



*Informe de divulgación*  
**CVSS**  
*Un sistema para valorar vulnerabilidades*

Tipo de documento: *Informe*  
Autor del documento: *AndalucíaCERT*  
Código del Documento: *CERT-IF-5902-140728*  
Edición: *0*  
Categoría: *Público*  
Fecha de elaboración: *28/07/2014*  
Nº de Páginas: *1 de 17*

<i>Informe de divulgación CVSS Un sistema para valorar vulnerabilidades</i>	Código	<i>CERT-IF-5902-140728</i>
	Edición	<i>0</i>
	Fecha	<i>28/07/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 2 de 17

## 1 TABLA DE CONTENIDOS

<a href="#">TABLA DE CONTENIDOS.....</a>	<a href="#">2</a>
<a href="#">OBJETO Y ALCANCE.....</a>	<a href="#">3</a>
<a href="#">INTRODUCCIÓN .....</a>	<a href="#">3</a>
<a href="#">FUNCIONAMIENTO DE CVSS .....</a>	<a href="#">5</a>
<a href="#">INDICADORES.....</a>	<a href="#">6</a>
<a href="#">VECTORES.....</a>	<a href="#">13</a>
<a href="#">HERRAMIENTAS.....</a>	<a href="#">13</a>
<a href="#">UN EJEMPLO PRÁCTICO: CVE-2003-0818.....</a>	<a href="#">14</a>
<a href="#">OTROS SISTEMAS DE PUNTUACIÓN DE VULNERABILIDADES.....</a>	<a href="#">16</a>
<a href="#">CONCLUSIONES.....</a>	<a href="#">16</a>
<a href="#">GLOSARIO.....</a>	<a href="#">17</a>
<a href="#">REFERENCIAS.....</a>	<a href="#">17</a>

<i>Informe de divulgación CVSS Un sistema para valorar vulnerabilidades</i>	Código	<i>CERT-IF-5902-140728</i>
	Edición	<i>0</i>
	Fecha	<i>28/07/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. <b>3</b> de 17

## 2 OBJETO Y ALCANCE

El objetivo de este documento es describir el funcionamiento del sistema de puntuación de vulnerabilidades CVSS (Common Vulnerability Scoring System) usado para establecer una métrica común en el proceso de evaluación de vulnerabilidades.

Este documento va destinado al personal de la Junta de Andalucía y al público en general. En éste se describe el funcionamiento general del sistema CVSS, las distintas métricas utilizadas, así como un ejemplo práctico de cómo medir una vulnerabilidad conocida usando este sistema.

## 3 INTRODUCCIÓN

### ¿Qué es CVSS?

En la actualidad, los departamentos encargados de la gestión de los activos de TI deben identificar y evaluar las vulnerabilidades a través de una gran variedad de sistemas hardware y plataformas de software. Es por ello que se hace necesario poder establecer una prioridad según un nivel de riesgo con el objetivo de evaluar qué vulnerabilidades son potencialmente más peligrosas y, por tanto, más urgentes de tratar.

CVSS (Common Vulnerability Scoring System) es una propuesta que intenta estandarizar una métrica común para evaluar vulnerabilidades. La idea es obtener un valor medible que nos ofrezca una idea del peligro potencial que supone la presencia de una vulnerabilidad determinada, ayudando a transmitir y evaluar la gravedad y permitiendo determinar la urgencia y prioridad de la misma.

Este sistema ofrece lo siguiente:

- **Puntuaciones de vulnerabilidad estandarizadas:** Permite la normalización de la valoración sobre vulnerabilidades en todas las plataformas de una organización (hardware y software). Con esto podrán establecer umbrales en su política de gestión de vulnerabilidades, donde establecer el tiempo y la urgencia con la que tiene que ser validada y remediada.
- **Framework abierto:** Las características individuales de la vulnerabilidad que han llevado a la asignación de la puntuación son de dominio público.
- **Riesgo priorizado:** Existe un tipo de valoración que depende del contexto concreto de cada organización en el que tenga lugar la vulnerabilidad. Esto permite representar el riesgo real de una organización.

<i>Informe de divulgación CVSS Un sistema para valorar vulnerabilidades</i>	Código	<i>CERT-IF-5902-140728</i>
	Edición	<i>0</i>
	Fecha	<i>28/07/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 4 de 17

## ¿Quién es el propietario de CVSS?

CVSS se encuentra bajo la custodia del [Forum of Incident Response and Security Teams \(FIRST\)](#), sin embargo es un estándar completamente abierto y libre. Ninguna organización “posee” CVSS, no siendo obligatorio pertenecer a FIRST para usar o aplicar CVSS. La única petición de FIRST es que las organizaciones que publiquen los resultados se ajusten a las directrices descritas en la guía de referencia de CVSS y aporten información de cómo se obtuvo.



## ¿Qué es lo que CVSS mide?

CVSS mide características de una vulnerabilidad en base a tres métricas:

- **Métrica base:** Aspectos de la vulnerabilidad constantes en el tiempo y entorno. Estas métricas se basan en características intrínsecas de la propia vulnerabilidad y que no dependen más que de su propia naturaleza. Ejemplo: La complejidad para ser explotada, si es local o remota, o si se requiere autenticación, así como el grado en que compromete la confidencialidad, integridad y disponibilidad del sistema.
- **Métrica temporal:** Miden aspectos de la vulnerabilidad que pueden cambiar en el tiempo, pero no dependen del entorno en el que tenga lugar. Ejemplo: La existencia de un parche que la corrija en ese momento, la existencia de un programa público que permita que sea explotada y aprovechada.
- **Métricas del entorno ó medioambiental:** Características que son relevantes y particulares del entorno en el que se presentan. Permiten que la medición se adecúe a nuestra organización.

De la métricas base se deriva una puntuación de 0 a 10, que puede verse reducida en función de los valores de las métricas "temporal" y "medioambiental".

Los aspectos o características a los que nos referimos para cada métrica y que permiten calcular su valor son denominados **indicadores**.

<i>Informe de divulgación</i> <i>CVSS Un sistema para valorar vulnerabilidades</i>		Código	<i>CERT-IF-5902-140728</i>
		Edición	<i>0</i>
		Fecha	<i>28/07/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 5 de 17	

## ¿Quién usa CVSS?

CVSS es usado por diferentes tipos de organizaciones, entre ellas encontramos:

- **Proveedores de boletines de vulnerabilidades:** Que se encargan de publicar, tanto de manera comercial como sin ánimo de lucro, boletines con la puntuación usando la métrica CVSS. Estos boletines ofrecen además otro tipo de información como la fecha de descubrimiento de la vulnerabilidad, sistemas afectados y enlaces a los proveedores para las recomendaciones de resolución.
- **Proveedores de Software de aplicaciones:** Que proporcionan las puntuaciones base y los vectores CVSS a sus clientes. Esto les ayuda a establecer la gravedad de las vulnerabilidades de sus productos y ayuda a los clientes a gestionar el riesgo de manera eficaz.
- **Organizaciones de usuarios:** Muchas organizaciones privadas usan las métricas CVSS de manera interna para tomar decisiones fundamentadas relativas a a gestión de vulnerabilidades.
- **Empresas de gestión de riesgos de seguridad:** Que usan las calificaciones CVSS como entrada para el cálculo del riesgo de la organización o el nivel de amenaza.
- **Investigadores:** El diseño abierto de CVSS permite a los investigadores, establecer sus propias puntuaciones así como realizar análisis estadísticos de las vulnerabilidades y de sus propiedades.

## 4 FUNCIONAMIENTO de CVSS

En este punto describiremos cómo se realiza el cálculo de las métricas de CVSS que nos permitirán evaluar una vulnerabilidad.

CVSS proporciona por cada métrica un conjunto de **indicadores** que van a tenerse en cuenta y a los que se irán asignando valores numéricos. Con todos los indicadores valorados obtendremos el **vector** de la métrica. Un vector es una cadena de texto que contiene los valores asignados a cada indicador. Éste sirve para tener definido cómo hemos sacado los valores de cada métrica.

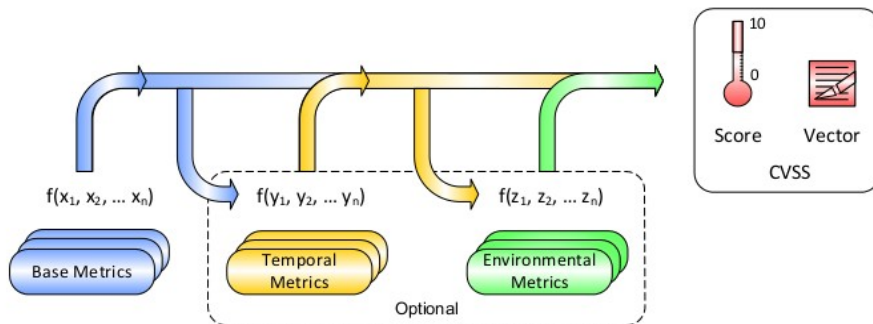
La primera métrica que debemos obtener es la métrica base. Por tanto deberemos de asignar los valores a sus indicadores y crear el vector de la métrica. A partir de éste obtendremos una puntuación entre 0 y 10.

La métrica base se puede afinar mediante la asignación de valores a las métricas temporales y de entorno. Estas son útiles para proporcionar un contexto adicional para una vulnerabilidad determinada al reflejar con mayor precisión el riesgo que representa la vulnerabilidad con el entorno concreto del usuario.

La métrica temporal se obtendría de forma similar a la métrica base. Ésta es calculada a partir de los valores que asignemos a sus indicadores, y a partir de esto obtendremos el vector asociado. Además, la ecuación temporal se combina a la puntuación base para producir una puntuación de 0 a 10. Y de igual forma con la métrica de entorno. La ecuación de entorno combinará la puntuación temporal para producir

<b>Informe de divulgación</b> <b>CVSS Un sistema para valorar vulnerabilidades</b>		Código	CERT-IF-5902-140728
		Edición	0
		Fecha	28/07/2014
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 6 de 17	

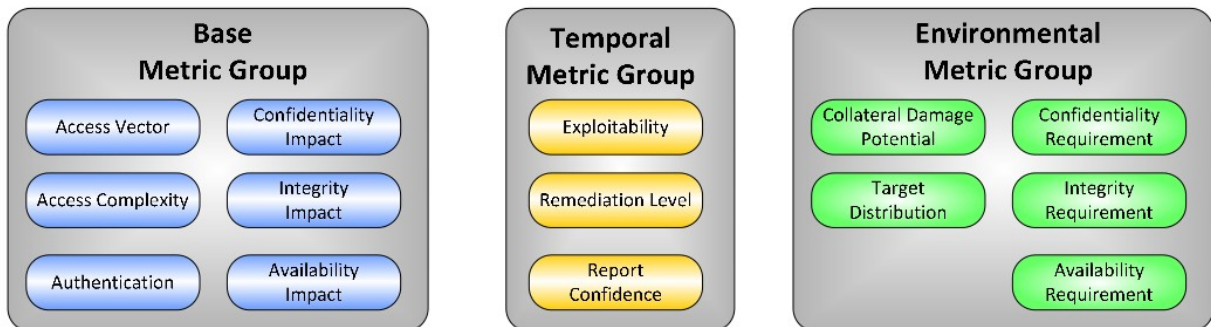
una puntuación de entorno entre 0 y 10. Se puede observar el funcionamiento general en el siguiente esquema:



## 5 INDICADORES

En general, los indicadores base y temporales son especificados por los proveedores de productos de seguridad, proveedores de aplicaciones o mediante los boletines de vulnerabilidades, ya que suelen tener mejor información sobre las características de la vulnerabilidad que los usuarios. Sin embargo, las métricas de entorno deben ser especificadas por los usuarios ya que son éstos los que mejor pueden determinar el impacto potencial de una vulnerabilidad en su propio entorno.

Como hemos indicado anteriormente, CVSS distingue entre tres métricas básicas. Éstas, a su vez se descomponen en indicadores, como se puede observar en la siguiente imagen:



En los siguientes puntos vamos a describir cada una de las indicadores que se tienen en cuenta en el cálculo de cada una de las métricas.

<i>Informe de divulgación</i> <i>CVSS Un sistema para valorar vulnerabilidades</i>		Código	<i>CERT-IF-5902-140728</i>
		Edición	<i>0</i>
		Fecha	<i>28/07/2014</i>
Tipo de documento: <i>Informe</i>		Categoría: <i>Público</i>	Pág. 7 de 17

## 5.1 INDICADORES BASE

Engloba las características de una vulnerabilidad que permanecen constantes. Entre estas características se encuentran:

- **Acceso:** Los indicadores Vector de acceso, la Complejidad de acceso y la Autenticación capturan cómo se accede a la vulnerabilidad y si requiere especiales para poder explotarla.
- **Impacto:** Esta característica viene definida por cómo afecta la vulnerabilidad al activo en cuanto a Confidencialidad, Integridad y Disponibilidad se refiere. Miden el impacto cómo un grado de pérdida en cada una de las dimensiones de la seguridad.

### 5.1.1 Vector de acceso (AV)

Este indicador proporciona información sobre la ubicación del atacante en el instante de llevar a cabo la explotación de la vulnerabilidad.

Valores	Descripción del tipo de explotación
Local (L)	Mediante acceso local. Requiere acceso físico o una cuenta local. Ejemplo: ataques mediante periféricos (USB) y escalado de privilegios locales (sudo).
Red adjacente (A)	Mediante acceso a la red adjacente Ejemplo: redes locales, Bluetooth, IEEE 802.1 y segmento local Ethernet.
Red (N)	Mediante acceso a la red. El atacante no requiere acceso a la red local o de acceso local. Ejemplo: desbordamiento de buffer RPC.

### 5.1.2 Complejidad de acceso (AC)

Mide la complejidad del ataque requerido para explotar la vulnerabilidad. Cuanto menor sea la complejidad requerida, mayor será la puntuación.

Valores	Descripción
Alto (H)	Existen condiciones de acceso especializadas. Ejemplo: hay que contar con privilegios elevados, depende de métodos de ingeniería social que podrían ser detectables, configuración vulnerable rara de ver en la práctica.
Medio (M)	Las condiciones de acceso son poco especializadas. Ejemplo: el ataque requiere algo de ingeniería social, la configuración del afectado no es la predeterminada, hace falta obtener algo de información antes de realizar el ataque, el ataque se limita a un cierto grupo o usuarios con cierto nivel de autorización.
Bajo (L)	No existen condiciones de acceso especializados. Ejemplo: accesos anónimos, configuraciones por defecto, requerimiento de pocas habilidades técnicas.

<i>Informe de divulgación CVSS Un sistema para valorar vulnerabilidades</i>		Código	<i>CERT-IF-5902-140728</i>
		Edición	<i>0</i>
		Fecha	<i>28/07/2014</i>
Tipo de documento: <i>Informe</i>		Categoría: <i>Público</i>	Pág. 8 de 17

### 5.1.3 Autenticación (AU)

Mide el número de veces que un atacante debe autenticarse en un objetivo para explotar la vulnerabilidad. No mide la complejidad del proceso de autenticación.

Valores	Descripción
Multiple (M)	Requiere que el atacante se autentique dos o más veces, incluso si las credenciales son las mismas. Ejemplo: autenticación a un sistema operativo además de proporcionar las credenciales para acceder a una aplicación alojada en el sistema.
Simple (S)	Se requiere una instancia de autenticación para acceder y explotar la vulnerabilidad.
Ninguno (N)	La autenticación no es necesaria para acceder y explotar la vulnerabilidad.

### 5.1.4 Impacto en la confidencialidad (C)

Mide el impacto en la confidencialidad cuando una vulnerabilidad es explotada con éxito. Un mayor impacto en la confidencialidad aumenta el valor del indicador.

Valores	Descripción
Ninguno (N)	No hay impacto en la confidencialidad del sistema.
Parcial (P)	Existe una considerable liberación de información. El acceso a algunos ficheros del sistema es posible, pero el atacante no tiene control sobre que obtiene. Ejemplo: una vulnerabilidad que libera sólo ciertas tablas de una base de datos.
Completa (C)	Hay una total liberación de la información. Todos los ficheros del sistema han sido liberados.

### 5.1.5 Impacto en la integridad (I)

Mide el impacto en la integridad cuando una vulnerabilidad es explotada con éxito. Un mayor impacto en la integridad aumenta el valor del indicador.

Valores	Descripción
Ninguno (N)	No hay ningún impacto en la integridad del sistema.
Parcial (P)	Es posible la modificación de algunos archivos del sistema y la información, pero el atacante no tiene control sobre lo que se puede modificar, o el alcance de a lo que puede afectar es limitada. Ejemplo: los archivos del sistema o aplicación pueden ser modificados, pero o bien el atacante no tiene control sobre los archivos que se ven afectados o sólo puede modificar archivos en un contexto limitado o alcance.
Completa (C)	Compromiso total de la integridad del sistema. El atacante puede modificar cualquier archivo del sistema destino.



<b>Informe de divulgación</b> <b>CVSS Un sistema para valorar vulnerabilidades</b>		Código	<i>CERT-IF-5902-140728</i>
		Edición	<i>0</i>
		Fecha	<i>28/07/2014</i>
Tipo de documento: <i>Informe</i>		Categoría: <i>Público</i>	Pág. 9 de 17

### 5.1.6 Impacto en la disponibilidad (A)

Mide el impacto en la disponibilidad cuando una vulnerabilidad es explotada con éxito. Un mayor impacto en la disponibilidad aumenta el valor del indicador.

Valores	Descripción
Ninguno (N)	No hay ningún impacto en la disponibilidad del sistema.
Parcial (P)	Hay una disminución del rendimiento o interrupciones en la disponibilidad de los recursos. Ejemplo: ataque de inundación basado en red que permite a un número limitado de conexiones exitosas el acceso a un servicio de Internet.
Completa (C)	Se produce un falta de acceso total al recurso afectado. El atacante hace que el recurso esté totalmente no disponible.

## 5.2 INDICADORES TEMPORALES

Es común que la amenaza planteada por una vulnerabilidad pueda cambiar medida que pasa el tiempo. CVSS tiene en cuenta este hecho y para ello se definen los indicadores temporales. Éstos son:

- Explotabilidad
- Estado de la solución
- Confianza en el informe de la vulnerabilidad

Los indicadores de entorno son opcionales, el valor resultante no tendrá ningún efecto en la puntuación.

### 5.2.1 Explotabilidad (E)

Mide el estado actual de las técnicas de explotación o la disponibilidad del [exploit](#) para el aprovechamiento de la vulnerabilidad. Si el exploit está disponible públicamente o si ni siquiera es necesario un exploit para aprovecharla, el número de posibles atacantes aumenta y con ello la probabilidad de ser atacados. Por tanto la vulnerabilidad se torna más grave.

Valores	Descripción
No comprobados (U)	El código de explotación no está disponible, o el exploit es totalmente teórico.
Prueba de concepto (POC)	Prueba de concepto o demostración de un ataque no práctico para la mayoría de los sistemas disponibles. El código o técnica no es funcional en todas las situaciones o puede requerir una modificación sustancial por un atacante con altas habilidades técnicas.
Funcional (F)	Código exploit funcional disponible. El código funcionará en la mayoría de las situaciones.
Alto (H)	No es necesario un exploit o es explotable por código autónomo móvil y los detalles son ampliamente disponibles. El código funciona en cada situación, o está siendo activamente liberado vía agente autónomo móvil (como gusano o virus).
No definido (ND)	Este valor no influye en el indicador. Usar para omitir este indicador.

<b>Informe de divulgación</b> <b>CVSS Un sistema para valorar vulnerabilidades</b>		Código	<i>CERT-IF-5902-140728</i>
		Edición	<i>0</i>
		Fecha	<i>28/07/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 10 de 17	

### 5.2.2 Estado de la solución (RL)

Habitualmente, las vulnerabilidades no están parcheadas en el momento en que se hacen públicas. Los paliativos (workaround) o [hotfixes](#) pueden ofrecer soluciones temporales hasta que el fabricante publique una solución oficial. Cada una de estas fases se ajusta a una puntuación del indicador, decreciendo la urgencia a medida que se acerca la solución final. Cuanto menos oficial y permanente es la solución disponible, más alta es la puntuación de la vulnerabilidad.

Valores	Descripción
Solución oficial (DE)	Una solución oficial está disponible. Parche o actualización disponible.
Solución temporal (TF)	No hay solución oficial, pero sí temporal. Incluye casos en los que el proveedor emite una revisión temporal, herramienta o solución.
Workaround (W)	No hay solución oficial del proveedor. Los usuarios de la tecnología afectada crean un parche para evitar o mitigar la vulnerabilidad.
No disponible (U)	No hay solución disponible o es imposible de aplicar.
No definido (ND)	Este valor no influye en el indicador. Usar para omitir este indicador.

### 5.2.3 Confianza en el informe (RC)

Este factor determina el grado de confianza en la existencia de la vulnerabilidad y la credibilidad de los detalles técnicos conocidos y reportados sobre ella. A veces se publican vulnerabilidades (por ejemplo, en foros), sin ningún tipo de comprobación o confirmación oficial sobre la veracidad o alcance de la información. El hecho de que se muestren estos detalles, que sea confirmado por la parte afectada o que sea reconocido por el fabricante aumenta las probabilidades de que esta vulnerabilidad tengan efecto en el sistema al que afecta.

Valores	Descripción
Sin confirmar (UC)	Hay una sola fuente no confirmada o múltiples informes contradictorios. Hay poca confianza en la validez de los informes.
No corroborada (UR)	Hay varias fuentes no oficiales, compañías de seguridad independientes u organizaciones de investigación.
Confirmada (C)	Ha sido confirmada por el proveedor. También puede ser confirmada cuando su existencia la confirma un acontecimiento externo, como la publicación de un exploit funcional o de prueba de concepto o de explotación generalizada.
No definida (ND)	Este valor no influye en el indicador. Usar para omitir este indicador.

<b>Informe de divulgación</b> <b>CVSS Un sistema para valorar vulnerabilidades</b>		Código	CERT-IF-5902-140728
		Edición	0
		Fecha	28/07/2014
Tipo de documento: <i>Informe</i>		Categoría: <i>Público</i>	Pág. 11 de 17

### 5.3 INDICADORES DE ENTORNO

Las diferencias entre un entorno u otro puede tener una gran repercusión en el riesgo que una vulnerabilidad supone para una organización. Este grupo de indicadores engloban las características de una vulnerabilidad asociadas al entorno del usuario. No existe un valor "universal" para esta métrica, como es el de la base, sino que cada administrador podrá calcular el suyo.

Los indicadores de entorno, al igual que los temporales, son opcionales e incluyen un valor que no tiene ningún efecto en la puntuación.

La puntuación final para la métrica de entorno está compuesta de 2 grupos de indicadores:

- Modificadores generales de entorno
  - Daños colaterales potenciales
  - Distribución del objetivo
- Modificadores de impacto

El valor calculado de esta métrica será por tanto un par de valores. Por ejemplo: (8, 9'6)

#### 5.3.1 Daños colaterales potenciales (CDP)

Mide el potencial de pérdida de vidas humanas o bienes materiales a través del daño, robo de bienes o de equipos. ¿Cuánto daño me haría la explotación de esta vulnerabilidad? También puede medir la pérdida económica de la productividad o los ingresos. Cuanto mayor sea el potencial de daño, mayor será la puntuación.

Valores	Descripción
Ninguno (N)	No hay posibilidad de pérdida de vidas, bienes físicos, productividad o ingresos.
Bajo (L)	Una explotación exitosa puede provocar un leve daño físico o a la propiedad. O bien, puede haber una ligera pérdida de ingresos o de productividad en la organización.
Bajo-Medio (LM)	Puede provocar daños físicos o en la propiedad moderados. O, puede haber una moderada pérdida de los ingresos o en la productividad en la organización.
Medio-Alto (MH)	Puede resultar una pérdida física significativa o en la propiedad. O, puede haber una pérdida significativa en los ingresos o en la productividad.
Alto (H)	Puede provocar daños y pérdida catastróficos. O, puede haber una pérdida catastrófica en los ingresos o en la productividad.
No definido (ND)	Este valor no influye en el indicador. Usar para omitir este indicador.

<b>Informe de divulgación</b> <b>CVSS Un sistema para valorar vulnerabilidades</b>		Código	<i>CERT-IF-5902-140728</i>
		Edición	<i>0</i>
		Fecha	<i>28/07/2014</i>
Tipo de documento: <i>Informe</i>		Categoría: <i>Público</i>	Pág. <b>12</b> de 17

### 5.3.2 Distribución del objetivo (TD)

Mide la proporción de los sistemas vulnerables. Tiene como objetivo aproximar el porcentaje de sistemas que podrían verse afectados por la vulnerabilidad. Cuanto mayor sea la proporción de los sistemas vulnerables, mayor será la puntuación.

Valores	Descripción
Ninguno (N)	No existen sistemas destino o los objetivos son tan especializados que sólo existen en un entorno de laboratorio. 0% del entorno está en riesgo.
Bajo (L)	Existen objetivos en el entorno, pero en pequeña escala. Entre un 1% - 25% de todo el entorno está en riesgo.
Mediano (M)	Existen objetivos en el entorno, en escala media. Entre el 26% - 75% del total está en riesgo.
Alto (H)	Existen objetivos en una escala considerable. Entre el 76% - 100% del total se considera en riesgo.
No definido (ND)	Este valor no influye en el indicador. Usar para omitir este indicador.

### 5.3.3 Modificadores de impacto: Requerimientos de seguridad (CR, IR, AR)

Permite al analista personalizar la puntuación dependiendo de la importancia del activo afectado en una organización, medido en términos de confidencialidad, integridad y disponibilidad. Si se considera que para las funciones que desempeña un activo la disponibilidad es más importante, se puede asignar un mayor valor a ésta en relación a las otras dos dimensiones.

Estos indicadores modifican la puntuación base con una nueva ponderación para la confidencialidad, integridad y disponibilidad.

Valores	Descripción
Bajo (L)	Pérdida de [C   I   D] puede que tenga un efecto negativo limitado en la organización.
Medio (M)	Pérdida de [C   I   D] puede que tenga un efecto adverso en la organización.
Alto (H)	Pérdida de [C   I   D] puede que tenga un efecto adverso catastrófico en la organización.
No definido (ND)	Este valor no influye en el indicador. Usar para omitir este indicador.

<i>Informe de divulgación CVSS Un sistema para valorar vulnerabilidades</i>		Código	CERT-IF-5902-140728
		Edición	0
		Fecha	28/07/2014
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 13 de 17	

## 6 VECTORES

El conjunto de indicadores y sus valores asignados que conforman una métrica es representado mediante una estructura de datos llamada vector.

Cada indicador en el vector es representado por su abreviatura, seguida seguida ":" y el valor asignado al indicador. Se utiliza la barra inclinada "/" para separar los indicadores. Si no se va a utilizar un indicador temporal o de entorno se le asigna "ND" (no definido).

- **Base:** AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
- **Temporal:** E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/RC:[UC,UR,C,ND]
- **De entorno:** CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H,ND]/ IR:[L,M,H,ND]/AR:[L,M,H,ND]

Así, por ejemplo, tengamos una vulnerabilidad con los siguientes indicadores base:

- Vector acceso: Bajo("Low")
- Complejidad de acceso: Media ("Medium")
- Autenticación: Ninguno
- Impacto Confidencialidad: No definido
- Impacto Integridad: Parcial
- Impacto Disponibilidad: Completa ("Complete")

El vector que representa este conjunto es el siguiente: "AV: L / AC: M / Au: N / A: N / I: P / A: C"

## 7 HERRAMIENTAS

A continuación se muestran algunas herramientas que nos resultarán útiles a la hora de realizar el cálculo de las métricas CVSS.

- Calculadora CVSS:
  - [NVD Calculator](#)
  - [Security Database Calculator](#)
- Webs y bases de datos de vulnerabilidades:
  - [CVE details](#)
  - [National Vulnerability Database \(NVD\)](#)
  - [Open Sourced Vulnerability Database \(OSBDV\)](#)

Muchas de estas webs suelen almacenar además información general de las vulnerabilidades, incluyendo documentación, pruebas de concepto, soluciones, versiones a las que afecta, etc.

<b>Informe de divulgación</b> <b>CVSS Un sistema para valorar vulnerabilidades</b>		Código	CERT-IF-5902-140728
		Edición	0
		Fecha	28/07/2014
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 14 de 17	

## 8 UN EJEMPLO PRÁCTICO: CVE-2003-0818

Vamos a ver como ejemplo la vulnerabilidad descrita en el [CVE-2003-0818](#) (Microsoft Windows ASN.1 Library Integer Handling Vulnerability). En Septiembre de 2003, se descubrió una vulnerabilidad que afectaba una librería llamada ASN.1 de los sistemas operativos Windows. De conseguir explotarse, esta vulnerabilidad permitiría a un atacante ejecutar código a su elección en el sistema víctima con privilegios de administración.

### Métrica Base

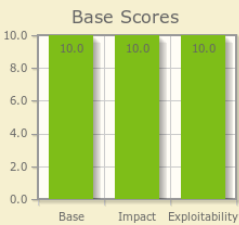
- Es explotable de manera remota, por tanto, Vector de acceso (AV) se establecería a "Red" (Network).
- La complejidad del acceso (AC) se establecería en "Baja" (Low), debido a que no es necesario que se cumplan circunstancias especiales para la explotación de la vulnerabilidad.
- No es necesario autenticarse en el sistema para la explotación de la vulnerabilidad, por tanto, Autenticación (AU), se establecería a "None".
- Cada uno de los indicadores de impacto se ajusta en "completa" por la posibilidad de un compromiso total del sistema. En conjunto, estas medidas producen una puntuación máxima de la base 10.0.

El vector base para esta vulnerabilidad es por lo tanto:  $AV: N / AC: L / Au: N / A: C / I: C / A: C$

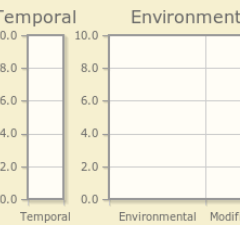
### Common Vulnerability Scoring System Version 2 Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the [CVSS standards guide](#) to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

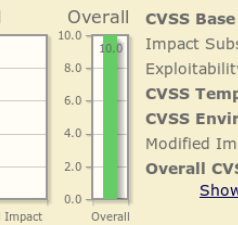
**Base Scores**



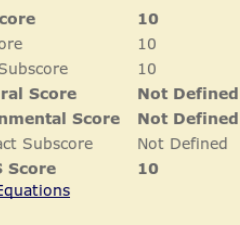
**Temporal**



**Environmental**



**Overall**



<b>CVSS Base Score</b>	<b>10</b>
Impact Subscore	10
Exploitability Subscore	10
<b>CVSS Temporal Score</b>	<b>Not Defined</b>
<b>CVSS Environmental Score</b>	<b>Not Defined</b>
Modified Impact Subscore	Not Defined
<b>Overall CVSS Score</b>	<b>10</b>
<a href="#">Show Equations</a>	

**CVSS v2 Vector (AV:N/AC:L/Au:N/C:I/C:A:C)**

▼ Base Score Metrics

**Exploitability Metrics**

Access Vector (AV)\*

Local (AV:L)    Adjacent Network (AV:A)    Network (AV:N)

Access Complexity (AC)\*

High (AC:H)    Medium (AC:M)    Low (AC:L)

Authentication (Au)\*

Multiple (Au:M)    Single (Au:S)    None (Au:N)

**Impact Metrics**

Confidentiality Impact (C)\*

None (C:N)    Partial (C:P)    Complete (C:C)

Integrity Impact (I)\*

None (I:N)    Partial (I:P)    Complete (I:C)

Availability Impact (A)\*

None (A:N)    Partial (A:P)    Complete (A:C)

\* - All base metrics are required to generate a base score.

Si queremos además, calcular las métricas temporales y de entorno, quedaría de la siguiente manera:

<b>Informe de divulgación</b> <b>CVSS Un sistema para valorar vulnerabilidades</b>		Código	CERT-IF-5902-140728
		Edición	0
		Fecha	28/07/2014
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 15 de 17	

### Métricas temporales

- Se verifica la existencia de exploits públicos y funcionales, por lo que la Explotabilidad (E) se establece en "Funcional".
- En febrero de 2004, Microsoft lanzó el parche MS04-007 que solucionaba la vulnerabilidad, por lo que el indicador Nivel de Recuperación (RL) se establece en "Solución oficial".
- La vulnerabilidad se encuentra plenamente confirmada por el fabricante, por lo que el indicador Confianza en el informe (RC) se establecerá en "Confirmado".

Todo esto, nos devuelve una **puntuación temporal de 8,3**.

### Métricas de entorno:

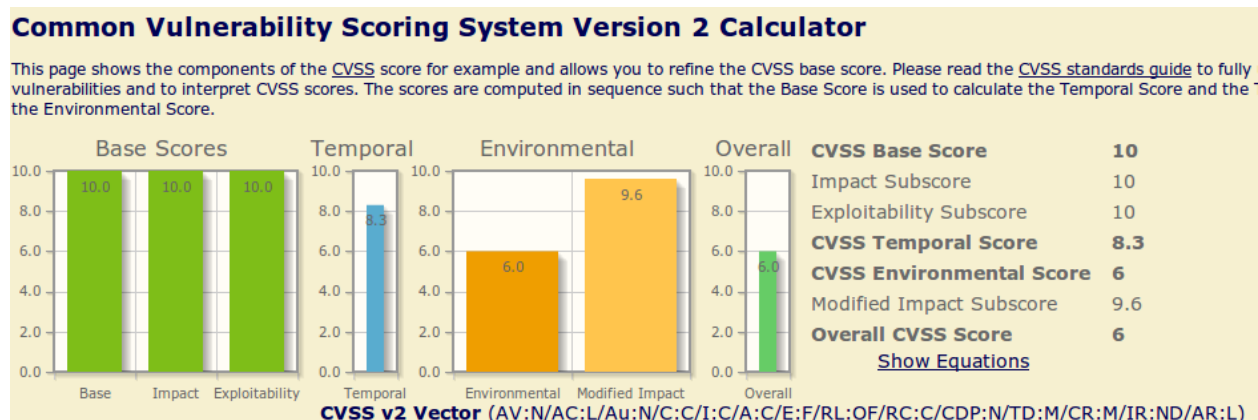
Para el sistema afectado, en nuestra organización los requerimientos de seguridad son los siguientes:

- Disponibilidad: Baja
- Confidencialidad: Media
- Integridad: No aplica

En cuanto a los modificadores de entorno generales, tenemos los siguientes valores para los indicadores definidos:

- Posibles daños colaterales: Ninguno (N)
- Distribución del objetivo: Mediano (M)

La puntuación de la métrica de entorno podría ser la siguiente: **(6, 9'6)**



El vector CVSS resultante es el siguiente:

(AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C/CDP:N/TD:M/CR:M/IR:ND/AR:L)

<i>Informe de divulgación</i> <i>CVSS Un sistema para valorar vulnerabilidades</i>		Código	<i>CERT-IF-5902-140728</i>
		Edición	<i>0</i>
		Fecha	<i>28/07/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 16 de 17	

## 9 OTROS SISTEMAS DE PUNTUACIÓN DE VULNERABILIDADES

Además de CVSS, existen otros sistemas de evaluación de vulnerabilidades, algunos gestionados por organizaciones sin ánimo de lucro. Cada uno tiene sus ventajas, pero principalmente difieren entre ellos por lo que miden:

- **CERT/CC:** Produce una puntuación numérica entre 0 y 180. Considera factores tales como si la infraestructura de Internet está en riesgo o qué tipo de condiciones previas son necesarias para explotar la vulnerabilidad.
- **SANS:** Considera si la debilidad se encuentra en las configuraciones por defecto o sistemas de cliente o servidor.
- **Microsoft:** Intenta reflejar la dificultad de explotación y el impacto global de la vulnerabilidad.

A pesar de que son útiles, estos sistemas de puntuación proporcionan un enfoque único para todos. Es decir, no tienen métricas temporales ni medioambientales, por lo que asumen que el impacto de la vulnerabilidad es constante para cada individuo y la organización.

## 10 CONCLUSIONES

Uno de los temas más críticos sobre el que gira el mundo de la seguridad es el estudio y control de vulnerabilidades. Pero, ¿quién y cómo se valora la gravedad de una vulnerabilidad? ¿Qué es exactamente un riesgo "alto" o una "vulnerabilidad crítica"? ¿Es cierto que según quien describa el fallo, la gravedad parecerá más o menos grave? Resulta complejo valorar el peligro de forma objetiva y para solucionar esto nació CVSS (Common Vulnerability Scoring System).

Ningún sistema de valoración de vulnerabilidades es perfecto. No obstante, su uso resulta imprescindible para identificar, evaluar y priorizar las vulnerabilidades que afecten a nuestros activos. Esto nos permitirá planificar mejor y priorizar las actuaciones basándonos un nivel de riesgo.

CVSS permite establecer, utilizando un marco abierto y libre, valoraciones sobre las vulnerabilidades que nos pueden afectar proporcionándonos una idea global de la criticidad de éstas de forma rápida, simple y comprensible.



<b>Informe de divulgación</b> <b>CVSS Un sistema para valorar vulnerabilidades</b>		Código	<i>CERT-IF-5902-140728</i>
		Edición	<i>0</i>
		Fecha	<i>28/07/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. <b>17</b> de 17	

## 11 GLOSARIO

**Amenaza:** Circunstancia que tiene el potencial de causar un daño o una pérdida a un activo.

**Riesgo:** El riesgo es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al activo.

**Vulnerabilidad:** Debilidad del sistema informático que puede ser utilizada para causar un daño.

**Confidencialidad:** Propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

**Integridad:** Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas, es decir, mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

**Disponibilidad:** Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones, es decir, el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

**Exploit:** Software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

## 12 REFERENCIAS

- [FIRST: A Complete Guide to the Common Vulnerability Scoring System Version 2.0](#)
- [Cisco: Common Vulnerability Scoring System Q & A](#)