

Abad Bautista, L., Patiño García, G. C., Blancas Nuñez, D. V., & Chamoli Falcón, A. W. (2025). Desmitificando el ethical hacking: consideraciones culturales en economías emergente. En A. B. Benalcázar (Coord). *Enfoques Interdisciplinarios en Ciencias Sociales. Análisis de Problemáticas Contemporáneas (Volumen III)* (pp. 83-99). Religación Press. <http://doi.org/10.46652/religacionpress.316.c563>



Capítulo 4

Desmitificando el ethical hacking: consideraciones culturales en economías emergentes

Leonor Abad Bautista, Guiceli Codina Patiño García, Diana Veronica Blancas Nuñez, Andy Williams Chamoli Falcón

Resumen

El panorama actual de la ciberseguridad, caracterizado por el aumento sostenido de ciberataques, subraya la imperiosa necesidad de adoptar prácticas de ethical hacking en los países en vías de desarrollo. El presente estudio tiene como propósito examinar las consideraciones culturales y sociales que inciden en la consolidación de una cultura de ethical hacking que sea tanto responsable como ética en estos contextos. Mediante una revisión bibliográfica, se analizaron diversas fuentes científicas y estudios recientes que abordan la interrelación entre cultura, sociedad y ciberseguridad. Los hallazgos revelan que las percepciones culturales, las estrategias educativas y las normas sociales desempeñan un papel determinante en la aceptación y práctica del ethical hacking, así como en la superación de los obstáculos culturales que dificultan su implementación. Esta investigación pone de manifiesto la necesidad de diseñar e implementar enfoques que integren dichas dimensiones culturales en los programas de fortalecimiento de la ciberseguridad. En conclusión, los resultados sugieren que el éxito de las iniciativas orientadas al ethical hacking no dependerá exclusivamente de las competencias técnicas, sino también de una comprensión profunda de los factores culturales y sociales que moldean su adopción. Este enfoque integrador abre nuevas líneas de investigación en un campo de creciente relevancia global.

Palabras clave: cultura; ethical hacking; percepción; responsabilidad social; educación

Introducción

En el escenario actual, donde todo está digitalizándose cada vez más rápido, el *ethical hacking* se ha vuelto algo clave para reducir ciberataques y mejorar la seguridad digital, sobre todo en países que están en vías de desarrollo. La creación de una cultura de *ethical hacking*, que sea coherente con principios éticos y responsables, se enfrenta a muchos desafíos de tipo cultural y social que hay que entender a fondo. El *ethical hacking*, que básicamente es cuando se hacen pruebas de seguridad controladas en sistemas informáticos para encontrar y corregir fallos, no solo necesita conocimientos técnicos, sino también una fuerte base ética (Toro et al., 2023). Por eso, meter todos estos elementos en la formación de los expertos en ciberseguridad es fundamental si lo que se busca es tener un marco fiable, basado en la integridad y el respeto profesional.

La verdad es que, según varios estudios, los factores culturales y sociales influyen mucho, ya que lo ético depende también de cosas como la educación, las normas sociales o incluso la manera en que la tecnología se percibe en cada país (Antonio, 2024). Esto, más que todo, se nota en países emergentes, que tienen culturas muy diversas y donde estas cosas afectan bastante en cómo se acepta y se aplica el *ethical hacking*. Varios autores ya han dicho que, si se ignoran estos aspectos, se pueden cometer errores o incluso tener prácticas no adecuadas que dañan la imagen del profesional y afectan la seguridad digital (Toro et al., 2023).

Otras investigaciones han dicho que hay que tener reglas claras y estructuras de gobernanza que no solo regulen, sino que también promuevan un entorno ético en el uso de tecnologías como esta (Estrada et al., 2021). En ese sentido, tanto una buena gobernanza como que la sociedad participe activamente, son puntos clave. Si los profesionales cuentan con principios éticos bien definidos, es menos probable que actúen por interés personal o por presiones externas que pongan en peligro la privacidad de los usuarios o la integridad del sistema (Rocha et al., 2023).

Estudiar más a fondo cómo la cultura y los aspectos sociales influyen en el *ethical hacking* no solo ayuda a cerrar huecos en la literatura, sino que también podría servir para armar políticas públicas o programas de capacitación que promuevan una cultura ética en seguridad digital. Entender todos estos factores es clave para empoderar a los que trabajan en ciberseguridad, especialmente en países en desarrollo, con el fin de tener espacios digitales más seguros y justos.

En estos últimos diez años, el interés por el *ethical hacking* ha crecido mucho en países emergentes, gracias al avance de la digitalización y el desarrollo de infraestructura tecnológica. Pero su implementación no es tan simple porque hay obstáculos sociales y culturales que complican todo. Esta revisión bibliográfica

busca analizar esas dinámicas con más detalle, para entender cómo podrían influir en la forma en que se adopta el *ethical hacking*.

La bibliografía reciente empieza a mostrar cómo la cultura organizacional y los factores sociales influyen en las buenas prácticas de ciberseguridad. Un ejemplo es lo que dicen Zyoud y Lutfi (2024), quienes encontraron una relación directa entre una buena cultura de seguridad en las empresas y la aplicación de estas prácticas en Emiratos Árabes Unidos. Eso indica que cuando las condiciones institucionales son favorables, es más fácil aplicar el *ethical hacking*. Por otro lado, Al-Hawamleh (2024), explica que, aunque la cultura organizacional no siempre tiene un impacto directo, sí puede tener un peso importante en algunos casos, como en Arabia Saudita.

Todo esto reafirma que es fundamental conocer el entorno cultural para que cualquier programa de *ethical hacking* funcione bien. Además, hay que tener en cuenta el papel de los factores humanos en la seguridad digital. En esa línea, Nifakos et al. (2021), analizaron cómo afectan estos factores en el sector salud, y concluyeron que entrenar al personal y concientizarlos puede marcar la diferencia cuando se trata de reducir los riesgos.

A esto se suma lo que dice Al-Fatlawi (2024), quien remarca la importancia de empezar a formar en ciberseguridad desde el ámbito educativo. La educación formal, según el autor, puede ser una especie de catalizador para construir una buena cultura digital. Por eso, diseñar estrategias de enseñanza que tomen en cuenta la cultura local en países emergentes se ve como un camino útil para facilitar la aceptación del *ethical hacking*.

También está el planteamiento de Sadeghi et al. (2023), que dicen que una cultura institucional enfocada en la seguridad influye directamente en cómo se comportan los empleados frente a los riesgos informáticos. Eso refuerza la idea de que una buena cultura organizacional no debe limitarse a poner normas, sino que también debe ser asumida personalmente por los trabajadores. Entonces, incluir estos componentes culturales y sociales dentro del *ethical hacking* se vuelve algo clave para que sea legítimo y se mantenga en el tiempo.

Donde los estudios más recientes coinciden en que cosas como la cultura organizacional, la educación y la formación profesional son determinantes para construir una cultura ética en el hacking. Este artículo de revisión quiere meterse más en esas dimensiones, para aportar ideas que ayuden a implementar estas prácticas en países que aún están desarrollándose.

Sin embargo, la literatura académica sobre este tema todavía está en pañales, y faltan muchos estudios teóricos y prácticos que analicen en serio los aspectos culturales y sociales relacionados con el *ethical hacking* en países emergentes. Aunque hay textos que ya hablaron de cuestiones técnicas y legales, la parte ética y cultural casi no se ha tocado.

Según Hegde et al. (2022), sostiene que los principios éticos pueden variar mucho según el lugar, pero no entran a fondo en cómo eso afecta al *ethical hacking* en países en desarrollo. Lo mismo pasa con Momeni et al. (2022), que hablan de ética en odontología, pero solo desde ángulos muy puntuales, sin ver cómo eso se puede aplicar a la ciberseguridad.

Además, Carvalho et al. (2024), en su trabajo sobre ingeniería de software en Brasil, muestran que no hay un marco claro que una la cultura empresarial con principios éticos sólidos. Esa misma falta de enfoque pasa también en el mundo del *ethical hacking*, lo que dificulta el diseño de buenas estrategias para hacerlo realidad.

También Alshawabkeh (2023), resalta el papel del liderazgo ético dentro de las organizaciones, aunque ese enfoque ha sido más explorado en empresas tradicionales y no tanto en el campo del *ethical hacking*, lo cual deja un vacío importante.

Y por último, hay estudios como el de Hess et al. (2023), que se enfocan en ética digital, pero lo hacen en sectores industriales concretos, sin mirar las necesidades específicas de los países emergentes. Esa falta de atención a lo local frena el desarrollo de propuestas que realmente se adapten a esos contextos.

Por eso, este artículo se propone llenar esos vacíos mediante un análisis riguroso que tenga en cuenta lo cultural y lo social en la adopción del *ethical hacking* en contextos emergentes, aportando así a crear mejores estrategias de seguridad digital adaptadas a esas realidades.

El objetivo del artículo es, entonces, analizar cómo los factores sociales y culturales influyen en que se adopte una cultura de *ethical hacking* en países en vías de desarrollo. Esto tiene que ver con llenar vacíos que todavía existen en los estudios actuales y avanzar hacia un conocimiento más completo del tema, resaltando por qué es urgente integrar el componente cultural en la formación y las estrategias relacionadas con el *ethical hacking*.

Metodología

Para poder abordar el objetivo de analizar las consideraciones culturales y sociales que afectan en la adopción de una cultura de *ethical hacking* ética y responsable en países que están en vías de desarrollo, se llevó a cabo un proceso sistemático para buscar y seleccionar las fuentes bibliográficas más adecuadas. La recolección de la información se hizo, sobre todo, usando bases de datos académicas bastante conocidas como Scopus, IEEE Xplore, Google Scholar, SciELO, Latindex y también PubMed. Para esto se usaron combinaciones

estratégicas de palabras clave, como: “*ethical hacking*”, “*Culture*”, “*Cybersecurity*”, “*Emerging countries*” y “*Social considerations*”. Gracias a esta estrategia de búsqueda, fue posible encontrar estudios relevantes que hayan sido publicados más o menos en los últimos cinco años, asegurando así que los hallazgos estén actualizados y que reflejen lo que se viene discutiendo actualmente sobre el *ethical hacking* y cómo se relaciona con lo cultural y lo social.

Durante la parte de selección de los estudios, se le puso énfasis a que las publicaciones tuvieran una buena calidad científica y que estén relacionadas con la temática del estudio. Como criterios de inclusión, se consideraron trabajos —tanto teóricos como aplicados— que abordaran directa o indirectamente la relación entre el *ethical hacking* y los factores culturales o sociales. También se tomaron en cuenta aquellas investigaciones que exploran cómo estas dimensiones pueden afectar la forma en que se implementan políticas de ciberseguridad en países emergentes. Igualmente, se incluyeron algunas revisiones bibliográficas o sistemáticas que aportan una mirada crítica sobre el estado actual de este tema.

En cambio, los criterios de exclusión se aplicaron a los artículos que no cumplían con ciertos mínimos de calidad académica, como, por ejemplo, los que no estaban revisados por pares o que tenían una metodología muy floja. También se dejaron de lado las publicaciones que solo se enfocaban en lo técnico del *ethical hacking*, sin entrar en el contexto social o cultural, ya que no ayudaban mucho al propósito que tiene este trabajo. Gracias a esta selección más precisa, se logró delimitar el corpus a estudios que realmente aportaran a entender de qué forma las variables culturales y sociales influyen en la forma en que se adopta o se legitima el *ethical hacking* en estos entornos donde todavía hay muchas brechas digitales y culturales.

Resultados

Pregunta de investigación 1: ¿Cuáles son las percepciones culturales sobre el *Ethical hacking* entre los jóvenes en países emergentes?

Percepciones culturales del ethical hacking.

El estudio de Noordegraaf y Kranenbarg (2023), explora las motivaciones y también las percepciones que tienen los jóvenes frente al *ethical hacking*, a partir de entrevistas cualitativas con personas que ya participan activamente en esta práctica. Gracias a esta metodología, se logró acceder a una comprensión más

profunda de las ideas culturales y sociales que los rodean. Los resultados indican que muchos de los jóvenes ven al *ethical hacking* como una herramienta útil para reforzar la ciberseguridad, pero al mismo tiempo, se enfrentan a ciertas presiones sociales que limitan su participación activa (Noordegraaf & Kranenbarg, 2023). Aun así, el estudio deja en evidencia que todavía no se entiende del todo cómo influyen exactamente los factores culturales, lo cual señala que es importante seguir investigando más este aspecto.

Por otro lado, Ige (2020), analiza las formas en que los estudiantes representan sus acciones en plataformas digitales. El estudio concluye que la forma de percibir el hacking y otras tecnologías está bastante influida por el entorno cultural y por normas sociales comunes. Aunque hay cada vez más interés por el *ethical hacking*, esas ideas sociales pueden tanto incentivar como frenar su aceptación. En conjunto, estos trabajos muestran que no basta con formar técnicamente, sino que hay que entender los marcos culturales que influyen en cómo se difunde esta práctica.

Pregunta de investigación 2: ¿Qué papel juegan los programas educativos en la promoción del ethical hacking en países emergentes?

Rol de la educación en el ethical hacking.

Melnikovas et al. (2023), analizan cómo la educación impacta en la manera en que los estudiantes se relacionan con el *ethical hacking*, para lo cual implementaron métodos de aprendizaje experiencial en un curso universitario. Los resultados mostraron que los estudiantes respondieron de manera positiva y que aumentó su interés por la ciberseguridad como campo profesional. El estudio destaca que incluir temas prácticos de *ethical hacking* en la educación superior puede ser clave para que los jóvenes se involucren más. Sin embargo, todavía no está claro cómo estos programas se ajustan a las diferencias culturales entre países.

En esa misma línea, Shakeel et al. (2024), insisten en la importancia de incorporar valores éticos en la educación, y advierten que, si no se tiene en cuenta el contexto cultural, estos programas pueden ser poco efectivos. Esta falta de adaptación deja ver que es necesario adecuar los contenidos educativos para que respondan a las características sociales de cada país emergente.

Pregunta de investigación 3: ¿Cuáles son las barreras culturales que enfrentan los profesionales al adoptar el ethical hacking en entornos laborales en países emergentes?

Barreras culturales en el ethical hacking.

Patra y Lenka (2023), investigan los límites culturales que encuentran las organizaciones en países emergentes cuando intentan implementar prácticas éticas. Usando un enfoque empírico, identificaron varias barreras, como la falta de respaldo organizacional y de cultura interna favorable al *ethical hacking*. A pesar de estos hallazgos, todavía hace falta profundizar en cómo estas barreras operan en países específicos.

También Winter y Chico (2023), señalan que la resistencia cultural es un obstáculo importante para adoptar innovaciones tecnológicas, incluyendo prácticas de ciberseguridad. En ambos estudios se coincide en que estas barreras culturales deben ser reconocidas y estudiadas con mayor detalle si se quiere facilitar el uso del *ethical hacking* en entornos laborales con características culturales diversas.

Pregunta de investigación 4: ¿De qué manera influyen las creencias y normas sociales en la práctica del ethical hacking?

Influencia de las normas sociales en el ethical hacking.

D'Avanzo et al. (2021), se enfocan en cómo las normas sociales se relacionan con la conducta ética dentro de las organizaciones. El estudio demuestra que las creencias compartidas en un entorno influyen bastante en la aceptación de comportamientos éticos, entre ellos los ligados al hacking. Sin embargo, se señala que todavía hay poca investigación comparativa entre distintos países emergentes.

De manera similar, Facca et al. (2020), sostienen que las normas sociales que dominan en un país o institución afectan directamente la voluntad de las personas de participar en prácticas éticas. En conjunto, estos hallazgos apuntan a la necesidad de construir marcos teóricos que permitan entender mejor cómo influyen las normas y creencias sociales en la práctica del *ethical hacking*.

Pregunta de investigación 5: ¿Qué mecanismos de regulación existen y cómo afectan la percepción del ethical hacking?

Regulación y percepción del ethical hacking.

Majrashi (2024), estudia cómo las políticas públicas y las normativas en ciberseguridad pueden moldear la percepción del ethical hacking en el ámbito profesional. Mediante casos prácticos en varios sectores, concluye que la existencia o no de regulaciones claras afecta directamente la forma en que se valora esta práctica. Aunque el estudio es relevante, no se profundiza en cómo varía esto según el país o el entorno cultural. Por su lado, Oke et al. (2020), señalan que las regulaciones también pueden influir en el deseo de las personas de adoptar estas prácticas. Por eso, conocer bien los marcos legales y ajustarlos al contexto de cada país podría ayudar a fomentar una mejor recepción del Ethical hacking en esos lugares.

Pregunta de investigación 6: ¿Cuál es la relación entre la ética profesional y el ethical hacking en países emergentes?

Ética profesional en el ethical hacking.

El trabajo de Al-Hawamleh (2024), se centra en cómo la ética profesional influye en las decisiones relacionadas con la ciberseguridad. A través de encuestas y entrevistas, se identificó que, aunque hay conciencia sobre la importancia de la ética, existen diferencias de criterio entre los profesionales, especialmente por falta de referencias adaptadas a los países emergentes.

Por otro lado, D'Allura et al. (2023), examinan cómo se usan los códigos éticos en empresas familiares y sostienen que, para que sean efectivos, hay que tener en cuenta las dinámicas culturales propias. Aunque no se enfocan en hacking específicamente, sus hallazgos se pueden aplicar, ya que resaltan la necesidad de entender cómo la ética profesional cambia según el sector y el país.

Pregunta de investigación 7: ¿Cómo pueden las iniciativas de responsabilidad social influir en la adopción de prácticas de ethical hacking?

Responsabilidad social y ethical hacking.

Liopa et al. (2023), estudian cómo la responsabilidad social corporativa (RSC) puede influir en el comportamiento ético, enfocándose en el área de la salud. Descubren que las organizaciones que incorporan valores éticos en su cultura institucional tienden a promover actitudes más responsables. Aunque no se trata directamente del *ethical hacking*, sus conclusiones dejan ver que la RSC puede jugar un papel importante si se adapta bien al contexto cultural.

Por su parte, Ogunfowora et al. (2023), destacan que el liderazgo ético y el compromiso con la RSC fortalecen la imagen de las organizaciones y hacen que sus empleados estén más dispuestos a participar en prácticas éticas, como el *hacking* responsable. Estos estudios abren el camino para seguir explorando cómo la RSC puede ser un motor para la adopción del *ethical hacking*, sobre todo en los países que están en desarrollo.

Discusión de resultados

La revisión de los resultados obtenidos en este estudio, sobre las consideraciones culturales y sociales que influyen en la adopción de una cultura de *ethical hacking* que sea responsable y ética, particularmente en países emergentes, ha permitido identificar hallazgos que resultan bastante relevantes y que ayudan a establecer un diálogo más cercano con lo que ya se ha dicho en la literatura especializada. Para empezar, se encontró que las percepciones culturales tienen un papel bastante importante en la forma en que los jóvenes entienden y aceptan el *ethical hacking*. Esto coincide con lo que mencionan Noordegraaf y Kranenburg (2023), quienes afirman que las presiones sociales pueden actuar tanto como un incentivo como también una barrera para que los jóvenes se involucren en estas prácticas. Sin embargo, este estudio va un poco más allá, al plantear que las normas sociales predominantes y el contexto cultural más inmediato influyen de forma directa en si estas iniciativas funcionan o no, un aspecto que no siempre ha sido tratado en profundidad por estudios anteriores.

Otro punto importante que surgió tiene que ver con el rol que cumplen los programas educativos en fomentar una cultura favorable al *ethical hacking*. En sintonía con lo que señalan Melnikovas et al. (2023), se pudo observar que la educación basada en prácticas concretas en el campo de la ciberseguridad puede

tener un impacto positivo en cómo los estudiantes se interesan por desarrollar una carrera en esta área. Sin embargo, también se identificó que estos programas no deberían implementarse de forma estandarizada, sino que deben tener en cuenta las diferencias culturales de cada región. Esta idea también es respaldada por Al-Hawamleh (2024), quien remarca la necesidad de contextualizar los marcos éticos dependiendo del entorno y la disciplina donde se apliquen.

En cuanto a las barreras culturales, los hallazgos obtenidos guardan relación con lo que plantean Patra y Lenka (2023), al reconocer que existen ciertos obstáculos tanto a nivel organizacional como cultural, los cuales dificultan que se implementen prácticas éticas en los entornos laborales. A pesar de eso, este estudio pone énfasis en que aún hay una gran necesidad de indagar más sobre los mecanismos que ayuden a superar estas barreras, lo cual es una línea que no ha sido muy abordada. En este sentido, los resultados sugieren que las iniciativas de responsabilidad social empresarial podrían funcionar como catalizadores para cambiar ciertas actitudes y fomentar una mejor recepción del *ethical hacking*, ayudando así a reducir la resistencia cultural que actualmente existe en algunos contextos.

A pesar de lo valioso que han sido estos hallazgos, el estudio no está libre de limitaciones. Primero, el enfoque utilizado, al centrarse en fuentes provenientes de contextos específicos, limita un poco la posibilidad de generalizar los resultados a otros países o regiones. Esta situación podría afectar el alcance y la aplicabilidad de las conclusiones si se las traslada a realidades culturales que son muy distintas. Por otro lado, aunque se hizo un esfuerzo por seleccionar fuentes actuales y pertinentes, se reconoce que hubiera sido útil incluir más evidencia empírica, lo que habría permitido enriquecer el análisis y tener una discusión más sólida y comparativa.

Teniendo en cuenta estas limitaciones, se recomienda que los próximos estudios avancen hacia investigaciones comparativas entre distintos países emergentes, para así poder entender mejor cómo las características culturales influyen —y de qué manera— en la aceptación del *ethical hacking*. También sería recomendable analizar la efectividad de los programas de formación ética en ciberseguridad desde metodologías más diversas, incluyendo realidades distintas y distintos marcos regulatorios. Este tipo de investigaciones, sin duda, pueden aportar de forma importante al desarrollo de estrategias que estén mejor adaptadas a cada país o región, y que fortalezcan el desarrollo de entornos digitales que sean éticos y más seguros.

Además, otro eje temático que merece ser explorado en mayor profundidad es el de la evolución normativa y la regulación específica del *ethical hacking* en distintos países. Si se logra articular los estudios sobre normas jurídicas con las dimensiones culturales, se podrían establecer mejores fundamentos para

impulsar que estas prácticas sean legítimas, aceptadas y eficaces dentro de las economías emergentes.

En conclusión, lo que se ha discutido a lo largo del estudio permite reforzar la idea de que el éxito de las estrategias que promueven el *ethical hacking* no puede depender únicamente de la formación técnica. Más bien, es indispensable generar una comprensión mucho más profunda de las estructuras culturales y de las normas sociales que las rodean. Esto hará posible una implementación más efectiva, ajustada al contexto y sostenible a lo largo del tiempo en los países emergentes.

Conclusiones

Los hallazgos de esta investigación han brindado una comprensión bastante profunda sobre cómo influyen las consideraciones culturales y sociales en la adopción de una cultura de *ethical hacking* que sea responsable y ética, sobre todo en los países emergentes. Se pudo constatar que las percepciones culturales son un factor clave en la forma en que los jóvenes aceptan o no este tipo de prácticas. Este resultado pone en evidencia la necesidad de promover procesos formativos más adecuados, que estén orientados a fortalecer una cultura de ciberseguridad que no solo sea técnica, sino también sensible al contexto cultural donde se desarrolla.

Además, se identificó que tanto la responsabilidad social corporativa como la ética profesional cumplen un papel importante en cómo se configuran las actitudes hacia el *ethical hacking*. Es decir, las organizaciones que tienen principios éticos como parte de su cultura tienden a ser más abiertas a implementar este tipo de prácticas responsables en materia de seguridad digital. Estos hallazgos no solo aportan al marco teórico sobre ciberseguridad, sino que también ofrecen ideas útiles para diseñar programas educativos y políticas públicas adaptadas a las condiciones particulares de los países en desarrollo.

Con respecto al objetivo inicial—explorar los factores culturales y sociales que influyen en la adopción de una cultura ética de hacking en países emergentes—, se puede afirmar que el estudio logró construir un marco teórico que aborda temas que usualmente no reciben tanta atención en la literatura académica. Se mostró cómo aspectos como las normas sociales, la cultura local y el sistema educativo están profundamente interconectados, afectando directamente la manera en que se perciben y se aplican estas prácticas. Esta articulación sugiere que no basta con proponer soluciones técnicas: se necesita un enfoque más integral, que tenga en cuenta la diversidad cultural y social de cada contexto.

Cabe mencionar que, al tratarse de una revisión bibliográfica, este artículo permite situar los hallazgos dentro de una perspectiva amplia, combinando

diferentes enfoques teóricos y datos empíricos sobre el *ethical hacking*. Sin embargo, también hay que reconocer que el estudio se basa únicamente en la literatura existente, lo que impone ciertas limitaciones al momento de generalizar los resultados. Por eso, se recomienda tomar con cautela algunas conclusiones, especialmente si se quiere aplicarlas a contextos muy distintos a los analizados.

Por último, este trabajo deja abiertas varias líneas para investigaciones futuras. Sería útil, por ejemplo, explorar con más detalle cómo las acciones de responsabilidad social empresarial pueden ayudar a fomentar el *ethical hacking* en distintos contextos culturales. También sería recomendable adaptar los programas de formación en ciberseguridad para que respondan mejor a las características sociales y educativas de diferentes comunidades. Además, los estudios comparativos entre países emergentes, enfocados en cómo se aplican políticas específicas sobre *ethical hacking*, podrían ayudar a construir una visión más completa y localizada del tema. Las limitaciones señaladas en este estudio refuerzan la idea de que es necesario seguir investigando las dinámicas sociales y los entornos locales para así construir una base sólida —tanto teórica como práctica— que apoye la adopción sostenible del *ethical hacking* en el futuro.

Referencias

- Al-Fatlawi, H. (2024). Awareness of cyber security aspects in distance education. *Journal of Pedagogical Sociology and Psychology*, 6(1), 77-88. <https://doi.org/10.33902/jpsp.202424403>
- Al-Hawamleh, A. (2024). Investigating the multifaceted dynamics of cybersecurity practices and their impact on the quality of e-government services: Evidence from the KSA. *Digital Policy, Regulation and Governance*, 26(3), 317-336. <https://doi.org/10.1108/dprg-11-2023-0168>
- Alshawabkeh, M. (2023). Effectiveness of ethical leadership on employee performance: Systematic literature review. *Különleges Bánásmód - Interdiszplináris Folyóirat*, 9(1), 101-112. <https://doi.org/10.18458/kb.2023.1.101>
- Antonio, J. (2024). Trayectoria y modelo de gobernanza de las políticas de inteligencia artificial (IA) de los países de América del Norte. *Justicia*, 29(45). <https://doi.org/10.17081/just.29.45.7162>
- Carvalho, L., Suzano, J., Batista, T., Santoro, F., & Oliveira, J. (2024). Ethics: ¿What is the Brazilian software engineering research scenario? *Journal of Software Engineering Research and Development*, 12(1). <https://doi.org/10.5753/jserd.2024.3395>
- D'Allura, G., Calabrò, A., & Santangelo, M. (2023). The adoption of codes of ethics in family businesses: Theoretical profiles and empirical evaluation. *Journal of Family Business Management*, 13(4), 1174-1189. <https://doi.org/10.1108/jfbm-03-2022-0028>
- D'Avanzo, E., Franch, M., & Borgonovi, E. (2021). Ethics and sustainable management: An empirical modelling of Carroll's pyramid for the Italian landscape. *Sustainability*, 13(21), 12057. <https://doi.org/10.3390/sui32112057>
- Estrada, A., Méndez, M., Alger, J., & Espinoza-Turcios, E. (2021). Utilización de pautas éticas en investigación por participantes en congreso científico estudiantil internacional, 2015. *Revista Médica Hondureña*, 89(2), 89-95. <https://doi.org/10.5377/rmh.v89i2.12366>
- Facca, D., Smith, M., Shelley, J., Lizotte, D., & Donelle, L. (2020). Exploring the ethical issues in research using digital data collection strategies with minors: A scoping review. *PLOS ONE*, 15(8). <https://doi.org/10.1371/journal.pone.0237875>
- Hegde, S., Garg, A., Murray-Rust, P., & Mietchen, D. (2022). Mining the literature for ethics statements: A step towards standardizing research ethics. *Research Ideas and Outcomes*, 8. <https://doi.org/10.3897/rio.8.e94685>
- Hess, J., Lin, A., Whitehead, A., & Katz, A. (2023). How do ethics and diversity, equity, and inclusion relate in engineering? A systematic review. *Journal of Engineering Education*, 113(1), 143-163. <https://doi.org/10.1002/jee.20571>
- Ige, O. (2020). What we do on social media! Social representations of school-children's activities on electronic communication platforms. *Heliyon*, 6(8), e04584. <https://doi.org/10.1016/j.heliyon.2020.e04584>

- Liopa, M., Geitona, M., & Latsou, D. (2023). Factors affecting the implementation of corporate social responsibility in the health technology industry in Greece. *Cureus*, 15(6). <https://doi.org/10.7759/cureus.39946>
- Majrashi, K. (2024). Determinants of public sector managers' intentions to adopt AI in the workplace. *International Journal of Public Administration in the Digital Age*, 11(1), 1–26. <https://doi.org/10.4018/ijpada.342849>
- Melnikovas, A., Lugo, R., Maennel, K., Brilingaitė, A., Sütterlin, S., & Juozapavičius, A. (2023). Teaching pentesting to social sciences students using experiential learning techniques to improve attitudes towards possible cybersecurity careers. *European Conference on Cyber Warfare and Security*, 22(1), 294–302. <https://doi.org/10.34190/eccws.22.1.1145>
- Momeni, N., Larijani, B., Razmi, H., Mohammadi, F., Mirzazadeh, A., & Asghari, F. (2022). Educational content of professional ethics in postgraduate dental education. *Journal of Dental Education*, 87(4), 454–461. <https://doi.org/10.1002/jdd.13149>
- Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, 21(15). <https://doi.org/10.3390/s21155119>
- Noordegraaf, J., & Kranenbarg, M. (2023). Why do young people start and continue with ethical hacking? A qualitative study on individual and social aspects in the lives of ethical hackers. *Criminology & Public Policy*, 22(4), 803–824. <https://doi.org/10.1111/1745-9133.12650>
- Ogunfowora, B., Andiappan, M., Stackhouse, M., & Varty, C. (2023). CEO ethical leadership as a unique source of substantive and rhetorical ethical signals for attracting job seekers: The moderating role of job seekers' moral identity. *Journal of Organizational Behavior*, 44(9), 1380–1399. <https://doi.org/10.1002/job.2725>
- Oke, A., Ladas, J., & Bailey, M. (2020). Ethical consumers: An exploratory investigation of the ethical food consumption behaviour of young adults in the north east of Scotland. *British Food Journal*, 122(11), 3623–3638. <https://doi.org/10.1108/bfj-10-2019-0801>
- Patra, B., & Lenka, U. (2023). Scientometric, fuzzy NGT and DEMATEL analysis for determining sustainable business practices for entrepreneurial firms. *Benchmarking: An International Journal*, 31(1), 162–185. <https://doi.org/10.1108/bij-02-2022-0091>
- Rocha, E., Guevara-Pezoa, F., & González-Sanabria, J. (2023). Análisis de patrones de publicación científica sobre ética en la ciencia. *Praxis Pedagógica*, 23(34), 72–94.

- Sadeghi, B., Richards, D., Formosa, P., McEwan, M., Bajwa, M., Hitchens, M., & Ryan, M. (2023). Modelling the ethical priorities influencing decision-making in cybersecurity contexts. *Organizational Cybersecurity Journal: Practice, Process and People*, 3(2), 127–149. <https://doi.org/10.1108/ocj-09-2022-0015>
- Shakeel, F., Kruiyen, P., & Thiel, S. (2024). Ethical leadership in the Netherlands: Testing the broader conceptualization and measurement scale. *International Journal of Public Leadership*, 20(2), 144–167. <https://doi.org/10.1108/ijpl-10-2023-0082>
- Toro, E., Duque, D., Rincón, M. L., Guerra, C., Olivares, F., Valenzuela, M., & Calia, C. (2023). Desafíos éticos para la investigación en Latinoamérica: Una aproximación desde el punto de vista de los investigadores. *Revista Latinoamericana de Bioética*, 23(2), 115–131. <https://doi.org/10.18359/rabi.6216>
- Winter, P., & Chico, T. (2023). Using the non-adoption, abandonment, scale-up, spread, and sustainability (NASSS) framework to identify barriers and facilitators for the implementation of digital twins in cardiovascular medicine. *Sensors*, 23(14). <https://doi.org/10.3390/s23146333>
- Zyoud, B., & Lutfi, S. (2024). The role of information security culture in zero trust adoption: Insights from UAE organizations. *IEEE Access*, 12, 72420–72444. <https://doi.org/10.1109/access.2024.3402341>

Demystifying ethical hacking: Cultural considerations in emerging economies

Desmistificação de hackers éticos: considerações culturais em economias emergentes

Leonor Abad Bautista

Universidad Cesar Vallejo | Piura | Perú

<https://orcid.org/0000-0002-1908-9338>

abautistal@ucvvirtual.edu.pe

Abogada, Docente de Postgrado en la Universidad Cesar Vallejo

Guiceli Codina Patiño García

Universidad Tecnológica del Perú | Piura | Perú

<https://orcid.org/0000-0002-8779-5058>

guiceli29@gmail.com

Abogada, Docente de Pregrado en la Universidad Tecnológica del Perú

Diana Verónica Blancas Nuñez

Universidad Tecnológica del Perú | Piura | Perú

<https://orcid.org/0009-0009-0962-5457>

C22339@utp.edu.pe

divebla2@gmail.com

Abogada, Docente de Pregrado en la Universidad Tecnológica del Perú

Andy Williams Chamoli Falcón

Investigador independiente | Piura | Perú

<https://orcid.org/0000-0002-2758-1867>

chamoliss@hotmail.com

Abogado, Docente de Pregrado en la Universidad Tecnológica del Perú

Abstract

The current cybersecurity landscape, marked by the sustained rise in cyberattacks, highlights the urgent need to adopt ethical hacking practices in developing countries. This study aims to examine the cultural and social considerations that influence the consolidation of a responsible and ethical culture of ethical hacking in these contexts. Through a literature review, various scientific sources and recent studies addressing the intersection of culture, society, and cybersecurity were analyzed. The findings reveal that cultural perceptions, educational strategies, and social norms play a decisive role in the acceptance and practice of ethical hacking, as well as in overcoming cultural barriers that hinder its implementation. This research underscores the necessity of designing and implementing approaches that incorporate these cultural dimensions into cybersecurity strengthening programs. In conclusion, the results suggest that the success of ethical hacking initiatives will not rely solely on technical competencies but also on a deep understanding of the cultural and social factors that shape its adoption. This integrative approach opens new avenues for research in a field of growing global significance.

Keywords: culture; ethical hacking; perception; social responsibility; education.

Resumo

O atual panorama da segurança cibernética, caracterizado pelo aumento sustentado de ataques cibernéticos, destaca a necessidade imperativa de adotar práticas de hackers éticas nos países em desenvolvimento. O presente estudo tem como objetivo examinar as considerações culturais e sociais que afetam a consolidação de uma cultura ética de hackers que é responsável e ética nesses contextos. Através de uma revisão bibliográfica, foram analisadas várias fontes científicas e estudos recentes que abordam a inter-relação entre cultura, sociedade e segurança cibernética. As descobertas revelam que as percepções culturais, estratégias educacionais e normas sociais desempenham um papel determinante na aceitação e prática de hackers éticos, bem como na superação de obstáculos culturais que dificultam sua implementação. Esta pesquisa mostra a necessidade de projetar e implementar abordagens que integram essas dimensões culturais nos programas de fortalecimento da segurança cibernética. Em conclusão, os resultados sugerem que o sucesso das iniciativas orientadas para o hacking ético não dependerá exclusivamente das competências técnicas, mas também de uma profunda compreensão dos fatores culturais e sociais que moldam sua adoção. Essa abordagem de integração abre novas linhas de pesquisa em um campo de crescente relevância global.

Palavras-chave: cultura; hacking ético; percepção; responsabilidade social; educação