Fortalecimiento de la ciberseguridad en entornos académicos, mediante la integración de soluciones SIEM y NAC de código abierto.

Daniel Felipe Palomo Luna

Director del Proyecto

Mg. Luis Fernando Zambrano Hernández

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Maestría en Ciberseguridad

Ibagué, febrero de 2026

Dedicatoria

El presente documento es fruto del apoyo, comprensión y, sobre todo, esfuerzo de mi familia al permitirme robarles tiempo para mi crecimiento académico, este y cualquier otro logro es dedicado con gratitud infinita a ellos dado que siempre han estado dispuestos a apoyarme en lo que está a su alcance.

Agradecimientos

A la Universidad Nacional Abierta y a Distancia UNAD, por permitirme enriquecer mis conocimientos, por facilitar los mecanismos para que la educación llegue a más personas y especialmente por permitirme la ejecución de este proyecto como opción de grado.

En sintonía con lo anterior, extiendo agradecimiento especial al ingeniero y magister Luis Fernando Zambrano, por su acompañamiento en el desarrollo del presente proyecto, por el tiempo destinado y por el compromiso que demostró desde el inicio hasta la finalización del mismo.

Resumen

El presente proyecto busca brindar alternativas de código libre para abordar en instituciones de educación superior la creciente necesidad de controlar el acceso a las redes de datos y a su vez, monitorear el comportamiento de los principales activos de información, todo esto amparado bajo un escenario de aplicación de conceptos en una entidad concreta, así mismo, el documento busca ser instrumento de apoyo para quienes deseen abordar esta temática como solución a problemas presupuestales dado que como ya se mencionó, la intención es recomendar herramientas no comerciales con lo cual lo reflejado acá podrá ser replicado en ambientes productivos sin necesidad de inversión económica más allá del tiempo y dedicación por parte del personal del área de Tecnología.

Palabras clave: Ciber resiliencia, Ciberseguridad, Gestión de riesgos, NAC, SIEM.

Abstract

This project seeks to provide open source alternatives to address the growing need for higher education institutions to control access to data networks and, in turn, monitor the behavior of key information assets. This is all supported by a scenario of applying these concepts to a specific institution. The document also aims to serve as a support tool for those wishing to address this issue as a solution to budgetary problems. As mentioned above, the intention is to recommend non-commercial tools so that the content presented here can be replicated in productive environments without requiring financial investment beyond the time and dedication of IT staff.

Keywords*:* Cyber resilience, Cybersecurity, NAC, Risk management, SIEM.

Tabla de contenido

Lista de Tablas

Lista de Figuras

Introducción

El presente proyecto tiene como propósito examinar las vulnerabilidades y riesgos en materia de ciberseguridad de las infraestructuras tecnológicas en las instituciones de educación superior, con un enfoque particular en el contexto colombiano y especialmente en una institución del orden regional. En un escenario donde la transformación digital atraviesa cada vez más procesos académicos y administrativos, la protección de los datos institucionales, estudiantiles y docentes se convierte en una responsabilidad crítica. Más allá de los aspectos técnicos, este proyecto busca también promover una reflexión institucional sobre la seguridad de la información como un pilar estratégico, y no como un gasto opcional. La tecnología, desde hace tiempo, ha dejado de ser un lujo operativo: hoy representa una inversión esencial en la continuidad, reputación y resiliencia de las universidades.

Durante el desarrollo del proyecto se ha adoptado un enfoque analítico-documental que recoge experiencias reales, marcos normativos y buenas prácticas internacionales, con el fin de construir un marco de referencia sólido para la futura implementación de soluciones SIEM (Security Information and Event Management) y NAC (Network Access Control). Es importante advertir que, si bien el texto ofrece un marco técnico y conceptual robusto, no pretende ofrecer soluciones universales ni reemplazar los procesos específicos de cada institución.

Este trabajo busca transmitir un mensaje claro: proteger los activos digitales de una universidad no es solo una cuestión de infraestructura tecnológica, sino una expresión concreta del compromiso institucional con la integridad, la confianza y el futuro.

Planteamiento del problema

Formulación del problema

En términos generales, la necesidad creciente de digitalizar procesos e información en las organizaciones ha traído consigo nuevos retos para el personal de gestión de tecnología, es por esto que de manera proporcional, se desarrollan herramientas que buscan servir de apoyo en la monitorización de los activos de información, y a su vez, servir de soporte para la toma de decisiones de manera sustentada; tal es el caso de los Sistemas de Gestión de Información y Eventos en Seguridad o SIEM (Praly, Delorme, & Mitaine, 2024), por sus siglas en inglés, que permiten centralizar el monitoreo de eventos y fortalecer la gobernanza de las Tecnologías de la Información. Ahora bien, tendencias como el "Bring Your Own Device - BYOD" añaden otra capa de complejidad al escenario descrito previamente, dado que los equipos que los usuarios traen a las organizaciones no siempre cuentan con sistemas de seguridad debidamente configurados; debido a esto, se empiezan a comercializar herramientas de Control de Acceso a las Redes o NAC, por sus siglas en inglés, las cuales brindan un control sobre quien accede a una red y sobre cual dispositivo lo puede hacer según los lineamientos o políticas definidas al interior de la organización todo esto, gracias a la verificación de la postura de seguridad de la terminal antes de conceder su acceso a la red corporativa. (FORTINET, 2024)

A partir de lo anterior, y dependiendo del nivel de madurez en términos de ciberseguridad, algunas entidades han optado por delegar la gestión del monitoreo de sus activos en terceros por medio de Centros de Operaciones de Seguridad o más conocidos por sus siglas en inglés, SOC, entidades que vienen siendo contratadas especialmente para esta gestión y que

desempeñan un papel fundamental en la protección de las organizaciones ante amenazas cibernéticas (Hata, Darus, Shafiee, Petrus, & Jamian, 2023). Sin embargo, no todas las entidades pueden acceder a este tipo de servicios especialmente por los altos costos asociados entendiendo que se requiere de personal con operación las 24 horas del día lo que obviamente incrementa los costos; ante esta situación, las herramientas OpenSource y en especial, la necesidad de personal técnico con capacidades de innovación, adaptación y total disposición de aprendizaje juegan un papel determinante dado que permiten poner en marcha soluciones a partir de las herramientas de acceso libre, para lo cual, solo se requiere apropiación de las mismas y dedicación para una curva de aprendizaje menor.

Así las cosas, en el presente proyecto se busca identificar herramientas libres que permitan abordar los dos problemas previos en instituciones que no logran contratar este servicio con terceros, por un lado, se plantearán herramientas que permitan centralizar la gestión de los logs generados por diferentes dispositivos tanto a nivel de infraestructura (servidores, equipos de cómputo e impresión) como también a nivel de red (switchs, Access point, etc), aunado a esto, se pretende identificar e integrar a la solución, herramientas de control de acceso a la red con lo cual se aumentará el nivel de gestión del personal de tecnología en pequeñas o medianas organizaciones redundando en estabilización y reducción de incidentes; lo anterior aplicando lo dicho por (Crespo Martinez, 2023)

"*El monitoreo y la revisión constante son parte de la planificación del proceso de gestión de riesgos*."

Pregunta problema

Por último, se abordará esta problemática a partir de la siguiente pregunta de investigación: ¿En qué medida las herramientas de software libre permiten gestionar redes e infraestructuras en escenarios productivos, sin impactar el componente presupuestal en las organizaciones y generando un aumento en el nivel de madurez en ciberseguridad?

Justificación

A partir del problema descrito previamente, la presente propuesta toma especial relevancia dado que busca satisfacer una necesidad latente en una institución educativa de tipo universitaria, esta institución cuenta con acreditación de alta calidad por parte de las entidades de regulación nacional por lo cual debe mantener ciertas características mínimas en la prestación de sus servicios como oferta de valor a sus estudiantes, es por esto que, la tecnología y especialmente el gobierno de TI debe aportar herramientas acordes a las necesidades, que permitan apoyar la toma de decisiones y sobre todo que se alineen a la estrategia de negocio (aun cuando en la academia no se habla de negocio, sino de capacidades de transformación del entorno) de tal manera que se alcance el máximo valor de cara a los usuarios en este caso estudiantes (Fernández Martínez & Llorens Largo, 2022). Cabe resaltar que tal entidad actualmente no cuenta con soluciones de control de acceso a la red ni de gestión de incidentes de ciberseguridad lo que la lleva en casos puntuales a actuar de manera reactiva más no preventiva.

Ahora bien, es importante recordar que, a diferencia de las entidades de índole comercial, las universidades cuentan con presupuestos ajustados y cada vez más reducidos, lo que los lleva a priorizar inversiones en docencia e investigación; dado esto, las soluciones de ciberseguridad comerciales muchas veces no son una opción válida, lo que, en últimas, limita las capacidades de protección de los datos. En este contexto, el presente proyecto busca proponer el fortalecimiento de la ciberseguridad en entornos académicos mediante la integración de soluciones SIEM y NAC de código abierto. Este tipo de herramientas representan una alternativa viable, económica y adaptable a las necesidades específicas de cada institución, permitiendo a las universidades acceder a tecnología avanzada sin el costo de licencias comerciales.

En resumen, la ejecución de este proyecto busca contribuir a que las universidades no solo optimicen sus sistemas de detección y respuesta a incidentes, sino también a consolidar una cultura de ciberseguridad basada en soluciones sostenibles y efectivas de código abierto, lo que redundará en un entorno educativo más seguro y a su vez generará mayor confianza en la comunidad académica compuesta por estudiantes, docentes e investigadores, así como también, en el personal administrativo.

Por último, es importante resaltar que esta propuesta se diferencia de otros tipos de proyecto, en que no se basará en herramientas propietarias (comerciales) ya que se centrará en adaptar soluciones libres concretamente para entornos académicos permitiendo que sea sostenible y escalable en el tiempo y satisfaciendo las necesidad y limitaciones particulares de la academia.

Objetivos

Objetivo general

Medir la ciberseguridad en entornos académicos mediante la evaluación de soluciones SIEM (Sistemas de Gestión de Información y Eventos de Seguridad) y NAC (Control de Acceso a la Red) de código abierto, con el fin de mejorar la gestión de incidentes y favorecer la protección de los activos informáticos.

Objetivos específicos

Examinar vulnerabilidades y riesgos de ciberseguridad en infraestructuras tecnológicas universitarias, a partir de un ejercicio de contextualización y revisión de fuentes documentales con el fin de establecer un marco de referencia para la implementación de herramientas SIEM y NAC.

Comparar soluciones SIEM y NAC de código libre que se adapten a las necesidades y limitaciones presupuestales de las universidades, con el fin de generar una taxonomía que permita reconocer sus principales capacidades de monitorización, control de acceso y gestión de eventos de seguridad.

Diseñar un plan que permita la implementación e integración de herramientas SIEM y NAC en infraestructuras tecnológicas de universidades, por medio de la definición de un proceso de despliegue progresivo y eficiente que minimice los posibles impactos en la operación académica.

Proponer indicadores de rendimiento y seguridad que permitan evaluar la efectividad de las herramientas de código abierto implementadas, con el fin de mejorar la detección temprana, gestión y resolución de incidentes sobre los activos informáticos.

Marco referencial

Antecedentes

Artículos recientes dan cuenta de que las universidades han identificado la necesidad de mejorar su visibilidad en cuanto a eventos informáticos, con lo cual han optado por implementar herramientas tipo SIEM, un ejemplo de esto se describe en el artículo “Las universidades recurren a los SIEM de última generación para mejorar la visibilidad en ciberseguridad” donde el autor hace un recuento sobre cómo varias universidades internacionales han migrando hacia este tipo de soluciones para integrar datos de múltiples fuentes (on-premises, nube, SaaS, endpoints) y aplican automatización, inteligencia y orquestación; algo en lo que hace especial énfasis y que se presenta literalmente a continuación es: *“Un SIEM de nueva generación ofrece a las agencias una plataforma de datos unificada que aplica inteligencia y análisis modernos en un flujo de trabajo en tiempo real. Algunos sistemas también incorporan capacidades de orquestación, automatización y respuesta de seguridad (SOAR), por lo que es importante comprender lo que se ofrece al elegir la herramienta SIEM adecuada para su misión.”* (Eddy, 2024)

Otro caso documentado de uso de herramientas tipo SIEM se describe por parte de (XCELIT, 2024) donde lograron ofrecer el servicio de monitoreo 24×7, análisis de incidencias, remediación automatizada e ingesta optimizada de datos de múltiples fuentes. Además, realizaron configuración de playbooks personalizados y reglas adaptativas para reducir alertas irrelevantes y centrarse en lo crítico para un cliente del ámbito educativo (proveedor global de servicios educativos) mediante una herramienta comercial con capacidades adicionales del tipo SOAR todo gestionado para fortalecer la postura de seguridad

Ahora bien, en lo que respecta a soluciones de control de acceso a la red, se destaca el caso de éxito de la Universidad de Denver en Estados Unidos, donde describen los beneficios que han obtenido al implementar una solución de control de acceso como servicio, para este caso particular, Portnox CLEAR, sin embargo, lo relevante es que lograron asegurar sus datos sin comprometer la prestación del servicio de su red WiFi a usuarios invitados e incluso a la comunidad vecina: *"Estamos ubicados en un vecindario poblado de Denver. No tenemos inconveniente en que la comunidad use nuestro Wi-Fi, pero necesitábamos un mecanismo que lo permitiera manteniendo seguros los datos de la universidad"* (PORTNOX, 2021)

Por su parte, un estudio académico de la Universidad de Educación en Ghana, da cuenta de la implementación PacketFence junto con herramientas de gestión remota en su campus universitario para el control de acceso a la red; para esto han puesto en funcionamiento un portal cautivo para autenticar usuarios y dispositivos que se conectaban a la red LAN del campus.

En este escenario, la solución permitió que los administradores resolvieran problemas de red remotamente, mejorar control de acceso y supervisar dispositivos autorizados todo bajo escenarios de software libre. (Agyare, Adu-Boahene, & Nikoi, 2022)

Marco conceptual

En el contexto de la transformación digital y el uso intensivo de tecnologías de información en instituciones universitarias, las superficies de ataque se han ampliado de forma considerable. El incremento en la sofisticación de las amenazas cibernéticas, sumado a la diversidad de dispositivos, usuarios y servicios en red, ha llevado a que las estrategias de seguridad tradicionales resulten insuficientes para proteger infraestructuras críticas.

Así las cosas, el presente capitulo será fundamental para entender estás nuevas dinámicas y toda la conceptualización técnica requerida, para esto se presentan los siguientes puntos a considerar:

Proactividad en términos de ciberseguridad:

El contexto actual de ciber amenazas exige un cambio de paradigma en las estrategias de protección. Tal como lo advierte Fortinet en la edición más reciente de su reporte anual de amenazas:

"La evidencia es clara: los atacantes invierten fuertemente en automatización, reconocimiento y operaciones escalables. Sus métodos operativos priorizan la velocidad, el sigilo y la escalabilidad, mientras que demasiadas organizaciones siguen sobrecargadas con ciclos de parches reactivos y estrategias de seguridad estáticas." (FORTINET, 2025)

Esta afirmación que realiza dicho fabricante de equipos de ciberseguridad, subraya la necesidad de implementar soluciones que permitan a las organizaciones anticiparse a los ataques y pasar de una estrategia reactiva o una proactiva. Herramientas como SIEM, que permiten el monitoreo y la correlación temprana de eventos, y NAC, que refuerza el control de acceso a la red en tiempo real, representan componentes esenciales en una arquitectura defensiva moderna. Pasar de la reacción a la gestión continua de la exposición (CTEM) es fundamental para reducir la superficie de ataque y mejorar la resiliencia institucional.

Pilares de la Seguridad de la Información:

También conocidos como la triada de la información o simplemente la triada, es un marco de seguridad ampliamente reconocido que define los objetivos principales de la seguridad de la información. La interconexión entre estos tres objetivos implica que cualquier violación puede tener consecuencias significativas.

Confidencialidad: De acuerdo con (Osaro Mitchell, 2024), la confidencialidad implica *"proteger la información para que no sea divulgada a individuos, entidades o procesos no autorizados"*, dicho de otra manera, la confidencialidad es la capacidad de divulgar información solo a quien por responsabilidad debe tener acceso a la misma.

Integridad: El mismo estudio anterior destaca que la integridad implica *"mantener y asegurar la exactitud y completitud de los datos a lo largo de su ciclo de vida"*, con lo cual es claro que este concepto hace referencia a la garantía de que un dato no ha sido alterado de manera no autorizada, bien sea desde el momento de su generación o en su almacenamiento, todo esto con el fin de asegurar que la información es precisa y completa.

Disponibilidad: Continuando por lo expuesto por el mismo autor, es correcto afirmar que es la virtud de poder contar con la información en el momento en que se requiera; en otras palabras, es la capacidad de ofrecer un dato al usuario autorizado cuando este lo requiera.

Ciberseguridad en la Gobernanza y Gestión de TI.

Partiendo del concepto de gobierno de TI, es importante dar un contexto al lector sobre la necesidad de facilitar las gestiones no solo al área de tecnología sino a la administración en general en las organizaciones; es por esto que surge la necesidad de apoyar el logro de los

objetivos trazados desde la administración y que la tecnología como fuente de apalancamiento debe gestionar; ya con este contexto, es claro que la ciberseguridad, vista como el mecanismo de protección de sistemas, redes y en general de activos informáticos, toma un papel determinante al procurar blindar estos elementos de ataques que pudieran afectar la normal operación de la entidad.

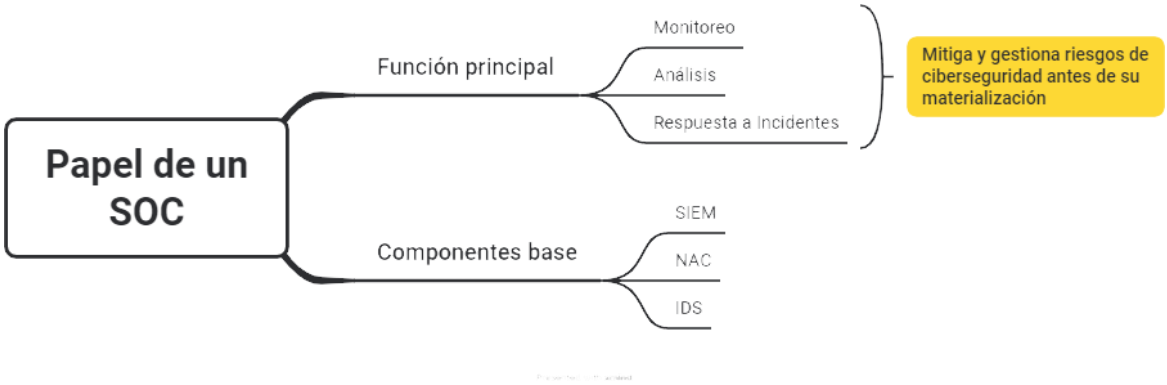
Para lograr lo anterior, surge la necesidad de describir las principales tecnologías disponibles para asegurar el acceso a la información:

Security Operations Center (SOC)

Los centros de operación en ciberseguridad se caracterizan principalmente por contar con un equipo importante de profesionales capacitados en temas de seguridad informática, así como también en reunir herramientas de software y hardware especializado en estos temas; es importante mencionar que tanto el personal como las herramientas deben trabajar en sinergia para un adecuado funcionamiento del SOC; otro dato importante a destacar es la capacidad de operar las 24 horas del día dado que los ataques pueden llegar en horarios no hábiles. Tal como lo mencionan (Paans , Schinagl, & Schoon, 2015) “El SOC se centra específicamente en las amenazas cibernéticas, el monitoreo, la investigación forense y la gestión y presentación de informes de incidentes”.

Figura 1

Aspectos relevantes de un SOC



Nota: En la ilustración se menciona a manera de resumen los principales aspectos a considerar al momento de plantear la generación de un Centro de Operaciones en Ciberseguridad.

Casos de uso mediante herramientas libres:

El control de acceso a la red es un tema que viene tomando relevancia con la proliferación de los dispositivos móviles y la necesidad del acceso a la información, cada vez más usuarios hacen uso de sus propios dispositivos en entornos laborales, tanto por temas contractuales como por aspectos de preferencia misma, tendencias como el BYOD (Sigla de *Bring Your Own Device*, trae tu propio dispositivo) preocupan a los administradores de infraestructura de IT, más aun en ambientes académicos como lo son las Universidades donde es común que estudiantes y personal docente se conecten a la red con equipos que no cumplen los mínimos estándares de seguridad; es por esto que en la Universidad del Valle se dieron a la tarea de generar un entorno de pruebas controladas donde principalmente implementaron control de acceso mediante protocolo 802.1X, el cual gestiona la autenticación, autorización y audita las conexiones al interior de sus sedes; como fruto de esta actividad, publicaron un artículo que si bien no es reciente, sigue siendo importante para corroborar que las herramientas de acceso libre son una

fuente importante de soluciones para entornos como el propuesto en este proyecto. (Arana, Villa, & Polanco, 2013)

En línea con lo anterior, (Kumar, 2015) afirma que mediante soluciones NAC, “las empresas pueden cerrar brechas de seguridad y fortalecer sus posturas con inteligencia de amenazas en tiempo real y aumentar su capacidad para remediar automáticamente cualquier amenaza potencial que se descubra” adicional a esto, lo más relevante de su artículo es que pronosticó en su época que los servidores compartirían datos contextuales con firewalls y otros componentes de seguridad para permitir la aplicación de políticas a un nivel de detalle superior, tal como se espera realizar con la presente propuesta de proyecto aplicado, dado que los delincuentes informáticos hoy por hoy son más persistentes lo que genera la necesidad de crear integraciones sinérgicas entre diferentes soluciones o herramientas de seguridad.

NIST Cybersecurity Framework (CSF)

Dado un aumento sostenido de la cantidad de incidentes de ciberseguridad en los Estados Unidos, el presidente Barack Obama, el 12 de febrero de 2013, emite la orden ejecutiva 13636 en donde se encarga al Instituto Nacional de Estándares y Tecnologías (NIST, por sus siglas en inglés) el desarrollo del Marco de ciberseguridad para la protección de infraestructuras críticas, lo que hoy se conoce como el Cybersecurity Framework (CSF). Dicho marco tomó como estrategia el basarse en estándares de la industria ya aceptados por el ecosistema de ciberseguridad (NIST SP 800-53 Rev.4, ISO/IEC 27001:2013, COBIT 5, CIS CSC, entre otros) y fue adaptado a la necesidad particular de cada infraestructura critica de dicha nación. A continuación, se detallan sus seis funciones, todas relacionadas entre sí:

Figura 2

Framework de ciberseguridad del NIST

Nota: Tomado de https://www.nist.gov/news-events/news/2023/08/nist-drafts-major-update-its-widely-used-cybersecurity-framework

Identificar: En esta función, una empresa debe conocer los riesgos actuales relacionados con ciberseguridad, así como la identificación de los activos clasificándolo por criticidad y proveedores, que representen un riesgo de ciberseguridad para la organización, con el fin de que esta pueda generar estrategias relacionadas con la gestión de riesgos y pueda cumplir las necesidades relacionadas con la gobernanza.

Proteger: En esta función, una empresa debe proteger los activos una vez priorizados los riesgos y los activos, con el fin de reducir el impacto de los eventos relacionados con ciberseguridad, así como reducir la probabilidad de ocurrencia de estos. En esta función se incluye la gestión de identidades (usuarios), métodos de autenticación, el control de acceso y la formación en ciberseguridad, las plataformas e infraestructura de TI, así como la formación de

los miembros de la organización con el fin de que puedan tomar conciencia en el ámbito de la ciberseguridad.

Detectar: En esta función se deben analizar y detectar los posibles ciberataques y compromisos, con el fin de descubrir anomalías de manera oportuna, IOC y otros eventos de seguridad que permitan identificar un ataque o incidente de seguridad. Esta función ayuda a mejorar actividades relacionadas con la respuesta a incidentes y actividades de recuperación.

Responder: Consiste en adoptar medidas en un incidente de seguridad que se ha detectado mediante actividades de contención que incluyen el análisis, mitigación, notificación y el reporte del incidente.

Recuperar: En esta función se realiza la restauración de los activos y de las operaciones que pudieron verse afectadas por un incidente. La restauración de esta debe realizarse de manera inmediata con el fin de reducir el impacto relacionado con el incidente de seguridad y realizar una comunicación pertinente durante la actividad de recuperación.

Gobernar: En su más reciente actualización, el *framework* incluyó la relacionado al gobierno de la seguridad, con esto, buscó fortalecer la estrategia y políticas generales que toda organización debe incluir para una adecuada gestión de riesgos.

Por otro lado, el marco NIST CSF 2.0 se alinea con la norma ISO 27001 dado que permite mejorar la postura de seguridad de una organización mediante la gestión de sus riesgos.

Cyber Kill Chain

Adaptado del ámbito militar hacia los modelos de ciberseguridad, *Cyber Kill Chain* es un marco de referencia que describe las etapas que normalmente sigue un atacante al momento de

intentar penetrar en un sistema informático, es importante resaltar que este marco fue desarrollado inicialmente por Lockheed Martin con la firme intención de ayudar a comprender el actuar de un ciberdelincuente con la intención de poder detener ataques desde sus primeras etapas, es por esto que el modelo describe una totalidad de siete etapas que permiten visualizar el alcance y accionar en diferentes momentos del ataque.

Marco teórico

Fundamentos de la Ciberseguridad en Entornos Universitarios

Hoy en día las Instituciones de Educación Superior enfrentan múltiples desafíos tanto en lo académico como en lo presupuestal, no es un secreto que cada vez son menos los aspirantes que llegan a un proceso de matrícula debido a la reducción de la natalidad que hoy es tendencia, por ende, los presupuestos son cada vez menores en este tipo de entidades; así las cosas, los entornos tecnológicos se vuelven complejos y en algunos casos descentralizados lo que propicia desafíos únicos en materia de ciberseguridad. El acceso distribuido, el uso de dispositivos personales (BYOD), y la amplia cantidad de usuarios con diferentes niveles de privilegio hacen que las universidades sean blancos atractivos para ciberataques.

Según (ISO/IEC, 2022), la gestión de la seguridad de la información debe considerar factores organizativos, técnicos y humanos, lo que obliga a las universidades a adoptar soluciones integrales que combinen prevención, detección y respuesta a incidentes.

No obstante, para instituciones de educación superior con limitaciones presupuestales y estructuras de seguridad en proceso de maduración, la adopción directa de arquitecturas XDR o SOAR puede representar una barrera técnica y financiera. En este sentido, la integración

estratégica de soluciones SIEM y NAC constituye una base estructural que puede evolucionar progresivamente hacia modelos de automatización avanzada y detección extendida.

NAC: Control de acceso y arquitectura

Tomando en consideración lo indicado en el artículo *Network Access Control: An Overview of Its Technologies and Approaches. ACM Computing Surveys* de los autores (Boubakr , Hakima, Rasheed , Spyridon, & Hassine, 2021) un NAC es una solución de seguridad que regula el acceso a los recursos de una red en función de políticas predefinidas, las cuales verifican la identidad y el cumplimiento de los requisitos de seguridad por parte de los dispositivos antes de permitir su acceso. NAC permite no solo gestionar quién y qué puede acceder a la red, sino también asegurar que los dispositivos estén actualizados y cumplan con las políticas de seguridad, minimizando así riesgos de vulnerabilidad.

El NAC es una solución que permite controlar quién accede a la red, desde qué dispositivo y con qué condiciones, aplicando políticas de seguridad que pueden bloquear, aislar o limitar el acceso dependiendo del nivel de cumplimiento del usuario o dispositivo.

Según (Parker & Bullock, 2017), “las soluciones NAC permiten a las organizaciones visibilizar y segmentar el acceso a sus redes, con base en criterios de autenticación, evaluación de seguridad y cumplimiento de políticas internas” Lo anterior en términos de aplicación en universidades puede aprovecharse por ejemplo en las redes Wi-Fi abiertas donde el NAC puede obligar a los usuarios a autenticarse con credenciales institucionales, verificar si el dispositivo está actualizado y limitar el acceso solo a internet sin permitir navegación por servidores internos. Adicional, dentro de las funciones destacadas que se pueden aprovechar está el control de acceso basado en roles (RBAC), el aislamiento de dispositivos comprometidos y el cumplimiento de políticas de seguridad (antivirus, parches).

SIEM: Concepto, funciones y aplicaciones

La tecnología SIEM nace de la necesidad de centralizar el análisis de incidentes de seguridad y eventos normales de la operación de una red de datos o infraestructura de cómputo, esto como aporte en la mejora de la visibilidad de eventos informáticos en una organización; en otras palabras, es la herramienta que permite recibir logs de diferentes equipos y analizar el accionar de cada dispositivo en una red de datos o sistema de información. Ahora bien, es una herramienta esencial para la gobernanza de TI, ya que ayuda a las organizaciones a cumplir con regulaciones y normativas de seguridad (como ISO/IEC 27001 o el RGPD) mediante la generación de informes y alertas automáticas basadas en políticas predefinidas.

Dicho en otras palabras, el SIEM (*Security Information and Event Management*) es una tecnología que permite recopilar, analizar, correlacionar y visualizar datos de eventos de seguridad generados por infraestructuras tecnológicas. Su finalidad es identificar amenazas, responder a incidentes y asegurar el cumplimiento de normativas, a través de una visión centralizada de la actividad en la red.

Según (IBM, 2023), "La gestión de eventos e información de seguridad (SIEM) es una solución de seguridad que ayuda a las organizaciones a reconocer y abordar posibles amenazas y vulnerabilidades de seguridad antes de que tengan la oportunidad de interrumpir las operaciones comerciales". Ahora bien, en términos de aplicación de este tipo de tecnologías a los ambientes universitarios, a manera de ejemplo, un SIEM puede ser utilizado para monitorear accesos no autorizados a los servidores académicos, detectar intentos de fuerza bruta sobre el sistema de matrículas, o identificar movimientos laterales dentro de la red que puedan indicar una intrusión avanzada.

Evolución del SIEM hacia arquitecturas SOAR y XDR

Tal como lo afirma (Pino Medina, 2021) hoy en día los equipos de ciberseguridad en las organizaciones son reducidos y los eventos a analizar y responder son cada vez mayores, dado esto, es prudente destacar que las soluciones SIEM en algún punto se pueden quedar cortas y demandan un contexto o enfoque diferente; bajo este escenario es prudente hablar de tecnologías como SOAR (Security Orchestration, Automation and Response) y XDR (Extended Detection and Response).

En primer lugar, las plataformas SOAR amplían las capacidades del SIEM mediante la automatización de flujos de respuesta ante incidentes, permitiendo ejecutar playbooks, que pueden interpretarse como manuales de operación automatizada ante situaciones particulares, con lo cual se reduce el tiempo medio de respuesta (MTTR) y disminuye la carga operativa del equipo SOC al evitar intervención manual de este. Según (Gartner, 2022), las soluciones SOAR permiten transformar procesos manuales en respuestas orquestadas, integrando múltiples herramientas de seguridad en un ecosistema automatizado.

Por su parte, el enfoque XDR propone una visión unificada de detección y respuesta que integra telemetría proveniente de endpoints, red, correo electrónico, nube y aplicaciones en general, superando las limitaciones de visibilidad parcial del SIEM tradicional (Palo Alto Networks, 2018). De acuerdo con Forrester (2023), XDR busca consolidar múltiples capas de seguridad en un modelo de análisis correlacionado de extremo a extremo.

Arquitectura Zero Trust

La arquitectura de confianza cero (Zero Trust) asume que ninguna entidad, ya sea interna o externa, debe ser automáticamente aceptada en la red de datos institucional, por lo que se

requiere verificar continuamente la identidad y el estado de los dispositivos. (National Institute of Standards and Technology - NIST, 2020)

Trayendo la anterior definición, el modelo ZTA se puede aplicar en la academia para restringir el acceso a información académica sensible solo a dispositivos y usuarios verificados, incluso si ya están dentro de la red.

Gestión de incidentes

En este punto es clave resaltar tal como lo afirman (Zhang, Ma, Wang, & Zhang, 2021) que una respuesta eficaz a incidentes requiere no solo herramientas tecnológicas (como SIEM o EDR), sino también procesos claros de identificación, contención, remediación y aprendizaje post-incidente: dichos autores destacan la importancia de implementar políticas de gestión de identidades robustas para proteger los recursos y datos sensibles en instituciones educativas, por ejemplo, dejan ver la necesidad de establecer protocolos para cuando un ransomware afecte plataformas académicas como los LMS o las bases de datos estudiantiles.

Gestión de identidades y accesos

En línea con lo anterior, IAM se refiere a los procesos que garantizan que solo las personas autorizadas accedan a recursos específicos, con privilegios adecuados. Es un complemento esencial a las herramientas NAC. Su aplicación en entornos universitarios se enfoca en la gestión y administración de accesos a sistemas de matrícula, laboratorios virtuales, o información privilegiada como puede ser el registro de notas, mediante autenticación multifactor (MFA) y roles basados en perfil académico.

Ciberresiliencia

Entendida como una capacidad crítica y evolutiva que permite a las organizaciones anticipar, resistir, adaptarse y recuperarse de eventos adversos en entornos digitales altamente complejos. Según (Araujo, Machado, & Passos, 2024), esta resiliencia va más allá de la prevención; se fundamenta en una gestión continua que incorpora la preparación, monitoreo, absorción de impactos, respuesta adaptativa, recuperación y aprendizaje. Esta perspectiva holística es vital para las instituciones que dependen de la tecnología para garantizar la continuidad operativa, como las universidades, donde un solo incidente puede paralizar procesos académicos, administrativos y afectar gravemente la reputación institucional.

El estudio también destaca que la planificación proactiva y el aprendizaje post-incidente son pilares esenciales para el fortalecimiento de la resiliencia, ya que permiten evolucionar y robustecer las defensas a partir de experiencias pasadas. En este sentido, la resiliencia no se limita a la contención de ataques, sino que es parte del ciclo de mejora continua en ciberseguridad. Esto cobra especial relevancia en entornos universitarios, donde la alta diversidad de dispositivos, usuarios y sistemas interconectados exige estructuras organizativas capaces de adaptarse y responder de forma dinámica ante amenazas crecientes como el *ransomware*, el acceso no autorizado o la filtración de datos personales.

Marco legal

A manera de contexto se describe a continuación marcos de trabajo o normatividad de amplia aceptación internacional, que, si bien no son de obligatorio seguimiento en la regulación nacional, si resultan altamente pertinente para los entornos universitarios en los cuales se enmarca la ejecución del presente proyecto:

Marco europeo: Reglamento General de Protección de Datos (GDPR)

El Reglamento General de Protección de Datos (GDPR), vigente en la Unión Europea desde 2018, constituye uno de los marcos normativos más avanzados en materia de privacidad y protección de datos personales. Si bien su aplicación directa se circunscribe a los Estados miembros de la UE, su influencia ha trascendido fronteras dado que puede ser aplicada en organizaciones que procesan datos personales de ciudadanos europeos, es por esto que sirve como referencia internacional para organizaciones y gobiernos. Su enfoque se basa en los principios de licitud, lealtad, transparencia, limitación de finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad, así como en el principio de responsabilidad demostrada. (Entrust Corporation, 2025)

En el contexto de las universidades colombianas, la adopción contextualizada del GDPR permite fortalecer las políticas internas de tratamiento de datos personales, especialmente respecto a la información de estudiantes, docentes, empleados y egresados, que suele incluir datos sensibles como rendimiento académico, historial médico o información socioeconómica. Al comparar el GDPR con la Ley 1581 de 2012 y el Decreto 1377 de 2013, se evidencia una compatibilidad conceptual, pero también una diferencia de madurez regulatoria: mientras la ley colombiana se centra en principios generales, el GDPR detalla obligaciones específicas en torno a evaluaciones de impacto, notificación de incidentes de seguridad, y la designación de delegados de protección de datos (DPO).

Por ello, integrar el GDPR como referencia estratégica no implica adoptar una regulación extranjera, sino incorporar buenas prácticas internacionales que complementan y perfeccionan el cumplimiento nacional. En la práctica, una universidad colombiana puede inspirarse en este modelo para diseñar protocolos de consentimiento informado digital, políticas de retención y

anonimización de datos académicos, y mecanismos de transparencia y trazabilidad en sistemas de información. De esta manera, el GDPR se convierte en un marco orientador que fortalece la gobernanza de datos y la confianza institucional en el entorno educativo.

Norma internacional ISO/IEC 27001:2022

En términos de seguridad de la información resulta casi imposible no hacer mención a esta norma, de hecho, es el estándar internacional más reconocido para la gestión de la seguridad de la información, aplicable a cualquier tipo de organización, incluidas las instituciones de educación superior que son el foco de este proyecto. Su más reciente actualización introdujo un enfoque más flexible, basado en riesgos, liderazgo y la mejora continua, que, aunque ya se manejaba en versiones previas, permite alineación con los principios de gobernanza digital contemporánea.

En el ámbito universitario colombiano, la aplicación de ISO/IEC 27001:2022 ofrece un marco claro para estructurar un Sistema de Gestión de Seguridad de la Información (SGSI) dentro del gobierno institucional (ISO/IEC, 2022). Las universidades manejan ecosistemas tecnológicos compuestos por plataformas académicas, sistemas administrativos, servicios en la nube, redes Wi-Fi, datos de investigación, entre otros, lo que las hace especialmente vulnerables a filtraciones, accesos no autorizados o interrupciones operativas. La implementación de la norma permite identificar activos críticos, establecer controles técnicos y administrativos y promover una cultura de seguridad institucional, coherente con la Política de Seguridad Digital del Estado colombiano (CONPES 3995, 2020)

Además, ISO 27001 facilita la integración con otros sistemas de gestión (calidad, ambiental, continuidad de negocio), contribuyendo a una visión transversal de la seguridad. En la práctica, una universidad podría certificar áreas específicas, como el centro de datos, la oficina

de tecnología o la plataforma institucional de aprendizaje virtual (LMS), para garantizar la confidencialidad, integridad y disponibilidad de la información. Así, este estándar se convierte en una herramienta fundamental para alinear la operación universitaria con estándares globales, generar confianza ante aliados internacionales y cumplir con exigencias crecientes de acreditación y responsabilidad digital.

Marco estadounidense: NIST Cybersecurity Framework 2.0 (CSF)

Si bien ya previamente se ha hecho mención a este marco, es necesario resaltar en este apartado su importancia para la gestión integral de riesgos de ciberseguridad, especialmente desde su más reciente actualización en el año 2024 donde incorporaron de forma explícita el concepto de gobernanza de la ciberseguridad como función central, junto con las funciones ya clásicas de identificación, protección, detección, respuesta y recuperación.

Este nuevo enfoque reconoce que la ciberseguridad no es únicamente un problema técnico, sino una responsabilidad estratégica y organizacional, donde la "Alta Dirección" debe asumir un rol activo en la gestión de riesgos y en la toma de decisiones informadas sobre inversiones en seguridad. (NIST, 2024)

En el contexto universitario colombiano, el NIST CSF 2.0 resulta especialmente aplicable debido a su enfoque modular y adaptable, lo cual permite a las instituciones ajustar su madurez digital según su capacidad y nivel de riesgo. Las universidades, al operar múltiples sistemas (académicos, financieros, administrativos, de investigación y redes de invitados), enfrentan amenazas que van desde ataques de ransomware hasta filtraciones de datos o suplantación de identidad. Mediante la aplicación progresiva del marco, es posible estructurar políticas y procesos en torno a cada función:

- **Identificar**: Inventario de activos tecnológicos, clasificación de información y evaluación de riesgos en plataformas académicas y de investigación.
- **Proteger**: Definición de controles de acceso, segmentación de red, cifrado de información y capacitación de usuarios.
- **Detectar**: Implementación de sistemas de monitoreo, correlación de eventos (SIEM) y alertas tempranas ante comportamientos anómalos.
- **Responder**: Protocolos de manejo de incidentes, roles de respuesta y comunicación ante brechas de seguridad.
- **Recuperar**: Planes de continuidad académica, restauración de servicios y lecciones aprendidas.
- **Gobierno**: Integración del riesgo digital en la planeación institucional, auditorías internas y cumplimiento normativo.

Para las universidades colombianas, adoptar este marco implica una oportunidad de alinear la gestión de la ciberseguridad con estándares internacionales, fortalecer su resiliencia digital y desarrollar capacidades de detección y respuesta proactiva frente a incidentes. Asimismo, su estructura permite mapear controles y procesos con la Política Nacional de Seguridad Digital (CONPES 3995, 2020) y con las exigencias de la Superintendencia de Industria y Comercio (SIC) en materia de protección de datos personales.

Reglamentación Nacional

En Colombia, la **Ley 1581 de 2012** y el **Decreto 1377 de 2013** establecen los principios y procedimientos para la protección de datos personales, mientras que la **Ley 1712 de 2014** (Ley de Transparencia y del Derecho de Acceso a la Información Pública) y el CONPES 3995 (Ya

mencionado previamente) sobre Confianza y Seguridad Digital definen las obligaciones institucionales en materia de gestión de información y ciberseguridad.

Estos instrumentos nacionales comparten fundamentos conceptuales con los marcos globales. Por ejemplo, el principio de “responsabilidad demostrada” (accountability) del GDPR encuentra correspondencia en las exigencias de la Ley 1581 sobre responsabilidad del responsable y encargado del tratamiento. Del mismo modo, el enfoque de gestión del riesgo y mejora continua de ISO/IEC 27001:2022 refuerza los lineamientos del CONPES 3995 para la adopción de sistemas integrales de seguridad digital en el sector educativo. Por su parte, el NIST CSF 2.0, con su nueva función de Govern, se alinea con la tendencia estatal hacia la gobernanza tecnológica y la madurez institucional en la administración de riesgos cibernéticos, promoviendo estructuras de liderazgo, métricas y auditoría que las universidades pueden adoptar sin contravenir el marco local.

En la práctica, la articulación de estos referentes permite que las universidades colombianas eleven su nivel de cumplimiento, madurez y confianza digital. Adoptar elementos del GDPR mejora la protección de los datos de estudiantes, docentes y egresados; aplicar ISO 27001 optimiza la gestión técnica y documental de la seguridad de la información; y seguir el NIST CSF fortalece la capacidad operativa de detección y respuesta ante incidentes. Todo ello contribuye directamente al cumplimiento de la normativa nacional y a la consolidación de un entorno académico seguro, resiliente y éticamente comprometido con la privacidad y la transparencia.

De esta manera, la educación superior en Colombia puede proyectarse como un sector que integra estándares globales para consolidar su competitividad y legitimidad institucional,

fomentando una cultura de ciberseguridad alineada tanto con la regulación local como con las mejores prácticas internacionales.

Diseño metodológico

Para dar desarrollo al presente proyecto se plantea interacción directa con el personal del área de Tecnología de una Institución Universitaria con Acreditación de Alta Calidad y de carácter regional, mediante encuentros presenciales y análisis de fuentes primarias que permitan evidenciar el nivel de madurez en ciberseguridad de la institución, para esto, se hará uso de instrumentos como cuestionarios y entrevistas debidamente acordadas entre las partes, análisis de datos estadísticos sobre cantidad de usuarios y equipos activos en la red, así como también identificación de los principales Sistemas de Información requeridos para la adecuada prestación del servicio educativo y el normal funcionamiento de la entidad. Tomando en consideración lo anterior, la intención es llevar a cabo una investigación de tipo aplicada, donde el enfoque permita evaluar variables tanto cualitativas (patrones de uso o desafíos actuales) como cuantitativas (rendimiento y seguridad de la infraestructura actual), mediante las cuales se pueda analizar la pertinencia o efectividad de implementar herramientas libres en la gestión de ciberseguridad en los entornos académicos.

En términos técnicos, se plantea la adopción del *framework* de ciberseguridad del NIST, el cual permitirá aumentar el nivel de gestión de los riesgos informáticos a partir del seguimiento de sus diferentes etapas, todo de manera controlada y documentada.

Análisis de Vulnerabilidades y Riesgos en Infraestructuras Tecnológicas Universitarias: Fundamentos para la Implementación de Soluciones SIEM y NAC

Las instituciones de educación superior en Colombia, como cualquier otra organización (sin importar el tipo), se ven abocadas a la necesidad de hacer uso de plataformas tecnológicas para su correcto funcionamiento, ahora bien, es sabido que en la era digital, la información es quizás el activo más preciado para las altas gerencias, es por esto que resulta especialmente importante examinar desde el presente capitulo los riesgos y vulnerabilidades más relevantes en las infraestructuras tecnológicas particularmente del sector de la educación superior en Colombia, esto con el fin de establecer un marco de referencia para una posible posterior implementación de herramientas SIEM *(Security Information and Event Management)* y NAC *(Network Access Control)*.

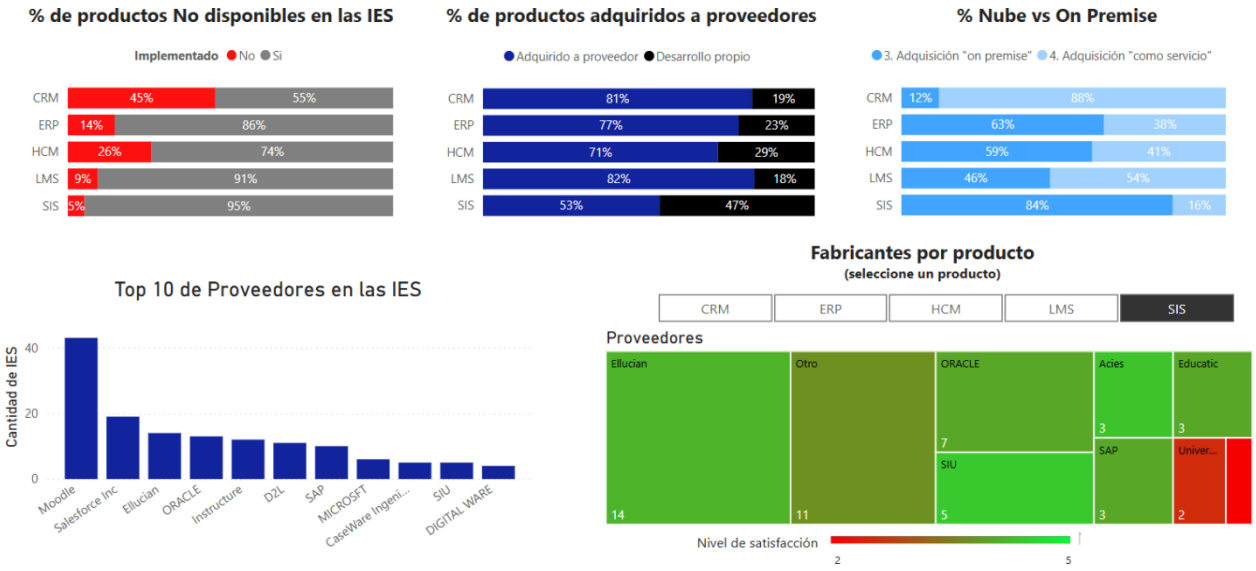
Contextualización de las Infraestructuras Tecnológicas Universitarias:

Las Universidades requieren hoy por hoy para su operación diferentes sistemas e infraestructuras tecnológicas que van desde las típicas redes cableadas e inalámbricas, hasta servidores y bases de datos de propósito específico, sin embargo, en términos de Sistemas de Información o Plataformas, es común encontrar en este tipo de organizaciones mínimamente un ERP (*Enterprise Resource Planning* - Sistema de Planificación de Recursos Empresariales), un SIS (*Student Information System* - Sistema de Información Estudiantil) y un LMS (*Learning Management System* - Sistema de Gestión de Aprendizaje), obviamente, dependiendo del nivel de madurez digital de cada institución se podrá contar con mayor o menor cantidad de plataformas. A manera de contexto, se aprecia en la figura 3 parte del informe colaborativo generado por el grupo MetaRed TIC sobre los productos comúnmente utilizados por este tipo de instituciones, catalogados como críticos para su normal funcionamiento y de los cuales vale la

pena precisar que, al interactuar con diferentes niveles de usuario, amplían la superficie de ataque y demandan políticas de autenticación y segmentación que garanticen el acceso seguro:

Figura 3

Productos de Tecnología Informática críticos en las Universidades Iberoamericanas



Nota: Se observa extracto del reporte colaborativo del Grupo de Trabajo Internacional de relación con proveedores con el compendio de herramientas o plataformas normalmente utilizadas en instituciones de educación superior en Iberoamérica. (MetaRed TIC, 2024)

Es importante poner en consideración que los anteriores sistemas requieren de flexibilidad en su parametrización, debido a los diferentes roles necesarios para la operación institucional: Estudiantes, Docentes y Administrativos; lo que, en últimas, puede ampliar la superficie de ataque.

Principales Amenazas y Vulnerabilidades:

Entre las amenazas más comunes que se encuentran en las Instituciones de Educación Superior, se pueden destacar las siguientes:

- **Ransomware**, como en el caso de la Universidad Nacional de Colombia (SEMANA, 2023).
- **Filtración de datos sensibles**, como lo ocurrido en el ataque a la Universidad de La Salle. (SEMANA, 2023)
- **Secuestro de información,** caso denunciado por la Universidad Piloto de Colombia quienes emitieron un comunicado oficial advirtiendo a su comunidad académica dicha eventualidad (MuchoHacker, 2023), así mismo, la Pontificia Universidad Javeriana se vio afectada en dos de sus sedes a nivel nacional donde incluso los atacantes llegaron al punto de exigir el pago de una recompensa. (El Colombiano, 2021).
- **Suplantación de identidad y secuestro de cuentas institucionales**, como ocurrió con la Universidad El Bosque. (El Espectador, 2021)
- **Vulnerabilidades en aplicaciones web y plataformas** no actualizadas.

Los anteriores casos evidencian un patrón recurrente en el ecosistema académico colombiano: la falta de planes de contingencia formales y de monitoreo continuo, así como el escaso entrenamiento del personal en ciberseguridad. En consecuencia, se justifica la necesidad de soluciones que integren visibilidad, control de acceso y respuesta ante incidentes.

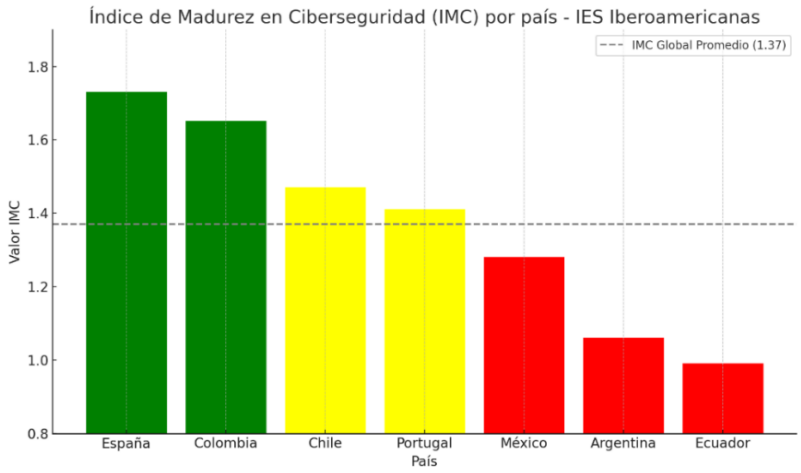
Ahora bien, pese a lo anterior hay que mencionar que Colombia está avanzando hacia una madurez estructural en términos de ciberseguridad, pero con desafíos críticos en cuanto a presupuesto, talento y procesos formales se refiere, esto de acuerdo a lo expuesto en el Índice de

Madurez de Ciberseguridad de Instituciones de Educación Superior iberoamericanas o IMC de IES, donde se destaca que existen fortalezas como país en cuanto a infraestructura, comunicaciones, gestión de accesos y análisis de intrusiones, así como también, falencias en lo que tiene que ver con planes de recuperación debidamente formalizados, presupuestos exclusivos para ciberseguridad y formalización normativa aún en desarrollo, vale la pena mencionar que lo anterior es basado en un índice de madurez que analiza aspectos como el gobierno de la seguridad, la protección de infraestructuras, la capacidad de detección, recuperación ante incidentes y la gestión de identidades. (MetaRed TIC, 2024)

La siguiente figura ilustra claramente el nivel de madurez en ciberseguridad de las Instituciones de Educación Superior por país, destacando a Colombia como líder junto a España según lo concluido en el Índice de Madurez:

Figura 4

Comparación del IMC por país

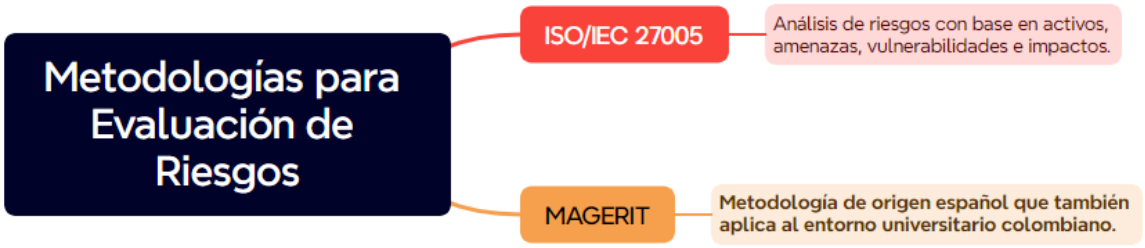


Nota: Se aprecia en la gráfica los niveles de madurez por país, donde el color verde representa un nivel catalogado como intermedio o L2, mientras el amarillo da cuenta de un nivel cercano al promedio o L1 alto, y el color rojo, bajo nivel de madurez (L0 o L1)

Evaluación de Riesgos en el Escenarios Universitarios:

Figura 5

Metodologías para evaluar riesgos



Nota: En la ilustración se presenta a manera de resumen, los aspectos más relevantes de la ejecución de esta metodología.

Inicialmente es prudente mencionar que un adecuado análisis de riesgos debe considerar la mayor cantidad de aristas posibles, sin embargo, como mínimo se debería incluir la medición del impacto en términos de reputación hacia los posibles estudiantes; el impacto operativo, el cual se asocia con la capacidad de resistir ante interrupciones de servicios y, finalmente el impacto de tipo legal por si existe alguna normatividad que las instituciones deban cumplir por su naturaleza.

Marco de Referencia para la Implementación de SIEM y NAC:

A partir de lo anterior y en el marco del alcance del primer objetivo específico de este proyecto, se sugiere a manera de estrategia o apoyo ante un proceso de implementación tomar en consideración los siguientes aspectos antes de pensar concretamente en qué tipo de herramientas de ciberseguridad utilizar, importante destacar que como cualquier herramienta o sistema a

implementar, las instituciones de educación superior deben adelantar ciertos procesos internos previos, en los cuales se centrará este apartado:

Gestión del cambio y cultura organizacional: Este punto no es exclusivo de proyectos de tecnología, pero es crucial si se espera que un proceso llegue a feliz término dado cuando un usuario no está en sintonía con las dinámicas y proyecciones institucionales, serán obstáculos que dificultarán la correcta ejecución generando retrasos en los cronogramas definidos.

Para mitigar este punto se sugieren campañas de sensibilización a nivel de talleres o capacitaciones para toda la comunidad universitaria, así mismo, ya centrados en la temática de ciberseguridad generar actividades que permitan afianzar o adquirir conocimientos específicos sobre acceso seguro a las infraestructuras institucionales.

Gobierno de TI: Es necesario sentar las bases u organizar el área de tecnologías de la información en el marco de la pertinencia institucional para dar soporte a los posibles lineamientos en materia tecnológica, para esto, se sugiere especialmente lo siguiente:

Formar un Comité de Seguridad de la Información, con participación del área de Gestión de Tecnología, Rectoría, la academia, el apoyo jurídico y administrativa.

Designar responsables para roles como: Administrador de SIEM, Administrador de NAC, responsable de tratamiento de incidentes.

Políticas institucionales de seguridad de la información: Partiendo de lo dicho en el punto anterior, es fundamental la generación de lineamientos o políticas que permitan soportar las medidas de protección de cara a los usuarios, para esto es necesario contar mínimamente con lo siguiente:

Crear o actualizar una Política Institucional de Seguridad Informática, que contemple el monitoreo, control de accesos, tratamiento de incidentes y manejo de datos sensibles.

Establecer normativas de acceso a la red para personal, estudiantes, contratistas e invitados.

Preparación de Infraestructuras requeridas: Desde lo técnico, es fundamental contar con un adecuado y actualizado inventario o mapeo de activos, esto es un requisito pensando en la necesidad de implantar soluciones de tipo NAC, es por esto que la entidad debe estar en la capacidad de identificar y documentar todos los dispositivos conectados a la red, incluyendo *switches*, *routers*, servidores, *endpoints*, dispositivos BYOD con el fin de poder facilitar el proceso de generación de perfiles. Ahora bien, en cuanto a condiciones mínimas para desplegar las soluciones se deberá garantizar espacio para alojar el sistema ya sea en máquinas físicas o virtuales con gran capacidad de almacenamiento, especialmente para logs del SIEM; conectores o agentes de integración con sistemas prioritarios como los Firewalls, los *switch core*, las consolas de gestión a nivel de seguridad *endpoint* y servicios críticos como Directorio Activo o herramientas de Gestión de Identidad. Por otro lado, pensando concretamente en soluciones del tipo NAC, se debe garantizar los siguientes puntos:

- Infraestructura de red administrada *(switches, APs)* que soporte 802.1X y RADIUS.
- Base de datos de usuarios autenticados (LDAP/AD).
- Segmentación de red preparada para aplicar políticas dinámicas de acceso (por VLAN, por rol, por ubicación física).

Ciclo de vida del acceso a la red: Dado que desafortunadamente no siempre se cuenta con documentación de procesos, es necesario definir y establecer el ciclo de vida del proceso de acceso a las redes corporativas; para esto es clave tomar en consideración la necesidad de

automatizar el proceso de *onboarding* y *offboarding* de dispositivos y como ya se ha mencionado, Aplicar políticas según tipo de usuario: Estudiante (acceso limitado y monitoreado), Personal administrativo (acceso medio) y Directivos / IT (acceso privilegiado con controles adicionales).

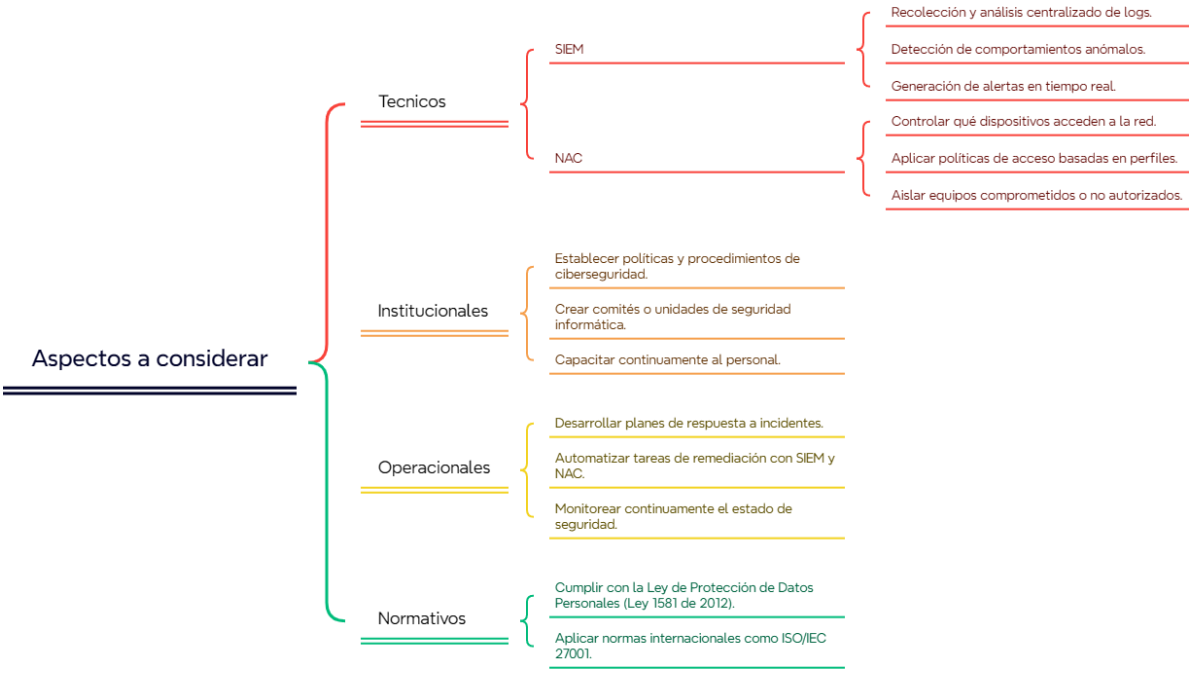
Monitoreo y respuesta a incidentes: Definir procedimientos de detección, análisis, escalamiento y respuesta ante incidentes; con esto, ante una situación real se podrá tener claridad sobre los pasos a seguir para su gestión y contención. En línea con esto último, sería importante también diseñar ejercicios simulados de ciberataques o brechas que permitan entrenar al equipo para adquirir las destrezas necesarias y saber cómo proceder ante este tipo de situaciones.

Normatividad y regulación: Es importante que desde las áreas de Gestión Humana y especialmente desde las de apoyo jurídico se puedan establecer cláusulas de confidencialidad en los contratos de cada colaborador dado el manejo de información institucional, así mismo, aplicaría también para proveedores o terceros que intervengan en procesos internos; por otro lado, se deben establecer o gestionar la periodicidad en la contratación de auditorías externas especializadas en ciberseguridad.

Finalmente, a manera de conclusión de lo expuesto hasta el momento, se resalta que implementar este tipo de herramientas en el contexto universitario colombiano no solo requiere infraestructura tecnológica, sino un ecosistema de procesos internos sólidos, que incluyan políticas claras, gobernanza estructurada, cultura institucional en seguridad, y mecanismos de respuesta bien definidos. A continuación, en la figura número 6 se resaltan los aspectos considerados necesarios para iniciar de manera acertada un proceso de implementación de este tipo de soluciones:

Figura 6

Puntos claves o Marco Referencial



Nota: En la ilustración se presenta a manera de resumen los puntos clave que se deben considerar previo al proceso de implementar herramientas de tipo NAC y SIEM.

Taxonomía y Viabilidad de Implementación de Herramientas SIEM y NAC en Instituciones de Educación Superior

En la actualidad, las instituciones de educación superior (IES) enfrentan crecientes desafíos en materia de ciberseguridad, derivados de la masificación del acceso a la red, la proliferación de dispositivos personales (BYOD), y la creciente dependencia de infraestructuras digitales críticas como sus sistemas académicos, financieros, de recursos humanos o de gestión del aprendizaje en línea. La necesidad de adoptar tecnologías que permitan una gestión integral de la seguridad en estos entornos ha llevado a explorar soluciones que combinen visibilidad, control y capacidad de respuesta en tiempo real, siendo las herramientas SIEM y NAC las más relevantes.

El presente capítulo tiene como propósito desarrollar una taxonomía técnica comparativa de herramientas SIEM y NAC orientadas a instituciones de educación superior, considerando criterios de arquitectura, modelo de despliegue, capacidades de integración, escalabilidad, soporte comunitario/comercial y viabilidad presupuestal.

A partir de dicha clasificación se seleccionaron dos soluciones de código abierto —Wazuh como SIEM y PacketFence como NAC— para su instalación, configuración y validación en un entorno controlado, con el fin de evaluar su aplicabilidad real en un contexto universitario. La selección se fundamentó en criterios de madurez del proyecto, documentación técnica disponible, comunidad activa y alineación con los requerimientos identificados en el diagnóstico institucional.

De acuerdo con el informe sobre el panorama mundial de amenazas de Fortinet, el 70% de los incidentes en la nube en el sector educativo ocurren debido a accesos indebidos desde ubicaciones geográficas inusuales y configuraciones erróneas de seguridad (FORTINET, 2025). Ante esta realidad, el uso combinado de herramientas SIEM y NAC se propone como una

estrategia que no solo permita monitorear la red, sino también restringir y gestionar dinámicamente los accesos con base en políticas de cumplimiento.

Asimismo, el IMC de MetaRed evidencia que las universidades que han logrado establecer equipos de ciberseguridad medianamente estructurados (entre 3 y 5 personas) alcanzan índices de madurez superiores (IMC > 1,60), en contraste con aquellas que carecen de soluciones tecnológicas básicas de protección (MetaRed TIC, 2024). Esto refuerza la necesidad de contar con herramientas viables técnica y financieramente que acompañen el desarrollo de capacidades institucionales.

En este contexto, se presenta a continuación una ficha técnica comparativa de herramientas SIEM y NAC, con énfasis en aquellas que puedan ser adoptadas por universidades en proceso de fortalecimiento digital aun con limitaciones presupuestales, aportando así a la toma de decisiones estratégicas sobre su infraestructura de ciberseguridad.

Herramientas SIEM

Wazuh

Antes de describir la herramienta como tal, es importante ampliar su contexto y mencionar que gracias a la misma un administrador de sistemas puede responder de manera proactiva a diferentes vectores de riesgo al instante, por ejemplo, es posible detectar configuraciones inseguras sobre un equipo gracias a su módulo de Evaluación de configuración de seguridad (SCA) o identificar versiones de software desactualizadas o con problemas ya conocidos gracias al módulo de gestión de vulnerabilidades, asimismo, el módulo de inventario de activos mejora la visibilidad de los puntos potenciales de ataque, permitiendo que el personal técnico tome

decisiones basadas en evidencia centralizada; por otro lado, su capacidad de detección de intrusiones basada en reglas y comportamiento así como la integración con fuentes externas de logs permiten dar respuesta en diferentes ámbitos lo cual fortalece la postura de seguridad institucional al reducir activamente la superficie de ataque y mejorar el tiempo de reacción ante eventos, lo que justifica la elección de dicha herramienta en el marco del desarrollo de este proyecto.

En cuanto a su arquitectura, Wazuh es una plataforma de seguridad open source distribuida que integra un servidor central, agentes instalados en los equipos a monitorear y un motor de indexación soportado sobre Elastic Stack. Su modelo híbrido permite combinar monitoreo basado en agentes con análisis centralizado de logs, facilitando la correlación de eventos en tiempo real; por otro lado, su propio fabricante destaca que *"Wazuh se ha consolidado como una de las soluciones SIEM más robustas de código abierto gracias a su integración con Elastic Stack y sus capacidades de detección de amenazas en tiempo real."* (Wazuh, 2024)

Proceso de Instalación.

Los siguientes pasos están orientados a partir de lo sugerido en el propio sitio web de la herramienta[1]:

Descarga y extracción de la última versión del producto:

```
curl -sO https://packages.wazuh.com/4.13/wazuh-install.sh
```

[1] Instalación de Wazuh Manager: https://documentation.wazuh.com/current/deployment-options/wazuh-from-sources/wazuh-server/index.html

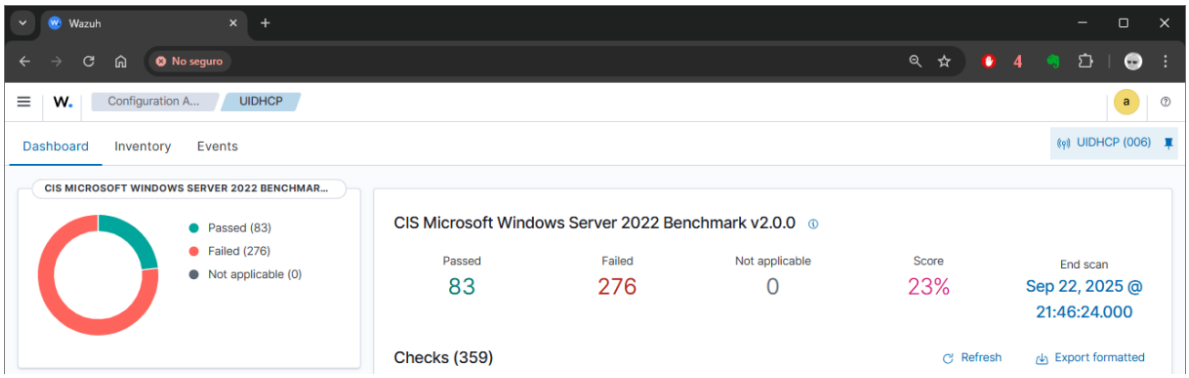
Instalación mediante el asistente de configuración:

```
sudo bash ./wazuh-install.sh -a
```

Luego de un tiempo que puede variar según las capacidades del servidor o máquina virtual, el proceso estará terminado y se generarán credenciales de acceso vía web para el usuario "*admin*"

Figura 7

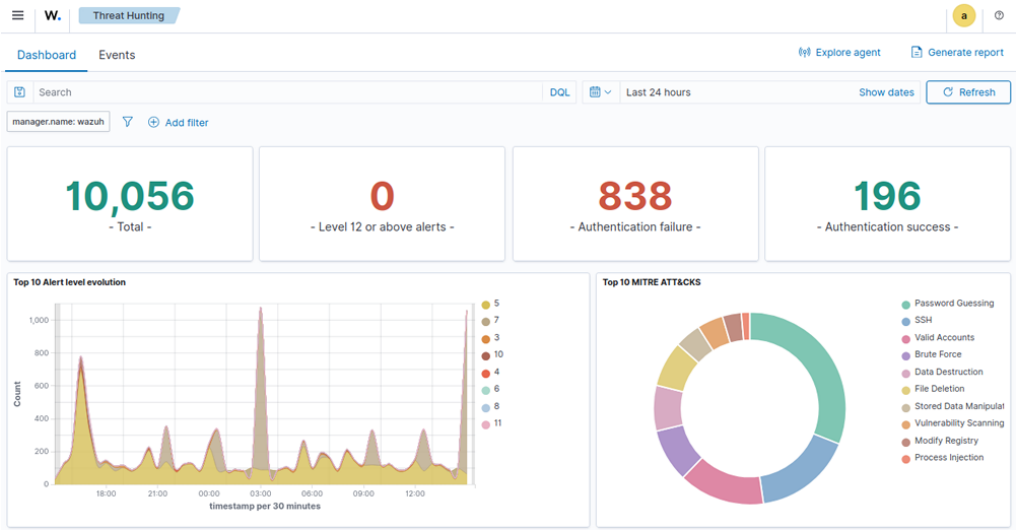
Módulo Evaluación de configuración de seguridad en ejecución



Nota: La figura presenta el módulo Security Configuration Assessment (SCA) de Wazuh, el cual evalúa automáticamente el nivel de cumplimiento de un equipo monitoreado frente a estándares de configuración segura previamente definidos (por ejemplo, CIS Benchmarks).

Figura 8

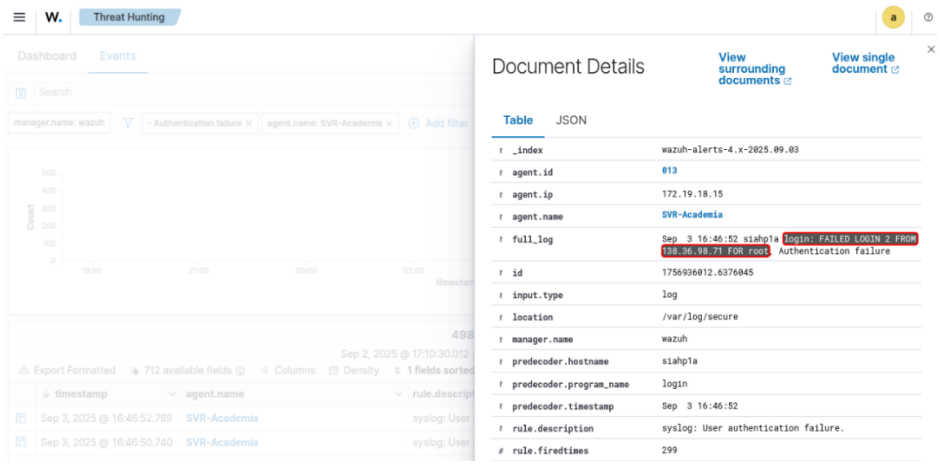
Identificación de ataque de diccionario



Nota: Se aprecia en la captura que gracias al monitoreo activo y especialmente al módulo Threat Hunting de la herramienta, se logró evidenciar y detener un ataque de diccionario mediante el cual pretendían acceder vía SSH a uno de los equipos administrados en la institución.

Figura 9

Detalles del atacante descubierto



Nota: Se resalta en la captura la dirección IP del atacante la cual gracias a la herramienta pudo ser identificada de manera temprana; luego de esto, a nivel perimetral se bloqueó todo tráfico proveniente de esa dirección hacia la red y recursos institucionales.

Los resultados obtenidos durante la fase de validación evidenciaron la capacidad de la herramienta para detectar intentos de acceso no autorizado mediante ataques de fuerza bruta SSH, generando alertas en tiempo real y permitiendo la aplicación de controles perimetrales correctivos.

Cabe mencionar que el tiempo promedio de detección para el caso expuesto fue inferior a 10 minutos, lo cual demuestra la pertinencia de su implementación como mecanismo de monitoreo continuo en entornos universitarios.

Herramientas NAC

PacketFence

Solución NAC (*Network Access Control*) de código abierto, diseñada para ofrecer control de acceso a la red basado en políticas, segmentación, autenticación, aislamiento y detección de comportamiento anómalo. Desarrollada por la empresa canadiense Inverse Inc., está orientada especialmente a entornos académicos, hoteleros y corporativos con redes LAN y WiFi mixtas; en cuanto a su arquitectura es de tipo modular y se caracteriza por combinar autenticación 802.1X, portal cautivo, integración con servicios de directorio (LDAP/AD) y mecanismos de aislamiento dinámico de dispositivos. Su diseño permite aplicar políticas de control de acceso basadas en identidad, rol o cumplimiento de requisitos de seguridad del endpoint.

Proceso de Instalación.

Es importante mencionar que el proceso de instalación está muy bien documentado en la página oficial del producto, sin embargo, se resalta lo evidenciado desde la propia experiencia donde se sufrieron ciertos problemas de compatibilidad con distribuciones Linux de la familia Debian, en un primer momento se optó por hacer uso de Linux Ubuntu aun cuando en la página se expresa literalmente que los sistemas soportados oficialmente son Red Hat Enterprise Linux (RHEL) 8 y Debian 11; lo anterior conociendo que Ubuntu es una distribución derivada de Debian por lo que comparten el mismo manejador de paquetes y kernel, sin embargo, al seguir los pasos descritos en la sección 4.3.3 del instructivo (Inverse inc, 2025),[2] se observó que ciertas dependencias requeridas por PacketFence para su funcionamiento no se logran instalar; dado esto la interfaz gráfica nunca se logró implementar; así las cosas, fue necesario desplegar una nueva máquina virtual donde se instaló Debian y desde esta se realizaron los siguientes pasos:

Adición del repositorio:

```
    apt-get update
    apt install gnupg sudo curl
    curl -fsSL https://inverse.ca/downloads/GPG_PUBLIC_KEY | gpg --dearmor -
o /etc/apt/keyrings/packetfence.gpg
```

Definición de la url asociada al repositorio de descargas PacketFence:

```
    echo "deb [signed-by=/etc/apt/keyrings/packetfence.gpg]
http://inverse.ca/downloads/PacketFence/debian/14.1 bookworm bookworm" > \
    /etc/apt/sources.list.d/packetfence.list
```

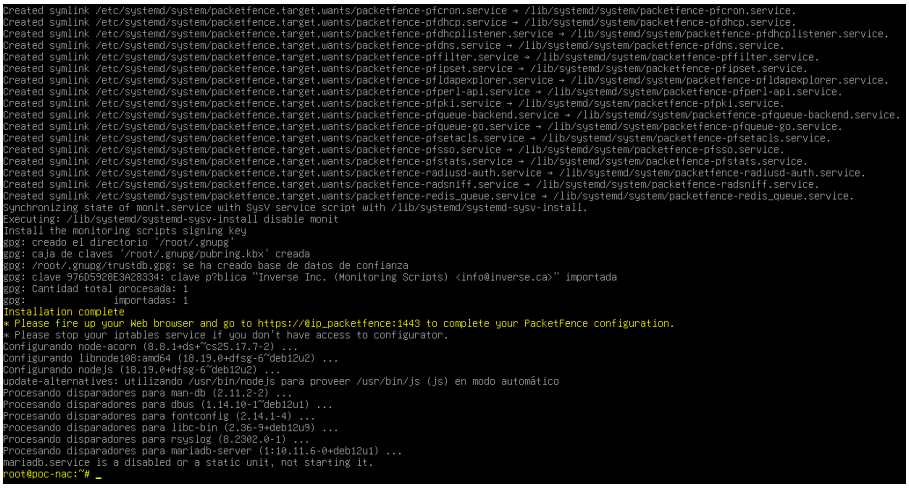
Instalación de paquetes asociados:

```
    apt-get update
    apt-get install packetfence
```

[2] 4.3.3. Software Installation disponible en: https://www.packetfence.org/doc/PacketFence_Installation_Guide.html#_debian_based_systems

Figura 10

Finalización del proceso de instalación

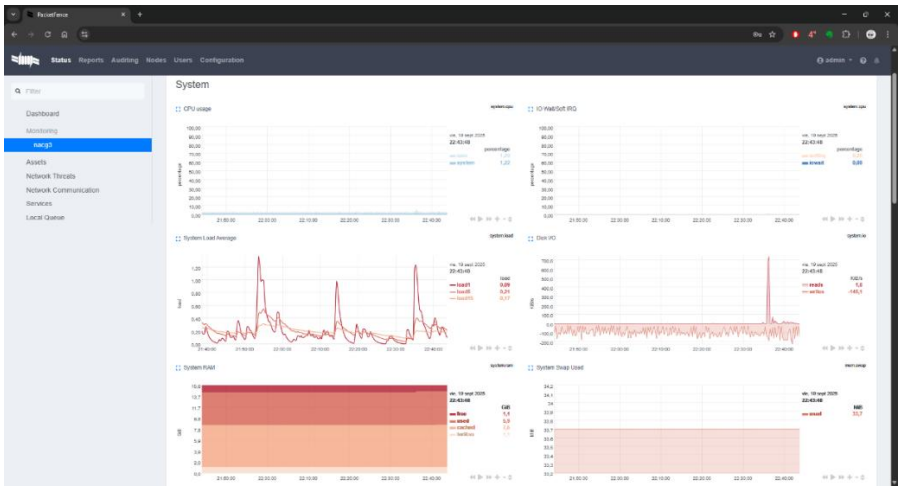


Nota: Se observa en la captura de pantalla la confirmación generada desde la terminal de Linux, de la finalización del proceso.

Luego de terminado el proceso de instalación, se ingresa vía navegador web a la dirección IP asignada a la máquina virtual y se empieza la parametrización final del NAC:

Figura 11

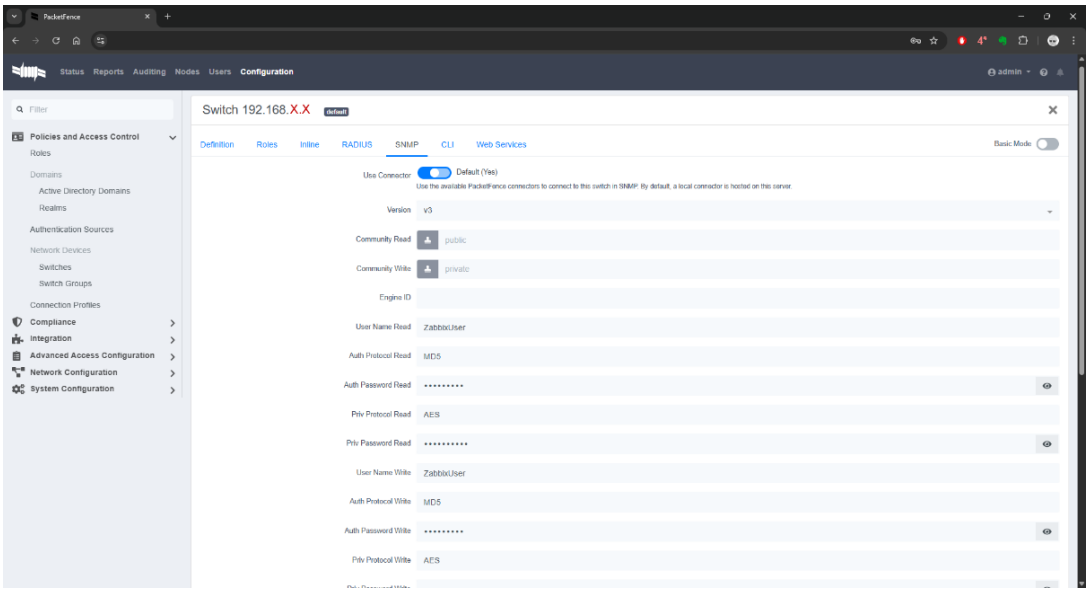
Interfaz web PacketFence



Nota: Se evidencia en la figura el panel de administración del NAC ya implementado, especialmente se observa el módulo de monitoreo donde se ilustra el consumo a nivel de hardware sobre la máquina virtual desplegada.

Figura 12

Inclusión de un switch administrado



Nota: En la sección de Administración se muestra el módulo de registro de dispositivos de red, específicamente la incorporación de switches gestionables para el control de acceso a nivel de puertos físicos.

Es importante precisar que para que un switch pueda integrarse con una solución NAC como PacketFence, es indispensable que cumpla con ciertos requerimientos técnicos, entre ellos:

- Soporte para el estándar IEEE 802.1X (autenticación basada en puerto).
- Compatibilidad con VLAN dinámicas para segmentación de red.

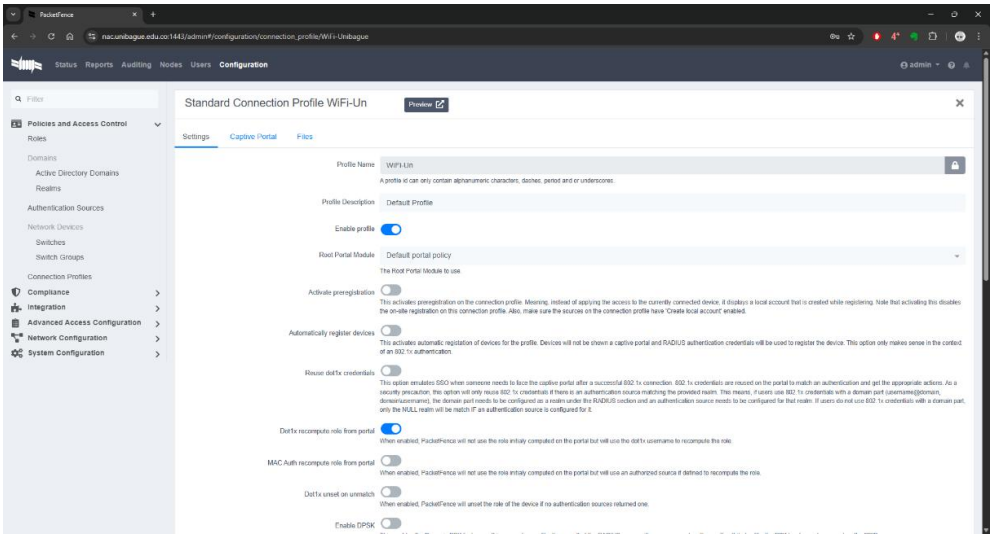
- Capacidad de autenticación RADIUS.
- Gestión remota mediante protocolos como SSH, SNMP o API propietaria.

En el caso particular del despliegue realizado, se registró un switch Aruba 2930F, equipo de capa 3 administrable que soporta 802.1X, autenticación RADIUS y asignación dinámica de VLAN, lo que permite su integración directa con PacketFence para aplicar políticas de control de acceso basadas en identidad.

Es importante resaltar también que switches no administrables o que no soporten 802.1X no pueden integrarse adecuadamente con soluciones NAC, ya que carecen de mecanismos para aplicar políticas de autenticación y segmentación por puerto.

Figura 13

Creación de perfil de conexión



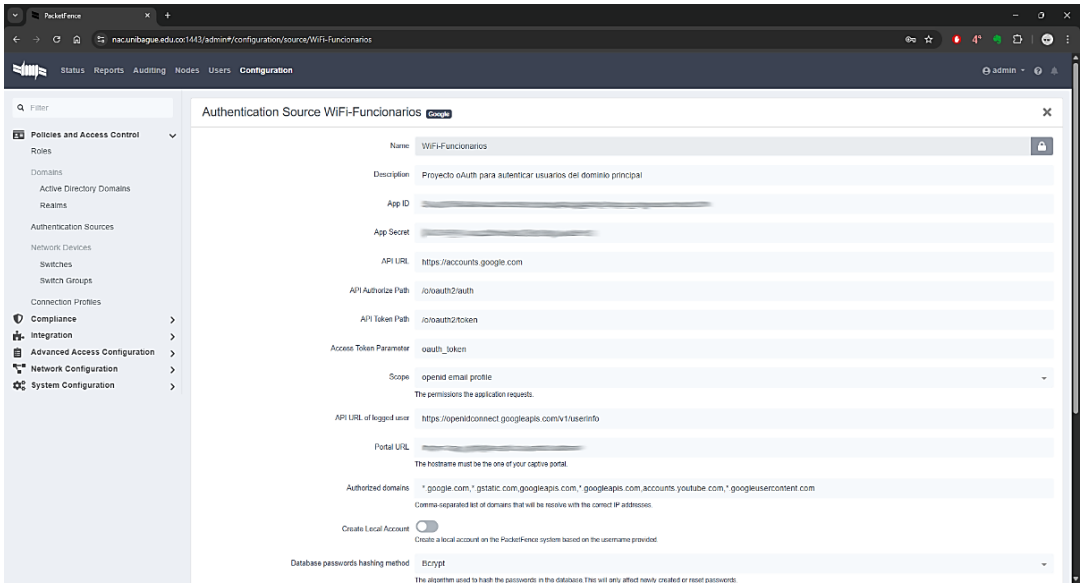
Nota: En la captura se presentan los parámetros de configuración de un perfil de conexión, el cual en PacketFence corresponde a un conjunto de políticas que determinan el método de autenticación, el tipo de acceso permitido y las reglas de segmentación aplicables a un dispositivo o usuario al intentar conectarse a la red.

Un perfil en PacketFence define aspectos como el uso de portal cautivo, autenticación 802.1X, validación mediante servidor RADIUS o autenticación federada (por ejemplo, OAuth con Google Workspace), dichos perfiles se aplican dinámicamente cuando un dispositivo intenta acceder a la red WiFi y es redirigido al flujo de autenticación correspondiente. Una vez el usuario completa el proceso de validación, PacketFence evalúa las políticas asociadas al perfil y asigna la VLAN o nivel de acceso definido, permitiendo así segmentación lógica basada en identidad.

Este mecanismo constituye un componente esencial del modelo NAC, ya que permite aplicar control de acceso contextual en función del tipo de usuario, rol institucional o cumplimiento de políticas de seguridad.

Figura 14

Autenticación vía oAuth 2.0

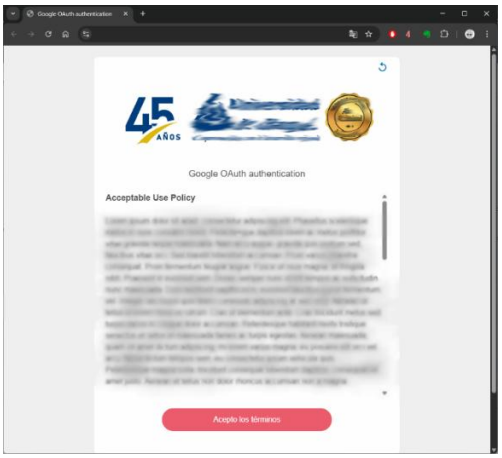


Nota: La figura muestra la integración del NAC con un proveedor de identidad externo mediante el estándar OAuth 2.0, específicamente Google Workspace institucional.

Vale la pena destacar que la opción anterior permite autenticación federada, evitando así el almacenamiento local de credenciales y reduciendo riesgos asociados a la gestión descentralizada de usuarios, lo que fortalece el nivel de seguridad al centralizar la identidad de los usuarios en un proveedor confiable como lo es Google en este caso.

Figura 15

Portal cautivo con validación vía Google



Nota: La captura evidencia la personalización del portal de autenticación de usuarios mediante cuentas de correo de la institución (Google WorkSpace), paso previo al inicio de sesión en las redes WiFi de la institución.

Casos de Uso. Estadísticas de uso en universidades.

Según el mismo sitio web del fabricante, PacketFence funciona muy bien con más de 8000 dispositivos registrados en una infraestructura de más de 200 switches y casi 400 puntos de acceso inalámbricos en la Universidad del Pacifico en Seattle, asimismo, precisan que *"PacketFence ha sido implementado con éxito en varias universidades canadienses y francesas, proporcionando control de acceso granular y políticas de seguridad adaptables sin costo de licenciamiento."* (Inverse Inc., 2023)

Tabla 1 Comparativo de Herramientas SIEM y NAC

Herramienta	Tipo	Agentes requeridos	Portal cautivo	802.1X	Dashboards	Integraciones	Observaciones	Opciones comerciales
PacketFence	NAC	No	Sí	Sí	Parcial	LDAP, AD, oAuth, escáner de vulnerabilidades	Ideal para entornos mixtos con WiFi y LAN.	Comparable a Cisco ISE o HPE Aruba ClearPass en funciones básicas; menor soporte comercial pero **alta adaptabilidad.**
FreeRADIUS	NAC	No	No	Sí	No	LDAP, AD, oAuth	Ligero y flexible, ideal para autenticación simple.	Parcialmente comparable con FortiNAC y Microsoft NPS, pero sin soporte nativo en la nube
OpenNAC	NAC	Sí	No	Parcial	No	LDAP, AD, oAuth	Requiere agentes; poco mantenido.	Comparado con ForeScout CounterACT, Ha pasado a ser solución de **pago**.
Wazuh	SIEM	Sí	No	No	Sí	Elastic Stack, Kibana	Fuerte en correlación de eventos y análisis de logs.	Alternativa libre a Splunk o QRadar; menor automatización, pero **sin costos de licencia**.
Graylog	SIEM	No	No	No	Sí	SNORT, Suricata, pfSense	Compatible con Docker y contenedores.	Comparable con Splunk, pero **sin costos por volumen de datos** y con escalado horizontal
SIEMonster	SIEM	Opcional	No	No	Sí	IDS, AWS, Azure, PacketFence	Alta escalabilidad, arquitectura modular.	Escalable y modular similar a IBM QRadar; **requiere mayor conocimiento técnico** para mantenimiento.

Nota. Esta tabla muestra los principales datos a destacar de cada herramienta analizada

Discusión comparativa: herramientas de código libre vs opciones comerciales

Las herramientas open source presentadas en la Tabla 1 —entre ellas Wazuh, PacketFence, FreeRADIUS y SIEMonster— representan alternativas viables para instituciones de educación superior con limitaciones presupuestales, pues eliminan el costo de licenciamiento y ofrecen una alta flexibilidad en la personalización; sin embargo, el éxito depende directamente del nivel de madurez organizacional en ciberseguridad de dichas instituciones. Estas soluciones permiten a los equipos técnicos adaptar las configuraciones a sus necesidades específicas y mantener la soberanía tecnológica sobre sus datos.

Sin embargo, al compararlas con herramientas comerciales ampliamente utilizadas en entornos corporativos, como IBM QRadar, Splunk Enterprise, Aruba ClearPass o Cisco Identity Services Engine (ISE), se observan diferencias notables en tres ejes clave:

- **Costo total de propiedad (TCO):** Las soluciones open source reducen los costos iniciales de implementación, pero requieren inversión continua en talento técnico interno para garantizar estabilidad y mantenimiento. Por el contrario, las soluciones comerciales implican licencias y suscripciones costosas, aunque disminuyen la carga operativa gracias al soporte especializado y actualizaciones automáticas.

- **Soporte y escalabilidad:** Las herramientas libres dependen de comunidades activas y foros, lo cual puede generar retrasos en la resolución de incidencias. En cambio, las soluciones comerciales ofrecen soporte 24/7 y opciones de escalamiento vertical y horizontal más sencillas, especialmente en entornos híbridos o en la nube.

- **Integración y facilidad de uso:** Mientras Wazuh o SIEMonster pueden igualar la capacidad de correlación y análisis de eventos de Splunk o QRadar, las plataformas

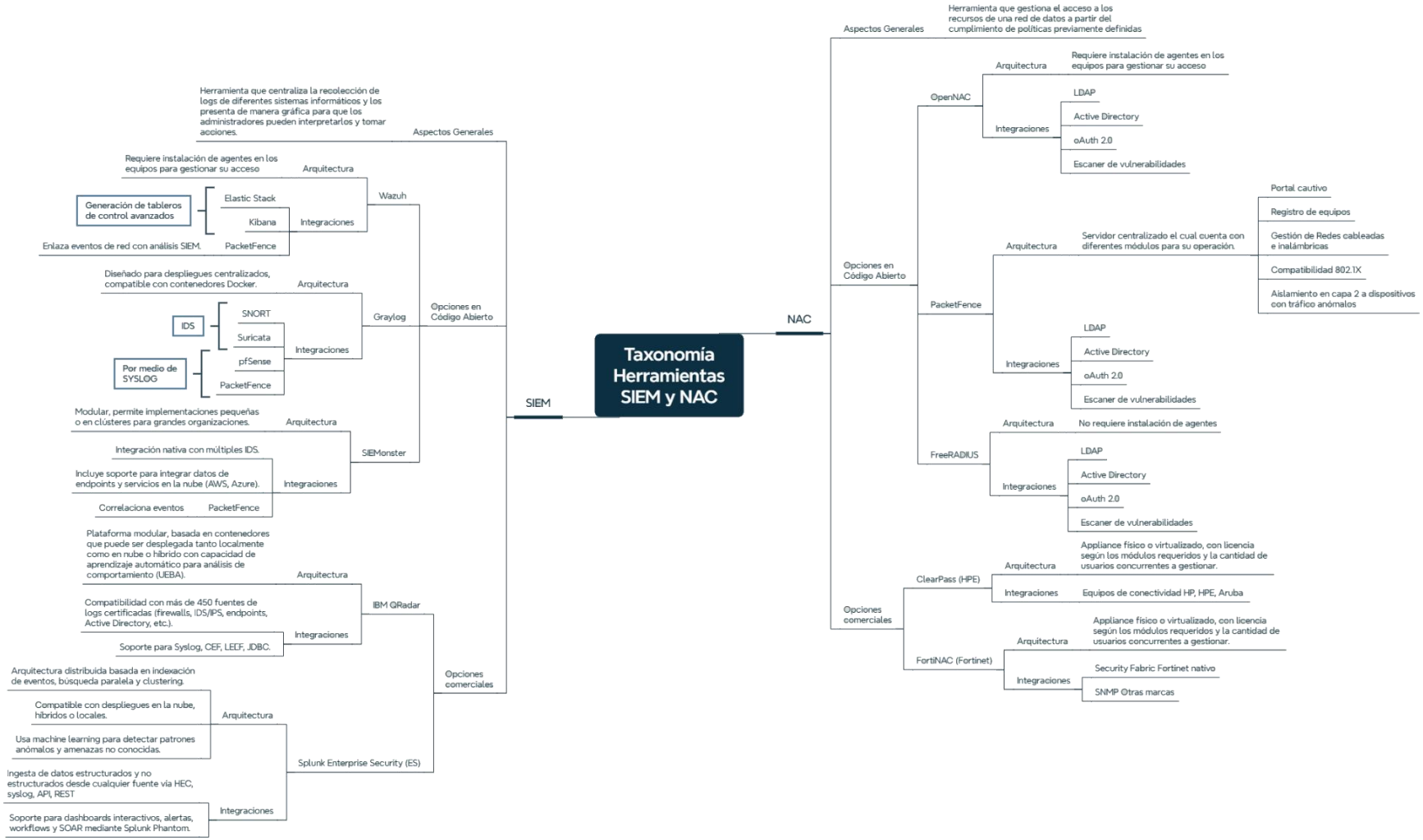
comerciales suelen incluir interfaces más intuitivas y dashboards preconfigurados que reducen los tiempos de aprendizaje.

En síntesis, la elección entre soluciones open source o comerciales debe sustentarse en el nivel de madurez tecnológica de la institución, la disponibilidad de talento especializado y la estrategia de sostenibilidad a largo plazo. Para las universidades con recursos limitados, pero con personal técnico capacitado, la adopción de herramientas libres como Wazuh y PacketFence resulta una opción estratégica, equilibrando costo, autonomía y capacidad de innovación

A partir de lo anterior, a continuación, se presenta en la figura 16 una taxonomía que resume las principales capacidades a manera de comparativa entre las opciones tanto de herramientas de control de acceso como de monitoreo de eventos analizadas hasta este punto en el marco del desarrollo del presente capitulo, en la misma, el lector podrá sacar sus propias conclusiones sobre qué herramienta utilizar para su caso y necesidad particular tomando en consideración las siguientes categorías: Tipo de solución, modelo de despliegue, capacidades de autenticación y control, posibles integraciones externas y el nivel de soporte o madurez del proyecto; lo anterior permitirá identificar posibles similitudes funcionales entre las soluciones libres y las comerciales facilitando la toma de decisiones en los entornos académicos..

Figura 16

Taxonomía de herramientas SIEM y NAC



Plan estratégico para la implementación progresiva de soluciones SIEM y NAC en infraestructuras universitarias

Este capítulo tiene como propósito diseñar un plan de implementación progresiva y eficiente para soluciones de gestión de eventos e información de seguridad (SIEM) y control de acceso a la red (NAC), enfocado en minimizar los impactos sobre la operación académica en universidades. A partir del marco teórico y el análisis de vulnerabilidades realizados en capítulos anteriores, se propone una estrategia de despliegue alineada con los marcos internacionales de ciberseguridad la cual busca asegurar sostenibilidad, escalabilidad y resiliencia institucional frente a posibles incidentes de ciberseguridad.

Consideraciones previas a la implementación

Evaluación de Madurez de Seguridad

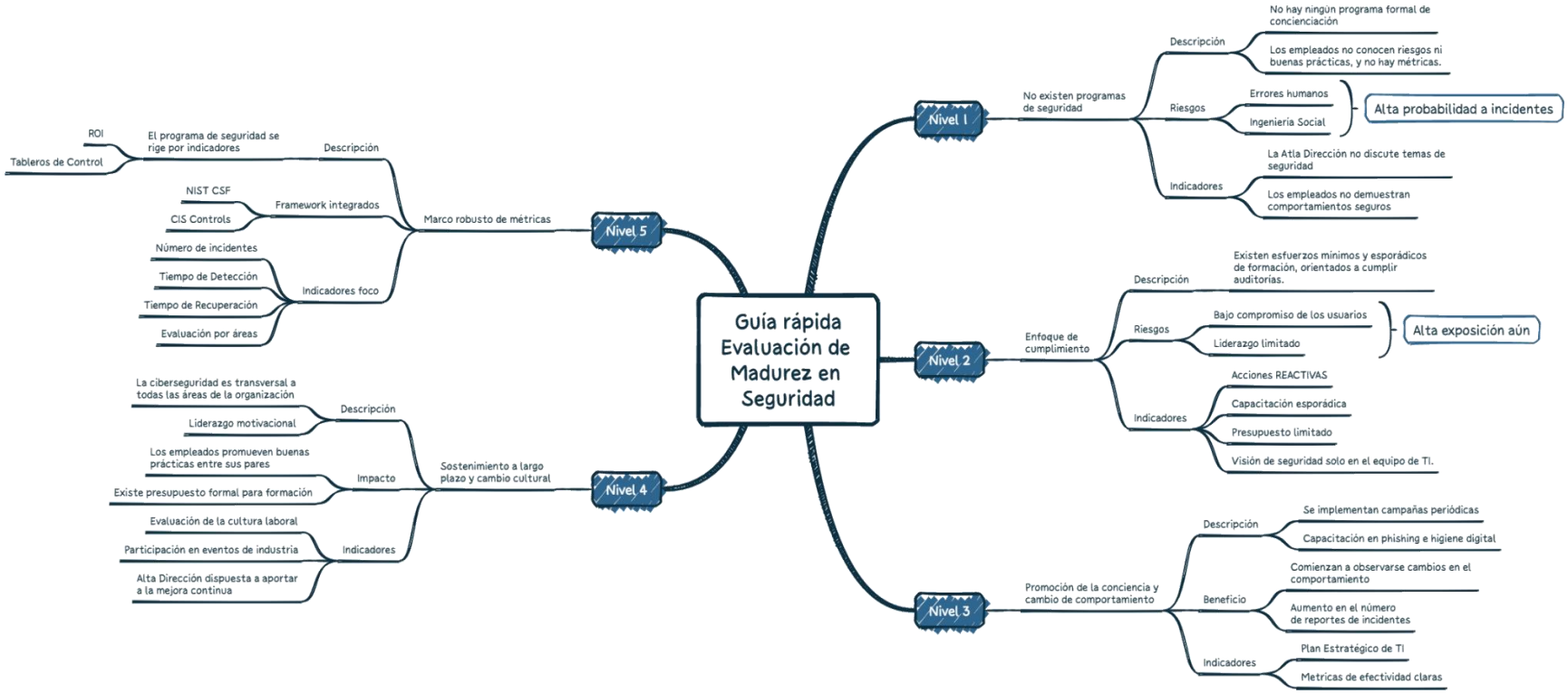
Antes del despliegue de soluciones tecnológicas, es indispensable evaluar el nivel de madurez institucional en ciberseguridad. Se recomienda aplicar marcos como el *Cybersecurity Framework* (*CSF)* del Instituto Nacional de Estándares y Tecnología de los Estados Unidos o el Modelo Integrado de Madurez de Capacidades (CMMI por sus siglas en ingles)[3], los cuales permiten identificar brechas entre la situación actual y el estado deseado. (NIST, 2024)

Ahora bien, para un diagnóstico más puntual y sin entrar en la minucia requerida, se sugiere poner en consideración la siguiente guía que se centra principalmente en el factor humano y sirve para identificar de manera preliminar el nivel de seguridad en el cual se encuentra una institución objeto de estudio, y a partir de esta, iniciar ya un proceso con mayor detalle y rigurosidad:

[3] Disponible en el sitio web oficial del Instituto CMMI: https://cmmiinstitute.com/cmmi

Figura 17

Guía rápida para evaluación del nivel de seguridad existente



Nota: Se observa en la figura indicadores que permitirían determinar el nivel actual de compromiso o madurez en términos de seguridad informática en una organización a partir de lo definido por (SANS Institute, 2023)

Identificación de Actores y Roles

La identificación de actores y roles en el proceso de implementación de soluciones SIEM y NAC no solo responde a la necesidad de clarificar responsabilidades técnicas, sino también al propósito de fortalecer una cultura institucional de ciberseguridad. Cada actor dentro de la organización —desde el personal administrativo y académico hasta los equipos de TI y comités directivos— contribuye de manera directa al nivel de madurez y resiliencia digital de la universidad.

En este sentido, el Comité de Ciberseguridad Institucional debe asumir un rol estratégico que trascienda la gestión de incidentes. Su función debe incluir la formación, sensibilización y comunicación activa a toda la comunidad universitaria. Se recomienda que el comité lidere campañas periódicas de concienciación sobre buenas prácticas digitales, manejo seguro de datos personales, prevención de incidentes y uso responsable de la infraestructura tecnológica. Estas campañas pueden articularse con la Oficina de Comunicaciones y la Dirección de Talento Humano para asegurar un impacto transversal y constante.

Asimismo, se sugiere el desarrollo y aprobación de políticas internas de seguridad de la información —avaladas por el Consejo Directivo— que regulen aspectos como el acceso a la red, la gestión de contraseñas, el uso de dispositivos personales (BYOD) y los procedimientos de respuesta ante incidentes. Estas políticas deben incorporar mecanismos de auditoría, control y actualización periódica, garantizando que la seguridad sea entendida como un valor institucional y no como una responsabilidad exclusiva del área técnica.

Finalmente, se recomienda establecer un programa anual de sensibilización institucional, liderado por el Comité de Ciberseguridad, que incluya capacitaciones técnicas, simulacros de phishing, talleres prácticos y retroalimentación sobre incidentes reales ocurridos en el entorno

universitario. Estas iniciativas fortalecen la cultura de seguridad, fomentan la corresponsabilidad y contribuyen al desarrollo de una ciber-resiliencia universitaria sostenible.

Con la intención de que las decisiones que se tomen en el anterior comité sean de estricto cumplimiento, se debe establecer el mismo mediante resolución oficial y garantizar interdisciplinariedad entre sus miembros, dicha resolución debe ser emitida desde la propia Rectoría de cada institución.

Determinación del Nivel de Riesgo Aceptable

Más allá de la identificación de actores y responsabilidades, la definición del plan estratégico debe considerar explícitamente el apetito al riesgo de la institución educativa. El apetito al riesgo se entiende como el nivel de exposición que una organización está dispuesta a aceptar en el cumplimiento de sus objetivos estratégicos (NTC-ISO 31000, 2018). En el contexto universitario, este concepto resulta determinante para definir el alcance, profundidad y nivel de automatización de las soluciones SIEM y NAC a implementar.

Una institución con bajo apetito al riesgo —por ejemplo, aquellas que gestionan información sensible de investigación, datos financieros críticos o convenios internacionales— se inclinará por priorizar soluciones con mayor automatización, redundancia, alta disponibilidad y posiblemente soporte comercial especializado. Por el contrario, universidades con restricciones presupuestales y un apetito al riesgo moderado podrían optar por arquitecturas open source escalables que, si bien requieren mayor capacidad técnica interna, permiten un crecimiento progresivo acorde con su madurez organizacional; ante esto es prudente recordar que según el Índice de Madurez en Ciberseguridad, 6 de cada 10 IES colombianas utilizan el 10% de su presupuesto tecnológico en temas asociados a ciberseguridad (MetaRed TIC, 2024)

En consecuencia, el Comité de Ciberseguridad debe definir formalmente el nivel de riesgo aceptable antes de seleccionar la arquitectura tecnológica, ya que el apetito al riesgo influye directamente en variables como inversión presupuestal, nivel de automatización (SIEM vs SIEM + SOAR), cobertura de activos y tiempos de respuesta esperados (MTTD y MTTR). Esta definición fortalece la coherencia entre estrategia institucional, gobernanza del riesgo y decisiones técnicas.

Proceso de Despliegue Progresivo

Se presenta a continuación un plan estructura en fases secuenciales que buscan optimizar y garantizar un correcto despliegue de las soluciones propuestas, el mismo va desde etapas de preparación hasta la mejora continua sugerida en las normas ISO

Fase 1: Preparación y Planificación

Objetivo: Determinar el nivel actual de madurez en ciberseguridad y las brechas técnicas y organizacionales, mediante la aplicación de marcos como NIST CSF e ISO 31000, incorporando la definición del nivel de riesgo aceptable institucional, con el fin de orientar el alcance y tipo de soluciones SIEM–NAC a implementar.

Responsables

- Dirección de TI
- Comité de Ciberseguridad
- Auditor interno o externo

Requerimientos técnicos

- Acceso a inventario de activos

- Diagramas de red actualizados
- Políticas vigentes de seguridad

Entregables

- Informe de diagnóstico
- Matriz de brechas
- Línea base de seguridad institucional

Indicadores

- % de activos inventariados
- Nivel de madurez actual (escala 1–5)

Duración estimada: 4 a 6 semanas

Descripción general:

Como es de esperarse, el primer paso es determinar en qué escala o nivel de madurez de seguridad se encuentra la institución y definir los actores, políticas y procedimientos que guiarán todo el posible proceso de implementación a parir de este diagnóstico inicial, para lo cual, se toma en consideración el Framework de ciberseguridad del NIST y especialmente su función de identificación, la cual trae consigo la necesidad de conocer los activos tecnológicos, el entorno institucional y los riesgos asociados; es por esto que, el primer paso que las instituciones deben dar es realizar la evaluación de madurez en ciberseguridad, para esto se pueden apoyar en los modelos CMMI (*Capability Maturity Model Integration*, enfocado en procesos) y (MetaRed TIC, 2024) los cuales permiten medir la capacidad institucional frente a la gestión de riesgos.

Esta primera fase establece las bases estratégicas y organizacionales para la adopción de soluciones SIEM y NAC de manera controlada y bajo procesos enmarcados en la filosofía del mejoramiento continuo, característica propia de la norma ISO 27001. Cabe resaltar, que el resultado esperado de esta fase es una línea base de seguridad institucional que sirva como punto de partida para definir prioridades de inversión y determinar el alcance de las herramientas SIEM y NAC a implementar para robustecer su infraestructura o capacidades actuales.

Asimismo, se debe conformar un Comité de Ciberseguridad integrado por la Dirección de TI, la Vicerrectoría Administrativa, la Oficina Jurídica (Representada en las oficinas de Secretaría General y contratación) y representantes académicos, formalizado mediante resolución rectoral. Este comité garantizará la interdisciplinariedad y el cumplimiento de la Ley 1581 de 2012 sobre protección de datos personales, estableciendo responsabilidades y mecanismos de seguimiento.

Cumplido este primer paso, se sugiere a manera de lista de chequeo validar las siguientes acciones:

- Revisión de políticas institucionales en materia de ciberseguridad, seguridad informática y seguridad de la información
- Evaluación de posibles necesidades de integración con sistemas como
    - Active Directory: Para gestionar identidades, correlacionar eventos por usuario y aplicar políticas por grupo o rol.
    - LDAP: Como base de datos de usuarios, para validar autenticación en NAC o registros en SIEM.
    - Plataformas académicas: Para detectar comportamientos anómalos, accesos no autorizados, o fallos de integridad de cuentas.

- Selección de herramientas (comerciales o de código abierto) compatibles con la infraestructura existente; para esto es importante tomar en consideración la información relacionada previamente en la tabla 1 donde se sugieren herramientas concretas; asimismo, es fundamental poder garantizar que el despliegue de cualquiera de estas soluciones SIEM y NAC sea escalable, interoperable y sostenible dentro del entorno institucional. A manera de recomendación, para universidades en fase inicial o con bajo presupuesto, se sugiere iniciar con Wazuh como herramienta SIEM, por su compatibilidad con múltiples fuentes de datos, comunidad activa y escalabilidad; mientras que, como herramienta NAC, PacketFence es altamente recomendado por su madurez, soporte de múltiples protocolos, y adopción global en universidades (Inverse Inc., 2023)

Es importante precisar que, aunque Wazuh y PacketFence no implican costos de licenciamiento por uso, su implementación no está exenta de costos asociados. La adopción de soluciones de código abierto conlleva requerimientos de implementación asociados a infraestructura (servidores físicos o virtuales en entornos on-premise o en la nube), así como horas de ingeniería dedicadas a instalación, configuración, ajuste de reglas, monitoreo continuo y mantenimiento evolutivo, dicho en otras palabras, demanda una curva de aprendizaje que se debe contemplar y que debe ser medida en horas hombre y tipo de dedicación (parcial o total).

En este sentido, el análisis financiero debe considerar el costo total de propiedad (TCO), incluyendo recursos humanos especializados, actualizaciones de seguridad, gestión de vulnerabilidades y posibles necesidades de soporte externo. En instituciones con equipos técnicos reducidos, estos costos operativos pueden representar un desafío significativo, por lo

que la decisión de adoptar herramientas open source debe alinearse con el nivel de riesgo aceptable y la capacidad interna de sostenibilidad técnica.

Fase 2: Diseño Técnico de la Arquitectura SIEM–NAC

Objetivo: Definir la arquitectura física y lógica necesarias para adecuada implementación de herramientas SIEM y NAC en Instituciones de Educación Superior

Responsables

- Dirección de TI
- Coordinador de Infraestructura y Redes de telecomunicaciones

Requerimientos técnicos

- Servidor SIEM (Máquina virtual):
  - CPU: 8 vCPUS
  - RAM: 8 Gb
  - Disco Duro: 80 Gb

- Servidor NAC (Máquina virtual):
  - CPU: 4 vCPUS
  - RAM: 16 Gb
  - Disco Duro: 200 Gb
- Switchs: Equipos con soporte 802.1X + RADIUS, funcionalidades capa 3; para el caso particular se trabajó con equipos marca Aruba referencia 2930f
- Autenticación de usuarios: LDAP o directorio activo

Entregables

- Documento de arquitectura
- Diagrama de integración
- Plan de implementación técnica

Duración estimada: 3–4 semanas

Descripción general:

Esta fase del plan tiene un propósito muy puntual dado que la idea es definir las capacidades o arquitectura sugerida, para esto se diseña la topología lógica a implementar, se describen los componentes funcionales y las dependencias a nivel de infraestructura. En esta etapa se especifican los servidores requeridos (físicos o virtuales), el dimensionamiento de recursos (CPU, memoria, almacenamiento y capacidad de indexación), la segmentación de red mediante VLAN, los mecanismos de autenticación centralizada (LDAP/Active Directory), y los protocolos de interoperabilidad como Syslog, SNMP, RADIUS y 802.1X. Asimismo, se establecen los flujos de ingesta y correlación de logs, las políticas de retención de eventos, y los criterios de alta disponibilidad y respaldo que aseguren continuidad operativa del ecosistema SIEM–NAC.

Respecto a los productos, los mismos permitirán validar la viabilidad técnica antes del piloto, reducir riesgos de incompatibilidad y garantizar que la solución diseñada sea escalable, segura y alineada con las funciones Detect, Protect y Respond del NIST Cybersecurity Framework.

Fase 3: Piloto Controlado

Objetivo: Validar funcionalidad e integración de las herramientas en un entorno controlado, el cual será priorizado en un área o VLAN específica para medir desempeños y escalar posteriormente.

Responsables

- Coordinador de Infraestructura y Redes de telecomunicaciones
- Personal de soporte técnico
- Usuarios de área objeto de análisis

Actividades

- Instalación de Wazuh.
- Configuración inicial de PacketFence.
- Integración con LDAP/AD.
- Registro de switches administrables.
- Configuración de perfiles de conexión.
- Simulación de incidentes (fuerza bruta, acceso indebido).

Requerimientos técnicos

- Servidor SIEM (Máquina virtual):

Criterios de validación

- Detección exitosa de intentos no autorizados.
- Segmentación efectiva de dispositivos.

- Integración funcional con AD.

Duración estimada: 6–8 semanas

Descripción general:

En esta fase se ejecuta una implementación piloto en un entorno controlado, por ejemplo, un segmento de red o VLAN específico que puede ser el de un laboratorio de clase o una nueva red creada para el propósito particular; en esta fase, lo relevante es validar la compatibilidad de las herramientas seleccionadas, la eficacia de las políticas de seguridad y la capacidad del personal técnico.

Las herramientas recomendadas para el entorno universitario tal como se ha venido mencionado son:

- **Wazuh**, como solución SIEM, por su escalabilidad, compatibilidad con múltiples fuentes de datos y comunidad activa de soporte.
- **PacketFence**, como NAC, por su madurez, soporte para 802.1X y adopción generalizada en instituciones educativas.

Durante el piloto se deben configurar reglas de correlación de eventos, autenticación LDAP/Active Directory, y monitoreo de tráfico.

Además, se recomienda realizar simulaciones de incidentes (por ejemplo, intentos de acceso no autorizado o conexiones anómalas), documentando resultados e impactos.

El éxito de esta fase se medirá mediante indicadores como tasa de falsos positivos, número de alertas críticas detectadas, y disponibilidad del sistema durante las pruebas.

Fase 4: Expansión Progresiva

Objetivo: Extender cobertura de la solución a toda la infraestructura a partir de los resultados y experiencias de la fase anterior, con el ánimo de aumentar el nivel de gestión y aseguramiento de la red de datos institucional.

Responsables

- Dirección de TI
- Coordinador de Infraestructura y Redes de telecomunicaciones
- Personal de soporte técnico
- Usuarios de área objeto de análisis

Actividades

- Instalación de agentes adicionales.
- Integración con demás equipos activos de la red así como también de firewalls.
- Activación de automatización de respuesta.
- Capacitación técnica interna.

Indicadores

- Porcentaje de cobertura en activos monitoreados.
- Porcentaje de switchs integrados al NAC.
- Reducción de incidentes críticos.
- Reducción de incidentes críticos,
- Disminución del tiempo medio de detección (MTTD), y
- Cumplimiento de los controles ISO/IEC 27001:2022.

Duración: 3–6 meses (dependiendo tamaño institucional)

Descripción general:

Con base en los resultados del piloto, la expansión progresiva busca extender la cobertura del SIEM y NAC a todas las dependencias de la institución. Esta fase debe realizarse de manera gradual, iniciando con las áreas menos críticas que permitan estabilizar o mejorar el proceso en cada iteración y luego de esto, avanzar hacia el resto de la infraestructura (por ejemplo, en áreas como financiera, la propia academia y laboratorios de investigación).

Ahora bien, cabe resaltar que esta fase se alinea de manera directa con la función **Detectar** del framework de ciberseguridad del NIST, enfocada en mejorar la visibilidad y correlación de eventos; es por esto que la herramienta Wazuh debe configurarse para integrar logs de diferentes fuentes como servidores, routers, firewalls y aplicaciones institucionales mediante el despliegue de agentes de monitoreo y telemetría. Simultáneamente, PacketFence aplicará políticas de control de acceso basadas en roles, dispositivos y contexto.

De acuerdo con la función **Responder**, se implementarán procedimientos de respuesta automatizada a incidentes, incluyendo:

- Aislamiento de dispositivos comprometidos.
- Notificación a administradores mediante alertas en tiempo real.
- Ejecución de scripts correctivos en casos recurrentes.

Fase 5: Operación, Monitoreo y Mejora Continua

Objetivo: Establecer un modelo operativo permanente para la gestión integrada de las soluciones SIEM y NAC, mediante la implementación de mecanismos formales de monitoreo

continuo, medición de indicadores de desempeño (KPIs), revisión periódica de configuraciones y ejecución de simulacros técnicos, con el fin de garantizar la sostenibilidad, efectividad y mejora continua de la postura de ciberseguridad institucional.

Responsables

- Dirección de TI
- Coordinador de Infraestructura y Redes de telecomunicaciones
- Personal de soporte técnico

Actividades

- Integración con mesa de ayuda.
- Creación de dashboards ejecutivos.
- Revisión trimestral de KPIs.
- Simulacros semestrales de incidentes.
- Actualización de reglas.

KPIs permanentes

- MTTD
- MTTR (Tiempo Medio de Respuesta)
- Disponibilidad del SIEM/NAC
- Porcentaje de cumplimiento ISO 27001
- Número de dispositivos aislados preventivamente

Descripción general:

Esta fase consolida la infraestructura SIEM–NAC como un ecosistema institucional interconectado y autosostenible. Su propósito es garantizar la continuidad operativa y la mejora continua de la ciberseguridad universitaria.

Siguiendo la función **Recuperar** del framework del NIST y la norma ISO 22301, se propone la implementación de estrategias de recuperación ante desastres (DRP) y planes de continuidad (BCP) que se salen del alcance de este proyecto, pero que en términos de una ciberseguridad transversal deben ser construidos por cada institución según sus propias necesidades.

Por otro lado, en esta fase juega un papel determinante el ciclo de Deming o mejora continua PHVA, el cual se puede aplicar de la siguiente manera:

- **Planear**: análisis de incidentes y priorización de mejoras.
- **Hacer**: aplicación de cambios técnicos y organizacionales.
- **Verificar**: evaluación de resultados mediante KPIs.
- **Actuar**: estandarización de buenas prácticas y capacitación del personal.

La fase final debe incluir la automatización de alertas, la integración del SIEM con sistemas de mesa de ayuda y la creación de dashboards ejecutivos para el seguimiento de incidentes y por último y no menos importante, una estrategia de comunicación para informar a usuarios sobre cambios implementados.

Recomendaciones Técnicas y Operativas

- Uso de estándares interoperables: Syslog, SNMP, 802.1X.
- Políticas de control de acceso dinámico.
- Planes de capacitación para personal técnico y sensibilización institucional.
- Estrategia de comunicación para informar a usuarios sobre cambios.

Evaluación de Impacto y Contingencia

- Definición de KPIs: tiempo medio de detección, tasa de remediación, disponibilidad de servicios.
- Ejecución de simulacros de incidentes.
- Plan de reversión en caso de afectación significativa a servicios críticos.

A continuación, se presenta a manera de resumen la estimación de tiempos requeridos para un adecuado desarrollo del proyecto en la tabla 2:

Tabla 2

Cronograma de referencia

Fases	Duración Estimada
Diagnóstico	1 mes
Diseño	1 mes
Piloto	2 meses
Despliegue	3–6 meses
Operación continua	Permanente
Total estimado	**7-10 meses**

Conclusiones del Capítulo

El diseño de un plan de despliegue progresivo para soluciones SIEM y NAC representa un componente clave en la transición hacia infraestructuras universitarias resilientes. Su éxito depende de la articulación entre tecnología, procesos y cultura institucional. La implementación modular permite minimizar impactos y generar aprendizajes iterativos que fortalecen la postura de seguridad de la organización. En conclusión, la implementación de herramientas SIEM y NAC en instituciones universitarias no puede entenderse únicamente como una medida técnica de control o vigilancia, sino como parte integral de una estrategia de ciberresiliencia institucional. Tal como lo plantean (Araujo, Machado, & Passos, 2024), estas soluciones deben ser desplegadas considerando el ciclo completo de resiliencia cibernética, que abarca desde la preparación proactiva, pasando por la detección y respuesta adaptativa, hasta la recuperación y aprendizaje post-incidente.

En este sentido, SIEM y NAC no son tecnologías aisladas, sino componentes articuladores de una cultura de seguridad y mejora continua, que permiten a las universidades no solo defenderse de amenazas actuales, sino también aprender de los incidentes, reducir su impacto futuro y fortalecer sus capacidades operativas. Su integración exitosa demanda planificación estratégica, liderazgo institucional y una visión a largo plazo, en la cual la tecnología se convierte en un facilitador de continuidad académica y protección del ecosistema digital educativo.

Propuesta de Indicadores para la Evaluación del Rendimiento y Seguridad de Herramientas Open Source en la Gestión de Incidentes

Evaluar la efectividad de las herramientas de código abierto implementadas para la gestión de incidentes en infraestructuras universitarias requiere establecer métricas claras, objetivas y alineadas con buenas prácticas internacionales. Esta evaluación no solo permite verificar si las soluciones adoptadas —como Wazuh y PacketFence— cumplen con su propósito técnico, sino que también aporta insumos para mejorar los procesos de detección temprana, gestión y resolución de incidentes. De esta forma, se favorece un enfoque de mejora continua en la ciberseguridad institucional.

Diversos organismos internacionales han propuesto marcos de referencia para el diseño y monitoreo de indicadores clave en ciberseguridad. Por ejemplo, el estándar ISO/IEC 27004:2022 recomienda establecer métricas relacionadas con la eficacia de los controles de seguridad y su alineación con los objetivos organizacionales. Por su parte, la guía NIST SP 800-61r3 (publicada en 2023) enfatiza que la respuesta ante incidentes debe integrarse dentro de la gestión general del riesgo cibernético, siguiendo las funciones del Cybersecurity Framework (CSF) 2.0: Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar. Además, introduce de manera explícita el concepto de mejora continua bajo las funciones de Identificar y Mejorar.

Diseño de indicadores y metodología utilizada

Es importan precisar que la definición de los indicadores propuestos no responde únicamente a experiencias propias o recopilación conceptual de métricas ampliamente utilizadas en ciberseguridad, sino que se fundamenta en un proceso metodológico estructurado compuesto

por cuatro etapas:

Identificación de objetivos de control asociados a la integración SIEM–NAC

- Alineación con marcos de referencia internacionales (NIST CSF 2.0, NIST SP 800-61r3 e ISO/IEC 27004:2022)
- Priorización según impacto operativo y viabilidad de medición
- Validación de cobertura frente al problema de investigación.

En primer lugar, se identificaron los procesos críticos derivados de la implementación de SIEM y NAC: detección temprana, contención de incidentes, recuperación de servicios, cobertura de activos y mejora continua. Posteriormente, estos procesos fueron mapeados contra las funciones del NIST CSF 2.0 (Detección, Respuesta, Recuperación, Identificación y Gobierno), garantizando coherencia con estándares reconocidos internacionalmente.

En este contexto, los indicadores que se proponen reflejan no solo la capacidad de detección y respuesta, sino también la preparación institucional, la recuperación post-incidente y la implementación de aprendizajes derivados.

Clasificación de los indicadores según su naturaleza

Con el fin de responder explícitamente al objetivo específico relacionado con la propuesta de indicadores de rendimiento y seguridad, los indicadores fueron clasificados en dos categorías:

- Indicadores de rendimiento, orientados a medir la eficiencia operativa, tiempos de respuesta, disponibilidad y desempeño del ecosistema SIEM–NAC.

- Indicadores de seguridad, enfocados en evaluar la postura de protección institucional, reducción de superficie de ataque, cumplimiento normativo y fortalecimiento de la resiliencia organizacional.

A continuación, se presenta una tabla con indicadores revisados que permiten evaluar estas dimensiones de manera integral y que buscan apoyar a las instituciones a aumentar su postura de seguridad de manera sustentada

Tabla 3 Indicadores de rendimiento y seguridad

Indicador	Clasificación	Descripción	Relación con NIST SP 800-61r3 / CSF 2.0	Responsable	Fuente de datos	Notas de utilidad
Tiempo promedio de detección (MTTD)	Rendimiento	Intervalo entre el inicio del incidente y su detección efectiva	Detectar	Administrador SIEM	Logs SIEM y NAC	Mide la capacidad de respuesta temprana
Tiempo promedio de contención / respuesta (MTTRc)	Rendimiento	Tiempo desde la detección hasta que se implementa una acción de contención efectiva	Responder	Analista de eventos / Equipo SOC	Logs SIEM, NAC y mesas de ayuda	Indica eficiencia de respuesta operativa
Tiempo de recuperación (RT)	Rendimiento	Tiempo desde la contención del incidente hasta la restauración completa de servicios	Recuperar	Administrador de infraestructura / CISO	Logs SIEM, NAC y mesas de ayuda	Útil para evaluar impacto sobre la continuidad de servicios académicos
Tasa de falsos positivos / alertas erróneas	Rendimiento	Porcentaje de alertas generadas que no representan amenazas reales	Detectar / Identificar y Mejorar.	Analista de eventos	Consola SIEM, reportes de correlación	Refleja la precisión de las reglas del SIEM / NAC
Porcentaje de activos cubiertos / monitoreados	Seguridad	Proporción de endpoints, servidores y dispositivos bajo vigilancia	Identificar / Proteger	Administrador NAC	Consola NAC, inventario de activos institucional	Permite estimar la superficie de ataque controlada
Número de incidentes por categoría / severidad	Seguridad	Conteo de eventos clasificados (malware, acceso no autorizado, etc.)	Detectar / Responder	Administrador SIEM / SOC	Logs SIEM, reportes diarios de incidentes	Apoya análisis de riesgos y priorización de recursos

Indicador	Clasificación	Descripción	Relación con NIST SP 800-61r3 / CSF 2.0	Responsable	Fuente de datos	Notas de utilidad
Alertas críticas resueltas dentro de SLA	Rendimiento	Porcentaje de incidentes críticos atendidos dentro del tiempo pactado	Responder	Coordinador de seguridad / SOC	Sistema de tickets, registros SIEM	Mide cumplimiento de acuerdos de nivel de servicio
Lecciones aprendidas formalizadas / mejoras implementadas	Seguridad	Número o porcentaje de incidentes que resultan en acciones documentadas de mejora	Identificar y Mejorar.	Comité de Ciberseguridad / CISO	Informes posts-incidentes, actas del comité	Clave para procesos de retroalimentación institucional
Disponibilidad del sistema SIEM / NAC	Rendimiento	Proporción del tiempo en que las herramientas están operando sin fallos	Gobernar	Área de infraestructura	Panel de monitoreo (Zabbix u otro)	Afecta la continuidad de la vigilancia y el monitoreo
Nivel de satisfacción del usuario	Rendimiento	Sirve para medir la percepción de utilidad de la herramienta	Responder / Recuperar	Dirección de Tecnología	Formulario interno	Paralelamente se alinea con la fase de análisis post-incidente descrita en el NIST SP 800-61r3
Porcentaje de cumplimiento normativo	Seguridad	Valida alineación con políticas institucionales y normas ISO 27001	Gobernar	Oficial de Seguridad	Auditorías internas	Evalúa madurez y cumplimiento regulatorio

Nota. Los indicadores que se presentan en la tabla se inspiran en las directrices de NIST SP 800-61r3 e ISO/IEC 27004:2022, adaptados al contexto universitario

Los indicadores de desempeño técnico (MTTD, MTTRC, RT y tasa de falsos positivos) permiten medir la eficacia operativa del SOC y la capacidad de respuesta de las herramientas SIEM y NAC frente a incidentes reales.

A su vez, los indicadores de gestión (activos cubiertos, lecciones aprendidas, disponibilidad del sistema) reflejan la madurez institucional en ciberseguridad, vinculándose con las funciones Detectar, Responder y Recuperar del NIST CSF 2.0, y con las actividades post-incidente descritas en el NIST SP 800-61r3.

Esta combinación fortalece la visión integral del rendimiento y permite que la universidad avance hacia un modelo de mejora continúa sustentado en datos verificables.

Criterios de priorización y validación

Los anteriores criterios han sido seleccionados según lo siguiente:

- Relevancia estratégica: Grado en que el indicador impacta la continuidad académica.
- Posibilidad de medición: Disponibilidad de datos verificables desde SIEM, NAC o sistemas de tickets.
- Impacto en reducción de riesgo: Capacidad del indicador para evidenciar disminución de superficie de ataque o tiempo de exposición.
- Alineación normativa: Correspondencia directa con NIST CSF 2.0 o ISO/IEC 27004.
- Aplicabilidad transversal: Posibilidad de ser implementado en universidades de diferentes tamaños.

Por otro lado, si se tiene en cuenta la norma (ISO/IEC 27004, 2022) es prudente mencionar que un proceso de medición permite apoyar la mejora continua y que puede aplicarse

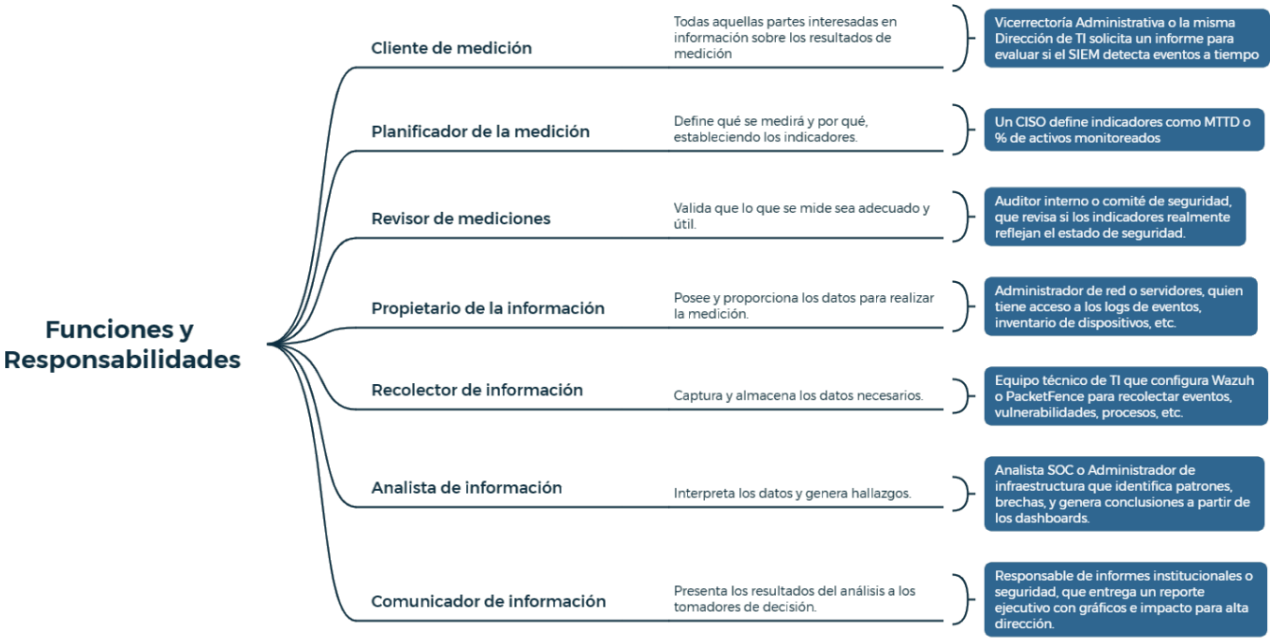
a cualquier proceso o actividad; bajo ese contexto y citando literalmente lo definido en la norma el primer indicador de la anterior tabla toma mayor sentido:

"*¿Cuánto tiempo después de la ocurrencia de un evento tarda el control en detectar que el evento se ha producido?"*

Por otro lado, la misma norma es clara en determinar que toda institución debe definir por sí misma quien debe monitorear, medir, analizar o evaluar sus indicadores en términos de seguridad; así las cosas, la alta dirección de cada universidad deberá reglamentar y designar recursos concretos para esta labor, se sugiere tomar en consideración los siguientes roles para una adecuada proyección:

Figura 18

Roles a considerar para gestión de los indicadores



Nota: Los roles descritos en la figura son los sugeridos por la norma ISO 27004 en su literal 6.5

Análisis de cobertura y suficiencia de los indicadores

Con el fin de validar la suficiencia del conjunto propuesto, se realizó un mapeo de los indicadores frente a las seis funciones del NIST CSF 2.0 (Gobierno, Identificación, Protección, Detección, Responder y Recuperar).

El análisis evidenció que:

- Las funciones de detección y respuesta presentan mayor densidad de indicadores (MTTD, MTTR, tasa de falsos positivos, incidentes por severidad).
- Las funciones de identificación y protección están representadas mediante el porcentaje de activos cubiertos.
- La función de recuperación se mide a través del tiempo de recuperación respectivo (RT).
- La función de gobierno se aborda mediante cumplimiento normativo y formalización de lecciones aprendidas.

No obstante, se identificó una posible brecha en métricas predictivas o proactivas, como indicadores de exposición anticipada a vulnerabilidades, lo cual abre una línea futura de mejora.

Conclusiones

Las universidades como entes que prestan servicios a terceros requieren para su operación de infraestructura tecnológica que puede ser susceptible de amenazas por agentes externos, gracias a lo realizado, se logra evidenciar casos concretos en Colombia y a partir de los mismos, se logró generar un marco de referencia que creó las bases para entender la necesidad de instalar soluciones que gestionen este tipo de incidentes y brinden al área de Tecnología las herramientas necesarias para anticipar o reaccionar a los mismos.

Para un adecuado proceso de despliegue de herramientas NAC y SIEM se debe realizar un proceso previo que debe ser riguroso en el sentido de identificar el tipo de infraestructura con el que se cuenta internamente en la institución y a partir de esta, seleccionar la herramienta que se ajuste de mejor manera a la necesidad puntual; ahora bien, existen etapas previas que no necesariamente son técnicas y que son vitales para un adecuado proceso de implementación, para esto el marco referencial expuesto en capitulo asociado al primer objetivo específico es clave.

Se logra evidenciar que en el ámbito del software libre se cuenta con importantes herramientas que brindan soluciones a necesidades puntuales, es gratificante ver como la comunidad trabaja en pro de compartir y mejorar la ciberseguridad tanto en entornos académicos como comerciales; ahora bien, el proceso para un despliegue adecuado va a depender de las particularidades de cada organización, pero siempre debe ser analizado de manera transversal y en pro de los objetivos y la visión de la entidad.

Por último, toda arquitectura de seguridad siempre será susceptible de mejora; así las cosas es necesario que se considere un proceso de medición e indicadores que permitan evaluar si el desempeño es el esperado o si se deben ajustar ciertos elementos o procesos para garantizar un mejor desempeño, todo esto en busca de una mejor postura de ciberseguridad en las

organizaciones; así mismo, es clave reforzar el factor de concientización del equipo humano para aumentar el nivel de efectividad en la detección, gestión y resolución de incidentes de manera temprana sobre los activos informáticos.

Recomendaciones

En primer lugar, es muy importante que las instituciones de educación superior consideren reglamentar las áreas de Ciberseguridad, que se vea necesidad de consolidar equipos de especialistas en la materia y no se piense en esta necesidad como una función más por asignar a un colaborador, este equipo debería responder mínimamente a la Dirección de Tecnología e idealmente a la Alta Dirección; lo anterior, redundará en una mejor respuesta ante posibles eventos de contingencia o crisis en términos de seguridad digital y formalizará las practicas que posiblemente hoy se realicen a nivel de operación, pero sin una estrategia clara detrás de las mismas.

En consonancia con lo anterior, los equipos de ciberseguridad requieren de ciertos presupuestos debidamente institucionalizados, aun cuando la operación se soporte en soluciones libres, existe la necesidad de contar con dinero para campañas de socialización o modernización y a nivel de infraestructura; es importante que la ciberseguridad se vea como inversión y no como un gasto al final del día.

Otro factor esencial es la capacitación continua del personal, no solo a nivel técnico sino también académico y administrativo; todos los colaboradores de las IES se vuelven la primera defensa en términos de ciberseguridad.

Para finalizar, las herramientas acá expuestas demandan de actualización constante, dado que día a día los incidentes y la tecnología detrás de los mismos, va cambiando y aumentando el nivel de complejidad, con lo cual se invita a las instituciones a revisar periódicamente las recomendaciones de los propios sitios fabricantes de las soluciones para aplicar lo respectivo.

Referencias bibliográficas

Inverse Inc. (2023). *PacketFence Deployment Cases in Higher Education*. Obtenido de Sitio web Inverse.

Agyare, R., Adu-Boahene, C., & Nikoi, S. N. (2022). Gestión segura de redes remotas y control de acceso a la red: el caso del campus de Kumasi de la Universidad de Educación. *Revista Internacional de Ingeniería de Sistemas, 6*(1), 18-45. Obtenido de https://doi.org/10.11648/j.ijse.20220601.13

Arana, J. R., Villa, L. A., & Polanco, O. (16 de Mayo de 2013). Implementation del control de acceso a la red mediante los protocolos de autenticación, autorización y auditoría. *Ingeniería y Competitividad, 15*(1), 127-137. Obtenido de https://doi-org.bibliotecavirtual.unad.edu.co/10.25100/iyc.v15i1.2626

Araujo, M. S., Machado, B. A., & Passos, F. U. (2024). Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance. *Applied Sciences (2076-3417), 14*(5), 2116. doi:10.3390/app14052116

Boubakr , N., Hakima, K., Rasheed , H., Spyridon, M., & Hassine, M. (2021). Access Control Mechanisms in Named Data Networks: A Comprehensive Survey. *ACM Computing Surveys (CSUR), 54*, 1 - 35. doi:https://doi.org/10.1145/3442150

CONPES 3995. (1 de Julio de 2020). *Política Nacional de Confianza y Seguridad Digital.* Obtenido de Consejo Nacional de Política Económica y Social: https://colaboracion.dnp.gov.co/cdt/Conpes/Econ%C3%B3micos/3995.pdf

Crespo Martinez, E. (2023). Curso Internacional para CISO de Universidades. Buenos Aires, Argentina.

Eddy, N. (9 de Agosto de 2024). *Las universidades recurren al SIEM de última generación para mejorar la visibilidad cibernética.* Obtenido de EdTech Magazin: https://edtechmagazine.com/higher/article/2024/08/universities-turn-next-gen-siem-improved-cyber-visibility

El Colombiano. (23 de Noviembre de 2021). *Atacan a la Javeriana: cibersecuestro de sus datos en dos ciudades*. Obtenido de https://www.elcolombiano.com/colombia/secuestran-datos-de-la-universidad-javeriana-en-colombia-LB16067491

El Espectador. (28 de Junio de 2021). *La Universidad El Bosque fue víctima de un ciberataque*. Obtenido de https://www.elespectador.com/educacion/la-universidad-el-bosque-fue-victima-de-un-ciberataque/

Entrust Corporation. (2025). *¿Qué es el GDPR?* Obtenido de https://www.entrust.com/es/resources/learn/what-gdpr

Fernández Martínez, A., & Llorens Largo, F. (2022). *Gobierno de las TI para universidades.* Madrid, España: CRUE.

FORTINET. (2024). *¿Qué es el control de acceso a la red (NAC)?* Obtenido de https://www.fortinet.com/lat/resources/cyberglossary/what-is-network-access-control

FORTINET. (28 de Abril de 2025). *Fortinet Global Threat Landscape Report 2025*. Obtenido de https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-landscape-report-2025.pdf

Gartner. (2022). *Market Guide for Security Orchestration, Automation and Response Solutions.* Gartner Research.

Gómez Prado, S. P., Sandoval Bonilla, N. A., Ibadango Urbano, J. A., & Cortes, A. (2023). *Propuesta de implementación de SIEM en un centro de capacitación, con tres casos de usos, utilizando Mitre attack.* Obtenido de Repositorio Digital Universidad Internacional del Ecuador - UIDE: https://repositorio.uide.edu.ec/handle/37000/6615

Hata, M., Darus, M., Shafiee, M., Petrus, E., & Jamian, Y. (2023). A Log Aggregation Design Criteria for Robust SIEM (Security Information and Event Management) in Enhancing Threat Detection. *2023 IEEE 8th International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, (págs. 1-6).

IBM. (2023). *¿Qué es la gestión de eventos e información de seguridad (SIEM)?* Obtenido de https://www.ibm.com/mx-es/topics/siem

Inverse inc. (19 de Febrero de 2025). *Guia de Instalación*. Obtenido de Sitio web de PacketFence: https://www.packetfence.org/doc/PacketFence_Installation_Guide.html#_installation

ISO/IEC. (2022). *Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de la Seguridad de la Información. Requisitos NTC-ISO/IEC 27001.* IEC - ICONTEC.

ISO/IEC 27004. (2022). *Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la información. Monitoreo, medición, análisis y evaluación.* ICONTEC.

MetaRed TIC. (24 de Octubre de 2024). *Índice de Madurez en Ciberseguridad de las IES Iberoamericanas.* Obtenido de https://www.metared.org/content/dam/metared/imc/MetaRed_IMC_2024.pdf

MetaRed TIC. (15 de Noviembre de 2024). *Un informe colaborativo revela el estado de 13 productos TIC críticos en las Instituciones de Educación Superior Iberoamericanas.* Obtenido de https://www.metared.org/global/novedades/informe-metared-productosTI-criticos-ies-iberoamericanas.html

MuchoHacker. (5 de Enero de 2023). *Universidades colombianas bajo el ataque de ciberdelincuentes*. Obtenido de https://muchohacker.lol/2023/01/universidades-colombianas-bajo-el-ataque-de-ciberdelincuentes/

National Institute of Standards and Technology - NIST. (Agosto de 2020). *Special Publication 800-207 - Zero Trust Architecture.* Estados Unidos: Departamento del Comercio. doi:10.6028/NIST.SP.800-207

NIST. (26 de Febrero de 2024). *El Marco de Seguridad Cibernética (CSF) 2.0.* doi:10.6028/NIST.CSWP.29.spa

NTC-ISO 31000. (2018). *Gestión del riesgo. Directrices.* ICONTEC.

Osaro Mitchell, C. O. (6 de Enero de 2024). Confidentiality, Integrity, and Availability in Network Systems: A Review of Related Literature. *International Journal of Innovative Science and Research Technology*, *8*(12). doi:10.5281/zenodo.10464076

Pacheco Fernández, A. E., Suarez Santamaría, L. I., & González Chacón, J. H. (31 de 05 de 2021). *Aplicar la Metodología OCTAVE de Identificación de Amenazas y*

Vulnerabilidades en una Entidad Bancaria. Obtenido de https://proyectosmaestrias.virtual.uniandes.edu.co/images/mlC4bCJ5XSVNmWQUD6uN4V2gJFMiZDbyVCkn22QE.pdf

Palo Alto Networks. (2018). *¿Qué es la detección y respuesta extendidas (XDR)?* Obtenido de https://www.paloaltonetworks.lat/cyberpedia/what-is-extended-detection-response-XDR

Parker, J. T., & Bullock, J. (2017). *Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework.* Wiley. doi:10.1002/9781119183457

Pino Medina, A. (2021). *Plataformas SOAR. Respuesta orquestada y automatizada de la seguridad.* Universitat Oberta de Catalunya (UOC). Obtenido de https://hdl.handle.net/10609/132128

PORTNOX. (18 de Agosto de 2021). *Universidad destacada de EE. UU. supera desafíos de acceso a la red con NAC en la nube.* Obtenido de Casos de Éxito: https://v2catalog.com/wp-content/uploads/2024/07/UD-Case-Study-5.25.21.pdf

Praly, P., Delorme, M., & Mitaine, Y. (10 de Diciembre de 2024). Retour d'expérience : déploiement d'un SIEM et d'un SOAR. *JRES (Journées réseaux de l'enseignement et de la recherche).*

SANS Institute. (1 de Diciembre de 2023). *Security Awareness Maturity Model v3: A Roadmap to Manage Human Cyber Risk.* Obtenido de SANS Security Awareness: https://sansorg.egnyte.com/dl/sQgEZSYXTY

SEMANA. (2 de Abril de 2023). *Los detalles secretos del grave hackeo que sufrió la Universidad Nacional*. Obtenido de Nación:

https://www.semana.com/nacion/articulo/asi-fue-el-hackeo-del-que-fue-victima-la-universidad-nacional/202335

Wazuh. (2024). *SIEM Solution Overview*. Obtenido de Wazuh Documentation.

XCELIT. (2024). *Caso práctico de Microsoft Sentinel SIEM y SOAR administrados.* Obtenido de https://xcelit.io/case-studies/case-study-siem-soar/

Zhang, Y., Ma, L., Wang, X., & Zhang, J. (2021). A Secure and Scalable Access Control Scheme for Cloud-Based University Systems. *IEEE Access*(9), 6224–6233. doi:10.1109/ACCESS.2020.3047325