REVISTA CIENTÍFICA GUACAMAYA

Vol.10| N.º 2| abril – septiembre 2026| ISSN 2616-9711

pp. 8-16

Ciberseguridad industrial en Panamá: herramientas, brechas y agenda futura

Industrial Cybersecurity in Panama: Tools, Gaps, and a Future Agenda

[1.] Reynaldo Castillo, [2.] Miguel Vargas-Lombardo, [3.] Huriviades Calderón-Gómez, [4.] Cristian Moreno-De La Cruz

[1.] Universidad Tecnológica de Panamá, Facultad de Ingeniería en Sistemas Computacionales, Panamá

reynaldo.castillo@utp.ac.pa, https://orcid.org/0009-0009-0316-0599

[2.] Universidad Tecnológica de Panamá, Facultad de Ingeniería en Sistemas Computacionales, Panamá.

miguel.vargas@utp.ac.pa, https://orcid.org/0000-0002-2074-2939

[3.] Universidad Tecnológica de Panamá, Facultad de Ingeniería en Sistemas Computacionales, Panamá.

huriviades.calderon@utp.ac.pa, https://orcid.org/0000-0002-6118-1154

[4.] Universidad Tecnológica de Panamá, Facultad de Ingeniería en Sistemas Computacionales, Panamá.

cristian.moreno@utp.ac.pa, https://orcid.org/0000-0002-9315-648X

Recibido: 27/10/2025 - Aceptado: 11/2/2026

DOI https://doi.org/10.48204/j.guacamaya.v10n2.a9789

Resumen

El estudio analiza el estado de la ciberseguridad industrial en Panamá y la utilidad real de las herramientas de protección en redes de información y sistemas de control industrial (SCI). Se adopta un enfoque mixto que combina una revisión de literatura reciente y una encuesta exploratoria aplicada a once profesionales del sector. Los hallazgos evidencian una paradoja operacional: aunque el 100% de las organizaciones declara que la ciberseguridad es prioritaria, solo el 63,6% reporta contar con planes de contingencia y el 63,6% indica políticas de acceso formalizadas. Asimismo, el 27,3% ha experimentado vulnerabilidades y el 45,5% ha debido resolver brechas de seguridad. Estas cifras sugieren una brecha sistémica entre la intención estratégica y la ejecución táctica. En términos de impacto actual, la adopción de SIEM, IDS/IPS, segmentación de redes y actualización de parches se asocia con mejoras en detección y respuesta, pero persisten limitaciones relativas a interoperabilidad, integración con sistemas heredados y capacidades del talento humano. Como proyección, se propone una agenda futura basada en cinco ejes: (i) madurez por dominios según NIST CSF; (ii) ingeniería de seguridad por diseño en SCI; (iii) telemetría unificada y XDR con analítica avanzada; (iv) programas de gestión del cambio y cultura de ciberseguridad; y (v) medición de riesgo operacional con indicadores líderes y rezagados. El trabajo contribuye con evidencia local y una hoja de

Vol.10| N.º 2| abril – septiembre 2026| ISSN 2616-9711

ruta de mejora continua que permite contrastar el impacto actual con el potencial de reducción de riesgo al institucionalizar prácticas de seguridad de última generación.

Palabras clave: ciberseguridad industrial; sistemas de control industrial (SCI); SIEM; IDS/IPS; gestión de riesgos.

Abstract

This study examines the state of industrial cybersecurity in Panama and the real-world effectiveness of security tools for information networks and industrial control systems (ICS). A mixed-methods approach combines a recent literature review with an exploratory survey of eleven industry professionals. Results reveal an operational paradox: although 100% of organizations state that cybersecurity is a priority, only 63.6% report contingency plans and 63.6% formal access policies. Moreover, 27.3% have experienced vulnerabilities and 45.5% have had to remediate security breaches. These figures suggest a systemic gap between strategic intent and tactical execution. In terms of current impact, SIEM, IDS/IPS, network segmentation, and patch management are associated with improved detection and response, yet limitations persist regarding interoperability, legacy integration, and workforce capabilities. Looking forward, a five-pillar agenda is proposed: (i) domain maturity using the NIST CSF; (ii) security-by-design engineering for ICS; (iii) unified telemetry and XDR with advanced analytics; (iv) organizational change and security culture; and (v) operational risk measurement with leading and lagging indicators. The paper provides local evidence and a roadmap for continuous improvement that contrasts current impact with the potential risk reduction achieved by institutionalizing state-of-the-art security practices.

Keywords: industrial cybersecurity; industrial control systems (ICS); SIEM; IDS/IPS; risk management.

Introducción

La aceleración de la transformación digital y la convergencia TI/TO han multiplicado la superficie de ataque de los sistemas de control industrial (SCI), al tiempo que han incrementado la complejidad de su gobierno técnico y organizacional. A diferencia de los entornos puramente informacionales, donde la confidencialidad suele dominar la función objetivo, en los SCI la disponibilidad y la seguridad física de personas, activos y procesos operativos constituyen restricciones críticas; por ello, el impacto de un incidente trasciende la pérdida de datos e incide directamente en la continuidad del negocio y la resiliencia social (Whitman & Mattord, 2009; Lee & Chen, 2019). La exposición de protocolos industriales y dispositivos de campo a redes IP y servicios remotos antes aislados o "air-gapped" ha erosionado supuestos de seguridad perimetral y obliga a adoptar enfoques de defensa multinivel y "zero trust" adecuados a las particularidades de la operación industrial (González Gallego, 2018; Johnson & Edwards, 2018).

En la literatura especializada se observa una maduración de las prácticas de seguridad hacia arquitecturas segmentadas por zonas y conductos, controles preventivos y detectivos en profundidad, y capacidades de telemetría centralizada que habilitan detección y respuesta en tiempo (casi) real. De forma operativa, esto se traduce en el despliegue coordinado de IDS/IPS, SIEM y, más recientemente, XDR y analítica avanzada sobre telemetría unificada, junto con la gestión rigurosa de parches, listas blancas y hardening de PLC/SCADA, HMI y redes industriales (Soucase Iranzo, 2021; Smith, 2018; Ramírez Quevedo, 2024). A nivel de gobernanza, los marcos de referencia de mayor adopción como National Institute of Standards and Technology (NIST)

Vol.10| N.º 2| abril – septiembre 2026| ISSN 2616-9711

Cybersecurity Framework (CSF) en su versión más reciente promueven ciclos de mejora continua que integran identificación, protección, detección, respuesta y recuperación, con métricas de desempeño y riesgo operacional para alinear prioridades con el apetito de riesgo de la organización (NIST, 2024; López & Pérez, 2017).

No obstante, persisten brechas sociotécnicas que limitan el impacto de dichas prácticas: la interoperabilidad con bases instaladas heterogéneas, la integración con sistemas heredados, la disponibilidad de talento especializado y la consolidación de una cultura de ciberseguridad capaz de sostener el cambio organizacional (Brown & Evans, 2019; Cavelty, 2008). Estas brechas se manifiestan en asimetrías entre la prioridad estratégica declarada y la ejecución táctica efectiva: las organizaciones asignan alta prioridad a la ciberseguridad, pero muestran niveles dispares en políticas de acceso, planes de contingencia, cobertura de parches y práctica de ejercicios de respuesta (García, 2019; García & col., 2020).

En este contexto, el presente trabajo aporta evidencia empírica local y una agenda de cierre de brechas. Metodológicamente, combina revisión de literatura reciente con una encuesta exploratoria a profesionales del sector industrial en Panamá (n=11), cuyos hallazgos permiten contrastar el estado actual de adopción de controles (p. ej., SIEM, IDS/IPS, segmentación, gestión de parches) con las exigencias de marcos de referencia y mejores prácticas (Mercado Páez, 2019; Ramírez Quevedo, 2024; NIST, 2024). Con base en estos resultados, se propone una hoja de ruta en cinco ejes madurez por dominios (CSF), seguridad por diseño en SCI, telemetría unificada/XDR, gestión del cambio y cultura, e indicadores líderes/rezagados (p. ej., MTTD, MTTR, cobertura de parches en activos críticos) orientada a reducir de manera medible la probabilidad e impacto de incidentes en infraestructuras críticas (Smith, 2018; Soucase Iranzo, 2021). La sección de Materiales y Métodos detalla el enfoque adoptado y la sección de Resultados y Discusión contrasta la prioridad declarada con la capacidad operativa observada en el caso panameño.

Materiales y Métodos

Diseño del estudio. Se adoptó una investigación con enfoque mixto (cuantitativo y cualitativo), de alcance exploratorio–descriptivo con un diseño no experimental y de corte transversal, integrado por dos componentes: (i) una revisión de literatura sobre herramientas y prácticas de ciberseguridad en redes industriales y sistemas de control industrial (SCI), y (ii) una encuesta estructurada aplicada a profesionales del sector industrial en Panamá. Este enfoque permitió contrastar el estado del arte con la evidencia local de adopción de controles y prácticas de gobernanza (López & Pérez, 2017; Lee & Chen, 2019; NIST, 2024).

Revisión de literatura. La búsqueda abarcó el período 2018–2025 en bases y catálogos académicos (IEEE Xplore, Scopus, ACM Digital Library, ScienceDirect y SpringerLink), empleando combinaciones de términos en español e inglés: industrial cybersecurity, industrial control systems, ICS security tools, SIEM, IDS/IPS, network segmentation, XDR, risk management, NIST CSF, ISO/IEC 27001 y equivalentes. Se incluyeron artículos revisados por pares, libros y actas de congreso con aplicación explícita a contextos industriales o a marcos de referencia (NIST CSF, ISO/IEC 27001). Se excluyeron trabajos puramente conceptuales sin vinculación con SCI, documentos redundantes o fuera de alcance. La extracción se centró en: (a) categorías de control (p. ej., segmentación por zonas y conductos; hardening; gestión de parches; SIEM/IDS/IPS/XDR), (b) mecanismos de gobierno y métricas (funciones del CSF e

Vol.10| N.º 2| abril – septiembre 2026| ISSN 2616-9711

indicadores de riesgo), y (c) factores sociotécnicos (cultura, talento, interoperabilidad) (Whitman & Mattord, 2009; González Gallego, 2018; Smith, 2018; Soucase Iranzo, 2021; Hidalgo Martínez, 2023; Ramírez Quevedo, 2024; NIST, 2024).

Encuesta y participantes. El segundo componente consistió en una encuesta estructurada dirigida a profesionales con responsabilidades en operaciones, tecnología o seguridad en organizaciones industriales panameñas. Se utilizó un muestreo no probabilístico por conveniencia y cadenas de referencia (snowball) a través de redes profesionales. La muestra final estuvo compuesta por once (n = 11) participantes que cumplieron los criterios de inclusión (experiencia demostrable en entornos TI/TO o SCI y residencia laboral en Panamá).

Instrumento y operacionalización. El cuestionario incluyó ítems cerrados (respuestas Sí/No/Tal vez, según aplicara), alineados con dominios y funciones de NIST CSF y con prácticas del SGSI ISO/IEC 27001 (Hidalgo Martínez, 2023; NIST, 2024). Las variables observadas fueron: prioridad institucional de la ciberseguridad; existencia de planes de contingencia; políticas de control y gestión de accesos; experiencias con vulnerabilidades; y experiencias de resolución de brechas. La validez de contenido se aseguró mediante juicio de tres expertos (profesionales de ciberseguridad industrial), quienes evaluaron claridad, pertinencia y cobertura según los constructos teóricos (Brown & Evans, 2019; Johnson & Edwards, 2018). Previo al levantamiento, se realizó una prueba piloto con dos profesionales para verificar la comprensión de los ítems y el flujo del formulario.

Procedimiento de recolección. La encuesta se administró en línea, de forma anónima y voluntaria, informando el objetivo del estudio y las garantías de confidencialidad. No se recopilaron datos personales sensibles ni identificadores directos. El cuestionario permaneció abierto el tiempo suficiente para completar la muestra prevista (n = 11).

Análisis de datos. Se aplicó estadística descriptiva con cálculo de porcentajes y conteos para cada ítem (n = 11). Para efectos de contraste coherente con el objetivo de revelar brechas entre prioridad declarada y ejecución táctica se calcularon diferenciales (“brechas”) entre proporciones de intención estratégica y adopción efectiva de controles (p. ej., diferencia entre la proporción que declara la ciberseguridad como prioritaria y la proporción que reporta planes de contingencia o políticas de acceso) (Smith, 2018; Soucase Iranzo, 2021; Ramírez Quevedo, 2024). El procesamiento se efectuó con hojas de cálculo y scripts reproducibles; las Figuras 1–5 se generaron a partir de la agregación de respuestas y reflejan la distribución porcentual por ítem.

Aspectos éticos. Dado el carácter no experimental y el uso de respuestas anónimas, el estudio se enmarca en riesgo mínimo. Se garantizó el consentimiento informado al inicio de la encuesta y la protección de la confidencialidad de los participantes, en línea con buenas prácticas para estudios en ciberseguridad organizacional (Cavelty, 2008; Johnson & Edwards, 2018).

Limitaciones metodológicas. Como estudio exploratorio con muestra pequeña y no probabilística, los hallazgos no son generalizables a todo el sector industrial panameño; sin embargo, proporcionan señales empíricas útiles para (i) priorizar ejes de mejora y (ii) diseñar estudios confirmatorios de mayor escala, combinando métricas operativas (MTTD, MTTR, cobertura de parches) con auditorías técnicas y análisis de logs en SIEM/IDS/XDR (Lee & Chen, 2019; NIST, 2024).

Resultados y Discusión

Se confirma consenso declarativo sobre la prioridad de la ciberseguridad (100%; 11/11), (Figura1). No obstante, tal como se observa en la Tabla 1, el 63,6% reporta planes de

Vol.10| N.º 2| abril – septiembre 2026| ISSN 2616-9711

contingencia y el 63,6% políticas formales de acceso, lo que revela una brecha de ejecución del 36,4%. Adicionalmente, el 27,3% ha experimentado vulnerabilidades y el 45,5% ha resuelto brechas, lo que sugiere exposición residual y capacidad reactiva heterogénea. Este patrón es consistente con organizaciones que han adoptado controles de primera ola (segmentación básica, SIEM, IDS/IPS) pero aún carecen de una gestión integral de riesgos, pruebas de intrusión periódicas y automatización de respuesta.

Contrastando el impacto actual con el alcance futuro, la madurez puede incrementarse mediante: (i) gobierno multidominio alineado a NIST CSF (identificar-proteger-detectar-responder-recuperar); (ii) ingeniería segura por diseño en PLC/SCADA y segmentación con zonas y conductos; (iii) telemetría convergente TI/TO con correlación avanzada (UEBA, ML) y XDR; (iv) programas de cultura y capacitación con métricas de adopción; y (v) métricas operacionales (MTTD/MTTR, tasa de incidentes de severidad alta, cumplimiento de parches en activos críticos). Estas acciones permitirían reducir la probabilidad y el impacto de incidentes y cerrar la brecha entre intención y práctica observada en la encuesta.

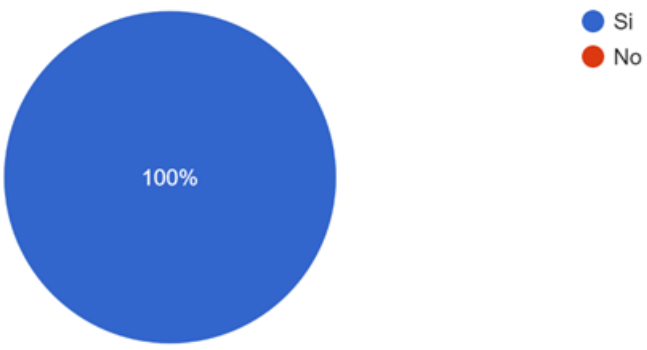
Tabla 1

Resumen de resultados de la encuesta

Ítem	Categoría	Porcentaje	Conteo (N)
Prioridad institucional de ciberseguridad	Sí	100.0%	11
Plan de contingencia	Sí / No / Tal vez	63.6% / 27.3% / 9.1%	7 / 3 / 1
Políticas de acceso	Sí / No	63.6% / 36.4%	7 / 4
Experiencia con vulnerabilidades	Sí / No	27.3% / 72.7%	3 / 8
Resolución de brechas	Sí / No / Tal vez	45.5% / 36.4% / 18.2%	5 / 4 / 2

Figura 1

Importancia institucional de la ciberseguridad (Sí=100%)



Vol.10| N.º 2| abril – septiembre 2026| ISSN 2616-9711

Figura 2

Existencia de plan de contingencia (Sí/No/Tal vez).

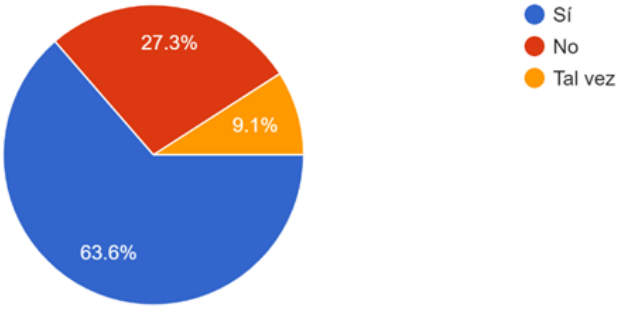


Figura 3

Políticas de acceso a la red industrial (Sí/No).

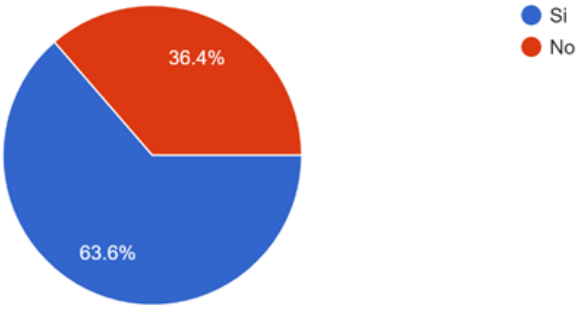
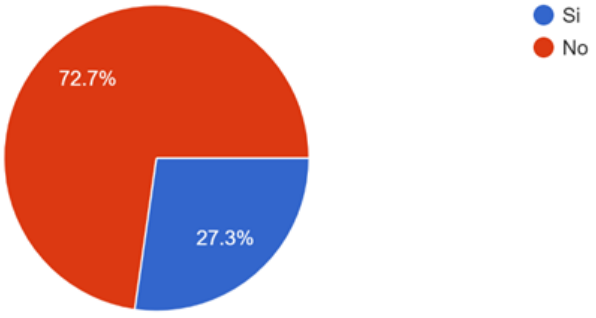


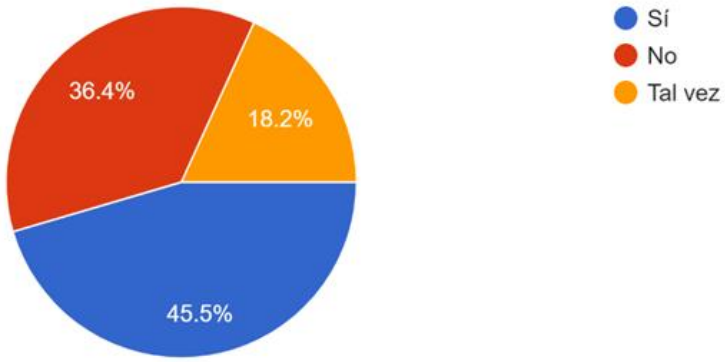
Figura 4

Experiencia con vulnerabilidades (Sí/No).



Vol.10| N.º 2| abril – septiembre 2026| ISSN 2616-9711

Figura 5
Experiencia resolviendo brechas (Sí/No/Tal vez).



Conclusiones

La evidencia empírica local confirma una coherencia estratégica respecto a la prioridad de la ciberseguridad industrial, pero también una ejecución incompleta de controles clave en los SCI panameños. Aunque la totalidad de las organizaciones encuestadas declara la ciberseguridad como prioritaria, persisten brechas de implementación en planes de contingencia y políticas de acceso (36,4 puntos porcentuales frente a la prioridad declarada), así como experiencias no triviales de vulnerabilidades y remediación de brechas. Este desalineamiento entre intención y capacidad operativa es consistente con lo reportado en la literatura para entornos con base instalada heterogénea y restricciones operativas de alta criticidad (Lee & Chen, 2019; Brown & Evans, 2019).

Desde una perspectiva técnico-organizacional, los hallazgos sugieren que el despliegue de controles de primera ola (p. ej., SIEM, IDS/IPS, segmentación) debe integrarse en un programa de seguridad por diseño para SCI, con gestión orquestada de parches, telemetría convergente TI/TO y gobernanza alineada a marcos de referencia como NIST CSF. Tal integración habilita ciclos de mejora continua sobre las funciones Identificar-Proteger-Detectar-Responder-Recuperar, soportados en indicadores líderes y rezagados (p. ej., MTTD, MTTR, cobertura de parches en activos críticos, tasa de incidentes de alta severidad), lo cual incrementa la capacidad de anticipación, contención y recuperación ante eventos disruptivos (NIST, 2024; Smith, 2018; Soucase Iranzo, 2021; Ramírez Quevedo, 2024).

El contraste antes/después propuesto por la agenda de mejora permite establecer metas operativas verificables: (antes) prioridad declarada alta con controles disparejos y respuesta predominantemente reactiva; (después) madurez por dominios con objetivos cuantificados p. ej., cobertura de parches >90 % en activos críticos en ≤60 días, MTTD < 4 h y MTTR < 24 h, planes de contingencia y pruebas en ≥85 % de las unidades operativas, y políticas de acceso formalizadas y auditables. En términos de impacto, estas metas se asocian con una reducción esperada tanto de la probabilidad como del impacto de incidentes, contribuyendo a la resiliencia operativa y a la continuidad del negocio en infraestructuras críticas (Whitman & Mattord, 2009; López & Pérez, 2017).

En el plano científico y práctico, el estudio aporta: (i) evidencia local reciente sobre adopción de controles en SCI; (ii) una operacionalización mínima de brechas (intención vs. ejecución) que puede replicarse con muestras mayores; y (iii) una hoja de ruta de cinco ejes (madurez CSF, seguridad por diseño, telemetría/XDR, cultura y gestión del cambio,

Vol.10| N.º 2| abril – septiembre 2026| ISSN 2616-9711

e indicadores de riesgo) para orientar inversiones y priorización. Limitaciones como el tamaño muestral y el muestreo no probabilístico invitan a estudios confirmatorios multi-sectoriales que integren métricas operativas, telemetría real (SIEM/IDS/XDR) y auditorías técnicas longitudinales, así como análisis de costo-beneficio y modelos de riesgo específicos por proceso industrial (Lee & Chen, 2019; NIST, 2024).

En síntesis, la agenda propuesta habilita un incremento medible de madurez y una reducción del riesgo alineada con estándares contemporáneos; su adopción progresiva, con supervisión de indicadores y aprendizajes iterativos, se perfila como condición necesaria para sostener la seguridad de personas, activos y servicios esenciales en el contexto panameño (NIST, 2024; Smith, 2018; Soucase Iranzo, 2021).

Referencias

Brown, K., & Evans, T. (2019). Building a cybersecurity culture in industrial environments. Journal of Industrial Security, 8(2), 77–89.

Cavelty, M. D. (2008). Cyber-security and threat politics. Routledge.

C, A., & Doe, B. (2020). Challenges in implementing security tools in industrial networks. International Conference on Industrial Security, 110–125.

García, M. P. (2019). Impact of vulnerabilities in industrial control systems security. International Journal of Industrial Engineering, 56–71.

González Gallego, I. (2018). Estudio de la ciberseguridad industrial: Pentesting y laboratorio de pruebas de concepto. Universidad Politécnica de Madrid.

Hidalgo Martínez, W. D. (2023). Evaluación de riesgos para un SGSI con base en ISO/IEC 27001 aplicado a un proveedor de servicios de internet.

Johnson, R., & Edwards, P. (2018). Ethical considerations in implementing security tools in industrial environments. Journal of Cyber Ethics, 25, 332–345.

Lee, F., & Chen, L. (2019). Challenges and opportunities of machine learning in ICS security. IEEE Transactions on Industrial Informatics, 25(4), 321–335.

López, R., & Pérez, J. (2017). Avances en ciberseguridad industrial. Ediciones UPC.

Mercado Páez, M. (2019). Descripción y análisis de los desafíos para la generación de ventajas competitivas basadas en big data y analytics en telecomunicaciones.

National Institute of Standards and Technology. (2024.). *Cybersecurity Framework*. https://www.nist.gov/cyberframework

Ramírez Quevedo, L. (2024). Tecnologías de defensa frente a inteligencia de amenazas y ciberataques. InnDev, 3(1), 127–141.

Smith, A. J. (2018). Evaluating the efficacy of security tools in protecting industrial control systems. Journal of Cybersecurity, 123–137.

Soucase Iranzo, A. (2021). Implementación de un sistema IPS en un modelo de red industrial. Universitat Politècnica de València.

Whitman, M., & Mattord, H. (2009). Principios de seguridad de la información. Cengage Learning.