ANÁLISIS DE SOLUCIONES PARA EL MONITOREO DE SEGURIDAD ACTIVA Y PASIVA DE INFRAESTRUCTURAS TECNOLÓGICAS APOYADO EN UN SERVICIO DE SOC

JULIAN DAVID MORA MONTOYA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLIN
2021

ANÁLISIS DE SOLUCIONES PARA EL MONITOREO DE SEGURIDAD ACTIVA Y PASIVA DE INFRAESTRUCTURAS TECNOLÓGICAS APOYADO EN UN SERVICIO DE SOC

JULIAN DAVID MORA MONTOYA

PROYECTO DE GRADO – MONOGRAFÍA PRESENTADO PARA OPTAR POR EL TÍTULO DE
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Asesora
YOLIMA ESTHER MERCADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLIN
2021

NOTA DE ACEPTACIÓN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Con amor dedico este trabajo a mis padres, que con su apoyo y comprensión me han acompañado en cada etapa vivida, colaborándome de manera indirecta, minimizando mis preocupaciones, también lo dedico a mi esposa que con su apoyo, consagración y paciencia me ha brindado su acompañamiento haciendo que el desarrollo de las actividades sea posible, también a la empresa para la cual trabajo actualmente que me ha brindado su apoyo económico para el desarrollo de la especialización y la asesora y tutora Yolima Ester Mercado por su orientación, apoyo y acompañamiento durante el desarrollo del trabajo.

AGRADECIMIENTOS

Agradezco profundamente a mis amigos, familiares y compañeros que con su apoyo han hecho posible el desarrollo de las diferentes actividades, agradezco también a la universidad por crear los espacios y las posibilidades para que se puedan llevar a cabo los estudios de manera virtual, lo cual facilita en gran parte el llevar la educación a más lugares.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ILUSTRACIONES

Pág.

LISTA DE ANEXOS

pág.

GLOSARIO

AMENAZA Se puede entender como amenaza una situación desfavorable que pueda generar una afectación en los servicios, lo cual podrá generar una indisponibilidad o afectación en el funcionamiento normal de los servicios,

ATAQUE ACTIVO Este tipo de ataques generan una alteración en el flujo de los datos para realizar cambios de manera no autorizada.

ATAQUE DE FUERZA BRUTA Este tipo de ataques como su nombre lo indica generan ataques mediante la ejecución de acciones repetitivas hasta lograr la alteración de un sistema, ejemplo, ejecución de contraseñas diferentes de manera repetitiva hasta obtener la real.

CIBERATAQUE Ataque a los sistemas de información generado a través de la red de telecomunicaciones.

CIBERDELINCUENTE Atacante que genera alteraciones a los sistemas de información haciendo un uso inadecuado de las tecnologías de la información.

CONFIDENCIALIDAD Es preciso mantener la información de manera segura para que no sea accedida por personas no autorizadas, establecer controles limitando los accesos permitirá garantizar que la información sea manejada adecuadamente y evitar fugas de información.

CSOC Centro de operaciones de ciberseguridad

CSIRT De sus siglas en ingles es el centro de respuesta para incidentes de seguridad en tecnologías de la información.

CVE De sus siglas en ingles se traducen a Vulnerabilidades y Exposiciones Comunes

DENEGACIÓN DE SERVICIO DoS Afectación a un sistema de información debido a múltiples peticiones simultaneas desde un mismo origen, generando la indisponibilidad de este.

DENEGACIÓN DE SERVICIO DISTRIBUIDA DDoS Afectación a un sistema de información debido a múltiples peticiones simultaneas desde diferentes orígenes, generando la indisponibilidad de este.

DISPONIBILIDAD Uno de los pilares fundamentales de la seguridad de la información el cual consta en que un sistema, repositorio o información se encuentren accesibles en el momento que se requiera.

FALSO NEGATIVO Diagnostico con un análisis a destiempo puede llevar a generar una falsa conclusión, si no se cuenta con la suficiente información y el correcto análisis podría determinarse un resultado negativo que podría llegar a ser falso.

FALSO POSITIVO Un resultado positivo sin un adecuado análisis o depuración de la información que lleve a descartar los elementos que pueden estar generando una alerta de un elemento valido o conocido, lo cual no se debería presentar.

INCIDENTE DE SEGURIDAD Daño, alteración, acceso o modificación de los sistemas de manera fraudulenta o no autorizada, podría derivarse también del aprovechamiento de una vulnerabilidad o brecha de seguridad.

INGENIERÍA SOCIAL Técnica utilizada para engañar a los usuarios mediante comunicaciones de suplantación haciendo creer que se trata de un evento real para extraer información.

LOG Serie de registros generados por los sistemas que permiten evidenciar la trazabilidad de las acciones realizadas.

PLAYBOOK Son las reglas de juego definidas para responder de manera oportuna ante una necesidad.

SANDBOX herramienta utilizada para realizar pruebas de elementos informáticos de manera controlada simulando las acciones en un ambiente aislado para no generar afectaciones en los sistemas reales.

SIEM De sus siglas en ingles es la herramienta que se utiliza para la Gestión de información y eventos de seguridad, el cual permite centralizar y gestionar de manera adecuada los eventos generados por los sistemas.

SOC Centro de operaciones de seguridad.

SOAR Es la automatización de tareas de seguridad definido en flujos de trabajo construidos y documentados con antelación.

VULNERABILIDAD Una o varias debilidades expuestas en un sistema de información que podrán ser aprovechadas por un atacante para realizar afectaciones o ejecutar acciones no autorizadas.

RESUMEN

El presente documento se encontrará documentación relacionada con lo que se debe tener en cuenta para llevar a cabo un diseño de un servicio de monitoreo de ciber seguridad en una organización, factores clave a tener en cuenta, contemplando diversas opciones de recolección de los datos, tipos de logs, servicio SOC, acciones de respuesta automatizada para garantizar una pronta reacción ante un posible incidente de ciberseguridad, con base a las recomendaciones que puedan existir en los marcos de referencia como NIST, circular externa 007 de 2018 de la super intendencia financiera de Colombia, para que con base a esta información se logre comprender las necesidades y fortalecer un esquema de monitoreo que pueda alimentar al equipo de respuesta a incidentes de ciberseguridad de las organizaciones.

Uno de los elementos principales en la prevención de delitos informáticos es el monitoreo, el cual permitirá una identificación oportuna de acciones anómalas en los sistemas de información lo cual es un indicio de que algo puede estar pasando, durante el desarrollo de los objetivos se ha trabajado en la identificación de las necesidades de una organización basado en las cinco funciones del marco de trabajo de NIST y como estas pueden aportar a la identificación oportuna y respuesta ante amenazas, así mismo se argumentan los principales ataques cibernéticos a los cuales están expuestas las organizaciones en Colombia, con base a esto realizar un plan estratégico que permita proteger la seguridad de la información en las organizaciones, se seleccionan algunas herramientas del mercado necesarias para la implementación de un centro de operaciones de seguridad con el cual se busca tener mucho más que una recolección y análisis de logs, en la actualidad el SOC debe actuar de una manera más avanzada es por esto que se proponen estrategias para la mejora y fortalecimiento del servicio, llevando a cabo la identificación, predicción, respuestas automatizadas y otras acciones para garantizar la estabilidad de las organizaciones y la protección continua de su información.

Palabras clave: Correlación, CSOC, Detección de amenazas, Monitoreo, SIEM, SOAR, SOC.

ABSTRACT

In this document you will find documentation related to what must be taken into account to carry out a design of a cyber security monitoring service in an organization, key factors to take into account, considering various data collection options, types of logs, SOC service, automated response actions to guarantee a prompt reaction to a possible cybersecurity incident, based on the recommendations that may exist in reference frameworks such as NIST, external circular 007 of 2018 of the financial superintendency of Colombia, so that based on this information it is possible to understand the needs and strengthen a monitoring scheme that can feed the response team to incidents of cybersecurity of organizations.

One of the main elements in the prevention of computer crimes is monitoring, which will allow timely identification of anomalous actions in information systems, which is an indication that something may be happening. During the development of the objectives, work has been done. in the identification of the needs of an organization based on the 5 functions of the NIST framework and how these can contribute to the timely identification and response to threats, as well as the main cyber-attacks to which organizations are exposed in Colombia, based on this, to carry out a strategic plan that allows protecting the security of information in organizations, some necessary market tools are selected for the implementation of a security operations center with which it is sought to have much more than a collection and log analysis, currently, the SOC must act in a more advanced way This is why strategies are proposed for the improvement and strengthening of the service, carrying out identification, prediction, automated responses and other actions to guarantee the stability of organizations and the continuous protection of their information.

Keywords: CSOC, Monitoring, Threat detection, SIEM, SOAR, SOC.

INTRODUCCIÓN

Estando de acuerdo en que se trabajara en el análisis de soluciones para el monitoreo de seguridad activa y pasiva de infraestructuras tecnológicas apoyado en un servicio de SOC, es necesario tener conocimiento por parte de las empresas en Colombia de cuantos ataques cibernéticos se generan cada día en la web dirigidos a diferentes tipos de organizaciones, en la actualidad existe un uso progresivo de las tecnologías de información[1], por lo cual las empresas cada vez exponen más recursos hacia internet para facilitar la interacción con sus clientes y empleados.

Constantemente las empresas se ven involucradas en diversos ataques cibernéticos, podría ser un malware descargado de un sitio web, mediante un correo electrónico de phishing, acceder a sitios de suplantación, suministrar información personal o corporativa en sitios no autorizados, almacenar o compartir archivos de uso confidencial de la empresa en páginas o programas de uso no corporativo, entre otros elementos de los cuales pueden suceder y no son detectados.[2]

Con base a esto se lleva a cabo el trabajo de análisis de soluciones para el monitoreo de seguridad activa y pasiva de infraestructuras tecnológicas apoyado en un servicio de SOC, Centro de operaciones de seguridad, mediante el cual se buscar principalmente brindar una documentación que sirva de apoyo a las organizaciones en la toma de decisiones a la hora de seleccionar soluciones para el monitoreo y gestión de la seguridad de la información, de esta manera podrán contar con alternativas que permitan el acceso a una base de conocimiento para la toma de decisiones a la hora de implementar un servicio SOC.

---

[1] (MinTIC - *Así Avanzó Colombia En Conectividad Durante 2021*)

[2] Centro de Capacidades para la Ciberseguridad de Colombia (C-4)

El servicio de SOC permite a las organizaciones realizar un monitoreo continuo de sus principales activos de información, el cual mediante unas fases iniciales de reconocimiento puede aplicar herramientas de inteligencia que permitan conocer el comportamiento de sus usuarios y sus sistemas, lo cual facilitara la detección oportuna de cambios de comportamiento, permite establecer parámetros y controles para identificar la ejecución de actividades no autorizadas y anómalas de manera continua realizando actividades de correlación con diversas fuentes de información.

Para una organización contar con un servicio de monitoreo desde un SOC es una oportunidad de identificar de manera oportuna eventos, amenazas o incidentes de seguridad y poder actuar de manera rápida para prevenir afectaciones mayores.

En Colombia existen diferentes organizaciones que han venido fortaleciendo herramientas para la detección de incidentes de ciberseguridad, como lo es el CSIRT de la policía nacional[3], estos brindan diversas herramientas para el reporte de eventos identificados como maliciosos o sospechosos así mismo brindan un canal de denuncia para estos delitos y lograr fortalecer controles que permitan mitigar los riesgos a nivel nacional generando comunicaciones de manera general, así mismo se brinda información importante para conocer las cifras, clasificaciones de ataques, tipos, cuáles son los más comunes, entre otra información valiosa para aplicar controles de mitigación en las empresas.

En el presente trabajo se plantean diferentes alternativas para lograr llevar a cabo la adecuada implementación de un servicio de monitoreo que sea de utilidad para las empresas colombianas.

[3] (*Equipo de Respuesta a Incidentes de Seguridad Informática de La Policía Nacional CSIRT-PONAL*)

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En los últimos años, las tecnologías de información han venido teniendo un incremento potencial tanto en Colombia[4] como a nivel mundial **"la recuperación económica del mercado digital seguirá impulsando las inversiones en tecnología"[5]**, se ha venido presentando un aumento de dispositivos conectados a las redes de comunicación[6] lo cual trae consigo incrementos significativos en los recursos, aplicaciones, servicios entre otros elementos necesarios para garantizar un adecuado funcionamiento.

Con relación al crecimiento mencionado anteriormente, también de la misma manera se ve reflejado el incremento de los ataques cibernéticos[7] el cual constantemente expande sus alcances a las nuevas tecnologías, tratando de identificar y explotar diferentes tipos de vulnerabilidades, en ocasiones brechas de seguridad generadas por un ciclo inadecuado de desarrollo en el cual no se contemplan las necesidades de seguridad, es fundamental para las organizaciones contar con estrategias que le permitan identificar, gestionar, tratar y mitigar los riesgos de ciberseguridad ya que en la mayoría de los casos las empresas no se dan cuenta si están siendo atacadas o no cuentan con sistemas de monitoreo que les permita tener una reacción oportuna ante posibles eventos o amenazas de seguridad.

---

[4] (MinTIC - Así Avanzó Colombia En Conectividad Durante 2021)

[5] (ComputerWorld, El Gasto TI En El Mundo Crecerá Un 5,1% En 2022)

[6] Informe Global Sobre el Entorno Digital 2022

[7] SIEDCO Policía, SPOA, Fiscalía, ADenunciar.

En Colombia y en el mundo se han venido presentando diversos cambios, entre ellos el más significativo en el último año ha sido la pandemia mundial del Covid-19, el cual ha traído consigo una aceleración de implementación de nuevas alternativas de comunicación, conectividad, transferencia de información, entre otras necesidades que han ido surgiendo para poder continuar con el desarrollo de las actividades de la mejor manera posible, lo cual trae consigo una necesidad de aplicar nuevas estrategias de monitoreo para garantizar la adecuada protección de la información.

Con base a esta información es necesario investigar alternativas de monitoreo que permitan la identificación y gestión oportuna de eventos e incidentes de seguridad, de esta manera garantizar que se pueda llevar a cabo las respectivas remediaciones y ajustes para evitar incidentes mayores o lograr identificar y corregir la causa raíz de un incidente de seguridad y de esta manera evitar que se vuelva a presentar.

1.2 FORMULACIÓN DEL PROBLEMA

¿Qué beneficio tendrían las empresas colombianas al llevar a cabo la implementación de un servicio de SOC, que permita realizar el monitoreo, seguimiento y análisis de las actividades sobre sus activos tecnológicos con el fin de identificar actividades anómalas de manera continua?

2 JUSTIFICACIÓN

Los motivos que conllevan al desarrollo del presente trabajo, es lograr la identificaciones de las diferentes alternativas para cubrir las necesidades que actualmente tienen las organizaciones para un correcto monitoreo de ciberseguridad sobre sus activos de información tecnológicos y aplicativos, planteando diferentes alternativas para fortalecer la detección oportuna de posibles eventos o amenazas cibernéticas, de este modo garantizar la adecuada protección de la información, para esto es necesario la implementación de buenas prácticas y estándares para proteger los activos críticos de información, infraestructura tecnológica, sistemas de información y comunicaciones, fomentando la mejora continua, estableciendo lineamientos para la configuración de logs de auditoría sobre todos los sistemas lo cual permitirá la correlación de eventos y registros de auditoría de sus principales fuentes de información permitiendo una detección oportuna de eventos e incidentes de ciberseguridad y realizando una gestión adecuada de los hallazgos que permita lograr el restablecimiento de los servicios en el menor tiempo posible, de esta manera fortalecer la confidencialidad, integridad y disponibilidad de la información que permitan mantener la confianza de los clientes.

En la ilustración 1, se puede evidenciar la tipificación de la conducta de los delitos informáticos en Colombia y como ha sido su comportamiento durante los últimos años con base al informe de cibercrimen emitido por el centro cibernético de la policía nacional en el año 2019 el cual se genera cada 2 años.

Ilustración 1. cifras de denuncias cibercrimen en Colombia

Fuente 1. SIEDCO Policía, SPOA Fiscalía, A Denunciar. Cifras denuncias 2015- 2019

Los ataques cibernéticos han tenido un aumento significativo en el año 2020 y lo que va del 2021, según las cifras del centro de delitos cibernéticos de la policía nacional de Colombia, y lo expuesto por el coronel Luis Fernando Atuesta al diario Portafolio en julio de 2020[8], esta cifra aumento en un 59% en el primer semestre del año 2020 comparado con el mismo periodo del 2019, se presentaron 17.211 casos denunciados, 6.340 más que en el primer semestre del 2019[9]. Las empresas han adoptado estrategias para continuar desempeñando sus actividades empleando recursos tecnológicos, así mismo también se han aumentado los ataques, las organizaciones en ocasiones pueden no detectar de manera oportuna que están siendo atacadas lo cual puede causar una perdida representativa de su información, indisponibilidad, daño reputacional, entre otros, contar con un monitoreo de seguridad mediante un SOC ayudara a ser oportunos en la identificación de ataques y de esta manera ejecutar las acciones necesarias en el menor tiempo posible.

[8] ATUESTA, Luis Fernando, centro cibernético de la Policía Nacional

[9] Ibid.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar soluciones para que las organizaciones establezcan una estrategia de monitoreo activo y pasivo de la seguridad de la información y de la infraestructura tecnológica mediante la incorporación de un servicio de SOC.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar la información relevante del marco de trabajo de NIST, así como los principales elementos que deben tenerse en cuenta y serán de utilidad para incorporación de un servicio de SOC en las organizaciones colombianas.

- Argumentar los principales ataques cibernéticos a los cuales están expuestas las organizaciones en Colombia que permita la identificación oportuna de amenazas con la implementación de un servicio de monitoreo de ciberseguridad.

- Seleccionar diferentes soluciones en el mercado para la implementación de un sistema de monitoreo de servicios tecnológicos en las organizaciones desde un SOC.

- Proponer estrategias que ayuden a fortalecer los sistemas de monitoreo de ciberseguridad para las organizaciones con alternativas que permitan llevar a cabo la respuesta oportuna ante amenazas de seguridad buscando reducir los tiempos.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Ciberseguridad en las empresas: En la actualizad y desde hace algunos años se ha venido evidenciando un crecimiento exponencial en el uso de las tecnologías de la información, así como la aparición de nuevos dispositivos conectados a la red, la expansión y mejoramiento continuo de las comunicaciones, con relación a esto también se tiene como resultado un incremento significativo en las amenazas de seguridad, el número de vulnerabilidades es mayor, los ataques cada vez aumentan por lo cual se genera la necesidad de proteger la información buscando mecanismos avanzados y efectivos que permitan a las organizaciones tener una visibilidad de lo que está pasando con sus sistemas, aplicaciones el tráfico que se genera desde y hacia internet así, tener una oportuna reacción ante una amenaza de seguridad y prevenir un posible incidente.

La pandemia del Covid-19 ha traído consigo un incremento del trabajo remoto, lo cual trae consigo múltiples implicaciones de seguridad, una descentralización de conexiones, diversas opciones de acceso a la información, los comercios han incrementado sus ventas en línea, implementación de sitios para la venta de productos, entre otros múltiples factores para tener en cuenta y fortalecer el monitoreo en las plataformas de las empresas. Para Adriana Ceballos, directora de desarrollo de programas del Tanque de Análisis y Creatividad de las Tic (TicTac) “la ciberseguridad es el área que mayor atención deberá tener en el 2021, pues un gran número de colaboradores seguirán operando desde sus hogares”[10]

[10] CEBALLOS, Adriana, Ciberseguridad, un punto crítico en el 2021 para las empresas. EL UNIVERSAL. Cartagena 05 de febrero de 2021

4.1.2 Retos de ciberseguridad y la pandemia del covid19: Con base a la información recolectada por la revista enter.co en su artículo “Ciberseguridad: uno de los retos que dejo el 2020” se puede evidenciar que durante el año 2020 se evidencio un incremento del 89% con relación al año 2019, llegando a tener 45.000 casos reportados de ciberdelitos.[11]

4.1.3 Delitos informáticos más relevantes: El delito que mayor crecimiento he impacto ha tenido ha sido la suplantación de sitios web, los ciberdelincuentes generan campañas de suplantación haciendo creer a sus víctimas que están recibiendo información de empresas conocidas, en la mayoría de los casos enviando correos que les solicitan sus datos personales haciéndoles creer que se requieren para una actualización o que sus cuentas no sean inactivadas, de esta manera logran obtener la información de los usuarios lo que les permite tener accesos a diferentes recursos.

Contar con una herramienta de monitoreo en tiempo real permite a las organizaciones tener un seguimiento y establecer mediante inteligencia artificial las acciones que normalmente ejecutan los usuarios, con base a esto es posible crear una correlación de los eventos y establecer alertas que se generen cuando se evidencia una actividad sospechosa o diferente a las que ya el sistema conoce, por ejemplo, sería posible identificar mediante un monitoreo si un usuario se está autenticando en su cuenta desde orígenes diferentes a los que usualmente utiliza, o se evidencia un cambio en la ubicación geográfica en un periodo corto de tiempo, es decir, el usuario que normalmente se autentica desde Colombia el día de hoy genero un movimiento normal a las 9 AM pero a las 9:30 AM genera una conexión desde Asia, por lo cual no es posible que haya realizado este desplazamiento en un periodo tan corto de tiempo, esto genera una alerta y mediante

[11] ARIAS, Diana, Ciberseguridad: uno de los retos que dejo el 2020 • ENTER.CO. 28 de enero de 2021

la configuración de diversas opciones sería posible establecer un bloqueo y de esta manera impedir de una manera oportuna que se ejecuten transacciones no autorizadas.[12]

4.1.4 Medición de ataques cibernéticos: En el mercado existen diversas aplicaciones de medición de ataques en tiempo real, por ejemplo, en el sitio https://threatmap.checkpoint.com/ se puede evidenciar en tiempo real el número de ataques que se han presentado en un día, este dato puede llegar a un promedio de 50 millones de ataques en un día.

4.1.5 Ataques más relevantes del 2020: Alguno de los ataques más relevantes del 2020 que han sido identificados a nivel mundial y tomados del "INFORME SOBRE SEGURIDAD CIBERNÉTICA 2021[13]" de CheckPoint son:

Solarwinds declara que hasta 18000 de sus clientes en todo el mundo se vieron afectados por la filtración de sus sistemas. según la evidencia, parece que los atacantes ingresaron en sus sistemas al menos un año antes de que se descubriera la filtración.[14]

Travelex, una empresa de divisas con sede en Londres estuvo paralizada por semanas debido a un ataque de Ransomware (conocido como REvil) por parte del grupo Sodinokibi. Travelex había iniciado negociaciones con el grupo, pero se negó a pagar la demanda de rescate de USD 6 millones a cambio de las claves de descifrado. Como represalia, los atacantes amenazaron con publicar 5 GB de información personal de los clientes que había sido robada y extraída antes del cifrado. Este fue uno de los ataques

[12] PORTAFOLIO, Cifras de ciberseguridad en Colombia prenden alarmas al cierre del 2020. Tendencias. 10 de diciembre de 2020.

[13] CHECK POINT. Informe Sobre Seguridad Cibernética2021

[14] Ibid

de Ransomware de “doble extorsión” de más alto perfil, en el que los atacantes filtran las redes corporativas, roban archivos confidenciales, cifran datos y exigen un rescate para descifrarlo, así como amenazan con publicar datos si no se cumple la demanda de rescate, para ejercer más presión sobre las víctimas.[15]

La cadena de hoteles Marriott ha notificado que ha tenido una fuga de información confidencial de más de 5 millones de clientes.[16]

4.1.6 Delitos informáticos que más afectan a los colombianos: Según el informe de tendencias de cibercrimen en Colombia presentado por CCIT y la policita nacional,[17] el delito informático que cuenta con el mayor índice de denuncias hace relación al hurto por medios informáticos con un total de 31058 casos, seguido por la violación de datos personales con un total de 8037 casos, sin duda alguna los delincuentes buscan obtener beneficios económicos mediante la obtención de accesos a la información de los usuarios para posteriormente lograr acceder a su información financiera y efectuar transacciones.

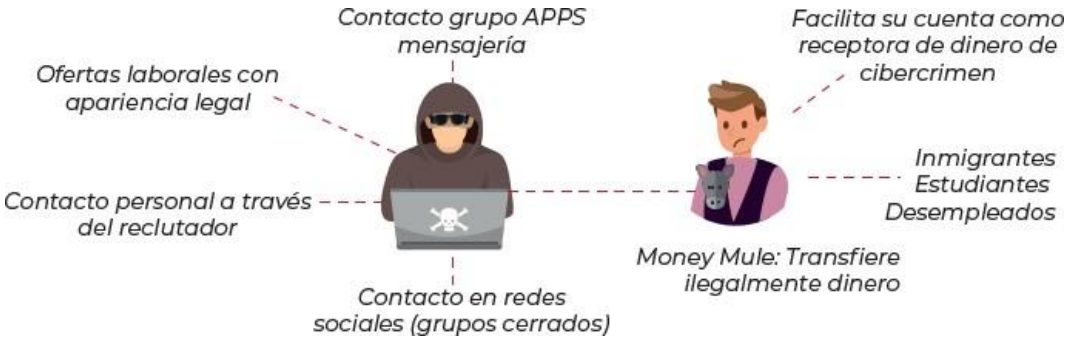
Existe un término conocido como Money mules, como se evidencia en la ilustración 2, son personas que prestan su identidad a organizaciones criminales para recibir dineros en sus cuentas producto de las acciones fraudulentas realizadas, estas personas hacen esto a cambio de una remuneración económica, muchas veces por desconocimiento lo cual podría acarrearles acciones legales.

[15] ABRAMS, Lawrence, Sodinokibi Ransomware Says Travelex Will Pay, One Way or Another. Bleepingcomputer. 9 de enero de 2020.

[16] LYLES, Taylor, Marriott discloses another security breach that may impact over 5 million guests - The Verge. 1 de abril de 2020.

[17] TICTAC, Tendencias del cibercrimen en Colombia 2019-2020

Ilustración 2. Money mules



Fuente 2. Informe de tendencias cibercrimen en Colombia 2019-2020

A continuación, se listan algunos de los ataques más comunes que se han identificado en Colombia durante el año 2019.

- Ataques BEC, (business Email Compromise)
- Ataques de Ransomware
- Ataques de DDoS.
- Ataques de Malware.
- SIM SWAPPING, Secuestro o cambio de SIM CARD
- Criptojacking

4.1.7 Algunos de los beneficios de implementar un SOC: A continuación, se relacionan algunos de los principales beneficios de llevar a cabo la implementación de un SOC para el monitoreo de en las organizaciones.

- Detectar ataques basados en la red
- Detectar ataques basados en host
- Eliminando vulnerabilidades de seguridad
- Apoyar a los usuarios autorizados

- Proporcionar herramientas para minimizar las pérdidas de información corporativa

Algunas de estas acciones cuentan con controles previos como, por ejemplo, firewalls o antimalware que en ocasiones puede que no logren detectar todas las amenazas o no se logran gestionar de una manera adecuada lo cual se puede optimizar con un servicio SOC.

4.1.8 Definición de la estrategia de monitoreo: Es necesario definir varias estrategias a la hora de construir un plan de monitoreo de ciberseguridad, por ejemplo, ir definiendo unos pasos a seguir ya que el servicio de monitoreo de ciberseguridad no mostrara resultados de la noche a la mañana.

Una estrategia de monitoreo y fortalecimiento de la ciberseguridad puede trabajarse muy de la mano con lo planteado por el Framework de NIST e ir ajustando la estrategia para cada uno de sus perfiles.

4.2 MARCO CONCEPTUAL

4.2.1 ¿Qué es un SOC?: El SOC, centro de operaciones de seguridad, tiene como principal función la recolección y correlación de eventos de seguridad de las fuentes monitoreadas, es muy importante definir con base a un inventario de activos de información previamente construido y clasificado cuáles son esas fuentes de información que brindan un mayor valor a la organización para la identificación oportuna de amenazas o ciberataques que se puedan estar presentando.

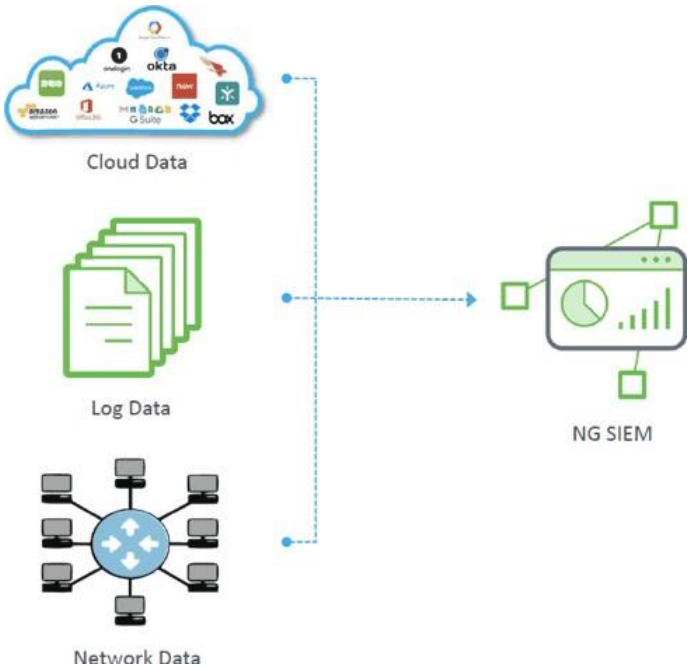
4.2.2 Algunas de las principales funciones del SOC: A continuación, se enumeran de manera enunciativa algunas de las principales funcionalidades de un SOC.

- Centralización de los eventos de seguridad
- Correlación de los eventos
- Identificación y análisis de los eventos y amenazas
- Contención, erradicación y recuperación
- Inteligencia de amenazas

4.2.3 SOC de nueva generación: A continuación, se relacionan algunas de las características necesarias para un SOC de nueva generación

- Como se evidencia en la Ilustración 3, se describe una de las principales características de un SIEM de nueva generación el cual debe recolectar y administrar datos de todas las fuentes de datos disponibles en los diferentes sistemas de información.

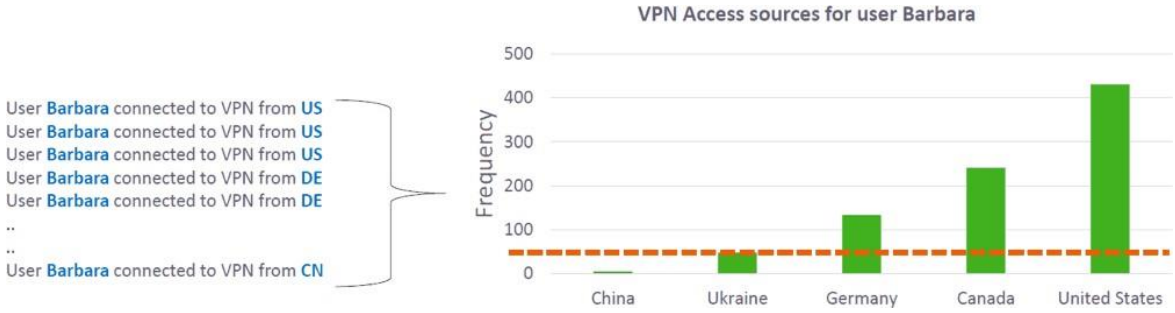
Ilustración 3. SIEM de nueva generación deberá acceder a todas las fuentes de datos



Fuente 3. EXABEAM 10 Features to be a Next-gen SIEM

- Contar con la capacidad de trabajar con una arquitectura de Big Data.
- Enriquecimiento de contexto de la información obtenida tanto de usuarios como los activos de información, de esta manera establecer una adecuada identificación de cambios.
- Ilustración 4, análisis de comportamiento de usuarios y entidades traducido de las siglas (UEBA) User and Entity Behavior Analysis, el análisis de comportamiento permite establecer unas líneas base de los usuarios y los activos monitoreados, de esta manera lograr identificar cambios inusuales que permitan actuar de una manera predictiva ante una posible amenaza.

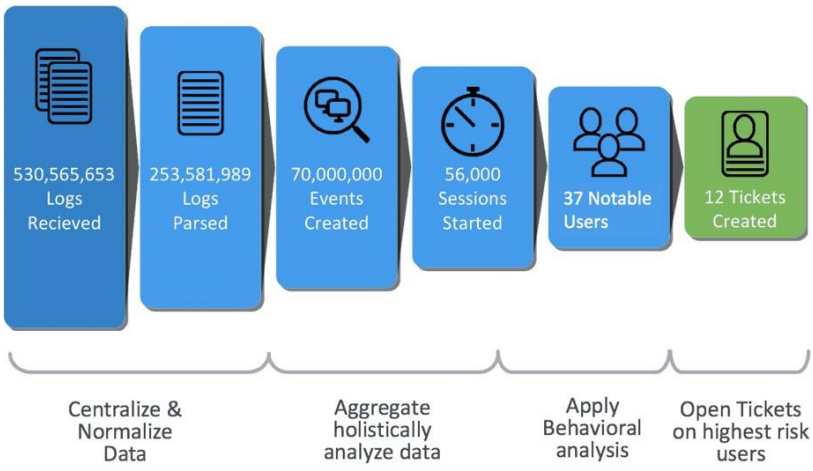
Ilustración 4. Ejemplo de comportamiento de un usuario



Fuente 4. EXABEAM 10 Features to be a Next-gen SIEM

- Identificación oportuna de posibles movimientos laterales dentro de la arquitectura de la organización.
- Mejoramiento continuo de los modelos de seguridad de la organización.
- Ilustración 5, correlación, depuración y priorización de incidentes para lograr identificar lo realmente importante para las organizaciones, a continuación, un ejemplo.

Ilustración 5. Priorización de incidentes que requieren investigación



Fuente 5. EXABEAM 10 Features to be a Next-gen SIEM

- Orquestación de eventos de seguridad y automatización de respuestas, de las siglas en inglés (SOAR) este término busca implementar acciones de respuesta automáticas que puedan ser aplicadas desde el centro de operaciones de seguridad, reduciendo tiempos de respuesta y aumentando la proactividad evitando posibles amenazas y propagaciones de un incidente.

4.2.4 ¿Qué es un NOC?: Por otro lado, existe el NOC, Centro de operaciones de red el cual se enfoca específicamente en el monitoreo de salubridad de los equipos monitoreando la disponibilidad y el rendimiento de estos, es una actividad independiente pero también importante para garantizar la disponibilidad de los servicios como uno de los pilares de la seguridad informática.

4.2.5 Algunas de las actividades del NOC: A continuación, se enumeran de manera enunciativa algunas de las actividades realizadas desde el NOC.

- Monitoreo y gestión de las configuraciones
- Monitoreo de la gestión de cambios
- Monitoreo de eventos de red
- Monitoreo del desempeño y optimización de los recursos es son esas fuentes que brindan un mayor valor a la organización.[18]

4.2.6 Framework NIST: En la ilustración 6, se describe de manera gráfica las 5 funciones del marco de trabajo de NIST, las cuales serán detalladas más adelante, estas son identificar, proteger, detectar, responder y recuperar, de cada una de estas se desprenden las categorías y subcategorías.

[18] NEWNET S.A. Centro de Monitoreo de Ciberseguridad. Bogotá Colombia.

Ilustración 6 Framework NIST

Fuente 6. (*NIST Releases Version 1.1 of Its Popular Cybersecurity Framework*)

4.2.7 IDENTIFICAR: El objetivo global de la fase de Identificar es identificar todos los activos, tanto de datos, como de software y hardware, y analizar los niveles de riesgo a los que están expuestos. Esto nos prepara para la siguiente fase, Proteger.

La fase de Identificar se divide en 5 tipos de controles: Gestión de activos, entorno empresarial, gobernanza, evaluación de riesgos, estrategia de gestión de riesgos, y gestión de riesgos de la cadena de suministro.

4.2.8 PROTEGER: El objetivo global de la fase de Proteger es implementar procedimientos y soluciones de software que nos permitan asegurar la confidencialidad, integridad, y disponibilidad de datos, asegurándonos que los datos correctos estén disponibles a las personas correctas, en el momento correcto.
La fase de Proteger se divide en 6 tipos de controles: gestión de identidad, autenticación, y control de acceso, concientización y capacitación, seguridad de los datos, procesos y procedimientos de protección de la información, mantenimiento, y tecnología de protección.

4.2.9 DETECTAR: El objetivo global de la fase de Detectar es detectar incidentes de seguridad informática, tales como escaneos, intentos de penetración, y eventos de movimientos laterales dentro de la red.
La fase de Detectar se divide en tres tipos de controles: anomalías y eventos, monitoreo continuo de la seguridad, y procesos de detección.

4.2.10 RESPONDER: El objetivo global de la fase de Responder es la implementación de procesos y software que nos permita mitigar los efectos de un ataque cibernético, prevenir la extracción de información, y eliminar la amenaza de la red.

La fase de Responder se divide en 5 tipos de controles: planificación de respuesta, comunicaciones, análisis, mitigación, y mejoras.

4.2.11 RECUPERAR: El objetivo global de la fase de Recuperar es restablecer la confidencialidad, integridad, y disponibilidad de los datos después de un ciberataque.

La fase de Recuperar se divide en tres tipos de control: planificación de la recuperación, mejoras, y comunicaciones.[19]

4.2.12 SOAR: Security Orchestration, Automation and Response, permite la ejecución de tareas de manera automatizada, para ofrecer una respuesta más ágil ante eventos e incidentes de seguridad, se presentan como utilidad para la respuesta mediante Playbooks previamente definidos.

[19] KELLER, Nicole, CYBERSECURITY FRAMEWORK.

Las tareas de detección requieran cada vez menos intervención manual para llevarse a cabo y, por ende, menos tiempo de respuesta.[20]

4.2.13 SIEM: (Security Incident and Event Management) es la herramienta encargada de llevar a cabo la recolección de los registros de eventos (logs) de diferentes fuentes de información, almacenarlos, analizarlos y de esta manera correlacionarlos para lograr identificar posibles eventos o incidentes de ciberseguridad.

4.2.14 Ventajas y beneficios de un SIEM: A continuación, se listarán una serie de ventajas y beneficios de un SIEM.

- Centralización de la información de seguridad.
- Automatización de tareas.
- Respuesta automática a eventos y amenazas.
- Disminución del tiempo de detección de ataques.
- Información rápida y eficiente para realizar análisis forense.
- Alertas de seguridades eficientes.
- Análisis y correlación de logs en tiempo real.
- Seguimiento de eventos.
- Mejor manejo del riesgo.
- Manejo de métricas de seguridad.
- Detección de activos.
- Evaluación de vulnerabilidades.
- Detección de violaciones de seguridad.
- Monitoreo de comportamiento.[21]

[20] MELÉNDEZ, Luciano. ¿De qué hablamos cuando hablamos de SOAR? 17 de julio de 2019.

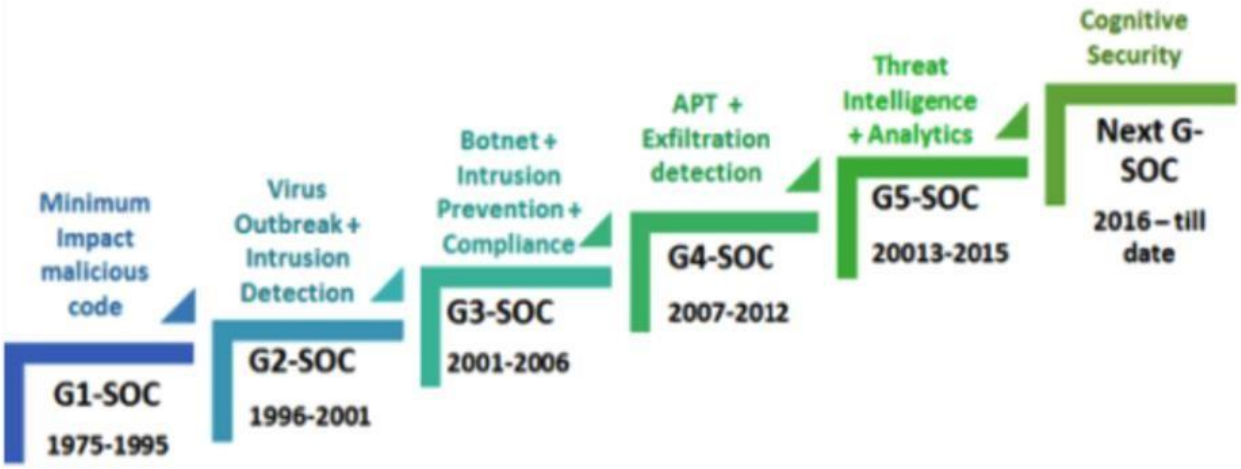
[21] PACHON, Camila. ¿Qué es SIEM y cómo funciona? Alcance e implementación. Nsit.

4.3 MARCO HISTÓRICO

4.3.1 Evolución del SOC: Con el paso de los años también el concepto de SOC ha venido evolucionando, se habla de un CSOC el cual sus siglas traducen centro de operaciones de ciber seguridad, el cual busca tener un alcance más avanzado a lo que usualmente se monitorea desde un SOC.

Los centros de operaciones de seguridad han venido evolucionando con el paso de los años, como se puede evidenciar en la ilustración 7, en sus primeras generaciones fueron implementados como una necesidad de identificación de código malicioso de impacto mínimo, pero con el paso de los años las tecnologías fueron avanzando de manera exponencial y así mismo fueron creciendo las necesidades de monitoreo.

Ilustración 7. Esquema de evolución SOC.



Fuente 7. MENDEZ Fonseca, Victor Julio, Universidad Piloto de Colombia, Marco Tecnológico de un SOC de Nueva Generación.2019

4.4 ANTECEDENTES O ESTADO ACTUAL

4.4.1 Monitoreo de ciberseguridad en las organizaciones: Ha ido cambiando y evolucionando con el paso de los años, a menudo escuchamos términos como SOC (Security Operation Center) y NOC (Network Operation Center). Como estrategias de monitoreo tanto de seguridad como de salubridad de los sistemas.

La implementación de un SOC en una organización requiere de una adecuada planeación e identificación de las necesidades, es ideal contar con una previa identificación y valoración de los activos de información de la organización, con base a esto realizar una selección de las fuentes primordiales y que puedan generar la información necesaria para la identificación, valoración, gestión de un evento, es importante resaltar que existen diferentes maneras de gestionar los logs lo cual puede varias de acuerdo al fabricante y a las tecnología de los sistemas implementados lo cual también requerirá un mayor o menor esfuerzo en el momento de llevar a cabo una integración con un SIEM.

Las necesidades y funcionamiento de un SOC han ido evolucionando a medida que los tipos de amenazas van cambiando, el centro de operaciones de seguridad se enfrenta a nuevos retos, las amenazas ya no son las mismas de antes donde se lograba identificar de manera sencilla una amenaza conocida o estática, han ido apareciendo elementos como las APT, que van cambiando de manera constante su comportamiento tratando de evadir los controles y no ser detectadas, los ataques de denegación de servicio comunes también han ido evolucionando y ya no se generan múltiples peticiones desde un mismo origen si no que se realizan de manera distribuida utilizando diferentes puntos para generar un ataque, posiblemente apoderándose de ordenadores de usuarios que acceden a internet y sus máquinas son infectadas.

Con base a esto se genera la necesidad de evolucionar las capacidades del SOC, es acá donde toma fuerza el SOC de nueva generación, el cual continua haciendo uso de

herramientas como el SIEM que es el elemento principal para lograr una adecuada correlación de los eventos, pero es necesario implementar y fortalecer elementos que permitan el reconocimiento e identificación de nuevos patrones, para esto es necesario incluir acciones de inteligencia artificial, análisis de comportamiento, establecer unos parámetros o líneas base de comportamiento que estén actualizándose constantemente, de esta manera conocer como es un comportamiento normal de un usuario, de una máquina, de un servidor, de una aplicación, con base a esta información lograr identificar de manera oportuna cambios que den indicios a un posible ataque de seguridad y actuar de manera oportuna.

En la actualidad ya no basta contar con un correlacionador de eventos o un SIEM que únicamente funcione como un gestor de logs y genere una cantidad de eventos o alertas que no serán gestionadas de manera oportuna por su alto volumen.

Es necesario la inclusión de elementos como:

- EDR (Endpoint Detection and Response)
- UEBA (User & Entity Behavior Analytics)
- TIP (threat intelligence platform)
- SOAR (Security Orchestration, Automation, and Response)

La automatización es fundamental para lograr tener un SOC eficiente y proactivo, la cantidad de alarmas y alertas generadas por las diferentes fuentes de información no son efectivas si se lleva a cabo una revisión tradicional.

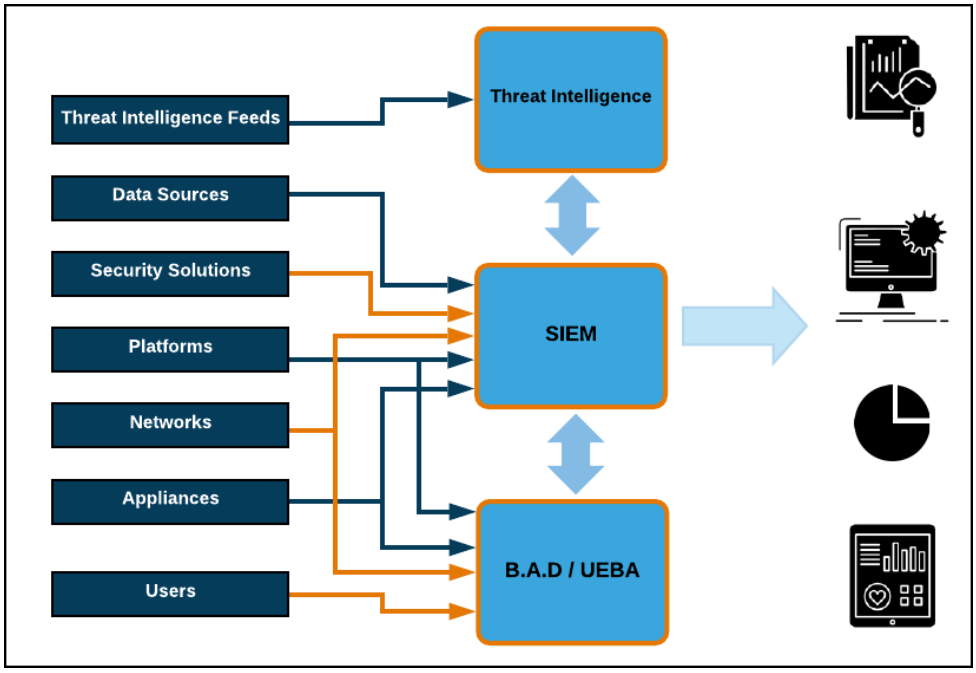
Por esta razón los SOC de nueva generación requieren la inclusión de estrategias que permitan analizar mediante inteligencia artificial lo que ocurre en tiempo real, clasificando información conocida y destacando la información relevante que posteriormente podrá ser analizada con mayor detalle por los analistas.

Como se observa en la ilustración 8, un SOC de nueva generación debe contar con al menos las siguientes capacidades para lograr brindar una adecuada detección de incidentes:

- Inteligencia de amenazas
- Capacidad para conectarse con diversas fuentes de datos.
- Diversas soluciones de seguridad
- Integración con múltiples plataformas
- Dispositivos de red.
- Aplicaciones
- Usuarios

Los cuales se integran de la siguiente manera:

Ilustración 8. NG SIEM

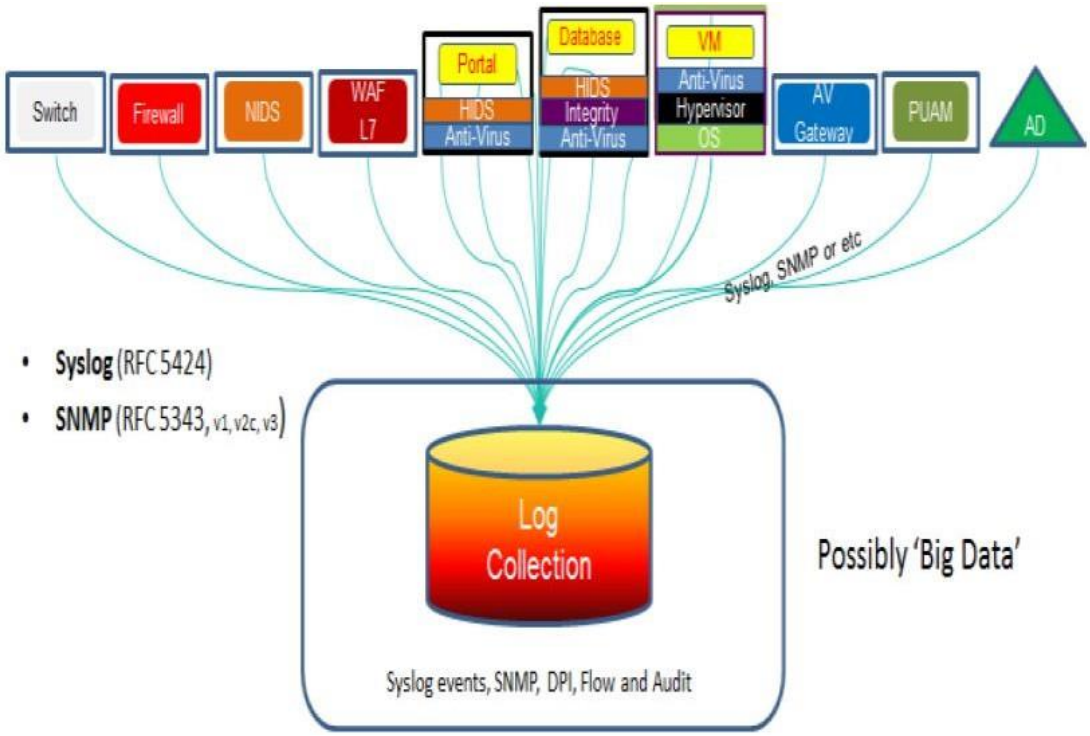


Fuente 8. MENDEZ Fonseca, Victor Julio, Marco Tecnológico de un SOC de Nueva Generación. P.6

Ilustración 9, los diversos dispositivos de la organización deben estar en la capacidad de generar logs o eventos de las diferentes actividades realizadas, para esto existen diferentes alternativas, la más común es Syslog, pero también existen otras alternativas como SNMP, Sysmon o mediante el consumo de un API en las nuevas tecnologías.

A continuación, se muestra como es un proceso de recolección de logs mediante un centralizador.

Ilustración 9. Colector de logs

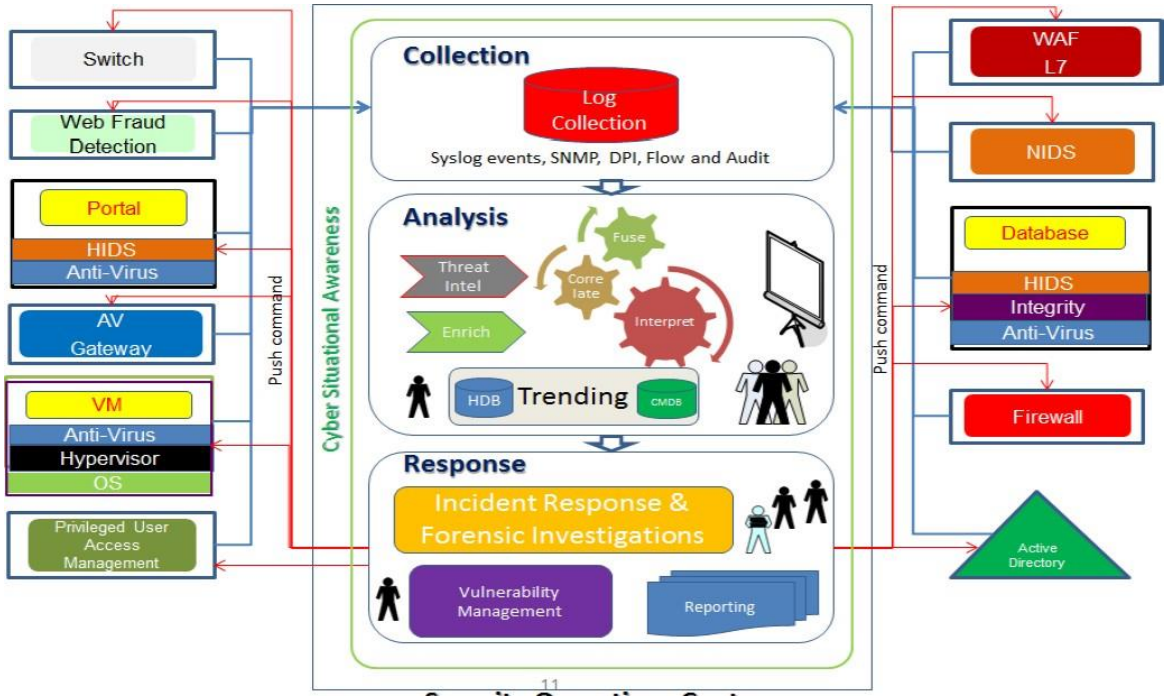


Fuente 9. (Onwubiko, Cyril)

El flujo del monitoreo pasa por diferentes fases, inicialmente se lleva a cabo la recolección y centralización de los registros mediante un colector o una herramienta, como se muestra en la ilustración 9. Posterior a esto los logs avanzan a un proceso de análisis que relaciona diferentes actividades, algunas de manera automatizada mediante inteligencia artificial y otras que deben ser realizadas por los analistas del centro de

operaciones de seguridad, con base a los resultados se debe dar una clasificación a la información, identificación de falsos positivos, o si es el caso generar el alertamiento y continuar con el proceso de respuesta, en la ilustración 10, se muestra una representación de lo que sería un proceso de recolección de logs, análisis y respuesta.

Ilustración 10. Centro de operaciones de seguridad



Fuente 10. (Onwubiko, Cyril)

4.5 MARCO LEGAL

Se lleva a cabo un levantamiento de información de la normativa Colombiana y actualmente se cuenta con la siguiente información relacionada con la protección de información, buscando garantizar la protección de los datos y los sistemas que se hacen uso de las tecnologías de la información, para esto es necesario contemplar los elementos que se listan a continuación:

- Circular externa 007 de 2018 emitida por la super intendencia financiera de Colombia
- Ley 1273 de 2009
- Ley 1581 de 2012

4.5.1 CIRCULAR EXTERNA 007 DE 2018. SFC: Con el fin de garantizar la protección de la información debido al crecimiento de las tecnologías de la información y la ciberseguridad, la super intendencia financiera establece requisitos que deben ser acatadas por las entidades financieras en Colombia, dentro de estos elementos

La circular en el numeral 3 establece las obligaciones generales en materia de ciberseguridad que deben ser aplicadas, en el subnumeral 3.2.8 define lo siguiente:

> 3.2.8. Realizar análisis de riesgo para determinar la pertinencia de contratar o implementar el servicio de un SOC, que puede ser manejado desde el exterior. El análisis debe identificar las características del proveedor y herramientas y servicios que se contratarán.[22]

Con esta se establece la obligación de las entidades financieras para la implementación de un SOC que permita monitorear de manera continua sus sistemas detectando, previniendo y gestionando de manera adecuada las amenazas, eventos o incidentes de ciberseguridad.

4.5.2 Ley 1273 de 2009: Esta ley surge con la necesidad de establecer acciones legales y garantizar la protección de la información y los datos, así como los sistemas de información y cualquier atentado o acción delictiva que atente contra la integridad, confidencialidad y disponibilidad de la información.

[22] SFC. CIRCULAR EXTERNA 007 DE 2018. Colombia, 6 de junio 2018. P. 4

Se establecen unos artículos en los cuales se reglamentan acciones, así mismo se establecen las sanciones y condenas a las cuales puede ser sometido quien incurra en alguna de estas acciones, a continuación, se listan algunos elementos que pueden ser consultados en la documentación oficial del gobierno de Colombia, ley 1273 de 2009.[23]

- Acceso abusivo a un sistema informático
- Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Interceptación de datos informáticos.
- Daño Informático.
- Uso de software malicioso.
- Violación de datos personales.
- Suplantación de sitios web para capturar datos personales.

Así mismo se presentan algunas circunstancias agravantes.

4.5.3 Ley 1581 de 2012: Esta ley establece las reglas generales para la protección y el manejo de los datos personales en Colombia, así mismo establecer los lineamientos y acciones que deben conocer los usuarios sobre el manejo de sus datos, actualización, uso, remoción, entre otros, adicionalmente como las empresas deben dar un correcto tratamiento a la información de los usuarios, bases de datos o archivos, garantizando unas condiciones adecuadas en el almacenamiento, divulgación, transporte y demás elementos necesarios para garantizar la confidencialidad, integridad y disponibilidad.

[23] Ley 1273 de 2009. Gobierno de Colombia.

La ley en su titilo 2[24] establece unos principios rectores, los cuales se listan a continuación, para obtener un mayor detalle pueden ser consultados en la documentación oficial.

- Principio de legalidad en materia de Tratamiento de datos
- Principio de finalidad
- Principio de libertad
- Principio de veracidad o calidad
- Principio de transparencia
- Principio de acceso y circulación restringida
- Principio de seguridad
- Principio de confidencialidad

Así mismo establece unas categorías especiales de datos, como lo son los datos sensibles.

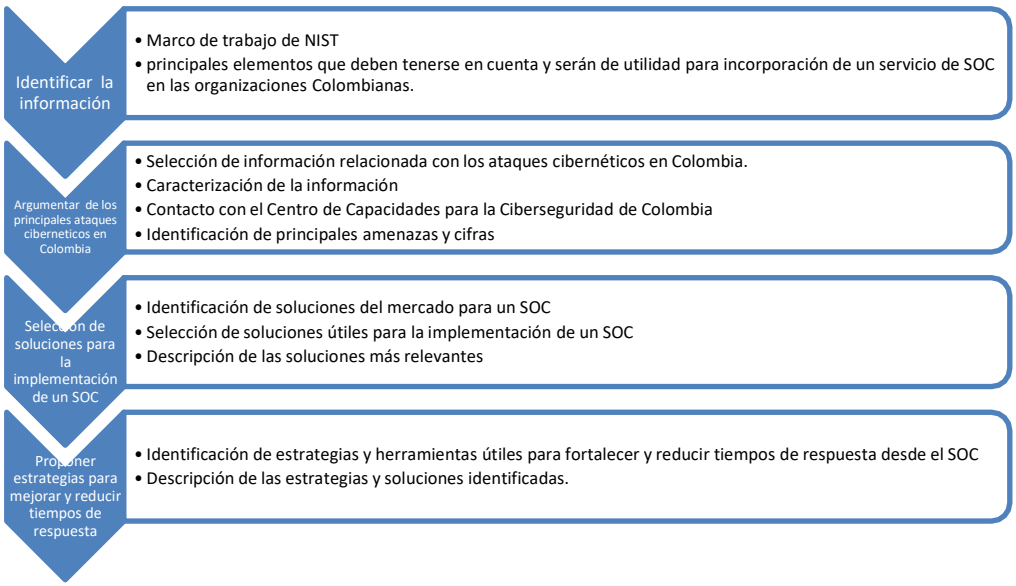
[24] Ley estatutaria 1581 de 2012, p 2,3

5 DESARROLLO DE LOS OBJETIVOS

Para llevar a cabo el cumplimiento del objetivo principal el cual consiste en brindar un apoyo a las organizaciones colombianas con la toma de decisiones a la hora de seleccionar soluciones para el monitoreo y gestión de la seguridad de la información, a partir de la revisión sistemática de diferentes fuentes documentales, para contar con alternativas que permitan el acceso a una base de conocimiento para la toma de decisiones.

En la ilustración 11, se describe de manera sencilla las actividades que ha sido necesario realizar actividades como, identificar, argumentar, seleccionar y proponer, mediante la obtención de diversas fuentes de información documental con referencias que permitan la identificación de alternativas para una solución de monitoreo de seguridad activa y pasiva de infraestructuras tecnológicas apoyado en un servicio de SOC.

Ilustración 11. Fases de la metodología implementada para el cumplimiento de los objetivos.



Fuente 11. Creación propia

5.1 IDENTIFICAR LA INFORMACIÓN RELEVANTE DEL MARCO DE TRABAJO DE NIST, ASÍ COMO LOS PRINCIPALES ELEMENTOS QUE DEBEN TENERSE EN CUENTA Y SERÁN DE UTILIDAD PARA INCORPORACIÓN DE UN SERVICIO DE SOC EN LAS ORGANIZACIONES COLOMBIANAS.

5.1.1 Marco para la mejora de la seguridad cibernética en infraestructuras críticas NIST: Con base a la información suministrada por el instituto nacional de estándares y tecnología NIST, es posible relacionar la siguiente información de utilidad para las organizaciones que desean llevar a cabo la implementación de estrategias de monitoreo continuo de sus sistemas de información mediante la implementación de un SOC.

El marco de ciberseguridad brinda diversas opciones que son de utilidad para cualquier tipo de organización que haga uso de herramientas tecnológicas para su operación, esta brinda diferentes alternativas que podrán ser aplicadas y ajustadas según sea la necesidad de cada organización.

La implementación de mejores prácticas y el intercambio de información, identificar las necesidades y asumir una responsabilidad para la mejora de una postura de seguridad en las organizaciones ayudan a un crecimiento general del país, fortaleciendo las comunicaciones y un manejo adecuado de la información.

Ilustración 12, se realiza un análisis del núcleo del marco para identificar los elementos que son de utilidad para las organizaciones que desean llevar a cabo la implementación de un centro de operaciones de seguridad, (SOC), el núcleo se compone por 4 elementos que serán detallados a continuación: funciones, categorías, subcategorías y referencias informativas.

Ilustración 12. Estructura del núcleo del marco

Fuente 12 NIST. Marco para la mejora de la seguridad cibernética en infraestructuras críticas. 16 de abril de 2018. P. 13.

A continuación, se detalla cada uno de los componentes del núcleo:

Funciones: describe las categorías principales, que son: Identificar, Proteger, Detectar, Responder, Recuperar, las cuales ayudan a las organizaciones en la identificación de actividades alineadas con las metodologías de gestión de incidentes, que les permitirá definir estrategias para actuar de manera adecuada ante la ocurrencia de un evento.

Categorías: Se desprenden a partir de las funciones, permiten identificar los enfoques describiendo cada uno de los puntos que deben ser abordados como, por ejemplo, conocer que se debe identificar, que se quiere proteger, como realizar la detección, como será la respuesta y posteriormente como llevar a cabo la recuperación.

Subcategorías: Brinda una breve descripción de cómo abordar cada una de las categorías dando un enfoque adecuado y describiendo las actividades técnicas que pueden llevarse a cabo para el cumplimiento de los resultados esperados.

Referencias informativas: En este campo se puede encontrar la referenciación a diferentes fuentes de información relacionadas que pueden ser de utilidad para el desarrollo de cada uno de los numerales, se encuentran diferentes normas, buenas prácticas, entre otros.

En la ilustración 13, se encuentran la descripción de los indicadores únicos utilizados en las funciones del marco de trabajo de NIST para su identificación, para tener una mayor comprensión, en la columna Identificador único de función se encuentra el identificador abreviado para cada una de las funciones, ejemplo “ID” para la función identificar, así mismo en la columna identificador único de categoría, se encuentra la unión entre en identificador único de la función con el de la categoría correspondiente, ejemplo, para la categoría Gestion de activos se definen las siglas “AM” para lo cual tendríamos que el identificador único “ID AM” corresponder a la categoría gestión de activos de la función identificar y así sucesivamente para cada una de las funciones y categorías.

Ilustración 13. Indicadores únicos de función y categoría

Identificador único de función	Función	Identificador único de categoría	Categoría
ID	Identificar	ID.AM	Gestión de activos
		ID.BE	Entorno empresarial
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	Proteger	PR.AC	Gestión de identidad y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología protectora
DE	Detectar	DE.AE	Anomalías y eventos
		DE.CM	Vigilancia continua de seguridad
		DE.DP	Procesos de detección
RS	Responder	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
RC	Recuperar	RC.RP	Planificación de recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

Fuente 13. NIST. Marco para la mejora de la seguridad cibernética en infraestructuras críticas. 16 de abril de 2018. P. 30.

Para identificar cuales elementos son de utilidad para las organizaciones que desean incluir en su ciclo de monitoreo continuo de ciberseguridad un centro de operaciones de seguridad (SOC) y como este puede ser apoyado con las funciones del núcleo del marco de ciberseguridad de NIST, se realiza un análisis de cada una se estas, identificando su función, categoría, subcategoría y referencias informativas, seleccionando los elementos más importantes para el tipo de servicio deseado.

Las siguientes tablas, han sido construidos por el autor con base a la información obtenida del documento “Marco para la mejora de la seguridad cibernética en infraestructuras críticas del Instituto Nacional de Estándares y Tecnología publicada el 16 de abril del 2018”.[25]

[25] NIST. Marco para la mejora de la seguridad cibernética en infraestructuras críticas. 16 de abril de 2018. Versión 1.1. p. 55.

En la tabla 1, relacionada a continuación, se realiza una identificación de los elementos más relevantes de la función **identificar** del marco de trabajo de NIST, seleccionando las categorías y subcategorías relevantes para tener en cuenta a la hora de incorporar un servicio de SOC en las organizaciones Colombianas, en cada uno de estos se relacionan las referencias informativas proporcionadas en el marco de trabajo, las cuales pueden ser de utilidad para complementar cada una de las subcategorías y un comentario suministrado por el autor.

Tabla 1. Función Identificar NIST

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
IDENTIFICAR (ID)	Gestión de activos (ID.AM): Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	ID.AM-1: Los dispositivos y sistemas físicos dentro de la organización están inventariados.	CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5	La gestión de los activos es uno de los elementos más importantes en el momento de llevar a cabo la implementación de un servicio de monitoreo de seguridad, ya que es la base para la toma de decisiones sobre los elementos más importantes a monitorear, tener unas definiciones establecidas que permitan establecer casos de uso para una adecuada correlación y alertamiento.
		ID.AM-2: Las plataformas de software y las aplicaciones dentro de la organización están inventariadas.	CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5	

Fuente 14. Creación propia con base al Framework de NIST

Tabla 1 (continuación)

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
IDENTIFICAR (ID)	Gestión de activos (ID.AM)	ID.AM-5: Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) se priorizan en función de su clasificación, criticidad y valor comercial.	CIS CSC 13, 14	
			COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02	
			ISA 62443-2-1:2009 4.2.3.6	
			ISO/IEC 27001:2013 A.8.2.1	
			NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6	
		ID.AM-6: Los roles y las responsabilidades de la seguridad cibernética para toda la fuerza de trabajo y terceros interesados (por ejemplo, proveedores, clientes, socios) están establecidas.	CIS CSC 17, 19	
			COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03	
			ISA 62443-2-1:2009 4.3.2.3.3	
			ISO/IEC 27001:2013 A.6.1.1	
			NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11	

Tabla 1 (continuación)

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
IDENTIFICAR (ID)	Gobernanza (ID.GV): Las políticas, los procedimientos y los procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización se comprenden y se informan a la gestión del riesgo de seguridad cibernética.	ID.GV-1: Se establece y se comunica la política de seguridad cibernética organizacional.	CIS CSC 19	En el momento de establecer actividades de monitoreo, es fundamental que los colaboradores de la organización conozcan cuáles son sus responsabilidades, tener una definición de roles, responsabilidades que permita identificar acciones no autorizadas y contemplar la normatividad vigente del país para no incurrir en violaciones o acciones no autorizadas.
			COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02	
			ISA 62443-2-1:2009 4.3.2.6	
			ISO/IEC 27001:2013 A.5.1.1	
			NIST SP 800-53 Rev. 4-1 controles de todas las familias de control de seguridad	
		ID.GV-2: Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos.	CIS CSC 19	
			COBIT 5 APO01.02, APO10.03, APO13.02, DSS05.04	
			ISA 62443-2-1:2009 4.3.2.3.3	
			ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1	
			NIST SP 800-53 Rev. 4 PS-7, PM-1, PM-2	

Tabla 1 (continuación)

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
IDENTIFICAR (ID)	Gobernanza (ID.GV)	ID.GV-3: Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.	CIS CSC 19	
			COBIT 5 BAI02.01, MEA03.01, MEA03.04	
			ISA 62443-2-1:2009 4.4.3.7	
			ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5	
			NIST SP 800-53 Rev. 4-1 controles de todas las familias de control de seguridad	
	Evaluación de riesgos (ID.RA): La organización comprende el riesgo de seguridad cibernética para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.	ID.RA-1: Se identifican y se documentan las vulnerabilidades de los activos.	CIS CSC 4	
			COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02	
			ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9,	
			4.2.3.12	
			ISO/IEC 27001:2013 A.12.6.1, A.18.2.3	
			NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	

Tabla 1 (continuación)

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
IDENTIFICAR (ID)	Evaluación de riesgos (ID.RA)	ID.RA-2: La inteligencia de amenazas cibernéticas se recibe de foros y fuentes de intercambio de información.	CIS CSC 4 COBIT 5 BAI08.01 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16	Es de utilidad para la adecuada gestión del centro de operaciones de seguridad SOC y el monitoreo continuo que se realiza, llevar a cabo una oportuna identificación y análisis de las vulnerabilidades existentes, bien sea ya conocidas o nuevas (de día 0), realizar una correlación e identificar como estas pueden afectar los activos de la organización, con base a esto establecer un alertamiento preventivo evitando así un posible incidente de seguridad, del mismo modo identificar los posibles impactos a los cuales podría estar expuesta la organización y definir los tiempos de respuesta mediante una priorización según el riesgo identificado.
		ID.RA-5: Se utilizan las amenazas, las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo.	CIS CSC 4 COBIT 5 APO12.02 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16	
		ID.RA-6: Se identifican y priorizan las respuestas al riesgo.	CIS CSC 4 COBIT 5 APO12.05, APO13.02 ISO/IEC 27001:2013 Cláusula 6.1.3 NIST SP 800-53 Rev. 4 PM-4, PM-9	

En la tabla 2, relacionada a continuación, se realiza una identificación de los elementos más relevantes de la función **proteger** del marco de trabajo de NIST, seleccionando las categorías y subcategorías relevantes para tener en cuenta a la hora de incorporar un servicio de SOC en las organizaciones Colombianas, en cada uno de estos se relacionan las referencias informativas proporcionadas en el marco de trabajo, las cuales pueden ser de utilidad para complementar cada una de las subcategorías y un comentario suministrado por el autor.

Tabla 2. Función Proteger NIST

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
PROTEGER (PR)	Gestión de identidad, autenticación y control de acceso (PR.AC): El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	PR.AC-1: Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.	CIS CSC 1, 5, 15, 16 COBIT 5 DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	En el momento de establecer un servicio de monitoreo de seguridad, se debe contemplar como medida principal las fuentes que gestionan los accesos, como lo son los servidores de directorio activo o aplicativos de gestión de identidades.

Fuente 15. Creación propia con base al Framework de NIST

Tabla 2. (Continuación)

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
PROTEGER (PR)	Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-4: Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.	CIS CSC 3, 5, 12, 14, 15, 16, 18 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.7.3 ISA 62443-3-3:2013 SR 2.1 ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24	De esta manera poder establecer controles de monitoreo con los accesos previamente definidos a los usuarios, logrando establecer alertas que permitan identificar comportamientos inusuales, prestamos de credenciales, accesos desde diferentes ubicaciones, intentos de conexiones a servidores o aplicativos no autorizados, entre otros factores.
		PR.AC-5: Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red).	CIS CSC 9, 14, 15, 18 COBIT 5 DSS01.05, DSS05.02 ISA 62443-2-1:2009 4.3.3.4 ISA 62443-3-3:2013 SR 3.1, SR 3.8 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7	

Tabla 2. (Continuación)

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
PROTEGER (PR)	Seguridad de los datos (PR.DS): La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	PR.DS-1: Los datos en reposo están protegidos.	CIS CSC 13, 14	Uno de los elementos más valiosos para las organizaciones son los datos, por esta razón, es de suma importancia establecer lineamientos para su almacenamiento, transporte y fuga de información, con base a estas definiciones, desde el monitoreo continuo, será necesario implementar reglas de correlación y alertamiento que permitan identificar acciones inusuales que se presenten en caso de que se evidencie un comportamiento inusual.
			COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06	
			ISA 62443-3-3:2013 SR 3.4, SR 4.1	
			ISO/IEC 27001:2013 A.8.2.3	
			NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28	
		PR.DS-2: Los datos en tránsito están protegidos.	CIS CSC 13, 14	
			COBIT 5 APO01.06, DSS05.02, DSS06.06	
			ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR	
			4.2	
			ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1,	
			A.13.2.3, A.14.1.2, A.14.1.3	
			NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12	

Tabla 2. (Continuación)

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
PROTEGER (PR)	Seguridad de los datos (PR.DS)	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.	CIS CSC 13 COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 ISA 62443-3-3:2013 SR 5.2 ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4,A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4	

Tabla 2. (Continuación)

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
PROTEGER (PR)	Procesos y procedimientos de protección de la información (PR.IP): Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	PR.IP-1: Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).	CIS CSC 3, 9, 11 COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	Contar con líneas base previamente definidas por la organización ayudara en la implementación de casos de uso específicos, definiendo puntos de monitoreo que permitan identificar acciones inusuales generando de esta manera el alertamiento, como fuente principal de alimentación al equipo de respuesta a incidentes de seguridad,

Tabla 2. (Continuación)

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
PROTEGER (PR)	Procesos y procedimientos de protección de la información (PR.IP)	PR.IP-9: Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).	CIS CSC 19 COBIT 5 APO12.06, DSS04.03 ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17	los cuales deberán actuar de manera oportuna permitiendo la continuidad de la operación del negocio si se presenta un incidente de seguridad, manteniendo un monitoreo continuo desde el centro de operaciones de seguridad, se facilita la detección oportuna y reducir tiempos de indisponibilidad.

Tabla 2. (Continuación)

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
PROTEGER (PR)	Tecnología de protección (PR.PT): Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, en consonancia con las políticas, procedimientos y acuerdos relacionados.	PR.PT-1: Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan en conformidad con la política.	CIS CSC 1, 3, 5, 6, 14, 15, 16 COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 NIST SP 800-53 Rev. 4 Familia AU	Establecer un adecuado registro de auditoria en los servicios, aplicativos y dispositivos es el elemento más importante para llevar a cabo el monitoreo de información desde un centro de operaciones de seguridad, la recolección de estos registros permite llevar a cabo la normalización y entendimiento, permitiendo así la identificación de elementos maliciosos en la operación.

En la tabla 3, relacionada a continuación, se realiza una identificación de los elementos más relevantes de la función **detectar** del marco de trabajo de NIST, seleccionando las categorías y subcategorías relevantes para tener en cuenta a la hora de incorporar un servicio de SOC en las organizaciones Colombianas, en cada uno de estos se relacionan las referencias informativas proporcionadas en el marco de trabajo, las cuales pueden ser de utilidad para complementar cada una de las subcategorías y un comentario suministrado por el autor.

Tabla 3. Función Detectar NIST

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
DETECTAR (DE)	Anomalías y Eventos (DE.AE): se detecta actividad anómala y se comprende el impacto potencial de los eventos.	DE.AE-1: Se establece y se gestiona una base de referencia para operaciones de red y flujos de datos esperados para los usuarios y sistemas.	CIS CSC 1, 4, 6, 12, 13, 15, 16 COBIT 5 DSS03.01 ISA 62443-2-1:2009 4.4.3.3 ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4	Es en esta fase donde toma mayor relevancia el monitoreo continuo, para lo cual surge la necesidad de llevar a cabo la implementación de un servicio de SOC, que lleve a cabo las actividades necesarias para la recolección, correlación, afinamiento y alertamiento de los registros de información.
		DE.AE-2: Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.	CIS CSC 3, 6, 13, 15 COBIT 5 DSS05.07 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4	

Fuente 16. Creación propia con base al Framework de NIST

Tabla 3. (Continuación)

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
DETECTAR (DE)	Anomalías y Eventos (DE.AE)	DE.AE-3: Los datos de los eventos se recopilan y se correlacionan de múltiples fuentes y sensores.	CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16	
			COBIT 5 BAI08.02	
			ISA 62443-3-3:2013 SR 6.1	
			ISO/IEC 27001:2013 A.12.4.1, A.16.1.7	
			NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	
		DE.AE-4: Se determina el impacto de los eventos.	CIS CSC 4, 6	
			COBIT 5 APO12.06, DSS03.01	
			ISO/IEC 27001:2013 A.16.1.4	
			NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4	
		DE.AE-5: Se establecen umbrales de alerta de incidentes.	CIS CSC 6, 19	
			COBIT 5 APO12.06, DSS03.01	
			ISA 62443-2-1:2009 4.2.3.10	
			ISO/IEC 27001:2013 A.16.1.4	
			NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8	

Tabla 3. (Continuación)

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
DETECTAR (DE)	Monitoreo Continuo de la Seguridad (DE.CM): El sistema de información y los activos son monitoreados a fin de identificar eventos de seguridad cibernética y verificar la eficacia de las medidas de protección.	DE.CM-1: Se monitorea la red para detectar posibles eventos de seguridad cibernética.	CIS CSC 1, 7, 8, 12, 13, 15, 16	Establecer acciones de monitoreo con base a las líneas base establecidas por la organización permitirán una detección oportuna de actividad sospechosa, eventos o posibles incidentes de seguridad, para esto es fundamental el monitoreo continuo de la red y dispositivos de información.
			COBIT 5 DSS01.03, DSS03.05, DSS05.07	
			ISA 62443-3-3:2013 SR 6.2	
			NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	
		DE.CM-3: Se monitorea la actividad del personal para detectar posibles eventos de seguridad cibernética.	CIS CSC 5, 7, 14, 16	
			COBIT 5 DSS05.07	
			ISA 62443-3-3:2013 SR 6.2	
			ISO/IEC 27001:2013 A.12.4.1, A.12.4.3	
			NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	
		DE.CM-4: Se detecta el código malicioso.	CIS CSC 4, 7, 8, 12	
			COBIT 5 DSS05.01	
			ISA 62443-2-1:2009 4.3.4.3.8	
			ISA 62443-3-3:2013 SR 3.2	
			ISO/IEC 27001:2013 A.12.2.1	
			NIST SP 800-53 Rev. 4 SI-3, SI-8	
		DE.CM-5: Se detecta el código móvil no autorizado.	CIS CSC 7, 8	
			COBIT 5 DSS05.01	
			ISA 62443-3-3:2013 SR 2.4	
			ISO/IEC 27001:2013 A.12.5.1, A.12.6.2	
			NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44	

Tabla 3. (Continuación)

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
DETECTAR (DE)	Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-6: Se monitorea la actividad de los proveedores de servicios externos para detectar posibles eventos de seguridad cibernética.	COBIT 5 APO07.06, APO10.05	
			ISO/IEC 27001:2013 A.14.2.7, A.15.2.1	
			NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4	
		DE.CM-7: Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados.	CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16	
			COBIT 5 DSS05.02, DSS05.05	
			ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1	
			NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	
	Procesos de Detección (DE.DP)	DE.DP-1: Los roles y los deberes de detección están bien definidos para asegurar la responsabilidad.	CIS CSC 19	
			COBIT 5 APO01.02, DSS05.01, DSS06.03	
			ISA 62443-2-1:2009 4.4.3.1	
			ISO/IEC 27001:2013 A.6.1.1, A.7.2.2	
			NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14	

Tabla 3. (Continuación)

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
DETECTAR (DE)	Se mantienen y se aprueban los procesos y procedimientos de detección para garantizar el conocimiento de los eventos anómalos.	DE.DP-2: Las actividades de detección cumplen con todos los requisitos aplicables.	COBIT 5 DSS06.01, MEA03.03, MEA03.04	Es necesario definir las responsabilidades del centro de operaciones de seguridad, las acciones que se deben implementar cuando se identifique una alerta, realizar cambios y afinamientos de manera continua y realizando pruebas a los casos de uso, de esta manera garantizar el adecuado funcionamiento del servicio y la detección, notificación y respuesta oportuna ante una posible amenaza.
			ISA 62443-2-1:2009 4.4.3.2	
			ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3	
			NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, SA-18, SI-4, PM-14	
		DE.DP-3: Se prueban los procesos de detección.	COBIT 5 APO13.02, DSS05.02	
			ISA 62443-2-1:2009 4.4.3.2	
			ISA 62443-3-3:2013 SR 3.3	
			ISO/IEC 27001:2013 A.14.2.8	
			NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, SI-3, SI-4, PM-14	

Tabla 3. (Continuación)

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
DETECTAR (DE)	Procesos de Detección (DE.DP):	DE.DP-4: Se comunica la información de la detección de eventos.	CIS CSC 19	
			COBIT 5 APO08.04, APO12.06, DSS02.05	
			ISA 62443-2-1:2009 4.3.4.5.9	
			ISA 62443-3-3:2013 SR 6.1	
			ISO/IEC 27001:2013 A.16.1.2, A.16.1.3	
			NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4	
		DE.DP-5: los procesos de detección se mejoran continuamente.	COBIT 5 APO11.06, APO12.06, DSS04.05	
			ISA 62443-2-1:2009 4.4.3.4	
			ISO/IEC 27001:2013 A.16.1.6	
			NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA- 5, SI-4, PM-14	

En la tabla 4, relacionada a continuación, se realiza una identificación de los elementos más relevantes de la función **responder** del marco de trabajo de NIST, seleccionando las categorías y subcategorías relevantes para tener en cuenta a la hora de incorporar un servicio de SOC en las organizaciones Colombianas, en cada uno de estos se relacionan las referencias informativas proporcionadas en el marco de trabajo, las cuales pueden ser de utilidad para complementar cada una de las subcategorías y un comentario suministrado por el autor.

Tabla 4. Función Responder NIST

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
RESPONDER (RS)	Planificación de la Respuesta (RS.RP): Los procesos y procedimientos de respuesta se ejecutan y se mantienen a fin de garantizar la respuesta a los incidentes de seguridad cibernética detectados.	RS.RP-1: El plan de respuesta se ejecuta durante o después de un incidente.	CIS CSC 19 COBIT 5 APO12.06, BAI01.10 ISA 62443-2-1:2009 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8	El centro de operaciones de seguridad deberá establecer las acciones que estén a su alcance para responder ante un posible incidente de seguridad, estas acciones deberán ser previamente definidas y documentas, es recomendable implementar playbooks para seguir estas indicaciones.

Fuente 17. Creación propia con base al Framework de NIST

Tabla 4. (Continuación)

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
RESPONDER (RS)	Comunicaciones (RS.CO): Las actividades de respuesta se coordinan con las partes interesadas internas y externas (por ejemplo, el apoyo externo de organismos encargados de hacer cumplir la ley).	RS.CO-1: El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.	CIS CSC 19 COBIT 5 EDM03.02, APO01.02, APO12.03 ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, A.16.1.1 NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8	El centro de operaciones de seguridad deberá contar con la documentación necesaria para saber cómo actuar cuando se presente un evento o incidente de seguridad, este funciona como fuente de alimentación del equipo de respuesta a incidentes de seguridad de la información quien a su vez será el encargado de establecer e implementar las acciones de respuesta.
		RS.CO-2: Los incidentes se informan de acuerdo con los criterios establecidos.	CIS CSC 19 COBIT 5 DSS01.03 ISA 62443-2-1:2009 4.3.4.5.5 ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8	

Tabla 4. (Continuación)

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
RESPONDER (RS)	Comunicaciones (RS.CO)	RS.CO-3: La información se comparte de acuerdo con los planes de respuesta.	CIS CSC 19 COBIT 5 DSS03.04 ISA 62443-2-1:2009 4.3.4.5.2 ISO/IEC 27001:2013 A.16.1.2, Cláusula 7.4, Cláusula 16.1.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4	
		RS.CO-4: La coordinación con las partes interesadas se realiza en consonancia con los planes de respuesta.	CIS CSC 19 COBIT 5 DSS03.04 ISA 62443-2-1:2009 4.3.4.5.5 ISO/IEC 27001:2013 Cláusula 7.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	

En la tabla 5, relacionada a continuación, se realiza una identificación de los elementos más relevantes de la función **recuperar** del marco de trabajo de NIST, seleccionando las categorías y subcategorías relevantes para tener en cuenta a la hora de incorporar un servicio de SOC en las organizaciones Colombianas, en cada uno de estos se relacionan las referencias informativas proporcionadas en el marco de trabajo, las cuales pueden ser de utilidad para complementar cada una de las subcategorías y un comentario suministrado por el autor.

Tabla 5. Función Recuperar NIST

Elementos útiles del núcleo para la implementación de un SOC				
Función	**Categoría**	**Subcategoría**	**Referencias informativas**	**Comentarios**
RECUPERAR (RC)	Mejoras (RC.IM): La planificación y los procesos de recuperación se mejoran al incorporar en las actividades futuras las lecciones aprendidas.	RC.IM-1: Los planes de recuperación incorporan las lecciones aprendidas.	COBIT 5 APO12.06, BAI05.07, DSS04.08 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6, Cláusula 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	Sera necesario evaluar lo sucedido e identificar si las detecciones y notificaciones se realizaron de manera adecuada y oportuna desde el centro de operaciones de seguridad, evaluar si es necesario realizar afinamientos en la correlación y alertamiento para que el servicio tenga una mejora continua.

Fuente 18. Creación propia con base al Framework de NIST

5.1.2 Circular externa 007 de 2018, super intendencia financiera de Colombia: El 5 de junio del año 2018, la super intendencia financiera de Colombia, emitió la circular externa 007 en la cual imparte instrucciones relacionadas con los requerimientos mínimos para la gestión de riesgos de ciberseguridad, siendo así se realiza la revisión de esta para identificar como deben las entidades financieras en Colombia asumir la necesidad de implementación de un centro de operaciones de seguridad (SOC) que permita realizar un monitoreo continuo de sus sistemas de información.

En el parágrafo segundo de dicha circular se indica como entrara a operar la circular, comenzando a regir 6 meses después de su publicación, algunos elementos deberán ser aplicados en un término de un año y otro a los 18 meses de su publicación que se realizó el 5 de junio de 2018, siendo así, la circular deberá estar cubierta para el 6 de diciembre del año 2020.

La circular en el numeral 3 establece las obligaciones generales en materia de ciberseguridad que deben ser aplicadas, en el subnumeral 3.2.8 define lo siguiente:

> "3.2.8. Realizar análisis de riesgo para determinar la pertinencia de contratar o implementar el servicio de un SOC, que puede ser manejado desde el exterior. El análisis debe identificar las características del proveedor y herramientas y servicios que se contratarán."[26]

5.1.3 Automatización de servicios de seguridad: El crecimiento tecnológico y el avance de las tecnologías lleva a las organizaciones a implementar nuevas estrategias para la gestión de la seguridad y la protección de sus activos tecnológicos, para lo cual es fundamental la adopción de nuevas estrategias, como lo es inteligencia de amenazas, automatización de respuestas, aplicación de inteligencia artificial para el análisis continuo de vulnerabilidades, es necesario contemplar estrategias y con base a la información

[26] SFC. CIRCULAR EXTERNA 007 DE 2018. Colombia, 6 de junio 2018. P. 4

relacionada anteriormente definir unos pasos a seguir para garantizar la protección de la organización ante posibles amenazas cibernéticas.

Las organizaciones deberán aplicar planes de crecimiento y fortalecimiento continuo que permitan establecer un plan de trabajo para fortalecer su postura de ciberseguridad y defensa, algunos elementos a tener en cuenta son:

- **Prevención;** ejecutar un análisis del estado actual de la organización, realizar un análisis de riesgos y aplicar los controles pertinentes para prevenir los riesgos identificados.
- **Detección:** una vez identificados los riesgos de la organización, esta deberá establecer acciones y herramientas que permitan llevar a cabo la oportuna detección de comportamientos anómalos dentro y fuera de la infraestructura, para lo cual se propone ejecutar actividades de monitoreo continuo, será necesario la adquisición de herramientas como SIEM, inteligencia de amenazas, aprendizaje del comportamiento de red que permita identificar variaciones y responder oportunamente, entre otros elementos que permitan llevar a cabo el monitoreo de los eventos y sucesos que ocurren en las plataformas tecnológicas.
- **Respuesta:** Establecer acciones de respuesta que puedan facilitar la reacción ante un evento o incidente de ciberseguridad, reduciendo los tiempos, documentar estas acciones en elementos como playbook o reglas de juego que permitan conocer de manera anticipada como proceder ante una situación de emergencia, emplear acciones de respuesta automatizada, mediante la aplicación de scripts e integraciones con las herramientas, SOAR.
- **Predicción:** Llevar a cabo monitoreos más amplios que permitan conocer la situación actual de la ciberseguridad, actuando de manera predictiva ante una posible amenaza, identificar nuevas vulnerabilidades, correlacionarlas con la infraestructura de la organización, aplicar elementos de análisis de comportamiento de usuarios y la organización, (UEBA) conocer y aprender cómo se mueve la organización y actividades ejecutan los usuarios de manera general

permitirá anticiparse a una posible alteración del comportamiento, actuando de manera oportuna para prevenir posibles incidentes de ciberseguridad. [27]

5.1.4 Como salir adelante a los ciberdelincuentes con la ayuda de un SOC: El reporte suministrado por la empresa de consultoría EY en octubre de 2014[28], hace relevancia a la importancia de un centro de operaciones de seguridad con un adecuado funcionamiento y con 10 elementos fundamentales a trabajar para que este aporte a la organización acciones de respuesta oportunas y tenga un desempeño exitoso.

- **Apoyo de la junta directiva**, es indispensable contar con el apoyo de la alta dirección y que se evidencien cuáles son los beneficios de contar con un SOC para la protección de los activos de información de la organización.
- **Inversión:** la madurez de un centro de operaciones de seguridad requiere una inversión de parte de las organizaciones, no solo económica sino también de recurso humano.
- **Estrategia:** Es fundamental trabajar para lograr los objetivos de la organización, construir una estrategia alineada con los niveles de riesgo, que permitan un crecimiento seguro y garantizar el adecuado cumplimiento de la protección de los activos de información.
- **Personas:** Un SOC requiere de personal con diversas capacidades y conocimientos, que cuenten con habilidades para realizar análisis de gran cantidad de datos y su vez lograr identificar las prioridades, contar con habilidades comunicativas para lograr una transferencia de conocimiento adecuada y oportuna con los demás equipos de soporte requeridos para el análisis de un posible incidente y lograr la resolución.

[27] B-SECURE. Para enfrentar los adversarios cibernéticos de hoy se necesita de una visión holística de seguridad.

[28]EY. Security Operations Centers helping you get aheadof cybercrime. 2014

- **Procesos:** Es necesario que el SOC comprenda los procesos de la organización, así mismo contribuya a una constante actualización aportando acciones de mejora con base a los hallazgos identificados durante el proceso de monitoreo continuo.
- **Tecnología:** Es necesario ir más allá de las tecnologías, la organización puede disponer de elementos muy sofisticados, pero se requiere un conocimiento adecuado que permita obtener el mayor provecho de este, es fundamental obtener un adecuado entrenamiento en el uso de herramientas y tecnologías, de esta manera las organizaciones podrán obtener el beneficio esperado, buscar alternativas con las tecnologías ya adquiridas y evitar compras innecesarias.
- **El entorno:** es fundamental que desde el SOC se tenga un amplio conocimiento de cómo opera la organización, cuáles son sus estrategias y necesidades, conocer las líneas base y un inventario de activos que este contantemente actualizado, esta información permitirá tomar mejores decisiones de manera oportuna ya que desde el servicio de monitoreo se evidencia una gran cantidad de información que requiere una adecuada depuración para lograr obtener resultados satisfactorios.
- **Análisis e informes:** El SOC recibe y correlaciona una gran cantidad de datos con el objetivo principal de encontrar elementos inusuales que puedan conllevar a un incidente de seguridad, con base a esta información el SOC debe estar en la capacidad de automatizar reportes, realizar analítica y lograr construir reportes importantes con base a la información recopilada.
- **Espacio físico:** Se debe contar con un espacio adecuado y aislado con fuertes controles de acceso que permitan al equipo realizar actividades de manera colaborativa, el SOC requiere la participación de diferentes colaboradores que logren obtener visión desde diferentes puntos de vista para lograr una adecuada identificación de elementos y configurar acciones afectivas.
- **Mejora continua:** El SOC es una solución que requiere de un continuo crecimiento y mejora de los procesos, es necesario realizar la revisión continua de la información recolectada, establecer nuevas estrategias que ayuden a fortalecer la detección y anticiparse a las amenazas que día a día surgen en la web, un centro de operaciones de seguridad requiere estar evaluando de manera continua la

infraestructura monitoreada, entenderla y crear y actualizar los casos de uso y reglas de correlación que permitan la oportuna detección de eventos e incidentes.

5.2 ARGUMENTAR LOS PRINCIPALES ATAQUES CIBERNÉTICOS A LOS CUALES ESTÁN EXPUESTAS LAS ORGANIZACIONES EN COLOMBIA QUE PERMITA LA IDENTIFICACIÓN OPORTUNA DE AMENAZAS CON LA IMPLEMENTACIÓN DE UN SERVICIO DE MONITOREO DE CIBERSEGURIDAD.

El gobierno de Colombia ha definido el centro cibernético de la policía nacional, el cual se encarga de realizar un monitoreo continuo a los ataques, eventos e incidentes cibernéticos que ocurren en el país, algunos de estos son denunciados y otros no son denunciados por la ciudadanía.

Se realiza un análisis de la información dispuesta por el CSIRT de la policía nacional de Colombia en sus fuentes de información, reportes y sitio web en el cual se puede realizar una validación en tiempo real del estado de los incidentes cibernéticos con lo cual se busca conocer cuáles son los principales ataques cibernéticos que se han identificado y reportado en organizaciones Colombianas los cuales servirán como base para argumentar las necesidades que se tienen actualmente en las empresas para la implementación de un centro de operaciones de seguridad, desde el cual se pueda llevar a cabo la aplicación de una correcta estrategia de ciberseguridad con base a las funciones del marco de trabajo del NIST, lo cual permitirá un correcto monitoreo, detección oportuna, respuesta, prevención y demás acciones para garantizar la protección de la seguridad de la información de manera continua.

La información relacionada a continuación es extraída del estudio de tendencias del Cibercrimen 2019-2020 suministrado por el Tanque de Análisis y Creatividad de las TIC

- TicTac de la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) y su programa SAFE en asocio con la Policía Nacional de Colombia.[29]

El estudio presentado se basa en la información suministrada por la ciudadanía, empresas, personas y entidades que sufren algún evento o incidente de ciberseguridad y generan su denuncia ante el centro cibernético policial, durante el años 2019 se recibieron 15948 denuncias relacionadas con infracciones a la ley 1273 de 2009, que fueron analizadas por los expertos en ciberseguridad, para construir acciones que permitan identificar amenazas, sensibilizar a la comunidad, prepararse para afrontar y prevenir incidentes cibernéticos y planear estrategias predictivas para lo que podría generarse en el año siguiente.

El centro cibernético policial brinda a la comunidad herramientas para el reporte y análisis de eventos, programas o archivos sospechosos, brindando acceso a una herramienta llamada SandBox o caja de arena conocida en el mundo de la ciberseguridad la cual realiza un análisis de los elementos para identificar si contiene acciones o elementos maliciosos.

Estas herramientas pueden ser consultadas en el sitio web del CSIRT de la policía nacional o a través del enlace https://cc-csirt.policia.gov.co/Sandbox allí se carga la información para que sea analizada y visualizar los resultados.

Ilustración 14, las cifras de denuncias de ciber delitos ha ido creciendo de manera significativa durante los últimos años, a continuación, se relaciona una gráfica del informe de tendencias de cibercrimen en la cual se puede evidenciar un crecimiento de poco más del 100% entre el 2015 y el 2019, esto refleja también el crecimiento del uso de las tecnologías de información en el país.

[29] TIC-TAC, CCIT, Ponal, Tendencias cibercrimen Colombia 2019-2020

Ilustración 14. Denuncias de ciberdelitos en los últimos años

Fuente 19. SIEDCO Policía, SPOA, Fiscalía, ADenunciar.

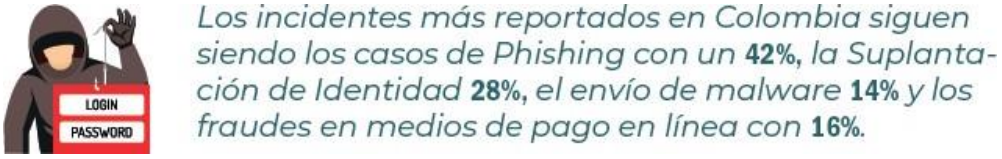
Ilustración 15, los incidentes que encabezan las denuncias en Colombia son los siguientes:

- Phishing
- Suplantación de identidad
- Envío de Malware
- Fraudes en medios de pago en línea

Como se evidencia en el reporte presentado por el centro cibernético de la policía nacional y lo indicado en la ilustración 15, los principales incidentes que se presentan actualmente en las organizaciones Colombianas y que han tenido un constante crecimiento van relacionados con la suplantación de identidad y los cuales buscan realizar ataques dirigidos al usuario final, las empresas de seguridad han venido trabajando de manera continua en el desarrollo y fortalecimiento de herramientas para la prevención de ciberataques y la detección y bloqueo de amenazas, es por esto que los ciberdelincuentes han ido cambiando sus estrategias y lo que buscan es aprovecharse del desconocimiento del usuario final, lo cual lo convierte en un punto débil para las organizaciones el cual puede ser mitigado mediante las capacitaciones y entrenamiento a los empleados pero en ocasiones no se da la importancia y no se realiza de manera consciente, con base a esto se puede observar que los ataques como el Phishing, la

suplantación de identidad y muchos otros que buscan engañar al usuario para obtener información o lograr accesos no autorizados les han dado resultados satisfactorios para lograr su cometido, es por esto que es importante establecer una adecuada estrategia de monitoreo aplicando estrategias como la inteligencia de amenazas, análisis de comportamiento, respuestas automatizadas las cuales permitirán con base al monitoreo conocer como es el comportamiento de los usuarios, de los sistemas, de la red y aplicar acciones en caso de evidenciar posibles cambios que puedan generar afectaciones al desarrollo de las operaciones.

Ilustración 15. Incidentes más reportados en Colombia

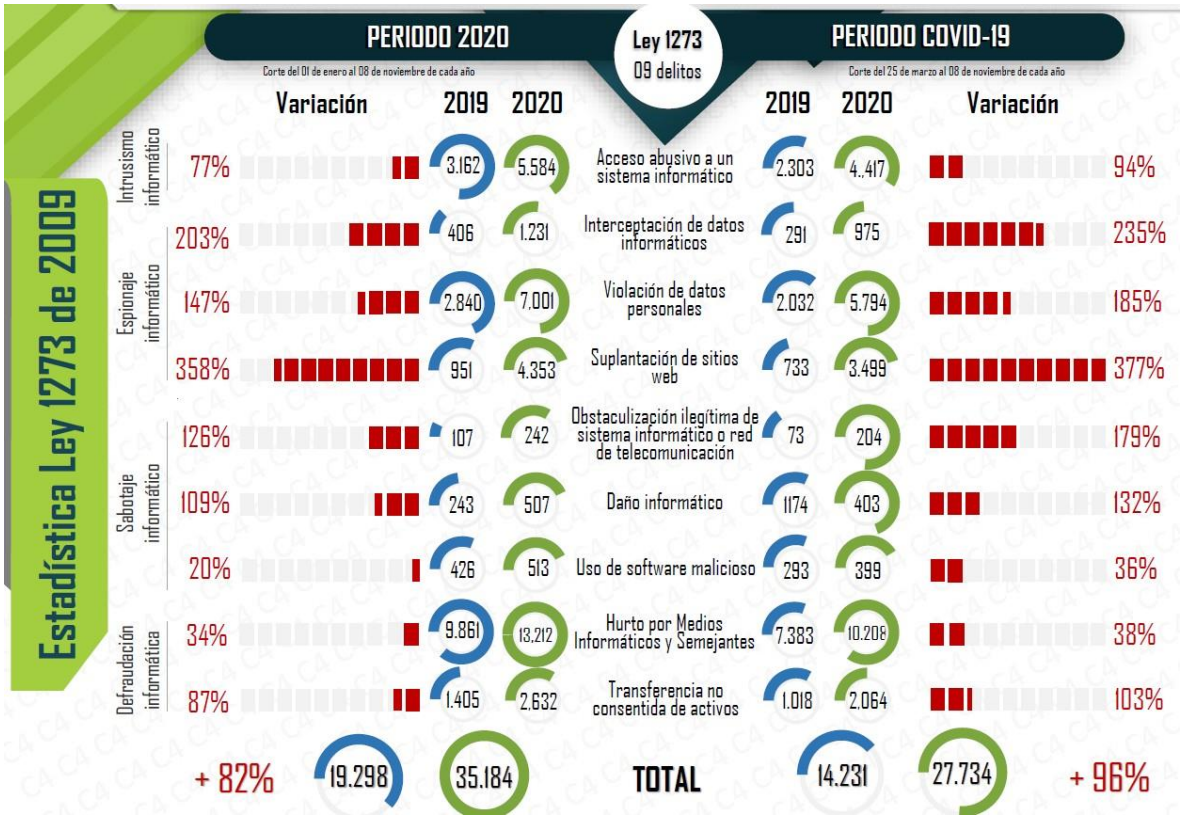


Fuente 20. Tic-Tac, CCIT, Ponal, Tendencias cibercrimen Colombia 2019-2020

Ilustración 16, el incremento del uso de las tecnologías de información, compras electrónicas y demás transacciones que se llevan a cabo en la web, incentiva a los ciberdelincuentes a desarrollar nuevas técnicas y estrategias para llevar a cabo ataques informáticos, a continuación, se relacionan las cifras comparativas de ataques relacionados con la ley 1273 de 2009 entre 2019 y 2020 con base al balance de cibercrimen del 2020 suministrado por el centro cibernético de la policía. [30]

[30] Balance Cibercrimen Policía, reporte BLSC20335DS1 semana #45

Ilustración 16. Balance Cibercrimen semana # 45 2020



Fuente 21. Balance Cibercrimen Policía, reporte BLSC20335DS1 semana #45 2020

Ilustración 17, en la cual se describe el porcentaje de afectación identificado por ciudad en Colombia con base al análisis de la información realizada por SIEDCO, sistema de información estadístico, delincuencial, contravencional y operativo de la policía nacional.

Ilustración 17. Afectación de incidentes por ciudad semana #45 de 2020

Fuente 22. SIEDCO

En la tabla 6, se realiza un comparativo de los delitos informáticos reportados al centro de operaciones de la policía separándolos por ciudad, comparando el año 2019 y el 2020.

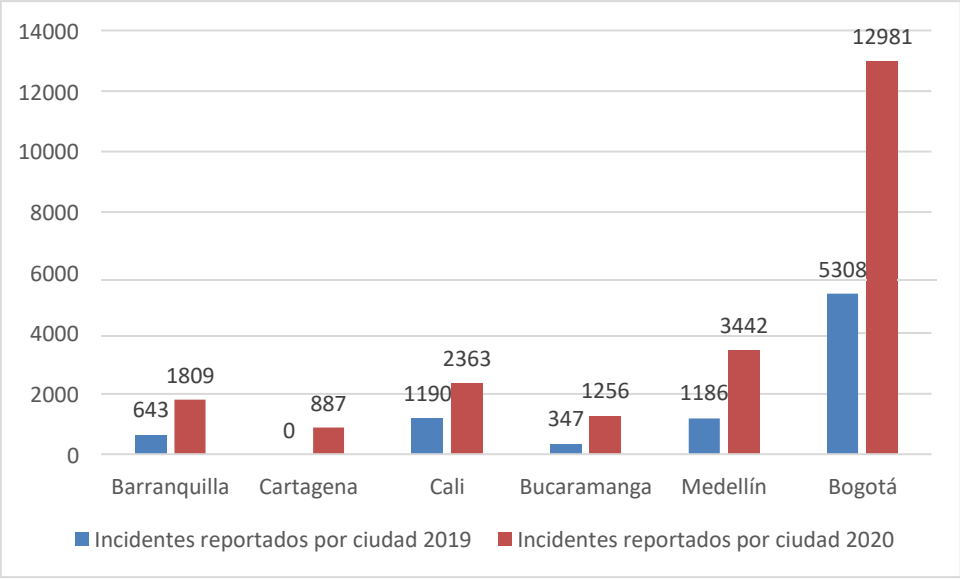
Tabla 6. Delitos informáticos por ciudad 2019-2020

Incidentes reportados por ciudad		
Ciudad	**2019**	**2020**
Barranquilla	643	1809
Cartagena	Sin registro	887
Cali	1190	2363
Bucaramanga	347	1256
Medellín	1186	3442
Bogotá	5308	12981

Fuente 23. Creación propia con información de SIEDCO

Ilustración 18, en la cual se grafica un comparativo de los delitos informáticos identificados en Colombia durante los periodos 2019 y 2020 por ciudad, en la cual se evidencia un crecimiento significativo para el año 2020 en todas las ciudades.

Ilustración 18. Delitos informáticos por ciudad comparativo 2019-2020



Fuente 24. Creación propia con base en información de SIEDCO

A continuación, se listan algunos de los ataques informáticos más comunes y reiterativos que han sido identificados por el centro cibernético de la policía nacional.

- Ataques BEC, compromiso de correo electrónico.
    - Estafa de CEO.
    - Suplantación de clientes.
- Ataques de Ransomware
- Ataques de DDoS
- Malware.
- SIM SWAPPING. (Secuestro o cambio de Sim Card)
- Cyptojacking, minería de criptomonedas.

5.2.1 Incidentes más relevantes en Colombia en 2020 y 2021: Tabla 7, se realizó una consulta directamente Centro de Capacidades para la Ciberseguridad de Colombia (C-4) Dirección de Investigación Criminal e INTERPOL mediante el correo electrónico dijin.cecip-jef@policia.gov.co solicitando información que puedan suministrar de los registros de incidentes del año 2020 y lo corrido del 2021 hasta el mes de julio, en respuesta han brindado la siguiente información.

Tabla 7. Tipo de incidentes y cifras 2020, Julio 2021

Modalidad	2020	2021
Estafa - compra/venta de productos/servicios en Internet	2800	1059
Malware	1141	378
Suplantación de Identidad	2144	1407
Phishing	2327	1948
Vishing	1176	347
Amenazas a través de redes sociales	1033	437
Smishing	663	306
Publicación de imágenes/videos con pornografía infantil	93	49
Injuria y/o Calumnia a través de redes sociales	727	246
Sextorsión	704	269
Ingeniería social	135	83
Cyberbullying	53	209
Carta nigeriana	341	183
Defacement	11	22
Ransomware	169	45
Skimming	62	6
Grooming	254	184
Spoofing	110	53
Estafa Turística	67	21
DDOS	23	5
Suplantación sim card	29	15
Fake News	10	4

Fuente 25. Centro de Capacidades para la Ciberseguridad de Colombia (C-4)

5.3 SOLUCIONES EN EL MERCADO PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO DE SERVICIOS TECNOLÓGICOS EN LAS ORGANIZACIONES DESDE UN SOC.

La implementación de un servicio de monitoreo se basa principalmente en la recolección de información de diferentes fuentes, esta actividad lo que busca es realizar la recopilación de los logs generados por las fuentes, centralizarlos, realizar una acción de

normalización y gestión para permitir la identificación oportuna de actividades inusuales y generar un alertamiento para que se implementen las acciones necesarias.
Una herramienta fundamental para llevar a cabo esta actividad es el SIEM, el cual se describe a continuación.

5.3.1 SIEM (Security Information and Event Management): El SIEM es la herramienta esencial para la implementación de un SOC, traduciendo sus siglas al español es la herramienta que permite la gestión de eventos e información de seguridad, las necesidades cada vez son mayores y se busca que estas herramientas no solo estén en la capacidad de realizar la recolección de logs si no también que se pueda llevar a cabo la investigación, ejecución de acciones de respuesta, a continuación se realizara una selección de algunas herramientas que han sido calificadas por Gartner[31] en su cuadrante mágico, describiendo sus fortalezas y precauciones de cada una de estas.

Ilustración 19, en el siguiente cuadrante, Gartner realiza la clasificación de los proveedores que prestan servicios de SIEM, clasificándolo su habilidad para hacer contra la integridad de la visión, con base a esto se ubican en uno de los 4 cuadrantes que son: jugadores del nicho, visionarios, líderes y retadores.

[31] (*Gartner. Magic Quadrant for Security Information and Event Management*)

Ilustración 19. Cuadrante mágico de Gartner SIEM

Fuente 26. Gartner (junio 2021)

5.3.2 Leaders: En este cuadrante Gartner ubica los proveedores que han tenido un alto desempeño en ventas de productos de SIEM, registran un número importante de clientes o un crecimiento significativo, ofrecen un producto que se adapta a las necesidades, proporcionando tecnologías que se cumplan con los requisitos actuales de las organizaciones y cuentan con buenos comentarios en el mercado.

5.3.3 Challengers: O retadores, como se puede observar en esta edición del cuadrante no se ubica ninguno, este cuadrante corresponde a empresas que brindan diferentes líneas de productos contando entre ellas con una base de SIEM, la cual puede estar en la capacidad de brindar alternativas básicas, pero no están lo suficientemente consolidadas y no han demostrado unos buenos resultados de éxito que permitan su consolidación.

5.3.4 Visionaries: Los visionarios muestran capacidades para el desarrollo funcional de los requisitos, pero cuentan con una menor capacidad de ejecución la cual se basa en una presencia baja en el mercado, lo cual se ve reflejado en bajas puntuaciones para sus funciones y características, el crecimiento y los ingresos que se tienen por la herramienta.

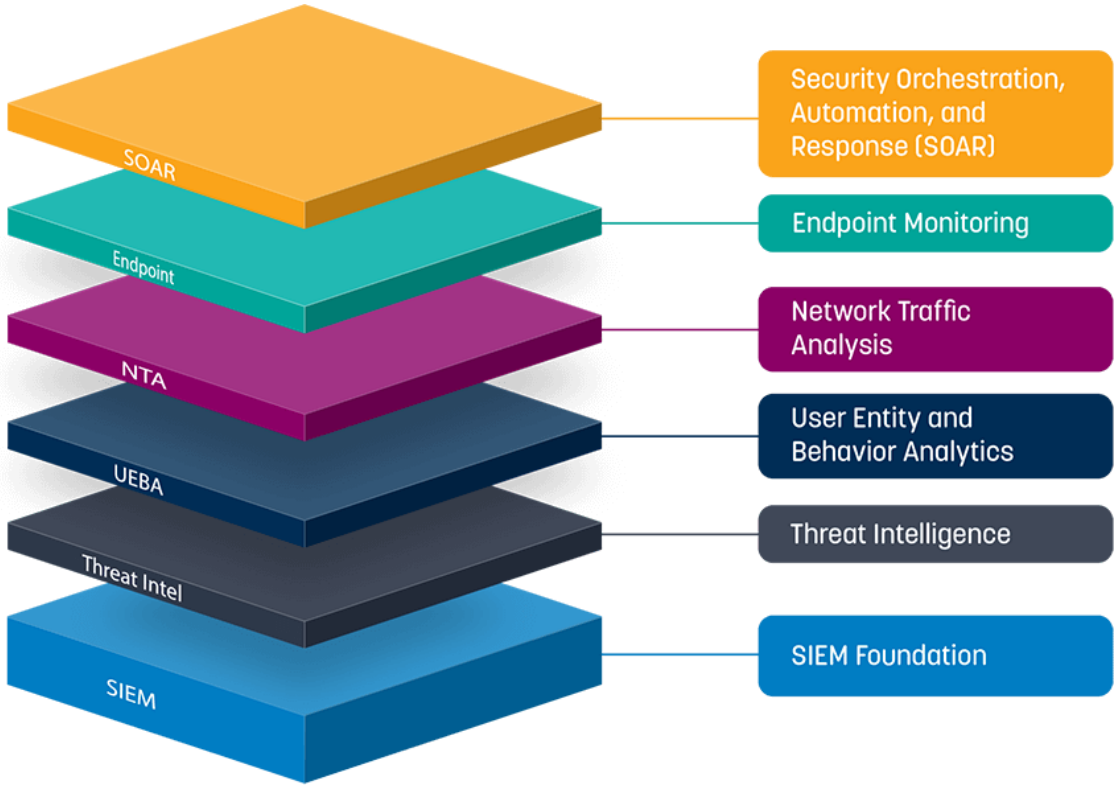
5.3.5 Niche players: Los jugadores de nicho, estos se enfocan en mercados específicos y proporcionan capacidades reducidas o limitadas en las capacidades de la herramienta SIEM, en esta clasificación se pueden encontrar proveedores en crecimiento y que han ido implementando sus herramientas en mercados pequeños y con funcionalidades específicas.

5.3.6 Herramientas SIEM en el mercado: A continuación, se realiza una selección y revisión de algunas herramientas con base al cuadrante Gartner

En esta sesión realizaremos una selección de las herramientas ubicadas en el cuadrante de líderes, para identificar cual es la herramienta ofrecida por estos fabricantes, identificar cuáles son sus principales ventajas y precauciones a tener en cuenta en el momento de realizar una selección.

5.3.6.1 LogRhythm SIEM: Ilustración 20, LogRhythm se ubica como líder en su cuadrante, en su sitio web oficial la empresa describe en una ilustración como es el funcionamiento actual de un SIEM, el cual con la evolución de las tecnologías ha pasado de ser un simple gestor de eventos a contar con diferentes capacidades, como se puede observar, el SIEM de LogRhytm realiza varias fases dentro de las cuales incorpora elementos como la detección inteligente y oportuna de amenazas, monitoreo de puntos finales, UEBA, SOAR, lo cual permite fortalecer tanto la detección oportuna como la respuesta.

Ilustración 20. SIEM LogRithm



Fuente 27. (SIEM Solution | Security Information & Event Management | LogRhythm)

LogRithm cuenta con una gran cobertura a nivel mundial y su herramienta es utilizada en diferentes sectores desde empresas pequeñas hasta las más grandes.
La herramienta puede ser implementada tanto en entornos en nube como físicos.
Licenciamiento: la herramienta ofrece diferentes alternativas de licenciamiento.

- Licencia perpetua, Precio por número promedio de mensajes por segundo por día
- Por suscripción, este cobro se genera por número de empleados.

Ventajas:

- Amplia cobertura a nivel mundial con presencia de un alto número de equipos y distribuidores.

- La empresa brinda opciones de prueba para que los clientes puedan conocer la herramienta e interactuar con su funcionamiento previo a su adquisición.
- LogRithm cuenta con un sistema maduro para la gestión e investigación de casos permitiendo la obtención de evidencias para las investigaciones.

Tener en cuenta:

- LogRithm no es el proveedor que cuenta con la herramienta mejor diseñada para ofrecer sus servicios en nube, este proveedor ha venido trabajando en la migración e implementación de estos servicios mientras continuar brindando sus servicios on premise, esto en comparación a otros proveedores que han desarrollado sus herramientas desde el inicio en entornos en nube.

5.3.6.2 InsightIDR – Rapid7: La solución InsightIDR ofrecida por la empresa Rapid 7, se encuentra ubicada como líder en el cuadrante mágico de Gartnet, la solución es utilizada principalmente en estados unidos, Europa y america latina, su solución es ofrecida 100% en nube y cuenta con diferentes alternativas para incluir otros módulos como: gestión de vulnerabilidades, SOAR, evaluación de la postura de seguridad en nube, análisis de trafico de red.

El licenciamiento que ofrece la herramienta es un licenciamiento temporal que se cobra según el número de activos a monitorear.

Ventajas:

- La herramienta cuenta con una gran capacidad de detección y análisis de amenazas, incorpora tecnologías como UEBA y permite una gestión adecuada de los informes y trazabilidad de la información.
- La herramienta cuenta con herramientas para la gestión de las fuentes de inteligencia que permiten la identificación oportuna de amenazas.

- Rapid7 ofrece la integración con servicios adicionales para la gestión de ciberseguridad y que permitan el monitoreo y la respuesta ante amenazas.

Tener en cuenta:

- La incorporación de otros servicios como el de SOAR debe ser incluida por separado.
- Los componentes ofrecidos por Rapid7 están ubicados en AWS y no tienen cobertura en todas las regiones, es necesario realizar las validaciones y confirmaciones, InsightIDR no está disponible en Sudamérica ni en Oriente Medio.[32]

5.3.6.3 Splunk: Es una herramienta que se brinda a nivel mundial y ha sido acogida por diferentes organizaciones, es posible implementarla en ambientes físicos, en nube o híbridos, Splunk no brinda de manera predeterminada herramientas como UEBA y SOAR, estas tienen que ser adquiridas de manera adicional.

El licenciamiento ofrecido es mediante suscripción y se cobra con base al volumen de eventos generados por día.

Ventajas:
Splunk cuenta con herramientas como:

- Inteligencia de amenazas integrada
- Alerta basada en riesgos
- Análisis de comportamiento impulsado por ML para la detección de amenazas desconocidas y avanzadas

[32] GARTNER. Magic Quadrant for Security Information and Event Management

- Herramientas de investigación flexibles que permiten una detección de amenazas más rápida

Tener en cuenta:

- Splunk puede resultar siendo una herramienta costosa ya que su método de licenciamiento genera un cobro por la cantidad de almacenamiento utilizado.
- La herramienta no cuenta con un entorno de operación completamente en nube lo cual puede resultar en una debilidad actualmente ya que las organizaciones buscan establecer los servicios en nube ahorrando costos de equipos y colocación.
- Con base a comentarios de clientes de Gartner se evidencia que se debe comprobar las características de asistencia para los que se encuentren ubicados en Latinoamérica y otras regiones.[33]

5.3.6.4 IBM – QRADAR: La solución SIEM brindada por IBM cuenta principalmente con su capacidad de SIEM sin muchas especificaciones adicionales, para lo cual IBM brinda diferentes tipos de herramientas que podrían ser incorporadas por separado de acuerdo con las necesidades, un ejemplo QRadar Network Insights para el monitoreo de redes o QRadar Vulnerability Manager para el monitoreo de vulnerabilidades.
Esta herramienta se encuentra disponible para ser instalada de manera física, en algunas de sus ofertas, así mismo su versión por consumo de EPS puede ser instalada en nube. El licenciamiento ofrecido se puede obtener en diferentes alternativas, por ejemplo, licencia perpetua o por suscripción, licenciamiento por consumo de eventos por segundo.

Sus principales características son:

- Recibe enormes cantidades de datos de fuentes locales y en la nube

[33] Ibid

- Aplica analítica integrada para detectar amenazas con precisión.
- Correlacione actividades relacionadas para priorizar incidentes.
- Analiza y normaliza automáticamente los registros.
- Inteligencia de amenazas y soporte para STIX/TAXII.
- Se integra inmediatamente con 450 soluciones.
- La arquitectura flexible puede implementarse en local o en la nube.
- Base de datos escalable, auto gestionable y auto sintonizable.[34]

Ventajas:

- Qradar cuenta con una capacidad de filtrado de los eventos que permite realizar una limpieza antes de la recolección, de esta manera se reduce el número de elementos no deseados y se optimiza la calidad del servicio.
- Realizando el filtrado de los eventos se logra reducir el número de eventos por segundo lo cual se verá reflejado en los costos.
- IBM cuenta con la herramienta UCM (QRadar Use Case Manager) que permite realizar diferentes actividades de analítica, permitiendo realizar un análisis de la información.
- IBM cuenta con una implementación de un colector que permite realizar el monitoreo de las redes en modo pasivo, evitando el acceso bidireccional lo que permite optimizar el rendimiento y su aplicación en entornos industriales.

Tener en cuenta:

- IBM se encuentra trabajando en la migración e incorporación de sus productos a servicios en nube lo cual podría presentar alteraciones durante el servicio debido a los cambios continuos.

[34] (*IBM QRadar SIEM - Visión general - Colombia | IBM*)

- Se han identificado algunas debilidades para las integraciones de colaboración, es necesario la implementación de herramientas de terceros y un complemento adicional para la implementación de SOAR.
- La herramienta puede resultar costosa para entornos grandes, las posibilidades de licenciamiento utilizadas puedes resultar siendo una limitante.

5.3.6.5 Exabeam Fusion SIEM: Se encuentra ubicando alrededor del mundo y ofrece sus servicios a grandes y medianas empresas, la solución se encuentra disponible como SaaS, alojada en nube lo cual es una ventaja ya que no se requiere de la implementación de infraestructura adicional, pero si es requerido también se cuenta con la posibilidad de una infraestructura hibrida.

La solución cuenta con elementos como:

- Lago de datos
- Analítica avanzada
- Cacería de amenazas
- Análisis de la entidad
- Gestion de casos
- Respuesta a incidentes

Estas alternativas son ofrecidas de manera separada y pueden ser incorporadas al servicio.

El licenciamiento ofrecido se basa en la cantidad de usuarios o entidades a monitorear.

Ventajas:

- La herramienta brinda una alternativa de almacenamiento de los registros de hasta 10 años.

- Se llevan a cabo búsquedas de manera inteligente y automatizada de anomalías, se realiza la normalización de los eventos, comprobación de indicadores de compromiso, entre otros elementos adicionales.
- Se brinda la alternativa modular que permite a los clientes adecuar la herramienta con base a sus necesidades.
- Cuenta con una herramienta madura para el análisis de comportamiento.

Tener en cuenta:

- Su servicio en nube se presta a través de Google Cloud plataforma y puede no estar disponible en todas las regiones, es necesario validar la cobertura.
- Ofrece un soporte limitado, que puede generar un alcance limitado de la herramienta.
- No cuenta con capacidades para el monitoreo de puntos finales o redes, para lo cual utiliza conexiones con productos líderes del mercado de código abierto.

5.3.6.6 Securonix Next-Gen SIEM: Es una herramienta que cuenta con capacidades de un SOC de nueva generación, ha sido construida de manera nativa en entornos de nube, algunas de sus características principales son, Data Lake, UEBA, SOAR, NDR, inteligencia de amenazas, análisis de comportamiento, entre otros elementos incorporados, su mercado esta mayormente posicionado en grandes y medianas empresas.
Licenciamiento, la herramienta se vende en licencias temporales y perpetuas.

Ventajas:

- Cuenta con una gran fortaleza en la protección de la integridad de los datos, incluye un control de acceso granular que permite la gestión de roles.
- Ha expandido sus capacidades estableciendo alianzas con diferentes socios lo cual permite la expansión a todos los mercados de una manera accesible.

- Cuenta con diversas alternativas para la aplicación de inteligencia de amenazas de manera nativa.

Tener en cuenta:

- La gestión de las plataformas resulta ser un poco compleja según la información recolectada por Gartner en su último informe de junio de 2021.[35]
- Se ha evidenciado un bajo rendimiento en la prestación de soporte para los productos.[36]
- Se debe comprobar las necesidades en el momento de asignar los recursos, la escalabilidad de manera local no resulta simple en el momento de un crecimiento.

5.3.6.7 Elastic Security: Es una herramienta que cuenta con diversas capacidades para la gestión de eventos, ha sido implementada a nivel mundial por diferentes tipos de organizaciones, desde grandes a pequeñas, una de las principales ventajas de esta herramienta es que puede ser implementada como una instalación auto gestionable o también puede ser consumida como un SaaS.
Licenciamiento: cuenta con diferentes niveles de suscripción, estándar y premium, así mismo cuenta con versiones gratuitas, este modelo se basa en los recursos de memoria utilizados para almacenar, buscar y analizar datos.

Ventajas:

- Cuenta con una versión gratuita en la suscripción estándar que cuenta con funcionalidades básicas de SIEM, a la cual se le pueden incorporar diferentes elementos adicionales para mayor desempeño.
- Cuenta con diferentes herramientas para la detección y monitoreo que pueden ser implementadas de manera gradual.

[35] GARTNER. (Magic Quadrant for Security Information and Event Management)

[36] Ibid

- Cuenta con una funcionalidad llamada Kibana Lens de Elastic que permite fortalecer la búsqueda de amenazas.

Existen algunas herramientas de software libre que también pueden ser de utilidad en el momento de llevar a cabo la implementación de un servicio SOC, a continuación, se listan algunas de ellas de manera informativa:

- OSSIM
- OSSEC
- Apache Metron
- SIEMonster
- Prelude SIEM
- Security Onion

5.4 ESTRATEGIAS QUE PERMITAN REDUCIR LOS TIEMPOS DE RESPUESTA ANTE EVENTOS E INCIDENTES DE CIBERSEGURIDAD DETECTADOS POR EL SOC.

5.4.1 SOAR: Las tecnologías de la información son cada vez más utilizadas en los diferentes entornos, al establecer capacidades de monitoreo y detección de amenazas, vulnerabilidades, eventos o incidentes de ciberseguridad, se busca contar con la capacidad de respuesta oportuna y en el menor tiempo posible, de esta manera garantizar que no se presente una afectación mayor.

SOAR (Security Orchestration, Automation and Response) es una herramienta de apoyo para el servicio SOC, hace referencia a la integración de diferentes mecanismos y herramientas, permitiendo automatizar y establecer acciones de respuesta, documentando y generando una mayor efectividad en un menor tiempo, de esta manera

los administradores de seguridad podrán estar tranquilos de que las respuestas se ejecuten en el momento preciso y reducir los riesgos cibernéticos.

5.4.2 UEBA: (User and Entity Behavior Analytics) traduciendo sus siglas tenemos que UEBA se trata del análisis de comportamiento de entidades y usuarios, la integración de este componente al servicio de monitoreo de SOC permite establecer un aprendizaje de las herramientas, estableciendo unas líneas base de los comportamientos de los usuarios y las entidades, de esta manera identificar y alertar de manera oportuna cuando se evidencie un cabio en el comportamiento conocido.

Conocer cómo funcionan las herramientas, equipos, tráfico de red, usuarios de la organización es una de las principales actividades a realizar y que permitirán la identificación oportuna de una posible alteración o manipulación de los sistemas por un tercero no autorizado.

5.4.3 PLAYBOOKS: La palabra PlayBook del inglés hace referencia a la construcción de reglas de juego, en el contexto de ciberseguridad hace referencia al establecimiento de las acciones para responder ante un posible incidente.

Es muy importante tener claro y previamente establecido el camino a seguir y definido como actuar para responder de manera oportuna.

No existen unas condiciones especiales para la construcción de esta documentación, se puede tomar como referencia las funciones del Framework de NIST que permitan seguir las acciones desde la identificación, detección, respuesta y recuperación ante un posible incidente.

5.4.4 INTELIGENCIA DE AMENAZAS: La inteligencia de amenazas es un elemento fundamental para incorporar dentro de la estrategia de monitoreo de ciberseguridad, es importante contemplar y establecer estrategias para la búsqueda anticipada de posibles amenazas que puedan representar un riesgo para la organización.

Establecer una estrategia de monitoreo y búsqueda anticipada de manera continua para realizar las búsquedas de información y análisis con bases de datos públicas y diversas fuentes de información, de esta manera lograr identificar la aparición de amenazas, vulnerabilidades y cualquier elemento que pueda generar afectaciones a los sistemas de la organización, de esta manera establecer alertamiento.

6 CONCLUSIONES

Con base a la información recolectada en este documento monográfico de análisis de soluciones para el monitoreo de seguridad activa y pasiva de infraestructuras tecnológicas apoyado en un servicio de SOC, el cual se ha desarrollado basado en los objetivos específicos planteados, es necesario extraer algunas conclusiones y recomendaciones que serán de suma utilidad para el lector.

- Con base a las validaciones realizadas sobre el marco de trabajo de NIST, se cuenta con una herramienta potencial que brinda diversas opciones para la mejora de la ciberseguridad en cualquier tipo de organización, este puede servir como referencia decidiendo cuales de sus elementos pueden ser aplicados, no es necesario trabajar con todas sus funciones, cada organización está en la libertad de acogerse a alguna de ellas con base a sus necesidades. Adicionalmente, en Colombia las organizaciones reguladas por la super intendencia financiera, según lo establecido en el numeral 3 de la circular externa 007 de 2018, deben realizar análisis de riesgo para determinar la pertinencia de contratar o implementar el servicio de SOC.

- En Colombia se ha definido un CSIRT liderado por la policía nacional, el cual se encarga de gestionar las denuncias interpuestas por la ciudadanía, bien sea personas naturales o empresas, con base a esto se identifican los principales ataques que se presentan en el país con base a lo identificado, los principales ataques son; phishing, suplantación de identidad, envío de malware, fraudes en medios de pago en línea, así mismo se argumenta cuáles son las estadísticas de crecimiento, se comparten de manera periódica y pueden ser consultadas de manera libre, con base a esta información se puede deducir que los ataques cibernéticos están en constante evolución y crecimiento, los ciber delincuentes cada día encuentran nuevas alternativas para evadir los controles.

- Existen en el mercado diferentes tipos de soluciones SIEM, de las cuales se realiza un análisis con base a la información suministrada por el cuadrante de Gartner, entre ellas; LogRhythm, InsightIDR, Splunk, QRADAR, Exabeam Fusion SIEM, Securonix Next-Gen SIEM, Elastic Security;las cuales son la base para establecer un centro de operaciones de seguridad, estas herramientas cuentan con diferencias tanto en las prestaciones como en los costos, se pueden encontrar en el mercado soluciones con diferentes tipos de licenciamiento, de acuerdo a las necesidades de la organización, así mismo también se puede optar por la implementación de herramientas de uso libre como: OSSIM, OSSEC, Apache Metron, SIEMonster, Prelude SIEM. Security Onion, las cuales pueden ser de utilidad para establecer un sistema de monitoreo en una organización de bajos recursos.

- Las estrategias de ataques cibernéticos han ido evolucionando con el paso del tiempo, con base a esto se ha venido trabajando en la definición de nuevas estrategias para fortalecer el monitoreo, la detección y respuesta oportuna de amenazas, con base a esto se debe garantizar que una estrategia de monitoreo no debe basarse en una simple recolección de logs, sino que debe ir más allá de lo convencional apoyándose en nuevas alternativas como las propuestas. SOAR, UEBA, implementación de Playbooks, inteligencia de amenazas, lo cual permitirá estar un paso delante de los atacantes.

7 RECOMENDACIONES

- Para llevar a cabo el establecimiento de un centro de operaciones de seguridad en las empresas colombiana, es necesario identificar el estado actual de la organización y cuáles son las necesidades, para esto se recomienda trabajar con base a lo establecido en las diferentes funciones del marco de trabajo de NIST, los elementos más relevantes para un servicio de SOC han sido destacados en este documento.

- Se recomienda tener siempre visibles los posibles ataques cibernéticos que se presentan de manera recurrente, con base a esto establecer y evaluar las acciones que permitan identificar de manera proactiva la presencia de uno de ellos, así mismo realizar actividades de sensibilización con los usuarios de la organización para fortalecer la detección desde la primera línea de defensa.

- El establecimiento de un SOC en organizaciones Colombianas tiene como base el uso de una herramienta SIEM, se recomienda realizar una adecuada selección identificando que esta permita realizar diferentes acciones para la detección y respuesta, es necesario tener claro que no es una herramienta que únicamente realizara la recolección y centralización de logs, en la actualidad se requiere ir más allá de lo convencional, es fundamental proponer e implementar acciones automatizadas de detección y respuesta haciendo uso de nuevas alternativas tecnológicas, esto permitirá reducir de manera significativa los tiempos empleados para garantizar una adecuada solución y brindar el valor esperado a las organizaciones con el servicio SOC.

- Implementar dentro de los controles de la organización un Centro de operaciones de seguridad SOC, el cual permitirá mantener un monitoreo continúo detectando

posibles alteraciones e inconsistencias en el transcurso de las operaciones y de esta manera responder de manera oportuna.

8 DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación de este (Si es informe técnico por seminario o créditos de maestría, no tiene jurado); con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de ANÁLISIS DE SOLUCIONES PARA EL MONITOREO DE SEGURIDAD ACTIVA Y PASIVA DE INFRAESTRUCTURAS TECNOLÓGICAS APOYADO EN UN SERVICIO DE SOC, puedan acceder al documento.

BIBLIOGRAFÍA

Alruwaili, Fahad F., y T. Aaron Gulliver. SOCaaS: Security Operations Center as a Service for Cloud Computing Environments. n.º 2, 2014, p. 10.

Andrade, Roberto, y Jenny Torres. «Enhancing Intelligence SOC with Big Data Tools». 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), IEEE, 2018, pp. 1076-80.

Bhatt, Sandeep, et al. E Operational Role of Security Information. 2014, p. 7.

Biggeri, Patricio Hernán. Centro de operaciones de seguridad: estrategia, diseño y gestión. [En línea] Trabajo Final de Maestría. Universidad de Buenos Aires Facultad de Ciencias Económicas Escuela de Estudios de Posgrado. Buenos Aires, 2018. [Consultado 1 de junio 2021] Disponible en: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1202_BiggeriPH.pdf

Ceballos Lopez, Adriana, Equipo TicTac. Evaluación retos y amenazas a la ciberseguridad. Bogota D.C. 2021. p. 33.

Centro Cibernetico Policial de Colombia. Balance Cibercrimen BLSC20335DS1. Bogotá D.C. 2020. p. 2

Check Point Software technologies ltd. INFORME SOBRE SEGURIDAD CIBERNÉTICA 2021. 2021, p. 77.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1581. (17 de octubre de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. En Diario oficial. Octubre de 2012. p.11.

Colombia. Superintendencia Financiera De Colombia. Circular Externa 007 De 2018. Junio 05. 2018. p. 6

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (5 de enero de 2009). por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En Diario oficial. Enero, 2009. p.2

Crowley, Chris. Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey. 2019, p. 26.

Crooks, David, y Liviu Vâlsan. «Building a Minimum Viable Security Operations Centre for the Modern Grid Environment». Proceedings of International Symposium on Grids & Clouds 2019 — PoS (ISGC2019), Sissa Medialab, 2019, p. 010.

¿De qué hablamos cuando hablamos de SOAR? [En línea] consultado 3 de octubre de 2021. Disponible en: https://www.digitizeme.blog/digitizeme-latam/de-qu%C3%A9-hablamos-cuando-hablamos-de-soar.

Definición de inteligencia de amenazas [En línea] Inteligencia de ciberamenazas, Kaspersky. Consultado el 3 de octubre de 2021. Disponible en: https://latam.kaspersky.com/resource-center/definitions/threat-intelligence.

Deloitte. Evento: Panorama actual de la ciberseguridad. Nuevas soluciones para la gestión de la ciberseguridad. 2018. p. 24

EY. Security Operations Centers — Helping You Get Ahead of Cybercrime.2014. p. 20.

Feng, Charles, et al. «A User-Centric Machine Learning Framework for Cyber Security Operations Center». 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), IEEE, 2017, pp. 173-75.

Fusion SIEM [En línea] Exabeam. Consultado el 2 de octubre de 2021. Disponible en: https://www.exabeam.com/product/fusion-siem/.

Gartner Reprint.[en línea] Consultado el 2 de octubre de 2021. Disponible en: https://www.gartner.com/doc/reprints?id=1-26Q3T88Y&ct=210706&st=sb.

Gobierno de Colombia. Plan Nacional de Desarrollo 2018-2022 Pacto por Colombia, pacto por la equidad. Bogota D.C. 2018. p. 212

Heurck, Christian Van. Study on CSIRT Landscape and IR Capabilities in Europe 2025. 2019, p. 34.

Hernandez, Nelson. NOC/SOC Integration: Opportunities for Increased Efficiency in Incident Response within Cyber-Security. 2018, p. 28.

IBM QRadar SIEM [en línea] Visión general - Colombia IBM. Consultado el 2 de octubre de 2021. Disponible en: https://www.ibm.com/co-es/products/qradar-siem.
INCIBE. Glosario de términos de ciberseguridad, una guía de aproximación para el empresario. 2021. p. 82.

Kelley, Diana, y Ron Moritz. «Best Practices for Building a Security Operations Center». Information Systems Security, vol. 14, n.º 6, enero de 2006, pp. 27-32.

La inteligencia de amenazas o Cyber Threat Intelligence. [en línea] consultado el 3 de octubre de 2021. Disponible en: https://www.campusciberseguridad.com/blog/item/150-la-inteligencia-de-amenazas-o-cyber-threat-intelligence.

La solución SIEM en la nube que estaba esperando: Rapid7. [en línea] consultado el 2 de octubre de 2021. Disponible en: https://www.rapid7.com/solutions/siem/.

Márquez, Iván Duque, y Marta Lucía Ramírez Blanco. Presidente de la República. Bases Del Plan Nacional De Desarrollo 2018-2022. Bogotá D.C. 2018, p. 1459.

Mendez Fonseca, Victor Julio. Marco Tecnológico de un SOC de Nueva Generación. Universidad Piloto de Colombia. Especialización en seguridad informática. 2019. p.12.

Muniz, Joseph, et al. Security Operations Center: Building, Operating, and Maintaining Your SOC. Cisco Press, 2016. p.600

National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. NIST CSWP 04162018, National Institute of Standards and Technology, 16 de abril de 2018, p. NIST CSWP 04162018. DOI.org (Crossref), doi: 10.6028/NIST.CSWP.04162018.

OEA y Asobancaria. Desafíos Del Riesgo Cibernético En El Sector Financiero Para Colombia Y América Latina. 2019. p. 172

Onwubiko, Cyril. «Cyber Security Operations Centre: Security Monitoring for Protecting Business and Supporting Cyber Defense Strategy». 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), IEEE, 2015, pp. 1-10.

Publications [Sitio web]. Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. [consultado 15 de mayo de 2021] Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

¿Qué es SOAR? [En línea] consultado 3 de octubre de 2021. Disponible en https://www.redhat.com/es/topics/security/what-is-soar.

¿Qué es un Playbook de respuesta incidente? – BLOGDELCISO. [En línea] consultado 3 de octubre de 2021. Disponible en: https://blogdelciso.com/2019/08/17/que-es-un-playbook-de-respuesta-incidente-y-porque-me-deberia-preocupar-no-tener-uno/.

Quintero, Carlos Argáez. EQUIPO DE POLICÍA NACIONAL. Tendencias Cibercrimen Colombia 2019-2020. 2019. p. 36.

Radu, Sabina Georgiana. «Comparative Analysis of Security Operations Centre Architectures; Proposals and Architectural Considerations for Frameworks and Operating Models». Innovative Security Solutions for Information Technology and Communications, editado por Ion Bica y Reza Reyhanitabar, vol. 10006, Springer International Publishing, 2016, pp. 248-60.

República de Colombia. Consejo Nacional de Política Económica y Social. Lineamientos De Política Para Ciberseguridad Y Ciberdefensa. Bogotá D.C. 2011. p. 43

Román Torres, María José, Proceso para definir y establecer un centro de operaciones de seguridad (SOC) en una organización financiera. Master universitario en seguridad informática. Universidad internacional de la rioja. Guayaquil. 2019. 112p.

Ruefle, Robin. Defining Computer Security Incident Response Teams. 2007. p. 8.

SANS Institute InfoSec Reading Room. Building a World-Class Security Operations Center: A Roadmap. 2015. p. 12.

Santos, Omar, y Joseph Muniz. CCNA Cyber Ops SECOPS 210-255 Official Cert Guide. Cisco Press, 2017. p. 546

SANS. Future SOC: Security Operations Center Survey. 2017. p. 27

Scronkronk, Gronko. Building a Security Operations Center. 2015. p. 32.

Scarfone, Karen, y Peter Mell. Guide to Intrusion Detection and Prevention Systems (IDPS) (Draft). 2012. p. 111.

SIEM [en línea] Cyber Security Solutions, Splunk. Consultado el 2 de octubre de 2021. Disponible en: https://www.splunk.com/en_us/cyber-security/siem.html.

SIEM en el Elastic Stack [en línea] Elastic Security, Elastic SIEM. Consultado el 2 de octubre de 2021. Disponible en: https://www.elastic.co/es/siem/.

SIEM Solution [en línea] Security Information & Event Management LogRhythm. Consultado el 2 de octube de 2021. Disponible en: https://logrhythm.com/solutions/security/siem/.

Soto, Esteban Gutierrez. Transformación digital y los retos regulatorios hacía el nuevo Consumidor Financiero. 2019. p. 19.

Super Intendencia Financiera de Colombia. Riesgos Emergentes y Prioridades de Supervisión. Bogota D.C. 2019. p. 18

Super intendencia de sociedades. Procedimiento De Gestión De Logs Y Registros De Auditoría. Bogotá D.C. 2017. p.7.

SWIMLANE. Security Orchestration, Automation and Response (SOAR) Capabilities. 2021. p. 17

Thompson, Eric C. Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents. Apress, 2018. p. 184

Thompson, Eric C. Designing a HIPAA-Compliant Security Operations Center: A Guide to Detecting and Responding to Healthcare Breaches and Events. Apress, 2020. p. 241.

Wagner, Cynthia, et al. «MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform». Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, ACM, 2016, pp. 49-56.

Wold Economic Forum. The Global Risk Report 2020. 2020. p. 102

Write a Review About an IT Solution Reviews 2021 [en línea] Gartner Peer Insights. Consultado el 3 de octubre de 2021. Disponible en: https://www.gartner.com/reviews/market/user-and-entity-behavior-analytics.

Zimmerman, Carson. Ten Strategies of a World-Class Cybersecurity Operations Center. 2014. p. 346.

ANEXOS

ANEXO A. RESUMEN ANALÍTICO ESPECIALIZADO -RAE

Fecha de Realización:	17/10/2021
Programa:	Especialización en seguridad informática
Línea de Investigación:	Gestión de sistemas
Título:	Análisis De Soluciones Para El Monitoreo De Seguridad Activa Y Pasiva De Infraestructuras Tecnológicas Apoyado En Un Servicio De SOC
Autor(es):	Mora Montoya Julian David
Palabras Claves:	Correlación, CSOC, Detección de amenazas, Monitoreo, SIEM, SOAR, SOC.
Descripción:	El presente documento encontrara documentación relacionada con lo que se debe tener en cuenta para llevar a cabo un diseño de un servicio de monitoreo de ciber seguridad en una organización, factores clave a tener en cuenta, contemplando diversas opciones de recolección de los datos, tipos de logs, servicio SOC, acciones de respuesta automatizada para garantizar una pronta reacción ante un posible incidente de ciberseguridad, con base a las recomendaciones que puedan existir en los marcos de referencia como NIST, circular externa 007 de 2018 de la super intendencia financiera de Colombia, para que con base a esta información se logre comprender las

	necesidades y fortalecer un esquema de monitoreo que pueda alimentar al equipo de respuesta a incidentes de ciberseguridad de las organizaciones.

Fuentes bibliográficas destacadas:

Biggeri, Patricio Hernán. Centro de operaciones de seguridad: estrategia, diseño y gestión. [En línea] Trabajo Final de Maestría. Universidad de Buenos Aires Facultad de Ciencias Económicas Escuela deEstudios de Posgrado. Buenos Aires, 2018. [Consultado 1 de junio 2021] Disponible en: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1202_BiggeriPH.pdf

Ceballos Lopez, Adriana, Equipo TicTac. Evaluación retos y amenazas a la ciberseguridad. Bogota D.C. 2021. p. 33.

Centro Cibernetico Policial de Colombia. Balance Cibercrimen BLSC20335DS1. Bogotá D.C. 2020. p. 2

Crooks, David, y Liviu Vâlsan. «Building a Minimum Viable Security Operations Centre for the Modern Grid Environment». Proceedings of International Symposium on Grids & Clouds 2019 — PoS (ISGC2019), Sissa Medialab, 2019, p. 010.

Fusion SIEM [En línea] Exabeam. Consultado el 2 de octubre de 2021. Disponible en: https://www.exabeam.com/product/fusion-siem/.

Gartner Reprint.[en línea] Consultado el 2 de octubre de 2021. Disponible en: https://www.gartner.com/doc/reprints?id=1-26Q3T88Y&ct=210706&st=sb.

Mendez Fonseca, Victor Julio. Marco Tecnológico de un SOC de Nueva Generación. Universidad Piloto de Colombia. Especialización en seguridad informática. 2019. p.12. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. NIST CSWP 04162018, National Institute of Standards and Technology, 16 de abril de 2018, p. NIST CSWP 04162018. DOI.org (Crossref), doi: 10.6028/NIST.CSWP.04162018.	
Contenido del documento:	El presente documento tiene como objetivo analizar soluciones para que las organizaciones establezcan una estrategia de monitoreo activo y pasivo de la seguridad de la información y de la infraestructura tecnológica mediante la incorporación de un servicio de SOC. dentro de este se podrá encontrar información relevante con la identificación de información del marco de trabajo de NIST relevante para ser aplicada en un servicio de monitoreo, principales ataques cibernéticos identificados en Colombia a los cuales están expuestas las organizaciones, diferentes herramientas de SIEM para la implementación de un SOC y estrategias que ayudaran a fortalecer los sistemas de monitoreo de ciberseguridad para las organizaciones con alternativas que permitan llevar a cabo la respuesta oportuna ante amenazas de seguridad buscando reducir los tiempos.

Conceptos adquiridos:	En el contenido del documento, se adquieren conceptos como: Reconocer y comprender que es un SOC, que es un SOC de nueva generación, Framework NIST y cada una de sus funciones, identificar, proteger, detectar, responder, recuperar, SOAR SIEM y sus principales ventajas, UEBA, Playbooks, Inteligencia de amenazas, entre otros elementos importantes para establecer servicio de monitoreo de seguridad.
Conclusiones:	Con base a las validaciones realizadas sobre el marco de trabajo de NIST, se cuenta con una herramienta potencial que brinda diversas opciones para la mejora de la ciberseguridad en cualquier tipo de organización, este puede servir como referencia decidiendo cuales de sus elementos pueden ser aplicados, no es necesario trabajar con todas sus funciones, cada organización está en la libertad de acogerse a alguna de ellas con base a sus necesidades. Adicionalmente, en Colombia las organizaciones reguladas por la super intendencia financiera, según lo establecido en el numeral 3 de la circular externa 007 de 2018, deben realizar análisis de riesgo para determinar la pertinencia de contratar o implementar el servicio de SOC.

	En Colombia se ha definido un CSIRT liderado por la policía nacional, el cual se encarga de gestionar las denuncias interpuestas por la ciudadanía, bien sea personas naturales o empresas, con base a esto se identifican los principales ataques que se presentan en el país con base a lo identificado, los principales ataques son; phishing, suplantación de identidad, envío de malware, fraudes en medios de pago en línea, así mismo se argumenta cuáles son las estadísticas de crecimiento, se comparten de manera periódica y pueden ser consultadas de manera libre, con base a esta información se puede deducir que los ataques cibernéticos están en constante evolución y crecimiento, los ciber delincuentes cada día encuentran nuevas alternativas para evadir los controles. Existen en el mercado diferentes tipos de soluciones SIEM, de las cuales se realiza un análisis con base a la información suministrada por el cuadrante de Gartner, entre ellas; LogRhythm, InsightIDR, Splunk, QRADAR, Exabeam Fusion SIEM, Securonix Next-Gen SIEM, Elastic Security;las cuales son la base para establecer un centro de operaciones de seguridad, estas herramientas cuentan con diferencias tanto en las prestaciones como en

	los costos, se pueden encontrar en el mercado soluciones con diferentes tipos de licenciamiento, de acuerdo a las necesidades de la organización, así mismo también se puede optar por la implementación de herramientas de uso libre como: OSSIM, OSSEC, Apache Metron, SIEMonster, Prelude SIEM. Security Onion, las cuales pueden ser de utilidad para establecer un sistema de monitoreo en una organización de bajos recursos. Las estrategias de ataques cibernéticos han ido evolucionando con el paso del tiempo, con base a esto se ha venido trabajando en la definición de nuevas estrategias para fortalecer el monitoreo, la detección y respuesta oportuna de amenazas, con base a esto se debe garantizar que una estrategia de monitoreo no debe basarse en una simple recolección de logs, sino que debe ir más allá de lo convencional apoyándose en nuevas alternativas como las propuestas. SOAR, UEBA, implementación de Playbooks, inteligencia de amenazas, lo cual permitirá estar un paso delante de los atacantes.