Common Vulnerability Scoring System v3.1: Specification Document (CVSS)

Documento de especificaciones del Sistema Común de Puntuación de Vulnerabilidades.

Realizado por: José Antonio Santos Gómez

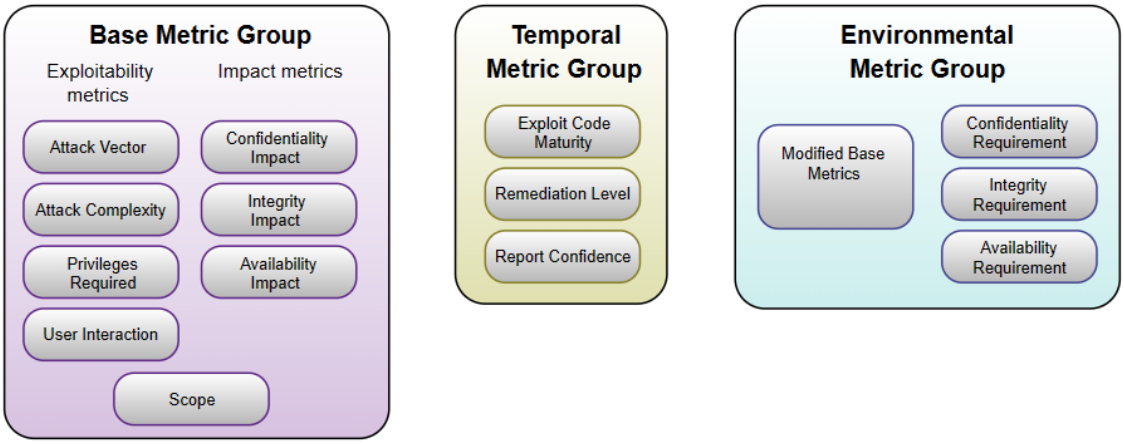
Fuente original de los datos: https://www.first.org/cvss/v3.1/specification-document

MÉTRICAS DE CVSS 3.1.

1. Introducción.

Las métricas de CVSS 3.1 consta de tres grupos: Base, Temporal y Ambiental. Cada grupo de métricas tiene un conjunto de métricas individuales que describen diferentes aspectos de una vulnerabilidad, como el vector de ataque, el nivel de privilegios requeridos, el impacto en la confidencialidad, la integridad y la disponibilidad, etc.

En la siguiente imagen se pueden observar los grupos y sus métricas:



Cada métrica tiene un conjunto de posibles valores que se asignan a una constante numérica. Estas constantes se utilizan en unas fórmulas para calcular una puntuación numérica que va de 0 a 10, siendo 10 la más grave.

La puntuación numérica también se representa como una cadena de vectores, que es una forma textual comprimida de los valores utilizados para derivar la puntuación. Este documento proporciona la especificación oficial de CVSS 3.1. Esta cadena sigue una nomenclatura estructurada y definida en este sistema de valoración de vulnerabilidades. Esta cadena puede ser interpretada para conocer en detalle las características de una vulnerabilidad.

2. Base Metrics- Métricas Base.

2.1. Exploitability Metrics- Métricas de explotación

Las métricas de explotación reflejan las características del elemento hardware o software que es vulnerable, a la que nos referimos formalmente como el componente vulnerable. Por lo tanto, cada una de las métricas de explotación que se enumeran a continuación debe puntuarse en relación con el componente vulnerable, y reflejar las propiedades de la vulnerabilidad que conducen a un ataque exitoso.

Las métricas de explotación específicas son:

- **Vector de ataque (AV)**: Este indicador refleja el contexto por el que es posible la explotación de la vulnerabilidad. Este valor de la métrica (y, en consecuencia, la puntuación base) será mayor cuanto más remoto (lógica y físicamente) pueda estar un atacante para explotar el componente vulnerable. La lista de los posibles valores se presenta en la tabla siguiente:

Valor	Abreviatura	Descripción
Red	N	La vulnerabilidad se puede explotar desde cualquier lugar, incluso desde redes externas y de Internet.
Adyacente	A	La vulnerabilidad se puede explotar desde una red adyacente o lógicamente conectada usando la misma tecnología de conexión.
Local	L	La vulnerabilidad requiere acceso local al sistema o a un servicio oculto. El atacante se conecta al sistema directamente o mediante un servicio, como puede ser SSH. También cuando se consigue propiciando la acción de un usuario para explotar la vulnerabilidad, por ejemplo: con técnicas de ingeniería social.
Físico	P	La vulnerabilidad requiere acceso físico al dispositivo vulnerable. También se incluyen ataques con dispositivos que físicamente se deben conectar al equipo, como un USB.

- **Complejidad del ataque (AC)**: Esta métrica describe las condiciones que están fuera del control del atacante y que deben existir para explotar la vulnerabilidad. Como se describe a continuación, tales condiciones pueden requerir la recopilación de más información sobre el objetivo, o excepciones computacionales. La puntuación base es mayor para los ataques menos complejos. La lista de los posibles valores se presenta en la tabla siguiente:

Valor	Abreviatura	Descripción
Baja	L	No hay condiciones especiales en el acceso al equipo o no se requiere ninguna interacción con el usuario.
Alta	H	Se requiere una condición difícil o improbable, o se requiere alguna interacción con el usuario. Se deben estudiar las condiciones del equipo y su entorno para el éxito del ataque.

- **Privilegios requeridos (PR)**: Esta métrica describe el nivel de privilegios que un atacante debe poseer antes de explotar con éxito la vulnerabilidad. La puntuación base es mayor si no se requieren privilegios. La lista de los posibles valores se presenta en la tabla siguiente:

Valor	Abreviatura	Descripción
Ninguno	N	No se requieren privilegios para explotar la vulnerabilidad.
Bajos	L	Se requieren privilegios que proporcionan un control básico del usuario sobre el componente vulnerable.
Altos	H	Se requieren privilegios que proporcionan un control significativo o total sobre el componente vulnerable. (Administrador)

- **Interacción del usuario (UI)**: Esta métrica captura el requisito de que un usuario humano, distinto del atacante, participe en el compromiso exitoso del componente vulnerable. Esta métrica determina si la vulnerabilidad se puede explotar únicamente a voluntad del atacante, o si un usuario separado (o un proceso iniciado por el usuario) debe participar de alguna manera. La puntuación base es mayor cuando no se requiere interacción del usuario. La lista de los posibles valores se presenta en la tabla siguiente:

Valor	Abreviatura	Descripción
Ninguna	N	No se requiere ninguna interacción del usuario para explotar la vulnerabilidad.
Requerida	R	Se requiere alguna interacción del usuario para explotar la vulnerabilidad. Ejemplo: el éxito depende de la instalación de una aplicación específica por parte de un administrador del sistema.

2.2. Scope (S) – Métrica de Alcance

Esta métrica captura si una vulnerabilidad en un componente vulnerable afecta a recursos en componentes más allá de su ámbito de seguridad.

Un ámbito de seguridad es un mecanismo (por ejemplo, una aplicación, un sistema operativo, un firmware, un entorno de sandbox) que define y hace cumplir el control de acceso en términos de cómo ciertos sujetos/actores (por ejemplo, usuarios humanos, procesos) pueden acceder a ciertos objetos/recursos restringidos (por ejemplo, archivos, CPU, memoria) de forma controlada. Si una vulnerabilidad en un componente vulnerable puede afectar a un componente que está en un ámbito de seguridad diferente al del componente vulnerable, se produce un cambio de ámbito. Intuitivamente, siempre que el impacto de una vulnerabilidad rompe una frontera de seguridad/confianza e impacta en componentes fuera del ámbito de seguridad en el que reside el componente vulnerable, se produce un cambio de ámbito.

La puntuación base es mayor cuando se produce un cambio de ámbito. Estos son los posibles valores para esta métrica:

Valor	Abreviatura	Descripción
Sin cambio	U	Una vulnerabilidad en un componente vulnerable no afecta a ningún componente que esté en un ámbito de seguridad diferente al del componente vulnerable.
Cambiado	C	Una vulnerabilidad en un componente vulnerable afecta a un componente que está en un ámbito de seguridad diferente al del componente vulnerable.

2.3. Impact Metrics (Métricas de impacto)

Las métricas de impacto capturan los efectos de una vulnerabilidad explotada con éxito en el componente que sufre el peor resultado que está más directamente y previsiblemente asociado con el ataque. Las métricas de impacto son:

- **Confidencialidad (C)**: Mide el impacto a la confidencialidad de los recursos de información gestionados por un componente de software debido a una vulnerabilidad explotada con éxito. La puntuación base es mayor cuando la pérdida para el componente afectado es mayor. Los posibles valores son:

Valor	Abreviatura	Constante
Ninguno	N	No hay impacto en la confidencialidad.
Bajo	L	Hay un impacto bajo en la confidencialidad.
Alto	H	Hay un alto impacto en la confidencialidad.

- **Integridad (I)**: Mide el impacto a la integridad de una vulnerabilidad explotada con éxito. La integridad se refiere a la confiabilidad y veracidad de la información. La puntuación base es mayor cuando la consecuencia para el componente afectado es mayor. Los posibles valores son:

Valor	Abreviatura	Constante
Ninguno	N	No hay impacto en la integridad.
Bajo	L	Hay un impacto bajo en la integridad.
Alto	H	Hay un impacto alto en la integridad.

- **Disponibilidad (A)**: Mide el impacto a la disponibilidad del componente afectado resultante de una vulnerabilidad explotada con éxito. Mientras que las métricas de impacto de confidencialidad e integridad se aplican a la pérdida de confidencialidad o integridad de los datos utilizados por el componente afectado, esta métrica se refiere a la pérdida de disponibilidad del propio componente afectado, como un servicio de red. La puntuación base es mayor cuando la consecuencia para el componente afectado es mayor. Los posibles valores son:

Valor	Abreviatura	Constante
Ninguno	N	No hay impacto en la disponibilidad.
Bajo	L	Hay un impacto bajo en la disponibilidad.
Alto	H	Hay un impacto alto en la disponibilidad.

3. Temporal Metrics – Métricas Temporales.

Las métricas temporales miden el estado actual de una técnica de explotación o la disponibilidad de un código, la existencia de parches o soluciones alternativas, o el conocimiento de la existencia de una vulnerabilidad.

Las métricas temporales son opcionales y se pueden omitir si no se dispone de información suficiente o relevante.

Las métricas temporales específicas son:

- **Madurez del código de explotación (E)**: Esta métrica mide la probabilidad de que la vulnerabilidad sea atacada, y se basa normalmente en el estado actual de las técnicas de explotación, la disponibilidad de código de explotación o la explotación activa “en el mundo real”. La disponibilidad pública de código de explotación fácil de usar aumenta el número de posibles atacantes al incluir a los que no tienen habilidades, lo que aumenta la gravedad de la vulnerabilidad. Los posibles valores son:

Valor	Abreviatura	Descripción
No disponible	N	No hay información suficiente para elegir ninguno del resto de valores. Este valor equivale a asignar el valor High (H).
No probado	U	No hay exploit disponible, o este exploit es teórico.

Prueba de concepto	P	Se ha publicado un código de prueba de concepto o una demostración. Esta técnica o código no es funcional en muchas ocasiones y se necesitan modificaciones por parte de un atacante experimentado.
Funcional	F	Se ha publicado un código de explotación funcional que puede causar en la mayoría de casos un impacto indeseado en el componente vulnerable.
Alto	H	Se ha publicado un código de explotación de alta calidad que es consistente y fiable en el éxito de la explotación. Este exploit es ampliamente conocido y es autónomo o no es necesario un exploit (lanzamiento manual).

- **Nivel de remediación (RL)**: El nivel de remediación de una vulnerabilidad es un factor importante para la priorización. La vulnerabilidad típica no tiene parche cuando se publica inicialmente. Las soluciones alternativas o los parches provisionales pueden ofrecer una remediación provisional hasta que se emita un parche o una actualización oficial. Cada una de estas etapas ajusta la puntuación temporal hacia abajo, reflejando la disminución de la urgencia a medida que la remediación se hace definitiva. Los posibles valores son:

Valor	Abreviatura	Descripción
Oficial	O	Se ha publicado una solución completa y permanente por el autor o el proveedor del componente vulnerable. Esta puede ser mediante un parche o una actualización.
Temporal	T	Existe una solución temporal oficial que reduce el impacto de la vulnerabilidad.
Provisional	W	Existe una solución provisional no oficial, como un parche creado por usuario para mitigar la vulnerabilidad.
No disponible	U	No hay solución conocida para la vulnerabilidad o esta solución es imposible de aplicar.
No definido	X	No se dispone de información sobre el nivel de remediación. Tiene el mismo efecto que elegir “no disponible” (U).

- **Confianza en el informe (RC)**: Esta métrica mide el grado de confianza en la existencia de la vulnerabilidad y la credibilidad de los detalles técnicos conocidos. A veces sólo se publica la existencia de vulnerabilidades, pero sin detalles específicos. Por ejemplo, se puede reconocer un impacto como indeseable, pero no se conoce la causa raíz. La vulnerabilidad puede ser corroborada posteriormente por una investigación que sugiere dónde puede estar la vulnerabilidad, aunque la investigación no esté segura. Finalmente, una vulnerabilidad puede ser confirmada mediante el reconocimiento del autor o proveedor de la tecnología afectada. La urgencia de una vulnerabilidad es

mayor cuando se sabe que existe con certeza. Esta métrica también sugiere el nivel de conocimiento técnico disponible para los posibles atacantes. Los posibles valores son:

Valor	Abreviatura	Descripción
Desconocido	U	Se ha publicado la existencia de la vulnerabilidad, pero no se ha verificado su existencia o se ha proporcionado poca información.
Razonable	R	Se ha publicado información suficiente para sugerir la existencia de la vulnerabilidad o para proporcionar detalles útiles sobre el impacto o la explotación.
Confirmado	C	Se ha confirmado la existencia de la vulnerabilidad mediante el reconocimiento del autor o el proveedor del componente vulnerable, o mediante la publicación de pruebas o análisis detallados.
No definido	X	No existe suficiente información para elegir ningún otro valor. Este valor equivale a elegir “confirmado” (C). No tiene impacto en la puntuación de su métrica.

4. Environmental Metrics – Métricas Ambientales.

Estas métricas permiten al analista personalizar la puntuación CVSS dependiendo de la importancia del activo de TI afectado para la organización del usuario, medida en términos de controles de Confidencialidad, Integridad y Disponibilidad. Las métricas son el equivalente modificado de las métricas base y se les asignan valores basados en la ubicación del componente dentro de la infraestructura organizacional.

Las métricas ambientales específicas son:

- **Requisitos de seguridad (CR, IR, AR)**: Estas métricas permiten al analista personalizar la puntuación CVSS en función de la importancia del activo de TI afectado para la organización del usuario, medida en términos de confidencialidad, integridad y disponibilidad. Cada requisito de seguridad tiene tres posibles valores: Bajo, Medio o Alto. El efecto completo en la puntuación ambiental está determinado por las métricas de impacto base modificadas correspondientes. Es decir, estas métricas modifican la puntuación ambiental al reponderar las métricas de impacto de confidencialidad, integridad y disponibilidad modificadas. Por ejemplo, el impacto de confidencialidad modificado (MC) tiene un mayor peso si el requisito de confidencialidad (CR) es Alto. Del mismo modo, el impacto de confidencialidad modificado tiene un menor peso si el requisito de confidencialidad es Bajo. El peso del impacto de confidencialidad modificado es neutro si el requisito de confidencialidad es Medio. Este mismo proceso se aplica a los requisitos de integridad y disponibilidad. Los posibles valores se muestran en la siguiente tabla:

Requisito de seguridad	Abreviatura	Valor numérico
No definido	X	No hay información suficiente para elegir ningún otro valor. No tiene impacto en la puntuación de la métrica y es equivalente a seleccionar Medio (M).
Bajo	L	La pérdida de Confidencialidad/Integridad/Disponibilidad tiene solamente un pequeño efecto adverso limitado para la organización o agentes asociados como empleados o clientes.
Medio	M	La pérdida de Confidencialidad/Integridad/Disponibilidad tiene un serio efecto adverso para la organización o agentes asociados como empleados o clientes.
Alto	H	La pérdida de Confidencialidad/Integridad/Disponibilidad tiene un catastrófico efecto adverso para la organización o agentes asociados como empleados o clientes.

- **Métricas base modificadas**: Estas métricas permiten al analista anular las métricas base individuales en función de las características específicas del entorno del usuario.

  El efecto completo en la puntuación ambiental está determinado por las métricas base correspondientes. Es decir, estas métricas modifican la puntuación ambiental al anular los valores de las métricas base, antes de aplicar los requisitos de seguridad ambiental. Por ejemplo: la configuración predeterminada para un componente vulnerable puede ser ejecutar un servicio de escucha con privilegios de administrador, para el que un compromiso podría otorgar al atacante impactos de confidencialidad, integridad y disponibilidad que son todos Altos. Sin embargo, en el entorno del analista, ese mismo servicio de Internet podría estar ejecutándose con privilegios reducidos; en ese caso, la confidencialidad modificada, la integridad modificada y la disponibilidad modificada podrían establecerse cada una en Bajo.

  Por brevedad, sólo se mencionan los nombres de las métricas base modificadas. Cada métrica ambiental modificada tiene los mismos valores que su métrica base correspondiente, más un valor de No definido.

  No definido es el valor predeterminado y utiliza el valor de la métrica de la métrica base asociada. Los posibles valores se muestran en la siguiente tabla:

Métrica base modificada	Abreviatura	Valores posibles
Vector de ataque	MAV	N, A, L, P, X
Complejidad de ataque	MAC	L, H, X
Privilegios requeridos	MPR	N, L, H, X
Interacción del usuario	MUI	N, R, X
Alcance	MS	U, C, X

Confidencialidad	MC	N, L, H, X
Integridad	MI	N, L, H, X
Disponibilidad	MA	N, L, H, X

5. Escala de puntuación cualitativa de severidad.

Para algunos propósitos, es útil tener una representación textual de las puntuaciones numéricas de Base, Temporal y Ambiental. Todas las puntuaciones se pueden asignar a las calificaciones cualitativas definidas en la suigente tabla:

Puntuación CVSS	Calificación
0.0	Ninguno
0.1 - 3.9	Bajo
4.0 - 6.9	Medio
7.0 - 8.9	Alto
9.0 - 10.0	Crítico

Como ejemplo, una puntuación CVSS de Base de 4.0 tiene una calificación de severidad asociada de Medio.

La utilización de estas calificaciones cualitativas de gravedad es opcional, y no hay ningún requisito para incluirlas al publicar las puntuaciones CVSS. Están destinadas a ayudar a las organizaciones a evaluar y priorizar adecuadamente sus procesos de gestión de vulnerabilidades.

6. Vector String - Cadena Vectorial.

La cadena vectorial de CVSS v3.1 es una representación textual de un conjunto de métricas de CVSS. Algunos aspectos importantes de este punto son:

- **Formato de la cadena vectorial**: La cadena vectorial comienza con la etiqueta “CVSS:” y una representación numérica de la versión actual, "3.1". La información de las métricas sigue en forma de un conjunto de métricas, cada una precedida por una barra inclinada, “/”, que actúa como un delimitador.

  Cada métrica es un nombre de métrica en forma abreviada, dos puntos, “:”, y su valor de métrica asociado en forma abreviada. Las formas abreviadas se definen anteriormente en esta especificación (entre paréntesis después de cada nombre de métrica y valor de métrica). Ejemplo: AV:N

- **Orden y omisión de las métricas**: Una cadena vectorial debe contener las métricas en el orden que se muestra en siguiente tabla, aunque otros ordenamientos son válidos. Todas las métricas de base deben incluirse en una cadena vectorial.

  Las métricas temporales y ambientales son opcionales, y las métricas omitidas se consideran que tienen el valor de No definido (X). Las métricas con un valor de No definido pueden incluirse explícitamente en una cadena vectorial si se desea.

Los programas que leen las cadenas vectoriales de CVSS v3.1 deben aceptar las métricas en cualquier orden y tratar las temporales y ambientales no especificadas como No definidas. Una cadena vectorial no debe incluir la misma métrica más de una vez.

- **Ejemplos de cadenas vectoriales**: Por ejemplo, una vulnerabilidad con valores de métricas de base de "Vector de ataque: Red, Complejidad de ataque: Baja, Privilegios requeridos: Altos, Interacción del usuario: Ninguna, Alcance: Sin cambios, Confidencialidad: Baja, Integridad: Baja, Disponibilidad: Ninguna" y sin métricas temporales o ambientales especificadas produciría la siguiente cadena vectorial:

  CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N

  El mismo ejemplo con la adición de "Explotabilidad: Funcional, Nivel de remediación: No definido" y con las métricas en un orden no preferido produciría la siguiente cadena vectorial:

  CVSS:3.1/S:U/AV:N/AC:L/PR:H/UI:N/C:L/I:L/A:N/E:F/RL:X

- A continuación, se muestra la tabla con los grupos de métricas y su orden:

Métrica	Abreviatura	Valores	¿Obligatorio?
Grupo de métricas base	**/**		**Sí**
Vector de ataque	AV	N, A, L, P	Sí
Complejidad de ataque	AC	L, H	Sí
Privilegios requeridos	PR	N, L, H	Sí
Interacción del usuario	UI	N, R	Sí
Alcance	S	U, C	Sí
Impacto en la confidencialidad	C	N, L, H	Sí
Impacto en la integridad	I	N, L, H	Sí
Impacto en la disponibilidad	A	N, L, H	Sí
Grupo de métricas temporales	**/**		**No**
Maduración Código Exploit	E	X, U, P, F, H	No
Nivel de remediación	RL	X, O, T, W, U	No
Confianza en el reporte	RC	X, U, R, C	No
Grupo de métricas ambientales	**/**		**No**
Requerimiento de confidencialidad	CR	X, L, M, H	No
Requerimiento de integridad	IR	X, L, M, H	No
Requerimiento de disponibilidad	AR	X, L, M, H	No
Vector de ataque modificado	MAV	X,N,A,L,P	No

Complejidad de Ataque Modificada	MAC	X,L,H	No
Privilegios requeridos Modificado	MPR	X,N,L,H	No
Interacción del usuario Modificado	MUI	X,N,R	No
Alcance Modificado	MS	X,U,C	No
Impacto modificado en la confidencialidad	MC	X, N, L, H	No
Impacto modificado en la integridad	MI	X, N, L, H	No
Impacto modificado en la disponibilidad	MA	X, N, L, H	No

Las métricas de la base son obligatorias, mientras que las métricas temporales y ambientales son opcionales. Las métricas no especificadas se consideran como No definidas (X).