Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1521

(03/2016)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Intercambio de información de ciberseguridad – Intercambio de estados/vulnerabilidad

Sistema común de puntuación de vulnerabilidades 3.0

Recomendación UIT-T X.1521

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	**X.1520–X.1539**
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1521

Sistema común de puntuación de vulnerabilidades 3.0

Resumen

En esta Recomendación relativa al sistema común de puntuación de vulnerabilidades (CVSS, *common vulnerabilities scoring system*) se describe un marco abierto para la comunicación de las características y repercusiones de las vulnerabilidades de las tecnologías de la información y las comunicaciones (TIC) en particular en el software comercial o de código fuente abierto utilizado en redes de telecomunicaciones, en los dispositivos de usuario final o en cualquier otro tipo de TIC capaces de ejecutar software. El objetivo de esta Recomendación es permitir a los gestores de las TIC, proveedores de boletines de vulnerabilidades, vendedores de productos de seguridad, vendedores de aplicaciones e investigadores, utilizar un lenguaje común para la asignación de una valoración numérica a las vulnerabilidades de las TIC.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1521	2011-04-20	17	11.1002/1000/11062
2.0	ITU-T X.1521	2016-03-23	17	11.1002/1000/12614

Palabras clave

CVSS, CYBEX, mesures, système d'évaluation des vulnérabilités courantes

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Introducción

El sistema común de puntuación de vulnerabilidades (CVSS) proporciona un marco abierto para la comunicación de las características y gravedad de las vulnerabilidades del software. El CVSS consta de tres grupos: Base, Temporal y Ambiental. El grupo Base representa las características intrínsecas de una vulnerabilidad, el grupo Temporal refleja las características de una vulnerabilidad que cambia con el tiempo, y el grupo Ambiental refleja las características de una vulnerabilidad que son peculiares del entorno del usuario. La métrica Base genera una puntuación del 0 al 10 que puede modificarse posteriormente con la puntuación de la métrica Temporal y Ambiental. La puntuación CVSS también se expresa mediante un vector cadena, representación textual abreviada de los valores utilizados para obtener la puntuación. La presente Recomendación constituye la especificación oficial del CVSS v3.0.

El CVSS v3.0 incorpora una serie de mejoras sustanciales con respecto al CVSS v2.0 y no es compatible con dicha versión. Al utilizar el CVSS v2.0 se pusieron de manifiesto varias limitaciones de esa especificación. Entre ellas cabe citar las siguientes: puntuación de las vulnerabilidades en un entorno virtual, representación de vulnerabilidades "indirectas" tales como las secuencias de comandos en sitios cruzados, e imposibilidad de captar las interdependencias entre aplicaciones del mismo sistema y las acciones de captura de un usuario no atacante. En el punto 2 del Apéndice I se ofrece más información sobre las mejoras de la v3.0.

En el curso de los trabajos para intentar resolver esas limitaciones, el Grupo de Trabajo CVSS se dio cuenta de que no era posible mantener la compatibilidad con el CVSS v2.0. Aunque reconocemos que esta incompatibilidad provocará algunos problemas en los sistemas existentes que utilizan y procesan CVSS v2.0, creemos que la versión 3.0 aporta suficiente valor para compensar esa desventaja. Estamos recomendando encarecidamente a los usuarios y distribuidores que actualmente producen y procesan el CVSS v2.0, que migren al CVSS v3.0.

Aunque la especificación CVSS v2.0 seguirá estando disponible con fines históricos, dejará de estar en vigor. Se insta a los implementadores de herramientas y procesos a que adopten la especificación CVSS v3.0 pero que sigan dando soporte a la v2.0 a fin de procesar las vulnerabilidades existentes ya identificadas en la especificación v2.0.

Recomendación UIT-T X.1521

Sistema común de puntuación de vulnerabilidades 3.0

1 Alcance

Esta Recomendación presenta una solución normalizada para la comunicación de las características e impactos de las vulnerabilidades de las tecnologías de la información y las comunicaciones (TIC) utilizando métricas Temporales y Ambientales que aplican información contextual para reflejar con la mayor exactitud el riesgo que dichas vulnerabilidades comportan para el entorno específico de cada usuario.

Esta Recomendación es técnicamente equivalente y compatible con el documento "*Common Vulnerability Scoring System* (CVSS) *version* 3", 10 de junio de 2015 que puede encontrarse en el sitio web http://www.first.org/cvss.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, por referencia a las mismas en este texto, constituyen disposiciones de esta Recomendación. En la fecha de publicación, las ediciones citadas estaban en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios de esta Recomendación a que consideren la posibilidad de aplicar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en el marco de esta Recomendación no confiere al mismo, como documento autónomo, el rango de Recomendación.

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

En esta Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 vulnerabilidad [b-ITU-T X.1500]: cualquier punto débil que pueda explotarse con el fin de vulnerar un sistema o la información que éste contiene.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los términos siguientes:

3.2.1 acceso: capacidad de un sujeto para visualizar, modificar o comunicarse con un objeto. El acceso permite el flujo de información entre el sujeto y el objeto.

3.2.2 disponibilidad: acceso fiable y oportuno a datos y recursos por individuos autorizados.

3.2.3 confidencialidad: principio de seguridad destinado a asegurar que la información no se revela a sujetos no autorizados.

3.2.4 integridad: principio de seguridad que asegura que la información y los sistemas no son modificados de forma maliciosa o accidental.

3.2.5 riesgo: impacto relativo que tendría la explotación de una vulnerabilidad en el entorno de un usuario.

3.2.6 amenaza: probabilidad o frecuencia de ocurrencia de un evento perjudicial.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las abreviaturas y acrónimos siguientes:

A Impacto en la Disponibilidad (*availability impact*)

AC Complejidad del acceso (*access complexity*)

AR Requisito de Disponibilidad (*availability requirement*)

ARP Protocolo de resolución de direcciones (*address resolution protocol*)

AV Vector de acceso (*access vector*)

C Impacto en la Confidencialidad (*confidentiality impact*)

CIA Confidencialidad, Integridad y Disponibilidad (*confidentiality, integrity, and availability*)

CPU Unidad central de procesamiento (*central processing unit*)

CR Requisito de Confidencialidad (*confidentiality requirement*)

CVE Exposición común a la vulnerabilidad (*common vulnerability exposure*)

CVSS Sistema común de puntuación de vulnerabilidades (*common vulnerability scoring system*)

CWE Enumeración común de debilidades (*common weakness enumeration*)

DMA Acceso directo a la memoria (*direct memory access*)

DNS Sistema de nombres de dominio (*domain name system*)

DOM Modelo objeto de documento (*document object model*)

DoS Denegación de servicio (*denial-of-dervice*)

E Madurez del código de explotación (*exploit code maturity*)

I Impacto en la Integridad (*integrity impact*)

ICT Tecnologías de la información y la comunicación (i*nformation and communication technologies*)

ID IDentificador

IP Protocolo de Internet (*internet protocol*)

IR Requisito de Integridad (*integrity requirement*

ISC Subpuntuación del Impacto (*impact sub score*)

TI Tecnología de la información

LAN Red de área local (*local area network*)

MA Disponibilidad modificada (*modified availability*)

MAC Complejidad del ataque modificada (*modified attack complexity*)

MAV Vector de ataque modificado (*modified attack vector*)

MC Impacto en la Confidencialidad modificado (*modified confidentiality impact*)

MI Integridad modificada (*modified integrity*)

MPR Privilegios requeridos modificados (*modified privileges required*)

MS Ámbito modificado (*modified scope*)

MUI Interacción del usuario modificada (*modified user interaction*)

NIST Instituto nacional de normas (*national institute of standards*)

OS Sistema operativo (*operating system*)

OSI Interconexión de sistemas abiertos (*open systems interconnection*)

PCI DSS Norma de seguridad de datos de la industria de las tarjetas de pago (*payment card industry data security standard*)

PR Privilegios requeridos (*privileges required*)

RC Confianza de la información (*report confidence*)

RL Nivel de remedio (*remediation level*)

RPC Llamada a distancia a un procedimiento (*remote procedure call*)

S Ámbito (*scope*)

SCAP Protocolo de automatización de contenidos (*security content automation protocol*)

SQL Lenguaje de consulta estructurado (*structured query language*)

TCP Protocolo de control de la transmisión (*transmission control protocol*)

UI Interacción del usuario (*user interaction*)

USB Bus universal serie (*universal serial bus*)

VM Máquina virtual (*virtual machine*)

XSS Secuencias de comandos en sitios cruzados (*cross site scripting*)

5 Convenios

Ninguno.

6 Acerca del sistema común de puntuación de la vulnerabilidad

El sistema común de puntuación de la vulnerabilidad (CVSS) es un marco abierto para comunicar las características y la gravedad de las vulnerabilidades del software. Consta de tres grupos de métricas: Base, Temporal y Ambiental. El grupo Base representa las cualidades intrínsecas de una vulnerabilidad, el grupo Temporal refleja las características de una vulnerabilidad que cambia con el tiempo, y el grupo Ambiental representa las características de una vulnerabilidad que son peculiares del entorno del usuario. La métrica Base genera una puntuación del 0 al 10 que puede modificarse posteriormente con la puntuación de las métricas Temporal y Ambiental. La puntuación CVSS también se representa por un vector cadena, representación textual comprimida de los valores utilizados para obtener la puntación. La presente Recomendación contiene la especificación oficial del CVSS v3.0.

6.1 Introducción

Las vulnerabilidades del software, el hardware y el microcódigo suponen un riesgo crítico para cualquier organización que explote una red de computadores, y pueden resultar difíciles de clasificar y mitigar. El sistema común de puntuación de la vulnerabilidad (CVSS) proporciona un modo de capturar las características principales de una vulnerabilidad, y genera una puntuación numérica que refleja su gravedad, así como una representación textual de dicha puntuación. A continuación, la puntuación numérica puede trasladarse a una representación cualitativa (por ejemplo, baja, media y crítica) para que las organizaciones evalúen y prioricen adecuadamente sus procesos de gestión de la vulnerabilidad.

En resumen, el CVSS tiene tres importantes ventajas. En primer lugar, proporciona puntuaciones normalizadas de la vulnerabilidad. Cuando una organización utiliza un algoritmo de puntuación de las vulnerabilidades común para todas las plataformas TI, puede aprovechar una sola política de gestión de vulnerabilidades que defina el máximo tiempo admisible para validar una determinada vulnerabilidad y ponerle remedio. En segundo lugar, proporciona un marco abierto. La asignación de una puntuación arbitraria por un tercero puede dar lugar a que los usuarios se confundan. Con el CVSS, las características individuales utilizadas para calcular una puntuación son transparentes. Cuando se calcula la puntuación Ambiental, la vulnerabilidad se integra en el contexto de cada organización, contribuye a que se entiendan mejor los riesgos que comporta esta vulnerabilidad para la organización.

La presente Recomendación constituye la especificación oficial del CVSS v3.0.

6.1.1 Métrica

El CVSS se compone de tres grupos de métricas: Base, Temporal y Ambiental, cada una de las cuales consta de un conjunto de métricas, tal como se muestra en la Figura 1.

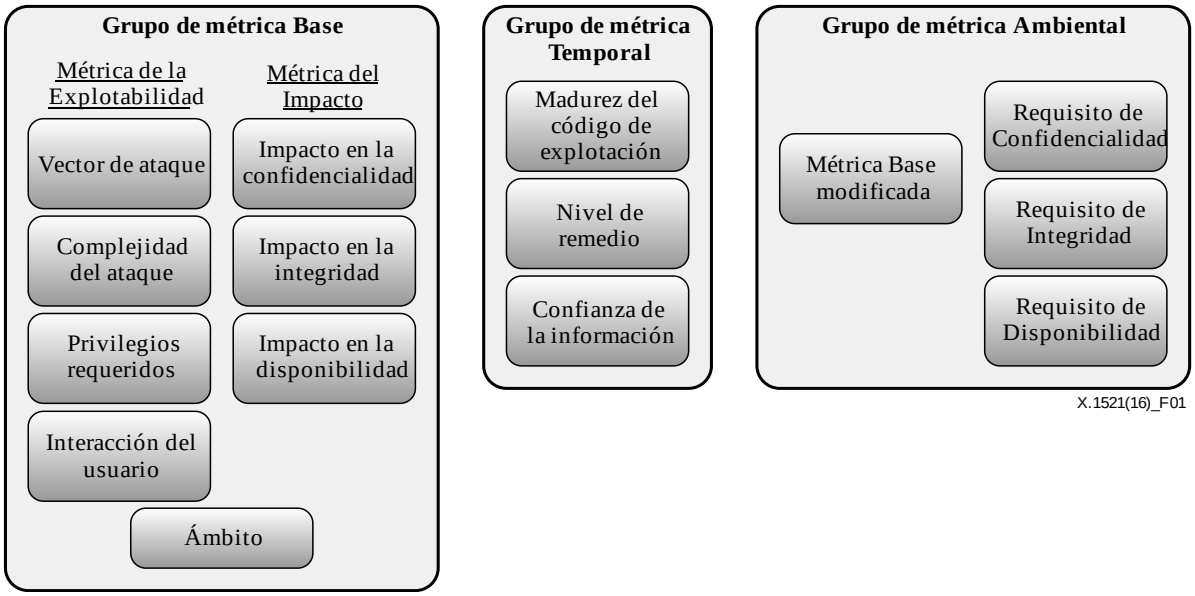


Figura 1 – Grupos de métricas del CVSS v3.0

El grupo de métrica Base representa las características intrínsecas de una vulnerabilidad que son constantes a lo largo del tiempo y en los distintos entornos del usuario. Está integrado por dos conjuntos de métricas: la métrica de la Explotabilidad y la métrica del Impacto.

La métrica de la Explotabilidad refleja la facilidad y los medios técnicos gracias a los cuales puede explotarse la vulnerabilidad. O sea, representa las características de *lo que es vulnerable*, y que definimos formalmente como *componente vulnerable*. Por otra parte, la métrica del Impacto refleja la consecuencia directa del éxito de una aplicación maliciosa, y representa las consecuencias para *lo que sufre el impacto*, que denominamos formalmente el *componente afectado*.

Aunque el componente vulnerable suele ser una aplicación, módulo o controlador de software, etc. (o incluso un dispositivo físico), el componente afectado puede ser una aplicación de software, un dispositivo físico o un recurso de red. Este potencial para medir el impacto de una vulnerabilidad ajena a un componente físico, es una de las características clave del CVSS v3.0. Esta propiedad se captura y se trata más a fondo en la métrica del Ámbito, que se presenta más adelante.

El grupo de métrica Temporal refleja las características de una vulnerabilidad que puede cambiar con el tiempo aunque no en todos los entornos de usuario. Por ejemplo, la existencia de un juego de

herramientas de explotación de vulnerabilidades que sea fácil de manejar aumentaría la puntuación del CVSS, mientras que la creación de un parche oficial la reduciría.

El grupo de métrica Ambiental representa las características de una vulnerabilidad que son relevantes y peculiares de un entorno de usuario determinado. Esta métrica permite que el analista de las puntuaciones incorpore controles de seguridad que puedan mitigar las posibles consecuencias, así como promover o degradar la importancia de un sistema vulnerable dependiendo de su riesgo empresarial.

Estas métricas se exponen más detalladamente a continuación.

6.1.2 Puntuación

Cuando las métricas Base son valores asignados por un analista, la ecuación Base calcula un rango de valores de puntuación entre 0,0 y 10,0, tal como se muestra en la Figura 2.

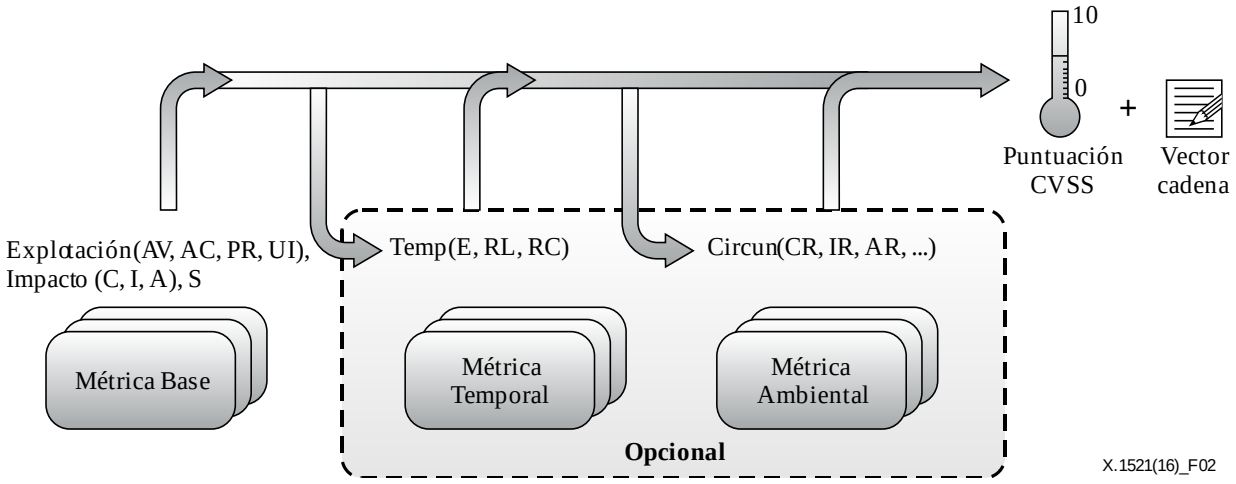


Figura 2 – Métricas y ecuaciones del CVSS

Concretamente, la ecuación Base procede de dos subecuaciones: la ecuación de subpuntuación de la Explotabilidad y la ecuación de subpuntuación del Impacto. La ecuación de la subpuntuación de la Explotabilidad procede a su vez de la métrica Base de la Explotabilidad, mientras que la ecuación de la subpuntuación del Impacto procede de la métrica Base del impacto.

La puntuación Base puede perfeccionarse con la puntación de las métricas Temporal y Ambiental para reflejar con más exactitud el riesgo que comporta una vulnerabilidad para el entorno del usuario. Sin embargo, no se necesitan para esta puntuación las métricas Temporal y Ambiental.

Normalmente, las métricas Base y Temporal las especifican los analistas de boletines de vulnerabilidad, los fabricantes de productos de seguridad y los desarrolladores de aplicaciones porque suelen poseer la información de mayor exactitud sobre las características de una vulnerabilidad. Por otra parte, la métrica Ambiental suelen especificarlas organizaciones de usuarios finales porque son los más capacitados para evaluar el impacto potencial de una vulnerabilidad en su propio entorno informático.

Las métricas CVSS de puntuación también generan un vector cadena, representación textual de los valores de las métricas utilizados para puntuar la vulnerabilidad. Este vector cadena es concretamente una cadena de caracteres formateada que contiene cada uno de los valores asignados a cada métrica y debe mostrarse siempre junto con la puntuación de la vulnerabilidad.

Las ecuaciones de cálculo de la puntuación y el vector cadena se explican más adelante.

Obsérvese que todas las métricas deben puntuarse respetando la hipótesis de que el atacante ya haya localizado e identificado la vulnerabilidad. Es decir, no es necesario que el analista tenga en cuenta

cómo se ha identificado la vulnerabilidad. Además, es probable que la puntuación de la vulnerabilidad la establezcan muchos tipos de individuos diferentes (por ejemplo, fabricantes de software, analistas de boletines de vulnerabilidad, fabricantes de productos de seguridad, etc.), sin embargo, hay que hacer hincapié en que la puntuación de la vulnerabilidad debe ser imparcial para el individuo y su organización.

6.2 Métrica Base

6.2.1 Métrica de la Explotabilidad

Como se ha indicado anteriormente, la métrica de la Explotabilidad refleja las características de *lo* que es vulnerable, que denominamos formalmente el *componente vulnerable*. Así pues, cada una de las métricas de la Explotabilidad relacionadas a continuación debe puntuar con relación al componente vulnerable y reflejar las propiedades de la vulnerabilidad a las que se debe el éxito del ataque.

6.2.1.1 Vector de ataque (AV)

Esta métrica refleja el contexto que hace posible la explotación de la vulnerabilidad. El valor de esta métrica (y por consiguiente la puntuación Base) será mayor cuanto mayor sea la distancia (lógica y física) a la que se encuentre el atacante que explota el componente vulnerable. La hipótesis es que el número de atacantes potenciales a una vulnerabilidad que pueda explotarse por Internet es mayor que el número de atacantes potenciales a una vulnerabilidad para cuya explotación se necesite el acceso físico a un dispositivo y que, por consiguiente, alcanza una puntuación más alta. La relación de valores posibles se muestra en el Cuadro 1.

Cuadro 1 –Vector de ataque

Valor de la métrica	Descripción
Red (N)	Una vulnerabilidad explotable por un acceso desde la red supone que el componente vulnerable está vinculado a una pila de red y que el trayecto del atacante atraviesa la capa 3 (capa de red) OSI (interconexión de sistemas abiertos). Esta vulnerabilidad suele denominarse "explotable a distancia" y puede concebirse como un ataque perpetrado a una distancia de uno o más saltos de red (por ejemplo, a través de los límites de la capa 3 de los encaminadores (*routers*)). Un ejemplo de ataque por red es el de un atacante que provoque una denegación de servicio (DoS) con el envío de un paquete TCP (protocolo de control de la transmisión) manipulado a propósito, por la Internet pública (por ejemplo, CVE-2004-0230).
Adyacente (A)	Una vulnerabilidad explotable por acceso a una red adyacente supone que el componente vulnerable está vinculado a la pila de red, aunque el ataque se limita a la misma red física (por ejemplo, Bluetooth, IEEE 802.11) o lógica (por ejemplo, subred local IP (protocolo de Internet)) y no puede perpetrarse a través del límite de la capa 3 OSI (por ejemplo un encaminador). Un ejemplo de ataque adyacente sería el de una inundación de ARP (protocolo de resolución de direcciones) (IPv4) o de descubrimiento de vecinos (IPv6) que provocara una denegación de servicio en el segmento de la LAN (red de área local). Véase asimismo CVE-2013-6014.
Local (L)	Una vulnerabilidad explotable a través de un acceso local supone que el componente vulnerable no está vinculado a la pila de red y el trayecto del atacante utiliza las capacidades de lectura/grabación/ejecución. Es posible que, en algunos casos, el atacante inicie una sesión local para explotar la vulnerabilidad; en otros puede esperar a que sea la interacción con el usuario (UI) la que ejecute el fichero malintencionado.

Cuadro 1 –Vector de ataque

Valor de la métrica	Descripción
Físico (P)	Para que una vulnerabilidad pueda explotarse con acceso físico, es necesario que el atacante tenga contacto físico con el componente vulnerable o lo manipule. La interacción física puede ser breve (tal como el ataque de la malvada limpiadora[1]) o persistente. Un ejemplo de este tipo de ataques es el de un ataque de arranque en frío, que permita que el atacante tenga acceso a las claves de encriptación del disco tras acceder físicamente al sistema, o ataques periféricos tales como los de acceso a una memoria USB (bus universal serie) o Firewire.

6.2.1.2 Complejidad del ataque (AC)

Esta métrica describe las condiciones que escapan al control del atacante pero que deben darse para que éste pueda explotar la vulnerabilidad. Como se describe a continuación, es posible que esas condiciones exijan la recopilación de información adicional acerca del objetivo, la presencia de ciertos valores de configuración del sistema, o excepciones computacionales. Es importante hacer hincapié en que la evaluación de esta métrica excluye por completo la necesidad de que se produzca una interacción con el usuario para poder explotar la vulnerabilidad (estas condiciones se recogen en la métrica de Interacción del usuario). El valor de esta métrica es tanto mayor cuanto menor es la Complejidad del ataque. La relación de los valores posibles se presenta en el Cuadro 2.

Cuadro 2 – Complejidad del ataque

Valor de la métrica	Descripción
Baja (L)	No existen condiciones especiales de acceso ni circunstancias atenuantes. El atacante puede esperar atacar con éxito repetidas veces al componente vulnerable.
Alta (H)	El éxito del ataque depende de circunstancias que escapan al control del atacante. O sea, el éxito del ataque no depende de la voluntad del atacante pero exige que éste invierta un cierto esfuerzo en la preparación o ejecución del ataque al componente vulnerable antes de que se pueda esperar que un ataque tenga éxito.[2] Por ejemplo, el éxito de un ataque puede depender de que el atacante supere alguna de las siguientes circunstancias: • El atacante debe efectuar un reconocimiento específico del objetivo. Por ejemplo, valor de los parámetros de la configuración, números de secuencia, secretos compartidos, etc. • El atacante debe preparar el entorno del objetivo para aumentar las probabilidades de éxito del ataque. Por ejemplo, repetición de los ataques para ganar una carrera o contrarrestar técnicas avanzadas de mitigación de los ataques. • El atacante debe insertarse en el trayecto lógico entre el objetivo y el recurso solicitado por la víctima a fin de leer y/o modificar las comunicaciones que cursan por la red (por ejemplo, el ataque del intermediario).

1 Véase la descripción del ataque de la malvada limpiadora en https://www.schneier.com/blog/archives/2009/10/evil_maid_attac.html.

2 Obsérvese que no especificamos la magnitud del esfuerzo necesario. Nos limitamos a señalar la necesidad de ejercer un cierto esfuerzo para poder explotar la vulnerabilidad.

6.2.1.3 Privilegios necesarios (PR)

Esta métrica describe el nivel de privilegios que debe poseer un atacante *antes* de poder explotar con éxito una vulnerabilidad. Esta métrica es mayor cuando no se necesitan privilegios. La relación de valores posibles se presente en el Cuadro 3.

Cuadro 3 – Privilegios necesarios

Valor de la métrica	Descripción
Ninguno (N)	El atacante carece de autorización antes del ataque y, por consiguiente, no necesita ningún acceso a la configuración ni a los ficheros para perpetrar el ataque.
Bajo (L)	El atacante está autorizado con privilegios (o sea, los necesita) que proporcionan capacidades básicas de usuario que normalmente sólo afectarán a la configuración y los ficheros que posee el usuario. Otra posibilidad es que el atacante con un bajo nivel de privilegios tenga la capacidad de afectar únicamente a recursos no sensibles.
Alto (H)	El atacante está autorizado con privilegios (o sea, los necesita) que le confieren un control significativo (por ejemplo, administrativo) sobre el componente vulnerable que podría afectar a la configuración de cualquier componente y a los ficheros.

6.2.1.4 Interacción del usuario (UI)

Esta métrica recoge la necesidad de que un usuario, distinto del atacante, participe en la amenaza del componente vulnerable para que ésta tenga éxito. Esta métrica determina si la vulnerabilidad puede explotarse únicamente a discreción del atacante o si deber participar, en mayor o menor medida, un usuario independiente (o un proceso iniciado por un usuario). El valor de esta métrica es máximo cuando no se necesita la interacción de ningún usuario. La relación de valores posibles se presenta en el Cuadro 4.

Cuadro 4 – Interacción del usuario

Valor de la métrica	Descripción
Ninguno (N)	El sistema vulnerable puede atacarse sin interacción de ningún usuario.
Requerida (R)	El éxito de la explotación de esta vulnerabilidad exige que el usuario adopte ciertas medidas antes de poder explotar esta vulnerabilidad. Por ejemplo, sólo es posible el éxito de la explotación durante la instalación de una aplicación por el administrador del sistema.

6.2.2 Ámbito (S)

Una importante propiedad que recoge CVSS v3.0 es la capacidad de que una vulnerabilidad de un componente de software repercuta en recursos ajenos a sus medios y privilegios. Esta consecuencia se representa por la métrica del Ámbito de la autorización o, simplemente, el Ámbito.

En sentido estricto, el Ámbito se refiere a la recopilación de privilegios definidos por una autoridad informática (por ejemplo, una aplicación, un sistema operativo o un entorno de cuarentena (*sandbox*)) para facilitar el acceso a recursos de computación (por ejemplo, ficheros, CPU (unidad central de procesamiento), memoria, etc.). Estos privilegios se asignan con arreglo a algún método de identificación y autorización. A veces, la autorización puede ser simple o controlada someramente por reglas o normas predefinidas. Por ejemplo, cuando se envía tráfico de Internet a un conmutador (*switch*) de la red, éste acepta el tráfico que llega a sus puertos y hay una autoridad que controla el flujo de tráfico con destino a los puertos de otros conmutadores.

Cuando la vulnerabilidad de un componente de software gobernado por un ámbito de autorización puede afectar a los recursos gobernados por otro ámbito de autorización, es que se ha producido un cambio de ámbito.

Resulta bastante intuitivo considerar el cambio de ámbito como la salida de una cuarentena; un buen ejemplo sería el de la vulnerabilidad de una máquina virtual que permitiera que el atacante borrase ficheros del sistema operativo (OS) del servidor (tal vez, incluso su propia máquina virtual (VM)). En este ejemplo, existen dos autoridades independientes: una que define y aplica los privilegios para la máquina virtual y sus usuarios, y otra que define y aplica los privilegios para el servidor en el que está configurada la máquina virtual.

No se produciría el cambio de ámbito, por ejemplo, con una vulnerabilidad de Microsoft Word que permitiera que el atacante amenazara a todos los ficheros del sistema operativo (OS), porque es la misma autoridad la que aplica los privilegios de la instancia de Word correspondiente al usuario y los ficheros del sistema del servidor.

La puntuación Base es mayor cuando se produce un cambio de ámbito. La relación de valores posibles se presenta en el Cuadro 5.

Cuadro 5 – Ámbito

Valor de la métrica	Descripción
Sin cambio (U)	La explotación de una vulnerabilidad sólo puede afectar a los recursos gestionados por la misma autoridad. En este caso, el componente vulnerable y el componente afectado son el mismo.
Cambiado (C)	La vulnerabilidad explotada puede afectar a recursos ajenos a los privilegios de autorización previstos por el componente vulnerable. En este caso, el componente vulnerable es distinto del afectado.

6.2.3 Métrica del Impacto

La métrica del Impacto se refiere a las propiedades del componente afectado. Independientemente de que una vulnerabilidad explotada con éxito afecte a uno o varios componentes, la métrica del Impacto se puntúa dependiendo del componente que sufra el peor resultado asociado más directa y previsiblemente a un ataque con éxito. O sea, los analistas deben restringir los impactos a un resultado final razonable que crean, con cierto margen de confianza, que un atacante puede alcanzar.

De no haberse producido un cambio de ámbito, la métrica del Impacto deberá reflejar cómo afecta éste a la Confidencialidad, Integridad y Disponibilidad (CIA) del componente vulnerable. Sin embargo, cuando se haya producido un cambio, la métrica del Impacto reflejará en impacto en la CIA del componente vulnerable o en la del afectado, dependiendo de cuál obtenga el resultado más desfavorable.

6.2.3.1 Impacto en la Confidencialidad (C)

Esta métrica mide el impacto en la Confidencialidad de los recursos de información gestionados por un componente de software debido al éxito de la explotación de una vulnerabilidad. La Confidencialidad se refiere a la restricción del acceso a la información y su divulgación para limitarlos exclusivamente a los usuarios autorizados, así como para evitar la divulgación a quienes no están autorizados así como su acceso. La relación de valores posibles se presenta en el Cuadro 6. El valor de esta métrica aumentará con la magnitud de las pérdidas que sufra el componente afectado.

Cuadro 6 – Impacto en la Confidencialidad

Valor de la métrica	Descripción
Alto (H)	La pérdida de Confidencialidad es total, lo que provoca que todos los recursos del componente afectado se divulguen al atacante. Otra posibilidad es que se consiga el acceso a una cierta información restringida y que la información revelada tenga una repercusión directa y grave. Por ejemplo, que un atacante robe la contraseña del administrador o las claves de encriptación privadas de un servidor web.
Bajo (L)	Hay cierta pérdida de Confidencialidad. Se consigue el acceso a información restringida pero el atacante no controla qué información consigue, o bien la magnitud o el tipo de pérdidas son limitados. La información revelada no provoca una pérdida grave ni directa al componente afectado.
Nulo (N)	No hay pérdida de Confidencialidad en el componente afectado.

6.2.3.2 Impacto en la Integridad (I)

Esta métrica mide el impacto en la Integridad de una vulnerabilidad explotada con éxito. La Integridad se refiere a la confiabilidad y veracidad de la información. La relación de valores posibles se presenta en el Cuadro 7. El valor de esta métrica aumenta con las consecuencias para el componente afectado.

Cuadro 7 – Impacto en la Integridad

Valor de la métrica	Descripción
Alto (H)	La pérdida de Integridad es total o se pierde la protección por completo. Por ejemplo, el atacante puede modificar todos y cada uno de los ficheros protegidos por el componente afectado. Otra posibilidad es que sólo se puedan modificar algunos ficheros pero que la modificación malintencionada tenga consecuencias directas y graves para el componente afectado.
Bajo (L)	Aunque la modificación de los datos sea posible, el atacante no controla sus efectos. Otra posibilidad es que la modificación sea restringida. La modificación de los datos no tiene una repercusión directa ni grave sobre el componente afectado.
Nulo (N)	No hay pérdida de Integridad en el componente afectado.

6.2.3.3 Impacto en la Disponibilidad (A)

Esta métrica mide el impacto en la Disponibilidad del componente afectado como consecuencia del éxito de la explotación de una vulnerabilidad. Aunque la métrica del Impacto en la Confidencialidad y en la Integridad se aplique a la pérdida de Confidencialidad e Integridad de los datos utilizados por el componente afectado (por ejemplo, información, ficheros), esta métrica se refiere a la pérdida de Disponibilidad del propio componente afectado, tal como un servicio en red (por ejemplo, web, base de datos, correo-e). Puesto que la Disponibilidad se refiere a la accesibilidad de los recursos de información, los ataques que consumen ancho de banda de la red, ciclos de procesador o espacio en disco repercuten en la Disponibilidad del componente afectado. La relación de valores posibles se presenta en el Cuadro 8. Este valor de la métrica aumenta con las consecuencias para el componente afectado.

Cuadro 8 – Impacto en la Disponibilidad

Valor de la métrica	Descripción
Alto (H)	La pérdida de Disponibilidad es total lo que permite que el atacante tenga la posibilidad de provocar una denegación total de acceso a los recursos del componente afectado; esta pérdida puede ser sostenida (mientras el atacante continúe perpetrando el ataque) o persistente (cuando la condición se mantenga una vez terminado el ataque). Otra posibilidad es que el atacante pueda provocar la denegación de una cierta disponibilidad y que ésta tenga consecuencias directas graves para el componente afectado (por ejemplo, cuando el atacante no pueda perturbar las conexiones existentes aunque sí impedir que se realicen nuevas conexiones; o cuando el atacante puede explotar repetidas veces una vulnerabilidad que, en cada ataque con éxito, provoque sólo la fuga de una pequeña cantidad de memoria, pero que tras los repetidos ataques provoque la total indisponibilidad del servicio).
Bajo (L)	Se reduce la calidad de funcionamiento o se producen interrupciones en la disponibilidad de un recurso. Aunque sea posible repetir la explotación de la vulnerabilidad, el atacante no podrá denegar por completo el servicio a los usuarios legítimos. Los recursos del componente afectado están parcialmente disponibles todo el tiempo o lo están totalmente durante parte del tiempo, pero en conjunto no hay consecuencias directas graves para el componente afectado.
Nulo (N)	No hay impacto en la disponibilidad del componente afectado.

6.3 Métrica Temporal

La métrica Temporal mide el estado actual de las técnicas de explotación o la disponibilidad del código de explotación, la existencia de posibles parches o procedimientos alternativos, y la confianza que merece la descripción de una vulnerabilidad.

6.3.1 Madurez del código de explotación (E)

Esta métrica mide la probabilidad de que se perpetre un ataque contra la vulnerabilidad y suele basarse en el estado actual de las técnicas de explotación, la disponibilidad del código de explotación o la explotación activa "fuera del laboratorio".

La disponibilidad pública de un código de explotación fácil de utilizar aumenta el número de atacantes potenciales al incluir a los inexpertos, acentuando de este modo la gravedad de la vulnerabilidad. Es posible que, en un principio, la explotación en el mundo real sea sólo teórica. Esto puede venir seguido de la publicación del código de prueba del concepto, el código de explotación funcional o de suficientes detalles técnicos como para explotar la vulnerabilidad. Además, es posible que el código de explotación disponible evolucione desde demostración de la prueba de concepto a un código de explotación que permita explotar con éxito la vulnerabilidad consecuentemente. En los casos graves, puede hacerse llegar como la parte útil de un gusano o virus de red u otras herramientas de ataque automatizadas.

La relación de valores posibles se presenta en el Cuadro 9. Cuanto mayor sea la facilidad de explotación de una vulnerabilidad, mayor será la puntuación de la vulnerabilidad.

Cuadro 9 – Madurez del código de explotación

Valor de la métrica	Descripción
Sin definir (X)	La asignación de este valor a la métrica no influye en la puntuación. Se trata de una indicación a una ecuación de puntuación para que pase por alto esta métrica.
Alta (H)	Existe un código funcional autónomo o no se necesita la explotación (se activa manualmente) y los detalles se pueden conseguir fácilmente. El código de explotación funciona en cualquier situación, o se distribuye mediante un agente autónomo (tal como un gusano o virus). Es probable que los sistemas conectados por la red encuentren intentos de exploración o explotación. El desarrollo de los programas de explotación de las vulnerabilidades ha alcanzado el nivel de herramientas automáticas fiables, fáciles de conseguir y utilizar.
Operativa (F)	Se puede conseguir el código de explotación operativo. Este código funciona en la mayor parte de las situaciones en las que existe una vulnerabilidad.
Prueba de concepto (P)	Se puede conseguir el código de la prueba de concepto, o bien una demostración de ataque no es práctica para la mayor parte de los sistemas. El código o la técnica no son operativos en todas las situaciones y es posible que el atacante experto tenga que introducir modificaciones sustanciales.
Sin demostrar (U)	No es posible conseguir el código de explotación de la vulnerabilidad, o bien la explotación es teórica.

6.3.2 Nivel de remedio (RL)

El Nivel de remedio de una vulnerabilidad es un factor importante para la priorización. Normalmente, en el momento de la publicación de una vulnerabilidad se carece de parche para la misma. Las soluciones temporales alternativas o parches en caliente pueden ser remedios provisionales hasta que se disponga de un parche oficial o de una actualización. Cada una de dichas etapas reduce la puntuación temporal, que refleja así una urgencia decreciente cuando el remedio pasa a ser definitivo. La relación de valores posibles se presenta en el Cuadro 10. Cuanto menos oficial y permanente sea una solución, mayor será la puntuación de la vulnerabilidad.

Cuadro 10 – Nivel de remedio

Valor de la métrica	Descripción
Sin definir (X)	La asignación de este valor a la métrica no influye en la puntuación. Se trata de una indicación a una ecuación de puntuación para que pase por alto esta métrica.
Indisponible (U)	O bien no existe una solución disponible o bien ésta es imposible de aplicar.
Solución alternativa (W)	Hay disponible una solución que ni es oficial ni la ha desarrollado el fabricante. En algunos casos, los mismos usuarios de la tecnología afectada crean un parche o facilitan la búsqueda de una solución alternativa para mitigar la vulnerabilidad.
Arreglo temporal (T)	Existe un arreglo oficial de carácter temporal. Esto incluye los casos en que el fabricante distribuye un parche en caliente, una herramienta o una solución alternativa de carácter transitorio.
Arreglo oficial (O)	Hay disponible una solución completa del fabricante. O bien el fabricante ha distribuido un parche oficial o hay una actualización disponible.

6.3.3 Confianza de la información (RC)

Esta métrica mide el grado de confianza en la existencia de la vulnerabilidad y la credibilidad de la información técnica conocida. Algunas veces sólo se publica la existencia de una vulnerabilidad sin detalles específicos. Por ejemplo, un impacto puede considerarse indeseable pero es posible que no llegue a conocerse qué lo ha provocado. La vulnerabilidad puede confirmarse después por una investigación que indique dónde puede estar la vulnerabilidad aunque puede ser que la investigación no sea cierta. Por último, la vulnerabilidad puede confirmarla el autor o el fabricante de la tecnología afectada. La urgencia de una vulnerabilidad es mayor cuando se conoce con certidumbre su existencia. Esta métrica también indica el nivel de conocimientos técnicos al alcance de los posibles atacantes. La relación de valores posibles se presenta en el Cuadro 11. Cuanto más se valide la vulnerabilidad por el fabricante o por otras fuentes fidedignas, mayor será la puntuación.

Cuadro 11 – Confianza de la información

Valor de la métrica	Descripción
Sin definir (X)	La asignación de este valor a la métrica no influye en la puntuación. Se trata de una indicación a una ecuación de puntuación para que pase por alto esta métrica.
Confirmada (C)	Existe un informe detallado o es posible conseguir una reproducción operativa (las explotaciones operativas pueden proporcionarla). Se puede conseguir el código fuente para verificar independientemente las conclusiones de la investigación, o bien el autor o fabricante del código afectado ha confirmado la presencia de la vulnerabilidad.
Razonable (R)	Se han publicado detalles significativos, pero, o bien los investigadores no tienen plena confianza en la causa última o no tienen acceso al código fuente para confirmar sin lugar a dudas todas las interacciones que pueden dar lugar a ese resultado. Existe sin embargo una confianza razonable en que el fallo puede reproducirse y que se pueda verificar por lo menos un impacto (las explotaciones del tipo prueba de concepto pueden proporcionarlo). Un ejemplo sería el de una redacción detallada de la investigación de una vulnerabilidad con una explicación (posiblemente confusa o de las que "se deja como ejercicio para el lector") que ofrezca garantías de que pueden reproducirse los resultados.
Desconocida (U)	Hay informes de impactos que indican la presencia de una vulnerabilidad. Estos informes indican que la causa de la vulnerabilidad es desconocida; también puede ser que los informes sobre la causa o los efectos de la vulnerabilidad sean dispares. Los informadores no están seguros de la auténtica naturaleza de la vulnerabilidad y hay poca confianza en la validez de los informes, o bien puede aplicarse una puntuación Base estática, dadas las diferencias expuestas. Un ejemplo sería el del informe de un fallo que señalara una avería intermitente pero no reproducible, habiendo evidencias de corrupción de la memoria que parecen indicar que puede producirse una denegación de servicio e incluso repercusiones más graves.

6.4 Métrica Ambiental

Esta métrica permite que el analista adapte la puntuación CVSS dependiendo de la importancia del activo TI afectado para la organización del usuario, medida en términos de los controles de seguridad complementarios/alternativos implementados, la Confidencialidad, la Integridad y la Disponibilidad. Está métrica es la modificación del equivalente de la métrica Base. La asignación de los valores de la misma se realiza con arreglo al encuadre de la componente en la infraestructura de la organización.

6.4.1 Requisitos de seguridad (CR, IR, AR)

Estas métricas permiten al analista diseñar a la medida la puntuación CVSS en función de la importancia que tenga el activo TI (tecnología de la información) afectado para la organización del

usuario, medida en términos de Confidencialidad, Integridad y Disponibilidad. Es decir, si un activo TI soporta una función de negocio para la que la disponibilidad sea de la máxima importancia, el analista podrá asignar un valor superior a la Disponibilidad que a la Confidencialidad o a la Integridad. Cada requisito de seguridad tiene tres valores posibles: Bajo, Medio y Alto.

El efecto total de la puntuación Ambiental está determinado por las correspondientes métricas Base del impacto modificadas. Es decir, esas métricas modifican la puntuación Ambiental al ponderar de nuevo las métricas modificadas del impacto en la Confidencialidad, la Integridad y la Disponibilidad. Por ejemplo, la métrica modificada del impacto en la Confidencialidad (MC) tiene un peso mayor si el requisito de Confidencialidad (CR) es Alto. Análogamente, la métrica modificada del impacto sobre la Confidencialidad reduce su peso si el requisito de Confidencialidad es bajo. La ponderación de la métrica modificada del impacto en la Confidencialidad es neutral si el requisito de Confidencialidad es Medio. La misma lógica se aplica a los requisitos de Integridad y Disponibilidad.

Nótese que el requisito de Confidencialidad no afectará a la puntuación Ambiental si al impacto (Base modificado) sobre la Confidencialidad se le da el valor Nulo. Asimismo, un aumento del requisito de Confidencialidad de Medio a Alto no cambiará la puntuación Ambiental si la métrica del Impacto (Base modificada) se establece en Alta. Ello se debe a que la subpuntuación del Impacto (parte de la puntuación Base modificada que calcula impacto) ya tiene el valor máximo de 10.

En el Cuadro 12 se enumeran los posibles valores de los requisitos de seguridad. Por brevedad, se utiliza el mismo cuadro para las tres métricas. Cuanto mayor sea el requisito de Seguridad, mayor será la puntuación (recuérdese que el valor por defecto es Medio).

Cuadro 12 – Requisitos de seguridad

Valor de la métrica	Descripción
Sin definir (X)	La asignación de este valor a la métrica no influye en la puntuación. Se trata de una indicación a una ecuación de puntuación para que pase por alto esta métrica.
Altos (H)	Es probable que la pérdida de [Confidencialidad | Integridad | Disponibilidad] tenga un efecto catastrófico en la organización o en los individuos ligados a ésta (tales como empleados o clientes).
Medios (M)	Es probable que la pérdida de [Confidencialidad | Integridad | Disponibilidad] sólo tenga un efecto adverso grave en la organización o en individuos ligados a ésta (tales como empleados o clientes).
Bajos (L)	Es probable que la pérdida de [Confidencialidad | Integridad | Disponibilidad] sólo tenga un efecto adverso limitado en la organización o en individuos ligados a ésta (tales como empleados o clientes).

6.4.2 Métrica Base modificada

Esta métrica permite al analista ajustar la métrica Base en función de las modificaciones que existan en el entorno de éste. O sea, si el entorno ha provocado cambios generales en el software afectado y las diferencias pueden afectar a su Explotabilidad, Ámbito o Impacto, el entorno podrá reflejarlo mediante una puntuación Ambiental adecuadamente modificada.

El efecto total de la puntuación Ambiental está determinado por la correspondiente métrica Base. Es decir, esta métrica modifica la puntuación Ambiental por reasignación de los valores de la métrica (Base) antes de aplicar los Requisitos de Seguridad (Ambiental). Por ejemplo, la configuración por defecto para un componente vulnerable podría ser ejecutar un servicio de escucha con privilegios de administrador, para los que un compromiso podría otorgar a un atacante impactos en la Confidencialidad, la Integridad y la Disponibilidad de valor Alto. 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 tener el valor Bajo.

Por concisión, sólo se mencionan los nombres de las métricas Base modificadas. Cada métrica Ambiental modificada tiene los mismos valores que su correspondiente métrica Base más el valor "Sin definir".

El propósito de esta métrica es definir las mitigaciones implementadas en un determinado entorno. Es aceptable utilizar la métrica modificada para describir situaciones que aumenten la puntuación Base. Por ejemplo, es posible que la configuración por defecto de un componente consista en exigir más privilegios (PR: Alto) con el fin de acceder a una función particular, pero también es posible que no se requieran privilegios en el entorno del analista (PR: Nulo). El analista puede establecer un MPR: Nulo para reflejar la mayor gravedad de esta condición de su entorno.

La relación de valores posibles se presenta en el Cuadro 13.

Cuadro 13 – Métrica Base modificada

Métrica Base modificada	Valores correspondientes
Vector de ataque modificado (MAV)	Los mismos valores que la métrica Base correspondiente (véase la métrica Base *supra*), así como Sin definir (valor por defecto)
Complejidad del ataque modificada (MAC)	
Privilegios requeridos modificados (MPR)	
Interacción del usuario modificada (MUI)	
Ámbito modificado (MS)	
Confidencialidad modificada (MC)	
Integridad modificada (MI)	
Disponibilidad modificada (MA)	

6.5 Escala cualitativa de calificación de la gravedad

Para algunos fines es útil disponer de una representación textual de las puntuaciones numéricas Base, Temporal y Ambiental. Puede establecerse una correspondencia entre las puntuaciones y las calificaciones cualitativas definidas en el Cuadro 14.[3]

Cuadro 14 – Escala cualitativa de calificación de la gravedad

Calificación	Puntuación CVSS
Nula	0,0
Baja	0,1 – 3,9
Media	4,0 – 6,9
Alta	7,0 – 8,9
Críticas	9,0 – 10,0

[3] Obsérvese que esta correspondencia entre puntuaciones cuantitativas y cualitativas se aplica con independencia de que se trate de la puntuación de la métrica Base, la Temporal o Ambiental.

Por ejemplo, una puntuación Base del CVSS de 4.0 lleva asociada una calificación de gravedad Media. La utilización de calificaciones cualitativas de la gravedad es opcional y no es necesario incluirlas al publicar las puntuaciones CVSS. Su propósito es ayudar a las organizaciones a evaluar y priorizar adecuadamente sus procesos de gestión de vulnerabilidades.

6.6 El vector cadena

El vector cadena CVSS v3.0 es una representación textual de un conjunto de métricas CVSS. Se utiliza comúnmente para grabar o transferir la información de la métrica CVSS de forma concisa.

El vector cadena v3.0 comienza con la etiqueta "CVSS:" y una representación numérica de la versión actual, "3.0". Viene a continuación la información de la métrica en forma de un conjunto de métricas, viniendo precedida cada una de ellas por una barra oblicua, "/", como delimitador. Cada métrica lleva la abreviatura de su nombre, dos puntos, ":" y el valor correspondiente de forma abreviada. Las formas abreviadas se han definido anteriormente en la presente especificación (entre paréntesis tras el nombre de cada métrica y de su valor), y se resumen en el cuadro siguiente.

Las métricas pueden especificarse en cualquier orden dentro del vector cadena, aunque en el Cuadro 15 se muestre el orden preferido. Todas las métricas Base deben incluirse en un vector cadena. Las métricas Temporal y Ambiental son optativas, y se considera que todas las métricas omitidas tienen el valor Sin definir (X). Si se desea, las métricas que tengan el valor Sin definir pueden incluirse explícitamente en un vector cadena. Los programas que lean vectores cadena v3.0 deberán aceptar las métricas en cualquier orden y tratar las Temporales y Ambientales que no se hayan definido como Sin definir. Un vector cadena no debe incluir una misma métrica dos o más veces.

Cuadro 15 – Vectores Base, Temporal y Ambiental

Grupo de métrica	Nombre de la métrica y abreviatura	Valores posibles	¿Obligatoria?
Base	Vector de ataque, AV	[N,A,L,P]	Sí
	Complejidad del ataque, AC	[L,H]	Sí
	Privilegios requeridos, PR	[N,L,H]	Sí
	Interacción del usuario, UI	[N,R]	Sí
	Ámbito, S	[U,C]	Sí
	Confidencialidad, C	[H,L,N]	Sí
	Integridad, I	[H,L,N]	Sí
	Disponibilidad, A	[H,L,N]	Sí
Temporal	Madurez del código de explotación, E	[X,H,F,P,U]	No
	Nivel de remedio, RL	[X,U,W,T,O]	No
	Confianza de la información, RC	[X,C,R,U]	No
Ambiental	Requisito de Confidencialidad, CR	[X,H,M,L]	No
	Requisito de Integridad, IR	[X,H,M,L]	No
	Requisito de Disponibilidad, AR	[X,H,M,L]	No
	Vector de ataque modificado, MAV	[X,N,A,L,P]	No
	Complejidad del ataque modificada, MAC	[X,L,H]	No

Cuadro 15 – Vectores Base, Temporal y Ambiental

Grupo de métrica	Nombre de la métrica y abreviatura	Valores posibles	¿Obligatoria?
Ambiental	Privilegios requeridos modificados, MPR	[X,N,L,H]	No
	Interacción del usuario modificada, MUI	[X,N,R]	No
	Ámbito modificado, MS	[X,U,C]	No
	Confidencialidad modificada, MC	[X,N,L,H]	No
	Integridad modificada, MI	[X,N,L,H]	No
	Disponibilidad modificada, MA	[X,N,L,H]	No

Por ejemplo, una vulnerabilidad con los valores de la métrica Base "Vector de ataque: Red, Complejidad del ataque: Baja, Privilegios requeridos: Alto, Interacción del usuario: nula, Ámbito: Sin cambios, Confidencialidad: Baja, Integridad: Baja, Disponibilidad: Nula" y sin métrica Temporal ni Ambiental especificadas, generaría el siguiente vector:

CVSS:3.0/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 remedio: Sin definir", y con la métrica en un orden distinto del preferido generaría el siguiente vector:

CVSS:3.0/S:U/AV:N/AC:L/PR:H/UI:N/C:L/I:L/A:N/E:F/RL:X

6.7 Definición del esquema XML CVSS v3.0

La definición del esquema XML (XSD) CVSS define la estructura del fichero XML que contiene el valor de las métricas CVSS y sirve para almacenar o transferir dichos datos en formato XML. El XSD puede obtenerse de https://www.first.org/cvss/cvss-v3.0.xsd

6.8 Ecuaciones del CVSS v3.0

A continuación se definen las ecuaciones del CVSS v3.0.

6.8.1 Base

La puntuación Base es función de las ecuaciones de las subecuaciones de puntuación del Impacto y la Explotabilidad. La puntuación de base se define del siguiente modo,

If (Impacto sub puntuación <=0) else, 0

Ámbito Sin cambios[4] $Roundup(Minimum[(Impacto + Explotabilidad), 10])$

Ámbito cambiado $Roundup(Minimum[1{,}08 \times (Impacto + Explotabilidad), 10])$

[4] Donde "Roundup" se define como el número más pequeño, con un decimal, que es igual o mayor que la variable independiente. Por ejemplo, Roundup(4,02) es 4,1; y Roundup(4,00) es 4,0.

Y la subpuntuación del Impacto (ISC) se define así,

Ámbito sin cambios $6{,}42 \times ISC_{Base}$

Ámbito cambiado $7{,}52 \times [ISC_{Base} - 0{,}029] - 3{,}25 \times [ISC_{Base} - 0{,}02]^{15}$

siendo

$$ISC_{Base} = 1 - \left[\left(1 - Impacto_{Conf}\right) \times \left(1 - Impacto_{Integ}\right) \times \left(1 - Impacto_{Dispon}\right)\right]$$

Y la subpuntuación de explotabilidad es,

$$8{,}22 \times Vector\_ataque \times Complejidad\_ataque \times Privilegios\_requeridos \times Interacción\_usuario$$

6.8.2 Temporal

La puntuación temporal se define del siguiente modo,

$$Roundup(PuntuaciónBase \times MadurezCódigoExplotación \times NivelRemedio \times ConfianzaInformación)$$

6.8.3 Ambiental

La puntuación Ambiental se define del siguiente modo,

If (Impacto modificado Sub Puntuación <= 0*)*	0 *else,*
If Ámbito modificado es Sin cambios	*Roundup(Roundup (Minimum [* × (Impacto.mod + Explotabilidad.mod) ,10]) × Madurez del código de explotación × Nivel de remedio × Confianza de la información)
If Alcance modificado es Cambiado	*Roundup(Roundup (Minimum [1,08* × (Impacto.mod + Explotabilidad.mod) ,10]) × Madurez del código de explotación × Nivel de remedio × Confianza de la información)

Y la subpuntuación del Impacto modificado se define del siguiente modo,

If Alcance modificado es Sin cambios	$6{,}42 \times \left[ISC_{Modificado}\right]$
If Alcance modificado es Cambiado	$7{,}52 \times \left[ISC_{Modificado} - 0{,}029\right]$-3,25× $\left[ISC_{Modificado} - 0{,}02\right]^{15}$

siendo

$$ISC_{Modificado} = Minimum\left[\left[1 - \left(1 - I_{Conf}.mod \times CR\right) \times \left(1 - I_{Integ}.mod \times IR\right) \times \left(1 - I_{Dispon}.mod \times AR\right)\right], 0{,}915\right]$$

La subpuntuación de la Explotabilidad modificada es,

$$8{,}22 \times Vector\_ataque.mod \times Complejidad\_ataque.mod \times Privilegios\_requeridos.mod \times Interacción\_usuario.mod$$

6.8.4 Nivel de las métricas

El valor de las métricas se define en el Cuadro 16.

Cuadro 16 – Valor de la métricas

Métrica	Valor de la métrica	Valor numérico
Vector del ataque/ Vector del ataque modificado	Red	0,85
	Red adyacente	0,62
	Local	0,55
	Físico	0,2
Complejidad del ataque/ Complejidad del ataque modificada	Baja	0,77
	Alta	0,44
Privilegios requeridos/ Privilegios requeridos modificados	Nulos	0,85
	Bajos	0,62 (0,68 si Ámbito/Ámbito modificado es Cambiado)
	Altos	0,27 (0,50 si Ámbito/Ámbito modificado es Cambiado)
Interacción del usuario/ Interacción del usuario modificada	Nula	0,85
	Requerida	0,62
Impacto C,I,A/ Impacto C,I,A modificado	Alto	0,56
	Bajo	0,22
	Nulo	0
Madurez del código de explotación	Sin definir	1
	Alta	1
	Operativa	0,97
	Prueba de concepto	0,94
	Sin demostrar	0,91
Nivel de remedio	Sin definir	1
	Indisponible	1
	Solución alternativa	0,97
	Arreglo temporal	0,96
	Arreglo oficial	0,95
Confianza de la información	Sin definir	1
	Confirmada	1
	Razonable	0,96
	Desconocida	0,92
Requisitos de seguridad – Requisitos C,I,A (CR)	Sin definir	1
	Alto	1,5
	Medio	1
	Bajo	0,5

6.8.5 Breve comentario sobre las ecuaciones y la puntuación del CVSS v3.0

La fórmula CVSS v3.0 constituye una aproximación matemática a todas las combinaciones de métricas posibles clasificadas por orden de gravedad (que integran una tabla de consulta de la vulnerabilidad). Para generar la fórmula CVSS v3.0, el Grupo de Interés Especial (SIG) genera la tabla de consulta asignando el valor v3.0 de las métricas a vulnerabilidades reales, y un grupo de gravedad (bajo, medio, alto, crítico). Una vez definidos los intervalos numéricos aceptables para cada nivel de gravedad, el SIG colaboró con Deloitte & Touche LLP para ajustar los parámetros de la fórmula a fin de alinear las combinaciones de métricas v3.0 con las clasificaciones de seguridad propuestas por el SIG.

Dado el limitado número de resultados numéricos (101 resultados que van de 0,0 a 10,0), las múltiples combinaciones de puntuación pueden producir el mismo resultado numérico. Además, puede que se omitan algunas puntuaciones numéricas debido a que los pesos y cálculos se obtienen de la clasificación de gravedad de las combinaciones de métricas. Por otra parte, en ciertos casos, las combinaciones de métricas pueden desviarse del umbral de gravedad deseado. Esto es inevitable y no es fácil efectuar una corrección sencilla porque los ajustes de un valor de la métrica o parámetro de la ecuación para arreglar una desviación, provoca otras desviaciones potencialmente más graves.

Por consenso, al igual que en el CVSS v2.0, a la desviación aceptable se le da el valor de 0,5. Es decir, todas las combinaciones de valores de las métricas utilizadas para obtener los pesos y los cálculos generarán una puntación numérica en su nivel de gravedad asignado, o a menos de 0,5 de dicho nivel asignado. Por ejemplo, una combinación cuya calificación prevista sea "Alta" podrá tener una puntuación numérica entre 0,0 y 10,0 para que mantenga la compatibilidad con las versiones anteriores.

Apéndice I

Guía del usuario del CVSS v3.0

(Este apéndice no forma parte integral de la presente Recomendación.)

I.1 Introducción

Esta guía suplementa el documento oficial de la especificación CVSS v3.0 con información adicional, destacando los cambios pertinentes con respecto a la v2.0 y ofreciendo directrices sobre puntuación y los criterios de puntuación.

El Sistema común de puntuación de la vulnerabilidad (CVSS) proporciona un medio de recopilar las principales características de una vulnerabilidad, y generar una puntuación numérica que refleje su gravedad, así como una representación textual dicha puntuación. A continuación, la puntuación numérica puede traducirse en una representación cualitativa de la misma (tal como baja, media, alta y crítica) para ayudar a las organizaciones a que evalúen y prioricen adecuadamente sus procesos de gestión de vulnerabilidades.

El CVSS presenta tres importantes ventajas:

– Proporciona puntuaciones normalizadas de vulnerabilidades: cuando una organización utiliza un algoritmo común para puntuar las vulnerabilidades de todas sus plataformas TI, puede aprovechar las ventajas de una política única de gestión de vulnerabilidades que defina el máximo tiempo admisible para validar y remediar una determinada vulnerabilidad.

– Proporciona un marco abierto: la asignación por un tercero de una puntuación de valoración a una vulnerabilidad puede confundir a los usuarios. Mediante el CVSS, las características individuales utilizadas para obtener una puntuación son transparentes.

– El CVSS ayuda a priorizar los riesgos. Cuando se calcula la puntuación Ambiental, la vulnerabilidad se vuelve contextual para cada organización y contribuye a ofrecer una mejor comprensión del riesgo que comporta una cierta vulnerabilidad para la organización.

Desde la primera versión, aparecida en 2004, el CVSS ha gozado de una amplia aceptación. En septiembre de 2007, se adoptó el CVSS v2.0 como parte de la Norma de seguridad de datos de la industria de tarjetas de pago (PCI DSS, *Payment Card Industry Data Security Standard*). Para cumplir la norma PCI DSS, los comerciantes que procesan tarjetas de crédito deben demostrar que ninguno de sus sistemas informáticos tiene una vulnerabilidad con una puntuación CVSS mayor o igual de 4,0. En 2007, el Instituto Nacional de Normas (NIST, *National Institute of Standards*) incluyó el CVSS v2.0 en su protocolo de automatización de contenidos de seguridad (SCAP, *security content automation protocol*).[5] En abril de 2011, se adoptó oficialmente el CVSS v2.0 como norma internacional de puntuación de vulnerabilidades (UIT-T X.1521)[6].

I.2 Cambios en CVSS v3.0

Dada la amplia adopción del CVSS v2.0, identificaron varias oportunidades de mejora que provocaron el desarrollo de la versión 3.0 y que se describen detalladamente a continuación.

---

5 Véase http://scap.nist.gov/.

6 Véase https://www.itu.int/rec/T-REC-X.1521-201104-I/en.

I.2.1 Ámbito, componente vulnerable y componente afectado

El CVSS v2.0 daba problemas a los fabricantes cuando tenían que puntuar vulnerabilidades que amenazaban a todo su software pero que sólo afectaban parcialmente al sistema operativo del servidor. En la versión v2.0, las vulnerabilidades se puntuaban con relación al sistema operativo del servidor, lo que dio lugar a que un fabricante de aplicaciones adoptase un convenio de métrica del impacto "Parcial+".[7] El CVSS v3.0 aborda este problema con la actualización del elemento que genera la puntación de la métrica del Impacto y con una nueva métrica denominada Ámbito (que se analiza más adelante). Por ello, un importante cambio conceptual del CVSS v3.0 es la capacidad de puntuar vulnerabilidades que existen en un componente de software (denominado formalmente el *componente vulnerable*) pero que repercute en otro componente independiente del software, el hardware o las redes (y que se denomina formalmente el *componente afectado*), como se representa en la Figura I.1.[8]

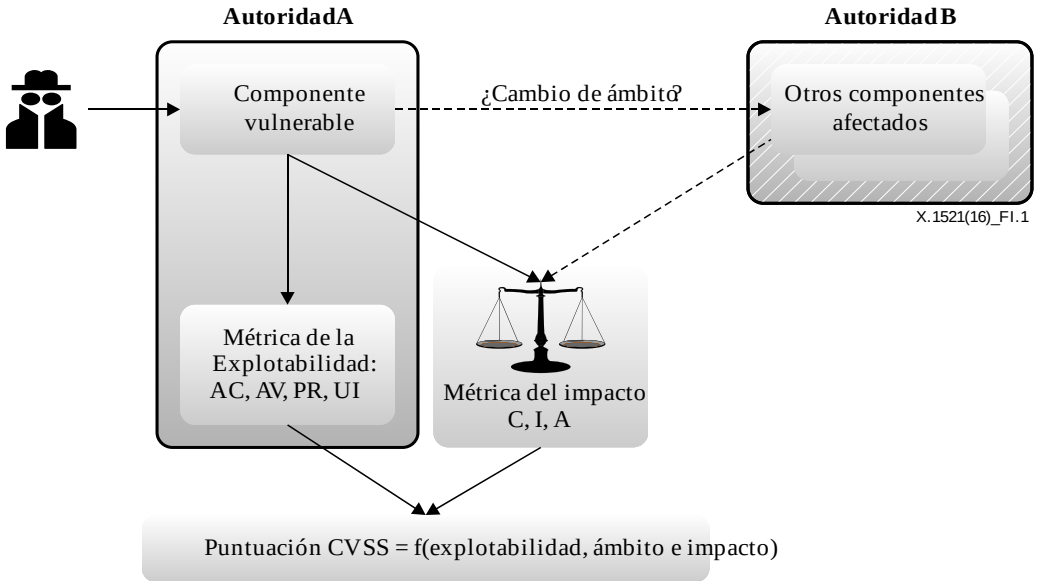


Figura I.1 – Cambio de ámbito

Por ejemplo, considérese una vulnerabilidad de una máquina virtual que ponga en peligro al sistema operativo del servidor. El componente vulnerable es la máquina virtual mientras que el componente afectado es el sistema operativo del servidor. Como esos dos componentes gestionan independientemente privilegios sobre recursos informáticos, representan autoridades (autorizaciones) independientes. En la Figura I.1, la "Autoridad A" gestiona la máquina virtual mientras que la "Autoridad B" gestiona el OS del servidor. Cuando hay dos autoridades implicadas en la explotación de una vulnerabilidad, el CVSS considera que se ha producido un *cambio de ámbito*. Esta condición se capta mediante una nueva métrica, el Ámbito.

Como se muestra en la Figura I.1, cuando se puntúan vulnerabilidades en CVSS v3.0, la métrica de Explotabilidad se puntúa en relación con el componente vulnerable. O sea, se puntúa considerando el componente que sufre el defecto de codificación. Por otra parte, la métrica Impacto se puntúa con relación al componente afectado. En algunos casos, no se produce el cambio de entorno. Sin embargo, en otros casos, puede producirse un impacto sobre el componente vulnerable así como sobre el componente afectado. En estos casos, se produce un cambio de ámbito y la métrica del Impacto en la

---

7 Véase, por ejemplo, http://www.oracle.com/technetwork/topics/security/cvssscoringsystem-091884.html.

8 Obsérvese que el componente vulnerable es un programa de software (sistema operativo del servidor, aplicación de Internet, controlador de dispositivo, etc.) y que el componente afectado puede ser otro programa de software, un dispositivo de hardware o un recurso de red).

Confidencialidad, la Integridad y la Disponibilidad debe reflejar el impacto de mayor gravedad, ya sea en el componente más vulnerable o en el componente más severo.

En el caso de una vulnerabilidad que permita el robo del fichero de contraseñas, aunque pueda haber pasos subsiguientes, el atacante procurará acceder a una cuenta sin autorización, el resultado más directo es la pérdida de Confidencialidad del fichero del sistema local. A causa de ello, no habrá cambio de ámbito. Sin embargo, en el caso de una vulnerabilidad que permita que un atacante sobreescriba la tabla ARP de un encaminador, existirán dos impactos. Primero sobre el fichero del sistema del encaminador (impacto en la Integridad del componente vulnerable) y después en los servicios de Internet atendidos por el encaminador (impacto en la Disponibilidad de los sistemas afectados). Dado que la puntuación debe reflejar el resultado más grave, la puntuación de la métrica del Impacto puede reflejar o bien la pérdida de integridad del componente vulnerable o bien la pérdida de disponibilidad de los servicios de Internet, según sea más grave una u otra.[9]

I.2.2 Vector de acceso

El Vector de acceso (de la v2.0) se denomina ahora Vector de ataque, pero sigue reflejando la "lejanía" del atacante respecto del componente vulnerable. O sea, cuanto más alejado se encuentre el atacante, mayor será la puntuación Base. Además, esta métrica distingue ahora entre los ataques locales que necesitan acceder a un sistema local (por ejemplo, el ataque a una aplicación de escritorio) y los ataques físicos que requieren el acceso físico a la plataforma para explotar la vulnerabilidad (por ejemplo, un ataque al Firewire, la USB o el jailbreaking).

I.2.3 Complejidad del ataque

La Complejidad del acceso (en la v2.0) combinaba dos temas: una condición del software, el hardware o las redes que escapa al control del atacante y que debe existir o producirse para que se pueda explotar con éxito la vulnerabilidad (por ejemplo, una condición de carrera de software, o configuración de la aplicación), y la necesidad de interacción humana (por ejemplo, cuando es necesario que el usuario ejecute un programa malintencionado). Por ello, la Complejidad del acceso se ha separado en dos métricas, la Complejidad del ataque (que aborda la primera condición) y la **Interacción del usuario** (que aborda la segunda).

I.2.4 Privilegios requeridos

La nueva métrica, **Privilegios requeridos**, sustituye a la métrica autenticación de la v2.0. En vez de medir el *número de veces* que un atacante debe autenticarse independientemente ante un sistema, los Privilegios requeridos capturan el *nivel de acceso* necesario para el éxito de un ataque. Concretamente, los valores Alto, Bajo y Nulo de esta métrica reflejan los privilegios requeridos por un atacante para explotar la vulnerabilidad.

I.2.5 Métrica del Impacto

Los valores Ninguno, Parcial y Completo de las métricas del **impacto en la Confidencialidad, la Integridad y la Disponibilidad** de la v2.0 se han sustituido por Nulo, Bajo y Alto. En vez de representar el *porcentaje* (la proporción) global de los sistemas afectados por un ataque, los nuevos valores de las métricas reflejan el *grado* global del impacto causado por un ataque. Por ejemplo, aunque la vulnerabilidad Heartbleed[10] sólo ocasionó la pérdida de una pequeña cantidad de información, el impacto fue bastante grave. En el CVSS v2.0 esto se habría puntuado como Parcial, pero en el CVSS v3.0 esto se puntúa acertadamente como Alto.

---

9 Para más información, véase el documento con ejemplos que acompaña a esta guía.

10 Véase http://heartbleed.com/.

Además, en el ejemplo anterior, la métrica del Impacto refleja ahora las consecuencias para el componente afectado, y éste puede ser, o no, el mismo que el componente que tiene la vulnerabilidad que se explota.

I.2.6 Métrica Temporal

La influencia de la métrica Temporal se ha reducido en la v3.0 con respecto a la v2.0. La explotabilidad se denomina ahora Madurez del código de explotación para reflejar más adecuadamente lo que la métrica mide.

I.2.7 Métrica Ambiental

Las métricas ambientales Distribución del Objetivo y Potencial Daño Colateral se han sustituido por factores modificados que acomodan la mitigación de controles o las debilidades de control que puedan existir en el entorno del usuario, susceptibles de reducir o aumentar el impacto de una vulnerabilidad explotada con éxito.

I.2.8 Escala cualitativa de calificación

Algunas organizaciones han creado sistemas de correspondencia de las puntuaciones Base del CVSS v2.0 con calificaciones cualitativas. Ahora, el CVSS v3.0 ofrece una correspondencia normalizada entre las puntuaciones numéricas y los calificativos de la gravedad: nula, baja, media, alta y crítica, como se explica en la especificación CVSS v3.0. La utilización de estas calificaciones cualitativas de la gravedad es opcional y no es necesario especificarlas en la publicación de las puntuaciones CVSS.

Se invita a las organizaciones que utilicen la puntuación CVSS v3.0 y deseen emplear un sistema *alternativo* de calificación de la gravedad, a que utilicen calificativos diferentes o a declarar sin ambages que sus calificaciones no se ajustan a las especificaciones CVSS v3.0, para evitar confusiones.

I.2.9 Resumen de cambios

Una consecuencia importante de estos cambios es que las puntuaciones de la v2.0 y la v3.0 no siempre son comparables. Por ejemplo, una aplicación vulnerable que pudiera quedar totalmente expuesta se habría puntuado con el valor Parcial para el impacto en la Confidencialidad, la Integridad y la Disponibilidad de las métricas de la v2.0, mientras que en la v3.0 esta misma vulnerabilidad se valoraría ahora como Alta en la métrica del Impacto en la Confidencialidad, la Integridad y la Disponibilidad.

En el Cuadro I.1 se presenta un resumen de los cambios con respecto a la v2.0.

Cuadro I.1 – Cambios de la v2.0 a la v3.0 del CVSS

Versión 2.0	Versión 3.0
Las vulnerabilidades se puntúan con respecto al impacto global sobre la plataforma del servidor.	Las vulnerabilidades se puntúan ahora con respecto al impacto sobre el componente afectado.
No se consideran las situaciones en las que una vulnerabilidad de una aplicación repercute en otra aplicación del mismo sistema.	Ahora hay una nueva métrica, el Ámbito, que acomoda las vulnerabilidades cuando *lo que sufre el impacto* (el componente afectado) es diferente de *lo que es vulnerable* (el componente vulnerable).
El Vector de acceso puede combinar ataques que requieran el acceso al sistema local y ataques al hardware.	Ahora, los valores Local y Físico están separados en la métrica del Vector de ataque.

Cuadro I.1 – Cambios de la v2.0 a la v3.0 del CVSS

Versión 2.0	Versión 3.0
A veces, la Complejidad del acceso combina la configuración del sistema y la Interacción del usuario.	Esta métrica se ha dividido en Complejidad del ataque (que representa a la complejidad del sistema) e Interacción del usuario (que representa la implicación del usuario en un ataque con éxito).
En la práctica, las puntuaciones de la métrica de Autenticación estaban sesgadas hacia dos de los tres resultados posibles y no captaban eficazmente el aspecto interesante de la vulnerabilidad.	La nueve métrica de Privilegios requeridos sustituye a la Autenticación y refleja ahora los grandes privilegios requeridos por el atacante en vez del número de veces que el atacante debe autenticarse.
Las métricas del Impacto reflejaban el porcentaje de impacto causado a una aplicación vulnerable.	El valor de la métrica del Impacto refleja ahora el grado de impacto y se ha cambiado a Nulo, Bajo y Alto.
La métrica Ambiental de la distribución del objetivo y el Potencial daño colateral no tienen ninguna utilidad.	La Distribución del objetivo y el Potencial daño colateral se han sustituido por los factores mitigantes.
CVSS v2.0 no admite la puntuación de múltiples vulnerabilidades en el mismo ataque.	Aunque no sea una métrica oficial, se proporcionan directrices sobre la puntuación de múltiples vulnerabilidades con el encadenamiento de vulnerabilidades.
No se facilitan directrices oficiales sobre sistemas de puntuación cualitativa.	Se ha establecido una correspondencia entre los intervalos numéricos y una escala de calificación cualitativa de cinco valores.

I.3 Guía para el cálculo de las puntuaciones

A continuación se presentan varias propuestas para los analistas que calculan las puntuaciones con el CVSS v3.0.

I.3.1 La puntuación CVSS en el ciclo de vida dela explotación de la vulnerabilidad

Para entender cómo puntuar el impacto de las vulnerabilidades, los analistas deben restringir los impactos a un solo impacto final razonable que consideren que el atacante pueda efectuar. La capacidad de causar este impacto debe estar soportada por la subpuntuación de la Explotabilidad como mínimo, pero también puede incluir detalles descriptivos de la vulnerabilidad. Por ejemplo, considérense las dos vulnerabilidades siguientes:

En la vulnerabilidad 1, un atacante remoto no autenticado puede enviar una petición trivial amañada a un servidor web que hace que éste revele la contraseña descifrada de la cuenta raíz (administrador). El analista sólo sabe por la métrica de la subpuntuación de la Explotabilidad y la descripción de la vulnerabilidad que el atacante tiene acceso para enviar una petición camuflada al servidor web a fin de explotar la vulnerabilidad. El impacto debería llegar hasta ahí; aunque el atacante *pueda* utilizar esas credenciales para, en su momento, ejecutar el código como administrador, no se sabe que el atacante tenga acceso a la pantalla de introducción de la contraseña ni que conozca el método de ejecutar mandatos con esas credenciales. El acceso a esa contraseña supone solamente una grave pérdida directa de Confidencialidad:

– Puntuación Base: 7,5[CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N].

En la vulnerabilidad 2, un usuario local con bajo nivel de privilegios puede enviar una petición trivial amañada al sistema operativo que provoque que éste revele la contraseña descifrada de la cuenta raíz (administrador). El analista sólo sabe por la métrica de la subpuntuación de la Explotabilidad y la descripción de la vulnerabilidad que el atacante tiene acceso al sistema operativo y puede iniciar una sesión como atacante local con bajo nivel de privilegios. El acceso a esa contraseña supone solamente una grave pérdida directa de Confidencialidad, Integridad y Disponibilidad porque el analista puede, dentro de lo razonable, emitir mandatos desde la cuenta raíz/administrador (se supone que el atacante puede terminar la sesión de su propia cuenta e iniciar otra como raíz):

– Puntuación Base: 7,8[CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H].

I.3.2 Impactos en la Confidencialidad e Integridad frente a impactos en la Disponibilidad

La métrica de la Confidencialidad y la Integridad se refiere a los impactos que afectan a los *datos* que utiliza el servicio, por ejemplo, la alteración dolosa de contenidos de la web o el robo de ficheros del sistema. La métrica del Impacto en la Disponibilidad se refiere al *funcionamiento* del servicio, es decir, la métrica de la Disponibilidad expresa la calidad de funcionamiento y la explotación del propio servicio – no la disponibilidad de los datos. Una vulnerabilidad de un servicio de Internet tal como la web, el correo-e o el sistema de nombres de dominio (DNS) que permitiese que un atacante modificara o borrase todos los ficheros web de un directorio, ocasionaría únicamente un impacto en la Integridad y no en la Disponibilidad. Esto se debe a que el servicio web seguiría funcionando adecuadamente – pero sirviendo contenidos alterados.

I.3.3 Vulnerabilidades locales explotadas por atacantes remotos

En CVSS v2.0, la recomendación de puntuación 5 rezaba así: "cuando una vulnerabilidad pueda explotarse tanto localmente como desde la red, debería elegirse el valor "red". Cuando una vulnerabilidad pueda explotarse localmente y desde redes adyacentes, pero no desde redes a distancia, debería elegirse el valor "red adyacente". Cuando una vulnerabilidad pueda explotarse desde una "red adyacente" y desde redes a distancia, debería elegirse el valor "red"". Esta directriz inducía a confusión cuando un atacante quería engañar a un usuario para que descargase un documento amañado de un servidor web remoto, explotando una vulnerabilidad en el mecanismo de análisis sintáctico de un fichero. En este caso, los analistas que utilizasen CVSS v2.0 considerarían estas vulnerabilidades como "red", generando puntuaciones con las cadenas métricas:

– AV:N/AC:M/Au:N/C:P/I:P/A:P, o AV:N/AC:M/Au:N/C:C/I:C/A:C.

Esta directriz se ha mejorado en CVSS v3.0 clarificando la definición de los valores Red y Adyacente de la métrica del Vector de ataque. Concretamente, los analistas sólo deberían puntuar Red o Adyacente cuando la vulnerabilidad estuviese vinculada a la pila de red. A las vulnerabilidades que necesiten la interacción del usuario para descargar o recibir el contenido malicioso (que también puede introducirse localmente, por ejemplo mediante memorias USB) debe otorgárseles el valor Local.

Por ejemplo, una vulnerabilidad del sistema de análisis sintáctico de documentos que no necesite la red para ser explotada debe puntuarse normalmente con el valor Local, con independencia del método utilizado para distribuir el documento malicioso (por ejemplo, podría tratarse del enlace a un sitio web, o hacerse a través de una memoria USB).

I.3.4 Vulnerabilidades de las secuencias de comandos en sitios cruzados

En CVSS v2.0, se necesitaban directrices específicas sobre generación de puntuaciones no nulas para vulnerabilidades de las secuencias de comandos en sitios cruzados (XSS), debido a que las vulnerabilidades se puntuaban con respecto al sistema operativo del servidor que contenía la vulnerabilidad. Una vulnerabilidad XSS normal generaba una puntuación que describía un impacto parcial en la Integridad debido a la modificación de la respuesta del servidor web al cliente: AV:N/AC:M/Au:N/C:N/I:P/A:N. Esto se mantenía incluso para vulnerabilidades de las secuencias de comandos en sitios cruzados (XSS) basadas en el modelo de objeto de documento (DOM) que,

aunque puedan deberse a la interacción con el servidor, se explotan totalmente en el lado del cliente (por ejemplo, cuando el JavaScript entregado por el servidor analiza la sintaxis de la cadena de caracteres de la petición enviada al servidor).

Éste es uno de los escenarios clave para los que se diseñó el Ámbito – donde el que sufre los impactos no es el componente vulnerable (por ejemplo, el servidor web, o el JavaScript entregado por el servidor web), sino el componente cuyos privilegios son gestionados por una autoridad independiente (por ejemplo, el entorno del navegador del cliente). Así pues, en CVSS v3.0, las vulnerabilidades de las secuencias de comandos en sitios cruzados no tienen que limitarse a los escasos o inexistentes impactos en el servidor, pudiendo puntuarse ahora los impactos que sufre el cliente. Una vulnerabilidad XSS reflejada que permita a un atacante entregar un enlace malintencionado a una víctima y ejecutar un JavaScript en su navegador podría puntuarse del siguiente modo:

– CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

I.3.5 El intermediario

CVSS v3.0 acomoda explícitamente la puntuación de los ataques del intermediario. Aunque en la v2.0 no se contemplaban explícitamente, en la v3.0 este tipo de ataques se contempla en la métrica de la Complejidad del ataque.

I.3.6 Vulnerabilidades del hardware

Aunque el CVSS está diseñado principalmente para puntuar vulnerabilidades del software e impactos en éste, la v3.0 está más adaptada para puntuar los impactos que afecten a los componentes del hardware y repercutan sobre las redes.

I.3.7 Encadenamiento de vulnerabilidades

El CVSS está diseñado para clasificar y calificar vulnerabilidades individuales. Sin embargo, es importante dar soporte a las necesidades de la comunidad de analistas de vulnerabilidades acomodando situaciones en las que se exploten múltiples vulnerabilidades en el curso de un solo ataque para amenazar a un servidor o una aplicación. La puntuación de múltiples vulnerabilidades de este modo se denomina Encadenamiento de vulnerabilidades. Obsérvese que ésta no es una métrica oficial, sino que se incluye como directriz para los analistas que puntúan este tipo de ataques.

Al puntuar una cadena de vulnerabilidades, es responsabilidad del analista identificar qué vulnerabilidades se combinan para formar la puntuación encadenada. El analista debe enumerar las distintas vulnerabilidades y sus puntuaciones, junto con la puntuación encadenada. Por ejemplo, esto puede comunicarse con un aviso de divulgación de vulnerabilidad publicado en una página web.

Además, el analista puede incluir otros tipos de vulnerabilidades relacionadas que podrían encadenarse con las vulnerabilidades que se puntúan. Concretamente, el analista podría enumerar tipos genéricos (o clases) de vulnerabilidades relacionadas que suelan encadenarse entre sí, o facilitar descripciones adicionales de prerrequisitos. Por ejemplo, se podría describir cómo hay ciertos tipos de vulnerabilidades de Inyección SQL (lenguaje de consulta estructurado) que son precursoras de un ataque XSS (secuencias de comandos en sitios cruzados) o cómo otorgaría privilegios locales un cierto tipo de desbordamiento de la memoria tampón. La enumeración de los tipos genéricos o clases de vulnerabilidades ofrece la información mínima necesaria para avisar a otros usuarios, posiblemente sin informar a los atacantes de las nuevas oportunidades de explotación.

Otra posibilidad es que el atacante identifique (en forma de lista de vulnerabilidades legibles por la máquina y analizables sintácticamente, como identificadores (ID) de exposición común a la vulnerabilidad (CVE) o enumeración de debilidades comunes (CWE)) una lista exhaustiva de vulnerabilidades específicas relacionadas que se sepa están encadenadas (o tengan muchas posibilidades de estarlo) a una o varias de las vulnerabilidades encadenadas que se puntúan a fin de explotar un sistema IT. En el caso de que una vulnerabilidad pueda explotarse únicamente después de haber cumplido ciertos prerrequisitos (tales como el de explotar previamente otra vulnerabilidad),

resulta aceptable combinar dos o más puntuaciones CVSS para describir la cadena de vulnerabilidades puntuando la métrica de la subpuntuación de la Explotabilidad menos restrictiva y puntuando la métrica de subpuntuación del Impacto más efectivo. En el siguiente ejemplo se utilizan las subpuntuaciones de la Explotabilidad, el Ámbito y el Impacto para describir la cadena:

La Vulnerabilidad A es: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H, y, como puede verse en el vector, necesita un usuario local con bajo nivel de privilegios para poder ser explotada. Mientras que la Vulnerabilidad B es: AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L y facilita la ejecución de código por un atacante remoto sin privilegios en un sistema con Bajo nivel de impactos si un usuario local interacciona para llevar a cabo el ataque. Así pues, dadas A y B, la cadena C puede describirse como la cadena de B -> A: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H que combina la Explotabilidad de B, permaneciendo inalterado el Ámbito en ambos casos, y el Impacto de A, porque si se puede explotar B y, por ello, ejecutar el código como usuario local, se habrá satisfecho el prerrequisito para lanzar subsiguientemente A causando un impacto como consecuencia de la vulnerabilidad A.

I.4 Glosario de términos

Autoridad: Contenedor informático que gestiona los privilegios de los recursos. Son ejemplos de autoridades una aplicación de base de datos, un sistema operativo y un entorno de cuarentena.

Puntuación encadenada: Puntuación Base generada por las puntuaciones de dos o más vulnerabilidades encadenadas.

Vulnerabilidades encadenadas: Véase encadenamiento de vulnerabilidades.

Componente: Se refiere a un componente de software o de hardware.

Componente de software: Programa o módulo de software con instrucciones de ordenador ejecutables, por ejemplo, un sistema operativo, una aplicación de Internet o un controlador de dispositivo.

Componente de hardware: Un dispositivo informático físico.

Componente afectado: El componente que sufre las consecuencias de que se explote la vulnerabilidad. Puede tratarse del propio componente vulnerable o, si se ha producido un cambio de ámbito, de otro diferente.

Privilegios: Conjunto de derechos (normalmente de lectura, grabación y ejecución) otorgados a un usuario o proceso de éste que define el acceso a los recursos informáticos.

Recursos: Software u objeto de red al que accede, modifica o que consume un dispositivo informático, por ejemplo, ficheros informáticos, memoria, ciclos de CPU o ancho de banda.

Ámbito: Conjunto de privilegios definidos y gestionados por una autoridad de autorización cuando otorga el acceso a los recursos informáticos.

Vulnerabilidad: Debilidad o defecto de un componente de software (o hardware).

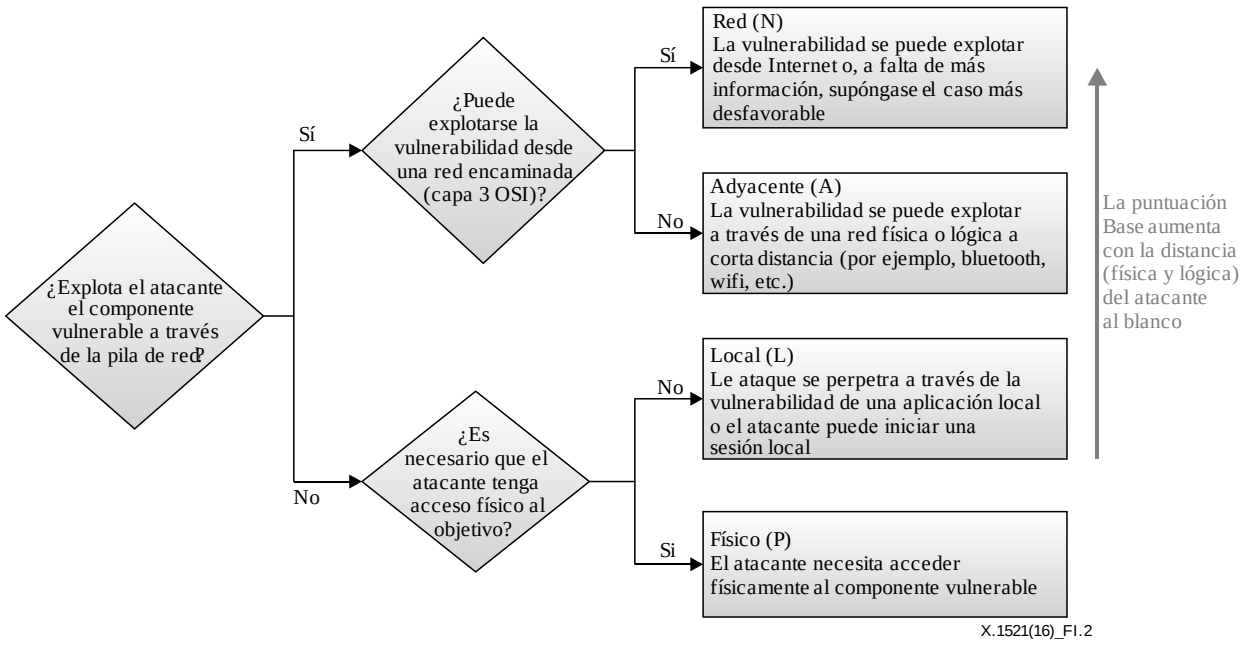
Encadenamiento de la vulnerabilidad: Explotación secuencial de múltiples vulnerabilidades para atacar un sistema IT, cuando uno o más intentos de explotación de la vulnerabilidad al final de la cadena exigen la terminación con éxito de los anteriores intentos de explotación para poder ejecutarse. Véase la definición de http://cwe.mitre.org/documents/glossary/#Chain.

Componente vulnerable: Componente de software (o hardware) que tiene la vulnerabilidad y que debería parchearse.

I.5 Criterios de puntuación

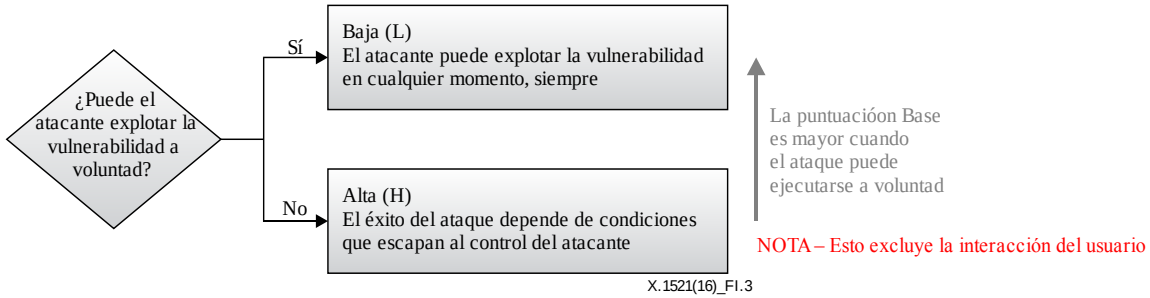
Los criterios de puntuación constituyen una rápida referencia para la calificación de las vulnerabilidades en v3.0. Tienen por objeto suplementar el análisis expuesto en el documento de las especificaciones.

I.5.1 Vector de ataque



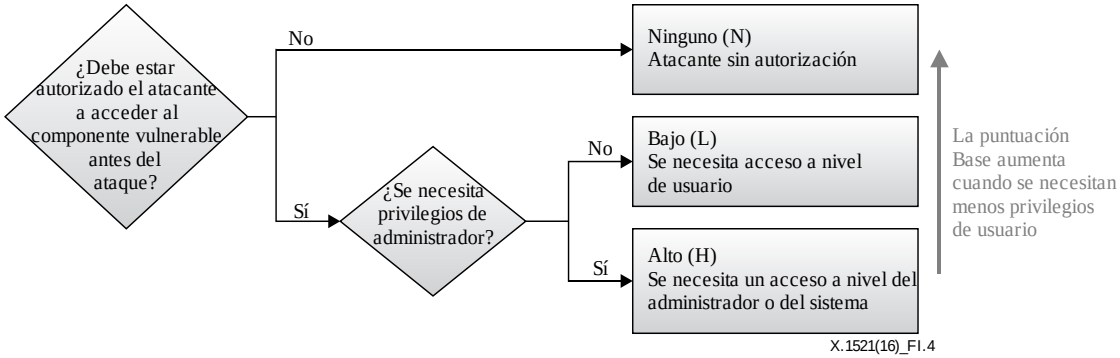
X.1521(16)_FI.2

I.5.2 Complejidad del ataque



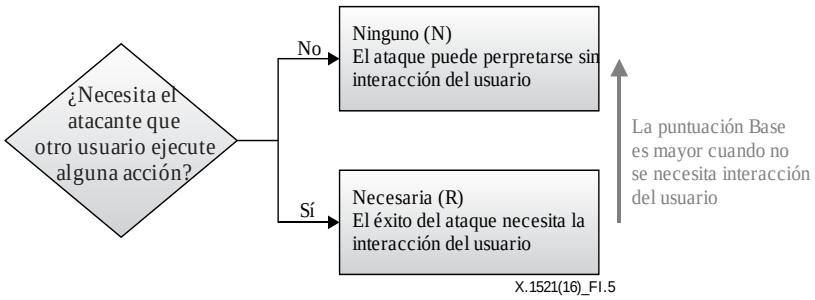
X.1521(16)_FI.3

I.5.3 Privilegios requeridos

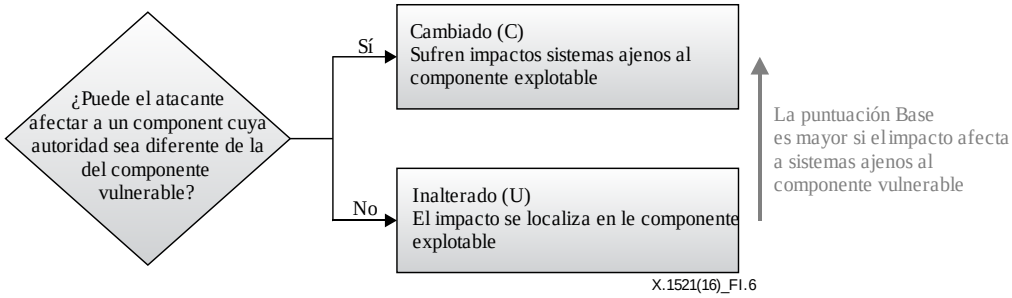


X.1521(16)_FI.4

I.5.4 Interacción del usuario

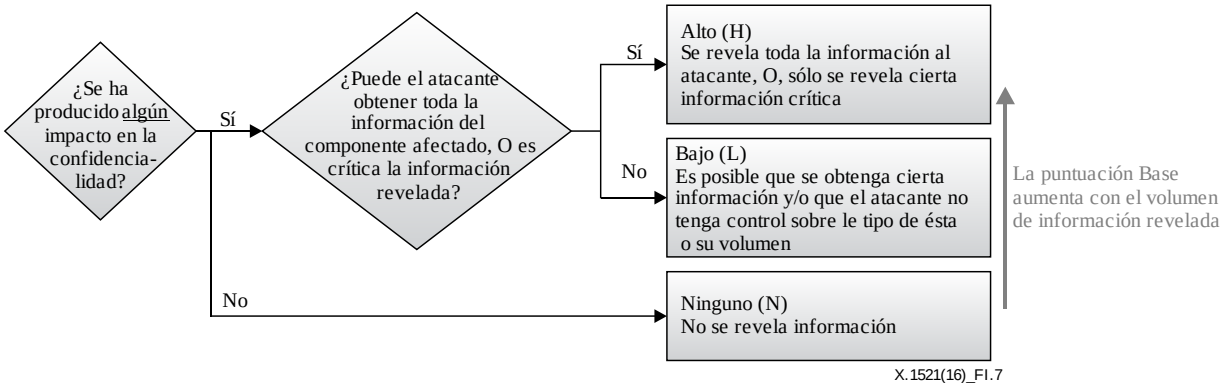


I.5.5 Ámbito

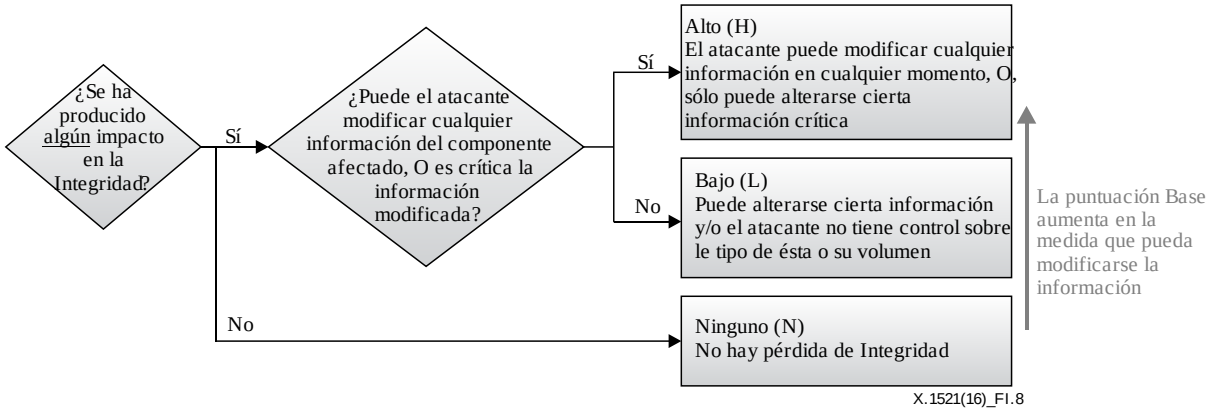


Nota, cundo no se produce un cambio de ámbito, el impacto en la Confidencialidad, la Integridad y la Disponibilidad refleja las consecuencias sobre el componente vulnerable, de lo contrario reflejarían las consecuencias sobre el componente que sufre el mayor impacto.

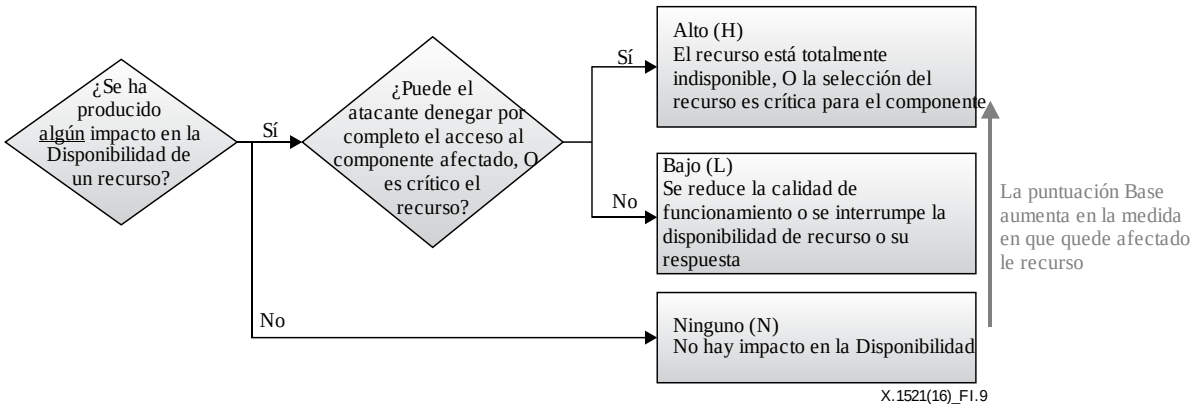
I.5.6 Impacto en la Confidencialidad



I.5.7 Impacto en la Integridad



I.5.8 Impacto en la Disponibilidad



Apéndice II

Recursos y enlaces

(Este apéndice no forma parte integral de la presente Recomendación.)

A continuación se indican referencias útiles a documentos adicionales sobre el CVSS v3.0.

Recurso	Localización
Documento de especificación	Incluye las descripciones de las métricas, las fórmulas y el vector cadena, y puede consultarse en: http://www.first.org/cvss/specification-document
Guía del usuario	Incluye una ampliación del análisis del CVSS v3.0, unos criterios de puntuación y un glosario, y se puede consultar en: http://www.first.org/cvss/user-guide
Documento de ejemplos	Incluye ejemplos prácticos de puntuaciones CVSS v3.0 y se puede consultar en: https://www.first.org/cvss/examples
Logotipo CVSS v3.0	Imágenes de alta y baja resolución que se pueden obtener de: http://www.first.org/cvss/identity
Calculadora CVSS v3.0	Implementación de referencia de las ecuaciones del CVSS v3.0 y se puede consultar en: http://www.first.org/cvss/calculator/3.0
Esquema XML	Definiciones del esquema que se encuentran en: https://www.first.org/cvss/cvss-v3.0.xsd

Bibliografía

[b-UIT-T X.1500] Recomendación UIT-T X.1500 (2011), *Aspectos generales del intercambio de información de ciberseguridad*.

[b-UIT-T X.1524] Recomendación UIT-T X.1524 (2011), *Lista de puntos débiles comunes*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2017