



Universidad CENFOTEC

Maestría Profesional en Ciberseguridad

Documento final Proyecto de Investigación Aplicada 2

Tema

Fortaleciendo la ciberseguridad en Costa Rica:
Monitoreo, pilar en la detección de amenazas

Autores

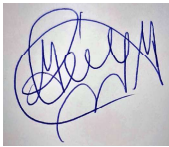
Espinoza Reyes José Manuel | Vargas Villalobos Roberto

Fecha

Febrero, 2024

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría Profesional en Ciberseguridad**, requisito para optar por el título de grado de **Maestría**, para los estudiantes: **Espinoza Reyes José Manuel y Vargas Villalobos Roberto**.



Digitally signed by
MIGUEL PEREZ
MONTERO (FIRMA)
Date: 2024.03.04
19:12:58 -06'00'

M.Sc. Miguel Pérez Montero
Tutor

REBECA ESQUIVEL
FLORES (FIRMA)

Firmado digitalmente por REBECA
ESQUIVEL FLORES (FIRMA)
Fecha: 2024.03.06 10:26:01 -06'00'

M.Sc. Rebeca Esquivel Flores
Lector 1

KENNETH IRVIN
MONGE
QUIROS (FIRMA)

Firmado digitalmente
por KENNETH IRVIN
MONGE QUIROS (FIRMA)
Fecha: 2024.03.16
11:05:06 -06'00'

M.Seg. Kenneth Irvin Monge Quirós
Lector 2



San José, Costa Rica, 1 de marzo de 2024

Fortaleciendo la ciberseguridad en Costa Rica: Monitoreo, pilar en la detección de amenazas (Febrero 2024)

Roberto Vargas Villalobos¹, José Espinoza Reyes², MSc. Miguel Pérez Montero³

¹rvargasv@ucenfotec.ac.cr
²jespinozar@ucenfotec.ac.cr
³mperez@ucenfotec.ac.cr

RESUMEN A través de los últimos años, Costa Rica se ha convertido en víctima de importantes ciberataques, donde destacan las carencias de ciberseguridad en el sector público, y señalan la necesidad de un proceso de monitoreo preciso y analítico de los datos de seguridad en tiempo real, enfocado en la detección de amenazas cibernéticas, las cuales cada día son más complejas y elaboradas. Ante esta creciente vulnerabilidad, el artículo presenta un análisis minucioso sobre la situación actual de la postura de seguridad cibernética nacional, donde no solo señala estas deficiencias críticas, sino que propone una solución tangible y avanzada con un enfoque estratégico, en forma de un marco de referencia sólido, cuya adopción por parte de las organizaciones les permite enfrentar los riesgos existentes, así como también anticiparse y prepararse para las futuras evoluciones del panorama cibernético. Dicho marco se fundamenta en modelos y buenas prácticas reconocidas a nivel global, como NIST, CIS, MITRE ATT&CK y OWASP, por lo que se torna innovador debido a la inexistencia de documentación de apoyo dirigida a las instituciones gubernamentales en este contexto. Su flexibilidad y adaptabilidad ofrecen una herramienta de alto valor a considerar para la implementación efectiva del proceso de monitoreo basado en la vigilancia constante en tiempo real, aportando una perspectiva fundamentada en el riesgo organizacional, que destaca la importancia de recopilar, analizar y correlacionar eventos de seguridad de manera centralizada. Además enfatiza la relevancia de estudiar incidentes en profundidad y recomienda el uso de matrices de calor para establecer la severidad de alertas e incidentes de manera diferenciada. Complementariamente, aborda los desafíos actuales, abre la puerta a futuras investigaciones y aplicaciones prácticas, proporcionando una guía valiosa para fortalecer la ciberseguridad en Costa Rica.

ABSTRACT Throughout these last years, Costa Rica has become a victim of significant cyberattacks that highlight the deficiencies in cybersecurity in the public sector and point out the need of a more precise and analytical process to monitor security data in real time. Said process would be focused on the detection of cyberthreats since they are becoming more complex and elaborate every day. In the face of this growing vulnerability, the article presents a thorough analysis on the current situation regarding national cybersecurity, where it points out these critical deficiencies and also proposes a tangible and advanced solution with a strategic approach, in the form of a solid reference framework, whose adoption allows organizations to face existing risks and anticipate and prepare for future evolution of the cyber landscape. This framework is based on models and practices that are globally recognized, such as NIST, CIS, MITRE ATT&CK and OWASP, which are innovative due to the lack of supporting documentation aimed at government institutions in this context. Its flexibility and adaptability make it a high-value tool to consider for the effective implementation of the monitoring process which is based on constant real-time surveillance, and provides a perspective based on organizational risk which highlights the importance of collecting centrally, analyzing and correlating security events. It also emphasizes the relevance of studying incidents in depth and recommends the use of heat matrices to establish the severity of alerts and incidents in a differentiated manner. Additionally, it addresses current challenges and opens the door to future research and practical applications, therefore providing valuable guidance to strengthen cybersecurity in Costa Rica.

PALABRAS CLAVE Estrategia y monitoreo continuo de ciberseguridad, detección de ciberamenazas, brechas, incidentes y ataques de seguridad, estándares y buenas prácticas, sector público.

I. INTRODUCCIÓN

La adopción de Internet por las organizaciones, en conjunto con la acelerada evolución tecnológica y la dependencia implícita que conlleva, han establecido la ciberseguridad como un asunto crítico desde perspectivas globales, regionales, nacionales y sectoriales. En paralelo, la criminalidad se ha manifestado en forma de complejas y elaboradas amenazas cibernéticas que provocan un impacto importante en pérdidas económicas a través de variados tipos de ataques, mediante la identificación y explotación de diversas vulnerabilidades (Rosales, 2023).

Ante esta realidad tecnológica, y riesgo cibernético, es requerida una estrategia robusta que plasme las contramedidas necesarias de alto nivel, tácticas y técnicas, donde el monitoreo continuo se define como la piedra angular en la detección de amenazas y potenciales incidentes, con el objetivo de fortalecer la postura de ciberseguridad de las organizaciones (Jaiswar, 2023).

La declaración del monitoreo continuo, como pilar fundamental en el eje de detección, se argumenta basado en la relevancia que aporta sobre la visibilidad integral de los ecosistemas tecnológicos e interacción con el ámbito exterior, mediante la recolección, análisis y correlación centralizada de datos de valor, obtenidos de múltiples componentes de las infraestructuras, que permiten comprender la evolución de los eventos y reconocer anomalías en el comportamiento normal del entorno.

Para ejemplificar la importancia de un monitoreo preciso de seguridad en tiempo real se pueden citar los eventos suscitados en Costa Rica, los cuales tuvieron visibilidad a nivel mundial y cuyo impacto negativo fue consecuencia de una detección tardía que no permitió brindar una respuesta efectiva a los incidentes, ni permitió a los responsables de la gestión de crisis tomar decisiones acertadas y a tiempo por falta de información relevante (AESA - EY Consortium, 2022).

La ilustración número 1, sintetiza una muestra de la variedad de ataques y grupos adversarios, donde es posible reconocer que su alcance llega a todos los continentes. A pesar de que los números estadísticos de los diversos análisis realizados, por múltiples organizaciones de investigación, señalan exorbitantes cantidades de variaciones de malware y ransomware, pérdidas económicas millonarias y efectos negativos desastrosos para muchas compañías, es necesario comprender que cantidades mayores de incursiones son detectadas, contenidas y mitigadas como resultado de buenas prácticas aplicadas por medio del proceso de monitoreo continuo en ciberseguridad.



	Fecha	País	Objetivo	Grupo	Ataque
1	mayo-2022	Zambia	Banco de Zambia	Hive	Ransomware
2	mayo-2023	Etiopia	10 entidades del Estado aprox.	Mysterious Team Bangladesh (MTB)	DDoS
3	diciembre - 2022	Australia	MediBank	REvil	Exfiltración de datos
4	diciembre - 2022	Nueva Zelanda	Mercury IT	Lockbit	Compromiso en cadena suministros
5	enero-2023	España	Diversas compañías españolas	Mealybug	Campañas de phishing
6	julio-2023	Francia	Diplomáticos	Mustang Panda	Malware
7	junio-2023	India	All India Institute of Medical Sciences (AIIS)	China	Acceso no autorizado
8	julio-2023	Japón	Puerto de Nagoya	Lockbit 3.0	Ransomware
9	agosto-2022	Estados Unidos	MaliChimp	Scatter Swine	Ingeniería Social
10	mayo-2023	Canadá	Metro Vancouver Transit Police	CLOP	Explotación vulnerabilidad día zero (Moveit)
11	abril-2022	Perú	Ministerio del interior	Conti	Filtración de documentos confidenciales
12	setiembre-2022	Colombia	IFX Networks	RansomHouse	Interrupción de servicios
13	abril-2022	Costa Rica	Ministerio de Hacienda	Conti	Doxing
13	mayo-2022	Costa Rica	Caja Costarricense del Seguro Social (CCSS)	Hive	Cifrado de servidores

Ilustración número 1. Síntesis de variedad de ciberataques y grupos adversarios a nivel mundial - periodo 2022-2023.
Fuente: Confección propia.

En este punto es necesario comprender que la detección es un control fundamental en cualquier estrategia de seguridad cibernética, cuya base crítica debe apoyarse en un proceso sólido de monitoreo fundado sobre estándares y buenas prácticas internacionales, como lo son el Instituto Nacional de Estándares de los Estados Unidos (NIST, por sus siglas en inglés) y el Centro para la Seguridad de Internet (CIS, por sus siglas en inglés) quienes proporcionan recomendaciones precisas para la implementación de la supervisión de eventos de seguridad. Adicionalmente, se subraya la relevancia de enriquecer estas bases con los marcos de la Fundación de Código Abierto para la Seguridad de Aplicaciones (OWASP, por sus siglas en inglés) y de la Corporación MITRE, conocido como las Tácticas, Técnicas y Conocimiento Común de los Adversarios (ATT&CK, por sus siglas en inglés, y conocido como MITRE ATT&CK), así como la importancia de emplear mecanismos y herramientas clave como el uso de Centros de Operaciones de Seguridad (SOC, por sus siglas en inglés), Gestores de Seguridad de la Información y Eventos (SIEM, por sus siglas en inglés) y la inteligencia de amenazas e indicadores de compromiso.

II. MÉTODO

En el presente artículo se hace uso de un grupo importante de normas, las cuales permiten establecer un fundamento sólido para definir una propuesta de un marco de referencia para el monitoreo de eventos de ciberseguridad en las instituciones del sector público. Se considera el estándar de NIST como la base principal, debido a su robustez y detalle, donde se establece un ciclo asentado en cinco pilares: identificación, protección, detección, respuesta y recuperación. Los controles CIS refuerzan el planteamiento con recomendaciones más precisas en términos de implementación y deja de lado los elementos administrativos como políticas y lineamientos. Los marcos anteriores son fortalecidos con la matriz de MITRE ATT&CK, la cual permite aplicar las recomendaciones en cada fase de un ataque, dependiendo de la táctica, técnica y procedimiento utilizado por el adversario, y adicionalmente funciona como una fuente de información que permite perfilar al atacante. Por último, pero no menos importante, se complementa con la aplicación de las recomendaciones de OWASP, enfocadas en la generación, detalle y precisión de los datos registrados en bitácora, según la actividad de las aplicaciones que conviven dentro de cada ecosistema tecnológico, enriqueciendo con información de valor agregado la trazabilidad y la comprensión del evento analizado.

A. NIST

El estándar de NIST, mediante su publicación del marco de ciberseguridad SP800-137 basado en riesgo, engloba dentro del proceso de detección, los controles administrativos, como lo son definiciones de políticas, disposiciones, procedimientos y

guías, que establecen las bases para implementar y ejecutar los controles técnicos necesarios, los cuales son requeridos para identificar potenciales amenazas y anomalías dentro del entorno tecnológico. De manera complementaria aporta las recomendaciones y pasos a seguir para establecer un ciclo de monitoreo continuo y un proceso de medición que permita verificar de forma numérica la efectividad de los controles establecidos. También hace referencia a las necesidades de capacidad técnicas, talento y experiencia del recurso humano, los requerimientos de mecanismos y herramientas en la parte tecnológica, así como la integración de ambos para realizar las tareas con precisión y eficacia (Dempsey et al., 2011).

B. CIS

El marco de CIS corresponde a un conjunto de buenas prácticas de libre acceso, dividido en 20 controles críticos, cuyo origen se fundamenta en ataques reales y contramedidas aplicadas para su contención y mitigación de impacto. Su objetivo específico es brindar una guía para la implementación de acciones priorizadas con la finalidad de minimizar el potencial riesgo de las amenazas cibernéticas. El enfoque se centra en la identificación de las áreas más críticas y la selección de las medidas defensivas que aporten mayor valor, dentro de las que se pueden determinar herramientas como el SIEM, la inteligencia de amenazas o acciones concretas como el análisis de bitácoras. La organización CIS tiene como principio que las herramientas son efectivas cuando se implementan dentro de un proceso de monitoreo de ciberseguridad continuo, donde se complementan con personas y procesos, lo cual fortalece las capacidades y habilidades para prevenir, detectar y responder ante amenazas cibernéticas (CIS, 2021).

C. MITRE ATT&CK

Este marco de trabajo se define como una base de datos estructurada a través de una matriz exhaustiva y organizada, donde se reflejan las fases de un ataque cibernético, cuyo contenido es poblado mediante la observación de ataques específicos y la información se clasifica en técnicas, tácticas y procedimientos; esto permite perfilar al adversario y sus objetivos. La importancia de este contenido radica en la relevancia que aporta para el proceso de monitoreo continuo, en la definición precisa de los casos de uso a implementar para la detección temprana de potenciales amenazas e incidentes de ciberseguridad. Aunado a lo anterior, el aporte informativo robustece los argumentos en la toma de decisiones acertada ante un evento de ofensiva cibernética. Adicionalmente, el detalle de la documentación proporciona a las organizaciones un insumo de valor, que enriquece los procesos de identificación de puntos susceptibles a potenciales brechas de seguridad o vulnerabilidades explotables, con impactos negativos o críticos dentro del entorno tecnológico (Mitre Corporation, 2020).

D. OWASP

El proyecto OWASP no se reconoce como un marco de trabajo, sin embargo, su enfoque está basado en riesgos de seguridad en las aplicaciones web, cuyo principal objetivo es proveer recomendaciones importantes en materia de bitácoras, herramientas y recursos, considerados elementos clave para el desarrollo y ejecución de las tareas y actividades del proceso de monitoreo continuo de seguridad cibernética. Dentro del proyecto OWASP Top 10 2021, específicamente en el riesgo A09 (Fallas en el registro y monitoreo), se aportan guías que orientan en la definición de datos esenciales que deben contener los registros generados de cada actividad o tarea ejecutada por el sistema, lo que brinda mayor visibilidad y profundidad en la trazabilidad, análisis y comprensión de los eventos valorados por los analistas de seguridad. La definición de este riesgo apunta a fortalecer las capacidades para detectar y responder ante brechas activas de ciberseguridad, por medio de la generación de registros estandarizados con datos de valor relevantes de cada aplicación o componente de esta (OWASP, 2021).

Después de identificar las fortalezas que presentan estos marcos y buenas prácticas en ciberseguridad, se comprende que su integración complementaria proporciona un sólido fundamento para robustecer la capacidad del monitoreo continuo de eventos de seguridad, a través de la identificación y detección de las amenazas cibernéticas, marcos y buenas prácticas que pueden ser aplicables a mejorar la protección y respuesta en los entornos tecnológicos de las instituciones del sector público costarricense.

III. ¿CÓMO ESTAMOS?

Luego de los eventos de ciberataques, reconocidos internacionalmente en el año 2022, Costa Rica se posicionó como un objetivo de interés para adversarios cibernéticos, que dejaron en evidencia severas carencias dentro de la postura de seguridad en instituciones gubernamentales. Uno de los hallazgos más importantes es la falta de un proceso eficiente de monitoreo continuo de ciberseguridad en un contexto nacional, sectorial e institucional, que hubiese podido mitigar el impacto negativo a nivel económico, social, comercial y político. En materia de seguridad cibernética, la visibilidad se comprende como la capacidad de conocer e interpretar lo que sucede en el entorno tecnológico de las organizaciones y detectar cuando algún evento o acción sobrepasa los umbrales de comportamiento regular. A partir del argumento de

ciberseguridad señalado por Quade (2018) donde indica que no se puede proteger lo que no se ve o no se conoce, se entiende que la falta de supervisión de seguridad en las organizaciones se traduce en un vacío en los controles de detección, donde se potencializa el riesgo de ataques como consecuencia de la falta de visibilidad en los entornos tecnológicos, lo que se considera una vulnerabilidad crítica y acarrea por defecto un incremento de las posibilidades de movimientos y acciones sigilosas por parte de los atacantes sin ser detectados, un debilitamiento de la resiliencia ante intrusiones cibernéticas y una disminución importante en las capacidades de respuesta y toma de decisiones eficaz ante eventos de crisis en seguridad de la información.

El país, como miembro activo de varias organizaciones y acuerdos internacionales en materia de ciberseguridad, participa de manera diligente en auditorías y estudios, realizados por organismos internacionales, que evalúan la postura de seguridad nacional. Dichas valoraciones ubican al país dentro de una fase de desarrollo tecnológico en crecimiento y asignan una calificación positiva respecto a capacidades normativas, en referencia a leyes, políticas, lineamientos, directrices y demás. Sin embargo, los mismos estudios demuestran una brecha con relación al área técnica y operativa, donde se constata que los controles definidos no son implementados o ejecutados de manera oportuna y eficaz, tema que es igualmente detallado en los informes de la Entidad de Fiscalización Superior de Costa Rica.

La iniciativa del índice nacional de ciberseguridad (NCSI por sus siglas en inglés) fundamenta su evaluación en tres categorías básicas: generalidades de la seguridad cibernética, líneas base y gestión de crisis e incidentes. En lo que corresponde a la primera, el país se coloca en una posición aceptable en materia de desarrollo de políticas, educación y cooperación internacional, caso contrario es lo concerniente al análisis e información de amenazas cibernéticas, donde no se cuenta con ninguno de los requerimientos evaluados. Sobre la categoría de líneas base de ciberseguridad, se determinan fortalezas en la protección de datos y el ofrecimiento de servicios de confianza e identificación electrónica, no así en los lineamientos asociados a la seguridad de los servicios esenciales y digitales. Con relación a la tercera y última, sobre los indicadores de gestión, se identifican fortalezas en los temas de colaboración internacional y lucha contra el cibercrimen. También se determina la nula capacidad en materia de gobernanza y administración de crisis cibernéticas como una debilidad importante. Adicionalmente, se denota un dato interesante sobre la respuesta a incidentes, donde se cuenta con las entidades y normativas necesarias, pero no se tienen los recursos y capacidades técnicas y operativas para su ejecución (NCSI, 2022).

Por su parte, la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés) mediante su índice global de ciberseguridad (GCI por sus siglas en inglés) asienta su modelo de valoración sobre cinco pilares fundamentales: legal, técnico, organizativo, capacitación y cooperación. En congruencia con el NCSI, el cumplimiento de los requerimientos definidos para el primer pilar, correspondientes a la legislación nacional y los instrumentos normativos y regulatorios, son satisfactorios. De la misma manera, sobre el área técnica se identifica una brecha importante como consecuencia de la falta de capacidades en materia de detección de ciberamenazas, la gestión de crisis cibernéticas y la respuesta ante incidentes. En relación al ámbito organizativo, se representa como una fortaleza la existencia de una estrategia nacional de ciberseguridad vigente, la cual incorpora aspectos importantes como es el eje de detección y la implementación de procesos para el monitoreo cibernético en el contexto nacional y sectorial. Al igual que el índice anteriormente descrito, el pilar de capacitación evalúa positivamente los aspectos de formación educativa a nivel académico en seguridad informática, sin embargo, propone como oportunidad de mejora su inclusión en la educación primaria y secundaria, además del desarrollo de capacidades especializadas. Asimismo, valora satisfactoriamente la conformación de comunidades reconocidas de profesionales. Finalmente, y también coherente con el NCSI, los indicadores asociados a la cooperación obtienen una calificación positiva a raíz de la participación del país como miembro activo de organismos y foros internacionales relacionados con temas de ciberseguridad y afines (International Telecommunication Union (ITU), 2021).

Desde una perspectiva nacional, la legislación ha delegado en el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt) la responsabilidad de velar por los temas relacionados con ciberseguridad, y por lo tanto asume la rectoría de las gestiones necesarias para mantener y fortalecer la postura de seguridad del país y a la vez el compromiso de alcanzar el cumplimiento de los requerimientos evaluados por los organismos internacionales. La institución cuenta con el Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR), unidad del equipo de expertos en la materia cuya responsabilidad consta de prevenir y responder ante eventos cibernéticos que potencialmente puedan afectar al sector público y que cuenta con las facultades requeridas de coordinación tanto con los Poderes del Estado como con las instituciones gubernamentales. A pesar de que sus obligaciones y funciones están claramente definidas, la Contraloría General de la República ha señalado limitaciones y deficiencias en el Ministerio en materia de gobernanza y coordinación, así como en el CSIRT-CR en cuanto a recursos, capacidades y experiencia (Contraloría General de la República, 2022). Ante esta realidad, se publica la nueva estrategia nacional de ciberseguridad que pretende solventar las brechas para el año 2027, la cual cuenta con un enfoque basado en riesgos y se fundamenta en los pilares de evaluación del GCI (May Grosser, 2023).

Para asegurar el éxito de la estrategia, resulta imperativo contar con una participación activa de equipos multidisciplinarios e interinstitucionales. No obstante, al reconocer que una de las brechas más significativas radica en el ámbito técnico, se vuelve esencial aprovechar las recomendaciones y buenas prácticas establecidas en diversos marcos y proyectos de ciberseguridad. Estos elementos desempeñan un papel fundamental en la implementación y fortalecimiento de un proceso efectivo de detección de amenazas, a través del monitoreo de la seguridad cibernética. Este enfoque es aplicable a nivel nacional, sectorial e institucional, destacando la relevancia crucial de incorporar estos estándares para mejorar la resiliencia ante posibles ciberamenazas.

Resultado del análisis detallado de la normativa referente, se determina que el marco de ciberseguridad NIST, mediante su función de detección, señala la necesidad de un monitoreo continuo de activos y sistemas de información para identificar eventos de ciberseguridad y evaluar la efectividad de los controles establecidos, asimismo, resalta la importancia de detectar actividad anómala de manera temprana y la comprensión de su potencial impacto. Los controles CIS complementan el proceso de detección a partir de la buena práctica sobre gestión de bitácoras de auditoría en la plataforma tecnológica, así como su recolección y centralización, esto con el fin de analizar y correlacionar los datos colectados que permita alcanzar una visibilidad integral del entorno y un entendimiento de su comportamiento, con el propósito de identificar de manera anticipada alguna potencial amenaza y responder efectivamente. Mediante la matriz de tácticas, técnicas y procedimientos de MITRE ATT&CK se enriquece el proceso de detección al brindar detalle sobre elementos específicos que requieren monitoreo y la forma de aplicarlo. Adicionalmente, la documentación contenida aporta la capacidad de perfilar los potenciales atacantes, lo cual brinda información de valor para la toma de decisiones y la respuesta del equipo de atención de alertas e incidentes. Por último, OWASP aporta un valor agregado al incluir, dentro del proceso de monitoreo continuo de ciberseguridad, la recopilación de información contenida en bitácoras como estructuras con datos estandarizados y de calidad, que registran el uso y actividad de las aplicaciones, características que permiten mayor profundidad en el flujo de análisis y detección de eventos ciberseguridad.

La aplicabilidad y el valor del resultado de la implementación de los controles descritos anteriormente se sintetizan en la ilustración número 2, donde se plasma el flujo de ataque perpetrado por el adversario cibernético Conti contra la infraestructura tecnológica del Ministerio de Hacienda en abril del 2022 según Ilascu (2022), en complemento con las contramedidas aplicables que hubiesen permitido una posible detección de la intrusión en diferentes fases del ataque, por ende una respuesta más efectiva y un menor impacto. Dentro de la misma, se puede comprender la integración que tienen los marcos y buenas prácticas descritas anteriormente y se señala la relevancia de un proceso de monitoreo continuo de ciberseguridad en diferentes puntos del entorno organizacional.

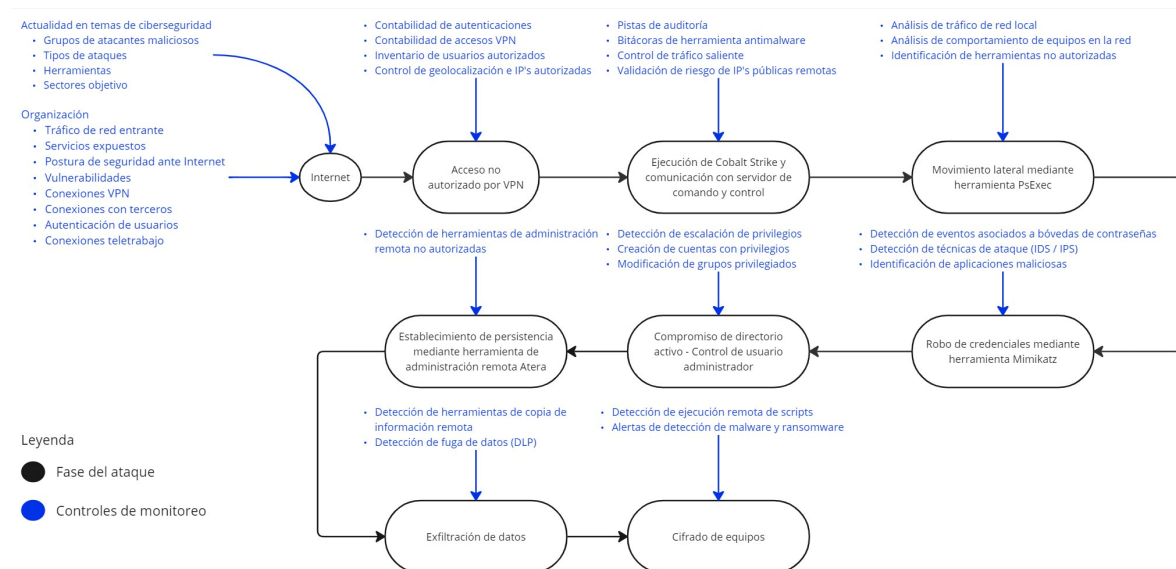


Ilustración número 2 - Flujo de técnica de ataque de grupo Conti y controles de detección
Fuente: Confección propia basada en los resultados de este estudio.

La versatilidad que aporta el uso complementario de los controles estipulados en las regulaciones de ciberseguridad para un proceso de supervisión integral, permite un análisis exhaustivo de las tácticas empleadas por atacantes reconocidos desde diversas perspectivas y brinda potenciales abordajes de alerta y respuesta. Al utilizar la información de la matriz de MITRE

ATT&CK como referencia, la ilustración número 3 diagrama la metodología utilizada por el grupo ciberdelincuente Hive según Basque Cybersecurity Agency (2022), responsable del incidente cibernético que impactó la Caja Costarricense del Seguro Social (CCSS) en mayo 2022 y define los puntos del entorno que requieren monitoreo continuo de ciberseguridad.



Ilustración número 3 - Flujo de técnica de ataque de grupo Hive y controles de detección
Fuente: Confección propia basada en los resultados de este estudio.

El detalle de las ilustraciones 2 y 3 evidencia el potencial de los controles para fortalecer las actividades en materia de detección temprana de ciberamenazas e incidentes, sin embargo, se requiere de un plan mayor que permita la implementación sistemática y organizada de un proceso de monitoreo continuo de ciberseguridad. En este punto del tiempo se manifiesta la relevancia de la nueva estrategia de ciberseguridad de Costa Rica, publicada en noviembre del 2023, donde se incluye un capítulo dedicado al eje de detección, que engloba dentro de las recomendaciones instaurar centros de operaciones de seguridad a nivel nacional y sectorial. Dicho documento está alineado con los cinco pilares del marco NIST y enfocado directamente sobre las medidas de seguridad cibernética evaluadas por la ITU mediante el GCI, que de igual manera aportan el insumo necesario para el cumplimiento de los requerimientos de indicadores evaluados en el NCSI. Adicionalmente, para cada objetivo estratégico, se definen diversas líneas de acción, que determinan el grado de participación y colaboración a nivel institucional para integrarse al programa nacional de fortalecimiento de la postura de ciberseguridad.

IV. ¿QUÉ OFRECEMOS?

El objetivo del monitoreo de seguridad es preservar la reputación de las organizaciones, proteger la privacidad de los datos, garantizar la disponibilidad de los servicios, así como prevenir el uso indebido de los mismos. Este proceso es habilitado mediante la estrategia de ciberseguridad organizacional, la cual forma parte de la gestión de riesgos integral de la institución y se basa en la premisa de que la seguridad de la información no se puede lograr únicamente mediante medidas estáticas o puntuales, sino que requiere una vigilancia constante y actualizada. La ilustración número 4, contextualiza de forma panorámica, el proceso desde su fundamento, donde se reconocen tres enfoques relevantes: uno es el cumplimiento de configuración, seguido por la gestión de vulnerabilidades y pruebas de seguridad, y finalmente el análisis de eventos y anomalías, siendo este último el elemento más robusto en la detección temprana de ciberamenazas, ya que fortalece la capacidad de respuesta y la eficacia en la toma de decisiones, con el fin de reducir el impacto de las brechas de seguridad y evitar la evolución a incidentes mayores.

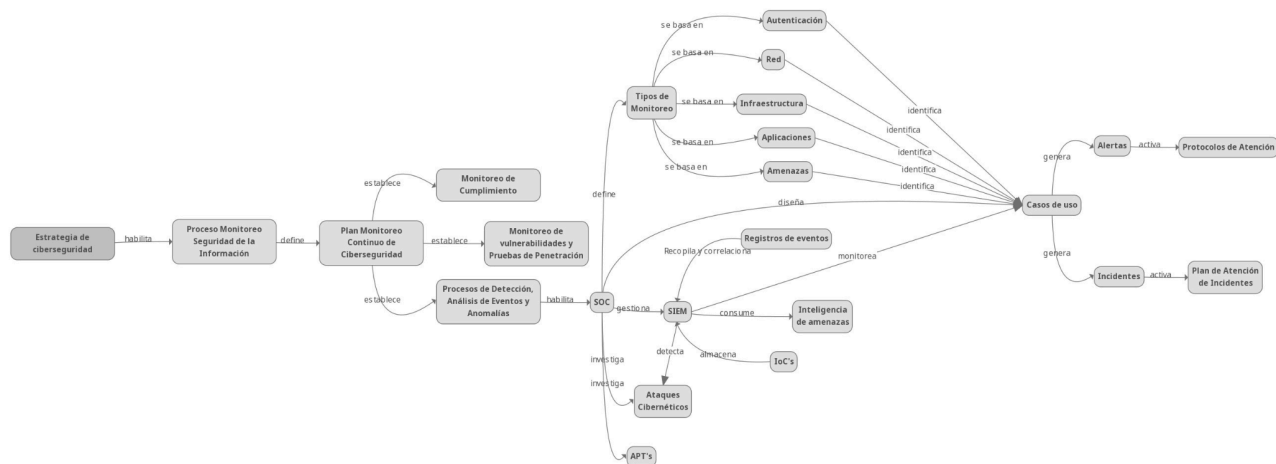


Ilustración número 4 - Mapa conceptual del proceso de monitoreo continuo de ciberseguridad propuesto por los autores de este estudio.

Fuente: Confección propia basada en los resultados de este estudio.

El mapa conceptual propuesto identifica dentro del proceso de detección, la interrelación de los componentes administrativos y técnicos necesarios para implementar mecanismos y controles, lo que aporta visibilidad dentro del contexto cibernético de la organización y permite establecer un SOC como el pilar centralizado para ejecutar el monitoreo continuo de ciberseguridad con base en el análisis de eventos (Azmi et al., 2016).

En el ámbito de la ciberseguridad, se reconoce que la tecnología por sí sola no es totalmente efectiva, por lo que se complementa con una gestión adecuada por parte del recurso humano, quien a su vez se apoya en procedimientos estandarizados para llevar a cabo sus funciones de manera correcta. Por lo tanto, se entiende que la interacción entre estos tres agentes esenciales (recurso humano, tecnología y procedimientos) es fundamental para el funcionamiento óptimo y la madurez de un SOC, y por tanto, se considera el cerebro y corazón del proceso de análisis de eventos en un sistema de monitoreo continuo. El nivel de madurez depende directamente del estado de desarrollo individual de cada uno de estos agentes. A medida que cada uno de ellos avanza y mejora en su evolución, la detección de amenazas e incidentes cibernéticos se vuelve más efectiva y precisa. Esta sinergia es un enfoque integral que reconoce la importancia de cada agente y su contribución para alcanzar una postura de seguridad robusta en el entorno actual (Criollo Hernandez et al., 2021).

Al comprender la relevancia e importancia de un SOC desde una perspectiva de seguridad, la propuesta desarrollada en la investigación sobre un marco de referencia para monitoreo continuo en instituciones del sector público de Costa Rica se convierte en una valiosa herramienta, cuyo objetivo se centra en proveer una guía adaptable para la implementación y mejora continua del proceso, con base en buenas prácticas internacionales y alineada con la Estrategia Nacional de Ciberseguridad 2023-2027, y a través de la cual se brinda un enfoque sólido y orientado hacia la seguridad, para fortalecer las capacidades de monitoreo y reforzar de manera consistente la respuesta ante amenazas e incidentes cibernéticos.

A. Marco de referencia

El marco de referencia se construye sobre una estructura organizada donde se describe la visión general de la propuesta, los requerimientos, los tipos de monitoreo y finalmente, la evaluación de la criticidad de alertas e incidentes. Este documento engloba una breve descripción explicativa sobre la propuesta en general, las normativas utilizadas como base y su intención. Asimismo se definen los objetivos específicos y el alcance, los cuales aportan la información necesaria para justificar su implementación o mejora sobre los entornos de infraestructura de las instituciones del sector público costarricense. Adicionalmente incluye una guía de uso que proporciona de manera detallada una metodología de aplicación, con la finalidad de definir un plan de trabajo ordenado para llevar a cabo el proceso de operación de un sistema de monitoreo continuo de ciberseguridad mediante un SOC.

B. Requerimientos

El planteamiento propone una lista detallada sobre requerimientos básicos necesarios, identificados durante la investigación, para establecer un proceso robusto de monitoreo continuo de seguridad cibernética en las organizaciones. Esta se complementa con una serie de requisitos deseables con el objetivo de fortalecer las bases de la implementación y elevar el nivel de madurez a lo largo del ciclo de vida mediante la mejora continua.

Los requerimientos definen en primera instancia la importancia del recurso humano, además de las aptitudes técnicas y de conocimiento necesarias para la ejecución de actividades y tareas propias del proceso. Con fundamento en los estándares internacionales y las buenas prácticas de NIST y CIS, este marco recomienda una clasificación del recurso humano en tres niveles distintos, donde se definen los roles, responsabilidades y alcance de las funciones con base en las capacidades técnicas, el conocimiento y la experiencia del funcionario. El primer nivel, siendo el más bajo, contempla tareas de triaje, es decir, la clasificación y priorización de eventos de seguridad según su magnitud, potencial impacto y criticidad del riesgo. Lo anterior los ubica como la primera línea de detección en el proceso de análisis, monitoreo y notificación de anomalías, alertas e incidentes. Adicionalmente, este equipo tiene las habilidades necesarias para atender y resolver consultas de baja complejidad. El nivel dos, corresponde al equipo cuyo personal con habilidades técnicas y conocimiento intermedio el cual cuenta con más experiencia en el campo, por lo que sus funciones se definen como la inteligencia del proceso de monitoreo, donde sus responsabilidades se enfocan en la analítica detallada y la investigación profunda de los eventos de seguridad con el objetivo de formular, mantener y documentar los casos de uso utilizados para la detección de ciberamenazas, generar las alertas y proveer información precisa de valor a los equipos de respuesta durante incidentes y eventos de crisis cibernéticas. De manera complementaria, debido al conocimiento del entorno y la experiencia, se delega sobre este grupo la responsabilidad de gestión del SIEM, la atención de consultas de complejidad media y aquellas que sean escaladas por los analistas del primer nivel. Por último, se define el equipo de analistas de nivel tres como el punto más alto del proceso de monitoreo, el cual abarca al personal experimentado con capacidades técnicas avanzadas en el campo de la ciberseguridad y habilidades blandas de interacción con personal jerárquico no técnico de otras unidades de la organización. Este rol comprende la responsabilidad de definir los orígenes de datos que alimentarán al SIEM, así como las fuentes de inteligencia de amenazas que serán consumidas. También, como personal crítico del equipo de respuesta ante incidentes, debe tener un conocimiento actualizado del contexto cibernético, las ciberamenazas y los grupos adversarios, con la finalidad de identificar mediante investigación, cacería de amenazas o validación y evaluación de casos de uso, los potenciales riesgos de ciberseguridad que puedan afectar e impactar a la organización. Finalmente, el equipo de analistas de este nivel tiene a cargo la atención y resolución de consultas de alta complejidad, así como las escaladas por los niveles inferiores.

Los procedimientos son parte de los requerimientos básicos, cuya importancia radica en la estandarización y documentación de los roles y responsabilidades por cada uno de los niveles de analistas, donde su contenido define de manera detallada las actividades y tareas a realizar, lo que permite un funcionamiento fluido y preciso del proceso de monitoreo continuo de seguridad cibernética y marca un punto clave en la interrelación necesaria entre personas y tecnología en un SOC. Es importante señalar que los procedimientos se consideran elementos dinámicos, por lo tanto requieren una revisión y actualización periódica, adaptados a la realidad de cambio constante en el ámbito cibernético.

Con respecto al requerimiento tecnológico se determina la necesidad de un SIEM como parte fundamental de la tríada conformada con personas y procedimientos. Esta herramienta se convierte en el punto centralizado de recolección y correlación de eventos, lo cual facilita mediante los casos de uso basados en la matriz de MITRE ATT@CK y su comparación con indicadores de compromiso, la detección de amenazas de manera temprana, misma que permite la activación de alertas para la pronta respuesta por parte de los equipos responsables. Este componente del ecosistema de ciberseguridad debe tener capacidades de analítica suficientes para reducir el impacto de potenciales incidentes a través de los datos recolectados de las distintas fuentes. Uno de los aspectos más importantes del SIEM, es el almacenamiento histórico e inalterable de los eventos recibidos, lo cual proporciona a los equipos de seguridad la realización de análisis forenses, cacerías de amenazas y la generación de informes técnicos y ejecutivos sobre las tendencias cibernéticas del entorno tecnológico y la postura de ciberseguridad organizacional en materia de detección y protección. Dependiendo del modelo funcional de las organizaciones y de los recursos económicos disponibles, la herramienta puede ser de paga o gratuita e implementable en nube o en sitio. También permite que la gestión se realice por personal interno o por parte de un tercero bajo un esquema de contratación.

Otros requerimientos corresponden a la selección adecuada de fuentes de datos que provean la información necesaria para poder generar e implementar casos de uso adecuados a los contextos de seguridad. Es importante señalar la necesidad de que los orígenes sean estandarizados e integrables de manera sencilla al SIEM y en el caso de las aplicaciones que las bitácoras contemplen las recomendaciones brindadas en el proyecto de OWASP Top 10. En relación a los casos de uso se deben considerar elementos como la documentación que expliquen su origen, su objetivo, y brinden un entendimiento general del mismo. La efectividad y precisión de estos para la detección de amenazas y anomalías está estrechamente relacionada con la calidad de datos obtenidos de las bitácoras. Además de lo anterior, es necesario contar con una matriz de escalamiento en la cual se defina el flujo que deben llevar las tareas y alertas para su debida atención de manera eficiente en tiempo y forma. Finalmente, se requiere una herramienta o plataforma que permita el registro de los alertamientos e incidentes con el propósito de poder dar seguimiento y trazabilidad a estos eventos por medio de la documentación.

En lo que se refiere a elementos deseables, es necesario considerar una política de seguridad de la información que establezca el compromiso de la alta gerencia, una unidad de negocio que habilite al personal para asumir y ejecutar las tareas de supervisión de forma dedicada, y un proceso constante de capacitación y formación con el objetivo de mantener actualizado al equipo en temas de ciberseguridad y monitoreo.

C. *Tipos de monitoreo*

El marco de referencia ofrece una variedad de cinco tipos de monitoreo por aplicar, donde contempla cada elemento y su utilidad, lo cual brinda una amplia perspectiva sobre las capacidades de monitoreo que pueden alcanzar las entidades públicas y de igual manera ofrece la versatilidad de aplicarse acorde a las necesidades y posibilidades de cada una de estas. La clasificación de estos permite una supervisión del entorno desde diversas perspectivas, lo cual proporciona una visibilidad integral del entorno de ciberseguridad en las entidades.

El monitoreo de la red contempla la recolección y el análisis de todos los datos generados por la comunicación debido a la interconexión de los nodos dentro del entorno tecnológico y su interacción con el contexto externo, cuyo fundamento se basa sobre el diseño de arquitectura, lo cual permite de manera natural comprender los flujos lógicos del tráfico y detectar de manera temprana potenciales anomalías que puedan interpretarse como debilidades, vulnerabilidades, brechas, ataques o incidentes de seguridad cibernética. Por lo general las fuentes de datos utilizadas para este modelo incluyen los dispositivos de comunicación, los cortafuegos, las alertas generadas por herramientas de detección y prevención de intrusos, las plataformas de control de navegación y los dispositivos de análisis de tráfico. Es importante señalar que la capacidad de visibilidad que se alcance en este contexto depende directamente de la cantidad de orígenes de datos y la calidad de estos. Adicionalmente, es necesario contar con un conocimiento suficiente para interpretar los campos de los eventos registrados con el objetivo de poder determinar cuales tienen un valor importante para las tareas de monitoreo. Los resultados que se obtienen de este tipo de supervisión abarcan la detección y alerta temprana de amenazas, la validación del cumplimiento en la aplicación de buenas prácticas asociadas como segmentación de red y uso de protocolos seguros, las tendencias de volumen de tráfico de red, así mismo, el comportamiento organizacional en cuanto al uso de internet, las categorías y cantidad de sitios visitados. Todas las métricas anteriores se convierten en insumos importantes para la definición o depuración de los controles de seguridad y las líneas base de aseguramiento de red.

Otra de las ventajas de este tipo de monitoreo es la identificación de indicadores de compromiso asociados a archivos, comandos, cargas útiles y demás, obtenidos mediante la desenscripción segura del tráfico de red, donde es importante excluir datos sensibles que puedan comprometer la confidencialidad e integridad de las comunicaciones, como lo son identificadores de sesión entre otros. De manera complementaria, la integración con fuentes de inteligencia de amenazas robustecen las capacidades de detección, lo que permite al proceso de supervisión aplicar casos de uso con un mayor nivel de precisión.

Otro modelo se fundamenta en la supervisión sobre los elementos de la infraestructura, es decir, la recolección, análisis y correlación de eventos generados localmente por los equipos conectados al entorno tecnológico, cuyos registros se generan según las pistas de auditoría activas y permiten la trazabilidad de cada tarea, actividad o acción realizada de manera interna. Este nivel de visibilidad permite comprender el comportamiento habitual y detectar de manera temprana algún evento que genere actividad particular, por ejemplo, la instalación de un servicio nuevo no reconocido, la ejecución de un archivo o la modificación de una extensión de archivo que modifique el comportamiento de este, por citar algunos casos. Dentro del marco de referencia propuesto, se definen las bitácoras necesarias que deben alimentar al SIEM para estar en capacidad de implementar casos de uso precisos y específicos por cada tecnología, entendiendo por esto, tipo y versión de sistema operativo, motores de base de datos, herramientas de prevención de malware y servicios locales instalados. Un requisito importante para este modelo es la existencia de una base de datos actualizada de los activos tecnológicos de la organización, que habilite la capacidad de identificar los registros de las pistas de auditoría requeridas por cada nodo. Estas recomendaciones se apoyan en las buenas prácticas de los controles CIS y NIST, con el objetivo de contar con una visibilidad integral de los dispositivos que soportan los servicios tecnológicos de la organización, donde se obtiene como resultado la detección de anomalías causadas por errores de configuración o por intentos de actividad maliciosa ejecutada por algún atacante o intruso. De igual manera, estos registros se convierten en insumos de datos valiosos para la aplicación de acciones de contención y erradicación por parte de los equipos de respuesta de incidentes y para actividades de análisis forense digital en la reconstrucción de eventos. Este monitoreo también permite reconocer datos críticos relacionados a los servicios que soporta el equipo, como lo es el registro completo de una petición específica de un servicio web, la resolución de un nombre de dominio asociado a una dirección IP interna o externa mediante el servicio DNS, e inclusive el bloqueo entrante o saliente de algún tipo de aplicación no autorizada en el servicio de cortafuegos instalado a nivel local, situación que eleva en gran cantidad las posibilidades de potenciales casos de uso que se puedan implementar. Al igual que el modelo anterior, la automatización de la analítica de los eventos se puede potenciar con la integración de fuentes de inteligencia de

amenazas, pero requiere de la participación del recurso humano para que el flujo de notificación, atención y escalamiento sea funcional con base en los procedimientos establecidos previamente.

Uno de los elementos más críticos en cualquier plataforma tecnológica es el proceso de autenticación, ya que este determina si la cuenta, el usuario o la aplicación es quien dice ser y con base a su resultado permite o deniega el acceso al activo, por consecuencia, requiere de un monitoreo específico que examine de manera detallada todos los eventos relacionados con esta actividad, con el fin de revelar potenciales irregularidades del comportamiento usual y alertar sobre ataques de fuerza bruta, compromiso de credenciales, mal uso de cuentas de acceso o intentos de evasión del control. Para este modelo se deben considerar todas las plataformas locales o en nube, mediante las cuales se ofrece este servicio para consumo de la organización como fuentes de datos, así como se deben considerar todas las pistas de auditoría que permita la supervisión de este proceso al utilizar cuentas locales en los dispositivos. En la actualidad, como consecuencia de la criticidad de esta validación y la gran cantidad de técnicas existentes para violentar este control, la estandarización de los registros y la calidad de los datos contenidos es algo normal dentro de las bitácoras. Adicionalmente, existe una amplia documentación de libre acceso sobre técnicas y casos de uso reconocidos para la detección de múltiples amenazas asociadas, por ejemplo, ataques de tipo kerberoasting, golden ticket, pass-the-hash, impossible travel login, por citar algunos de los más conocidos, o también para identificar debilidades en el control, como lo es la falta de uso de múltiples factores de autenticación para acceso desde entornos remotos, vulnerabilidad ampliamente explotada por los adversarios y reconocida en la matriz de MITRE ATT&CK como la táctica de acceso inicial. Dentro del contexto interno, el monitoreo permite reconocer actividades lícitas o ilícitas de escalamiento de privilegios, según el tipo de evento, cuyo alertamiento temprano permite una disminución del potencial impacto.

Es importante remarcar que este monitoreo no solo se enfoca en el proceso de validación, sino que también debe abarcar eventos relacionados con las cuentas, como los cambios de contraseña, las acciones de creación, modificación, borrado, activación, desactivación o bloqueos, así como el uso de múltiples factores de autenticación según la modalidad permitida, entre otros. Como parte de los insumos, se debe contar con una base de datos centralizada y actualizada que almacene un inventario de las cuentas existentes que identifique su tipo y parametrizaciones generales, predefinidas según los procedimientos para dar de alta o de baja estos activos. Todo lo anterior faculta al equipo del SOC para implementar casos de uso precisos, según sea el servicio o las condiciones ambientales del usuario en cuestión.

El monitoreo de los registros de eventos generados por diversas aplicaciones es un componente esencial, el cual permite alcanzar los objetivos propuestos en el proyecto OWASP Top 10, que pretende la identificación de incidentes de seguridad, la violación de políticas, la detección de vulnerabilidades, el reconocimiento de actividades exitosas o fallidas de explotación y el establecimiento de líneas base de seguridad. Es por ello que este tipo de monitoreo está ligado a la necesidad de contar con la centralización y constante recolección de los registros en un repositorio consolidado que mantenga la integridad de las información y permita una visión unificada y actualizada del comportamiento de las aplicaciones en materia de seguridad, cuyo objetivo es identificar patrones, tendencias y posibles amenazas de manera proactiva. A pesar de que su contexto de visibilidad es más limitado en alcance, en comparación con los modelos anteriores debido a que se enfoca únicamente en la aplicación, el modelo brinda mayor profundidad y comprensión sobre las actividades y tareas que suceden dentro de esta. El marco de referencia propuesto contempla de forma individualizada cada uno de los elementos, donde se establece el detalle asociado para cada tipo de aplicación web o local, sea esta de caja, hecha a la medida o un desarrollo interno. De igual manera abarca los servicios SaaS, herramientas colaborativas y de conferencia en línea, donde la superficie de ataque es más amplia debido al entorno donde se consume. En complemento, el detalle de supervisión considera los registros de las bases de datos y los dispositivos de cortafuegos dedicados que las protegen, lo cual brinda visibilidad sobre acciones específicas realizadas por la lógica del sistema y permite una detección de comportamientos irregulares en la manipulación no autorizada de los objetos o la información. Asimismo, para este modelo se recomienda la integración con herramientas de monitoreo de la integridad de los archivos, cuyas alertas aceleran la identificación de cambios no autorizados y aporta capacidades de mayor precisión en el análisis de eventos. También se engloba la supervisión de la plataforma de correo electrónico, lo que impulsa la identificación de amenazas dirigidas por este medio, el cual se considera uno de los vectores de ataque más utilizados por grupos adversarios. Es importante señalar que este proceso se fundamenta sobre una base de datos de gestión de la configuración (CMDB por sus siglas en inglés) que contenga el registro de todas las aplicaciones autorizadas en la organización, así como los detalles de los componentes y su funcionalidad, datos que determinan los posibles casos de uso por implementar y definir la criticidad de estos.

Monitorear las amenazas desempeña un papel crucial en la defensa cibernética de la organización, ya que permite identificar y mitigar riesgos potenciales. En este sentido, es imperativo la integración con fuentes externas e internas de inteligencia de amenazas como controles específicos, con la finalidad de lograr una detección temprana de posibles eventos maliciosos y fortalecer la postura de seguridad organizacional. Estos servicios posibilitan la sincronización y alimentación de indicadores

de compromiso (IoC) previamente depurados y estructurados en los registros de referencia del SIEM. Este tipo de modelo considera múltiples elementos externos a la organización como la supervisión de actividad en la red oscura o profunda, lo cual faculta al equipo del SOC en mantener un conocimiento actualizado sobre el comportamiento y la actividad de grupos adversarios en relación a la entidad, y permite la definición de casos de uso pertinentes con fundamento en las técnicas, tácticas y procedimientos que ofrece la matriz de MITRE ATT&CK, con el objetivo de identificar potenciales rutas de ataque, así como anticipar posibles amenazas, facilitando una respuesta rápida y efectiva frente a posibles intrusiones. Dentro de este mismo contexto externo se recomienda el análisis de documentación de ciberseguridad generada por investigaciones y eventos cibernéticos relacionados, los cuales son accesibles a través de las publicaciones en foros, redes sociales, noticias y artículos, con el fin de dar seguimiento a las amenazas avanzadas persistentes (APT por sus siglas en inglés) activas o actividades de día cero. A este conocimiento se deben agregar los resultados de los análisis de vulnerabilidades realizados periódicamente sobre el entorno, lo que proporciona la visibilidad de las debilidades que puedan ser explotadas por los atacantes y establecer los mecanismos de detección necesarios. De manera complementaria, se considera la inclusión de los registros de alertas generadas por servicios externos o locales de protección y filtrado de correo electrónico. Estos ofrecen capacidades automatizadas para identificar campañas de phishing, spam y ataques cibernéticos activos en esta plataforma. La implementación de este modelo de monitoreo refuerza de manera contundente las capacidades proactivas y automatizadas, proporcionando datos relevantes y actualizados sobre el comportamiento activo de amenazas y adversarios a nivel mundial.

Estos modelos permiten a las entidades públicas adaptar sus estrategias de monitoreo según sus necesidades y posibilidades, brindando una visión integral y proactiva del entorno de ciberseguridad. Esto permite a las organizaciones anticiparse y responder eficazmente a las amenazas cibernéticas en constante evolución, mediante la supervisión de la red y la infraestructura, así como, la autenticación, aplicaciones y amenazas. Como parte de los elementos ofrecidos en el marco se aporta una plantilla básica como referencia para la definición y documentación de los casos de uso establecidos en las actividades de supervisión del ecosistema tecnológico, con el fin de fortalecer la postura de seguridad y ofrecer una defensa sólida contra diversos riesgos.

D. *Evaluación*

Como se ha destacado a lo largo del documento, la eficacia del proceso de monitoreo continuo de ciberseguridad radica en la estrecha relación entre personas, procedimientos y tecnología. Bajo esta premisa se comprende que la generación de alertas, función correspondiente al tercer elemento, no garantiza un nivel de seguridad intrínseco; es necesario establecer un flujo de atención ejecutado por el recurso humano, con base en lo definido en la documentación pertinente. El tratamiento de estas y los tiempos de respuesta dependen directamente de la criticidad que represente para la organización y el insumo necesario para la declaración de incidentes. Dentro de este contexto, la propuesta ofrece un capítulo de evaluación donde se sugieren matrices de calor para clasificar las alertas y los incidentes de seguridad cibernética, según la severidad basada en criterios de riesgo e impacto.

Las alertas corresponden al resultado de los casos de uso, donde por medio del análisis de uno o varios eventos de seguridad se determina el indicio sobre alguna anomalía dentro de la plataforma tecnológica, y establece el nivel de potencial afectación y criticidad en un contexto cibernético, dependiendo del activo donde se identifique. En el orden de priorizar una atención oportuna, las alertas se deben clasificar en niveles pertinentes, y en concordancia el marco recomienda el uso de la matriz de calor basado en el modelo CIS de cinco niveles, para evaluar la severidad de estas alertas de ciberseguridad, lo cual adquiere una relevancia crucial. Esta herramienta permite discernir con precisión el nivel de potencial afectación y criticidad en el contexto cibernético, adaptándose según el activo específico donde se identifiquen. El hacer uso de esta matriz de calor no solo mejora la capacidad de clasificación, sino que también proporciona una estructura metodológica que facilita la toma de decisiones informadas, permitiendo una respuesta estratégica y ágil ante los eventos de seguridad, priorizando según la gravedad percibida o la posibilidad de convertirse en incidente, en lugar de realizar evaluaciones genéricas.

Los incidentes de ciberseguridad se reconocen como una o varias alertas que conllevan algún tipo de impacto en la operación, estabilidad, continuidad o reputación de la organización, es por ello que requieren de un enfoque preciso y estructurado para su evaluación y respuesta. En este sentido, la propuesta del marco de referencia destaca la eficacia de la matriz de calor en tres niveles, respaldada por el modelo CIS. Este enfoque estratégico no solo propone la utilización de umbrales de impacto definidos de manera meticulosa, sino que también establece una metodología rigurosa que simplifica la toma de decisiones respecto a las acciones necesarias en términos de respuesta y contención. Cabe resaltar que el proceso para declarar un incidente de ciberseguridad y determinar su severidad se basa en procedimientos documentados que evalúan las condiciones de alerta, considerando la criticidad de los activos afectados según la identificación definida por la organización. La adopción de esta matriz de calor asegura una evaluación precisa y alineada con los objetivos estratégicos de la ciberseguridad de la organización y la matriz de escalamiento del plan de respuesta ante incidentes de seguridad cibernética.

Adicionalmente, el marco recomienda como medida complementaria la aplicación periódica de pruebas controladas por equipos de seguridad internos o por parte de terceros, con el objetivo de validar la eficacia de las reglas de detección y determinar la necesidad de realizar ajustes. Por otro lado, con la finalidad de evitar el fenómeno de fatiga de alertas que conlleva a una disminución en las capacidades de reacción e investigación de amenazas, la propuesta también sugiere la revisión constante de sensibilidad en la generación de alertas para lograr mantener un volumen manejable.

V. CONCLUSIONES

El marco de referencia basado en los resultados de este estudio de investigación, se erige como una guía esencial para la implementación y mejora continua del proceso de monitoreo de ciberseguridad, cuyo objetivo se enfoca en la detección temprana de amenazas y el fortalecimiento de las capacidades de respuesta rápida y eficiente ante incidentes de seguridad. Al tomar en cuenta la falta de este tipo de documentación que permite la orientación, se proporciona una herramienta de carácter novedoso y de valor para las organizaciones, mediante la cual se aporta un instrumento que ayuda a mejorar la postura en este, así como cumplir con los requisitos normativos y regulatorios relacionados con la seguridad de la información y en alineamiento con la estrategia nacional de ciberseguridad según lo dispuesto por el MICITT (2023). Su contenido define los requisitos básicos que las organizaciones deben considerar para la ejecución de las tareas de supervisión y las diferentes opciones de monitoreo con el fin de obtener una visibilidad integral a través de la complementación de varias perspectivas. El nivel de detalle en los tipos de monitoreo permite a los equipos de analistas determinar el origen de los registros requeridos, el objetivo de analizar los datos recopilados y la identificación de las potenciales fuentes de datos. Asimismo, se establecen los mecanismos de clasificación de severidad según riesgo e impacto de los eventos, que contribuyen con una adecuada priorización para las tareas de respuesta.

Es crucial subrayar que esta herramienta no se limita al contexto de la implementación de un plan de monitoreo continuo de ciberseguridad, sino que también plantea la apertura de nuevas oportunidades para la investigación y aplicación práctica de estos tipos de marcos de referencia en instituciones del sector público, validando su efectividad en entornos del mundo real, donde se sugiere la realización de mejoras continuas y la exploración de complementos al proceso de monitoreo, como el análisis de vulnerabilidades, evaluaciones de cumplimiento de configuraciones de seguridad o incluso la cacería de amenazas. Este trabajo también destaca la importancia de conceptos y temas estratégicos de ciberseguridad, que permiten la integración con planes de más alto nivel, donde se incluyen los procesos de identificación, protección, respuesta y recuperación para lograr una posición más robusta y resiliente ante las crecientes amenazas cibernéticas.

Finalmente, los resultados no solo reflejan los logros alcanzados en este trabajo de investigación, sino que también inspiran a futuros investigadores, profesionales y entidades a seguir fortaleciendo la ciberseguridad en Costa Rica y más allá, permitiendo una mayor comprensión de la defensa y ciberresiliencia e impulsando un progreso continuo en la lucha contra las amenazas cibernéticas, especialmente en el sector público.

REFERENCIAS

- [1] AESA - EY Consortium. (2022, November). Cybersecurity sector in Central America. Trade - European Commission. Retrieved May 27, 2023, from https://trade.ec.europa.eu/access-to-markets/en/country-assets/euca_05_Cybersecurity%20sector%20in%20Central%20America.pdf
- [2] Azmi, R., Tibben, W., & Win, K. T. (2016). Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy. CORE. Retrieved July 31, 2023, from <https://ro.uow.edu.au/cgi/viewcontent.cgi?article=1044&context=acis2016>
- [3] Basque Cybersecurity Agency. (2022, July). Hive Ransomware. Basque Cybersecurity Centre. Retrieved May 27, 2023, from https://www.ciberseguridad.eus/sites/default/files/2022-08/BCSC-Malware-Hive-TLPWhite_V1.pdf
- [4] CIS. (2021, May). CIS Critical Security Controls. CIS Center for Internet Security. Retrieved July 27, 2023, from <http://www.cisecurity.org/controls/>
- [5] Contraloría General de la República. (2022, December 20). INFORME N° DFOE-SOS-IF-00014-2022 INFORME DE AUDITORÍA DE CARÁCTER ESPECIAL ACERCA DE LA GOBERNANZA DE LA CIBERSEGURIDAD EN E. Contraloría General de la República. Retrieved June 11, 2023, from https://cgrfiles.cgr.go.cr/publico/docs_cgr/2022/SIGYD_D/SIGYD_D_2022026167.pdf
- [6] Criollo Hernandez, W. C., López Payés, M. A., & Yánes, J. I. (2021, October 30). Guía de aplicación para el monitoreo de ciberseguridad con herramientas de código abierto. ResearchGate. Retrieved July 31, 2023, from https://www.researchgate.net/publication/354582493_Guia_de_aplicacion_para_el_monitoreo_de_ciberseguridad_con_herramientas_de_codigo_abierto
- [7] Dempsey, K., Chawla, N. S., Johnson, A., Johnston, R., Jones, A. C., Orebaugh, A., Scholl, M., & Stine, K. (2011, September). NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. NIST Technical Series Publications. Retrieved July 26, 2023, from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf>
- [8] Ilascu, I. (2022, July 21). How Conti ransomware hacked and encrypted the Costa Rican government. Bleeping Computer. <https://www.bleepingcomputer.com/news/security/how-conti-ransomware-hacked-and-encrypted-the-costa-rican-government/>

- [9] International Telecommunication Union (ITU). (2021). Global Cybersecurity Index. ITU. Retrieved August 5, 2023, from <https://www.itu.int/pub/D-STR-GCI.01>
- [10] Jaiswar, Y. (2023, February 14). Cybersecurity Monitoring: Importance, Tools, Process. KnowledgeHut. Retrieved June 3, 2023, from <https://www.knowledgehut.com/blog/security/cybersecurity-monitoring>
- [11] May Grosser, S. (2023, November 13). Gobierno presentó Estrategia Nacional de Ciberseguridad 2023-2027. Delfino.cr. <https://delfino.cr/2023/11/gobierno-presento-estrategia-nacional-de-ciberseguridad-2023-2027>
- [12] MICITT. (2023, November 10). Estrategia Nacional de Ciberseguridad 2023-2027. MICITT. Retrieved November 13, 2023, from <https://www.micitt.go.cr/sites/default/files/2023-11/NCS%20Costa%20Rica%20-%2010Nov2023%20SPA.pdf>
- [13] Mitre Corporation. (2020, March 3). Design and Philosophy. MITRE ATT&CK®. Retrieved July 27, 2023, from https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf
- [14] NCSI. (2022, November 1). NCSI :: Costa Rica. NCSI. Retrieved August 6, 2023, from https://ncsi.ega.ee/country/cr_2022/
- [15] OWASP. (2021). OWASP/Top10. How to use the OWASP Top 10 as a standard - OWASP Top 10:2021. Retrieved July 27, 2023, from https://owasp.org/Top10/A00_2021_How_to_use_the_OWASP_Top_10_as_a_standard/
- [16] Quade, P. (2018, February 19). You can't protect what you can't see. CSO Online. Retrieved November 12, 2023, from <https://csoonline.com/article/564627/you-cant-protect-what-you-cant-see.html>
- [17] Rosales, D. (2023, May 15). La evolución de los ciberataques: un desafío para la ciberseguridad en un mundo híbrido. Revista Summa. Retrieved June 1, 2023, from <https://revistasumma.com/la-evolucion-de-los-ciberataques-un-desafio-para-la-ciberseguridad-en-un-mundo-hibrido/>