Journal of Management

JOURMAN

Crowdsourcing de Seguridad: Un Enfoque Colaborativo para la Ciberseguridad

Crowdsourcing for Security: A Collaborative Approach to Cybersecurity

Augusto Cortez Vásquez
acortezv@unmsm.edu.pe
ORCID 0000-0002-5188-7962

Universidad Nacional Mayor de San Marcos. Lima, Perú

RESUMEN

Este estudio muestra como el término "crowdsourcing" ha ganado prominencia como un enfoque revolucionario para la resolución de problemas y la generación de ideas. El crowdsourcing de seguridad representa un paradigma innovador en la ciberseguridad moderna, donde organizaciones aprovechan la inteligencia colectiva de comunidades globales de expertos en seguridad para identificar, reportar y remediar vulnerabilidades en sus sistemas. Este artículo examina cómo las plataformas de bug bounty y programas de divulgación responsable están transformando el modelo tradicional de seguridad informática, ofreciendo un enfoque más ágil, escalable y económicamente eficiente. A través del análisis de casos prácticos y datos empíricos, se demuestra que el crowdsourcing de seguridad no solo amplía la capacidad de detección de amenazas, sino que también fomenta una cultura de seguridad proactiva y colaborativa en el ecosistema digital.

Palabras clave: Crowdsourcing de seguridad; Bug bounty; Vulnerabilidades; Ciberseguridad colaborativa; Hacking ético

ABSTRACT

This study shows how the term "crowdsourcing" has gained prominence as a revolutionary approach to problem-solving and idea generation. Security crowdsourcing represents an innovative paradigm in modern cybersecurity, where organizations leverage the collective intelligence of global communities of security experts to identify, report, and remediate vulnerabilities in their systems. This article examines how bug bounty platforms and responsible disclosure programs are transforming the traditional cybersecurity model, offering a more agile, scalable, and cost-effective approach. Through the analysis of case

studies and empirical data, it is demonstrated that security crowdsourcing not only expands threat detection capabilities but also fosters a proactive and collaborative security culture within the digital ecosystem.

Key words: Security crowdsourcing; Bug bounty; Vulnerabilities; Collaborative cybersecurity; Ethical hacking

INTRODUCCIÓN

Con la irrupción de la Inteligencia artificial (IA) se ha redefinido muchas de las dinámicas de poder y confianza, paradójicamente, mientras que las personas entregan los datos a grandes corporaciones, desconfían de su entorno más cercano, creando un entorno social en donde todos somos potencialmente observados al mismo tiempo observadores. Las organizaciones modernas enfrentan un panorama de amenazas cibernéticas cada vez más complejo y sofisticado. El mundo del comercio electrónico ha experimentado un fuerte aumento de las ventas en línea, cambios que han sido aceptados por la mayoría de los empresarios y marcas online. No obstante, el aumento de los fraudes que acompaña a este incremento en las ventas es un efecto secundario para nada bienvenido (Shopify, 2024).

En la dimensión filosófica nos preguntamos ¿Dónde termina nuestra identidad física y comienza la digital? Cuando hackean tu correo o redes sociales, ¿te están robando parte de tu ser? Surge la cuestión de libertad vs seguridad, pues cada medida de seguridad afecta en alguna medida nuestra libertad. Los equipos internos de seguridad, aunque altamente capacitados, presentan limitaciones inherentes: recursos humanos finitos, perspectivas homogéneas debido a la familiaridad con los sistemas, y capacidad limitada para simular la diversidad de técnicas de ataque que emplean actores maliciosos reales.

La seguridad colaborativa se basa en la sabiduría colectiva, un fenómeno en el que grandes grupos de personas son, en conjunto, más inteligentes que los expertos individuales. Es de vital importancia tener en cuenta, que la digitalización también enfrenta el desafío de la desinformación. La facilidad para compartir información aumenta la propagación de noticias falsas. Es fundamental desarrollar sistemas robustos para verificar la autenticidad del testimonio y clasificar las noticias, temas, cuestionamientos y propuestas evaluando el testimonio colectivo (El_Pais, 2024).

Adicionalmente, el costo de mantener equipos de seguridad robustos con cobertura 24/7 resulta prohibitivo para muchas organizaciones, especialmente startups y empresas medianas. El tiempo promedio para detectar una brecha de seguridad se estima en varios meses, durante los cuales los atacantes pueden exfiltrar datos sensibles o establecer persistencia en los sistemas comprometidos.

Este estudio tiene como objetivos:
a) Analizar la efectividad del crowdsourcing de seguridad como complemento a las estrategias tradicionales de ciberseguridad

b) Evaluar los beneficios económicos y operativos de implementar programas de bug bounty
c) Identificar las mejores prácticas para estructurar programas de crowdsourcing de seguridad exitosos
d) Examinar los desafíos éticos, legales y técnicos asociados con este enfoque colaborativo
e) Proporcionar un marco de referencia para organizaciones que consideren adoptar esta metodología

La ciberseguridad consiste en un conjunto de prácticas orientadas a proteger sistemas informáticos, redes, dispositivos, programas y datos contra ataques digitales, accesos no autorizados, daños o robos. El ámbito digital ha experimentado una proliferación exponencial de amenazas, desde virus y malware hasta sofisticados ataques de phishing y ransomware.

El crowdsourcing es un modelo de producción que aprovecha la inteligencia colectiva, la contribución y la colaboración de una amplia audiencia o "multitud" para realizar tareas, resolver problemas o generar ideas. En lugar de depender de un grupo interno de expertos, el crowdsourcing se basa en la diversidad y la creatividad de una comunidad más extensa, utilizando plataformas digitales para facilitar la participación masiva (EAE, 2025).

El crowdsourcing de seguridad se define como la práctica de solicitar la participación de una comunidad externa y diversa de investigadores de seguridad para identificar vulnerabilidades, debilidades y riesgos en sistemas informáticos, aplicaciones y infraestructuras digitales.

METODOLOGÍA

Se empleó un enfoque de métodos mixtos que combina análisis cuantitativo y revisión sistemática de literatura para examinar la efectividad del crowdsourcing de seguridad en la identificación de vulnerabilidades.

El análisis cuantitativo se basó en la recopilación y análisis estadístico de datos provenientes de plataformas de bug bounty públicas, entre ellas HackerOne (hackerone.com), una de las plataformas más grandes con programas de empresas como Shopify, GitHub y PayPal; Bugcrowd (bugcrowd.com), otra plataforma líder con miles de programas activos de empresas importantes; Intigriti (intigriti.com), popular en Europa y con una comunidad activa de investigadores; YesWeHack (yeswehack.com), plataforma europea con programas en varios idiomas; Synack (synack.com), que requiere aplicación para unirse pero ofrece programas bien remunerados; y HackenProof (hackenproof.com), enfocada en proyectos blockchain y criptográficos.

Asimismo, se realizó una revisión sistemática de literatura mediante el examen de publicaciones académicas, reportes de la industria y documentación técnica publicada entre

los años 2015 y 2024. Para ello se consideraron datos primarios como estadísticas agregadas del Hacker-Powered Security Report 2024 de HackerOne, datos públicos del Priority One Report de Bugcrowd, así como información de programas públicos disponibles en plataformas como YesWeHack e Intigriti.

También se emplearon datos secundarios provenientes de publicaciones en conferencias de seguridad como Black Hat, DEF CON y RSA, reportes de vulnerabilidades del National Vulnerability Database (NIST) y estudios de caso publicados por organizaciones que implementaron programas de bug bounty exitosos.

Para el análisis cuantitativo se seleccionaron programas de bug bounty con al menos 12 meses de operación continua, organizaciones que divulgaron métricas públicas de rendimiento y plataformas con más de 1000 investigadores activos. En el análisis cualitativo se consideró la diversidad sectorial (tecnología, finanzas, salud y gobierno), la variedad en el tamaño organizacional (desde startups hasta empresas Fortune 500) y la representación geográfica distribuida.

Finalmente, se reconocen ciertas limitaciones metodológicas, entre ellas el posible sesgo de reporte debido a que algunas organizaciones pueden publicar selectivamente datos favorables, las diferencias en el alcance de los programas que dificultan comparaciones directas entre ellos y la dificultad para aislar el impacto específico del crowdsourcing de seguridad frente a otras iniciativas de seguridad que las organizaciones puedan implementar simultáneamente.

RESULTADOS

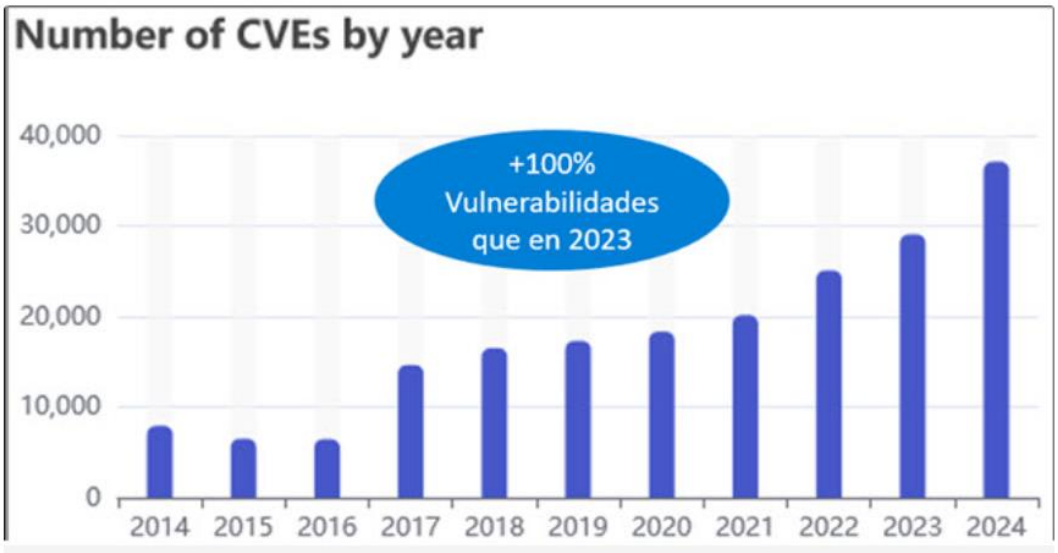
Los datos analizados revelan resultados significativos en relación con la efectividad del crowdsourcing de seguridad para la detección de vulnerabilidades en sistemas informáticos. Programas maduros de bug bounty reportan un promedio de entre 60 y 150 vulnerabilidades únicas por año, superando ampliamente la cantidad que equipos internos de seguridad suelen detectar mediante auditorías tradicionales. Un caso notable es el de Shopify, que reportó más de 1000 vulnerabilidades válidas en sus primeros dos años de programa público.

Asimismo, los investigadores externos logran identificar categorías de vulnerabilidades que auditorías internas frecuentemente pasan por alto, especialmente aquellas relacionadas con lógica de negocio, cadenas de ataque complejas y vectores no convencionales. Esto evidencia el valor de contar con una comunidad diversa de especialistas que analizan los sistemas desde múltiples perspectivas. En relación con la evolución de las vulnerabilidades reportadas, se observa una tendencia creciente en los últimos años.

En este contexto, se tomó como fuente de datos el reporte de Welivesecurity (2024), el cual muestra el histórico de vulnerabilidades reportadas por año.

Figura 1

Histórico de vulnerabilidades reportadas por año que muestra un pico de detecciones en 2024



Nota. Adaptado de Welivesecurity (2024).

DISCUSIÓN

El análisis de los resultados obtenidos evidencia que el crowdsourcing de seguridad representa una evolución significativa en las estrategias de protección digital adoptadas por las organizaciones modernas. A diferencia de los enfoques tradicionales basados exclusivamente en equipos internos o auditorías periódicas, los programas de bug bounty permiten aprovechar la inteligencia colectiva de comunidades globales de especialistas en seguridad informática, lo que incrementa considerablemente la capacidad de detección de vulnerabilidades.

La diversidad de perfiles profesionales, experiencias técnicas y enfoques de análisis presentes en estas comunidades facilita la identificación de vulnerabilidades que podrían pasar desapercibidas en evaluaciones de seguridad convencionales. Asimismo, la naturaleza continua de estos programas permite detectar fallos en etapas tempranas del desarrollo o inmediatamente después del despliegue de nuevas funcionalidades, reduciendo significativamente el tiempo de exposición a posibles ataques.

Otro aspecto relevante es el impacto económico de este modelo. En muchos casos, los programas de bug bounty resultan más eficientes en términos de costos que las auditorías tradicionales, ya que las organizaciones recompensan únicamente las vulnerabilidades válidas identificadas por los investigadores. No obstante, la implementación de este enfoque también plantea desafíos relacionados con la gestión de programas de divulgación

responsable, la definición de alcances claros y la necesidad de establecer marcos legales adecuados que regulen la interacción entre organizaciones e investigadores externos.

CONCLUSIONES

El crowdsourcing de seguridad se ha consolidado como un componente relevante dentro de las estrategias modernas de ciberseguridad, demostrando una alta efectividad en la identificación temprana de vulnerabilidades y en el fortalecimiento de las defensas digitales de las organizaciones. Los resultados analizados evidencian que los programas de bug bounty permiten ampliar significativamente la capacidad de detección de fallos de seguridad mediante la participación de una comunidad global de investigadores especializados.

Asimismo, este modelo colaborativo no sustituye las estrategias tradicionales de seguridad informática, sino que las complementa al incorporar mecanismos de vigilancia continua y evaluación permanente de los sistemas. En consecuencia, el crowdsourcing de seguridad contribuye al desarrollo de una cultura de seguridad más abierta, colaborativa y proactiva dentro del ecosistema digital, permitiendo a las organizaciones adaptarse con mayor rapidez a un entorno de amenazas cada vez más dinámico y complejo.

CONFLICTO DE INTERESES

El autor declara que no existe conflicto de intereses para la publicación del presente artículo científico.

REFERENCIAS

Bugcrowd. (2025). Crowdsourced security. https://www.bugcrowd.com/glossary/crowdsourced-security/

CrowdStrike. (2025). Resumen ejecutivo del Global Threat Report 2025. https://go.crowdstrike.com/2025-global-threat-report-es_la.html

Cruz, M. (2012). Conocimiento situado y el problema de la subjetividad del investigador.

EAE Business School. (2025). Fundamentos y definición del crowdsourcing. https://www.eaemadrid.com/es/blog/que-es-crowdsourcing

El País. (2006). Inteligencia colectiva: ¿La aprovecha su página web? https://elpais.com/tecnologia/2006/04/18/actualidad/1145348883_850215.html

Escudo Digital. (2025). Lo que gasta China en ciberseguridad: así construye su ciber-imperio. https://www.escudodigital.com/ciberseguridad/gasta-china-ciberseguridad-construye-ciber-imperio.html

ESED. (2024). Concepto bug bounty: qué es y por qué lo necesitamos. https://www.esedsl.com/blog/concepto-bug-bounty-que-es-y-por-que-lo-necesitamos

Fortinet. (2025). Informe global del panorama de amenazas de 2025. https://www.fortinet.com/lat/resources/reports/threat-landscape-report

Gonzales, F. (2012). Procesos de inteligencia colectiva y colaborativa en el marco de tecnologías web 2.0: conceptos, problemas y aplicaciones. https://www.redalyc.org/pdf/3691/369139948071.pdf

Infobae. (2025). Ciberataques en Perú superan los 748 millones de intentos en lo que va del 2025.

Infobae. (2025). Google pagará hasta 30,000 dólares por detectar fallos en su IA: así puedes participar. https://www.infobae.com/tecno/2025/10/07/google-pagara-hasta-30000-dolares-por-detectar-fallos-en-su-ia-asi-puedes-participar/

Merino, C. (s. f.). Inteligencia colectiva. Universitat Oberta de Catalunya. https://openaccess.uoc.edu/server/api/core/bitstreams/27ea646c-8e91-43fe-8823-4e2db40631cd/content

Oxford Review. (2025). Appreciation of diversity of thought: Definition and explanation. https://oxford-review.com/the-oxford-review-dei-diversity-equity-and-inclusion-dictionary/appreciation-of-diversity-in-thought-definition-and-explanation/

Shopify. (2024). La tecnología punta de Shopify protege a millones de comercios contra el fraude. https://www.shopify.com/es/blog/proteccion-contra-el-fraude

UNIR. (s. f.). Engagement: el compromiso del usuario con la marca. https://www.unir.net/revista/marketing-comunicacion/engagement/