



Sistema de Puntuación de Vulnerabilidades Comunes (CVSS)

UNA REVISIÓN INTEGRADORA DE FUNDAMENTOS,
PRÁCTICAS Y DESAFÍOS EMERGENTES

E-boletín Informativo CSIRT Académico
UNAD

Medio de divulgación: Correo Electrónico,
Sitio Web

Incluye: Noticias, alertas o informes
relacionados con la disciplina de la
ciberseguridad

Número Cuarenta [42]
Agosto de 2026

Universidad Nacional Abierta y a Distancia
(UNAD)

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 | Bogotá D.C
Correo electrónico:
csirt@unad.edu.co
Página web: <https://csirt.unad.edu.co>

Licencia Atribución – Compartir igual



Estado legal:
Periodicidad: Mensual
ISSN: 2806-0164

Edición electrónica, financiada por la
Universidad Nacional Abierta y a
Distancia (UNAD)

Vicerrectoría de Innovación y
Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas
Vicerrector

Escuela de Ciencias Básicas Tecnología e
Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo
Decano

Maestría en Ciberseguridad (ECBTI)
Ing. Sonia Ximena Moreno Molano
Líder de Programa

Especialización en Seguridad Informática
Ing. Cesar Antonio Villamizar
Líder de Programa

Semillero de Investigación Ceros y Unos,
adscrito al Grupo de Byte InDesign

Centro de Desarrollo Tecnológico CSIRT Académico UNAD

Ing. Luis Fernando Zambrano Hernández
Líder CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernandez

Revisó
Adm. Libardo Cárdenas Corral
Analista CSIRT Académico UNAD

La cantidad de vulnerabilidades divulgadas cada año con identificador CVE¹ supera con amplitud la capacidad de remediación de cualquier organización, lo que convierte la priorización en una tarea crítica de la gestión de la ciberseguridad. El Sistema de Puntuación de Vulnerabilidades Comunes (CVSS, por sus siglas en inglés) se ha consolidado como el lenguaje común para comunicar la severidad técnica de dichas vulnerabilidades, y su puntuación de 0.0 a 10.0 aparece en avisos de fabricantes, bases de datos públicas y herramientas de escaneo.

Este boletín académico presenta una revisión de la literatura científica sobre el CVSS, organizada en tres ejes temáticos: sus fundamentos y evolución hasta la versión 4.0, el cálculo e interpretación de la puntuación con casos reales de CVE, y las limitaciones del estándar junto con los enfoques que lo complementan en la priorización de vulnerabilidades.

¹ Common Vulnerabilities and Exposures: identificador público y único asignado a cada vulnerabilidad divulgada (por ejemplo, CVE-2021-44228).

Tabla de contenido

1. Introducción.....	5
2. Sistema de Puntuación de Vulnerabilidades Comunes (CVSS)	6
2.1. Fundamentos, evolución y estructura del CVSS	6
2.2. Cálculo e interpretación del CVSS: vector, escala de severidad y casos reales.....	8
2.3. Limitaciones del CVSS y enfoques complementarios de priorización	12
3. Conclusiones.....	14
4. Recomendaciones.....	15_
5. Referentes Bibliográficos	16_

1. Introducción

La gestión de vulnerabilidades es uno de los procesos más demandantes de un programa de ciberseguridad: cada semana se publican cientos de nuevas vulnerabilidades y los equipos de operaciones deben decidir cuáles corregir primero con recursos limitados. Antes de la aparición del CVSS, cada fabricante y cada herramienta empleaba escalas propias e incompatibles, lo que dificultaba comparar hallazgos y coordinar respuestas entre organizaciones (Mell et al., 2006). El CVSS surgió para resolver ese problema mediante un marco abierto, que hoy mantiene el Forum of Incident Response and Security Teams (FIRST)², y que expresa la severidad de una vulnerabilidad en una puntuación numérica acompañada de un vector³ que documenta cómo se obtuvo.

Su adopción ha sido tan amplia que la puntuación CVSS se utiliza de forma rutinaria como criterio de priorización e incluso como requisito contractual o normativo para los tiempos de remediación. Sin embargo, la literatura reciente advierte que el CVSS mide la severidad técnica y no el riesgo, y que su uso como único criterio de decisión conduce a priorizaciones poco eficientes (Spring et al., 2021; Howland, 2023). A ello se suman evidencias de inconsistencia entre evaluadores (Wunder et al., 2024) y de discrepancias entre las puntuaciones publicadas por distintas fuentes para una misma vulnerabilidad (Anwar et al., 2022).

El propósito de este boletín es sintetizar el estado del conocimiento sobre el CVSS desde una perspectiva académica y aplicada. El documento se estructura en tres ejes temáticos que van de lo conceptual a lo práctico: primero, los fundamentos, la evolución y la estructura de métricas del estándar; segundo, el cálculo e interpretación de la puntuación a partir de vulnerabilidades reales; y tercero, las críticas al modelo y los enfoques complementarios, como EPSS, el catálogo KEV y SSVC, que permiten transformar la severidad técnica en decisiones de remediación informadas.

² Forum of Incident Response and Security Teams (FIRST). Common Vulnerability Scoring System SIG. <https://www.first.org/cvss/>

³ Cadena de texto que codifica, en formato abreviado (métrica:valor), cada una de las métricas empleadas para calcular la puntuación.

Sistema de Puntuación de Vulnerabilidades Comunes (CVSS)

Fundamentos, aplicación práctica y desafíos en la priorización de vulnerabilidades

Autores

Luis Fernando Zambrano Hernandez

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

Hernando José Peña Hidalgo

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

Sonia Ximena Moreno Molano

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

Néstor Raúl Cárdenas Corral

Analista CSIRT Académico UNAD
Universidad Nacional Abierta y a Distancia
ORCID: orcid.org/0000-0003-3691-0148

2. Sistema de Puntuación de Vulnerabilidades Comunes (CVSS)

2.1. Fundamentos, evolución y estructura del CVSS

El CVSS se define como un marco abierto y estandarizado para capturar las características principales de una vulnerabilidad de software y producir una puntuación numérica que refleje su severidad, la cual puede traducirse a una categoría cualitativa (baja, media, alta o crítica) para apoyar los procesos de gestión de vulnerabilidades². Su diseño separa las propiedades intrínsecas de la vulnerabilidad de aquellas que dependen del tiempo o del entorno, lo que permite que distintos actores evalúen un mismo fallo con un lenguaje común (Mell et al., 2006).

El origen del estándar se remonta a una iniciativa del National Infrastructure Advisory Council (NIAC) de Estados Unidos, cuyo objetivo era reemplazar los sistemas de calificación propietarios y fragmentados que

impedían la colaboración entre equipos de seguridad⁴. Mell et al. (2006) presentaron formalmente el CVSS como un sistema universal y abierto, con tres grupos de métricas, Base, Temporal y Ambiental, y una fórmula que

⁴ IBM. ¿Qué es el sistema común de puntuación de vulnerabilidades (CVSS)? <https://www.ibm.com/mx-es/think/topics/cvss>

pondera la facilidad de explotación y el impacto sobre la confidencialidad, la integridad y la disponibilidad. La versión 2.0, publicada en 2007, consolidó esa estructura y su escala de tres niveles de severidad.

La versión 3.0 (2015) y su revisión 3.1 (2019) introdujeron cambios sustanciales: las métricas de privilegios requeridos (PR) e interacción del usuario (UI), el concepto de alcance (Scope) para reflejar impactos que trascienden el componente vulnerable y una nueva categoría de severidad crítica para puntuaciones de 9.0 a 10.0⁵. La coexistencia de puntuaciones v2 y v3.x en las bases de datos generó la necesidad de métodos de conversión entre versiones para dar continuidad a los procesos de gestión de vulnerabilidades (Nowak et al., 2023). Anwar et al. (2022) mostraron la magnitud del problema: al estimar puntuaciones v3 para las CVE que solo contaban con v2 en el National Vulnerability Database (NVD), cerca del 40 % cambiaba de categoría de severidad, con una tendencia marcada hacia valores más altos.

La versión 4.0, publicada por FIRST el 1 de noviembre de 2023, reorganiza el estándar en cuatro grupos de métricas². El grupo Base incorpora la métrica de requisitos de ataque (AT), redefine la interacción del usuario (ninguna, pasiva o activa) y sustituye el alcance por una evaluación separada del impacto sobre el sistema vulnerable (VC, VI, VA) y sobre los sistemas subsecuentes (SC, SI, SA). El grupo Temporal se reemplaza por el grupo de Amenaza, centrado en la madurez del exploit; el grupo Ambiental conserva los requisitos de seguridad del activo; y un nuevo grupo de métricas Suplementarias, como seguridad física, automatizable o urgencia del proveedor, aporta información adicional sin modificar la puntuación⁴.

La versión 4.0 también introduce una nomenclatura explícita (CVSS-B, CVSS-BT, CVSS-BE y CVSS-BTE) para indicar qué grupos de métricas intervinieron en el cálculo. Este cambio responde a una crítica recurrente: la mayoría de las puntuaciones publicadas son solo de tipo Base y, aun así, se interpretan como una medida

⁵ Fortinet. Common Vulnerability Scoring System (CVSS). <https://www.fortinet.com/lat/resources/c>

[yberglossary/common-vulnerability-scoring-system](https://first.org/yberglossary/common-vulnerability-scoring-system)

completa del riesgo (Spring et al., 2021). En la misma línea, Santana et al. (2024) proponen enriquecer el grupo de Amenaza con un modelo dependiente del tiempo

que estime la madurez del exploit a partir de evidencia empírica, en lugar de un valor estático asignado manualmente.

Ilustración 1.

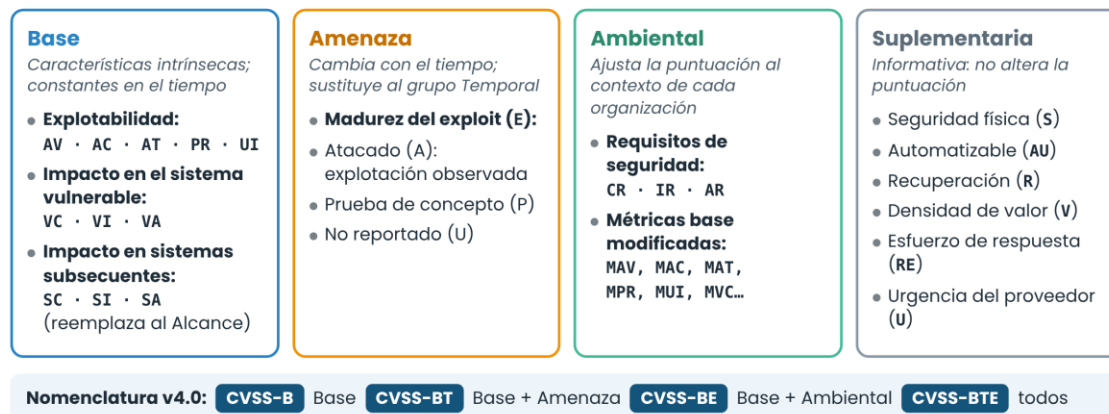
Evolución y estructura del CVSS: versiones y grupos de métricas de la versión 4.0

Evolución y estructura del CVSS

De la versión 1.0 a la 4.0: cada revisión buscó mayor precisión y mejor reflejo del contexto real



Grupos de métricas en CVSS v4.0



Elaboración propia a partir de la especificación CVSS v4.0 de FIRST² y de Mell et al. (2006).

2.2. Cálculo e interpretación del CVSS: vector, escala de severidad y casos reales

Cada puntuación CVSS se acompaña de un vector que registra el valor asignado a cada métrica, lo que hace el cálculo reproducible y verificable por terceros. La puntuación resultante se traduce a una escala cualitativa: en las versiones 3.x y 4.0, ninguna (0.0), baja (0.1–3.9), media (4.0–6.9), alta (7.0–8.9) y crítica (9.0–10.0); en la versión 2.0, baja (0.0–3.9), media (4.0–6.9) y alta (7.0–10.0)⁶. Estas puntuaciones son publicadas tanto por el NVD como

⁶ National Institute of Standards and Technology (NIST). National Vulnerability

Database: Vulnerability Metrics.
<https://nvd.nist.gov/vuln-metrics/cvss>

por las CNA⁷, por lo que una misma CVE puede tener más de una calificación.

La lectura del vector permite comprender por qué una vulnerabilidad obtiene una puntuación determinada. El caso de Log4Shell (CVE-2021-44228), en la biblioteca Apache Log4j, ilustra el escenario de máxima severidad: su vector CVSS v3.1 (Ilustración 2) indica que puede explotarse por red, con baja complejidad, sin privilegios ni interacción del usuario, con impacto alto en las tres dimensiones y con un alcance que trasciende el componente afectado, lo que produce una puntuación de 10.0. Un patrón similar se observa en la puerta trasera de XZ Utils (CVE-2024-3094), también calificada con 10.0, y en la inyección SQL de MOVEit Transfer (CVE-2023-34362), con 9.8.

Los casos reales muestran, además, que la versión del estándar influye en la categoría final. Heartbleed (CVE-2014-0160), en OpenSSL, obtuvo 5.0 (media) en CVSS v2.0 y 7.5 (alta) en CVSS v3.1, con un vector que refleja impacto exclusivamente sobre la confidencialidad⁶ (Ilustración 3). Este comportamiento es coherente con el desplazamiento

hacia severidades más altas documentado al pasar de v2 a v3 (Anwar et al., 2022; Nowak et al., 2023) y advierte sobre la comparación directa de puntuaciones de versiones distintas.

La subjetividad de algunas métricas genera discrepancias entre evaluadores. En Citrix Bleed (CVE-2023-4966), la CNA del fabricante asignó 9.4 (crítica) al considerar impacto alto en confidencialidad e integridad, mientras que el NVD publicó 7.5 (alta) al valorar solo la pérdida de confidencialidad. Wunder et al. (2024) estudiaron este fenómeno con 196 usuarios de CVSS y encontraron evaluaciones inconsistentes en métricas como el vector de ataque, la interacción del usuario y el alcance, incluso para tipos de vulnerabilidad muy comunes; además, el 68 % de los participantes modificó su calificación al repetir el ejercicio meses después.

La puntuación tampoco siempre está disponible a tiempo. Ruohonen (2019) analizó más de 88

⁷ CVE Numbering Authority: organización (fabricante, CERT o investigador) autorizada para asignar identificadores CVE y, con frecuencia, su puntuación CVSS.

000 vulnerabilidades y halló que, si bien la mitad recibía su puntuación CVSS en el día siguiente a la publicación de la CVE, existían retrasos atípicos de años. Para reducir esta carga, la investigación ha explorado la predicción automática de métricas a partir de la descripción textual: Shahid y Debar (2021) obtuvieron exactitudes de entre 83.79 % y 96.07 % por métrica con modelos BERT, y Manai et al. (2024) propusieron técnicas de inteligencia artificial explicable para que las CNA generen puntuaciones más rápido y con mayor confianza. Le et al. (2022) sistematizan estos enfoques basados en datos y advierten

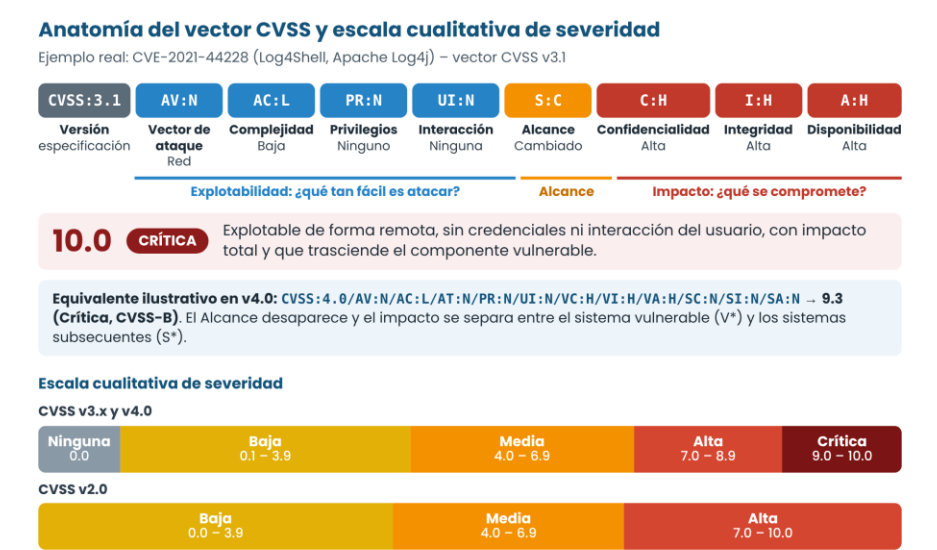
sobre la calidad de los conjuntos de entrenamiento.

Finalmente, una severidad alta, y no necesariamente crítica, puede tener consecuencias globales. EternalBlue (CVE-2017-0144), en el protocolo SMBv1 de Windows, tiene una puntuación de 8.8 (alta) y, sin embargo, fue el vector de propagación del *ransomware* WannaCry en 2017 y figura en el catálogo de vulnerabilidades explotadas activamente⁸. Este caso anticipa la discusión del siguiente apartado: la puntuación describe la severidad técnica, pero no la probabilidad ni el contexto de explotación.

⁸ Cybersecurity and Infrastructure Security Agency (CISA). Known Exploited Vulnerabilities

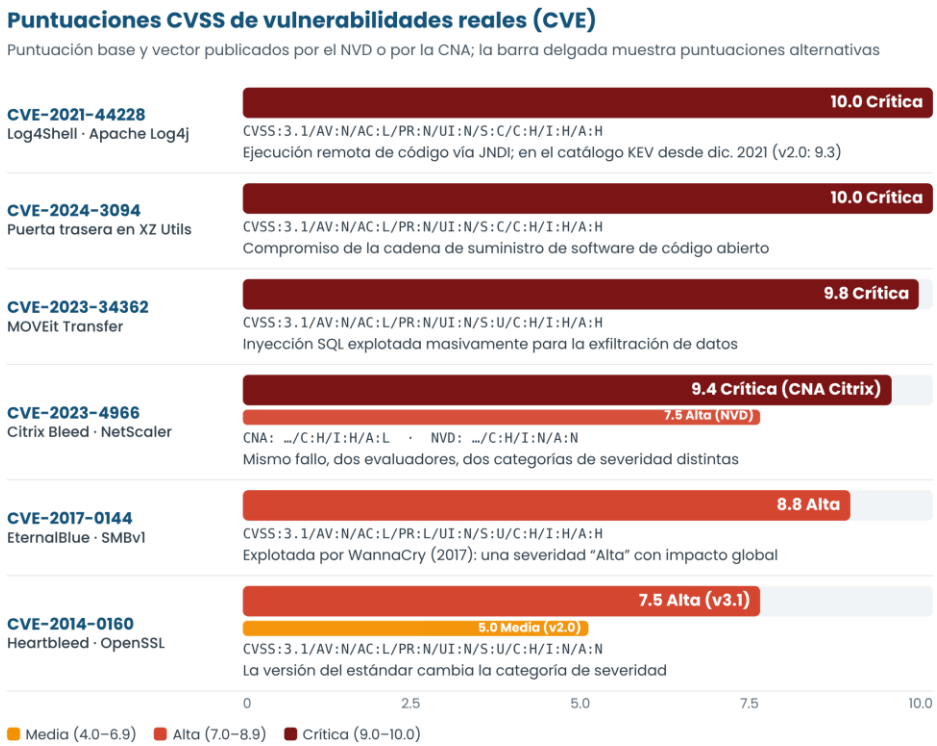
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

Ilustración 2.
Anatomía del vector CVSS y escala cualitativa de severidad



Elaboración propia con base en el NVD⁶ y la especificación de FIRST². El vector v4.0 se presenta a modo ilustrativo.

Ilustración 3.
Puntuaciones CVSS de vulnerabilidades reales (CVE)



Elaboración propia con datos públicos del NVD⁶ y de las CNA correspondientes.

2.3. Limitaciones del CVSS y enfoques complementarios de priorización

El propio FIRST aclara que el CVSS mide la severidad técnica de una vulnerabilidad y no constituye, por sí solo, una evaluación del riesgo². No obstante, en la práctica la puntuación Base suele utilizarse como sustituto directo del riesgo, una costumbre que la literatura identifica como la principal fuente de malas decisiones de priorización (Spring et al., 2021).

Las críticas al modelo son tanto conceptuales como empíricas. Spring et al. (2021) cuestionan que una fórmula con ponderaciones poco justificadas produzca una cifra de apariencia precisa que se usa para decisiones que no fue diseñada para respaldar. Howland (2023) va más allá y sostiene que el CVSS, pese a ser omnipresente, presenta fallas estructurales en su método de cálculo y en su capacidad para reflejar la gravedad real de las vulnerabilidades. En el plano empírico, Allodi y Massacci (2014), mediante estudios de casos y controles, demostraron que una puntuación alta es un predictor débil de la explotación en entornos reales y que priorizar únicamente por CVSS ofrece una reducción del riesgo limitada.

Como respuesta, han surgido enfoques complementarios. El Exploit Prediction Scoring System

(EPSS) estima, con un modelo basado en datos, la probabilidad de que una vulnerabilidad sea explotada en los siguientes 30 días, información que el CVSS no captura (Jacobs et al., 2021). El catálogo de vulnerabilidades explotadas conocidas (KEV) de CISA aporta evidencia confirmada de explotación activa⁸, y el modelo SSVC⁹ sustituye la puntuación por un árbol de decisión que incorpora la exposición del sistema y la misión de la organización.

Estos sistemas, sin embargo, no siempre coinciden. Koscinski et al. (2025) compararon CVSS, EPSS, SSVC y el índice de explotabilidad de Microsoft sobre vulnerabilidades de los ciclos de actualización mensuales y encontraron una concordancia débil entre ellos: solo cinco CVE aparecían en el top-100 de los cuatro sistemas, el CVSS generó

⁹ Stakeholder-Specific Vulnerability Categorization: modelo de decisión basado en árboles, promovido por CISA y

el CERT/CC. <https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc>

grandes grupos de empates (198 CVE compartían una misma puntuación en el top-20) y el EPSS asignó valores inferiores a 0.1 a nueve vulnerabilidades que sí fueron explotadas. La conclusión práctica es que ninguna métrica aislada basta para priorizar.

La dimensión que más se omite es el contexto. Las métricas Ambientales del CVSS permiten ajustar la puntuación a la criticidad de los activos y a los controles existentes, pero rara vez se utilizan. Ouraou (2025) plantea la

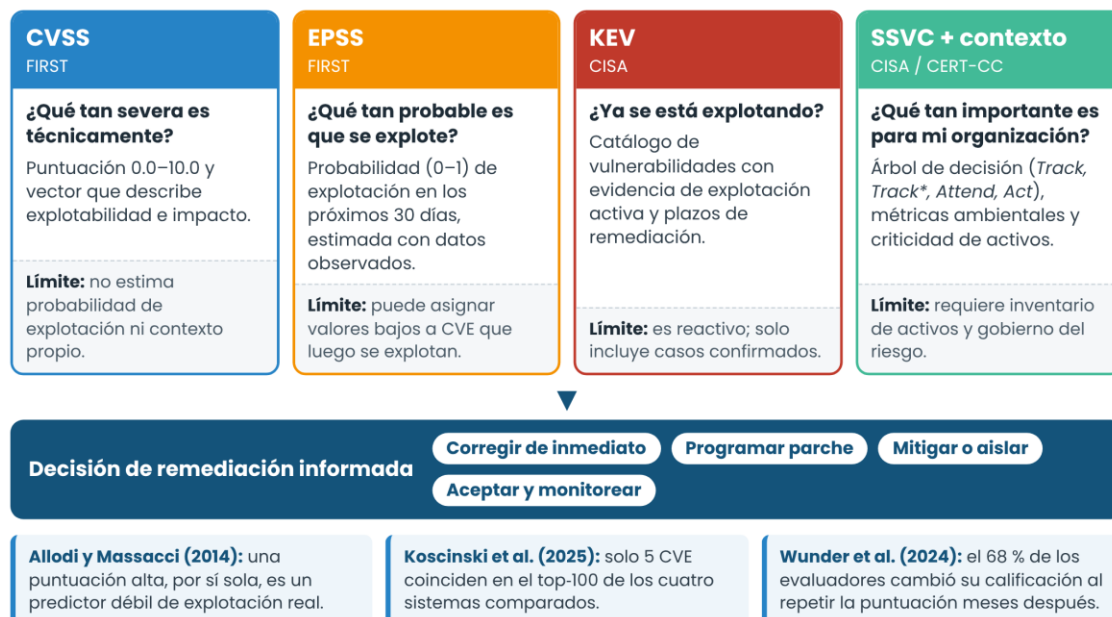
Ilustración 4.

El CVSS dentro de un modelo de priorización complementario

necesidad de repensar la contextualización de las CVE en entornos altamente conectados, donde el mismo fallo puede tener consecuencias muy distintas según la arquitectura, la exposición y la función del sistema afectado. Integrar severidad, probabilidad, evidencia de explotación y contexto organizacional constituye, por tanto, el enfoque recomendado por la literatura para una gestión de vulnerabilidades basada en el riesgo.

El CVSS dentro de un modelo de priorización complementario

La severidad técnica es una entrada de la decisión, no la decisión misma



Elaboración propia con base en Jacobs et al. (2021), Koscinski et al. (2025), Allodi y Massacci (2014) y Wunder et al. (2024).

3. Conclusiones

Este boletín permite identificar consensos claros sobre el papel del CVSS en la gestión de vulnerabilidades. En primer lugar, el CVSS se ha consolidado como el lenguaje común de la industria para comunicar la severidad técnica de las vulnerabilidades; su vector hace el cálculo transparente y reproducible, y su evolución hasta la versión 4.0 muestra un esfuerzo sostenido por representar con mayor precisión las condiciones de ataque, el impacto sobre sistemas subsecuentes y la madurez de la amenaza.

En segundo lugar, el análisis de vulnerabilidades reales evidencia que la puntuación depende de la versión del estándar y del evaluador. Casos como Heartbleed, que pasó de severidad media a alta entre versiones, o Citrix Bleed, calificada como crítica por el fabricante y como alta por el NVD, confirman los hallazgos de la literatura sobre inconsistencias en la puntuación y obligan a registrar siempre la versión, el vector y la fuente de cada calificación.

En tercer lugar, existe una convergencia en la literatura en que el CVSS mide severidad y no riesgo. Una puntuación alta no predice por sí sola la explotación, y vulnerabilidades con severidad alta, como EternalBlue, han tenido impactos globales. Por ello, el CVSS debe operar junto con indicadores de probabilidad (EPSS), evidencia de explotación activa (KEV) y modelos de decisión contextual (SSVC y métricas Ambientales).

Finalmente, la investigación reciente en predicción automática de métricas mediante aprendizaje automático abre una vía para reducir los retrasos y la subjetividad en la puntuación, aunque su adopción requiere datos de calidad, mecanismos de explicabilidad y validación por parte de analistas. El reto para las organizaciones no es abandonar el CVSS, sino usarlo de forma correcta: como una entrada necesaria, pero no suficiente, de la decisión de remediación.

4. Recomendaciones

A partir de los hallazgos sintetizados en este boletín, se formulan las siguientes recomendaciones dirigidas a equipos de gestión de vulnerabilidades, CSIRT, líderes de seguridad y responsables de la toma de decisiones tecnológicas:

- Registrar siempre la puntuación CVSS junto con su versión, su vector completo y la fuente que la emitió (NVD o CNA), evitando comparar directamente puntuaciones de versiones distintas.
- Planificar la transición hacia CVSS v4.0, actualizando herramientas, procedimientos y acuerdos de nivel de servicio, e identificando explícitamente la nomenclatura utilizada (CVSS-B, CVSS-BT, CVSS-BE o CVSS-BTE).
- No utilizar la puntuación Base como único criterio de priorización; combinarla con la probabilidad de explotación (EPSS) y con la evidencia de explotación activa del catálogo KEV.
- Aplicar las métricas Ambientales y los requisitos de seguridad (CR, IR, AR) a partir de un inventario actualizado de activos, de modo que la puntuación refleje la criticidad real de cada sistema para la organización.
- Adoptar modelos de decisión como SSVC para traducir la información técnica en acciones concretas y plazos de remediación coherentes con la misión institucional.
- Capacitar a los analistas en la evaluación de las métricas más propensas a inconsistencias, como el vector de ataque, la interacción del usuario y el alcance o impacto subsecuente, y establecer revisiones por pares para las vulnerabilidades críticas.
- Explorar, desde la academia y los CSIRT, el uso de modelos de aprendizaje automático explicables para apoyar la puntuación de vulnerabilidades, manteniendo siempre la validación humana de los resultados.

5. Referentes Bibliográficos

- Allodi, L., & Massacci, F. (2014). Comparing vulnerability severity and exploits using case-control studies. *ACM Transactions on Information and System Security*, 17(1), Artículo 1. <https://doi.org/10.1145/2630069>
- Anwar, A., Abusnaina, A., Chen, S., Li, F., & Mohaisen, D. (2022). Cleaning the NVD: Comprehensive quality assessment, improvements, and analyses. *IEEE Transactions on Dependable and Secure Computing*, 19(6), 4255–4269. <https://doi.org/10.1109/TDSC.2021.3125270>
- Howland, H. (2023). CVSS: Ubiquitous and broken. *Digital Threats: Research and Practice*, 4(1), Artículo 1. <https://doi.org/10.1145/3491263>
- Jacobs, J., Romanosky, S., Edwards, B., Adjerid, I., & Roytman, M. (2021). Exploit Prediction Scoring System (EPSS). *Digital Threats: Research and Practice*, 2(3), Artículo 20. <https://doi.org/10.1145/3436242>
- Koscinski, V., Nelson, M., Okutan, A., Falso, R., & Mirakhorli, M. (2025). *Conflicting scores, confusing signals: An empirical study of vulnerability scoring systems (Versión 1)*. arXiv. <https://doi.org/10.48550/arXiv.2508.13644>
- Le, T. H. M., Chen, H., & Babar, M. A. (2022). A survey on data-driven software vulnerability assessment and prioritization. *ACM Computing Surveys*, 55(5), Artículo 100. <https://doi.org/10.1145/3529757>

Manai, E., Mejri, M., & Fattahi, J. (2024). Helping CNAs generate CVSS scores faster and more confidently using XAI. *Applied Sciences*, 14(20), 9231.

<https://doi.org/10.3390/app14209231>

Mell, P., Scarfone, K., & Romanosky, S. (2006). Common vulnerability scoring system. *IEEE Security & Privacy*, 4(6), 85–89.

<https://doi.org/10.1109/MSP.2006.145>

Nowak, M. R., Walkowski, M., & Sujecki, S. (2023). Support for the vulnerability management process using conversion CVSS base score 2.0 to 3.x.

Sensors, 23(4), 1802. <https://doi.org/10.3390/s23041802>

Ouraou, M. (2025). Beyond the CVSS: Rethinking the contextualisation of CVEs in a connected world. *European Conference on Cyber Warfare and Security*, 24(1), 490–500. <https://doi.org/10.34190/eccws.24.1.3529>

Ruohonen, J. (2019). A look at the time delays in CVSS vulnerability scoring.

Applied Computing and Informatics, 15(2), 129–135.

<https://doi.org/10.1016/j.aci.2017.12.002>

Santana, M., Cogo, V. V., & de Sá, A. O. (2024). SecScore: Enhancing the CVSS threat metric group with empirical evidences (Versión 1). arXiv.

<https://doi.org/10.48550/arXiv.2405.08539>

Shahid, M. R., & Debar, H. (2021). CVSS-BERT: Explainable natural language processing to determine the severity of a computer security vulnerability from its description (Versión 1). arXiv.

<https://doi.org/10.48550/arXiv.2111.08510>

Spring, J. M., Hatleback, E., Householder, A. D., Manion, A., & Shick, D.

(2021). Time to change the CVSS? *IEEE Security & Privacy*, 19(2), 74–

78. <https://doi.org/10.1109/MSEC.2020.3044475>

Wunder, J., Kurtz, A., Eichenmüller, C., Gassmann, F., & Benenson, Z. (2024).

Shedding light on CVSS scoring inconsistencies: A user-centric study

on evaluating widespread security vulnerabilities. En 2024 *IEEE*

Symposium on Security and Privacy (SP) (pp. 1102–1121). IEEE.

<https://doi.org/10.1109/SP54263.2024.00058>