UNIVERSIDAD DON BOSCO
VICERRECTORÍA ACADÉMICA
FACULTAD DE INGENIERÍA

TRABAJO DE GRADUACIÓN PARA OPTAR AL GRADO DE:
Maestro(a) en Seguridad y Gestión de Riesgos Informáticos

PROYECTO:

Guía de aplicación para el monitoreo de ciberseguridad con herramientas de código abierto.

PRESENTADO POR
Inga. Wendy Carolina Criollo Hernández
Ing. Mario Aarón López Payés
Lic. José Ismael Yánez Acosta

ASESOR
Mg. René Arturo Angulo Arriaza

Antiguo Cuscatlán, La Libertad, El Salvador,
Centro América
2021

Contenido

Listado de Tablas y Figuras

1. Introducción

Con la presencia de la pandemia, se evidenció que el uso de las tecnologías es de suma importancia para la continuidad del negocio y operaciones que por tradición se habían ejecutado de forma presencial; y si lo bueno se acopla al ambiente digital, ¿Por qué no las malas prácticas?, tales como la estafa, robo y secuestro del activo más valioso de toda organización, “La información”.

En la que ahora muchos denominan nueva realidad, no debemos dejar de lado la seguridad de la información y se debe apostar a la creación de unidades encargadas al tratamiento de ello, debemos prestar vital atención a temas de ciberseguridad y no dejar que los incidentes que muchos ven lejanos pasen factura a la economía y reputación del negocio.

La presente guía busca proveer un marco de trabajo para el diseño, implementación y mejora de un Centro de Operaciones de ciberseguridad, en el cual este último provea a la organización sin importar el rubro, información oportuna del análisis de incidentes para para la toma de acciones preventivas y correctivas que puedan afectar las operaciones del negocio.

Tratándose además la presente guía de una solución de costo asequible y bajo la recomendación de herramientas de código abierto, se provee un conjunto de buenas prácticas, para que la implementación y mantenimiento del CSOC no sean vea limitado por el déficit presupuestario que las organizaciones presenten y/o el personal designado en el aseguramiento de la información.

2. Objetivo General y Específicos

2.1 Objetivo general

- Desarrollar una guía de aplicación para el monitoreo de ciberseguridad con herramientas de código abierto.

2.2 Objetivos específicos

- Definir marco de trabajo para el diseño, implementación, monitoreo y mejora de un CSOC.
- Establecer buenas prácticas para CSOC efectivos.
- Determinar la forma de utilizar herramientas de código abierto que apoyen las operaciones de un CSOC.

3. Metodología de trabajo

Para la creación de la guía de aplicación para el monitoreo de ciberseguridad con herramientas de código abierto, por lo cual se realizó investigación documental para identificar la terminología básica, componentes y herramientas de un centro de operaciones de ciberseguridad.

Los pasos seguidos para la construcción de la guía propuesta contemplaron:

i. La identificación de una problemática en el país a la cual aportar una solución de conocimiento propio.
ii. Definición del tema que daría soporte a la problemática a resolver.
iii. Delimitación de los objetivos, alcances y justificación relacionadas al tema definido.
iv. Elaboración de contenido temático de la investigación documental.
v. Recopilación de fuentes de información asociadas a la temática definidas en el paso anterior.
vi. Redacción del Estado del Arte.
vii. Elaboración del contenido temático de la guía de aplicación.
    a. Se definieron las secciones y los pasos a seguir para la implementación de un Centro de operaciones de Ciberseguridad con herramientas de código abierto.
    b. Se definió la estructura para la descripción de pasos de la guía de aplicación.
viii. Construcción de la metodología propuesta para la guía de aplicación
ix. Construcción de la guía de aplicación
    a. Se elaboraron los esquemas que ilustran la interacción de los pasos de la metodología.
    b. Se describieron los pasos de la guía de aplicación, elaborando los anexos necesarios para el seguimiento de dichos pasos.

4. Marco Conceptual

4.1 Centro de Operaciones de Ciberseguridad

Un Centro de Operaciones de Ciberseguridad (del inglés Cyber Security Operation Center, y en adelante CSOC) se define como una instalación desarrollada de manera centralizada donde se orquestan personas, procesos y tecnología para dotar a las organizaciones de capacidades de monitoreo continuo de las actividades cibernéticas en el contexto de operación para prevenir, detectar, escalar y recuperarse de incidentes de ciberseguridad; y así, finalmente asegurar la confidencialidad, integridad y disponibilidad de los activos de información (Alahmadi, 2019) (Majid & Zainol Ariff, 2019).

Alahmadi provee un ejemplo de una estructura típica de un CSOC donde se manifiesta la interrelación de las tres dimensiones involucradas. En esta estructura (Figura 1), al detectarse eventos de interés que pudieran evidenciar una amenaza en la red que se está protegiendo, los dispositivos afectados notifican tales eventos. Estas notificaciones son recolectadas y correlacionadas por el SIEM, el cuál emite alarmas que son verificadas por analistas de ciberseguridad y escaladas a gestores de incidentes si lo ameritan, quienes, junto a los propietarios de los sistemas involucrados, den una respuesta a la situación. Estos incidentes y otras posibles debilidades de la seguridad y los sistemas son, al final, reportadas a las partes interesadas, internas o externas, del negocio.

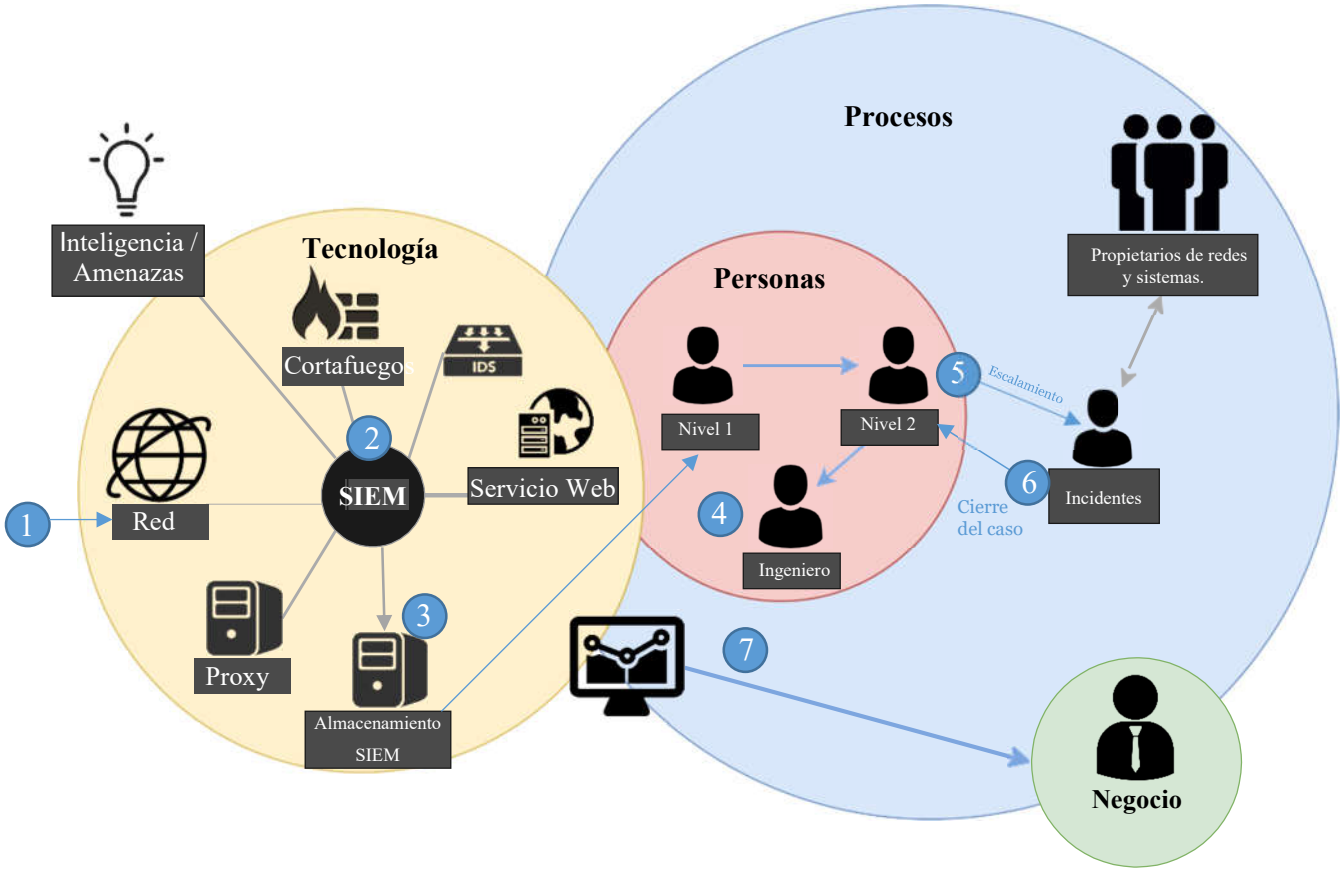

Figura 1. Tecnología, personas y procesos de un CSOC. Tomado de (Alahmadi, 2019). El proceso descrito inicia con un evento que se detecta en la una herramienta de red (1), se reciben los registros en el SIEM (2), se almacenan los registros correlacionados y se emite alerta al personal indicado (3), El personal atiende la incidencia (4), escalándola de ser necesaria (5), para resolver el incidente y dar por cerrado el caso (6). El negocio constantemente se encuentra consultado y verificando el comportamiento de incidentes en la organización (7)

4.2 Generaciones de CSOC

Las necesidades que, a lo largo de tiempo, se han tenido que enfrentar en el área de la ciberseguridad debido a la continua transformación de las amenazas informáticas, han impulsado mayores y mejores capacidades para la protección de la información de forma muy marcada, de modo que, los CSOC pueden clasificarse en una serie de generaciones que inician desde el nacimiento de Internet en la década de los 70. Hacia el año 2013, HP ESP Security Intelligence and Operations Consulting Services (2013) describía cinco generaciones de CSOC; sin embargo,

con el continuo avance tecnológico, hoy en día, podemos considerar una sexta generación, tal como lo detallan Cyber Intelligence Agency Bostwana (2016) y Compris Technologies AG (2021). Estas generaciones son:

- La primera generación (1975 – 1995): Se le conoce como la generación uno o G1-SOC y se caracterizaba realizar una recolección parcial de registros, defenderse de código malicioso de mínimo impacto y contar con un recurso humano poco especializado.
- La segunda generación (1976 – 2001): Conocida como generación dos o G2-SOC, se enfocaba en la detección de los intrusos y de los primeros brotes de malware, los cuales incluían virus y gusanos, que generaron gran impacto en las redes de grandes empresas y entidades gubernamentales. Se hablaba entonces de una de recolección exhaustiva de registros de red, dispositivos y sistemas; gestión de casos; y, correlación de eventos.
- Tercera generación (2001 – 2006): En este período, los delitos informáticos estaban en expansión. En el año 2003, aparecieron las primeras botnets que se usaban para el robo de identidades e información financiera, y donde los atacantes percibían grandes ganancias monetarias como producto de realizar estas actividades. Esta generación se caracterizó por contar con unos centros de ciberseguridad más maduros que ya consideraban la gestión de vulnerabilidades y se tenía mayor capacidad de respuesta ante incidentes. En el caso de los de centros de operaciones de ciberseguridad en las industrias privadas, se enfocaban también por apoyar el cumplimiento de marcos normativos como, por ejemplo, el de la industria de tarjetas de crédito, donde las emisoras de tarjetas de créditos exigieron a sus proveedores y socios de negocio adherirse a normas de seguridad y de protección de datos específicas.

- Cuarta generación (2007 – 2012): En esta época, el panorama sobre la seguridad informática dio un giro y cambio su foco de atención de la detección y prevención de intrusos a la detección de exfiltración y contención motivado por la aparición del hacktivismo, la ciberguerra, la aparición de las primeras amenazas avanzadas persistentes (del inglés Advance Persistent Threats o APTs) y la exfiltración de datos. Se enfatizó la investigación sistemática de incidentes de seguridad y de una correlación de datos exhaustivo.
- Quinta generación (2013 – 2015): Los CSOC de esta generación se vieron forzados a evolucionar dadas las amenazas cibernéticas que en este período mostraron también un ritmo elevado de evolución. Los productos y soluciones de seguridad comenzaron a implementar características de Machine Learning y el factor humano paso a jugar un papel activo en la detección de amenazas e intrusos.
- Sexta generación (2016 – a la fecha): Los centros de operaciones de ciberseguridad del futuro deben ser capaces de utilizar Big Data, Inteligencia Artificial y Machine Learning. Estos Next G-SOC deben enfocarse en la automatización y realizar funciones de Cyber Intelligence, Insider Threat, Red Team, Hunters, Cyber Innovation y Outreach. Esta generación de CSOC se adaptan de manera constante para enfrentar los retos y desafíos tanto del presente como del futuro.

4.3 Tipos de CSOC

Los CSOC también pueden ser clasificados considerando características como la capacidad de contraataque, escenarios de despliegue, propósito, técnicas de correlación, variantes de implementación y tenencia de estos. La Tabla 1 propuesta por (Miloslavskaya, 2016), recoge varios tipos de CSOC.

Tabla 1. Clasificación de los Centro de Operaciones de Ciberseguridad.

Característica	***Tipo***	***Descripción***
Capacidad de contraataque o neutralización	CSOC sin capacidad de contraataque	El CSOC actúa como un clásico sistema de detección de intrusiones (del inglés Intrusion Detection System o IDS): monitorea y prioriza eventos relacionados a la seguridad de la información. En caso de que se detecte un ataque, no se ejecutan acciones en respuesta. Estos CSOC se utilizan generalmente en entornos con altas demandas de disponibilidad (por ejemplo, en la banca o la medicina) porque los falsos positivos no conducen a la creación de nuevas reglas de seguridad ni al bloqueo de servicios. Los objetivos principales de este tipo de CSOC son: el procesamiento de datos de eventos de seguridad, la visualización y la priorización de eventos de seguridad, y el cumplimiento normativo.
	CSOC reactivo	El CSOC utiliza el concepto de un sistema de prevención de intrusiones (del inglés Intrusion Prevention System o IPS): el ataque no solo es detectado, sino que también se realizan funciones de mitigación para detener la propagación del ataque. El CSOC identifica todos los componentes del ataque, incluyendo las direcciones de los sistemas infractores y los comprometidos. Su capacidad de auto mitigación identifica los dispositivos con capacidad de realizar acciones sobre la ruta de ataque y proporciona los comandos adecuados que pueden emplearse para mitigar el riesgo. Los resultados se pueden utilizar de forma precisa y rápida para prevenir o contener el ataque. Este tipo de CSOC se utiliza

Característica	*Tipo*	*Descripción*
		comúnmente en entornos con alta demanda de confidencialidad. Su capacidad de responder de forma rápida y automática ante las amenazas es su ventaja clave.
Escenarios de despliegue	Centralizado	El CSOC está basado en un dispositivo o servidor dedicado que realiza todas las actividades relacionadas con la gestión de la seguridad de la información. Ventajas: Velocidad, facilidad de instalación, y costo relativamente bajo. Desventaja: Es apropiado solo para entornos pequeños o medianos.
	Distribuido	El CSOC utiliza varios dispositivos/servidores al mismo tiempo que realiza un equilibrio de carga entre ellos. La distribución de esta carga puede basarse en un principio geográfico (diferentes servidores son responsables de diferentes partes de la red) o en un principio funcional (parte de las funciones las realiza un servidor y otra parte las realiza otro). Debido a que se utilizan varios dispositivos, el costo del CSOC es mayor y el despliegue y el mantenimiento es más complejo, este equilibrio de carga da como resultado un mejor rendimiento y efectividad en general.
Objetivo o finalidad	Controlado	El CSOC permite observar el nivel de protección de los objetos de seguridad informática y pronosticar su cambio.
	Administrado	El CSOC ayuda a operar activamente los objetos de seguridad de la información.

Característica	*Tipo*	*Descripción*
	Crisis	El CSOC solo comienza a actuar durante las crisis.
Técnicas de correlación	Estadístico	El CSOC aplica algoritmos estadísticos para determinar la severidad de incidentes de seguridad informática y, entonces asignar una puntuación de amenaza en función del valor de los activos. Analiza el comportamiento de la red e identifica amenazas basadas en la presencia y probable severidad de los patrones de eventos anómalos. También permite medir la efectividad, dado que la cantidad de eventos anómalos deberían disminuir con el tiempo a medida que el entorno de la infraestructura se vuelve más seguro.
	Basado en reglas	El CSOC utiliza reglas predefinidas que aplican lógica condicional para identificar posibles escenarios de ataque mediante la observación de una serie especifica de eventos en un intervalo especifico dado. Las reglas pueden ser entregadas listas para usar por un proveedor o implementadas de manera personalizada después de un análisis cuidadoso del tráfico de red. Esta correlación es extremadamente eficaz para identificar amenazas en función del conocimiento previo de patrones de ataque. Muchos productos implementan un conjunto finito de reglas que cubren escenarios comunes y estos pueden ampliarse con reglas personalizadas. La correlación efectiva depende del soporte del proveedor para mantener el estado de las reglas. Una regla debe ser un evento de larga duración y el motor de las reglas debe mantener los eventos

Característica	*Tipo*	*Descripción*
		en estado durante un período de tiempo razonable hasta que otros eventos de calificación activen una alerta o la regla expire para el evento inicial. Sin esto, se experimentarán numerosos falsos positivos, o lo que es más importante, no se identificarán ataques lentos y bajos que se caracterizan por una pequeña cantidad de eventos diarios durante un largo período de tiempo. Entre los inconvenientes se encuentran el tiempo que supone mantener actualizados cientos de reglas, demasiados falsos positivos y falsos negativos ante técnicas de ataque innovadoras.
	Vulnerabilidad	El CSOC toma los datos de los eventos de seguridad de los IDS de la red y los correlaciona contra una base de datos de vulnerabilidades conocidas y los perfiles de vulnerabilidades de los equipos devueltos por un escáner de vulnerabilidades, para determinar una puntuación de cada activo. Esto, ayuda a eliminar los falsos positivos y ayuda al equipo de seguridad a determinar cuáles ataques son reales y qué activos son realmente vulnerables. Ventajas: la más efectiva para detectar escenarios de ataque específicos, incluidos aquellos escenarios que pueden ser nuevos para la infraestructura, y extremadamente buena para eliminar falsos positivos y maximizar la eficiencia al enfocarse en eventos de seguridad reales que corresponden a vulnerabilidades verdaderas. Desventajas: la creación de reglas para correlacionar ataques que explotan

Característica	*Tipo*	*Descripción*
		vulnerabilidades particulares de activos susceptibles es una tarea extremadamente laboriosa.
	Acuerdo de nivel de servicio (del inglés Service Level Agreement o SLA)	El CSOC vincula los eventos de seguridad a los requisitos establecidos en un SLA y es muy importante para las empresas porque ayuda a evaluar las pérdidas de los elementos de red comprometidos o los componentes que están fuera de servicio. El CSOC produce modelos de procesos de negocio y analiza el impacto en estos procesos desde diferentes incidentes de seguridad. Desventaja: La principal dificultad es la composición de procesos de negocio y la determinación del costo de los activos (las dificultades que son naturales para el análisis de riesgos orientado a procesos de tecnologías de información).
	Cumplimiento	El CSOC vincula los eventos de seguridad de la información a leyes, políticas y estándares de seguridad existentes (tanto corporativos como regulatorios). Necesita una instalación y configuración especial porque solo es posible una vinculación estática dado que cada infraestructura tiene su propia política de seguridad.
	Mixto	Cuando todos los tipos de correlación se aplican juntos, pueden mejorar enormemente la detección de ataques reales y la eficacia de la gestión de seguridad de la información. Cuando el personal de seguridad puede obtener un perfil de riesgo unificado de eventos basado en una puntuación de amenaza

Característica	*Tipo*	*Descripción*
		estadística, alertas basadas en reglas, vulnerabilidades asociadas, y el valor de los activos, su trabajo es mucho más fácil.
	CSOC sin correlación	Apropiado para redes pequeñas donde solo se realiza agregación de datos de los eventos de seguridad y todas las decisiones las toma el equipo de seguridad.
Variantes de implementación	Software	El CSOC se basa en software especializado instalado en uno o más servidores. Ventaja: La posibilidad de utilizar los servidores que forman parte del CSOC para tareas adicionales.
	Hardware	El CSOC es una solución lista para usar y basado en uno o varios servidores con software preinstalado. Ventaja: Menor tiempo de implementación. Desventaja: Dado que tiene un entorno aislado no puede instalarse software adicional en los servidores del CSOC.
	Solución de infraestructura	El CSOC es construido utilizando software y hardware existente (por ejemplo, una base de datos existente es utilizada para el almacenamiento de eventos de seguridad de la información; la consolidación de bases de datos de seguridad se implementa mediante técnicas de replicación; y las funcionalidades de normalización, agregación y correlación se implementan dentro de la base de datos mediante scripts SQL; etc.). Ventajas: bajo costo relativo de la solución y mayor flexibilidad. Desventajas: La necesidad de desarrollar el CSOC incluyen

Característica	*Tipo*	*Descripción*
		la normalización, agregación y reglas de correlación y programación SQL para implementar esas reglas.
Propiedad o tenencia	Interno	Ventajas: El conocimiento de la infraestructura es mayor que cuando se subcontrata, más efectivo, las soluciones son más fáciles de personalizar, mayor probabilidad de identificar correlaciones entre los componentes de la infraestructura, mejores precios de las herramientas. Desventajas: Grandes inversiones iniciales, necesidad de mostrar eficacia rápidamente, alto potencial de un conflicto de interés en el equipo de monitoreo de intrusiones, menor probabilidad de reconocer patrones a gran escala como lo hacen terceras partes especializadas con muchos años de experiencia.
	Subcontratado	Ventajas: Sin gastos de capital, a menudo más barato, menor potencial para un conflicto de intereses en el equipo de monitoreo de intrusiones, imparcial, y con acuerdos de niveles de servicio. Desventajas: Menor conocimiento de la infraestructura; disminución en vigilancia del personal, riesgo de mal manejo de datos externos; ninguna ganancia a largo plazo para la infraestructura.

4.4 Componentes

Tal como lo plantea Morillas & Raggi (2019), los módulos, procesos y actores, son pilares fundamentales en la creación de un CSOC, es por ello que en las secciones 4.4.1, 0 y 4.4.3 se profundizará sobre dichos componentes, sin dejar de lado, la descripción de algunas herramientas de utilidad para puesta en marcha de un Centro de Operaciones de Ciberseguridad (ver sección 4.4.4)

4.4.1 Módulos

En el año 2013, de acuerdo con IBM Corporation (2013), en su documento "Strategy considerations for building a security operations center", se reconocían como esenciales en un CSOC Empresarial funcionalidades o módulos como:

1. Monitoreo de amenazas de ciberseguridad: Su función es identificar y determinar en donde es posible la seguridad de una organización, para posteriormente identificar, correlacionar y priorizar amenazas.

   Este módulo requiere la incorporación de un SIEM, para la obtención de los registros de los dispositivos de seguridad pertenecientes a la infraestructura tecnológica que permitan la detección de amenazas.

2. Gestión de incidentes de ciberseguridad: Esta función abarca actividades de priorización de incidentes y escalamiento de incidentes basados en niveles de gravedad (Gravedad nivel 1,2,3); Establecimiento de procesos de notificación (A quien informar y cuando), Asignación de incidentes, considerando la antigüedad de ellos, Definir y hacer cumplir los niveles de servicios, Evaluar el desempeño del personal por medio del desarrollo de métricas.

3. Reclutamiento, retención y gestión de personal: en esta función recae la decisión de contratar personas ad-hoc a los roles dentro de un CSOC, y es que escoger personas competentes al cargo que se busca, permite a las organizaciones ahorrar tiempo y dinero, ya que se dan soluciones oportunas a los incidentes reportados.
4. Desarrollo, gestión y optimización de procesos: esta función permite establecer el orden. Metodología, para la resolución de incidente, indicando una cantidad de procesos por área para el funcionamiento de un CSOC[1].
5. Creación de estrategias de amenazas emergentes: dicha función busca la identificación constante de datos críticos, para generar políticas que apoyen a las estrategias de crecimiento del negocio, sin dejar de lado la designación de recurso económico para tecnología y servicios que apoyen a la ciberseguridad de la organización. Se deben definir métricas para la presentación de informes que midan la efectividad de los mecanismos de seguridad de la información que las estrategias han apoyado.

Para Antón Zambrano y Ariel (2020), ingenieros de telecomunicaciones de la Universidad de Guayaquil, un CSOC, debe poseer funciones encaminadas a: 1) Monitoreo continuo del comportamiento de la organización, 2) Registro de todas las actividades de comunicación de la organización, 3) Clasificación de la gravedad de las alertas, 4) Desarrollo y evolución de la defensa, 5) Recuperación ante incidentes.

4.4.2 Funciones y Procesos

El CSOC, al igual que cualquier otra unidad dentro de la estructura organizacional, debe tener funciones bien definidas que le permitan llevar a buen término la especializada tarea

[1] Funciones y Procesos 4.4.2

de asegurar el entorno o contexto en que se desenvuelve la organización; no obstante, a pesar de que en la literatura consultada se identifican fácilmente una serie de funciones, no hay un consenso en el número y alcance de estas. La Tabla 2 muestra una comparación entre las propuestas de diversos autores.

Tabla 2. Funciones del CSOC según diversos autores.

(Agyepong, Cherdantseva, Reinecke, & Burnap, 2020)	***(Schinagl, Schoon, & Paans, 2015)***	***(Onwubiko, 2015)***
• Monitoreo y detección • Análisis • Respuesta e informe • Inteligencia • Gestión de incidentes • Línea base y vulnerabilidades • Gestión de políticas y firmas • Cumplimiento y gestión del riesgo • Ejecución de pruebas de penetración • Forense y malware • Ingeniería y recolección de bitácoras	• Inteligencia • Línea base de seguridad • Monitoreo • Ejecución de pruebas de penetración • Forense	• Recolección • Análisis • Respuesta y forense

Como se observa, cada autor presenta con mayor o menor especificidad las funciones de un CSOC. Con el propósito de comprender con mayor detalle estas funciones, se presentan las descritas por Agyepong et al (2020):

- ✓ Monitoreo y detección: Esta función implica el monitoreo de sistemas de red computacionales, dispositivos y aplicaciones ejecutándose en estos dispositivos con el propósito de detectar cualquier actividad maliciosa o anormal.
- ✓ Análisis: Esta función implica una investigación a profundidad de las actividades anormales e inusuales observadas en la red de la organización.
- ✓ Respuesta e Informe: Implica la ejecución de acciones específicas según lo exijan los procesos de trabajo locales para mitigar o reducir el daño potencial de una amenaza identificada. Un punto importante es que la respuesta implica la generación de reportes tanto técnicos como no técnicos para las partes interesadas afectadas por los incidentes.
- ✓ Inteligencia: Implica la obtención de información sobre indicadores de compromiso (del inglés Indicators of Compromise, IOCs) de terceras partes o de fuentes abiertas con la finalidad de detectar actividades maliciosas.
- ✓ Gestión de Incidentes: Se refiere a la capacidad de preparar, identificar, y escalar un incidente. A esto le acompaña, la capacidad de formular un plan de contención y erradicación como parte de esta función.
- ✓ Línea base y vulnerabilidades: Requiere las actividades de aplicación de parches y reforzamiento de la seguridad en los sistemas computacionales con el fin de abordar cualquier debilidad conocida. La ejecución de escaneo de vulnerabilidades es una actividad esencial para el cumplimiento de esta función.

- ✓ Gestión de políticas y firmas: Se persigue mantener actualizadas las políticas y firmas de las herramientas técnicas utilizadas para detectar, prevenir y enfrentar ciberataques.
- ✓ Cumplimiento y gestión del riesgo: mediante esta función, el CSOC apoya el cumplimiento de requisitos obligatorios, industriales o reglamentarios relacionados a la naturaleza de las operaciones del negocio.
- ✓ Ejecución de pruebas de penetración: Involucra la simulación de ataques cibernéticos contra los sistemas de red computacionales de la organización para probar la defensa implementada y la reacción bajo ataque.
- ✓ Forense y malware: Se relaciona a la obtención y preservación de evidencia relacionada a actividades maliciosas.
- ✓ Ingeniería y recolección de bitácoras: La recopilación de registros proporciona un lugar centralizado para agregar todos los eventos de seguridad y la actividad transaccional.

Los procesos que cada organización adopta para el cumplimento de las funciones del Centro de Operaciones de Ciberseguridad varían de acuerdo al alcance que ellas tengan sobre las funciones. Es por ello por lo que para abordar los procesos que un CSOC puede poseer, en la Figura 2 indicamos los procesos preexistentes en CSOC comerciales como el que ofrece la empresa IBM.

Proceso analítico para la detección y solucionar problemas de seguridad

- Metodología de clasificación de incidentes
- Detección de incidentes y plazos analíticos para tomar medidas.
- Proceso de escalada de incidentes y seguimiento
- Ticketing para ayudar a garantizar que los incidentes conduzcan a análisis yremediacion
- Proceso para evaluar nuevas amenazas
- Proceso para escribir y probar nuevas reglas de detección
- Procesos forenses

Proceso comercial para la administración y deberes de gestión

- Retención de registros
- Uso inaceptable
- Comunicaciones internas y divulgación pública
- Proceso de cambio de política y verificación, incluidos cambios en dispositivos de puerta de enlace y cómo se revisan esas configuraciones
- El proceso de actualización de contenido y los casos de uso se actualizan
- Elaboración de informes e informes de métricas

Proceso operativo del día a dia

- Reclutamiento, retención, promoción y rotación de empleados
- Incorporación de nuevos empleados
- Capacitación en conciencia de seguridad de la empresa
- Formación de los empleado

Procesos técnológicos para la admisnitración de Sistemas, mantenimiento y gestión.

- Proceso de parche
- Proceso de actualización de firmware y actualizaciones de software
- Acceso a los procesos del dispositivo y de la estación de administración
- Proceso de implementación de nuevas tecnologías
- Proceso de verificación de estado
- Proceso de análisis y reparación de vulnerabilidades

Figura 2 Proceso analítico para la detección y solucionar problemas de seguridad. Retomado de "*Strategy considerations for building a security operations center*", *(IBM Corporation, 2013)*

4.4.3 Actores

Los actores que intervienen en el día a día de un CSOC son diversos, por lo que su complejidad depende de la madurez y naturaleza del negocio que lo posee, en tal sentido, a continuación, se presentarán una serie de tablas que describen los actores propuestos por diversos actores.

De acuerdo con Morillas & Raggi (2019), para la creación, implantación y/o mantenimiento de un Centro de Operaciones de Ciberseguridad, se requiere de 5 actores, los cuales se detallan en la Tabla 3.

Tabla 3. Descripción de actores que interactúan con un CSOC

Actor	***Descripción***	***Funciones***
Analista de Seguridad	Especialista en materia de seguridad, conocedor de los objetivos y activos del negocio.	1. Mapear los riesgos de la organización a partir de las amenazas y probabilidad de ocurrencia de un incidente. 2. Elaborar tickets de nuevos incidentes. 3. Realizar Informes de evaluaciones periódicas en la organización. 4. Comunicar al equipo sobre hallazgos en entidades de rubros afines a la organización.
Especialista de Seguridad	Especialista de soluciones de ciberseguridad, responsable de dar respuesta a incidentes de seguridad, centrándose en el análisis forense, malware y otros que permitan determinar la causa raíz de un incidente.	1. Recibe los incidentes reportados por el analista de Seguridad. 2. Identificar la causa raíz de los incidentes de ciberseguridad, por medio de análisis en profundidad. 3. Dar respuesta a los incidentes de ciberseguridad. 4. Elaboración y documentación de estrategias de mitigación, remediación y recuperación ante incidentes.

Actor	*Descripción*	*Funciones*
Identificador de Amenazas	Se apoya del Analista de seguridad, para el establecimiento de nuevas amenazas en el rubro del negocio, apoya a su vez al especialista de seguridad a dar respuesta a incidentes de alto nivel.	1. Realizar revisión de nuevos activos, para la determinación de vulnerabilidades, 2. Diseñar y ejecutar pruebas de penetración periódicas. 3. Elaborar reporte de hallazgos, documentando las nuevas amenazas y patrones de ataque. 4. Proponer mejoras y cambios en herramientas de ciberseguridad adoptadas por la organización.
Administrador del CSOC	Se trata del responsable del funcionamiento y operación del centro de operaciones de ciberseguridad.	1. Liderar al personal del CSOC. 2. Crear y ejecutar proyectos de mejora continua para el CSOC. 3. Gestionar y ejecutar fondos para la adquisición de herramientas, productos y/o servicios a disposición del CSOC. 4. Crear y ejecutar plantes de capacitación para el personal del CSOC. 5. Comunicar a las demás áreas sobre hallazgos, mejoras y/o funcionamiento del CSOC.
Ingeniero de Despliegue	Personal técnico, con conocimiento en la gestión e instalación de herramientas y servicios del CSOC.	1. Instalar y configurar herramientas y/o servicios de ciberseguridad en la infraestructura tecnológica de la organización. 2. Dar mantenimiento preventivo y/o correctivo a las herramientas instaladas.

Comparada con la tabla anterior, en la propuesta de Antón Zambrano & Ariel (2020) que se recoge en la Tabla 4, se contempla menos personal para el equipo de un CSOC, limitándose al establecimiento de tres analistas de seguridad (uno para cada nivel de seguridad del CSOC).

Tabla 4. Definición de roles de acuerdo con el nivel del CSOC

Actor	*Descripción*	*Funciones*
Analista de seguridad de soporte de nivel 1	Personal que recibe y examina las alertas reales del SIEM.	1. Monitoreo continuo de las alertas disparadas parametrizadas a partir de las necesidades del cliente. 2. Visualización de dashboards que permitan evaluar la postura de seguridad de las diferentes fuentes como lo son el Firewall, IPS, IDS, AD. 3. Eventos de Windows. 4. Recolección de información necesaria para análisis de Nivel 2
Analista de seguridad de soporte de nivel 2	Encargado de resolver los incidentes de ciberseguridad.	1. Ejecutar análisis especializado para correlacionar diferentes fuentes de seguridad. 2. Determinar si un sistema crítico o base de datos ha sido impactada. 3. Brindar recomendaciones de reparación frente a incidentes de seguridad. 4. Brinda soporte para nuevos métodos de análisis para la detección de amenazas.
Analista de seguridad de nivel 3	Especialista de seguridad, asignado a atender incidentes críticos	1. Realiza evaluaciones de vulnerabilidad y pruebas de penetración para evaluar la resiliencia de la organización 2. Aislar áreas de debilidad que necesitan atención. 3. Revisar alertas, inteligencia de amenazas y datos de seguridad. Identifica amenazas que han ingresado a la red brechas de seguridad y vulnerabilidades actualmente desconocidas.

Una tercera opción de identificar al personal que se involucra en un CSOC es la propuesta por Morales Gonzáles, Moreno Sánchez, & Ortigoza Pérez (2014) en su proyecto denominado “Propuesta de un modelo de centro de operaciones de seguridad (SOC) para la

fuerza aérea colombiana", en donde se destacan los actores los identifican con los roles de operador SOC, director SOC y CSIRT (Comité de seguridad). Esta opción se detalla en la Tabla *5*.

Tabla 5. Roles y responsabilidades propuestos para un CSOC Ad-Hoc.

Actor	***Descripción***	***Funciones***
Operador SOC	Rol técnico que se encarga del monitoreo e interpretación de eventos.	1. Realizar el monitoreo de la infraestructura tecnológica correlacionada en el SIEM. 2. Realizar la clasificación de los eventos (Real, sospechoso, falso positivo). 3. Realizar la escalación de incidentes.
Director SOC	Actor estratégico, responsable de la planificación, gestión y toma de decisiones para operar el SOC.	1. Planificar, coordinar y tomar decisiones estratégicas para la correcta operación del CSOC. 2. Garantizar la Disponibilidad, integridad y confidencialidad de los servicios que el CSOC brinda a la organización. 3. Realizar las gestiones de recurso para la remediación de incidentes.
Comité de Seguridad	Conjunto de personas relacionadas con el estado, para autorizar la actuación y remediación con un incidente.	1. Decretar el estado de un incidente. 2. Autorizar y dar el visto bueno para que se inicie el proceso de repuesta a incidentes. 3. Colaborar para la remediación de incidentes.

4.4.4 Herramientas

Las herramientas dentro de un sistema de operaciones de ciberseguridad, ver de manera clara las actividades que se han realizado dentro de nuestros sistemas, y por lo tanto las herramientas nos pueden ayudar a darnos datos que con un análisis rápido nos permitan a detectar situaciones que puedan dañar la integridad, confidencialidad y disponibilidad de la información de la organización (Concha, 2019).

Tabla 6. Herramientas y Funciones de un CSOC

Función del CSOC	***Herramienta***	***Uso de la Herramienta***
Monitoreo y detección	Herramientas de captura y análisis de tráfico de red	Inspeccionar paquetes de red con la finalidad de determinar la naturaleza de las actividades que se llevan a cabo en la red.
	Sistemas de detección/prevención de intrusiones.	Identificar oportunamente actividades anómalas o maliciosas.
	Sistemas de gestión de eventos e información de seguridad	Correlacionar eventos originados en diversas fuentes para agilizar la detección y respuesta ante ciberataques.
Análisis	Herramientas de inspección visual y procesamiento de datos	Realizar una investigación en profundidad de los logs, alertas, paquetes de tráfico de red, y eventos reportados por las herramientas de monitoreo y detección con el propósito de identificar, patrones, tendencias y causas de las actividades anómalas o maliciosas que puedan considerarse una amenaza para la organización.
Respuesta e Informe	Sistema de gestión de tiquetes y asistencia técnica	Creación y rastreo de tiquetes donde se documentan las acciones tomadas ante eventos de seguridad de interés.

Función del CSOC	*Herramienta*	*Uso de la Herramienta*
	Herramientas para preparación de informes	Producción de reportes tanto técnicos como no técnicos para informar a las partes interesadas sobre los incidentes de seguridad.
Ciber inteligencia	Noticias	Identificar violaciones de ciberseguridad que puedan afectar al negocio, a los socios de este, o afecten otras empresas con modelos de negocio similares.
	Redes sociales, así como, sitios especializados y boletines electrónicos	Obtener información sobre nuevas vulnerabilidades que los proveedores de hardware y software publican a través de estos recursos y que se relacionan con los activos informáticos que se pretenden proteger en la organización.
	Plataformas centralizadas de inteligencia de amenazas	Consultar diferentes bases de vulnerabilidades con la finalidad de clasificar amenazas potenciales de los activos de hardware y software de la organización.
Gestión de incidentes	Sistema de gestión y control de tiquetes	Documentar las acciones tomadas durante todo el proceso de gestión de incidentes de seguridad.
Línea base y vulnerabilidades	Gestores y Escáneres de vulnerabilidades	Identificar y corregir vulnerabilidades existentes en los sistemas evaluados.
	Sistemas de gestión de parchado	Desplegar actualizaciones de forma regular o bajo demanda con el propósito de solventar cualquier vulnerabilidad conocida en los sistemas de redes computacionales.
Gestión de políticas y firmas	Interfaces centralizadas o individuales de gestión de	Aplicar cambios de configuración en plataformas de seguridad con el propósito

Función del CSOC	*Herramienta*	*Uso de la Herramienta*
	dispositivos y aplicaciones de seguridad.	de detectar y responder a ataques de ciberseguridad.
Cumplimiento y gestión del riesgo	Escáneres de cumplimiento o conformidad	Determinar ajustes de configuración que necesitan ser aplicados en los sistemas de redes computaciones para ajustarse a marcos de trabajo específicos.
Ejecución de pruebas de penetración	Herramientas de pruebas de penetración	Probar las defensas implementadas en una organización y exponer posibles debilidades y vulnerabilidades mediante la simulación de ciberataques.
Forense y malware	Tecnologías de Sandboxing	Analizar y comprender el comportamiento de software malicioso en entornos aislados, controlados.
	Plataformas y herramientas de análisis forense digital	Obtener y preservar evidencias digitales de artefactos relacionados a actividades maliciosas.
Ingeniería y recolección de bitácoras	Soluciones de hardware y software orientados a la gestión del almacenamiento.	Tecnologías para gestionar de forma eficiente el almacenamiento de todos los datos e información que tienen relación a eventos de seguridad recopilados y generados por el CSOC.

Nota. Elaboración propia a partir de los trabajos «Towards a Framework for Measuring thePerformance of a Security Operations Center Analyst», por Agyepong et al., 2020,2020International Conference on Cyber Security and Protection of Digital Services (Cyber Security);«Integrating a Security Operations Centre with an Organization’s Existing Procedures, Policies,and Information Technology Systems», por Mutemwa et al., 2018,2018 International Conferenceon Intelligent and Innovative Computing Applications (ICONIC).

4.4.5 Fuentes de Datos e Información de Eventos de Ciberseguridad

Un CSOC requiere de datos e información relacionada a eventos de ciberseguridad provenientes tanto del interior de la organización como originada fuera de ella para poder

realizar sus funciones de forma efectiva. Estos datos e información deben originarse de fuentes relevantes para la organización y acordes al contexto en que realiza sus operaciones de negocio. La Tabla 7 recoge una clasificación de tales fuentes según lo documentan y ejemplifican Vielberth et al. (2020).

Tabla **7**.Fuentes Relevantes de Datos e Información de Eventos de Ciberseguridad.

Clasificación	***Ejemplo***
Software de seguridad	Plataformas de gestión de eventos e información de seguridad, sistemas de detección de intrusiones, sistemas de prevención de intrusiones, cortafuegos, antivirus, gestores de vulnerabilidades, sistemas de gestión de identidad y acceso.
Activos de red	Conmutadores de paquetes, enrutadores, servidores, dispositivos de usuario final, servidores proxy.
Entornos de virtualización	Hipervisores, introspección de máquinas virtuales, entornos de nube.
Tecnología operativa	Sensores, controladores lógico-programables.
Otro software	Análisis de Big Data de fuentes abiertas, Bases de datos, sistemas de gestión de identidad y acceso, servidores de correo, sistemas operativos.
Activos de seguridad física	Cámaras de seguridad, sistemas de control de acceso.
Inteligencia externa	Inteligencia de fuentes abiertas (OSINT), inteligencia proveniente de plataformas de intercambio de información de amenazas u otras organizaciones.
Personal	Empleados, personal externo.

Los referidos autores Vielberth, Böhm, Fichtinger, & Pernul (2020) también clasifican estos datos e información originados en las fuentes antes descritas en dos categorías, **datos de registros** e **inteligencia**. La **Figura** 3 ilustra estas fuentes y los tipos de datos e información que producen.

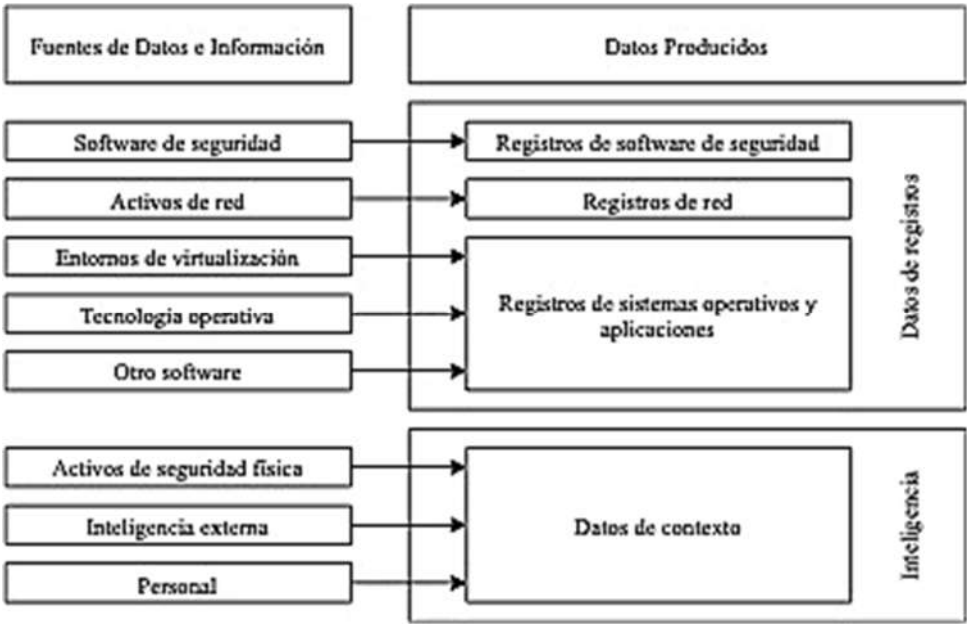

Figura 3. Fuentes de Datos y los Datos que Producen. *Adaptado de "Security Operations Center: A Systematic Study and Open Challenges [Centro de Operaciones de Seguridad: Un Estudio Sistemático y Desafíos Abiertos]" por Vielberth et al., 2020, IEEE Access, 8.*

4.4.6 Usos e importancia de la implementación de un sistema de monitoreo de eventos de seguridad de la información.

Las tecnologías a lo largo del tiempo han tenido cambios a pasos agigantados, en su uso e importancia. Hoy en día podemos afirmar que el personal que gestiona los *CSOC´s* son personas cualificadas y calificadas en su rama, lo que les permite responder de manera efectiva ante eventos de ciberseguridad. A continuación, describimos los usos e importancias que tienen los *CSOC´s* en la actualidad.

- Usos:
    - Uno de los principales usos que tiene un centro de operaciones de ciberseguridad es el monitoreo continuo, en donde se actúe de manera oportuna ante los ataques de malware, denegación de servicio, virus, piratas informáticos, entre otros. (Schinagl, Schoon, & Paans, 2015).
    - También existen cuatro usos primordiales que un centro de operaciones de ciberseguridad tiene los cuales son: prevención, detección, respuesta y predicción. Donde en la prevención se pueden realizar pruebas de seguridad, así como la revisión de los controles de ciberseguridad de la entidad; en la detección se debe contar con el monitoreo y con el descubrimiento de amenazas que rondan en el medio cibernético; en la respuesta debemos contar con la debida gestión, contención y recuperación efectiva; y en la predicción debemos pronosticar brechas de ciberseguridad que en el futuro nos puedan afectar. (B Secure, 2016).
    - Uso basado en la búsqueda de amenazas, los *CSOC's* están agregando la búsqueda de amenazas controlada por hipótesis para identificar de forma

proactiva a los atacantes avanzados y eliminar las alertas de las colas de los analistas que están en primera línea. (Microsoft, 2020).

- Importancia de la implementación:
    - La principal importancia de la implementación de un centro de operaciones de ciberseguridad es ayudar en la protección de los activos de información de una entidad determinada. (Mccoy & Jarpey, 2017)
    - Según Méndez Fonseca (2019) la implementación de un centro de operaciones de ciberseguridad nace de la necesidad de poder dar gestión y contención sobre las amenazas que se fueron creando, también por otro lado la importancia es lograr dar una respuesta oportuna y acertada sobre las ciber amenazas que existen en el medio.
    - La implementación debe incluir un CSOC integral donde se deben elaborar servicios seguros. Entre otras implementaciones se deben incluir CSOC impulsados por tecnologías en donde se sepa que sucede en un entorno operativo y donde los ingenieros puedan interactuar con los sistemas del centro de operaciones de ciberseguridad, contratados parcialmente (proveedor de hosting) y especializados que sirvan para proteger datos de sistemas SCADA y otros. (Schinagl, Schoon, & Paans, 2015).
    - Otra importancia de la implementación de un centro de operaciones de ciberseguridad es que nos ayudan a la reducción de costos (en caso de ser con software libre), a la optimización en la gestión de operaciones de seguridad, a la visibilidad global de las amenazas, adelantarse a los ciber ataques y por último nos ayuda a tener una gestión más proactiva donde la

velocidad y la eficacia de la automatización nos pueden ayudar a disuadir a los ciberdelincuentes que buscan un objetivo fácil. (Álvarez, 2020).

4.5 Clasificación de evento

Antes de entrar en detalle sobre la clasificación de eventos, es necesario establecer la diferencia entre un evento, alerta e incidente. Esta terminología de uso común para quienes se encargan del monitoreo en un CSOC se detalla en la Tabla 8.

Tabla 8. Cuadro de definiciones de las normativas ISO, ITIL y NIST

Normativa	***Evento***	***Alerta***	***Incidente***
ISO[2]	Ocurrencia o cambio de un conjunto particular de circunstancias	-	Uno o varios eventos de seguridad de la información no deseados, que tienen un impacto al comprometer las operaciones comerciales
ITIL[3]	Cualquier cambio de estado que es significativo para la gestión de un servicio u otro elemento de configuración.	-	Interrupción de un servicio o reducción en la calidad de un servicio no planificadas.
NIST[4]	Cualquier ocurrencia observable en una red o sistema		Violación o amenaza inminente de las políticas de seguridad informática, o prácticas de seguridad estándar

[2] Conceptos consultados en: Estándar ISO 2700:2018 IEC (ISO, 2018)

[3] Conceptos consultados en: ITIL® Foundation, (AXELOS, 2019)

[4] Conceptos consultados en: Computer Security Incident Handling Guide (Cichonski, Millar, Grance, & Scarfone, 2012)

Los eventos en los cuales un CSOC puede intervenir son múltiples y su clasificación dependerá de la normativa o estándar en el cual la organización haya basado sus políticas y controles. Se debe tomar como referencia a aquellos que se relacionan directamente con los activos que la organización considere críticos.

Si se parte de la definición de evento “Cambio… Cualquier ocurrencia observable en la red”, los eventos de ciberseguridad son todo lo que afecta o amenaza a la organización, que tiene un impacto directo en las operaciones del negocio y puede analizarse por medio de indicadores, en nuestro caso, fuentes de información crítica, tal como se indicó en la sección anterior

De acuerdo con Kent & Souppaya (2006) en la guía de gestión de registros de seguridad informática, los eventos pueden clasificarse de acuerdo con su origen las alertas, siendo estos Sistemas Operativos, Aplicaciones y Hardware

4.6 Políticas y buenas prácticas en la administración de un CSOC

Para mejorar la eficiencia y efectividad de los CSOC, a través de una investigación cualitativa en la que participaron empleados tanto de nivel operativo como táctico, se determinó que los principales problemas que deben enfrentarse para mejorar la eficiencia y efectividad de las operaciones de estos centros se encuentran (Kokulu, et al., 2019):

Tabla 9. Problemas que afectan la eficiencia y eficacia de los CSOC

Categoría	Subcategoría
Problemas operacionales	- Baja visibilidad de dispositivos y de la topología de la red - Defensa insuficiente ante tipos de ataques específicos. - Baja velocidad de respuesta - Métricas de evaluación insuficiente - Presupuesto insuficiente
Problemas tecnológicos	- Inteligencia de amenazas de baja calidad y sobrecargada - Baja calidad de reportes y registros - Alta tasa de falsos positivos - Herramientas con mal funcionamiento - Nivel de automatización insuficiente - Sistemas con poca usabilidad - Tecnologías de escala desafiantes
Problemas relacionados al conocimiento humano	- Baja conciencia situacional - Insuficiente entrenamiento de los analistas

5. Desarrollo de guía de aplicación para el monitoreo de ciberseguridad con herramientas de código abierto

Introducción

Considerando el impacto económico y reputacional que las organizaciones sufren debido a incidentes de ciberseguridad, se vuelve importante contar con una solución tecnológica que dé respuestas en tiempo real a los incidentes detectados, capaz de identificar el origen del incidente, así como los activos y procesos comprometidos por el incidente.

La seguridad de la información es un tema que preocupa a organizaciones de cualquier índole y país, ya que pese a contar con Sistemas de Gestión de Seguridad de la información (SGSI), las mismas son incapaces de identificar las amenazas cibernéticas que pueden perjudicar a sus activos de información, reflejando esa incapacidad en pérdidas significativas de dinero en manos de delincuentes, tal como se muestra en el Reporte de ciberseguridad 2020 realizado por el Banco Interamericano de Desarrollo, quien señala que dichas consecuencias son producto de un bajo nivel de madurez de las organizaciones. El actual panorama de amenazas cibernéticas se caracteriza por una rápida evolución hacia la perpetración de actividades maliciosas realizadas por cibercriminales que se encuentran mucho mejor organizados que en el pasado. Estos cibercriminales no solo son capaces de utilizar técnicas bien conocidas como el phishing o incluso explotar vulnerabilidades de día cero, sino que ahora pueden realizar sofisticados ataques a la cadena de suministros e infiltrarse a gran escala en las organizaciones. En contraposición a esta situación, los enfoques de seguridad que se implementan en el sector público y privado no podrán

responder adecuadamente a este nuevo panorama de amenazas sino se reinventan para la toma de decisiones basadas en el riesgo.

Para ello, las empresas se enfocan en operar bajo marcos de trabajos reconocidos a nivel global, para gestionar sus sistemas de seguridad de la información, pero existe un déficit de fuentes relacionadas a directrices apropiadas para operativizar la ciberseguridad.

Esta *Guía de aplicación para el monitoreo de ciberseguridad con herramientas de código abierto,* nace como respuesta a la falta de un marco de trabajo que permita la construcción y gestión de un Centro de Operaciones de Ciberseguridad con herramientas de código abierto y costos accesibles para las organizaciones de la región, apoyando particularmente a aquellas organizaciones que cuentan con un presupuesto limitado y personal de poca experticia técnica en la implementación de un CSOC.

Un CSOC es una iniciativa de carácter estratégico donde se orquestan personas, procesos y tecnología para dotar a las organizaciones de capacidades de monitoreo continuo de las actividades cibernéticas que acontecen en el contexto de sus operaciones, con el propósito de prevenir, detectar, escalar y recuperarse de incidentes de ciberseguridad. La finalidad de este CSOC consiste en proveer un entorno cibernético seguro para el cumplimiento de los objetivos estratégicos de las organizaciones en que la seguridad de la información y la gestión del riesgo tecnológico son parte integral de los procesos de negocio.

A continuación, encontrará una serie de pasos que servirán como guía a aquellas organizaciones que desean operativizar la ciberseguridad y que no cuentan con una guía metodológica que los oriente.

Metodología propuesta para la implementación de un CSOC

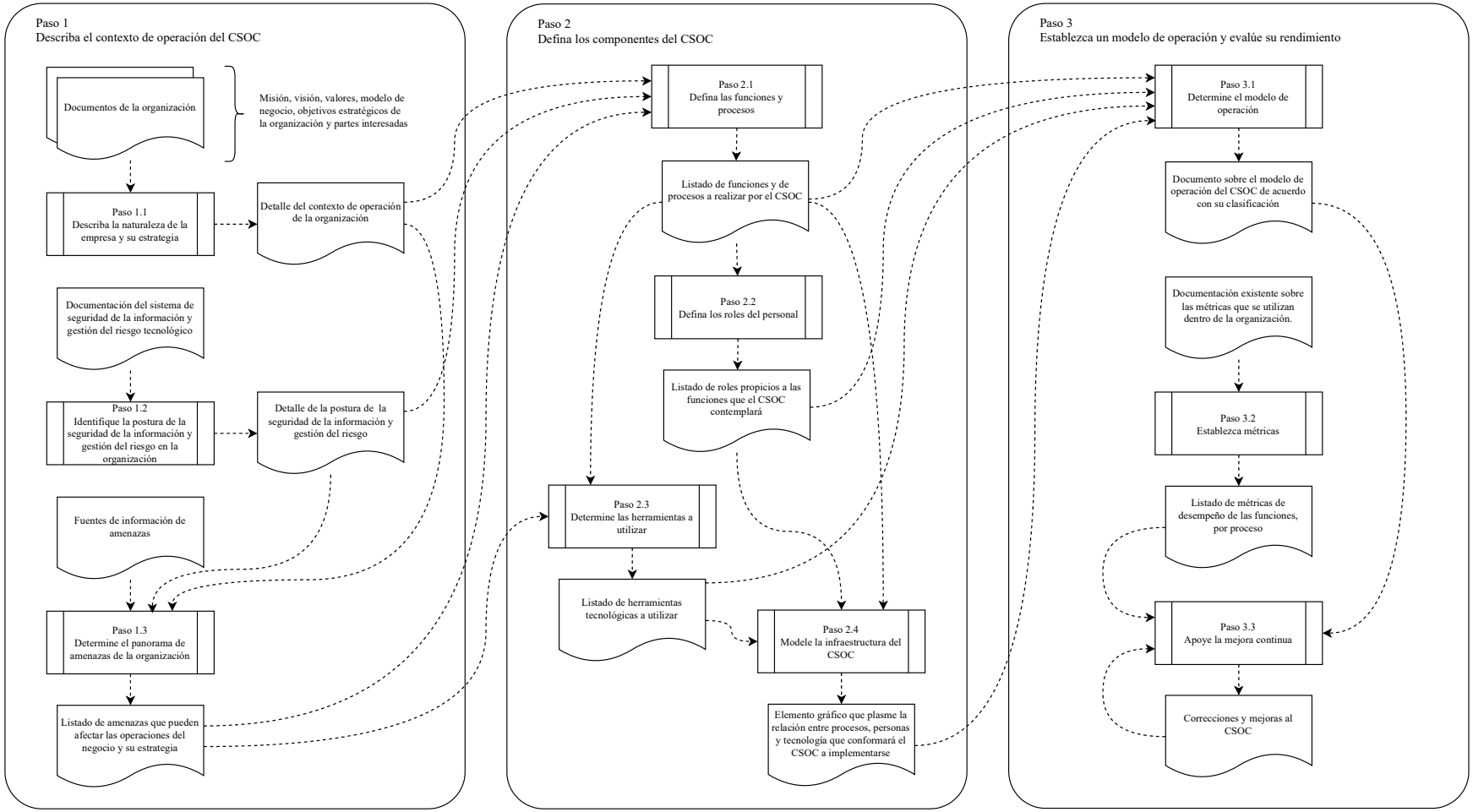

Figura 4 Metodología Propuesta para la implementación de un CSOC. Elaboración Propia

Paso 1. Describa el contexto de operación del CSOC

Es importante que la organización interesada en establecer un CSOC conozca el contexto en el que este va a operar. Este contexto incluye aspectos internos de la organización y otras de carácter externo que influyen en la consecución de sus objetivos. Los aspectos internos que debería considerar toda organización incluyen la naturaleza de la empresa y su estrategia, así como identificar el nivel de madurez de la seguridad de la información y gestión del riesgo. En cuanto a los aspectos externos, la organización debería considerar el panorama de ciber amenazas que enfrenta dado su modelo de negocio.

Describir el contexto de esta manera, ayuda a asegurar que la decisión de implementar un CSOC responda adecuadamente a las necesidades de confidencialidad, integridad y disponibilidad de los activos tecnológicos y de información que posee, a través del entendimiento de la misión, visión, valores, objetivos estratégicos y políticas que orientan las operaciones del negocio.

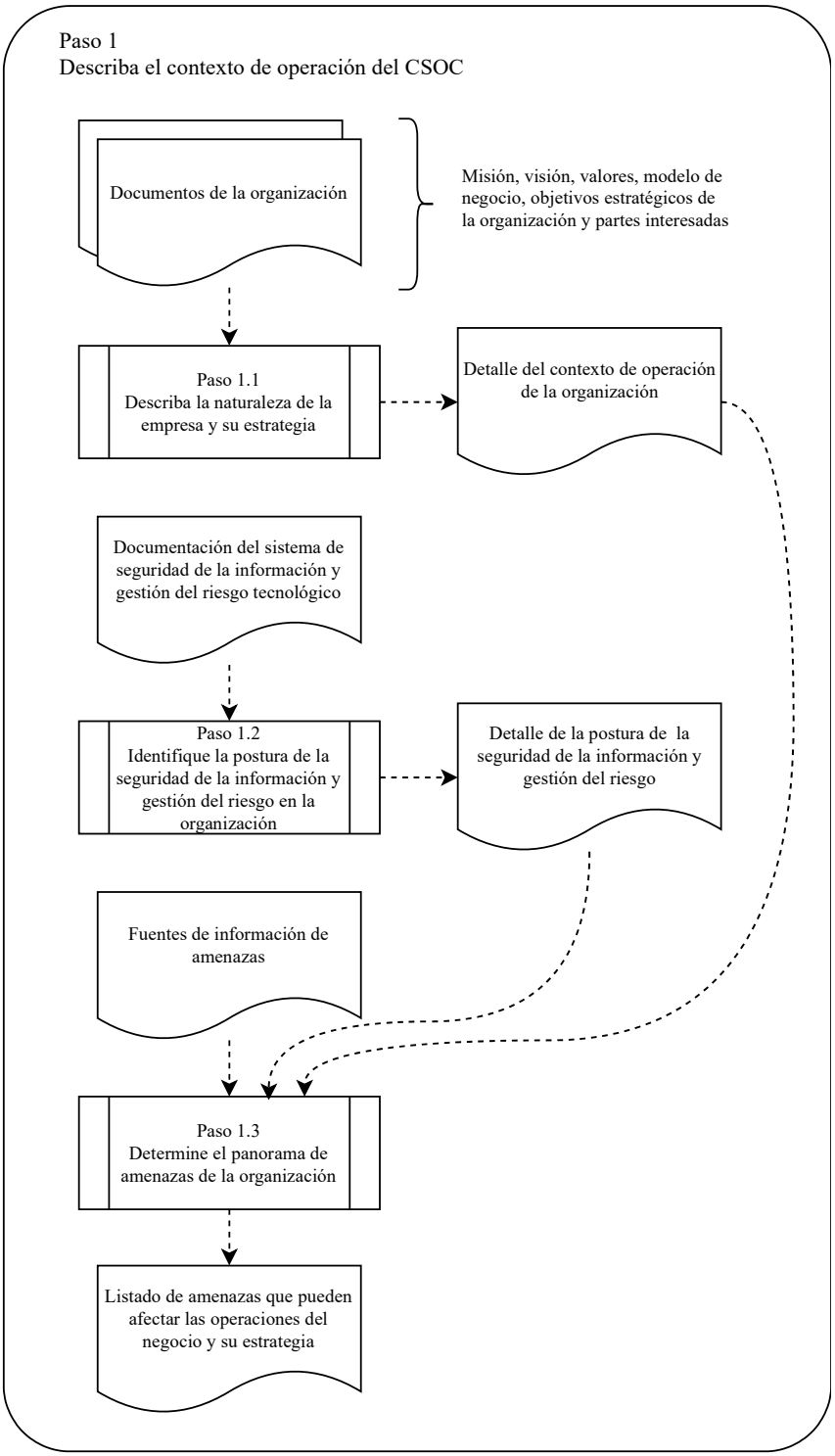

Figura 5 Diagrama de Flujo: Paso 1. Contexto de operación del CSOC. Elaboración Propia

Paso 1.1. Describa la naturaleza de la empresa y su estrategia

Entrada**:** Documentos de la organización que describen la misión, la visión, los valores, el modelo de negocio, los objetivos estratégicos de la organización y las partes interesadas.

Proceso: Deberían recopilarse los documentos que describen la naturaleza y estrategia de la organización y analizarlos para determinar el contexto de operación del CSOC.

Para realizar el análisis de la documentación recopilada, se recomienda auxiliarse de la matriz propuesta en el **Anexo A Listado de documentos que describen el contexto de operación del negocio**, a fin de obtener el detalle del contexto de operación de la organización.

Nota: Los aspectos indicados en la matriz, son lo mínimos requeridos para entender cómo opera y hacia dónde se encuentran encaminadas las actividades del negocio, por lo que, si considera necesario otros aspectos, puede incorporarlos en la matriz propuesta.

Salida: El detalle del contexto de operación de la organización conformado por elementos como: Misión, Visión, Valores, Objetivos estratégicos, Políticas, Partes interesadas y otros elementos importantes para el desempeño de las operaciones del negocio

Paso 1.2. Identifique la postura de la seguridad de la información y gestión del riesgo en la organización.

Entrada: Documentación del sistema de seguridad de la información y gestión del riesgo tecnológico implementado en la organización.

Proceso: Debería ser recopilada la documentación asociada a la política de la seguridad de la información, plan de tratamiento de riesgos, y controles y procedimientos que forman del sistema de seguridad de la información y gestión del riesgo tecnológico de la organización.

Salida: Detalle de la postura de la seguridad del sistema de gestión de la información y gestión del riesgo.

Paso 1.3. Determine el panorama de amenazas de la organización.

Entrada: Fuentes información de amenazas.

Proceso: Debería de recopilarse información que provenga de fuentes como:

- Centros de ciberseguridad de la localidad en la que opera el negocio. Por ejemplo, el SOC de la República Dominicana, el Centro de gestión de Incidentes Informáticos de Bolivia[5] y el Centro de Defensa Cibernética de Israel del Caribe.
- Documentación Técnica publicada por organizaciones de ciberseguridad. Por ejemplo, ISO/IEC 27005:2019. Gestión de riesgos de la Seguridad la

[5] Centro de gestión de Incidentes Informáticos de Bolivia

Información, Observatorio de la Ciberseguridad en América Latina y el Caribe (BID y OEA)[6] y/o el Instituto Nacional de Ciberseguridad[7].

- Estudios académicos de instituciones educativas que apliquen al sector de negocio de la organización.

Los criterios que la información seleccionada debería de cumplir son:

- Se relacione a aquellos riesgos que se han identificado que pueden afectar a los objetivos del negocio.
- Debe afectar directamente a las relacionadas a las tecnologías que posee la organización.
- Que se relacione con las amenazas identificadas en el área geográfica en la que la organización opera.
- Debe afectar directamente a las relacionadas al sector o rubro de la organización.

Para realizar el análisis de la información proveniente de las fuentes identificadas, se recomienda hacer uso de matriz indicada en el **Anexo B Matriz de análisis de fuentes de información para la identificación de amenazas.**, a fin de obtener el listado de amenazas aplicables al negocio.

Salida: Listado de amenazas que pueden afectar las operaciones del negocio y su estrategia.

[6] Observatorio de la Ciberseguridad en América Latina y el Caribe

[7] Instituto Nacional de Ciberseguridad

Paso 2. Defina los componentes del CSOC

Considérese este paso como medular en la implantación de un Centro de Operaciones de Ciberseguridad, ya que en este se identifican y definen los procesos, tecnologías y personas que operarán el CSOC.

El presente paso toma como entradas del paso anterior el detalle del contexto de la organización, la postura de este último referente a la ciberseguridad y el análisis del riesgo, así como el listado de amenazas que afectan a las operaciones del negocio.

Para la transformación de las entradas, este paso se auxilia de 5 anexos, que permiten identificar el Listado de funciones y procesos del CSOC, El listado de roles propicios a las funciones del CSOC, El listado de herramientas tecnológicas a utilizarse en el CSOC, así como un elemento gráfico que plasme la interacción de los elementos anteriores en una sola estructura.

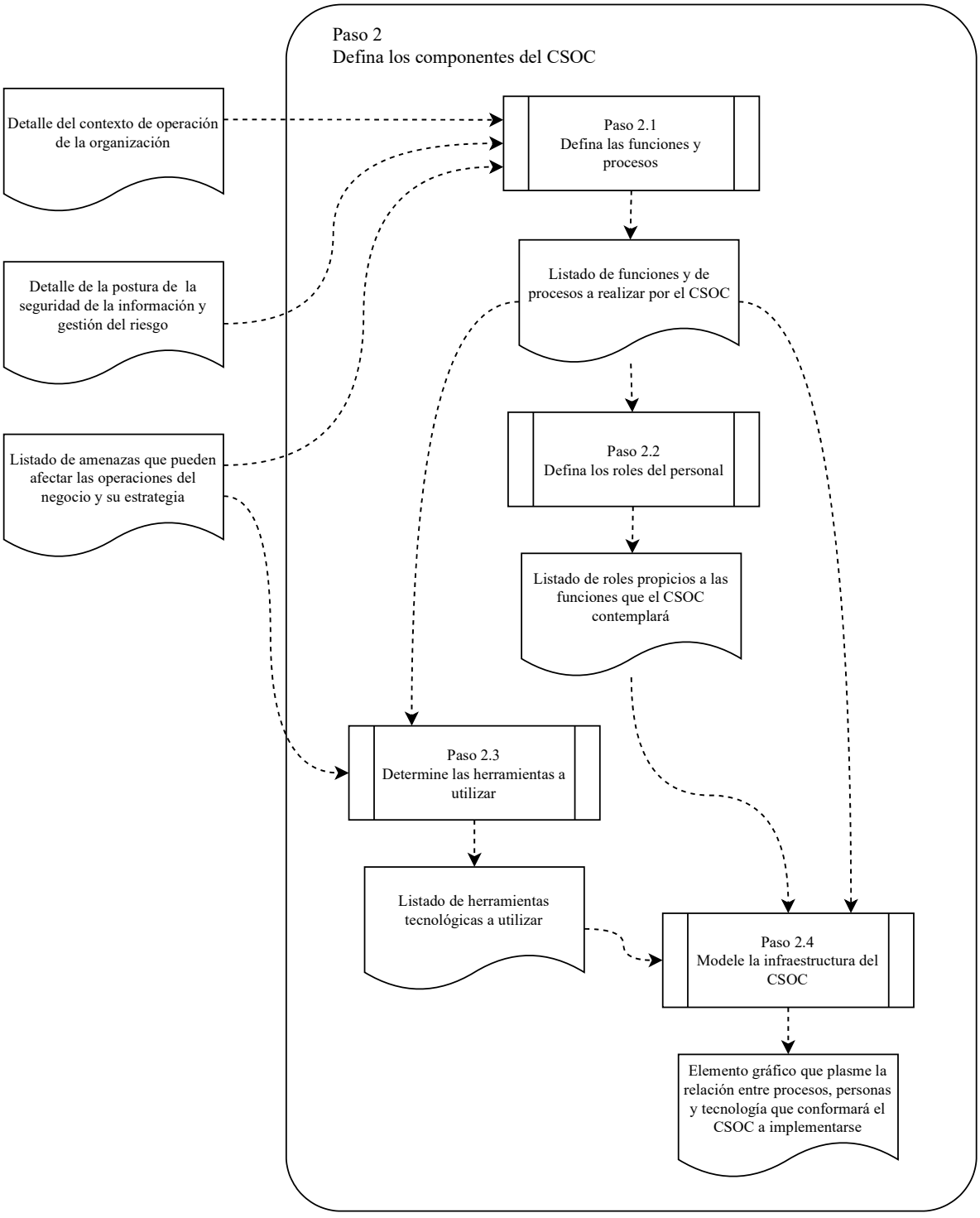

Figura 6 Diagrama de Flujo: Paso 2. Componentes del CSOC. Elaboración Propia

Paso 2.1. Defina las funciones y procesos

Entrada: El detalle del contexto de operación de la organización, detalle de la postura de la seguridad de la información y gestión del riesgo, y listado de amenazas que pueden afectar las operaciones del negocio y su estrategia.

Proceso: Se debería hacer una lectura y análisis sobre las entradas de este paso, y determinar el listado de funciones y procesos del CSOC por medio del llenado de la matriz de asignación propuesta en el **Anexo C Matriz de asignación de procesos por funciones.** a fin de conocer los procesos requeridos para el cumplimiento de las funciones definidas para el CSOC.

Para el cumplimiento de este paso, se sugieren las actividades siguientes:

1. Genere un listado de las funciones que el CSOC cumplirá; considerando entre ellas funciones como las siguientes:
    a. Monitoreo y detección de eventos de seguridad: implica el monitoreo de sistemas de red computacionales, dispositivos y aplicaciones ejecutándose en estos dispositivos con el propósito de detectar cualquier actividad maliciosa o anormal
    b. Análisis de los eventos de seguridad: implica una investigación a profundidad de las actividades anormales e inusuales observadas en la red de la organización.
    c. Respuesta e informe sobre los eventos de seguridad: Implica la ejecución de acciones específicas según lo exijan los procesos de trabajo locales para mitigar o reducir el daño potencial de una amenaza identificada. Un punto importante es que la respuesta implica la generación de reportes

tanto técnicos como no técnicos para las partes interesadas afectadas por los incidentes.

d. Ciber inteligencia: Implica la obtención de información sobre indicadores de compromiso (del inglés Indicators of Compromise, IOCs) de terceras partes o de fuentes abiertas con la finalidad de detectar actividades maliciosas.
e. Gestión de incidentes de ciberseguridad: capacidad de preparar, identificar, y escalar un incidente. A esto le acompaña, la capacidad de formular un plan de contención y erradicación como parte de esta función.
f. Gestión de vulnerabilidades: Requiere las actividades de aplicación de parches y reforzamiento de la seguridad en los sistemas computacionales con el fin de abordar cualquier debilidad conocida. La ejecución de escaneo de vulnerabilidades es una actividad esencial para el cumplimiento de esta función.
g. Gestión de políticas y firmas de equipos de ciberseguridad: persigue mantener actualizadas las políticas y firmas de las herramientas técnicas utilizadas para detectar, prevenir y enfrentar ciberataques.
h. Cumplimiento y gestión del riesgo tecnológico: apoya el cumplimiento de requisitos obligatorios, industriales o reglamentarios relacionados a la naturaleza de las operaciones del negocio.
i. Ejecución de pruebas de penetración: Involucra la simulación de ataques cibernéticos contra los sistemas de red computacionales de la

organización para probar la defensa implementada y la reacción bajo ataque.

j. Análisis forense: Se relaciona a la obtención y preservación de evidencia relacionada a actividades maliciosas

2. Genere una lista de procesos que permitan el cumplimiento de cada una d las funciones definidas para el CSOC.
3. Asocie los procesos provenientes del numeral anterior con las funciones definidas en el numeral 1 de este paso.
4. Redacte una descripción del proceso, dando respuesta a interrogantes como las siguientes:
    a. ¿Qué hace?
    b. ¿Cómo lo realiza?
    c. ¿Con que recursos?
    d. ¿Bajo qué propósito?

Nota: Considere dentro de la lista de procesos generados, procesos existentes en la organización que contribuyan a las funciones definidas; caso contrario, proponga nuevos procesos. Se recomienda realizar la documentación formal de los procesos del CSOC siguiendo los estándares definidos por la organización

Salida: Listado de funciones y de procesos a realizar por el CSOC.

Paso 2.2. Defina los roles del personal.

Entrada: Listado de funciones y de procesos a realizar por el CSOC.

Proceso: Se debería identificar los roles necesarios en virtud de cumplir con las funciones del CSOC auxiliándose de la tabla indicada en el **Anexo D Tabla de roles,**

funciones y competencias requeridas para el centro de operaciones de ciberseguridad., el cual posee información como:

a. Nombre del Rol: considere nombres homólogos a los existentes en el mercado nacional, regional o internacional, siempre y cuando sus funciones sean congruentes al rol a desempeñar.
b. Descripción del Rol: defina el grado de experiencia requerido, así como un detalle general de lo que realiza el puesto.
c. Funciones: defina las funciones del CSOC asociadas al rol nombrado.
d. Competencias Requeridas: defina el grado académico, conocimientos afines a las labores a desempeñar y las acreditaciones que dan valor agregado al cargo.

Salida: Listado de roles propicios a las funciones que el CSOC contemplará.

Paso 2.3. Determine las herramientas a utilizar

Entrada: Listado de funciones y de procesos a realizar por el CSOC y Listado de amenazas que pueden afectar las operaciones del negocio y su estrategia.

Proceso: Se debería determinar un listado de herramientas tecnológicas apropiadas, ya sea, que estas se encuentren implementadas o se considere implementar, pero que en cualquier caso pueden ser utilizadas para dar operatividad a las funciones y procesos del CSOC que se ha determinado que realizará para enfrentar el panorama de amenazas que se describe en el listado de amenazas que pueden afectar las operaciones del negocio y su estrategia. Para poder elaborar este listado de herramientas tecnológicas a podría considerar las siguientes actividades:

1. Identificar herramientas implementadas en la organización que puedan utilizarse para dar operatividad a las funciones y procesos que el CSOC realizará.
2. Investigar otras herramientas que puedan dar operatividad a las funciones y procesos que el CSOC realizará.
3. Determinar la viabilidad técnica de utilizar las herramientas existentes y las propuestas.
4. Establezca un cruce de funciones y de procesos contra las herramientas que se ha determinado son viables técnicamente.

Puede auxiliarse del **Anexo E. Herramientas de código abierto para la construcción de un CSOC.** para determinar la forma de utilizar herramientas de código abierto que apoyen las funciones y procesos que el CSOC realizará. también puede auxiliarse con el **Anexo F Tabla de herramientas a utilizar para el cumplimiento de las funciones.** para documentar este paso.

Salida: Listado de herramientas tecnológicas a utilizar.

Paso 2.4. Modele la infraestructura del CSOC

Entrada: Listado de funciones y de procesos a realizar por el CSOC, listado de roles propicios a las funciones que el CSOC contemplará y listado de herramientas tecnológicas a utilizar.

Proceso: Se debería crear un diagrama[8] que modele la integración entre procesos, personas y tecnologías, para visualizar, realizando las notas aclaratorias necesarias para identificar las relaciones entre los elementos antes mencionados.

[8] Un ejemplo del Modelo que se espera de este paso puede visualizarse en el **Anexo F Tabla de herramientas a utilizar para el cumplimiento de las funciones.**

Nota: El elemento gráfico debe contener las herramientas definidas en el paso 2.3, acopladas de tal manera que permita visualizarse la manera en la que todas se relacionan, la función que se está realizando y los roles que intervienen en la ejecución de esta última.

Salida: Elemento gráfico que plasme la relación entre procesos, personas y tecnología que conformará el CSOC a implementarse.

Paso 3. Establezca un modelo de operación y evalúe su rendimiento

Es necesario que, para establecer un modelo de operación del CSOC para una organización, se deberían especificar la clasificación de acuerdo a las características que definen el comportamiento de cómo se implanta y opera un CSOC; algunas de las características que permiten determinar el tipo de Centro de Operaciones de Ciberseguridad son las siguientes, la capacidad de contraataque, los escenarios de despliegue, el propósito, las técnicas de correlación, las variantes de implementación y propiedad o tenencia.

Definido el modelo de operación de la organización, se deberían definir un conjunto de métricas que evalúen las funciones del CSOC. Las funciones que podrían evaluarse son monitoreo y detección, análisis, respuesta e informe, gestión de incidentes, y línea base y vulnerabilidades.

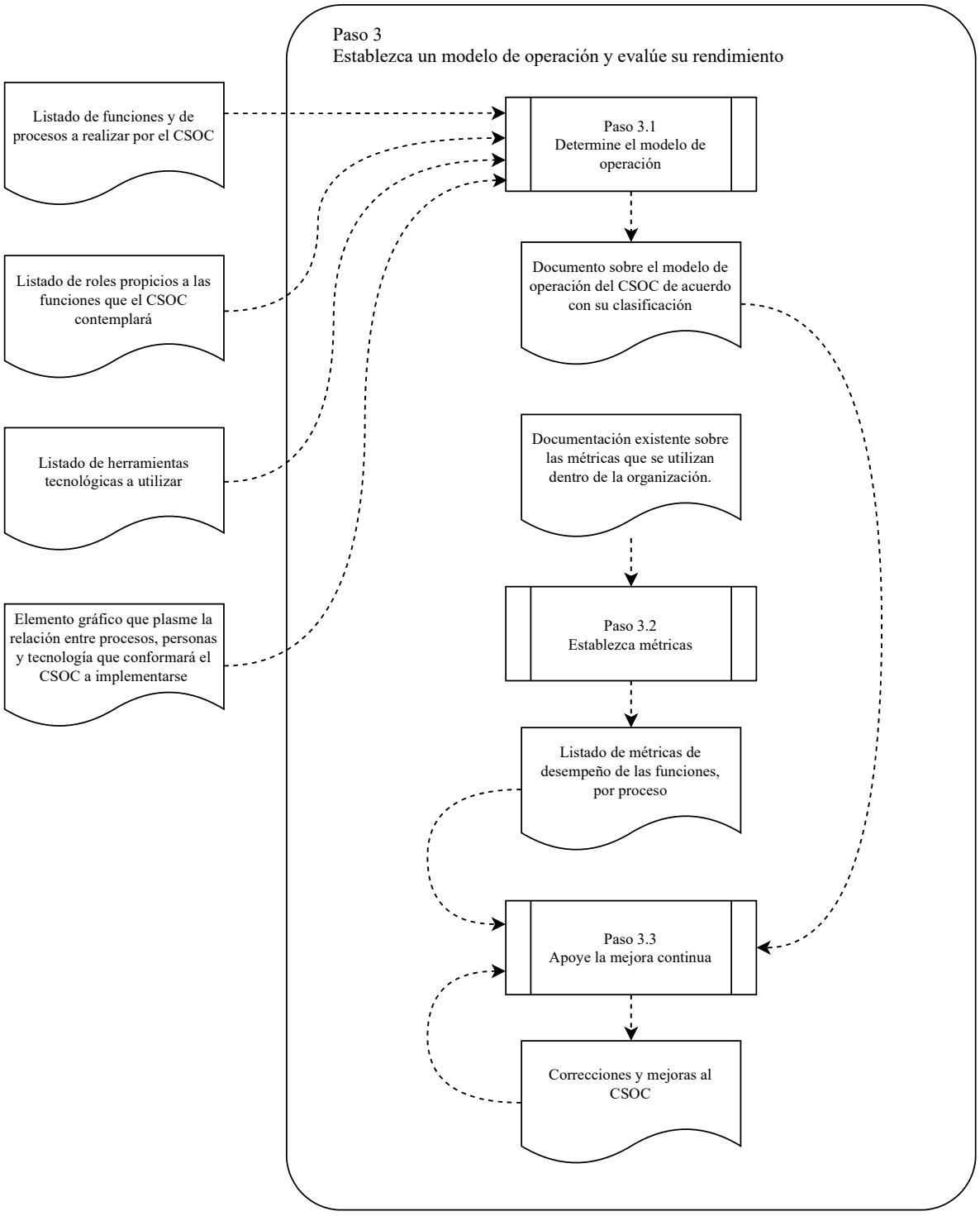

Figura 7 Diagrama de Flujo: Paso 3. Modelo de operación y evalúe su rendimiento. Elaboración propia.

Paso 3.1. Determine el modelo de operación

Entrada: Listado de funciones y de procesos a realizar por el CSOC, listado de roles propicios a las funciones que el CSOC contemplará, listado de herramientas tecnológicas a utilizar y Elemento gráfico que plasme la relación entre procesos, personas y tecnología que conformará el CSOC a implementarse.

Proceso: Para la determinación del modelo de operación del CSOC, se debería definir el alcance, misión y visión del CSOC este, seleccionando un modelo de operación que se acople a la realidad del negocio. Algunos de los modelos de los modelos de operación en la actualidad de acuerdo con sus características pueden clasificarse por:

1. Capacidad de contraataque o neutralización
    a. CSOC sin capacidad de contraataque: actúa como un clásico sistema de detección de intrusiones. monitorea y prioriza eventos relacionados a la seguridad de la información. En caso de que se detecte un ataque, no se ejecutan acciones en respuesta. Estos CSOC se utilizan generalmente en entornos con altas demandas de disponibilidad, por ejemplo, en la banca o la medicina.
    b. CSOC reactivo: utiliza el concepto de un sistema de prevención de intrusiones; el ataque no solo es detectado, sino que también se realizan funciones de mitigación para detener la propagación del ataque. El CSOC identifica todos los componentes del ataque, incluyendo las direcciones de los sistemas infractores y los comprometidos. Su capacidad de auto mitigación identifica los dispositivos con capacidad de realizar acciones sobre la ruta de

ataque y proporciona los comandos adecuados que pueden emplearse para mitigar el riesgo. Los resultados se pueden utilizar de forma precisa y rápida para prevenir o contener el ataque. Este tipo de CSOC se utiliza comúnmente en entornos con alta demanda de confidencialidad. Su capacidad de responder de forma rápida y automática ante las amenazas es su ventaja clave.

2. Escenarios de despliegue
    a. Centralizado: está basado en un dispositivo o servidor dedicado que realiza todas las actividades relacionadas con la gestión de la seguridad de la información. Ventajas: Velocidad, facilidad de instalación, y costo relativamente bajo. Desventaja: Es apropiado solo para entornos pequeños o medianos.
    b. Distribuido: utiliza varios dispositivos/servidores al mismo tiempo que realiza un equilibrio de carga entre ellos. La distribución de esta carga puede basarse en un principio geográfico (diferentes servidores son responsables de diferentes partes de la red) o en un principio funcional (parte de las funciones las realiza un servidor y otra parte las realiza otro). Debido a que se utilizan varios dispositivos, el costo del CSOC es mayor y el despliegue y el mantenimiento es más complejo, este equilibrio de carga da como resultado un mejor rendimiento y efectividad en general.

3. Objetivo o finalidad
    a. Controlado: permite observar el nivel de protección de los objetos de seguridad informática y pronosticar su cambio
    b. Administrado: ayuda a operar activamente los objetos de seguridad de la información.
    c. Crisis: solo comienza a actuar durante las crisis.
4. Técnicas de correlación
    a. Estadístico: aplica algoritmos estadísticos para determinar la severidad de incidentes de seguridad informática y, entonces asignar una puntuación de amenaza en función del valor de los activos. Analiza el comportamiento de la red e identifica amenazas basadas en la presencia y probable severidad de los patrones de eventos anómalos. También permite medir la efectividad, dado que la cantidad de eventos anómalos deberían disminuir con el tiempo a medida que el entorno de la infraestructura se vuelve más seguro.
    b. Basado en reglas: utiliza reglas predefinidas que aplican lógica condicional para identificar posibles escenarios de ataque mediante la observación de una serie especifica de eventos en un intervalo especifico dado. Las reglas pueden ser entregadas listas para usar por un proveedor o implementadas de manera personalizada después de un análisis cuidadoso del tráfico de red. Esta correlación es extremadamente eficaz para identificar amenazas en función del conocimiento previo de patrones de

ataque. Muchos productos implementan un conjunto finito de reglas que cubren escenarios comunes y estos pueden ampliarse con reglas personalizadas. La correlación efectiva depende del soporte del proveedor para mantener el estado de las reglas. Una regla debe ser un evento de larga duración y el motor de las reglas debe mantener los eventos *en estado* durante un período de tiempo razonable hasta que otros eventos de calificación activen una alerta o la regla expire para el evento inicial. Sin esto, se experimentarán numerosos falsos positivos, o lo que es más importante, no se identificarán ataques lentos y bajos que se caracterizan por una pequeña cantidad de eventos diarios durante un largo período de tiempo. Entre los inconvenientes se encuentran el tiempo que supone mantener actualizados cientos de reglas, demasiados falsos positivos y falsos negativos ante técnicas de ataque innovadoras.

c. Vulnerabilidad: toma los datos de los eventos de seguridad de los IDS de la red y los correlaciona contra una base de datos de vulnerabilidades conocidas y los perfiles de vulnerabilidades de los equipos devueltos por un escáner de vulnerabilidades, para determinar una puntuación de cada activo. Esto, ayuda a eliminar los falsos positivos y ayuda al equipo de seguridad a determinar cuáles ataques son reales y qué activos son realmente vulnerables. Ventajas: la más efectiva para detectar escenarios de ataque específicos, incluidos aquellos escenarios que pueden ser

nuevos para la infraestructura, y extremadamente buena para eliminar falsos positivos y maximizar la eficiencia al enfocarse en eventos de seguridad reales que corresponden a vulnerabilidades verdaderas. Desventajas: la creación de reglas para correlacionar ataques que explotan vulnerabilidades particulares de activos susceptibles es una tarea extremadamente laboriosa.

d. Acuerdo de nivel de servicio: vincula los eventos de seguridad a los requisitos establecidos en un SLA y es muy importante para las empresas porque ayuda a evaluar las pérdidas de los elementos de red comprometidos o los componentes que están fuera de servicio. El CSOC produce modelos de procesos de negocio y analiza el impacto en estos procesos desde diferentes incidentes de seguridad. Desventaja: La principal dificultad es la composición de procesos de negocio y la determinación del costo de los activos (las dificultades que son naturales para el análisis de riesgos orientado a procesos de tecnologías de información)
e. Cumplimiento: vincula los eventos de seguridad de la información a leyes, políticas y estándares de seguridad existentes (tanto corporativos como regulatorios). Necesita una instalación y configuración especial porque solo es posible una vinculación estática dado que cada infraestructura tiene su propia política de seguridad.

f. Mixto: Cuando todos los tipos de correlación se aplican juntos, pueden mejorar enormemente la detección de ataques reales y la eficacia de la gestión de seguridad de la información. Cuando el personal de seguridad puede obtener un perfil de riesgo unificado de eventos basado en una puntuación de amenaza estadística, alertas basadas en reglas, vulnerabilidades asociadas, y el valor de los activos, su trabajo es mucho más fácil.

g. Sin correlación: Apropiado para redes pequeñas donde solo se realiza agregación de datos de los eventos de seguridad y todas las decisiones las toma el equipo de seguridad.

5. Variantes de implementación

   a. Software: se basa en software especializado instalado en uno o más servidores. Ventaja: La posibilidad de utilizar los servidores que forman parte del CSOC para tareas adicionales.

   b. Hardware: es una solución lista para usar y basado en uno o varios servidores con software preinstalado. Ventaja: Menor tiempo de implementación. Desventaja: Dado que tiene un entorno aislado no puede instalarse software adicional en los servidores del CSOC.

   c. Solución de infraestructura: es construido utilizando software y hardware existente (por ejemplo, una base de datos existente es utilizada para el almacenamiento de eventos de seguridad de la información; la consolidación de bases de datos de seguridad se implementa mediante técnicas de replicación; y las

funcionalidades de normalización, agregación y correlación se implementan dentro de la base de datos mediante scripts SQL; etc.). Ventajas: bajo costo relativo de la solución y mayor flexibilidad. Desventajas: La necesidad de desarrollar el CSOC incluyen la normalización, agregación y reglas de correlación y programación SQL para implementar esas reglas.

6. Propiedad o tenencia
    a. Interno: Ventajas: El conocimiento de la infraestructura es mayor que cuando se subcontrata, más efectivo, las soluciones son más fáciles de personalizar, mayor probabilidad de identificar correlaciones entre los componentes de la infraestructura, mejores precios de las herramientas. Desventajas: Grandes inversiones iniciales, necesidad de mostrar eficacia rápidamente, alto potencial de un conflicto de interés en el equipo de monitoreo de intrusiones, menor probabilidad de reconocer patrones a gran escala como lo hacen terceras partes especializadas con muchos años de experiencia.
    b. Subcontratado: Ventajas: Sin gastos de capital, a menudo más barato, menor potencial para un conflicto de intereses en el equipo de monitoreo de intrusiones, imparcial, y con acuerdos de niveles de servicio. Desventajas: Menor conocimiento de la infraestructura; disminución en vigilancia del personal, riesgo de mal manejo de datos externos; ninguna ganancia a largo plazo para la infraestructura.

Puede auxiliarse del **Anexo H Matriz para la determinación del modelo de operación del CSOC** para definir los elementos básicos para la descripción del CSOC.

Nota: La información proveniente de este paso debe condensarse en un documento denominado “Modelo de operación del CSOC”, el cual servirá de consulta para conocer las tecnologías procesos y personas que se relacionan, en el **Anexo I Estructura para la construcción del Documento que describe el Modelo de Operación del CSOC.**, se visualiza un ejemplo de la estructura mínima del documento antes mencionado.

Salida: Documento sobre el modelo de operación del CSOC de acuerdo con su clasificación.

Paso 3.2. Establezca métricas.

Entrada: Documentación existente sobre las métricas que se utilizan dentro de la organización.

Proceso: Las métricas para evaluación del desempeño del CSOC son indicadores proveen información oportuna y útil para evaluar y controlar las funciones encomendadas con la finalidad de poder tomar decisiones que permitan mejorar de forma continua como se apoya a la estrategia del negocio. En un inicio, debería tomarse la documentación existente sobre las métricas que se utilizan dentro de la organización y validar si estas se relacionan a cada una de las funciones del CSOC a implementar. Posteriormente, debería proceder a establecer otras métricas no consideradas para cada una de las funciones.

Para poder establecer estas métricas puede utilizarse la metodología Objetivo – Pregunta – Métrica (del inglés Goal – Question – Metric, o GQM) que consiste en definir objetivos específicos, limitados, significativos, contextualizados

y documentados que el CSOC desea alcanzar; formular preguntas que permitan evaluar características específicas de las tecnologías, procesos y personas que conforman el CSOC; y métricas que permitan responder a estas preguntas de forma cuantitativa, entendible, validable, económica, repetible y comparable.

Se recomienda completar la tabla indicada en el **Anexo J Métricas por función**, en donde pueden listarse las métricas asociadas a cada función del CSOC.

Salida: Listado de métricas de desempeño de las funciones, por proceso.

Paso 3.3. Apoye la mejora continua.

Entrada: Documento sobre el modelo de operación del CSOC de acuerdo con su clasificación y listado de métricas de desempeño de las funciones por proceso.

Proceso: La organización debe realizar una revisión periódica de las funciones, de los procesos, de los roles, de las métricas y de las herramientas con el propósito de tomar acciones que permitan implementar mejoras que contribuyan a incrementar los resultados obtenidos sobre una base temporal contribuyendo de este modo al incremento continuo de la efectividad y eficiencia del CSOC.

Salida: Correcciones y Mejoras al CSOC.

6. Buenas Prácticas para un Centro de Operaciones de Ciberseguridad Efectivos.

En cuando a las buenas prácticas, estas pueden contemplar practicas referentes a gobierno, dirección, asignación financiera, y estrategias del CSOC, así como al Factor humano, tecnológico, procesos y su entorno de operación, en esta última práctica, se contemplan aspectos como espacio físico, medio ambiente y mejora continua.

A continuación, se lista el conjunto de buenas prácticas resultantes del análisis y discusión de los casos de éxitos recopilados, así como las referencias bibliográficas sobre la planeación, ejecución y monitoreo de un CSOC, dejar de lado de las buenas prácticas que tras la consulta de diversa bibliografía de las mejores prácticas que vale la pena comunicar por (Alahmadi, 2019) (Majid & Zainol Ariff, 2019) consisten en:

A. **Asegúrese de contar con el apoyo de la alta dirección.** *Para garantizar el funcionamiento y establecimiento de cultura de ciberseguridad de esta.*

B. **Gestione la asignación presupuestaria para el funcionamiento del CSOC.** *Para garantizar la operación de CSOC con recursos de última generación y apoyar a la tecnificación y capacitación continúa del personal que opera en la CSOC.*

C. **Establezca una estrategia para el CSOC**, ***que incluya una visión, misión y objetivos claros del contexto que aborden los riesgos existentes****. Para tener claras las funciones del CSOC y cumplir con las obligaciones de cumplimiento organizacional.*

D. **Asegúrese de contar con el talento humano capacitado y con las competencias requeridas por los roles desempeñados en el CSOC.** *Para garantizar la repuesta oportuna y efectiva a los incidentes de ciberseguridad por medio de personal con experiencia en la resolución de incidentes.*

E. Describa de forma clara los procesos bajos los cuales operará el CSOC

Para contar con la documentación básica que se trasmitirá a las partes interesadas y nuevas contrataciones, para acoplarse y comprender la forma de operar del CSOC y mantener su efectividad.

F. Seleccione la tecnología adecuada sacándole provecho a la existente e incorporando tecnología de acuerdo con los requisitos no cubiertos por la actual. *Para obtener el máximo rendimiento de las inversiones en tecnología.*

G. Asegúrese de apoyar al cumplimiento de los objetivos estratégicos de la organización priorizando la atención de incidentes. Para reaccionar de forma apropiada y eficaz.

H. Asegúrese de que el CSOC sea capaz de realizar el análisis de datos provenientes de múltiples sistemas y herramientas tecnológicas. *Para tener un panorama completo sobre los incidentes y producir informes completos para la respuesta de estos y toma de decisiones oportunas.*

I. **Elija una ubicación física segura y bien equipada para el funcionamiento del CSOC. C**ontar con un espacio o ubicación física determinada permite al personal que formara parte del CSOC una mejor coordinación para *acortar el tiempo de respuesta a un incidente y promover el intercambio de conocimientos, así como el trabajo en equipo.*

J. **Contemple un plan de capacitación continua en temas de ciberseguridad y evalue su desempeño.** *Para que las habilidades y el conocimiento del talento humano del CSOC, se mantenga actualizado en cuando al panorama de amenazas cibernéticas y las posibles acciones preventivas y correctivas que estas conlleven. Esta buen practica busca apoyar a la de Mejora continua del*

CSOC, mejorando las capacidades tecnológicas y su eficacia en la protección de la organización a todo nivel.

Conclusiones

i. La guía de implementación de un centro de operaciones de ciberseguridad con herramientas de código abierto es el abordaje inicial para la propuesta de un Marco de trabajo para el diseño, implementación y mejora continua de un Modelo de Centro de Operaciones de Ciberseguridad en la región.

ii. La decisión de implementar un centro de operaciones de ciberseguridad en las organizaciones debe tomar como punto de partida la concepción de un sistema de gestión de seguridad de la información, así como, la existencia de un análisis de riesgos previos, puesto que dicha implementación requiere lineamientos que los artefactos mencionados poseen.

iii. Si bien el buen diseño e implementación de un centro de Operación de Ciberseguridad aportan efectividad a las operaciones del negocio, se requiere hacer uso de buenas prácticas, para formalizar y operativizar el funcionamiento del CSOC, al cual hay que mantenerlo en mejora continua para que sus resultados sean cada vez más acertados y provechosos.

iv. El beneficio del uso de herramientas de código abierto para orquestar un centro de Operaciones de Ciberseguridad es el valor de la experiencia y conocimiento vertido por usuarios que contribuyen en la comunidad, así como, las adecuaciones que se puedan realizar a las herramientas, sin dejar de lado el costo de adquisición, el cual puede ser más bajo que herramientas con licencia de paga.

v. La guía que resulta de esta investigación es una respuesta a la ausencia de un marco de trabajo en la región que permita establecer el diseño, implementación y mejora continua de un CSOC compatible con los múltiples marcos de trabajo y normativas

existentes consultados y que han demostrado ser eficaces en diferentes entornos organizacionales.

vi. Un CSOC efectivo es la solución que toda organización busca para monitorear, prevenir y responder ante cualquier evento de ciberseguridad de interés y ciber amenaza que puede perjudicar a una organización, así como al consecuente impacto que, de materializarse un ciberataque, provocaría en términos financieros y reputacionales; sin embargo, la efectividad de estos CSOC se logra mediante la implementación de buenas prácticas que garanticen que la solución propuesta funciona de forma adecuada y asegura el cumplimiento de la triada de la ciberseguridad mediante la orquestación de sus componentes (el talento humano, las tecnologías y los procesos).

vii. Las herramientas tecnológicas que se utilizan en la operación de un CSOC comúnmente son de carácter especializado y de costo significativo, por lo que muchas veces, estas iniciativas se desarrollan bajo un enfoque de economías de escala donde la intención es dar servicio a múltiples instituciones u organizaciones; no obstante, la guía de implementación que se propone, considera múltiples iniciativas existentes en el entorno del software de código abierto que pueden ser utilizadas para apoyar las funciones y procesos de iniciativas ad hoc a cualquier tipo de negocio que procure la seguridad de sus activos de información.

Anexos

Anexo A Listado de documentos que describen el contexto de operación del negocio

DOCUMENTO	ELEMENTO	DESCRIPCIÓN DE ELEMENTOS DEL CONTEXTO
Documento 1	- Elemento 1 - Elemento 2 - Elemento n	- Detalle del elemento 1 - Detalle del elemento 2 - Detalle del elemento n
Documento 2	- Elemento 1 - Elemento 2 - Elemento n	- Detalle del elemento 1 - Detalle del elemento 2 - Detalle del elemento n
Documento n	- Elemento 1 - Elemento 2 - Elemento n	- Detalle del elemento 1 - Detalle del elemento 2 - Detalle del elemento n

Ejemplo de llenado de matriz que describe el contexto de operación del negocio:

DOCUMENTO	ELEMENTO	DESCRIPCIÓN DEL ELEMENTO DEL CONTEXTO
Manual de Procedimiento	Misión	Escriba el contenido de la misión de la organización: Ej. "Organizar la información de mundo y hacerla accesible a todos"
	Visión	Escriba el contenido de la visión de la organización:
	Valores	Escriba el contenido de los valores de la organización:
	Objetivos Estratégicos	Liste los objetivos estratégicos de la organización.
Manual del sistema de Gestión de Seguridad de la Información	Inventario de activos de información	Indique la lista de activos de información críticos y su descripción
	Políticas de seguridad de la información.	Mencione las Políticas que contribuyan al establecimiento de reglas y acciones parara el funcionamiento del CSOC
	Procedimientos para la Gestión de incidentes	Liste los procedimientos aplicables a la implementación del CSOC

Anexo B Matriz de análisis de fuentes de información para la identificación de amenazas.

FUENTES DE INFORMACIÓN	TIPO	CRITERIO PARA SU SELECCIÓN	AMENAZA QUE AFECTA A LA ORGANIZACIÓN
Fuentes de información 1	- Tipo de fuente información 1 - Tipo de fuente información 2 - Tipo de fuente información n	- Criterio de selección 1 - Criterio de selección 2 - Criterio de selección n	- Amenaza 1 - Amenaza 2 - Amenaza n
Fuentes de información 2	- Tipo de fuente información 1 - Tipo de fuente información 2 - Tipo de fuente información n	- Criterio de selección 1 - Criterio de selección 2 - Criterio de selección n	- Amenaza 1 - Amenaza 2 - Amenaza n
Fuentes de información n	- Tipo de fuente información 1 - Tipo de fuente información 2 - Tipo de fuente información n	- Criterio de selección 1 - Criterio de selección 2 - Criterio de selección n	- Amenaza 1 - Amenaza 2 - Amenaza n

Ejemplo de llenado de matriz de análisis de fuentes de información para la identificación de amenazas:

MATRIZ.

FUENTES DE INFORMACIÓN	**TIPO**	**CRITERIO PARA SU SELECCIÓN**	**AMENAZA QUE AFECTA A LA ORGANIZACIÓN**
- Observatorio de la Ciberseguridad en América Latina y el Caribe (BID y OEA).	- Documentación técnica publicada por organización de ciberseguridad	- Relación con las amenazas - Impactos reputaciones. - Política nacional de ciberseguridad.	- Hackers - Ciber criminales - Ciber terroristas - Funcionarios molestos.

Anexo C Matriz de asignación de procesos por funciones.

FUNCIÓN	PROCESO	DETALLE DEL PROCESO
Función 1	- Proceso 1	- Detalle del proceso 1
	- Proceso 2	- Detalle del proceso 2
	- Proceso n	- Detalle del proceso n
Función 2	- Proceso 1	- Detalle del proceso 1
	- Proceso 2	- Detalle del proceso 2
	- Proceso n	- Detalle del proceso n
Función n	- Proceso 1	- Detalle del proceso 1
	- Proceso 2	- Detalle del proceso 2
	- Proceso n	- Detalle del proceso n

Un ejemplo de cómo la matriz anterior debe completarse es el siguiente:

FUNCIÓN	PROCESO	DETALLE DEL PROCESO
Monitoreo y detección de eventos de seguridad:	Prevención de incidentes	**¿Qué hace?** Busca prevenir la ocurrencia de incidentes de ciberseguridad. **¿Cómo lo realiza?** Mediante la revisión periódica de los planes, políticas y controles de ciberseguridad, se establece un plan de capacitación, pruebas de penetración y auditorias, para posteriormente ejecutarlas, a fin de reducir la probabilidad de ocurrencia e impacto de un incidente de ciberseguridad. **¿Con que recursos?** Estas actividades se llevan a cabo con la intervención del analista de seguridad, el coordinador o líder del CSOC y dirección de la organización **¿Bajo qué propósito se?** Para la reducción de la probabilidad de ocurrencia e impacto de un incidente de ciberseguridad. **----** *"Busca prevenir la ocurrencia de incidentes de ciberseguridad.* *Mediante la revisión periódica de los planes, políticas y controles de ciberseguridad, se establece un plan de capacitación, pruebas de penetración y auditorias, para posteriormente ejecutarlas, a fin de reducir la probabilidad de ocurrencia e impacto de un incidente de ciberseguridad.*

		Estas actividades se llevan a cabo con la intervención del analista de seguridad, el coordinador o líder del CSOC y dirección de la organización *Para la reducción de la probabilidad de ocurrencia e impacto de un incidente de ciberseguridad "*
	Monitoreo de eventos de ciberseguridad	Busca detectar la ocurrencia de actividades maliciosas o anormales. Revisando constantemente los dashboards creados con los registros de actividades de la organización, se priorizará los eventos asociados a las métricas que indican una actividad maliciosa dentro de la organización, se levantará el incidente y será asignado para su resolución. Para lo antes descrito, será necesaria la intervención de un analista de seguridad para la detección de eventos y la resolución del incidente. Todo con el propósito de identificar y asignación en tiempo real incidentes de ciberseguridad, para una repuesta oportuna

Anexo D Tabla de roles, funciones y competencias requeridas para el centro de operaciones de ciberseguridad.

Roles	***Descripción***	***Funciones***	***Competencias Requeridas***
Rol 1	Descripción Rol 1	• Función 1 • Función 2 … • Función n	• Competencia 1 • Competencia 2 … • Competencia n
Rol 2	Descripción Rol 2	• Función 1 • Función 2 … • Función n	• Competencia 1 • Competencia 2 … • Competencia n
Rol 3	Descripción Rol 3	• Función 1 • Función 2 … • Función n	• Competencia 1 • Competencia 2 … • Competencia n
Rol n	Descripción Rol n	• Función 1 • Función 2 … • Función n	• Competencia 1 • Competencia 2 … • Competencia n

Se recomienda incorporar roles al CSOC bajo las especificaciones siguientes:

1. Director del CSOC: debe ser capaz de dirigir y gestionar las personas y tecnología que se relación con el CSOC (Jefe del CSOC)
2. Personal Operativo del CSOC: debe ser capaz de realizar las funciones que hayan decidido del CSOC (Analista de Seguridad de Nivel 1y2)
3. Personal Técnico: debe ser capaz de dar solución a los incidentes gestionados por el CSOC. (Analista de seguridad de Nivel 3)

Un ejemplo de cómo el formato anterior debe completarse es el siguiente:

TABLA DE ROLES, FUNCIONES Y COMPETENCIAS REQUERIDAS PARA EL CENTRO DE OPERACIONES DE CIBERSEGURIDAD.

Roles	***Descripción***	***Funciones***	***Competencias Requeridas***
Jefe del CSOC	Capaz de velar por el cumplimiento de las funciones del centro de operaciones de ciberseguridad.	- Comunicación con otras áreas y la alta dirección - Cumplimiento y gestión del riesgo tecnológico	- Capacidad de Negociación - Toma de decisiones. - Análisis de riesgos tecnológicos. - Comunicación efectiva - Gestión de los servicios del CSOC - Gestión de desempeño - Planificación de mejora continua
Analista de seguridad de nivel 1	Capaz de identificar eventos de seguridad que sean de interés	- Monitoreo y detección de eventos de seguridad. - Análisis de los eventos de seguridad	- Análisis de riesgos tecnológicos

Roles	***Descripción***	***Funciones***	***Competencias Requeridas***
Analista de seguridad de nivel 2	Capaz de priorizar los eventos de ciberseguridad y dar respuesta a los incidentes asignados	- Respuesta e informe sobre los eventos de seguridad. - Ciber inteligencia. - Gestión de incidentes de ciberseguridad.	- Comunicación efectiva
Analista de seguridad de nivel 3	Capaz de identificar vulnerabilidades y efectuar pruebas de penetración, para el ajuste de herramientas y resolución de incidentes escalados por el analista de seguridad 2	- Gestión de vulnerabilidades. - Gestión de políticas y firmas de equipos de ciberseguridad - Ejecución de pruebas de penetración - Análisis forense	- Gestión de investigaciones forenses - Conocimientos avanzados de comunicaciones, seguridad informática, programación.

Anexo E. Herramientas de código abierto para la construcción de un CSOC.

Función	Categoría de Herramientas	Herramienta Propuesta	Apoyo a la Operación del CSOC
Monitoreo y detección	Captura y análisis de tráfico de red	• Malcolm https://github.com/cisagov/Malcolm • Wireshark https://www.wireshark.org	Estas herramientas de captura de trafico de red benefician a la operación del CSOC permitiendo capturar y analizar tráfico atípico en la red que está bajo la responsabilidad del área de ciberseguridad.
	Sistemas de detección/prevención de intrusiones	• Snort https://www.snort.org • Suricata https://suricata.io	Esta categoría de herramientas permite al CSOC contar con la capacidad de poder monitorear continuamente el tráfico de red y analizarlo en tiempo real con el propósito de detectar cualquier tráfico atípico o característico de ataques que puedan perjudicar los activos de información que bajo la operación se desean proteger. También, le proveen de capacidad para automatizar y ejecutar acciones específicas sobre las detecciones realizadas.

	Sistemas de gestión de eventos de información de seguridad	• ELK Stack https://www.elastic.co/what-is/elk-stack • SIEMonster https://siemonster.com • Alienvault OSSIM https://cybersecurity.att.com/products/ossim	El principal beneficio que estas herramientas proporcionan al CSOC, es la capacidad de contar con un lugar de almacenamiento centralizado para poder colectar información sobre todos los eventos de interés a la ciberseguridad que es generada por todos los equipos objeto de monitoreo. Asimismo, le permite correlacionar eventos que permitan agilizar la detección de ciberataques. Y ejecutar acciones en respuesta a estos.
Análisis de eventos de ciberseguridad	Herramientas de inspección visual y procesamiento de datos	• ELK Stack https://www.elastic.co/what-is/elk-stack • SIEMonster https://siemonster.com • Alienvault OSSIM https://cybersecurity.att.com/products/ossim	Las herramientas de inspección y procesamiento de los datos recolectados permiten al CSOC realizar investigaciones de alto nivel sobre los logs, alertas, paquetes de tráfico de red, y eventos procesados con el propósito de identificar, patrones, tendencias y causas de las actividades anómalas o maliciosas que puedan considerarse una amenaza para la organización.

Respuesta e informe sobre eventos de ciberseguridad	Sistema de gestión de tiquetes y asistencia técnica	• Uvdesk Community Helpdesk https://github.com/uvdesk/community-skeleton	Herramientas que pertenecen a esta categoría permiten al CSOC dar soporte a los diferentes a sus procesos relacionados a la operación de la seguridad enfocado como servicio: solicitudes de cambios, gestión de incidentes y gestión de cambios, y reportes.
Ciber inteligencia	Noticias	• CyberNews https://cybernews.com	La función de ciber inteligencia se beneficia de herramientas que permitan consultar noticias de ciberseguridad al poder identificar eventos que puedan afectar al negocio al que se debe el CSOC.
	Redes sociales, sitios especializados y boletines electrónicos	• Cybersecurity & Infrastructure Security Agency Newsletters https://www.cisa.gov/publication/newsletters • SANS Internet Storm Center https://isc.sans.edu	Al consumir servicios ofrecidos por sitios especializados o utilizar boletines, el CSOC puede ganar ventaja de forma proactiva sobre posibles atacantes al conocer de primera mano vulnerabilidades que afectan a la infraestructura que debe proteger.
	Plataformas centralizadas de inteligencia de amenazas	• Collaborative Research into Threats https://crits.github.io • GOSINT https://github.com/ciscocsirt/GOSINT • Your Everyday Threat Intelligence https://yeti-platform.github.io	El uso de plataformas centralizadas de ciber inteligencia facilitan al CSOC la realización de tareas cotidianas como la integración, enriquecimiento y

			calificación de la información obtenida de diversas fuentes con la finalidad d responder a las amenazas en la medida en que estas ocurren.
Gestión de incidentes de ciberseguridad	Sistemas de gestión y control de tiquetes	• Uvdesk Community Helpdesk https://github.com/uvdesk/community-skeleton	Los sistemas de gestión y control de tiquetes ayudan al CSOC a documentar todos aquellos eventos de interés para la ciberseguridad que han ameritado de algún tipo de tratamiento bajo su operación. Esta documentación se relaciona a todas las acciones tomadas durante la ejecución de las fases del proceso de gestión de incidentes de seguridad. Estos sistemas también sirven como fundamento tecnológico para todos los procesos que el CSOC realiza según las funciones que debe ejecutar en la organización.
Línea base y vulnerabilidades	Gestores y escáneres de vulnerabilidades	• OpenVAS https://www.openvas.org	Para dar operatividad a las políticas de seguridad que establecen características específicas que deben poseer los activos informáticos, el CSOC se apoya en los gestores y escáneres de vulnerabilidades

			para determinar variaciones con respecto a la línea base de configuración y para identificar vulnerabilidades que pueden ser aprovechadas por atacantes.
	Sistemas de gestión de parchado	• Local Update Publisher http://www.localupdatepublisher.com • Patchman https://github.com/furlongm/patchman	El CSOC se auxilia de estos sistemas de gestión de parchado para aplicar parches y configuraciones que conduzcas a la eliminación o mitigación de vulnerabilidades detectadas en los activos informáticos.
Gestión de políticas y firmas de equipos de ciberseguridad	Interfaces centralizadas o individuales de gestión de dispositivos y aplicaciones de seguridad	• FirewallBuider http://fwbuilder.sourceforge.net • rConfig https://www.rconfig.com	Dentro de la operación del CSOC se requiere de herramientas que permitan realizar cambios a las políticas y las firmas de los equipos de ciberseguridad con el propósito de responder adecuadamente a ataques cibernéticos. El uso de estas herramientas ayuda al CSOC a implementar estos cambios de forma rápida y simplificada.
Cumplimiento y gestión del riesgo	Escáneres de cumplimiento	• Lynis https://github.com/CISOfy/lynis	Los escáneres de cumplimiento ayudan al CSOC a cumplir y gestionar el riesgo. De forma específica, ayudan a determinar ajustes de

			configuración que necesitan ser aplicados en los sistemas de redes computaciones cuya protección está a cargo del CSOC para que la organización pueda ajustarse a marcos de trabajo específicos.
Ejecución de pruebas de penetración	Herramientas de pruebas de penetración	• Kali Linux https://www.kali.org • Parrot OS https://www.parrotsec.org	El uso de herramientas para ejecutar pruebas de penetración, permiten al CSOC evaluar la efectividad de las medidas de seguridad implementadas para proteger los activos informáticos que tiene como misión proteger.
Forense y malware	Tecnologías de Sandboxing	• Cuckoo Sandbox https://cuckoosandbox.org • Sandboxie-plus https://sandboxie-plus.com	Los CSOC que requieren desarrollar funciones avanzadas como el análisis de software malicioso para comprender su comportamiento se auxilian de las herramientas de sandboxing para contar con entornos aislados y controlados para tal fin.
	Plataformas y herramientas de análisis forense digital	• Autopsy https://www.autopsy.com/	Los CSOC que necesitan dar operatividad a la función de análisis forense digital utilizan estas herramientas forenses para obtener y preservar evidencias digitales de artefactos relacionados a actividades maliciosas.

Anexo F Tabla de herramientas a utilizar para el cumplimiento de las funciones.

Función CSOC	Categoría de Herramienta	Herramientas Necesarias	Herramientas Existentes
Función 1	Categoría X	Herramienta a	Herramienta f
	Categoría Y	Herramienta b	Herramienta f
Función n	Categoría Z	Herramienta c	Herramienta f
	Categoría W	Herramienta a	Herramienta f

Ejemplo de llenado de tabla para la identificación de herramientas del CSOC

TABLA DE HERRAMIETAS A UTILIZAR PARA EL CUMPLIMIENTO DE LAS FUNCIONES.

Función CSOC	Categoría de Herramienta	Herramientas Existentes	Herramientas necesarias
Monitoreo y detección	Herramientas de captura y análisis de tráfico de red	- WIRESHARK	- MALCOLM
	Sistemas de detección/prevención de intrusiones.	- SNORT	-
Análisis	Herramientas de inspección visual y procesamiento de datos	- McAfee SIEM	- ELK

Anexo G Modelo de referencia para la infraestructura de un centro de operaciones de ciberseguridad

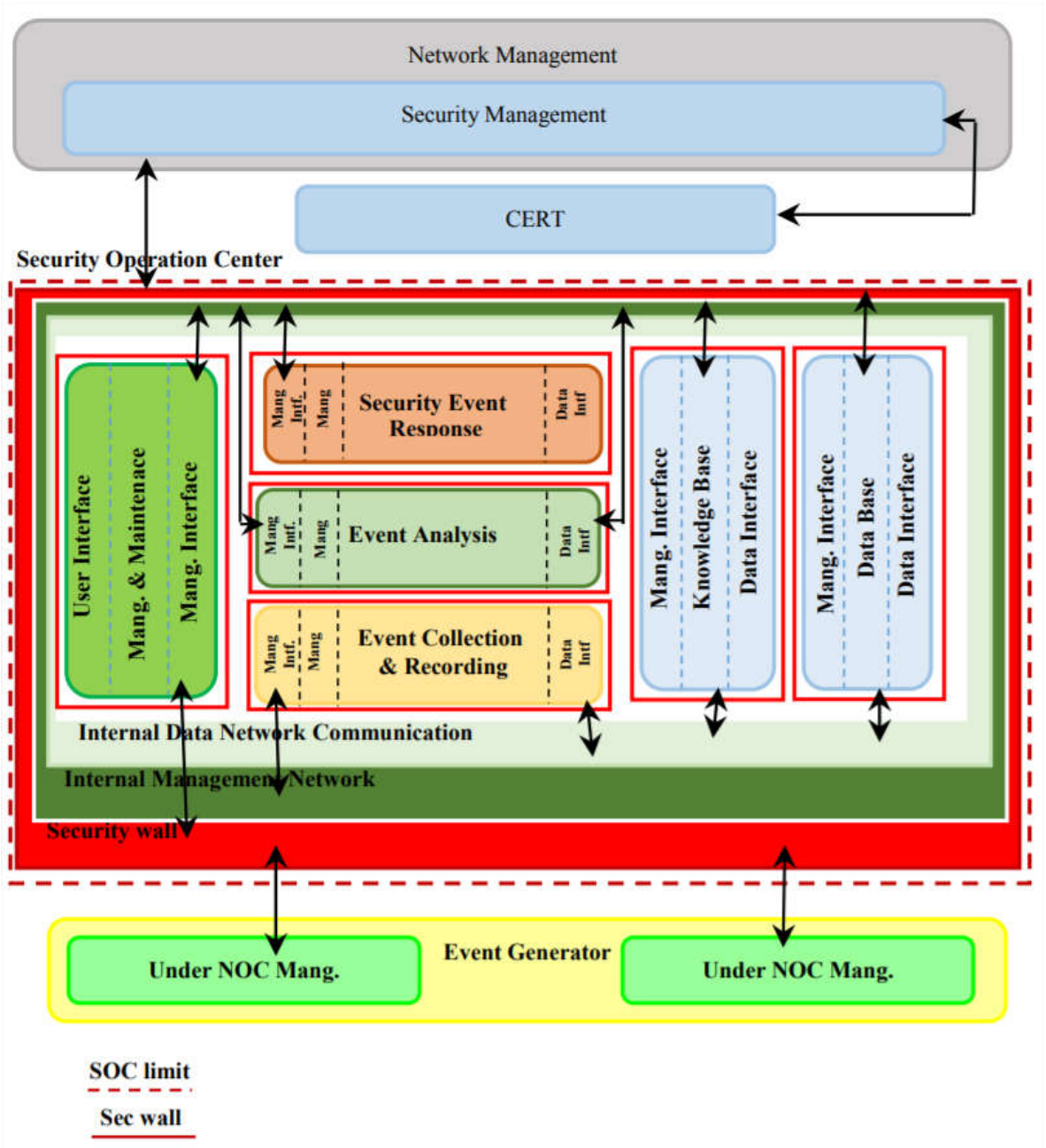

Figura 8. Modelo de referencia para la infraestructura de un centro de operaciones de ciberseguridad.

Fuente: (Tafazzoli & Gharaee Garakani, 2016).

Anexo H Matriz para la determinación del modelo de operación del CSOC

ELEMENTO DEL CSOC	DETALLE
Misión	*Definición de la Misión del CSOC*
Visión	*Definición de la Visión del CSOC*
Alcance	*Delimitación del alcance del CSOC*
Identificación del CSOC	**Capacidad de contraataque o neutralización:**
	Escenarios de despliegue:
	Objetivo o finalidad:
	Técnicas de correlación:
	Variantes de implementación:
	Propiedad o tenencia:

Anexo I Estructura para la construcción del Documento que describe el Modelo de Operación del CSOC.

PORTADA

VERSIONAMIENTO DEL DOCUMENTO

1. CONTEXTO DE LA ORGANIZACIÓN
    - 1.1.MISIÓN, VISIÓN, VALORES
    - 1.2.OBJETIVOS ESTRATÉGICOS
    - 1.3.NORMATIVA ASOCIADA A LA SEGURIDAD DE LA INFORMACIÓN
    - 1.4.PANORAMA DE AMENAZAS
2. MODELO DE OPERACIÓN DEL CSOC
    - 2.1.MISIÓN, VISIÓN Y ALCANCE DEL CSOC
    - 2.2.CLASIFICACIÓN DEL CSOC
3. COMPONENTES DEL CSOC
    - 3.1.FUNCIONES Y PROCESOS DEL CSOC
    - 3.2.ROLES DEL CSOC
    - 3.3.HERRAMIENTAS DEL CSOC
    - 3.4.METRICAS
4. MODELO DE INFRAESTRUCTURA DEL CSOC

Anexo J Métricas por función

Función	Proceso	Objetivo	Pregunta	Métrica (por función)
Función 1	- Proceso 1 - Proceso 2 - Proceso n	- Objetivo 1 - Objetivo 2 - Objetivo n	- Pregunta 1 - Pregunta 2 - Pregunta n	- Métrica del proceso 1 - Métrica del proceso 2 - Métrica del proceso n
Función 2	- Proceso 1 - Proceso 2 - Proceso n	- Objetivo 1 - Objetivo 2 - Objetivo n	- Pregunta 1 - Pregunta 2 - Pregunta n	- Métrica del proceso 1 - Métrica del proceso 2 - Métrica del proceso n
Función n	- Proceso 1 - Proceso 2 - Proceso n	- Objetivo 1 - Objetivo 2 - Objetivo n	- Pregunta 1 - Pregunta 2 - Pregunta n	- Métrica del proceso 1 - Métrica del proceso 2 - Métrica del proceso n

Un ejemplo de cómo el formato anterior debe completarse es el siguiente:

MÉTRICAS POR FUNCIÓN

Función	Proceso	Métrica (por función)
Monitoreo y detección	- Clasificación de incidentes	- Número de falsos positivos - Número de falsos negativos - Número de verdaderos positivos - Número de verdaderos negativos - Tiempo Promedio de detección
Análisis	- Gestión de registros	- Frecuencia de análisis de registros de auditoría para actividad inapropiadas - Ataques externos por origen geográfico - Ataques por severidad - Número de campañas de ataques dirigidas contra el Ministerio de Hacienda. - Eventos de seguridad relacionados a exfiltración de datos
Función n	- Proceso n	- Función n

Referencias

AXELOS. (Enero de 2019). *Glosario ITIL*. Obtenido de ITIL® Foundation: https://itservice.com.co/wp-content/uploads/Glosario-términos-y-definiciones-ITIL-4.pdf

Agyepong, E., Cherdantseva, Y., Reinecke, P., & Burnap, P. (15 de junio de 2020). Towards a Framework for Measuring the Performance of a Security Operations Center Analyst [Hacia un Marco de Trabajo para Medir el Desempeño de un Analista de Centro de Operaciones de Seguridad]. *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security).* Dublin, Irlanda: Institute of Electrical and Electronics Engineers (IEEE). doi:10.1109/CyberSecurity49315.2020.9138872

AlAhmadi, B. A. (2019). *Malware detection in security operation centres [PhD thesis]*. Michaelmas, Estados Unidos: University of Oxford.

Alahmadi, B. A. (2019). Malware Detection in Security Operation Centres. Oxford, Inglaterra: University of Oxford.

Álvarez, M. (09 de septiembre de 2020). *UST*. Obtenido de https://www.ust.com/es/insights/la-evolucion-del-soc-ante-el-nuevo-modelo-de-amenazas

ANTÓN ZAMBRANO, L. A., & ARIEL, M. L. (2020). *UNIVERSIDAD DE GUAYAQUIL.* Obtenido de UNIVERSIDAD DE GUAYAQUIL: http://repositorio.ug.edu.ec/bitstream/redug/49439/1/B-CINT-PTG-N.556%20Antón%20Zambrano%20Lenín%20Alejandro%20.%20Mosquera%20Litardo%20Anthony%20Ariel%20.pdf

B Secure. (2016). *B SECURE*. Obtenido de view-source:https://www.b-secure.co/centro-de-operaciones-de-ciberseguridad-csoc

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (Agosto de 2012). *National Institute of Standards and Technology.* Obtenido de National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Clavei.es. (16 de Abril de 2018). *Clavei.es*. Obtenido de https://www.clavei.es/blog/que-es-un-ids-o-intrusion-detection-system/

Compris Technologies AG. (2021). Open Source Security Operations Center (OS SOC) Architecture based on a Zero-Trust Model. Steinhausen, Suiza: Compris Technologies AG.

Concha, F. (Abril de 2019). *A2 Secure*. Obtenido de A2 Secure Web Site: https://www.a2secure.com/blog/ids-ips-hids-nips-siem-que-es-esto/

Cyber Intelligence Agency. (09 de septiembre de 2016). *Designing the Next Generation Cyber Security Operations Center (CSOC)*. Obtenido de CIA Botswana: https://www.ciabotswana.com/designing-next-generation-cyber-security-operations-center-csoc/

Director-IT. (2019). *Director-IT*. Obtenido de http://director-it.com/index.php/es/ssoluciones/seguridad/firewall-y-dmz/118-que-es-un-waf-web-application-firewall.html

DITECH. (Mayo de 2010). *DITECH*. Obtenido de http://ditech.com.co/soluciones-integrales/seguridad-informatica-en-redes/prevencion-de-intrusos-ips-2/

Figueroa Alemán, O. S., & Masache Narváez, V. E. (2018). *Análisis de tecnología de un centro de operaciones de ciberseguridad para un proveedor de servvicios de internet.* Quito: UNIVERSIDAD DE LAS AMÉRICA, "CARLOS LARREÁTEGUI MENDIETA".

Obtenido de http://dspace.udla.edu.ec/jspui/bitstream/33000/10041/1/UDLA-EC-TIRT-2018-16.pdf

HP ESP Security Intelligence and Operations Consulting Services. (2013). *Business White Paper: 5G/SOC: SOC Generations.* Estados Unidos: Hewlett-Packard Development Company, L.P.

IBM Corporation. (Diciembre de 2013). *IBM.* Obtenido de IBM Corporation: https://www.ibm.com/downloads/cas/1ZO3JEBZ

ISO. (2018). *INTERNATIONAL INTERNATIONAL ISO/IEC 27000:2018.* Switzerland. Obtenido de ISO 2700: https://www.iso27000.es/glosario.html

Kent, K., & Souppaya, M. (Septiembre de 2006). *National Institute of Standar and Technology.* Obtenido de National Institute of Standar and Technology: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

Kokulu, F. B., Soneji, A., Bao, T., Shoshitaishvili, Y., Ziming, Z., Doupé, A., & Ahn, G.-J. (2019). Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues. *Conference on Computer and Communications Security.* Londres: Association for Computing Machinery.

Majid, M., & Zainol Ariff, K. (2019). *European Union Digital Library.* Obtenido de https://eudl.eu/pdf/10.4108/eai.18-7-2019.2287841

Mccoy, S., & Jarpey, G. (2017). *Security Operations Center Guidebook: A Practical Guide for a Successful SOC.* Butterworth-Heinemann.

Mendez Fonseca, V. J. (2019). *Universidad Piloto de Colombia* . Obtenido de http://repository.unipiloto.edu.co/handle/20.500.12277/7937

Microsoft. (15 de 05 de 2020). *Microsoft.com*. Obtenido de https://docs.microsoft.com/es-es/azure/cloud-adoption-framework/organize/cloud-security-operations-center

Miloslavskaya, N. (Agosto de 2016). Security Operations Centers for Information Security Incident Management [Centros de Operaciones de Seguridad para la Gestión de Incidentes de Seguridad de la Información]. *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)* (págs. 131-136). Vienna, Austria: Institute of Electrical and Electronics Engineers (IEEE). doi:10.1109/FiCloud.2016.26

MORALES GONZÁLES, C. A., MORENO SÁNCHEZ, O. E., & ORTIGOZA PÉREZ, J. N. (2014). *PROPUESTA DE UN MODELO DE CENTRO DE OPERACIONES DE SEGURIDAD SOC PARA LA FUERZA AEREA COLOMBIANA.* BOGOTÁ: UNIVERSIDAD PILOTO DE COLOMBIA.

Morillas, C., & Raggi, N. (30 de Octubre de 2019). *Centro de Operaciones de Seguridad al Servicio del Negocio.* Obtenido de slideshare: https://es.slideshare.net/NicolsEzequielRaggi/centros-de-operaciones-de-seguridad-al-servicio-del-negocio

Mutemwa, M., Mtsweni, J., & Zimba, L. (2018). Integrating a Security Operations Centre with an Organization's Existing Procedures, Policies, and Information Technology Systems [Integrando un Centro de Operaciones de Seguridad con los Procedimientos, Políticas y Sistemas de una Organización]. *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)* (págs. 177-182). Mon Tresor, Mauricio: Institute of Electrical and Electronics Engineers (IEEE). doi:10.1109/ICONIC.2018.8601251

Onwubiko, C. (2015). Cyber Security Operations Centre: Security Monitoring for Protecting Business and Supporting Cyber Defense Strategy [Centro de Operaciones de Ciberseguridad: Monitoreo de la Seguridad para la Protección del Negocio y Apoyo a la Estrategia de Ciberdefensa]. *2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA).* Londres, Reino Unido: Institute of Electrical and Electronics Engineers (IEEE). doi:10.1109/CyberSA.2015.7166125

Oracle. (mayo de 2021). *Oracle* . Obtenido de https://www.oracle.com/es/database/security/que-es-un-waf.html#:~:text=Un%20Web%20Application%20Firewall%20(WAF,HTTPS%20y%20modelos%20de%20tr%C3%A1fico.&text=en%20el%20software%3A%20instalando%20una%20aplicaci%C3%B3n%20en%20el%20sistema%20operativo

Schinagl, S., Schoon, K., & Paans, R. (2015). A Framework for Designing a Security Operations Centre (SOC) [Un Marco de Trabajo para el Diseño de un Centro de Operaciones de Seguridad]. *Secure Cyberspace in 21st Century. Proceedings of the Hawaii International Conference on System Sciences (HICSS)* (págs. 2253-2262). Kauai, HI, USA: Institute of Electrical and Electronics Engineers (IEEE). doi:10.1109/HICSS.2015.270

Tafazzoli, T., & Gharaee Garakani, H. (Septiembre de 2016). *Researchgate.* Obtenido de ResearchGate GmbH: https://www.researchgate.net/profile/Tala-Tafazzoli/publication/315471789_Security_operation_center_implementation_on_OpenStack/links/5d1adf5492851cf4405ca050/Security-operation-center-implementation-on-OpenStack.pdf

Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). Security Operations Center: A Systematic Study and Open Challenges [Centro de Operaciones de Seguridad: Un

Estudio Sistemático y Desafíos Abiertos]. *IEEE Access, 8*, 227756-227779. doi:10.1109/ACCESS.2020.3045514

Wierzbieniec, G. (2018). *Architecture and design requirements for Enterprise Security Monitoring Platform.* Luleå: Lulea university of technology.