

Valores CVSS v3.1 (Common Vulnerability Scoring System)

Se utilizan para medir la severidad de las vulnerabilidades informáticas.

Métricas de Explotabilidad (Exploitability Metrics)

Representan la dificultad y las condiciones necesarias para explotar la vulnerabilidad.

- **AV (Vector de Ataque / Attack Vector):** Refleja la proximidad física o lógica del atacante.
 - **N** (Network / Red): Explotable de forma remota a través de Internet.
 - **A** (Adjacent / Adyacente): Requiere acceso a la red local, Bluetooth o subred común.
 - **L** (Local / Local): Requiere acceso directo al sistema operativo (consola, SSH) o interacción local.
 - **P** (Physical / Físico): Requiere interactuar físicamente con el hardware afectado.
 - **AC (Complejidad de Ataque / Attack Complexity):** Describe las condiciones de seguridad ajenas al atacante que deben darse.
 - **L** (Low / Baja): No se requieren condiciones especiales; el ataque es replicable y constante.
 - **H** (High / Alta): Depende de factores externos impredecibles (condiciones de carrera, romper cifrados, configuraciones raras).
 - **PR (Privilegios Requeridos / Privileges Required):** Nivel de autorización que debe tener el atacante antes del ataque.
 - **N** (None / Ninguno): El atacante no necesita credenciales ni accesos previos.
 - **L** (Low / Bajos): Requiere privilegios básicos de usuario estándar sin permisos administrativos.
 - **H** (High / Altos): Requiere privilegios de administrador o de sistema con control total.
 - **UI (Interacción del Usuario / User Interaction):** Si se necesita que una persona física colabore involuntariamente.
 - **N** (None / Ninguna): El ataque se ejecuta de forma totalmente automatizada sin ayuda humana.
 - **M** (Required / Requerida): El usuario debe realizar una acción (hacer clic en un enlace, abrir un archivo).
-

Métricas de Impacto (Impact Metrics)

Definen las consecuencias directas sobre los tres pilares de la seguridad de la información (CIA) y el alcance del sistema.

- **S (Alcance / Scope):** Determina si la vulnerabilidad afecta a componentes fuera de su propia arquitectura de seguridad.
 - **U** (Unchanged / Sin cambios): El impacto se limita estrictamente al recurso o entorno de software gestionado por la misma autoridad de seguridad.
 - **C** (Changed / Cambiado): El atacante puede saltar el entorno afectado e impactar un sistema diferente o una autoridad superior (por ejemplo, escapar de una máquina virtual al host).
 - **C (Confidencialidad / Confidentiality Impact):** Mide el nivel de acceso no autorizado a los datos del sistema.
 - **N** (None / Ninguno): No hay acceso a la información confidencial.
 - **L** (Low / Bajo): Acceso parcial a ciertos datos no críticos o lectura limitada de información.
 - **H** (High / Alto): Pérdida total de confidencialidad; acceso a todos los datos restringidos del sistema.
 - **I (Integridad / Integrity Impact):** Mide la capacidad del atacante para modificar o alterar la información de forma no autorizada.
 - **N** (None / Ninguno): Los datos permanecen intactos y protegidos contra modificaciones.
 - **L** (Low / Bajo): Modificaciones menores o parciales que no comprometen la estabilidad del sistema.
 - **H** (High / Alto): Alteración total de los datos; el atacante puede borrar o modificar archivos críticos del sistema. [3]
 - **A (Disponibilidad / Availability Impact):** Mide el impacto sobre el acceso legítimo a los servicios informáticos.
 - **N** (None / Ninguno): El rendimiento y el acceso al servicio no se ven afectados en absoluto.
 - **L** (Low / Bajo): Degradación parcial del rendimiento o interrupciones temporales leves.
 - **H** (High / Alto): Denegación total del servicio (DoS); el sistema queda completamente inoperable.
-