Arquitectura Modular de Ciberseguridad Basada en Software Libre

Hernando José Peña Hidalgo
Docente Investigador
CSIRT Académico UNAD
Universidad Nacional Abierta y a Distancia
ORCID: 0000-0002-3477-2645

Luis Fernando Zambrano Hernandez
Docente Investigador
Líder CSIRT Académico UNAD
Universidad Nacional Abierta y a Distancia
ORCID: 0000-0002-4690-3526

Sonia Ximena Moreno Molano
Líder Maestría en Ciberseguridad
Universidad Nacional Abierta y a Distancia
ORCID: 0000-0003-0392-1983

Jorge Eliecer Hernandez
Universidad Nacional Abierta y a Distancia
ORCID: 0000-0003-3198-7007

Resumen – El presente documento presenta la propuesta del diseño de un prototipo de infraestructura lógica para la operación del CSIRT-UNAD, fundamentado en la evaluación y selección de herramientas de software libre. La propuesta articula un ecosistema modular que integra Wazuh (correlación y monitoreo), Suricata (detección de intrusiones en red), ELK Stack (almacenamiento y visualización de logs), TheHive y Cortex (gestión y automatización de incidentes) y MISP (inteligencia de amenazas). El modelo cubre el ciclo completo de gestión de incidentes y se alinea con marcos como NIST, ENISA y SIM3 v2, además de políticas nacionales (CONPES 3995) y el Plan de Desarrollo Institucional de la UNAD. Los resultados evidencian viabilidad técnica y costo-efectividad, así como su valor para investigación aplicada, extensión académica y cooperación interinstitucional, posicionando al CSIRT-UNAD como referente universitario sostenible.

Palabras claves: CSIRT, Ciberseguridad, Gestión de Incidentes, Software Libre, Vulnerabilidad

Abstract - This document presents the proposed design of a prototype logical infrastructure for the operation of CSIRT-UNAD, based on the evaluation and selection of open-source tools. The proposal articulates a modular ecosystem that integrates Wazuh (correlation and monitoring), Suricata (network intrusion detection), ELK Stack (log storage and visualization), TheHive and Cortex (incident management and automation), and MISP (threat intelligence). The model covers the entire incident management cycle and aligns with frameworks such as NIST, ENISA, and SIM3 v2, as well as national policies (CONPES 3995) and UNAD's Institutional Development Plan. The results demonstrate technical feasibility and cost-effectiveness, as well as its value for applied research, academic outreach, and interinstitutional cooperation, positioning CSIRT-UNAD as a sustainable university benchmark.

Keywords: CSIRT, Cybersecurity, Incident Management, Open-Source Software,Vulnerability

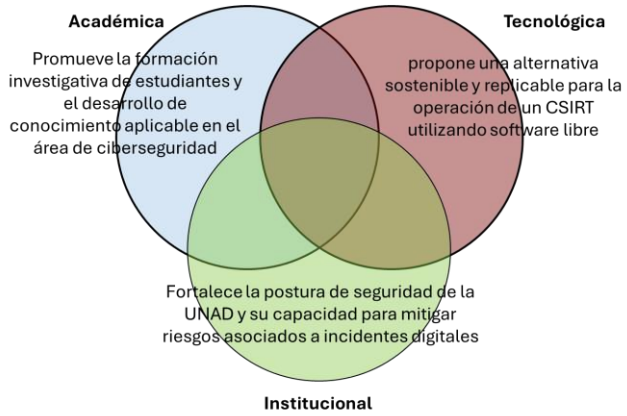
I. INTRODUCCIÓN

La seguridad digital es estratégica para la continuidad operativa. En Colombia, el Balance Anual del Cibercrimen 2022 reportó más de 16.000 incidentes, con crecimiento sostenido de ransomware, phishing y suplantación; el Informe SAFE 2021–2022 ratifica al cibercrimen como la tipología delictiva de mayor expansión. Organismos como NIST subrayan procesos estandarizados para

reducir el impacto y proteger activos; sin embargo, la creación de CSIRT suele verse limitada por costos de infraestructura y talento especializado, especialmente en instituciones académicas. En este contexto, las herramientas de software libre ofrecen una alternativa viable, flexible y auditable que favorece la independencia tecnológica y la apropiación social del conocimiento, en consonancia con lineamientos nacionales (CONPES 3995). Este proyecto determina un prototipo de infraestructura lógica para un CSIRT en la UNAD, orientado a brindar una solución sostenible y a fortalecer la formación investigativa, la generación de conocimiento aplicable y una cultura de ciberseguridad en el ámbito universitario.

Figura 1

Dimensiones de la justificación del proyecto



Fuente: Equipo de trabajo

II. Capítulo 1. Estado del arte de herramientas OSS para actividades CSIRT

A. Evolución histórica del uso de software libre en ciberseguridad

El uso de herramientas de software libre en la gestión de incidentes no es un fenómeno reciente. Desde principios de los años 2000, proyectos comunitarios como Snort (IDS), Nagios (monitoreo) y Wireshark (análisis de tráfico) ofrecieron alternativas viables frente a soluciones propietarias, particularmente en contextos académicos y en pequeñas empresas con presupuestos limitados. Hacia 2015, el surgimiento de Suricata (IDS/IPS) y la adopción del ecosistema Elastic Stack (ELK) marcaron un nuevo hito, al consolidarse como opciones robustas en proyectos empresariales y de investigación aplicada (Mardjan & Jahan, 2020)

B. Consolidación en el periodo 2019–2022

Entre 2019 y 2022, el software libre dejó de ser secundario para convertirse en eje central de arquitecturas críticas de seguridad. La Agencia de Ciberseguridad de la Unión Europea (ENISA, 2020) reportó que varios CSIRT nacionales incorporaron soluciones OSS como OTRS (gestión de tickets) y MISP (inteligencia de amenazas). En América Latina, la OEA promovió manuales técnicos para la adopción de MISP, facilitando el intercambio regional de indicadores de compromiso (EAS-OAS, 2024). En el ámbito académico, Rabby (2022) documentó la viabilidad de un SOC universitario basado exclusivamente en OSS, integrando Wazuh, Suricata y TheHive como núcleo operativo.

C. Categorías funcionales de herramientas OSS

El estado del arte permite clasificar las herramientas OSS según las fases del ciclo de gestión de incidentes (NIST, 2020; Open CSIRT Foundation, 2023):

Detección y monitoreo:

- Suricata y Snort, como IDS/IPS, identifican ataques conocidos y patrones de tráfico anómalo.
- Zeek, framework de análisis de tráfico, aporta contexto forense y registro detallado de conexiones (Zeek Project, 2022).

Correlación y análisis de eventos (SIEM):

- Wazuh, integrado con ElasticSearch y Kibana, centraliza logs y correlaciona alertas, con casos de éxito en entornos universitarios (Villegas et al., 2021).
- ELK Stack se ha consolidado para análisis avanzado y visualización de datos.

Gestión de incidentes y respuesta:

- TheHive y Cortex permiten la administración colaborativa de casos y la automatización de análisis (StrangeBee, 2022).

- Shuffle se posiciona como plataforma SOAR de código abierto para orquestar tareas y reducir tiempos de respuesta.

Inteligencia de amenazas:

- MISP se ha convertido en estándar global para intercambio de IoC[1], apoyado por ENISA y la OEA.
- Otras alternativas como OpenCTI y Yeti complementan la gestión de inteligencia (Yeti Project, 2022).

D. Ventajas y limitaciones identificadas

Las principales ventajas del OSS son:

- Costos reducidos: eliminación de licencias facilita adopción en universidades y pymes.
- Transparencia y auditabilidad: acceso al código fuente fortalece la confianza y permite personalización (Mardjan & Jahan, 2020).
- Flexibilidad e integración modular: facilita la construcción de ecosistemas híbridos (Vazão et al., 2019).

No obstante, persisten limitaciones:

- Curva de aprendizaje elevada, que exige talento especializado.
- Escalabilidad en entornos de gran volumen de datos, un reto documentado en experiencias de CSIRT latinoamericanos (Villegas, Carrión & Castro, 2021).
- Dependencia de la comunidad de desarrollo, lo que puede ralentizar la solución de incidentes críticos.
- 1.5 Pertinencia para el contexto universitario

Tabla 1

Herramientas de software libre para detección y monitoreo en apoyo a un CSIRT

Herramienta	Tipo	Funcionalidades clave	Aporta al CSIRT en…
Suricata	IDS/IPS	Inspección profunda de paquetes, detección en tiempo real	Detección de intrusiones y correlación con SIEM
Snort	IDS	Reglas de firmas, detección de ataques conocidos	Detección temprana en redes pequeñas/medianas
Zeek	Framework de tráfico	Registros detallados de conexiones y protocolos	Análisis forense y contextualización de incidentes
Wazuh	SIEM/EDR	Correlación de eventos, integridad de archivos, respuesta automática	Monitoreo central y contención inicial
ELK Stack	Analítica de logs	Recolección, procesamiento y visualización de eventos	Visibilidad integral y análisis de anomalías
Zabbix	Monitoreo TI	Supervisión de servidores, alertas en tiempo real	Continuidad de servicios y disponibilidad
Nagios	Monitoreo TI	Complementos comunitarios, alerta temprana	Preparación y gestión de infraestructura
OpenNMS	Gestión de redes	Métricas de rendimiento, alarmas	Identificación de fallos de red vinculados a incidentes

Fuente: Equipo de trabajo

El análisis realizado permite concluir que las herramientas OSS se han consolidado como una alternativa sostenible para la operación de CSIRT, favoreciendo la investigación aplicada y la cooperación interinstitucional. Para la UNAD, este estado del arte confirma la pertinencia de diseñar un prototipo de infraestructura lógica soportado en software libre, alineado con la Política Nacional de Confianza y Seguridad Digital (CONPES, 2020) y con el Plan de Desarrollo 2023–2034 UNAD 5.0

III. Capítulo 2. Evaluación de herramientas de software libre para la infraestructura lógica

A. Fundamentación de la evaluación

La construcción de un CSIRT no se limita a integrar herramientas técnicas, sino que implica una visión estratégica de largo plazo. En este sentido, la adopción de soluciones OSS representa una opción costo-efectiva, flexible y sostenible, que contribuye al avance hacia modelos de madurez reconocidos internacionalmente, como el SIM3 v2 (Open CSIRT Foundation, 2023). Este modelo evalúa la evolución del CSIRT en torno a su organización, capital humano, herramientas y procesos, ofreciendo un marco de referencia para orientar la selección tecnológica

[1] Indicador de Compromiso

B. Enfoque adoptado

Las herramientas seleccionadas para este análisis responden a las necesidades institucionales de la UNAD, pero también deben garantizar escalabilidad y sostenibilidad. Soluciones como Wazuh, Suricata, TheHive, Cortex, MISP y ELK Stack son evaluadas no solo por sus capacidades técnicas, sino por su potencial de integrarse en un ciclo de mejora continua, que permita alcanzar niveles superiores de calidad, interoperabilidad y cooperación interinstitucional

C. Criterios de evaluación

El proceso se fundamenta en referentes internacionales como ISO/IEC 27035 (ICONTEC, 2020), NIST SP 800-61 (NIST, 2020) y el propio SIM3 v2. Los criterios aplicados son los siguientes

Tabla 2

Criterios de evaluación para la selección de herramientas OSS en la infraestructura lógica de un CSIRT

Criterio	Descriptor	Escala de valoración (1–5)
Funcionalidad	Cobertura de capacidades técnicas: detección, correlación, análisis, respuesta, automatización.	1 = Muy limitada / 5 = Muy completa
Escalabilidad y flexibilidad	Adaptabilidad a distintos entornos (pymes, universidades, grandes empresas) y crecimiento en carga de datos.	1 = Poco escalable / 5 = Altamente escalable
Soporte y comunidad	Existencia de foros, documentación, actualizaciones frecuentes y contribuciones académicas.	1 = Nula comunidad / 5 = Comunidad activa y robusta
Compatibilidad e integración	Interoperabilidad con otras herramientas OSS o propietarias mediante APIs y estándares.	1 = Muy baja / 5 = Muy alta
Costos de adopción	Recursos requeridos para infraestructura, curva de aprendizaje y capacitación.	1 = Muy altos / 5 = Muy bajos
Cumplimiento normativo (opcional)	Alineación con estándares y marcos internacionales (ISO/IEC 27035, NIST 800-61, GDPR).	1 = No cumple / 5 = Cumple totalmente

Fuente: Equipo de trabajo.

Estos criterios fueron sistematizados en una matriz comparativa, con escala de valoración de 1 (muy limitado) a 5 (muy completo)

D. Resultados de la evaluación comparativa

Los resultados obtenidos confirman que soluciones como Wazuh, Suricata, TheHive, MISP y ELK Stack cumplen con altos niveles de funcionalidad, integración y soporte comunitario, siendo idóneas para una infraestructura universitaria. En particular:

- Wazuh destaca como núcleo SIEM de correlación y monitoreo.
- Suricata sobresale en detección en red, con gran comunidad de reglas y soporte.
- TheHive y Cortex aportan gestión colaborativa de incidentes y automatización.
- MISP se consolida como estándar en intercambio de inteligencia de amenazas.
- ELK Stack provee robustez en almacenamiento y visualización de logs

En contraste con suites propietarias, estas soluciones OSS presentan ventajas como reducción de costos, transparencia del código y flexibilidad, pero también limitaciones: mayor curva de aprendizaje, necesidad de capacitación y retos de escalabilidad en escenarios de alto volumen de datos

E. Pertinencia para la UNAD

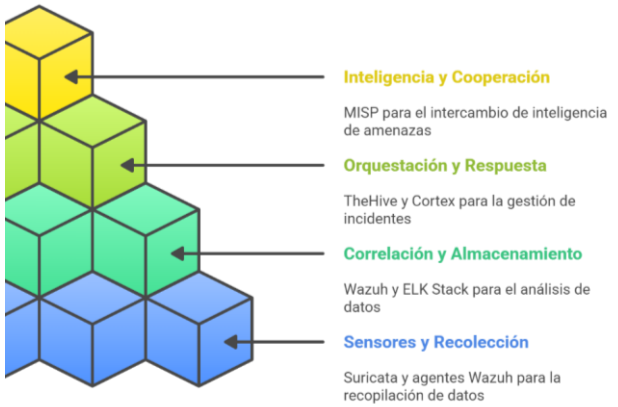
En el contexto universitario, estas características constituyen más una oportunidad que una barrera. La implementación de un stack OSS en el CSIRT-UNAD no solo permite fortalecer la protección institucional, sino también crear un laboratorio vivo de formación e investigación en ciberseguridad. De este modo, la UNAD alinea la selección tecnológica con la Política Nacional de Confianza y Seguridad Digital (CONPES 3995, 2020) y con los objetivos del Plan de Desarrollo 2023–2034, avanzando hacia modelos de madurez como SIM3 v2 y consolidando una estrategia sostenible de fortalecimiento académico y operativo

IV. Capítulo 3. Diseño de la infraestructura lógica alterna del CSIRT – Enfoque Modular y Escalable

El CSIRT-UNAD se concibe bajo un enfoque modular que permite incorporar gradualmente componentes especializados según las capacidades de la institución. De esta manera, el despliegue inicial de Wazuh y Suricata ofrece un núcleo funcional de monitoreo y detección, al cual se integran posteriormente plataformas como TheHive/Cortex y MISP. Esta modularidad garantiza flexibilidad para crecer en volumen de datos, usuarios y escenarios de operación, respondiendo a la necesidad de escalar sin comprometer la estabilidad del sistema (Jaikla y otros, 2022).

Figura 1

Diseño de una Arquitectura lógica propuesta del CSIRT



Fuente: Equipo de trabajo.

A. Fundamentación del diseño

El diseño de la infraestructura lógica para un CSIRT universitario es un paso estratégico que traduce los hallazgos teóricos de los capítulos anteriores en una propuesta tecnológica aplicable. No se trata únicamente de seleccionar herramientas, sino de integrarlas en un ecosistema coherente que garantice sostenibilidad, escalabilidad y pertinencia. De acuerdo con NIST SP 800-61 (2020), un CSIRT efectivo debe cubrir todo el ciclo de gestión de incidentes: preparación, detección, análisis, contención, erradicación y recuperación. Por su parte, ENISA (2020) recomienda la interoperabilidad y modularidad como principios básicos de cualquier arquitectura, mientras que la OEA (2024) impulsa el uso de plataformas libres de CTI, como MISP, para la cooperación regional

En el caso de la UNAD, la infraestructura no solo debe responder a la protección institucional, sino también convertirse en laboratorio pedagógico e investigativo para fortalecer competencias de estudiantes y docentes en ciberseguridad. Así, el diseño cumple una doble misión: proteger y educar.

B. Principios rectores

El diseño se construye sobre tres pilares estratégicos:

1. Fundamentación en marcos de referencia internacionales: la arquitectura refleja buenas prácticas de NIST, ENISA, OEA y se alinea con el modelo de madurez SIM3 v2 (Open CSIRT Foundation, 2023), que mide la evolución en organización, procesos, personas y herramientas
2. Enfoque modular y escalable: permite integrar progresivamente tecnologías según recursos y madurez institucional, evitando dependencias de un solo proveedor y reduciendo riesgos de obsolescencia.
3. Articulación académica: el CSIRT no solo protege activos críticos, sino que se convierte en un entorno de aprendizaje vivo para el entrenamiento en incident response, threat hunting y análisis forense.

C. Componentes de la arquitectura

El ecosistema propuesto es abierto, modular y basado en herramientas OSS que cumplen roles específicos y complementarios

Monitoreo y correlación:

- Wazuh (SIEM/EDR): núcleo del sistema. Centraliza alertas, correlaciona eventos, realiza análisis de integridad de archivos y detección de malware/rootkits. Además, soporta integración con ElasticSearch y Kibana para dashboards en tiempo real.
- ELK Stack (ElasticSearch, Logstash, Kibana): potencia la observabilidad, análisis de big data de seguridad y visualización avanzada de métricas.

Detección en red:

- Suricata (IDS/IPS): inspección profunda de paquetes, detección de ataques y generación de logs estructurados (EVE JSON) que se integran directamente en Wazuh/ELK para correlación.

-

Gestión y respuesta a incidentes:

- TheHive: plataforma de gestión de incidentes que permite el trabajo colaborativo entre analistas, con seguimiento de tareas, evidencias e informes.
- Cortex: motor de automatización que ejecuta analizadores sobre IoC (hashes, IPs, dominios, URLs), reduciendo el tiempo medio de respuesta (MTTR).

Inteligencia de amenazas y cooperación:

- MISP: plataforma estandarizada para compartir indicadores de compromiso (IoC) bajo formatos STIX/TAXII. Facilita la cooperación interinstitucional y la anticipación de campañas maliciosas, alineándose con buenas prácticas de ENISA y OEA.

Este stack OSS integrado cubre todo el ciclo de incident response, desde la detección inicial hasta el intercambio de inteligencia.

D. Fases de implementación

El despliegue se organiza de forma progresiva y evolutiva, en línea con el modelo de madurez SIM3 v2

- Fase 1 (Básica): implementación de Wazuh + Suricata + ELK. Esta etapa brinda visibilidad centralizada, correlación inicial de eventos y capacidad de detección temprana.

- Fase 2 (Formalización): integración de TheHive y Cortex, estableciendo procesos formales de gestión de incidentes y automatización de respuestas. Aquí el CSIRT pasa de lo reactivo a lo proactivo.

- Fase 3 (Cooperación): incorporación de MISP, conectando al CSIRT-UNAD con redes académicas y sectoriales, e institucionalizando el intercambio de inteligencia de amenazas.

E. Estrategias de adopción y mejora continua

- Integración nativa: vincular Suricata y Wazuh mediante formato EVE JSON, asegurando correlación inmediata.
- Optimización de almacenamiento: configurar ILM (Index Lifecycle Management) en ELK, con políticas de retención diferenciada (30–90 días en “hot”, hasta 12 meses en “warm/cold”).
- Playbooks iniciales: definir guiones operativos para incidentes comunes (phishing, ransomware, ataques de fuerza bruta), integrando TheHive/Cortex.
- Comunidades de confianza: configurar MISP con taxonomías adecuadas, respetando normas de protección de datos.
- Formación continua: asignar roles específicos (analista SIEM, operador IDS, gestor de incidentes, coordinador CTI) y establecer un plan de capacitación progresivo.
- KPIs de madurez: medir MTTD (Mean Time to Detect), MTTR (Mean Time to Respond), tasa de falsos positivos y cumplimiento de SLAs de respuesta

F. Pertinencia institucional

La propuesta se ajusta a la Política Nacional de Confianza y Seguridad Digital (CONPES 3995, 2020) y a los objetivos del Plan de Desarrollo 2023–2034 de la UNAD, consolidando una estrategia sostenible en ciberseguridad. Al posicionar a Wazuh como núcleo y a las demás herramientas como capas complementarias, la UNAD transita de un modelo reactivo a un modelo maduro, colaborativo y pedagógico, que integra seguridad, investigación y cooperación internacional

Figura 2

Arquitectura Lógica de un CSIRT con Herramientas de Software Libre

Fuente. Equipo de trabajo

I. IV. CONCLUSIÓN

El proyecto demuestra que el diseño de un CSIRT basado en herramientas de software libre es técnicamente viable y estratégico para instituciones educativas. Soluciones como Wazuh, Suricata, ELK Stack, TheHive, Cortex y MISP permiten construir un ecosistema modular que cubre detección, correlación, gestión de incidentes e inteligencia de amenazas, alcanzando niveles de desempeño comparables a los de arquitecturas propietarias.

La infraestructura propuesta se alinea con marcos internacionales (NIST, ENISA, SIM3 v2) y políticas nacionales (CONPES 3995 de 2020), proyectando al CSIRT como un instrumento de fortalecimiento de la madurez digital. Su carácter evolutivo, basado en fases, asegura que el proceso avance de manera sostenible en organización, procesos, herramientas y talento humano

La adopción de OSS elimina gastos de licenciamiento y ofrece transparencia, auditabilidad y flexibilidad de integración. Esto posibilita a la UNAD construir una capacidad robusta sin incurrir en costos prohibitivos, asegurando sostenibilidad financiera y técnica en el tiempo

El prototipo diseñado puede reducir significativamente los tiempos medios de detección (MTTD) y respuesta (MTTR), mejorar la trazabilidad de incidentes y fortalecer la cooperación interinstitucional mediante estándares abiertos como STIX/TAXII. Esto permite al CSIRT responder de forma más eficiente y con mejores métricas de desempeño

Más allá de la seguridad operativa, la propuesta tiene un alto valor pedagógico: convierte al CSIRT en un laboratorio vivo de formación e investigación aplicada, donde estudiantes y docentes pueden entrenarse en incident response, threat hunting y análisis forense, fortaleciendo así la cultura de ciberseguridad en la academia

El plan de implementación por fases —detección y monitoreo, formalización de procesos y cooperación mediante inteligencia de amenazas— garantiza una adopción progresiva que se adapta a los recursos disponibles y potencia la capacidad de

la UNAD para integrarse en redes académicas y sectoriales de ciberseguridad

REFERENCIAS

Abdul, W., Abdul, F., & Ammar, M. (2022). *Which open-source IDS? Snort, Suricata or Zeek.* https://www.sciencedirect.com/science/article/abs/pii/S1389128622002420?via%3Dihub

Andrade, R., & Torres, J. (2019). *Enhancing intelligence SOC with big data tools.* https://doi-org.bibliotecavirtual.unad.edu.co/10.1109/IEMCON.2018.8614779

Basis Technology. (2022). *Autopsy.* https://www.autopsy.com/

CaiVirtual. (2022). *Balance anual del cibercrimen en Colombia 2022.* https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202022.pdf

Castiblanco, A. (2024). *Aprovechamiento de soluciones de software libre en el montaje y puesta en marcha de un centro de respuesta a incidentes informáticos para organizaciones colombianas.* https://repository.unad.edu.co/handle/10596/61598

CCIT. (2022). *Informe SAFE: Tendencias del cibercrimen 2021–2022.* https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf

Congreso de Colombia. (2009). *Ley 1273 de 2009.* http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de Colombia. (2012). *Ley 1581 de 2012.* http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

CONPES. (2020). *Política nacional de confianza y seguridad digital (Documento CONPES 3995).* https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

EAS-OAS. (2024). *MISP Tecnical Manual.* https://shares.csirtamericas.org/s/4fz9FcdqePPDf8A/download/CSIRTAmericas%20MISP%20Technical%20Manual.pdf

ENISA. (2020). *HOW TO SETUP UP CSIRT AND SOC.* https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

Filigran. (2022). *OpenCTI.* https://filigran.io/platforms/opencti/

GDPR.eu. (2018). *General Data Protection Regulation GDPR.* https://gdpr.eu/

ICONTEC. (2020). *ISO/IEC 27032:2020 Tecnologías de la información. Técnicas de seguridad. Directrices para ciberseguridad.* https://ecollection-icontec-org.bibliotecavirtual.unad.edu.co/normavw.aspx?ID=77621

ICONTEC. (2020). *ISO/IEC 27035:2020 Tecnología de la información. Gestión de incidentes de seguridad de la información. Parte 1: Principios y procesos.* https://ecollection-icontec-org.bibliotecavirtual.unad.edu.co/normavw.aspx?ID=77621

ICONTEC. (2022). *ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información.* https://ecollection-icontec-org.bibliotecavirtual.unad.edu.co/normavw.aspx?ID=77621

Jaikla, T., Suksomboon, K., & Pattaranantakul, M. (2022). *Open-source SOC-as-a-Service for Strengthening Cybersecurity in Small and Medium Manufacturers in Thailand toward Industry 4.0.* https://apnic.foundation/projects/open-source-soc-as-a-service-for-strengthening-cybersecurity-in-small-and-medium-manufacturers-in-thailand-toward-industry-4-1/technicalreport/

Janampa, H., Huamani, H., & Meneses, Y. (2022). *Snort Open Source como detección de intrusos para la seguridad de la infraestructura de red.* https://www.redalyc.org/articulo.oa?id=378369292004

Kaspersky. (s.f.). *Return on security investment: Internal SOCs halve the financial impact of enterprise data breaches.* Return on security investment: Internal SOCs halve the financial impact of enterprise data breaches

Mardjan, M., & Jahan, A. (2020). *Using open source for security and privacy protection. Security and Privacy Reference Architecture.* https://security-and-privacy-reference-architecture.readthedocs.io/en/latest/10-using-oss.html

MinTIC. (2021). *Informe nacional de ciberseguridad 2021.* https://gobiernodigital.mintic.gov.co/

MISP Project. (2022). *Malware Information Sharing Platform (MISP).* https://www.misp-project.org/

Mohd, S., Li, S., & Arief, B. (2022). *Incident Response Practices Across National CSIRTs.* https://kar.kent.ac.uk/94119/1/Incident-Response-Practice.pdf

NIST. (2020). *Computer Security Incident Handling Guide (SP 800-61 Rev. 2).* https://doi.org/10.6028/NIST.SP.800-61r2

OISF. (2022). *Suricata IDS/IPS/NSM engine.* https://suricata.io/

Open CSIRT Foundation. (2023). *SIM3 v2 interim – Security Incident Management Maturity Model.* https://opencsirt.org/wp-content/uploads/2023/11/SIM3_v2_interim_standard.pdf

Presidencia de la República de Colombia. (2020). *Decreto 620 de 2020.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=118337

Quintero, J. (2018). *Implementación de un sistema de detección de intrusos en la red interna de la Alcaldía de Montería usando software libre.* https://repository.unad.edu.co/handle/10596/17438

Rabby, Z. (2022). *Building Security Operations Center (SOC) using open source technologies SIEM for industries.* https://dspace.bracu.ac.bd/xmlui/handle/10361/22720

Rincon, G., Avila, E., Navarrete, J., & Herrera, H. (2025). *Propuesta de modelo de un Centro de Operaciones de Seguridad Cibernética – CSOC - Open Source para empresas Mipymes*. http://hdl.handle.net/11371/7260

Rosero, W. (2021). *Diseño documental para la implementación del CSIRT para el caso de estudio de la Empresa Cibersecurity de Colombia LTAA.* https://repository.unad.edu.co/handle/10596/42000

Shuffle. (2022). *Shuffle Open Source SOAR platform.* https://shuffler.io/

StrangeBee. (2022). *Cortex Speed up analysis and make response easier.* https://strangebee.com/cortex/

StrangeBee. (2022). *TheHive Collaborative Case Management Platform for cybersecurity teams.* https://strangebee.com/thehive/

The Volatility Foundation. (2022). *Volatility.* https://volatilityfoundation.org/

UNAD. (2018). *Resolución 04256 de 2018.* https://sgeneral.unad.edu.co/images/documentos/resoluciones/2015/RES0_4256_20150303.pdf

UNAD. (2023). *Plan de Desarrollo Docenal 2023 - 2034 UNAD 5.0.* https://informacion.unad.edu.co/images/2023/PLAN_DE_DESARROLLO_2023-2034.pdF

Vazão, A., Santos, L., Piedade, M., & Rabadão, C. (2019). *SIEM Open Source Solutions: A Comparative Study.* https://doi-org.bibliotecavirtual.unad.edu.co/10.23919/CISTI.2019.8760980

Villegas, M., Carrión, D., & Castro, J. (2021). *CSIRT universitario: Guía de implementación para campus.* http://www.risti.xyz/issues/ristie39.pdf

Villegas, W., Ortiz, I., & Sanchez, S. (2021). *Proposal for an Implementation Guide for a Computer Security.* https://www.mdpi.com/2073-431X/10/8/102/pdf

Yeti Project. (2022). *Yeti: Open source threat intelligence platform.* https://yeti-platform.io/

Zeek Project. (2022). *Zeek: The network analysis framework.* https://zeek.org/