá. ICONTEC. 2017.

INCIBE. “Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?”. {En línea}. {15 de abril de 2022} disponible en: (https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian).

INCIBE. “Gestión de logs: Políticas de seguridad para la Pyme”. {En línea}. {15 de abril de 2022} disponible en: (https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/gestion-logs.pdf).

INTERPOL. “Ciberdelincuencia: Efector de la COVID-19”. {En línea}. {3 de febrero de 2022} disponible en: (https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19).

JACOBS, Pierre. ARNAB, Alapan. IRWIN, Barry. Classification of Security Operation Centers. En: Information Security for South Africa, 2013, pp 1-7.

JÁNOS, Fecher David. PHUOC DAI, Nguyen. Security concerns towards Security Operations centers. En: IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI), vol 12, 2018, pp. 273-278.

KEARY, Tim. “Comparitech. IDS vs IPS”. {En línea}. {15 de abril de 2022} disponible en: (https://www.comparitech.com/net-admin/ids-vs-ips/).

KNOWLEDGEHUT. “ITIL®4 Management Practices”. {En línea}. {21 de mayo de 2022} disponible en: (https://www.knowledgehut.com/tutorials/itil4-tutorial/itil-management-practices-processes).

MILOSLAVSKAYA, Natalia. Security Operations Centers for Information Security Incident Management. En: IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), vol 4, 2016, pp. 131-136.

MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES DE COLOMBIA. Guía para la Gestión y Clasificación de activos de Información. Bogotá. MINTIC. 2016.

MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES DE COLOMBIA. Guía de gestión de riesgos. Bogotá. MINTIC. 2016.

MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES DE COLOMBIA. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Bogotá. MINTIC. 2016.

MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES DE COLOMBIA. Modelo de Seguridad y Privacidad de la Información. Bogotá. MINTIC. 2021.

MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES DE COLOMBIA. Seguridad en la Nube. Bogotá. MINTIC. 2016.

MUNIZ, Joseph. MCINTYRE, Gary. ALFARDAN, Nadhem. Security Operations Center: Building, Operating, and Maintaining Your Soc. Hoboken: Cisco Press, 2015, pp 45 – 60.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Computer Security Incident Handling Guide. NIST Special Publication 800-61 (Revision 2). Washington D.C. NIST. 2012.

NESSUS. “Nessus Professional Price”. {En línea}. {7 de junio de 2022} disponible en: (https://es-la.tenable.com/products/nessus/nessus-professional)

PINZÓN, Iralda. Gestión del riesgo en Seguridad Informática. Bogotá, 2018. pp 3 – 5. Trabajo de grado (Especialista en Seguridad Informática). Universidad Piloto De Colombia. Facultad de ingeniería.

REPUBLICA DE COLOMBIA. (2022). Código Sustantivo del Trabajo. Decreto 2663 de 1950. Diario Oficial No. 51945. Bogotá. 1951.

SEN Kaushik. “Top 6 Free Network Intrusion Detection Systems (NIDS) Software in 2022”. {En línea}. {2 de junio de 2022} disponible en: (https://www.upguard.com/blog/top-free-network-based-intrusion-detection-systems-ids-for-the-enterprise).

SEMANA. “Colombia ocupó el tercer lugar en el ‘ranking’ de cibercrimen en América Latina”. {En línea}. {23 de febrero de 2022} disponible en: (https://www.semana.com/tecnologia/articulo/colombia-ocupo-el-tercer-lugar-en-el-ranking-de-cibercrimen-en-america-latina/202117/).

SPLUNK. “What is a SIEM?”. {En línea}. {6 de marzo de 2022} disponible en: (https://www.splunk.com/en_us/data-insider/what-is-siem.html).

SPLUNK. “Splunk Pricing”. {En línea}. {8 de junio de 2022} disponible en: (https://www.splunk.com/en_us/software/pricing.html).

SUPER INTENDENCIA FINANCIERA DE COLOMBIA. Circular Externa 007 de 2018. Bogotá. SFC. 2018.

SUPER INTENDENCIA FINANCIERA DE COLOMBIA. Circular Externa 008 de 2018. Bogotá. SFC. 2018.

SZARVÁK, Aniko. PÓSER, Valeria. Review of using Open Source Software for SOC for education purposes – a case study. EN: IEEE 25th International Conference on Intelligent Engineering Systems (INES), vol 25, 2012, pp 209-214.

TECNÓSFERA. “El cibercrimen no descansa, estas son las proyecciones para el 2020”. {En línea}. {6 de marzo de 2022} disponible en: (https://www.eltiempo.com/tecnosfera/dispositivos/cifras-de-ciberataques-de-2019-y-tendencias-para-el-2020-435508).

VEERAPPA, Babbu. “Security Operations Centre (SOC) in Utility Organizations”. {En línea}. {6 de marzo de 2022} disponible en: (https://sansorg.egnyte.com/dl/gtxpv0pW5T/?).

VIELBERTH, Manfred. BOHM, Fabian. FICHTINGER, Ines. PERNUL, Gunter. Security Operations Center: A Systematic Study and Open Challenges. En: IEEE Access, vol. 8, 2020, pp. 227756-227779.

ANEXOS

Enlaces a video de presentación del trabajo de grado:

Opción 1: https://youtu.be/7ZBMiFla_4Y

Opción 2: https://unadvirtualedu.sharepoint.com/:v:/s/TrabajodeGrado-SebastinCaballero/EXiskoZ34ipLimtDB_N6EDAB_9FWnmtVZ9MwqdrlA5Yluw?e=iptm4j