Estructuración de ataques informáticos por medio de playbooks

Structuring of computer attacks through playbooks

[1]John Freddy Quintero Tamayo, [2]Yenny Stella Nuñez Álvarez, [3]Nelly Alexandra Cuevas Nuñez

[1,2,3]Universidad Nacional Abierta y a Distancia, Colombia

Recibido: 20/10/2023 Aprobado 20/11/2023

Resumen

Este proyecto plantea la necesidad de establecer una base de datos de conocimiento que brinde orientación para responder a eventos o incidentes de ciberseguridad que puedan surgir dentro de la Universidad o involucrar a alguna de sus partes interesadas o comunidades objetivo. La iniciativa busca mejorar las capacidades de ciberseguridad de la Universidad y asegurar una respuesta rápida y efectiva ante posibles amenazas cibernéticas dentro de su comunidad y más allá. Al aprovechar el conocimiento colectivo, la base de datos se convertirá en un recurso valioso para proteger y salvaguardar el entorno digital de la Universidad. El propósito es fortalecer la preparación y respuesta frente a incidentes informáticos, fomentando la coordinación entre las partes involucradas y las comunidades objetivo. Asimismo, este proyecto representa un paso significativo hacia el establecimiento del Centro de Respuesta a Incidentes Informáticos, permitiendo a la Universidad enfrentar de manera proactiva y eficiente los desafíos de seguridad en un entorno tecnológico en constante evolución. La estructuración de un ataque informático es vital dentro de la operación de los grupos encargados de generar las respuestas a estos incidentes, por ese motivo las playbooks contemplarán descripciones del ataque, afectación al sistema, herramientas utilizadas para la contención, solución y recomendación. El proyecto aborda las acciones de automatización de las playbook gestionadas por el CSIRT académico de la Universidad Nacional Abierta y a Distancia (UNAD) utilizando la herramienta GLPI.

Palabras clave: aprendizaje, base de datos, conocimiento, procesos, respuesta, ataques informáticos.

Citación: Quintero Tamayo, J. F. ., Nuñez Alvarez, Y. S. ., & Cuevas Nuñez, N. A. . (2023). Estructuración de ataques informáticos por medio de playbooks. Publicaciones E Investigación, 17(4). https://doi.org/10.22490/25394088.7498

[1]john.quintero@unad.edu.co / https://orcid.org/0000-0003-0128-1214
[2]yenny.nunez@unad.edu.co / https://orcid.org/0000-0002-6868-6278
[3]nacuevasn@unadvirtual.edu.co / https://orcid.org/0009-0007-8496-2838

https://doi.org/10.22490/25394088.7498

Abstract

This project proposes the need to establish a knowledge database that provides guidance for responding to cybersecurity events or incidents that may arise within the University or involve any of its stakeholders or target communities. The initiative aims to enhance the University's cybersecurity capabilities and ensure a prompt and effective response to potential cyber threats within its community and beyond. By leveraging collective knowledge, the database will become a valuable resource to protect and safeguard the University's digital environment. The purpose is to strengthen preparedness and response to computer incidents, fostering coordination among involved parties and target communities. Additionally, this project represents a significant step towards establishing a Computer Security Incident Response Team (CSIRT) Center, enabling the University to proactively and efficiently address security challenges in a constantly evolving technological environment. The structuring of a computer attack is crucial within the operation of groups responsible for generating responses to these incidents, which is why the playbooks will include attack descriptions, system impact, tools used for containment, resolution, and recommendations. The project addresses the automation of playbooks managed by the academic CSIRT of the National Open University and Distance Learning (UNAD) using the GLPI tool.

Keywords: *Learning, database, knowledge, processes, response, computer attacks.*

1. Introducción

El presente trabajo aspira a proporcionar una sólida base teórica y práctica para la adopción de playbooks en el contexto universitario, contribuyendo así a fortalecer la seguridad informática y la capacidad de respuesta frente a incidentes de ciberseguridad en la Universidad Nacional Abierta y a Distancia (UNAD).

En pos de satisfacer las necesidades de protección de la confidencialidad, integridad y disponibilidad, resulta imprescindible un análisis exhaustivo de las ventajas que los playbooks aportan a la gestión de eventos e incidentes en los CSIRT de cualquier organización para enfrentar los ataques de ciberseguridad.

Es crucial profundizar en el conocimiento de cómo una playbook reúne las mejores prácticas y estrategias para llevar a cabo un proceso específico de manera efectiva y eficiente en el ámbito de una universidad. Tal conocimiento permitirá mejorar la gestión de proyectos, fomentar la colaboración y optimizar el desempeño de los equipos de trabajo, garantizando así la calidad y eficacia de los resultados obtenidos.

Asimismo, otro beneficio significativo de la implementación de una playbook en una universidad radica en la estandarización de los procesos, lo que conlleva una mejora palpable en la calidad y eficacia de los resultados, a la vez que reduce los errores y la necesidad de retrabajo.

Una playbook bien diseñada debe englobar diferentes elementos, tales como la definición precisa de objetivos, las mejores prácticas y procesos, las herramientas y recursos necesarios, así como los indicadores para el seguimiento y evaluación de su aplicación. Además, la playbook debe caracterizarse por su claridad, concisión y facilidad de uso, con el fin de asegurar su efectiva implementación en distintas áreas de la organización.

2. Materiales y métodos

La metodología del proyecto se encuentra basada en el desarrollo de tres fases las cuales son:

Fase 1. Idealización y conceptualización. Definición del alcance, pertinencia y viabilidad; análisis de

necesidad de conocimiento, planteamiento de solución práctica mediante investigación básica, elección de tema, pregunta de investigación, revisión de antecedentes, planteamiento de hipótesis y metodología (Pargar *et al*., 2019).

Fase 2. Ejecución. En esta fase, se valida la hipótesis mediante la depuración y análisis de datos para generar nuevos procedimientos, productos y herramientas que aporten soluciones a una población o área con base en la necesidad de nuevo conocimiento detectada (Pargar *et al*., 2019).

Fase 3. En los resultados y transferencia se realiza un balance objetivo de los resultados obtenidos y pruebas realizadas, garantizando la objetividad del análisis y demostración de la hipótesis inicial (Pargar *et al*., 2019) .

Las tres fases mencionadas anteriormente están vinculadas a través de ITIL versión 4.0, que abarca los dominios de estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continua del servicio (*ITIL | IT Service Management | Axelos*, 2019). Estos dominios son fundamentales para establecer procesos y desarrollar playbooks, con un enfoque en la mejora continua de la documentación de incidentes. La estructura de los dominios abordados en el proyecto es la siguiente:

A. *Estrategia del servicio (Service Strategy)* En este dominio se identifican tanto los objetivos de la playbook como las necesidades puntuales del CSIRT para un desarrollo coherente del proyecto.

B. *Diseño del servicio (Service Design)* Se establece el diseño y la estructura con la cual se desarrollarán las playbooks. En este dominio es importante definir el flujo de información el cual debe estar alineado con las buenas prácticas y la gestión de incidentes del CSIRT UNAD.

C. *Transición del servicio (service transition)* La gestión de transición teórica a un ambiente productivo debe ser orientado por medio de un sinnúmero de pruebas para documentar la efectividad del proyecto desarrollado y confirmar su correcto funcionamiento.

D. *Operación del servicio (service operation)* Una vez generadas las pruebas suficientes para identificar la eficacia de la playbook se procede a implementarla; en este dominio se resalta la coordinación de capacitación a los miembros de CSIRT y demás actores que intervengan en el desarrollo de la misma.

E. *Mejora continua del servicio (continual service improvement)* La mejora continua se basa en la revisión constante del modelo de playbook para identificar posibles cambios los cuales conlleven a la mejora de la misma, contribuyendo a identificar esas áreas de mejora.

3. Desarrollo

En el entorno actual de infraestructuras tecnológicas y de comunicación, las organizaciones enfrentan una serie de amenazas cibernéticas, como malware, virus, troyanos, gusanos, spyware, adware, phishing, ransomware, botnet, denegación de servicio distribuido DDos, entre otros (OEA, 2019). Estas amenazas ponen en riesgo los activos de información, la reputación corporativa, la propiedad intelectual, la continuidad del negocio y la confianza pública e interna. Para hacer frente a estas amenazas, las organizaciones adoptan estrategias de monitorización, aseguramiento y gestión de eventos, implementando equipos expertos conocidos como CSIRT Computer Security Incident Response Team (OEA, 2023). Estos equipos cuentan con habilidades y formación multidisciplinar y están dedicados a responder con inmediatez a los incidentes informáticos, mitigando así sus efectos y minimizando el impacto en la continuidad del negocio.

Los CSIRT se centran en la gestión de incidentes, análisis de vulnerabilidades y auditoría, respondiendo a incidentes informáticos y brindando soluciones proactivas basadas en un modelo integral de gestión de seguridad de la información. Este enfoque se orienta hacia la prevención y detección de eventos, generación

de alertas, monitoreo y difusión de información relacionada con seguridad de la información, así como el desarrollo de planes de continuidad de negocio y documentos de mejores prácticas (OEA, 2023). Para abordar esta problemática, se emplean los playbooks, que son colecciones de acciones correctivas definidas que se ejecutan de forma rutinaria. Estos playbooks proporcionan estrategias para organizar la respuesta a las amenazas, pudiendo ejecutarse manual o automáticamente en respuesta a alertas o incidentes específicos (Yelevin, 2023).

Sophos en su playbook destaca las tácticas que generalmente se identifican a través de las técnicas utilizadas para lograrlas y que se visualizan en la Tabla 1 donde se enumera las principales técnicas adversas asociadas con cada táctica de ataque durante 2020/2021. Los hallazgos se basan en datos de telemetría de Sophos, así como en informes de incidentes y observaciones de los equipos de Sophos Managed Threat Response (MTR) y Sophos Rapid Response en 2020 y principios de 2021. Los datos se clasifican según el marco MITRE ATT & CK (Pascual, 2021).

Se puede evidenciar con el ejemplo de playbooks creado por Sophos, que es un recurso de gran utilidad para el personal del Csirt, porque le permite conocer vectores de ataque para mejorar las acciones de contención y respuesta a incidentes, además es una herramienta de conocimiento que contribuye a la toma de decisiones al momento de gestionar los eventos que puedan amenazar la seguridad de la infraestructura TI y activos de información de la organización.

Tabla 1. The top techniques observed with each tactic in 2020/2021

The top 5 techniques observed with each tactic in 2020/2021

TA0001	Initial access
T1133	External Remote Services
T1190	Exploit Public-Facing Application
T1566	Phishing
T1078	Valid Accounts
T1195	Supply Chain Compromise

TA0002	Execution
T1059	Command and Scripting Interpreter
T1047	Windows Management Instrumentation
T1053	Scheduled Task/Job
T1569	System Services
T1204	User Execution

TA0003	Persistence
T1543	Create or Modify System Process
T1547.001	Registry Run Keys / Startup Folder
T1546.007	Netsh Helper DLL
T1547.010	Port Monitors
T1098	Account Manipulation

TA0004	Privilege escalation
T1059	Process Injection
T1047	Process Hollowing
T1053	SID-History Injection
T1569	.bash_profile and .bashrc
T1204	Security Support Provider

TA0005	Defense evasion
T1036	Masquerading
T1218	Signed Binary Proxy Execution
T1070	Indicator Removal on Host
T1562.001	Disable or Modify Tools
T1112	Modify Registry

TA0006	Credential access
T1552.002	Credentials in Registry
T1040	Network Sniffing
T1110	Brute Force
T1552.004	Private Keys
T1003	OS Credential Dumping

TA0007	Discovery
T1033	System Owner/User Discovery
T1007	System Service Discovery
T1016	System Network Configuration Discovery
T1046	Network Service Scanning
T1082	System Information Discovery

TA0008	Lateral movement
T1021.001	Remote Desktop Protocol
T1021.002	SMB/Windows Admin Shares
T1570	Lateral Tool Transfer
T1550.003	Pass the Ticket
T1550.002	Pass the Hash

TA0009	Collection
T1560.001	Archive via Utility
T1074	Data Staged
T1005	Data from Local System
T1039	Data from Network Shared Drive
T1409	Access Stored Application Data

TA00011	Command and control
T1105	Ingress Tool Transfer
T1090	Proxy
T1572	Protocol Tunneling
T1008	Fallback Channels
T1043	Commonly Used Port

TA0010	Exfliration
T1041	Exfiltration Over C2 Channel
T1048	Exfiltration Over Alternative Protocol
T1567.002	Exfiltration to Cloud Storage
T1567.001	Exfiltration to Code Repository
T1537	Transfer Data to Cloud Account

TA0040	Imapact
T1490	Inhibit System Recovery
T1486	Data Encrypted for Impact
T1485	Data Destruction
T1489	Service Stop
T1496	Resource Hijacking

SOPHOS

Fuente: Pascual, 2021.

Desarrollo de la playbook

Para desarrollar una playbook de gestión de incidentes de seguridad informática en la Universidad Nacional Abierta y a Distancia (UNAD), se pueden seguir los siguientes pasos:

- Seleccionar una aplicación libre para gestionar y administrar la playbook: hay varias herramientas libres disponibles para la gestión de playbooks, tales como TheHive, MISP, OpenCTI, entre otras. Es importante seleccionar una herramienta que sea compatible con el equipo de CSIRT de la UNAD y que permita la integración con otras herramientas utilizadas por la organización.

- Definir los flujos de trabajo de la playbook: se deben definir los flujos de trabajo que se seguirán para la gestión de incidentes y vulnerabilidades, especificando los pasos a seguir en cada etapa del proceso, las herramientas y sistemas involucrados, los roles y responsabilidades de los miembros del equipo de CSIRT, entre otros aspectos.

- Automatizar la playbook del CSIRT UNAD: es importante automatizar los procesos de la playbook para optimizar la gestión de incidentes y reducir el tiempo de respuesta. Se pueden utilizar herramientas de automatización para realizar acciones como el análisis de eventos, la detección de amenazas, la generación de alertas, entre otros.

- Realizar el mantenimiento de la playbook: es importante realizar un mantenimiento regular de la playbook para asegurar que se encuentre actualizada y se ajuste a las necesidades actuales de la organización. Se deben revisar y actualizar los flujos de trabajo, incluir nuevas herramientas y sistemas, y actualizar la información de contacto y los roles y responsabilidades de los miembros del equipo de CSIRT.

- Seguir buenas prácticas en la playbook: es importante seguir buenas prácticas para la gestión de incidentes de seguridad informática, como la documentación detallada de los incidentes, la utilización de herramientas y sistemas compatibles con los estándares de la industria, la comunicación clara y eficiente entre los miembros del equipo de CSIRT, entre otros aspectos.

En resumen, para desarrollar una playbook de gestión de incidentes de seguridad informática en la UNAD se debe seleccionar una aplicación libre para gestionar y administrar la playbook, definir los flujos de trabajo, automatizar la playbook, realizar el mantenimiento y seguir buenas prácticas. Esto permitirá tener una gestión eficiente y efectiva de los incidentes de seguridad informática en la organización.

A continuación, se presenta una posible estructura de una playbook para la gestión de incidentes de seguridad informática en la Universidad Nacional Abierta y a Distancia (UNAD):

Nombre del incidente o problema: [Insertar un nombre breve y claro que describa el incidente o problema]

Fecha y hora reporte incidente o problema: [Insertar la fecha y hora en que se reportó el incidente o problema]

Nivel de criticidad: [Insertar el nivel de criticidad asignado al incidente, de acuerdo con los criterios establecidos por el CSIRT de la UNAD]

CVE asociado si es una vulnerabilidad: [Insertar el número CVE asociado al incidente, si se trata de una vulnerabilidad conocida]

Afectación de la infraestructura TI UNAD: [Insertar la descripción de la afectación en la infraestructura TI de la UNAD, indicando los sistemas, servicios o redes afectados]

Afectación de activos: [Insertar la descripción de la afectación en los activos de la UNAD, como servidores, bases de datos, aplicaciones, entre otros]

Paso a paso de la solución del incidente: [Insertar un listado de los pasos a seguir para resolver el incidente o problema, incluyendo las acciones necesarias para minimizar el impacto en la infraestructura y los activos de la UNAD]

PoC de la solución: [Insertar una descripción de la prueba de concepto de la solución, indicando los resultados obtenidos y su efectividad en la resolución del incidente]

Pruebas de funcionamiento de la solución y el sistema: [Insertar una descripción de las pruebas de funcionamiento de la solución y del sistema, indicando los resultados obtenidos y su efectividad en la prevención de futuros incidentes]

Fecha y hora de la solución: [Insertar la fecha y hora en que se dio por finalizada la solución del incidente o problema]

Nombre ingeniero Csirt UNAD quien da la solución: [Insertar el nombre del ingeniero de CSIRT de la UNAD que proporcionó la solución al incidente o problema]

La playbook permite tener un registro detallado de la gestión de incidentes de seguridad informática en la UNAD, y proporciona un proceso estructurado y eficiente para la solución de incidentes, reduciendo el tiempo de respuesta y minimizando el impacto en la infraestructura y los activos de la organización. Además, la playbook facilita la documentación y el intercambio de información entre los miembros del equipo de CSIRT y otros departamentos de la organización, mejorando la comunicación y la colaboración en la gestión de incidentes. La documentación también incluye información detallada sobre el activo afectado, los pilares de la seguridad que se vieron vulnerables y una descripción del vector de ataque utilizado por el atacante para provocar el incidente (Hollenberger, 2023). Se proporciona una descripción clara y concisa de la afectación (Thangavelu *et al*., 2021) así como los pasos que se deben seguir para solucionarlo, respaldado con pruebas de concepto (PoC) de la solución. Además, se ofrecen recomendaciones para situaciones similares en el futuro, y se incluye documentación sobre el proceso de escalamiento y notificación.

Con estos parámetros y secciones claramente definidos, las playbooks se convierten en una herramienta eficiente para abordar incidentes de manera consistente y efectiva, proporcionando una guía completa para el equipo CSIRT de la UNAD. Las playbooks debe estar dotadas de procesos bien definidos con las líneas de acción a seguir en caso de un evento o incidente de ciberseguridad. Al automatizar estas bases de conocimiento se proporciona inmediatez y se evita tomar decisiones apresuradas, logrando gestionar y mitigar las amenazas críticas con mayor eficacia para la organización. A continuación, en la Figura 1, se exponen algunas playbooks que se implementaran para optimizar el quehacer del CSIRT.

Figura 1. Playbooks CSIRT.

Fuente: propia.

4. Discusión

El equipo especializado del CSIRT se encuentra constantemente en un ciclo de defensa, ataque y transición donde no es suficiente el buen instinto y la experiencia. Nadie sabe qué amenaza a la empresa más que los defensores de primera línea, por lo que los playbooks tienen la ventaja de poder enfocarse solo en las alertas que importan, donde se garantiza que los analistas tomarán la determinación con respecto a la validez inicial de la alerta frente a ellos lo más rápido posible, lo que permite manejar muchas más alertas entrantes y centrarse en incidentes reales o amenazas para la organización, según afirma Meny Har, vicepresidente de producto de Siemplify (Zurkus, 2018). Los playbooks son bases de conocimiento que deben ser actualizados constantemente, flexibles y adaptables a los nuevos retos de seguridad, con instrucciones claras y con información significativa que contribuya a tomar las mejores decisiones posibles para que puedan responder rápidamente a los incidentes de seguridad (Zurkus, 2018). Ricky Tang trabajó en varias multinacionales como BOCI, Telstra International, Fubon Bank, UBS e ING, con responsabilidades en seguridad cibernética, seguridad de la información, investigación de fraude y gestión de riesgos operativos de TI y ha establecido marcos de gestión de riesgos tecnológicos para FSI que se integran con marcos de riesgo empresarial, definiendo políticas y estándares, creando modelos operativos y procedimientos técnicos, administrando servicios operativos de seguridad cibernética, así como asegurando el cumplimiento de los requisitos reglamentarios (Tang, 2021). Dedica parte de su trabajo a la creación de playbooks de seguridad cibernética para

SOC basados en las mejores prácticas de la industria y estándares reconocidos con 4 elementos esenciales, la detección, la verificación, indicando cómo se analizan los eventos, la comunicación respecto a donde van las alertas y la acción explica lo que se puede hacer para mitigar o contener amenazas que utilizan una vulnerabilidad conocida, nuevas vulnerabilidades de threat intelligence, acceso privilegiado no autorizado, correo electrónico de phishing, datos confidenciales en Internet, sitios web fraudulentos, autenticación de fuerza bruta, anomalías de VPN, devolución de llamada de DNS entre otros (Tang, 2021). Microsoft ofrece dentro de sus servicios de soporte y soluciones tecnológicas playbooks pensados en mejorar las acciones de los equipos de gestión de incidentes para que optimicen sus tiempos de respuesta frente a los ataques de seguridad detectados para contener y remediar su daño. Se indica que a medida que ocurran nuevos ataques cibernéticos generalizados, como Nobellium y la vulnerabilidad de Exchange Server, Microsoft proporcionara playbooks detallados de respuesta a incidentes causados por phishing, password spray y app consent grant (Yelevin *et al*., 2023).

Conclusiones

El actual proyecto se encuentra en desarrollo aún, por ello hasta el momento, se ha realizado un análisis exhaustivo de eventos e incidentes de ciberseguridad en la UNAD, permitiendo identificar vectores comunes de exposición al riesgo informático. El diseño de líneas de acción basadas en casos de uso y eventos informáticos detectados en los activos de información de la Universidad ha avanzado significativamente, brindando una base sólida para responder a futuros eventos o incidentes informáticos.

Se han establecido procedimientos adecuados para dar respuesta a eventos o incidentes informáticos, basados en el marco de trabajo NIST, lo que asegura una respuesta efectiva ante situaciones de este tipo. Sin embargo, el trabajo en esta área aún está en curso y se espera mejorar aún más la efectividad de la respuesta informática. Hasta el momento se ha llevado a cabo un análisis exhaustivo de eventos e incidentes de ciberseguridad en la UNAD, permitiendo identificar vectores comunes de exposición al riesgo informático.

Referencias

Axelos (2019). ITIL | IT Service Management. https://www.axelos.com/certifications/itil-service-management

Dansimp *et al.* (24 de abril de 2023). Incident response playbooks. https://learn.microsoft.com/en-us/security/operations/incident-response-playbooks

Fauziyah, F., Wang, Z., & Joy, G. (2022). Knowledge Management Strategy for Handling Cyber Attacks in E-Commerce with Computer Security Incident Response Team (CSIRT). *Journal of Information Security, 13*(4), Article 4. https://doi.org/10.4236/jis.2022.134016

Giraldo Gallo, J. F. (s. f.). *Infraestructuras críticas cibernéticas en Colombia.* Gobierno de Colombia. https://www.ccit.org.co/wp-content/uploads/sesion-5-panel-infraestructuras-criticas-ciber-en-colombia.pdf

Haidar, M., Sucahyo, Y. G., Sukardi, T., & Gandhi, A. (2021). Analysis of Csirt Services in Facing Cyber Security Challenges in Indonesia. *2021 4th International Conference on Information and Communications Technology (ICOIACT),* 154-159. https://doi.org/10.1109/ICOIACT53268.2021.9563925

Harán, J. M. (3 de noviembre de 2020). Falta de profesionales en ciberseguridad: una brecha que crece. (s. f.). *Welivesecurity.* https://www.welivesecurity.com/la-es/2020/11/03/falta-profesionales-ciberseguridad-brecha-que-crece/

Hollenberger, J. (2023, mayo 2). A Guide to Incident Response Plans, Playbooks, and Policy. *CISO Collective. Fortinet Blog*. https://www.fortinet.com/blog/ciso-collective/incident-response-plans-playbooks-policy

IBM (s.f.). Costo de una filtración de datos 2023. de https://www.ibm.com/mx-es/reports/data-breach

MITRE ATT&CK® (2023). https://attack.mitre.org/

OEA (2023). Guía práctica para CSIRTs. Vol. 2. https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Guia-CSIRT%202023%20ESP%20Digital.pdf

OEA (s.f.). *Manual de supervisión de riesgos cibernéticos para juntas corporativas*. https://www.oas.org/es/sms/cicte/docs/ESP-Manual-de-Supervision-de-riesgos-ciberneticos-para-juntas-coporativas.pdf

OEA. (01 de agosto de 2009). *Democracia para la paz, la seguridad y el desarrollo.* https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=AVI-095/20

Pargar, F., Kujala, J., Aaltonen, K., & Ruutu, S. (2019). Value crea-

tion dynamics in a project alliance. *International Journal of Project Management, 37*(5), 716-730. https://doi.org/10.1016/j.ijproman.2018.12.006

Pascual, D. (18 de mayo de 2021). *El libro de jugadas del adversario activo 2021*. Sophos News. https://news.sophos.com/es-419/2021/05/18/el-libro-de-jugadas-del-adversario-activo-2021-2/

Rubio, D. (2023). *Evolución del sistema de gestión de incidentes de seguridad orientado a CSIRT de la UNLP-Ngen*. (Tesis de grado). Universidad Nacional de La Plata. http://sedici.unlp.edu.ar/handle/10915/154923

Scarone, K. (2023). How to create an incident response playbook | TechTarget. Security. https://www.techtarget.com/searchsecurity/tip/How-to-create-an-incident-response-playbook

Tang, R. T. (2021). (14) Cyber Security Playbook for SOCs #10 | LinkedIn. https://www.linkedin.com/pulse/cyber-security-playbook-socs-10-ricky-tang/?trk=pulse-article_more-articles_related-content-card

Thangavelu, M., Krishnaswamy, V., & Sharma, M. (2021). Impact of comprehensive information security awareness and cognitive characteristics on security incident management – an empirical study. *Computers & Security, 109,* 102401. https://doi.org/10.1016/j.cose.2021.102401

Vela Espín, F. (2021). Directrices y sus desafíos en la implementación del CSIRT en Ecuador. En: M. S. Botto-Tobar, O. Gómez, R. Rosero Miranda, A. Díaz Cadena (eds.). *Advances in Emerging Trends and Technologies. ICAETT 2020. Advances in Intelligent Systems and Computing*. Vol. 1302. Springer. https://doi.org/10.1007/978-3-030-63665-4_19

Yelevin *et al.* (2023, junio 21). Automatización de la respuesta a amenazas con cuadernos de estrategias en Microsoft Sentinel. https://learn.microsoft.com/es-es/azure/sentinel/automate-responses-with-playbooks

Zurkus, K. (2018, octubre 8). Does Your SOC Have a Security Playbook? Security Intelligence. https://securityintelligence.com/does-your-soc-have-a-security-playbook/