Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1525

(04/2015)

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 puntos débiles

Recomendación UIT-T X.1525

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 (1)	
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 (1)	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 (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1379
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de tecnología de libro mayor distribuido	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
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
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	X.1750–X.1759
SEGURIDAD DE 5G	X.1800–X.1819

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

Recomendación UIT-T X.1525

Sistema común de puntuación de puntos débiles

Resumen

En la Recomendación UIT-T X.1525 relativa al Sistema común de puntuación de puntos débiles (CWSS, *common weakness scoring system*) se describe un marco abierto para comunicar las características y repercusiones de los puntos débiles en las tecnologías de la información y las comunicaciones (TIC) durante el desarrollo de capacidades de software. El objetivo de esta Recomendación es permitir que los diseñadores de software de TIC, gestores, verificadores, proveedores de seguridad y servicios, compradores, proveedores de aplicaciones e investigadores utilicen un lenguaje común para puntuar los puntos débiles de las TIC que podrían manifestarse como vulnerabilidades al utilizar el software.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1525	17-04-2015	17	11.1002/1000/12357

* 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/.

© UIT 2020

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

ÍNDICE

Página

1 Alcance 1
2 Referencias 1
3 Definiciones 1
3.1 Términos definidos en otros documentos 1
3.2 Términos definidos en la presente Recomendación 2
4 Siglas y acrónimos 2
5 Convenios 3
6 Utilización del CWSS 3
6.1 Descripción del CWSS 4
6.2 Funcionamiento del CWSS 4
6.3 Puntuación CWSS 5
6.4 Usuarios del CWSS 6
7 Grupos métricos 7
7.1 Factores de los grupos métricos 7
7.2 Valores de incertidumbre y flexibilidad 9
7.3 Grupo métrico "hallazgo básico" 9
7.4 Grupo métrico "superficie de ataque" 15
7.5 Grupo métrico "contexto" 20
7.6 Fórmula de puntuación del CWSS 25
7.7 Vectores CWSS, ejemplos de puntuación y portabilidad de la puntuación ... 27
Bibliografía 31

Introducción

Los diseñadores de software reciben a menudo cientos o miles de informes de fallas (bugs) sobre puntos débiles detectados en su código. En determinadas circunstancias, estos puntos débiles pueden convertirse en vulnerabilidades explotables. Debido a este elevado volumen de puntos débiles notificados, los interesados suelen verse forzados a establecer prioridades sobre qué asuntos deben investigar y solucionar primero. En resumen, es necesario que las personas puedan argumentar y comunicarse entre sí sobre la importancia relativa de los distintos puntos débiles. Los métodos de puntuación que se emplean hoy en día son ad hoc o inadecuados para aplicarse a la evaluación, aún imprecisa, de la seguridad del software. El sistema común de puntuación de puntos débiles (CWSS) es un mecanismo para priorizar los puntos débiles del software de manera coherente, flexible y abierta, que permite incluir el contexto para diversos dominios empresariales y usos previstos del software. Se trata de un esfuerzo colectivo y colaborativo que trata de responder a las necesidades de los interesados de gobiernos, universidades e industria.

Los diseñadores de software de TIC, gestores, verificadores, proveedores de seguridad y servicios, compradores, proveedores de aplicaciones e investigadores utilicen un lenguaje común para la puntuación de puntos débiles de las TIC que podrían manifestarse como vulnerabilidades al utilizar el software. Así, necesitan priorizar dichos puntos débiles y encontrar soluciones para los que conllevan mayores riesgos. Cuando hay muchos puntos débiles que solucionar, cada uno valorado utilizando escalas diferentes, los diversos miembros de la comunidad de las TIC, los gerentes, verificadores, compradores y diseñadores tienen que adoptar una metodología para comparar los distintos puntos débiles y convertirlos en información útil que les permita tomar las medidas adecuadas.

Puesto que el CWSS constituye un método normalizado para caracterizar los puntos débiles, los usuarios del CWSS pueden recurrir métricas de la "superficie de ataque" y del contexto para aplicar la información contextual que refleje con la mayor exactitud el riesgo que entraña el software, a tenor del contexto empresarial particular al que está destinado y la función en concreta que desempeñará. Este método les permitirá tomar decisiones mejor informadas a la hora de mitigar los riesgos que entrañan los puntos débiles.

CWSS se basa en los trabajos realizados por la comunidad de ciberseguridad, como las numerosas vulnerabilidades reales especificadas en [b-ITU-T X.1520] – vulnerabilidades y exposiciones comunes (CVE) y el sistema de puntuación utilizado al examinar la gravedad de dichas vulnerabilidades públicamente conocidas gracias a [b-ITU-T X.1521] – Sistema común de puntuación de vulnerabilidades, así como la lista CWE (puntos débiles comunes) en la arquitectura del software y su diseño, código o instalación. Al elaborar el CWSS se pensó en que pudiera ofrecer valores razonables por omisión en ámbitos quizá desconocidos y, a su vez, la posibilidad de ajustarlo al contexto empresarial o técnico.

CWSS forma parte de un conjunto de Recomendaciones del UIT-T originalmente elaboradas por una comunidad amplia y mundial de usuarios que ha elaborado y hecho evolucionar una especificación abierta, que se pone a disposición del UIT-T para su adopción en la inteligencia de que al efectuar cualquier cambio o actualización de la misma se garantice una equivalencia y compatibilidad técnica completa y que en los debates sobre sus modificaciones y mejoras se apliquen los procedimientos de la comunidad de usuarios original e incluyan referencias explícitas a la versión que mantenga la comunidad de usuarios. Por consiguiente, en el momento en que se adopte la Recomendación UIT-T X.1525, se efectuará una verificación de debida diligencia y se formulará una declaración de equivalencia. A medida que la comunidad de usuarios aporte cambios, éstos se incorporarán puntualmente en las consiguientes versiones de la Recomendación gracias a una colaboración continua.

La Recomendación UIT-T X.1525 – Sistema común de puntuación de puntos débiles (CWSS) se ha preparado en colaboración con MITRE Corporation tomando en consideración la importancia de conservar, en la medida de lo posible, la compatibilidad técnica entre esta Recomendación UIT-T X.1525 – Sistema común de puntuación de puntos débiles (CWSS) y el "Sistema común de puntuación de puntos débiles (CWSS)", versión 1.0.1, de fecha 5 de septiembre de 2014 [https://cwe.mitre.org/cwss/cwss_v1.0.1.html].

Recomendación UIT-T X.1525

Sistema común de puntuación de puntos débiles

1 Alcance

La presente Recomendación describe un método normalizado para comunicar las características y repercusiones de los puntos débiles durante el desarrollo de capacidades software de TIC, mediante métricas de la "superficie de ataque" y del contexto con el fin de aplicar información contextual. El CWSS refleja con la mayor exactitud el riesgo para el usuario de la capacidad software, a tenor del contexto empresarial particular al que está destinado y la función empresarial concreta que el software ofrece al usuario.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, por referencia a las mismas en este texto, constituyen disposiciones de la presente 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 le confiere carácter 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 acceso [b-UIT-T X.1521]: 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.

3.1.2 disponibilidad [b-UIT-T X.1521]: acceso fiable y oportuno a datos y recursos realizado por individuos autorizados.

3.1.3 instancia de ataque [b-UIT-T X.1544]: ataque minucioso específico contra una aplicación o sistema destinado a vulnerabilidades o puntos débiles de ese sistema.

3.1.4 confidencialidad [b-UIT-T X.1521]: principio de seguridad destinado a garantizar que la información no se pone a disposición de sujetos no autorizados.

3.1.5 integridad [b-UIT-T X.1521]: principio de seguridad destinado a garantizar que la información y los sistemas no son modificados de forma maliciosa o accidental.

3.1.6 riesgo [b-UIT-T X.1521]: incidencia relativa que tendría en el entorno del usuario la explotación de una vulnerabilidad.

3.1.7 amenaza [b-UIT-T X.1521]: probabilidad o frecuencia de ocurrencia de un evento perjudicial.

3.1.8 vulnerabilidad [b-UIT-T X.1500]: cualquier punto débil que pudiera utilizarse para vulnerar un sistema o la información que contiene.

3.1.9 punto débil [b-UIT-T X.1524]: error o imperfección presente en el código, el diseño, la arquitectura o la instalación del software que puede, en un momento dado, convertirse en una vulnerabilidad o favorecer la aparición de otras vulnerabilidades.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se define el siguiente término:

3.2.1 viñeta: una viñeta es una manera formalizada y compartible de definir un contexto particular, la función que el software desempeña en dicho contexto y las prioridades de la organización en lo que respecta a la seguridad del software.

4 Siglas y acrónimos

En la presente Recomendación se utilizan las siguientes siglas y acrónimos:

AI Instancias de autentificación (*authentication instance*)

AL Capa del privilegio adquirido (*acquired privilege layer*)

AP Privilegio adquirido (*acquired privilege*)

AS Solidez de la autentificación (*authentication strength*)

ASLR Aleatorización del espacio de direcciones (*address space layout randomization*)

AV Vector de acceso (*access vector*)

BI Impacto en las actividades (*business impact*)

BVC Contexto de valor de las actividades (*business value context*)

CD Disco compacto (*compact disc*)

CIO Director de información (*chief information officer*)

CSO Director de seguridad (*chief security officer*)

CSRF Falsificación de petición en sitios cruzados (*cross-site-request-forgery*)

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

CWE Lista de puntos débiles comunes (*common weakness enumeration*)

CWRAF Marco común para el análisis de riesgos de puntos débiles (*common weakness risk analysis framework*)

CWSS Sistema común de puntuación de puntos débiles (*common weakness scoring system*)

DI Probabilidad de detección (*likelihood of discovery*)

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

DS Alcance del despliegue (*deployment scope*)

EC Eficacia del Control Externo (*external control effectiveness*)

EX Probabilidad de explotación (*likelihood of exploit*)

FC Confianza en el hallazgo (*finding confidence*)

FTP Protocolo de transferencia de ficheros (*file transfer protocol*)

HTML Lenguaje de marcaje de hipertexto (*hyper text markup language*)

IC Eficacia del Control Interno (*efficacité du contrôle interne*)

IN Nivel de interacción (*level of interaction*)

IP Protocolo Internet (*Internet protocol*)

NIST Instituto Nacional de Normas y Tecnología (*National Institute of Standards and Technology*)

OS Sistema operativo (*operating system*)

OWASP Proyecto abierto de seguridad de las aplicaciones web (*open web application security project*)

P Prevalencia (*prevalence*)

PCI DSS Norma de seguridad de datos para el sector de las tarjetas de pago (*payment card industry data security standard*)

RL Capa de privilegio necesario (*required privilege layer*)

RP Privilegio necesario (*required privilege*)

SAMATE Evaluación de herramientas y métricas de la garantía de la calidad del software (*software assurance metrics and tool evaluation*)

SANS Administración de sistemas, auditoría, redes y seguridad (*sysadmin, audit, networking, and security*)

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

SSL Capa de conexión de seguridad (*secure sockets layer*)

TI Impacto técnico (*technical impact*)

TIC Tecnología de la información y la comunicación

TLS Seguridad en la capa de transporte (*transport layer security*)

USB Bus serie universal (*universal serial bus*)

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

5 Convenios

Ninguno.

6 Utilización del CWSS

Actualmente, los diseñadores de software de TIC, gerentes, verificadores, proveedores de seguridad y servicios, compradores, proveedores de aplicaciones e investigadores deben identificar y evaluar los puntos débiles en el software que podrían manifestarse como vulnerabilidades al utilizarlo. Así, necesitan priorizar dichos puntos débiles y encontrar soluciones para los que conllevan mayores riesgos. Cuando hay muchos puntos débiles que solucionar, cada uno valorado utilizando escalas diferentes, los diversos miembros de la comunidad de las TIC, los gerentes, verificadores, compradores y diseñadores tienen que adoptar una metodología propia para comparar los distintos puntos débiles y convertirlos en información útil que les permita tomar las medidas adecuadas. El sistema común de puntuación de puntos débiles (CWSS) es un marco abierto que responde a esta necesidad. Presenta las siguientes ventajas:

- Mediciones cuantitativas: el CWSS ofrece una medición cuantitativa de los puntos débiles no solucionados que pudieran tener una aplicación software.
- Marco común: el CWSS ofrece un marco común para priorizar errores de seguridad ("puntos débiles") detectados en las aplicaciones software.

- Establecimiento de prioridades personalizado: el consumidor puede utilizar el CWSS junto con el Marco común para el análisis de riesgos de puntos débiles (Common Weakness Risk Analysis Framework, CWRAF) [b-CWRAF], para determinar los tipos más importantes de puntos débiles para su esfera de actividad, a fin de informarles en sus actividades de adquisición y protección, como parte del proceso más amplio de lograr garantía de calidad del software.

6.1 Descripción del CWSS

El CWSS está estructurado en tres *grupos métricos*: hallazgo básico, superficie de ataque y contexto, como se muestra en la Figura 1. Cada grupo consta de múltiples métricas – denominados también *factores* – que se utilizan para calcular la puntuación CWSS de un punto débil.

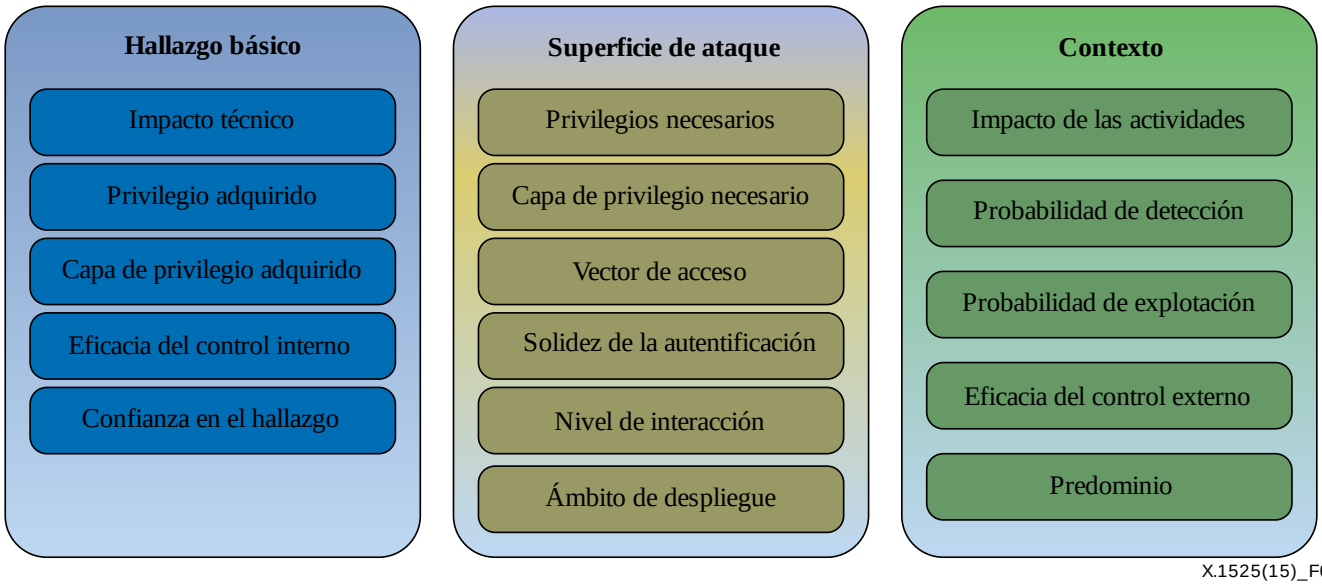

Figura 1 – Grupos métricos del CWSS

A continuación se describen estos grupos métricos:

- Hallazgo básico: indica el riesgo inherente del punto débil, el grado de confianza en la exactitud del hallazgo y la solidez de los controles. Este grupo métrico se examina en la cláusula 7.3.
- Superficie de ataque: los obstáculos que un atacante ha de superar para explotar el punto débil. Este grupo métrico se examina en la cláusula 7.4.
- Contexto: características del punto débil que son específicas de un determinado contexto operativo o entorno. Este grupo métrico se examina en la cláusula 7.5.

6.2 Funcionamiento del CWSS

Se asigna un valor a cada factor del grupo métrico hallazgo básico. Se aplica a estos valores la correspondiente ponderación y se calcula un subpuntuación del hallazgo básico. Esta subpuntuación está comprendida entre 0 y 100. Se aplica este mismo método a los otros dos grupos métricos, superficie de ataque y contexto; sus subpuntuaciones están en la gama de 0 a 1. Por último, las tres subpuntuaciones se multiplican entre sí, obteniéndose una puntuación CWSS entre 0 y 100, como se ilustra en la Figura 2.

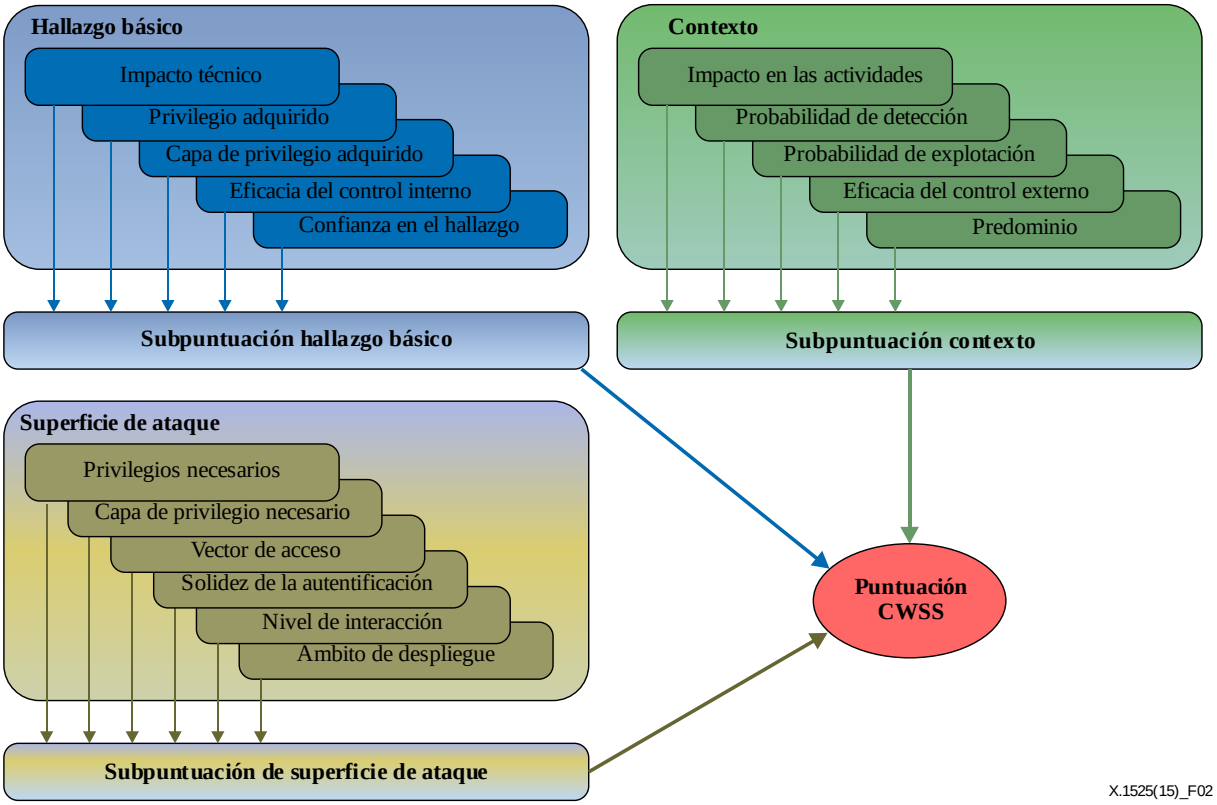

Figura 2 – Puntuación CWSS

6.3 Puntuación CWSS

La comunidad de interesados está colaborando con MITRE en la investigación de diversos métodos de puntuación diferentes a los que quizá haya de dar soporte el marco CWSS. Los cuatro métodos de puntuación actuales son:

Específica — Se puntúan los puntos débiles detectados en el diseño o realización de un paquete de software concreto ("específico"), por ejemplo, el desbordamiento de una memoria tampón en el nombre de usuario o una rutina de autentificación en la línea 1234 de server.c del paquete del servidor FTP. Las herramientas automáticas y los consultores de seguridad del software utilizan métodos concretos para evaluar la seguridad de un paquete de software en lo que respecta a sus puntos débiles.

Generalizada — Se puntúan clases de puntos débiles con independencia del paquete de software particular, a fin de priorizarlos (por ejemplo, "los desbordamientos de memoria tampón tienen prioridad más alta que los escapes de memoria"). Este es el método utilizado por CWE/SANS Top 25, OWASP Top Ten y otras actividades similares, pero también por algunos escáneres de código automáticos. Las puntuaciones generalizadas pueden diferir considerablemente de las específicas que se obtendrían al analizar exhaustivamente cada una de las clases de puntos débiles de un paquete de software específico. Por ejemplo, aunque la clase "desbordamiento de la memoria tampón" es importantísima para muchos diseñadores, las fallas en esta memoria pudieran ser menos importantes si no puede provocarlas directamente un atacante y su impacto queda reducido por los mecanismos de protección del sistema operativo (OS), como por ejemplo la aleatorización del espacio de direcciones (ASLR).

Adaptada al contexto	Modificar la puntuación con arreglo a las necesidades de un contexto analítico específico que pudiera integrar las prioridades de las actividades/misión, contexto de amenazas, tolerancia a riesgos, etc. Estas necesidades se indican mediante viñetas que vinculan las características inherentes de los puntos débiles con consideraciones empresariales de nivel más elevado. Este método podría aplicarse tanto a la puntuación específica como a la generalizada.
Combinada	Se combinan los resultados de múltiples puntuaciones de nivel inferior para obtener una sola puntuación general (o "grado"). Si bien la esta puntuación combinada sería más fácil de aplicar al método de puntuación específica, también podría utilizarse en la puntuación generalizada, como en el caso de 2010 CWE/SANS Top 25.

Obsérvese que la mayoría de los debates actuales sobre CWSS se concentra en el método de puntuación específica y el marco para la puntuación adaptada al contexto. Los métodos de puntuación combinada se tratarán ulteriormente. La puntuación generalizada se está desarrollando por separado, principalmente como parte de 2011 Top 25 y CWRAF.

Las puntuaciones CWSS pueden calcularse automáticamente, por ejemplo mediante una herramienta de análisis de código, o bien manualmente mediante un consultor o ingeniero de seguridad del software. Dado que el análisis automático no dispondrá probablemente de cierta información – como el contexto operativo de la aplicación – la puntuación CWSS podría realizarse posiblemente en múltiples rondas: en primer lugar, una herramienta calcula las puntuaciones CWSS automáticamente y luego una persona, en este caso un analista, añade manualmente la información adicional y vuelve a calcular las puntuaciones.

6.4 Usuarios del CWSS

En aras de la eficacia, el CWSS da soporte a múltiples casos de utilización por diferentes interesados en disponer de un sistema de puntuación coherente para priorizar los puntos débiles del software que podrían poner en riesgo productos, sistemas, redes y servicios. A continuación figuran varios ejemplos de los principales interesados:

- Diseñadores de software: a menudo trabajan con plazos breves, debido a los ciclos de publicación y a los limitados recursos. Por consiguiente, no pueden investigar y resolver todos y cada uno de los puntos débiles notificados. La opción es concentrarse en los más problemáticos y fáciles de resolver. Si los puntos débiles se detectan de manera automática, tienen la opción de concentrarse en aquellos con menor probabilidad de ser un falso positivo.
- Gestores de desarrollo de software: crean estrategias para priorizar y suprimir clases completas de puntos débiles en toda la base de código o al menos en la parte que se considera con más riesgo, posiblemente mediante la creación de la lista de los "N más importantes". Deben comprender la incidencia en la seguridad de integrar software de terceros, que tendrán posiblemente sus propios puntos débiles. Quizá también se haya de dar soporte a distintos requisitos de seguridad y prioridades para cada línea de producto.
- Clientes del software: los clientes, comprendidos el personal de compras, desean obtener software de terceros con un nivel razonable de garantía de calidad de que el proveedor del software ha realizado la debida diligencia para suprimir o evitar los puntos débiles más importantes para las actividades o misión del comprador. Entre los interesados están los directores de información (CIOs), los directores de seguridad (CSOs), los administradores de sistema y los usuarios finales del software.

- Gestores de seguridad de la empresa: los gestores de seguridad de la empresa tratan de minimizar los riesgos en su empresa, tanto las debidas a vulnerabilidades de productos de terceros como las debidas a vulnerabilidades (o puntos débiles) del software creado internamente. Quizá deseen utilizar un mecanismo de puntuación que pueda integrarse con otros procesos de gestión de la seguridad, tales como la combinación de los resultados de exploración de vulnerabilidades de terceros (las que son conocidas) con el análisis de aplicaciones a medida (para el software interno) con el fin de evaluar el riesgo general de un activo.
- Analistas y consultores de código: los analistas y consultores suelen disponer de sus propias técnicas de puntuación personalizadas, pero desean suministrar un mecanismo de puntuación coherente y reconocido por la comunidad para diferentes clientes.
- Evaluadores de capacidades de análisis de código: los evaluadores analizan y miden las capacidades de las técnicas de análisis de código (por ejemplo, NIST SAMATE). Podrían utilizar un mecanismo coherente de puntuación de puntos débiles para ayudar a hacer un muestreo de los hallazgos notificados y así comprender mejor la gravedad de dichos hallazgos en función de los métodos de puntuación ad hoc, que pueden variar sobremanera según la herramienta/técnica.
- Otros interesados: otros interesados son investigadores de vulnerabilidades, defensores del desarrollo seguro y analistas de la conformidad (por ejemplo, PCI DSS).

Al mes de junio de 2014 (cuando el CWSS 0.8 estaba vigente), había diversas materializaciones del CWSS en el mundo real. Los principales usuarios eran los analistas de código y los consultores de seguridad del software.

7 Grupos métricos

7.1 Factores de los grupos métricos

El CWSS consta de los siguientes factores, organizados de acuerdo a su grupo métrico, como se muestra en el Cuadro 1 siguiente. Cada factor se describe con mayor detalle en las cláusulas siguientes.

Cuadro 1 – Factores de los grupos métricos

Grupo	Nombre	Resumen
Hallazgo básico	Impacto técnico (TI)	La posible repercusión que pudiera tener el punto débil, suponiendo que pueda accederse y explotarse.
	Privilegio adquirido (AP)	Tipo de privilegios que obtiene el atacante que consiga explotar el punto débil.
	Capa de privilegio adquirido (AL)	La capa operativa en la que el atacante obtiene privilegios al explotar con éxito el punto débil.
	Eficacia del control interno (IC)	La capacidad del control para impedir al atacante explotar el punto débil.
	Confianza en el hallazgo (FC)	El grado de confianza en que el problema notificado es un punto débil que pudiera utilizar un atacante.
Superficie de ataque	Privilegio requerido (RP)	El tipo de privilegios que un atacante debe disponer de antemano para poder llegar al código/funcionalidad donde se encuentra el punto débil.
	Capa del privilegio requerido (RL)	La capa operativa en la que el atacante debe tener privilegios para tratar de atacar el punto.
	Vector de acceso (AV)	El canal por donde el atacante debe comunicar para alcanzar el código o funcionalidad que contiene el punto débil.
	Solidez de la autentificación (AS)	La solidez de la rutina de autentificación que protege el código/funcionalidad donde se encuentra el punto débil.
	Nivel de interacción (IN)	Acciones que debe realizar la víctima humana para que pueda darse un ataque exitoso.
	Ámbito de despliegue (SC)	Si el punto débil está presente en todas las instancias desplegables del software, o si se limita a un subconjunto de plataformas y/o configuraciones.
Contexto	Impacto empresarial (BI)	El posible impacto para las actividades o la misión si se consigue explotar el punto débil.
	Probabilidad de detección (DI)	La probabilidad de que el atacante pueda descubrir el punto débil.
	Probabilidad de explotación (EX)	La probabilidad de que, si se detecta un punto débil, un atacante con privilegios/autentificación/acceso pueda explotarlos.
	Eficacia del control externo (EC)	La capacidad de controlar o mitigar la exposición externa del software de modo que resulte más difícil a un atacante alcanzar y/o explotar el punto débil.
	Prevalencia (P)	Frecuencia con la que aparece este tipo de punto débil en el software.

7.2 Valores de incertidumbre y flexibilidad

El CWSS puede utilizarse en casos en los que se dispone de poca información al principio, pero la calidad de la información va mejorando con el tiempo. Cabe esperar que en muchos casos de utilización, la puntuación CWSS de una determinada debilidad detectada pueda variar frecuentemente a medida que se vaya obteniendo información. Diversas entidades podrían evaluar los distintos factores en momentos diferentes.

Cada factor CWSS dispone efectivamente de características "contextuales" o "temporales", por lo que no resulta particularmente útil adoptar los mismos tipos de grupos métricos que en el CVSS.

Muchos factores tienen en común los cuatro valores que se muestran en el Cuadro 2.

Cuadro 2 – Valores de los factores de incertidumbre y flexibilidad

Valor	Utilización
Desconocido	La entidad que calcula la puntuación no dispone de información suficiente para asignar un valor al factor. Este puede ser un índice de que se ha de proseguir la investigación. Por ejemplo, un escáner de código automático puede ser capaz de detectar ciertos puntos débiles, pero no puede detectar si se dispone de algún mecanismo de autentificación. El valor "desconocido" indica que la puntuación está incompleta o es un valor estimado y que, por tanto, se debe profundizar en el análisis. De esta manera se facilita la modelización de la información incompleta y para el Contexto del Valor Empresarial, influenciar las puntuaciones finales generados utilizando información incompleta. La ponderación de este valor es 0,5 para todos los factores, lo que generalmente produce una puntuación inferior; la adición de nueva información (es decir, la asignación de otro valor a algunos factores de valor "desconocido") dará lugar a un ajuste al alza o a la baja en función de la nueva información.
No aplicable	Se hace caso omiso del factor al calcular la puntuación. Esto permite al Contexto de Valor Empresarial dictaminar si un factor resulta pertinente para la puntuación final. Por ejemplo, un método de puntuación CWSS centrado en el cliente podría hacer caso omiso de la tentativa de resolución y un contexto de elevada garantía podría requerir investigar todos los hallazgos notificados, aun cuando se tenga escasa confianza en su exactitud. En el caso de puntos débiles hallados en un determinado paquete de software, cabe esperar que todos los hallazgos tendrán el mismo valor "No aplicable" para el factor que se hace caso omiso.
Cuantificado	El factor se puede ponderar utilizando una gama continua cuantificada de 0,0 a 1,0, en lugar de un conjunto definido de factores de valores discretos. No todos los factores son cuantificables de esta manera, pero permite la personalización adicional de la métrica.
Por omisión	Se puede fijar un valor por omisión de la ponderación del factor. Al clasificar el factor como por omisión permite la investigación y posible modificación posteriormente.

7.3 Grupo métrico "hallazgo básico"

El grupo métrico de hallazgo básico consta de los siguientes factores:

- Impacto técnico (TI)
- Privilegio adquirido (AP)
- Capa del privilegio adquirido (AL)
- Eficacia del control interno (IC)
- Confianza en el hallazgo (FC)

La combinación de los valores de impacto técnico, privilegio adquirido y capa del privilegio adquirido ofrece al usuario la capacidad de expresión. Por ejemplo, el usuario puede caracterizar el impacto técnico como "elevado" con privilegios de "Administrador" en la capa "aplicación".

7.3.1 Impacto técnico (TI)

El impacto técnico es el resultado potencial que debe tener el punto débil, suponiendo que éste pueda alcanzarse y explotarse. Este impacto se puede expresar con más precisión que los términos confidencialidad, integridad y disponibilidad.

El impacto técnico debería evaluarse respecto del privilegio adquirido (AP) y la capa del privilegio adquirido (AL).

Cuadro 3 – Ponderación del impacto técnico

Valor	Código	Peso	Descripción
Crítico	C	1,0	Control completo sobre el software analizado, hasta el punto de impedir las operaciones.
Elevado	H	0,9	Control considerable sobre el software analizado, o acceso a información muy sensible.
Medio	M	0,6	Control moderado del software analizado, o acceso a información moderadamente importante.
Bajo	L	0,3	Control mínimo sobre el software analizado, o acceso limitado a información relativamente importante.
Ninguno	N	0,0	No hay impacto técnico en el software analizado. Es decir, no genera vulnerabilidad alguna.
Por omisión	D	0,6	El valor de la ponderación por omisión es la media de los valores crítico, elevado, medio, bajo y ninguno.
Desconocido	UK	0,5	No se dispone de información suficiente para asignar un valor a este factor. Es necesario profundizar en el análisis. En el futuro se podrá asignar un valor diferente, que podría afectar a la puntuación.
No aplicable	NA	1,0	Se hace caso omiso de este factor en el cálculo de la puntuación, dado que no depende de cómo se establezca la prioridad de puntos débiles. Este factor quizá no sea aplicable en un contexto que exige garantías elevadas, en cuyo caso el usuario quizá desee investigar todos y cada uno de los puntos débiles hallados, con independencia del grado de confianza.
Cuantificado	Q		Este factor podría cuantificarse con ponderaciones personalizadas.

Si este conjunto de valores no es lo suficientemente exacto, los usuarios del CWSS pueden utilizar sus propios métodos cuantificados para obtener una subpuntuación. Uno de tales métodos consiste en utilizar el CWRAF (marco común de análisis de riesgos de puntos débiles) [b-CWRAF] a fin de definir una viñeta y una ficha de puntuación del impacto técnico. La ponderación del impacto se calcula utilizando una clasificación de la importancia específica de la viñeta para diferentes impactos técnicos que podrían resultar de la explotación del punto débil, por ejemplo, la modificación de datos sensibles, los privilegios obtenidos, el consumo de recursos, etc.

7.3.2 Privilegio adquirido (AP)

El privilegio adquirido identifica el tipo de privilegios que obtiene un atacante que desea explotar con éxito el punto débil.

Obsérvese que los valores son idénticos a los del privilegio requerido, pero las ponderaciones son diferentes.

En algunos casos, el valor de los privilegios adquiridos puede ser el mismo que en el de los privilegios requeridos, lo que implica 1) aumento del privilegio "horizontal" (por ejemplo, de un usuario sin privilegios a otro) o 2) aumento de privilegios en un espacio acotado (sandbox), como un usuario exclusivo del FTP (protocolo de transferencia de ficheros) que logra entrar al intérprete de comandos (shell).

Cuadro 4 – Ponderación del privilegio adquirido

Valor	Código (Nota)	Peso	Descripción
Administrador	A	1,0	El atacante obtiene acceso a una entidad con privilegios de administrador, raíz (root), SISTEMA o equivalente que implica control total del software analizado; o el atacante puede aumentar sus privilegios (inferiores) a los de administrador.
Usuario con privilegios parciales	P	0,9	El atacante obtiene acceso a una entidad con privilegios especiales, pero no suficientes como para ser administrador; o el atacante puede aumentar sus propios privilegios (inferiores) a un usuario con privilegios parciales. Por ejemplo, el usuario puede tener privilegios para hacer copias de seguridad, pero no para modificar la configuración del software o instalar actualizaciones.
Usuario ordinario	RU	0,7	El atacante obtiene acceso a una entidad con derechos de usuario ordinario sin privilegios especiales; o el atacante aumenta sus propios privilegios (inferiores) a los de un usuario ordinario.
Limitado/invitado	L	0,6	El atacante obtiene acceso a una entidad con derechos limitados o de "invitado" que restringen considerablemente las actividades autorizadas; o el atacante puede aumentar sus propios privilegios (inferiores) al de invitado. Nota: este valor no se refiere al de "sistema operativo invitado", concepto utilizado en entornos virtualizados.
Ninguno	N	0,1	El atacante no puede obtener acceso a ningún privilegio adicional aparte de los que ya dispone. (Obsérvese que este valor puede resultar útil en determinadas circunstancias en las que el atacante puede escapar del espacio acotado (sandbox) u otro entorno restrictivo, pero sin poder obtener privilegios adicionales o acceso como otros usuarios.)
Por omisión	D	0,7	Promedio de los valores de ponderación de ninguno, invitado, usuario ordinario, usuario con privilegios parciales y administrador.
Desconocido	UK	0,5	No se dispone de información suficiente para asignar un valor a este factor. Es necesario profundizar en el análisis. En el futuro se podrá asignar un valor diferente, que podría afectar a la puntuación.
No aplicable	NA	1,0	Se hace caso omiso de este factor en el cálculo de la puntuación, dado que no depende de cómo se establezca la prioridad de puntos débiles. Este factor quizá no sea aplicable en un contexto que exige garantías elevadas, en el que se desea aplicar estrictamente la separación de privilegios, incluso entre los usuarios que ya disponen de privilegios.
Cuantificado	Q		Este factor podría cuantificarse con ponderaciones personalizadas. Obsérvese que se admiten valores cuantificados en aras de la integridad; ahora bien, dado que los privilegios y los usuarios son entidades discretas, en determinadas circunstancias resultaría útil disponer de un modelo cuantificado.
NOTA – Existe un acrónimo para los valores (en inglés) de este factor, a saber, "RUNLAP" (RU, N, L, A, P) (Regular User, None, Limited, Admin, Partially-Privileged).			

7.3.3 Capa de privilegio adquirido (AL)

La capa de privilegios adquiridos es la capa operativa en la que el atacante obtiene privilegios al explotar con éxito el punto débil.

Cuadro 5 – Ponderación de la capa de privilegios adquiridos

Valor	Código (Nota)	Peso	Descripción
Aplicación	A	1,0	El atacante adquiere privilegios que permite el software analizado. (Si el software analizado forma parte esencial del sistema subyacente, como el núcleo de un sistema operativo, el valor "sistema" sería más adecuado.)
Sistema	S	0,9	El atacante obtiene privilegios en una máquina física o sistema subyacente que se utiliza para ejecutar el software analizado.
Red	N	0,7	El atacante adquiere privilegios para acceder a la red.
Infraestructura empresarial	E	1,0	El atacante adquiere privilegios en un elemento esencial de la infraestructura de la empresa, como un encaminador, un conmutador, el sistema de nombres de dominio (DNS), el controlador de dominio, el cortafuegos, la identidad del servidor, etc.
Por omisión	D	0,9	Promedio de las ponderaciones de aplicación, sistema, red e infraestructura de empresa.
Desconocido	UK	0,5	No se dispone de información suficiente para asignar un valor a este factor. Es necesario profundizar en el análisis. En el futuro se podrá asignar un valor diferente, que podría afectar a la puntuación.
No aplicable	NA	1,0	Se hace caso omiso de este factor en el cálculo de la puntuación, dado que no depende de cómo se establezca la prioridad de puntos débiles. Este factor quizá no sea aplicable en un contexto que exige garantías elevadas, en el que se desea aplicar estrictamente la separación de privilegios, incluso entre los usuarios que ya disponen de privilegios.
Cuantificado	Q		Este factor podría cuantificarse con ponderaciones personalizadas. Obsérvese que se admiten valores cuantificados en aras de la integridad; ahora bien, dado que las capas de privilegios son entidades discretas, en determinadas circunstancias resultaría útil disponer de un modelo cuantificado.
NOTA – Existe un acrónimo para los valores (en inglés) de este factor, a saber, "SANE" (S, A, N, E) (System, Application, Network, Enterprise Infrastructure).			

7.3.4 Eficacia del control interno (IC)

El control interno es un mecanismo de control, protección o mitigación creado específicamente en el software (ya sea por arquitectura, diseño o aplicación). La eficacia del control interno mide la capacidad del control para evitar que un atacante pueda explotar el punto débil. Por ejemplo, una rutina de validación de entrada que restrinja la longitud a 15 caracteres puede resultar moderadamente efectiva contra ataques XSS (secuencias de comandos en sitios cruzados) reduciendo el tamaño del artilugio (exploit) XSS con el que se puede ensayar.

Cuando existen múltiples controles internos o múltiples trayectos del código que pueden llegar al mismo punto débil, se aplica la siguiente guía:

- Para cada trayecto del código, se analiza cada control interno que figura a lo largo del trayecto del código y se selecciona el valor con menor ponderación (es decir, el control interno más robusto a lo largo del trayecto del código). Este valor se denomina Valor del Trayecto del Código.
- Se recopila todos los Valores de Trayecto del Código.
- Se selecciona el Valor de Trayecto del Código con mayor ponderación (es decir, el control más débil).

Este método evalúa cada trayecto del código en lo que respecta al control más sólido del trayecto del código (dado que el atacante tendrá que eludir dicho control), luego se selecciona el trayecto del código más débil (es decir, la ruta más fácil que pueda tomar el atacante).

Cuadro 6 – Ponderación de la eficacia del control interno

Valor	Código	Peso	Descripción
Ninguno	N	1,0	No existe control alguno.
Limitado	L	0,9	Existen métodos sencillos o restricciones casuales que podrían impedir a un atacante ocasional explotar el punto débil.
Moderado	M	0,7	El mecanismo de protección se utiliza normalmente pero tiene limitaciones conocidas que podría eludir con cierto esfuerzo un atacante experimentado. Por ejemplo, la codificación de entidades de lenguaje de marcaje de hipertexto (HTML) para impedir ataques XSS podría eludirse cuando la salida se encuentra en otro contexto, como en una hoja de estilos en cascada o un atributo de etiquetas HTML.
Indirecto (Defensa en profundidad)	I	0,5	El control no protege específicamente contra la explotación del punto débil, pero reduce de manera indirecta su impacto cuando se lanza con éxito un ataque, o dificulta la construcción de un artilugio (exploit) funcional. Por ejemplo, una rutina de validación podría limitar indirectamente el tamaño de una entrada, lo que dificulta al atacante construir una carga útil para efectuar un ataque por inyección SQL (lenguaje de consulta estructurado) o XSS.
El mejor disponible	B	0,3	El control sigue las prácticas más idóneas, aunque pudieran existir ciertas limitaciones que podría superar un atacante hábil y resuelto, posiblemente aprovechando también otros puntos débiles. Por ejemplo, el método de doble presentación para la protección contra CSRF (falsificación de petición en sitios cruzados) se considera uno de los más sólidos, pero se puede vencer si se emplean además con ciertas funcionalidades que permiten leer los encabezamientos HTTP en bruto.

Cuadro 6 – Ponderación de la eficacia del control interno

Valor	Código	Peso	Descripción
Completo	C	0,0	El control es totalmente eficaz respecto del punto débil, es decir, no hay falla o vulnerabilidad y la explotación de este problema no tiene consecuencias negativas. Por ejemplo, una operación de copia de memoria tampón que garantice que la memoria de destino es más grande que la de origen (más cualquier otra expansión indirecta del tamaño de la fuente original) no causará un desbordamiento.
Por omisión	D	0,6	Promedio de las ponderaciones de Completo, el mejor disponible, indirecto, moderado, limitado y ninguno.
Desconocido	UK	0,5	No se dispone de información suficiente para asignar un valor a este factor. Es necesario profundizar en el análisis. En el futuro se podrá asignar un valor diferente, que podría afectar a la puntuación.
No aplicable	NA	1,0	Se hace caso omiso de este factor de manera deliberada al calcular la puntuación dado que no depende de cómo se establezca la prioridad de puntos débiles.
Cuantificado	Q		Este factor podría cuantificarse con ponderaciones personalizadas.

7.3.5 Confianza en el hallazgo (FC)

La confianza en el hallazgo es el grado de confianza que se tiene en el problema notificado:

1) sea un punto débil, y
2) pueda desencadenarlo o utilizarlo un atacante.

Cuadro 7 – Ponderación de la confianza en el hallazgo

Valor	Código	Peso	Descripción
Veracidad demostrada	T	1,0	El atacante puede tener acceso al punto débil.
Veracidad demostrada localmente	LT	0,8	El punto débil se produce en una función o componente cuyo diseño se basa en la invocación segura de dicha función, pero no se sabe en qué medida el atacante pueda tener acceso a dicha función. Por ejemplo, una función de utilidad podría construir una consulta a base de datos sin codificar sus entradas, pero si sólo se invoca con cadenas de constantes, el hallazgo es localmente cierto.
Falsedad demostrada	F	0,0	El hallazgo es erróneo (es decir, el hallazgo es un falso positivo y no existe punto débil) y/o no hay nada que pueda hacer un posible atacante.
Por omisión	D	0,8	Promedio de las ponderaciones de veracidad demostrada, veracidad demostrada localmente y falsedad demostrada.
Desconocido	UK	0,5	No se dispone de información suficiente para asignar un valor a este factor. Es necesario profundizar en el análisis. En el futuro se podrá asignar un valor diferente, que podría afectar a la puntuación.
No aplicable	NA	1,0	Se hace caso omiso de este factor en el cálculo de la puntuación, dado que no depende de cómo se establezca la prioridad de puntos débiles. Este factor quizá no sea aplicable en un contexto que exige garantías elevadas, en cuyo caso el usuario quizá desee investigar todos y cada uno de los puntos débiles hallados, con independencia del grado de confianza.

Cuadro 7 – Ponderación de la confianza en el hallazgo

Valor	Código	Peso	Descripción
Cuantificado	Q		Este factor podría cuantificarse con ponderaciones personalizadas. Algunas herramientas de análisis de código disponen de mediciones precisas de la exactitud de los patrones de detección específicos.

7.4 Grupo métrico "superficie de ataque"

El grupo métrico "superficie de ataque" consta de los siguientes factores:

- Privilegios requeridos (RP)
- Capa de privilegios requeridos (RL)
- Vector de acceso (AV)
- Solidez de la autentificación (AS)
- Nivel de interacción (IN)
- Ámbito de despliegue (SC).

7.4.1 Privilegios necesarios (RP)

Por privilegios necesarios se entiende el tipo de privilegios que un atacante debe disponer para alcanzar el código/funcionalidad que contiene el punto débil.

Cuadro 8 – Ponderaciones de privilegios necesarios

Valor	Código (Nota)	Peso	Descripción
Ninguno	N	1,0	No se requieren privilegios. Por ejemplo, un motor de búsqueda por la web quizá no requiera privilegio alguno para buscar un término y visualizar los resultados.
Limitado/invitado	L	0,9	La entidad dispone de privilegios limitados o de "invitado" que pueden considerablemente restringir las actividades autorizadas; la entidad puede ser capaz de registrar o crear una nueva cuenta sin ningún requisito especial o prueba de identidad. Por ejemplo, una bitácora (blog) web puede permitir a los participantes crear un nombre de usuario e introducir una dirección válida de correo electrónico antes de poder hacer comentarios. Nota: este valor no se refiere al de "sistema operativo invitado", concepto utilizado en entornos virtualizados.
Usuario ordinario	RU	0,7	La entidad es un usuario ordinario sin privilegios especiales.
Usuario con privilegios parciales	P	0,6	La entidad es un usuario válido con privilegios especiales, pero no suficientes como para ser administrador. Por ejemplo, el usuario puede tener privilegios para hacer copias de seguridad, pero no para modificar la configuración del software o instalar actualizaciones.
Administrador	A	0,1	LA entidad tiene privilegios de administrador, raíz (root), SISTEMA o equivalente que implica control total del software o del sistema operativo subyacente.
Por omisión	D	0,7	Promedio de las ponderaciones para ninguno, limitado, usuario ordinario, usuario con privilegios parciales y administrador.

Cuadro 8 – Ponderaciones de privilegios necesarios

Valor	Código (Nota)	Peso	Descripción
Desconocido	UK	0,5	No se dispone de información suficiente para asignar un valor a este factor. Es necesario profundizar en el análisis. En el futuro se podrá asignar un valor diferente, que podría afectar a la puntuación.
No aplicable	NA	1,0	Se hace caso omiso de este factor en el cálculo de la puntuación, dado que no depende de cómo se establezca la prioridad de puntos débiles. Este factor quizá no sea aplicable en un contexto que exige garantías elevadas, en el que se desea aplicar estrictamente la separación de privilegios, incluso entre los usuarios que ya disponen de privilegios.
Cuantificado	Q		Este factor podría cuantificarse con ponderaciones personalizadas. Obsérvese que se admiten valores cuantificados en aras de la integridad; ahora bien, dado que los privilegios y los usuarios son entidades discretas, en determinadas circunstancias resultaría útil disponer de un modelo cuantificado.
NOTA – Existe un acrónimo para los valores (en inglés) de este factor, a saber, "RUNLAP" (RU, N, L, A, P) (Regular User, None, Limited, Admin, Partially-Privileged).			

7.4.2 Capa de privilegios requeridos (RL)

La capa de privilegios necesarios es la capa operativa en la que el atacante debe tener privilegios a fin de poder intentar atacar el punto débil.

Cuadro 9 – Ponderación de la capa de privilegios necesarios

Valor	Código (Nota)	Peso	Descripción
Aplicación	A	1,0	El atacante debe disponer de privilegios que permite el software analizado. (Si el software analizado forma parte esencial del sistema subyacente, como el núcleo de un sistema operativo, el valor "sistema" sería más adecuado.)
Sistema	S	0,9	El atacante debe disponer de privilegios en una máquina física o sistema subyacente que se utiliza para ejecutar el software analizado.
Red	N	0,7	El atacante debe disponer de privilegios para acceder a la red.
Infraestructura de la empresa	E	1,0	El atacante debe disponer de privilegios en un elemento esencial de la infraestructura de la empresa, como un encaminador, un conmutador, el DNS, el controlador de dominio, el cortafuegos, la identidad del servidor, etc.
Por omisión	D	0,9	Promedio de las ponderaciones de aplicación, sistema, red e infraestructura de empresa.
Desconocido	UK	0,5	No se dispone de información suficiente para asignar un valor a este factor. Es necesario profundizar en el análisis. En el futuro se podrá asignar un valor diferente, que podría afectar a la puntuación.

Cuadro 9 – Ponderación de la capa de privilegios necesarios

Valor	Código (Nota)	Peso	Descripción
No aplicable	NA	1,0	Se hace caso omiso de este factor en el cálculo de la puntuación, dado que no depende de cómo se establezca la prioridad de puntos débiles. Este factor quizá no sea aplicable en un contexto que exige garantías elevadas, en el que se desea aplicar estrictamente la separación de privilegios, incluso entre los usuarios que ya disponen de privilegios.
Cuantificado	Q		Este factor podría cuantificarse con ponderaciones personalizadas. Obsérvese que se admiten valores cuantificados en aras de la integridad; ahora bien, dado que las capas de privilegios son entidades discretas, en determinadas circunstancias resultaría útil disponer de un modelo cuantificado.
NOTA – Existe un acrónimo para los valores (en inglés) de este factor, a saber, "SANE" (S, A, N, E) (System, Application, Network, Enterprise Infrastructure).			

7.4.3 Vector de acceso (AV)

El vector de acceso identifica el canal a través del cual el atacante puede establecer la comunicación para llegar al código o funcionalidad donde se encuentra el punto débil. Obsérvese que estos valores son muy similares a los utilizados en CVSS, excepto en que el CWSS hace la diferencia entre el acceso físico y el local (intérprete de comandos/cuenta).

Si bien el vector de acceso y la capa de privilegios necesarios están relacionados, los dos factores son diferentes. Por ejemplo, el atacante con acceso "físico" a un encaminador podría ser capaz de afectar a la capa de red o de empresa.

Cuadro 10 – Ponderaciones del vector de acceso

Valor	Código	Peso	Descripción
Internet	I	1,0	El atacante debe disponer de acceso a Internet para llegar al punto débil.
Intranet	R	0,8	El atacante debe tener acceso a la intranet de la empresa que está protegida contra acceso directo desde Internet, mediante un cortafuegos por ejemplo, por el contrario la intranet es accesible por la mayoría de los miembros de la empresa.
Red privada	V	0,8	El atacante debe tener acceso a una red privada que sólo es accesible a un conjunto definido y reducido de partes fiables.
Red adyacente	A	0,7	El atacante debe tener acceso a una interfaz física de la red, como el dominio de difusión o de colisión del software vulnerable. Son ejemplos de redes locales las subredes del protocolo Internet (IP), Bluetooth, IEEE 802.11 y el segmento local Ethernet.
Local	L	0,5	El atacante debe disponer de una cuenta local interactiva (*shell* o intérprete de comandos) que actúe de interfaz directa con el sistema operativo subyacente.
Física	P	0,2	El atacante debe disponer de acceso físico al sistema en el que se ejecuta el software o, en su defecto, ser capaz de interactuar con el sistema por medio de interfaces tales como USB (bus serie universal), CD (compact disc), teclado, ratón, etc.
Por omisión	D	0,75	Promedio de ponderaciones de valores pertinentes.

Cuadro 10 – Ponderaciones del vector de acceso

Valor	Código	Peso	Descripción
Desconocido	U	0,5	
No aplicable	NA	1,0	Se hace caso omiso de este factor en el cálculo de la puntuación, dado que no depende de cómo se establezca la prioridad de puntos débiles.
Cuantificado	Q		Este factor podría cuantificarse con ponderaciones personalizadas. Obsérvese que se admiten valores cuantificados en aras de la integridad; ahora bien, dado que el vector de acceso es una entidad discreta, en determinadas circunstancias resultaría útil disponer de un modelo cuantificado.

7.4.4 Solidez de la autentificación (AS)

La solidez de la autentificación se refiere a la robustez de solidez de la rutina de autentificación que protege el código/funcionalidad donde se encuentra el punto débil.

Cuando se utilizan varias rutinas de autentificación o si existen dos o más trayectos de código, la puntuación puede realizarse del modo siguiente:

Cuando existen varias rutinas de autentificación o múltiples trayectos de código por los que se puede alcanzar el mismo punto débil, se aplica la siguiente guía:

- Para cada trayecto de código, se analiza cada rutina de autentificación que figura en el trayecto del código y se elige el valor con menor ponderación (es decir, la rutina de autentificación más robusta a lo largo del trayecto del código). Este valor se denomina Valor del Trayecto del Código.
- Se recopila todos los Valores de Trayecto del Código.
- Se selecciona el Valor de Trayecto del Código con mayor ponderación (es decir, el control más débil).

Este método evalúa cada trayecto del código en lo que respecta al control más sólido del trayecto del código (dado que el atacante tendrá que eludir dicho control), luego se selecciona el trayecto del código más débil (es decir, la ruta más fácil que pueda tomar el atacante).

Cuadro 11 – Ponderaciones de solidez de autentificación

Valor	Código	Peso	Descripción
Fuerte	S	0,7	El punto débil requiere los métodos más sólidos disponibles para vincular la entidad con una identidad del mundo real, como llave (token) hardware y/o autentificación multifactor.
Moderado	M	0,8	El punto débil requiere la autentificación utilizando métodos moderadamente robustos, como certificados de autoridades que no son de confianza, autentificación basada en conocimiento o contraseñas de un solo uso.
Débil	W	0,9	El punto débil requiere un método de autentificación simple y débil, que es fácil de eludir utilizando ataques de falsificación, diccionario o de repetición, como una contraseña estática.
Ninguno	N	1,0	El punto débil no requiere autentificación alguna.
Por omisión	D	0,85	Promedio de los valores de fuerte, moderado, débil y ninguno.

Cuadro 11 – Ponderaciones de solidez de autentificación

Valor	Código	Peso	Descripción
Desconocido	UK	0,5	No se dispone de información suficiente para asignar un valor a este factor. Es necesario profundizar en el análisis. En el futuro se podrá asignar un valor diferente, que podría afectar a la puntuación.
No Aplicable	NA	1,0	Se hace caso omiso de este factor en el cálculo de la puntuación, dado que no depende de cómo se establezca la prioridad de puntos débiles. Este factor quizá no sea aplicable en un contexto que exige garantías elevadas, donde se pretende eliminar todos los puntos débiles.
Cuantificado	Q		Este factor podría cuantificarse con ponderaciones personalizadas.

7.4.5 Nivel de interacción (IN)

El nivel de interacción se refiere a las acciones que debe realizar la víctima humana para que pueda darse un ataque exitoso.

Cuadro 12 – Ponderaciones del nivel de interacción

Valor	Código	Peso	Descripción
Automático	A	1,0	No se requiere la intervención humana.
Típico/ Limitado	T	0,9	El atacante debe convencer al usuario de realizar una acción habitual o considerada "normal" en el marco de una operación típica del producto. Por ejemplo, pulsar un enlace de una página web o previsualizar el cuerpo de un mensaje electrónico se considera un comportamiento habitual.
Moderado	M	0,8	El atacante debe convencer al usuario de realizar una acción que pudiera parecer sospechosa para un usuario prudente y experimentado. Por ejemplo: el usuario tiene que aceptar un aviso de que la carga útil del atacante puede tener contenido peligroso.
Oportunista	O	0,3	El atacante no puede controlar o influir directamente a la víctima y sólo puede aprovechar pasivamente los errores o acciones de otros.
Elevado	H	0,1	Se requiere muchísima ingeniería social, que aprovecha posiblemente la ignorancia o negligencia de la víctima.
Sin interacción	NI	0,0	No existe interacción posible, ni siquiera oportunista; en este caso el punto débil se convertiría en una "falla" en lugar de una vulnerabilidad. Como el objetivo del CWSS es la seguridad, la ponderación es 0.
Por omisión	D	0,55	Promedio de valores de automático, limitado, moderado, oportunista, elevado y sin interacción.
Desconocido	UK	0,5	No se dispone de información suficiente para asignar un valor a este factor. Es necesario profundizar en el análisis. En el futuro se podrá asignar un valor diferente, que podría afectar a la puntuación.

7.4.6 Alcance del despliegue (SC)

El alcance del despliegue identifica si el punto débil está presente en todas las instancias desplegables del software, o si se limita a un subconjunto de plataformas y/o configuraciones. Por ejemplo, un error de cálculo numérico podría ser únicamente aplicable a software que se ejecuta en un sistema operativo particular y una arquitectura de 64 bits o podría tratarse de un problema transversal del trayecto que sólo afecte a sistemas operativos en los que se utiliza "\" como separador de directorio.

Cuadro 13 – Ponderaciones del alcance del despliegue

Valor	Código (Nota)	Peso	Descripción
Todos	A	1,0	Presente en todas las plataformas y configuraciones
Moderado	M	0,9	Presente en plataformas o configuraciones comunes
Inusual	R	0,5	Sólo presente en plataformas o configuraciones inusuales
Potencialmente alcanzable	P	0,1	Potencialmente alcanzable (Nota 2), pero todos los trayectos del código son actualmente seguros y/o el punto débil está en un código sin usar
Por omisión	D	0,7	El promedio de las ponderaciones de los valores de RAMP
Desconocido	UK	0,5	No se dispone de información suficiente para asignar un valor a este factor. Es necesario profundizar en el análisis. En el futuro se podrá asignar un valor diferente, que podría afectar a la puntuación.
No aplicable	NA	1,0	Se hace caso omiso de este factor en el cálculo de la puntuación, dado que no depende de cómo se establezca la prioridad de puntos débiles.
Cuantificado	Q		Este factor podría cuantificarse con ponderaciones personalizadas. El usuario podría conocer qué porcentaje del software enviado (o soportado) contiene esta falla (bug).
NOTA 1 − Existe un acrónimo para los valores (en inglés) de este factor, a saber, "RAMP" (R, A, M, P) (Rare, All, Moderate, Potentially Reachable). NOTA 2 − "Potencialmente alcanzable" tiene ciertos aspectos en común con "Verdadero localmente" en el factor de confianza en el hallazgo (FC).			

7.5 Grupo métrico "contexto"

El grupo métrico "contexto" consta de los siguientes factores:

- Impacto empresarial (BI)
- Probabilidad de detección (DI)
- Probabilidad de explotación (EX)
- Eficacia del control externo (EC)
- Prevalencia (P).

7.5.1 Impacto en las actividades (BI)

El impacto en las actividades describe el posible impacto para las actividades o la misión si se consigue explotar el punto débil.

NOTA − Dado que cada organización tiene sus propias preocupaciones, con el CWSS 1.0 no se pretende hacer un desglose más exacto, por ejemplo, daños de tipo financiero, a la reputación, físico, jurídico o de otra índole. Este factor puede cuantificarse para tener en cuenta modelos definidos en el exterior.

Cuadro 14 – Ponderación del impacto empresarial

Valor	Código	Peso	Descripción
Crítico	C	1,0	Las actividades/misión podría fallar.
Elevado	H	0,9	Las operaciones relacionadas con las actividades/misión podrían verse considerablemente afectadas.
Medio	M	0,6	Las actividades/misión se verían afectadas, pero los daños no repercutirían en las operaciones ordinarias.
Bajo	L	0,3	Impacto mínimo en las actividades /misión.
Ninguno	N	0,0	Impacto nulo.
Por omisión	D	0,6	Promedio de las ponderaciones de crítico, elevado, medio, bajo y ninguno.
Desconocido	UK	0,5	No se dispone de información suficiente para asignar un valor a este factor. Es necesario profundizar en el análisis. En el futuro se podrá asignar un valor diferente, que podría afectar a la puntuación.
No aplicable	NA	1,0	Se hace caso omiso de este factor en el cálculo de la puntuación, dado que no depende de cómo se establezca la prioridad de puntos débiles. Este factor quizá no sea aplicable en contextos donde el impacto en las actividades es irrelevante o si el impacto analizado y examinado en los procesos analíticos queda fuera de la puntuación CWSS propiamente dicha.
Cuantificado	Q		Este factor podría cuantificarse con ponderaciones personalizadas. Algunas organizaciones podrían disponer de mediciones específicas para valorar los activos para las actividades, las cuales podrían integrarse en esta medición.

7.5.2 Probabilidad de detección (DI)

La probabilidad de detección es la probabilidad de que el atacante descubra el punto débil.

NOTA – En la versión CWSS 1.0 se consideró la posibilidad de eliminar este factor, dado que puede resultar difícil de medir y puede afectar a otros factores, tales como privilegios adquiridos, impacto técnico y prevalencia. Sin embargo, se ha preservado porque algunos diseñadores utilizan la probabilidad de detección para establecer la prioridad y determinar con qué rapidez se debe resolver un problema.

Cuadro 15 – Ponderación de la probabilidad de detección

Valor	Código	Peso	Descripción
Elevado	H	1,0	Es muy probable que el atacante pueda descubrir el punto débil rápidamente y con poco esfuerzo, utilizando para ello técnicas sencillas, sin acceso al código fuente u otros artefactos que simplifican la detección de puntos débiles.
Medio	M	0,6	El atacante puede ser capaz de descubrir el punto débil, pero necesita ciertas habilidades para ello, posiblemente acceso al código fuente o conocimientos de ingeniería inversa. Puede requerirse cierto tiempo para hallar el problema.
Bajo	L	0,2	Es improbable que el atacante descubra el punto débil si no tiene conocimientos muy especializados, dispone de acceso al código fuente (o su equivalente) e invierte mucho tiempo.
Por omisión	D	0,6	Promedio de los valores de elevado, medio, bajo.

Cuadro 15 – Ponderación de la probabilidad de detección

Valor	Código	Peso	Descripción
Desconocido	UK	0,5	No se dispone de información suficiente para asignar un valor a este factor. Es necesario profundizar en el análisis. En el futuro se podrá asignar un valor diferente, que podría afectar a la puntuación.
No aplicable	NA	1,0	Se hace caso omiso de este factor en el cálculo de la puntuación, dado que no depende de cómo se establezca la prioridad de puntos débiles. Este factor podría no ser aplicable si se parte del supuesto de que el atacante descubrirá todos los puntos débiles.
Cuantificado	Q		Este factor podría cuantificarse con ponderaciones personalizadas.

7.5.3 Probabilidad de explotación (EX)

La probabilidad de explotación es la probabilidad de que, si se detecta un punto débil, un atacante con privilegios/autentificación/acceso pueda explotarlo.

Cuadro 16 – Ponderación de la probabilidad de explotación

Valor	Código	Peso	Descripción
Elevado	H	1,0	Es altamente probable que el atacante explote este punto débil con éxito, con un artilugio fiable y fácil de crear.
Medio	M	0,6	El atacante puede probablemente explotar este punto débil, pero la probabilidad de éxito puede variar y tendrá que hacer varios intentos para conseguirlo.
Bajo	L	0,2	El atacante no podrá probablemente explotar este punto débil o la probabilidad de que lo consiga es muy pequeña.
Ninguno	N	0,0	El atacante no tiene ninguna probabilidad de éxito; es decir, el problema es una "falla", por cuanto el atacante no puede hacer nada ni aprovecharlo en modo alguno.
Por omisión	D	0,6	Promedio de los valores de elevado, medio y bajo. El valor "Ninguno" no se tiene en cuenta, puesto que cabe esperar que muy pocas de los puntos débiles hallados se puntuarán utilizando este valor, e incluirlo en el cálculo del promedio reduciría la ponderación a un nivel no intuitivo.
Desconocido	UK	0,5	No se dispone de información suficiente para asignar un valor a este factor. Es necesario profundizar en el análisis. En el futuro se podrá asignar un valor diferente, que podría afectar a la puntuación.
No aplicable	NA	1,0	Se hace caso omiso de este factor en el cálculo de la puntuación, dado que no depende de cómo se establezca la prioridad de puntos débiles. Por ejemplo, al ponderar quizá se pueda suponer que los atacantes podrían explotar todos los puntos débiles que encuentren o que están dispuestos a invertir recursos considerables para eliminar todos los posibles obstáculos que le impidan explotarlos.
Cuantificado	Q		Este factor podría cuantificarse con ponderaciones personalizadas.

Obsérvese que este factor se ve afectado por el impacto de un punto débil, dado que los atacantes suelen concentrarse en puntos débiles cuyo impacto es más grave. Otra posibilidad es que ataquen puntos débiles que son fáciles de explotar. También puede verse afectado por otros factores, tales como la eficacia de los controles interno y externo.

Podría parecer que el factor prevalencia también podría influir, pero éste guarda más relación con la probabilidad de detección.

7.5.4 Eficacia del control externo (EC)

La eficacia del control externo es la capacidad de controlar o mitigar la exposición externa del software de modo que resulte más difícil a un atacante alcanzar y/o explotar el punto débil. Por ejemplo, tecnologías tales como la ASLR (aleatorización del espacio de direcciones) reducen, pero no eliminan, la probabilidad de que se produzca un ataque por desbordamiento de memoria. Ahora bien, la ASLR no está directamente integrada en el propio software.

Cuando hay múltiples controles externos o múltiples trayectos del código que llevan hacia el mismo punto débil, se aplica la siguiente guía:

- Para cada trayecto del código, se analiza cada control externo que figura a lo largo del trayecto del código y se selecciona el valor con menor ponderación (es decir, el control externo más robusto a lo largo del trayecto del código). Este valor se denomina valor del trayecto del código.
- Se recopila todos los valores de trayecto del código.
- Se selecciona el valor de trayecto del código con mayor ponderación (es decir, el control más débil).

Este método evalúa cada trayecto del código en lo que respecta al control más sólido del trayecto del código (dado que el atacante tendrá que eludir dicho control), luego se selecciona el trayecto del código más débil (es decir, la ruta más fácil que pueda tomar el atacante).

Cuadro 17 – Ponderación de la eficacia del control externo

Valor	Código	Peso	Descripción
Ninguno	N	1,0	No hay control alguno.
Limitado	L	0,9	Existen métodos sencillos o restricciones casuales que podrían impedir a un atacante ocasional explotar el punto débil.
Moderado	M	0,7	El mecanismo de protección se utiliza normalmente, pero tiene limitaciones conocidas que podría eludir con cierto esfuerzo un atacante experimentado.
Indirecto (Defensa en profundidad)	I	0,5	El control no protege específicamente contra la explotación del punto débil, pero reduce de manera indirecta su impacto cuando se lanza con éxito un ataque, o dificulta la construcción de un artilugio (*exploit*) funcional. Por ejemplo, tecnologías tales como la ASLR (aleatorización del espacio de direcciones) reducen, pero no eliminan, la probabilidad de que se produzca un ataque por desbordamiento de memoria. Dado que la respuesta es normalmente salir del proceso, el resultado sigue siendo una denegación del servicio.
El mejor disponible	B	0,3	El control sigue las prácticas más idóneas, aunque pudieran existir ciertas limitaciones que podría superar un atacante hábil y resuelto, posiblemente aprovechando también otros puntos débiles. Por ejemplo, la seguridad en la capa de transporte (TLS) / capa de conexión segura (SSL 3) se mantienen activas en gran parte de la web, pero en general no se dispone de métodos más robustos debido a cuestiones de compatibilidad.

Cuadro 17 – Ponderación de la eficacia del control externo

Valor	Código	Peso	Descripción
Completo	C	0,1	El control es totalmente eficaz respecto del punto débil, es decir, no hay falla o vulnerabilidad y la explotación de este problema no tiene consecuencias negativas. Por ejemplo, un espacio acotado (*sandbox*) puede limitar las operaciones de acceso a ficheros a un solo directorio de trabajo, lo que protegería contra la explotación de traspaso de directorio. Se emplea una ponderación distinta de cero para indicar la posibilidad de que el control externo pueda suprimirse por accidente en el futuro, es decir, si se modifica el contexto del 'software'.
Por omisión	D	0,6	Promedio de las ponderaciones de Completo, el Mejor disponible, Indirecto, Moderado, Limitado y Ninguno.
Desconocido	UK	0,5	No se dispone de información suficiente para asignar un valor a este factor. Es necesario profundizar en el análisis. En el futuro se podrá asignar un valor diferente, que podría afectar a la puntuación.
No aplicable	NA	1,0	Se hace caso omiso de este factor de manera deliberada al calcular la puntuación dado que no depende de cómo se establezca la prioridad de puntos débiles.
Cuantificado	Q		Este factor podría cuantificarse con ponderaciones personalizadas.

7.5.5 Prevalencia (P)

La prevalencia de un hallazgo indica la frecuencia con la que aparece este tipo de punto débil en el software.

NOTA – Obsérvese que este factor podría suprimirse en futuras versiones. No obstante, guarda una relación demasiado estrecha con los métodos de puntuación generalizados y el CWRAF como para suprimirse en esta versión CWSS 1.0.

Este factor se ha concebido para utilizarse en puntuación generalizada de clases de puntos débiles, tales como el desarrollo de una lista personalizada de los N principales puntos débiles. Cuando se puntúa un determinado punto débil hallado en un contexto de análisis automático, es probable que el valor de este factor sea "No aplicable".

Cuadro 18 – Ponderación de prevalencia

Valor	Código	Peso (Nota)	Descripción
Generalizado	W	1,0	El punto débil se halla en la mayoría o todo el software en el entorno considerado y puede aparecer varias veces en el mismo paquete de software.
Elevado	H	0,9	El punto débil se halla muy a menudo, pero no está generalizado.
Común	C	0,8	El punto débil se halla periódicamente.
Limitado	L	0,7	El punto débil se halla raramente o nunca.
Default	D	0,85	Promedio de limitado, común, elevado y generalizado.
Desconocido	UK	0,5	No se dispone de información suficiente para asignar un valor a este factor. Es necesario profundizar en el análisis. En el futuro se podrá asignar un valor diferente, que podría afectar a la puntuación.

Cuadro 18 – Ponderación de prevalencia

Valor	Código	Peso (Nota)	Descripción
No aplicable	NA	1,0	Se hace caso omiso de este factor de manera deliberada al calcular la puntuación dado que no depende de cómo se establezca la prioridad de puntos débiles. Cuando se efectúa una puntuación específica de un determinado punto débil hallado en una aplicación, cabe esperar que la prevalencia sea irrelevante, por cuanto la aplicación en concreto y las técnicas analíticas determinan con cuánta frecuencia aparece el punto débil y muchos métodos de puntuación combinados generarán puntuaciones más altas si existen más puntos débiles.
Cuantificado	Q		Este factor podría cuantificarse con ponderaciones personalizadas. En algunos casos se podría disponer de datos exactos de la prevalencia, siempre y cuando el usuario busque datos de puntos débiles a un nivel inferior de granularidad. Por ejemplo, un diseñador puede buscar puntos débiles en una serie de productos o un fabricante de sistemas de auditoría de código podría medir la prevalencia a partir del software analizado en toda su clientela. En una versión anterior del CWSS, la prevalencia se calculaba a partir de los datos de votación en bruto recabados de la lista de los 25 primeros de 2010, en la que se utilizaban valores discretos (de 1 a 4) que luego se ajustaban a la gama de 1 a 10.
NOTA − Dado que el software puede ser víctima de un ataque con éxito aunque sólo tenga un punto débil, las ponderaciones seleccionadas no ofrecen una diferencia considerable entre cada uno.			

7.6 Fórmula de puntuación del CWSS

La puntuación en el CWSS 1.0 oscila entre 0 y 100. Se calcula de la siguiente manera:

```
SubpuntuaciónHallazgoBase * SubpuntuaciónSuperficieAtaque *
SubpuntuaciónContenxto
```

Los valores SubpuntuaciónHallazgoBase oscilan entre 0 y 100. Los valores de SubpuntuaciónSuperficieAtaque y SubpuntuaciónContexto oscilan entre 0 y 1.

7.6.1 Subpuntuación de hallazgo básico

La subpuntuación de hallazgo de base (SubpuntuaciónHallazgoBásico) se calcula del modo siguiente:

```
Base = [ (10 * ImpactoTécnico + 5*(PrivilegioAdquirido + CapaPrivilegioAdquirido)
+ 5*ConfianzaHallazgo) * f(ImpactoTécnico) * EficaciaControlInterno ] * 4,0
```

```
f(ImpactoTécnico) = 0 si ImpactoTécnico = 0;
de lo contrario f(ImpactoTécnico) = 1.
```

El valor máximo posible de la SubpuntuaciónHallazgoBásico es 100.

La definición de f(ImpactoTécnico) es equivalente a la del CVSS. Se utiliza para garantizar que si el Impacto Técnico es 0, los otros factores no generarán inadvertidamente una puntuación distinta de cero.

El ImpactoTécnico y la combinación PrivilegioAdquirido/CapaPrivilegioAdquirido pesan lo mismo, representando cada una un 40% de la SubpuntuaciónHallazgoBásico. (Cada uno genera un subvalor de valor máximo igual a 10). Se efectúa un ajuste en función de la confianza en el hallazgo básico, que representa el 20% de la Base (máximo de 5). La EficaciaControlInterno puede ajustar a la baja la puntuación, hasta 0, dependiendo de la solidez de los controles internos que se hayan aplicado a este asunto. Tras la aplicación de la EficaciaControlInterno, la gama de posibles resultados oscila entre 0 y 25, por lo que se recurre a un coeficiente de 4,0 para ajustar la SubpuntuaciónHallazgoBásico a valores entre 0 y 100.

7.6.2 Subpuntuación de superficie de ataque

La SubpuntuaciónSuperficieAtaque se calcula del modo siguiente:

```
[ 20*(PrivilegioNecesario + CapaPrivilegioNecesario + VectorAcceso) + 20*AlcanceDespliegue + 15*NivelInteracción + 5*SolidezAutentificación ] / 100,0
```

La combinación de privilegios necesarios/ acceso representa el 60% de la subpuntuación de superficie de ataque; el alcance del despliegue, otro 20%; la interacción, 15%; y la autentificación, 5%. No se confiere mucha importancia a los requisitos de autentificación, por cuanto se supone que exigir una prueba sólida de identidad no disuadirá considerablemente al atacante de tratar de explotar la vulnerabilidad.

Se obtiene un valor comprendido entre 0 y 100, que luego se divide por 100.

7.6.3 Subpuntuación de contexto

La SubpuntuaciónContexto se calcula del modo siguiente:

```
[ (10*ImpactoActividades + 3*ProbabilidadDetección + 4*ProbabilidadExplotacióin + 3*Prevalencia) * f(ImpactoActividades) * EficaciaControlExterno ] / 20,0
```

```
f(ImpactoActividades) = 0 si ImpactoActividades == 0; de lo contrario f(ImpactoActividades) = 1
```

El ImpactoActividades representa el 50% de la puntuación del contexto y puede generar una puntuación final igual a 0. El factor EficaciaControlExterno siempre es distinto de cero (para tener en cuenta el riesgo de que pueda suprimirse inadvertidamente si el contexto), pero puede repercutir considerablemente en el resultado final. La combinación de ProbabilidadDetección y ProbabilidadExplotación representa el 35% de la puntuación y la prevalencia un 15%.

7.6.4 Otras características de la fórmula

Se podrían representar muy diversos tipos de puntuaciones, pero el hecho de multiplicar muchos factores diferentes, junto con varios coeficientes de ponderación de valores reducidos, hará que la gama de posibles puntuaciones acuse una tendencia hacia valores más pequeños.

Dado que los valores "No aplicable" tienen un peso o ponderación igual a 1, la fórmula siempre tiene una puntuación máxima posible de 100,0. En casos extremadamente raros en los que ciertos factores se consideran no aplicables (por ejemplo, impacto técnico, impacto en las actividades y eficacia del control interno), la puntuación mínima posible podría ser distinta de cero.

Cuando se emplean valores por omisión en numerosos factores para una misma puntuación, utilizando ponderaciones promediadas como se define en CWSS 1.0, las puntuaciones acusarán una fuerte tendencia hacia valores pequeños. La ponderación promediada para un factor no responde necesariamente al valor más probable que podría utilizarse, de modo que la selección de las ponderaciones promediadas podría variar en futuras versiones. Lo ideal sería que la formula tuviera la propiedad de que la utilización de muchos valores por omisión produjera una puntuación relativamente cercana a 50; la selección de valores distintos a los valores por omisión modificará la puntuación final al alza o a la baja, obteniéndose así mayor precisión.

La utilización de valores "desconocidos" también hace que las puntuaciones obtenidas tiendan hacia valores bajos. Esta característica podría ser útil, puesto que la puntuación será mayor cuanto más información específica haya.

7.7 Vectores CWSS, ejemplos de puntuación y portabilidad de la puntuación

La utilización de códigos especificados para cada factor permite almacenar la puntuación CWSS en un formato compacto, analizable automáticamente y legible por personas que contenga información sobre cómo se generó la puntuación. Este formato es muy similar a la forma en que se construyen los vectores CVSS.

A diferencia del CVSS, no todos los factores CWSS pueden describirse simbólicamente mediante valores discretos. Todo factor puede cuantificarse con ponderaciones continuas que sustituyen a los valores discretos por omisión definidos inicialmente, utilizando el valor "Q". Cuando se calcula utilizando CWRAF, el factor impacto expresa efectivamente 32 impactos técnicos y capas diferentes, muchos de los cuales podrían no ser aplicables a un determinado punto débil. Al considerar cada impacto como un factor diferente se requeriría más o menos el doble de factores de los necesarios para calcular una puntuación CWSS. Por otra parte, la utilización en el CWRAF del contexto del valor de las actividades (BVC) para adaptar las puntuaciones a las preocupaciones específicas de cada actividad implica además que la puntuación CWSS y su vector puede resultar incoherente si se "transportan" a otros dominios o viñetas.

Habida cuenta de lo anterior, el vector CWSS 1.0 debería enumerar explícitamente el peso o ponderación de cada factor, aunque se aumente así el tamaño de la representación del vector.

El formato de un solo factor en el vector CWSS es el siguiente:

NombreFactor: Valor, Peso

Por ejemplo, `"P:NA,1.0"` indica un valor "No aplicable" para la prevalencia con una ponderación de 1.0. Así `"AV:P,0.2"` significa un valor "físico" para el vector de acceso con una ponderación de 0,2.

Los factores se separan con el carácter barra, por ejemplo:

```
AV:I,1.0/RP:G,0.9/AS:N,1.0
```

Expresión que enumera los valores y ponderación para el factor "AV" (vector de acceso), "RP" (nivel de privilegios necesario) y "AS" (solidez de la autentificación).

Si se facilita un CWSS sin la ponderación real de un valor, la implementación debería informar de un error o incoherencia, tratar de deducir la versión CWSS basada en los factores del vector y sus valores, recalcular la puntuación CWSS de acuerdo con la versión deducida y compararla con la puntuación original. Si las puntuaciones son incoherentes, la implementación debería notificar un posible error o incoherencia.

7.7.1 Ejemplo: aplicación esencial para las actividades

Supóngase que se informa de un punto débil en una aplicación que es la principal fuente de ingresos de una empresa y que, por ende, tiene un valor esencial para sus actividades. La aplicación permite a cualquier usuario de Internet crear una cuenta utilizando solamente una dirección de correo electrónico. El usuario puede explotar este punto débil para obtener privilegios de administrador en dicha aplicación, pero el ataque no puede tener éxito hasta que el administrador consulte un informe de las actividades de los usuarios recientes – algo bastante corriente. El atacante no puede tomar el control total de la aplicación, pero puede borrar usuarios y datos. Supóngase además que no hay controles que impidan explotar el punto débil, pero que para resolver el problema basta con unas líneas de código.

La situación podría representarse en el siguiente vector CWSS:

```
(TI:H,0.9/AP:A,1.0/AL:A,1.0/IC:N,1.0/FC:T,1.0/
RP:G,0.9/RL:A,1.0/AV:I,1.0/AS:N,1.0/IN:T,0.9/SC:A,1.0/
BI:C/0.9,DI:H,1.0/EX:H,1.0/EC:N,1.0/P:NA,1.0)
```

El vector se ha separado en varias líneas para facilitar su lectura. Cada línea representa un grupo métrico.

En el Cuadro 19 se indican los vectores y sus valores.

Cuadro 19 – Factores y valores para el ejemplo de aplicación esencial para las actividades

Factor	Valor
Impacto técnico	Elevado
Privilegio adquirido	Administrador
Capa de privilegio adquirido	Aplicación
Eficacia del control interno	Ninguna
Confianza en el hallazgo	Veracidad probada
Privilegios necesarios	Invitado
Capa de privilegios necesarios	Aplicación
Vector de acceso	Internet
Solidez de la autentificación	Ninguna
Nivel de interacción	Típico/Limitado
Alcance del despliegue	Todo
Impacto en las actividades	Crítico
Probabilidad de detección	Elevada
Probabilidad de explotación	Elevada
Eficacia del control externo	Ninguna
Prevalencia	No aplicable

La puntuación CWSS para este vector es 92,6, calculada del modo siguiente:

- SubpuntuaciónBásica:
  - `[ (10 * TI + 5*(AP + AL) + 5*FC) * f(TI) * IC ] * 4,0`
  - `f(TI) = 1`
  - `= [ (10 * 0,9 + 5*(1,0 + 1,0) + 5*1,0) * 1 * 1,0 ] * 4,0`
  - `= [ (9,0 + 10,0 + 5,0) * 1,0 ] * 4,0`
  - `= 24,0 * 4,0`
  - `= 96,0`
- SubpuntuaciónSuperficieAtaque:
  - `[ 20*(RP + RL + AV) + 20*SC + 15*IN + 5*AS ] / 100,0`
  - `= [ 20*(0,9 + 1,0 + 1,0) + 20*1,0 + 15*0,9 + 5*1,0 ] / 100,0`
  - `= [ 58,0 + 20,0 + 13,5 + 5,0 ] / 100,0`
  - `= 96,5 / 100,0`
  - `= 0,965`

- SubpuntuaciónContexto:
  - `[ (10*BI + 3*DI + 4*EX + 3*P) * f(BI) * EC ] / 20,0`
  - `f(BI) = 1`
  - `= [ (10*1,0 + 3*1,0 + 4*1,0 + 3*1,0) * 1 * 1,0 ] / 20,0`
  - `= [ (10,0 + 3.0 + 4,0 + 3,0) * 1,0 ] / 20,0`
  - `= 20,0 / 20,0`
  - `= 1,0`

La puntuación final es:

`96,0 * 0,965 * 1,0 = 92,64 == 92,6`

7.7.2 Ejemplo: Wiki no esencial para las actividades de la empresa

Considérese el siguiente vector CWSS. Se trata de un software wiki utilizado para seguir eventos sociales de una empresa mediana. Algunas de las características más importantes es el impacto técnico de que un usuario ordinario adquiera derechos de administración para la aplicación la aplicación. Como la aplicación no es esencial para las actividades de la empresa, el impacto general también es reducido. Obsérvese que el valor de la mayoría de los factores contextuales es "No aplicable".

`(TI:M,0,6/AP:A,1,0/AL:A,1,0/IC:N,1,0/FC:T,1,0/`

`RP:RU,0,7/RL:A,1,0/AV:I,1,0/AS:W,0,9/IN:A,1,0/SC:NA,1,0/`

`BI:L/0,3,DI:NA,1,0/EX:NA,1,0/EC:N,1,0/RE:NA,1,0/P:NA,1,0)`

El vector se ha separado en varias líneas para facilitar su lectura. Cada línea representa un grupo métrico.

En el Cuadro 20 se indican los vectores y sus valores.

Cuadro 20 – Factores y valores para el ejemplo de aplicación no esencial para las actividades

Factor	Valor
Impacto técnico	Medio
Privilegio adquirido	Administrador
Capa de privilegio adquirido	Aplicación
Eficacia del control interno	Ninguna
Confianza en el hallazgo	Veracidad probada
Privilegios necesarios	Usuario ordinario
Capa de privilegios necesarios	Aplicación
Vector de acceso	Internet
Solidez de la autentificación	Débil
Nivel de interacción	Automático
Alcance del despliegue	No aplicable
Impacto en las actividades	Pequeño
Probabilidad de detección	No aplicable
Probabilidad de explotación	No aplicable
Eficacia del control externo	Ninguna
Prevalencia	No aplicable

La puntuación CWSS para este vector es 51,1, calculada del modo siguiente:

- SubpuntuaciónBásica:
  - `[ (10 * TI + 5*(AP + AL) + 5*FC) * f(TI) * IC ] * 4,0`
  - `f(TI) = 1`
  - `= [ (10 * 0,6 + 5*(1 + 1) + 5*1) * f(TI) * 1 ] * 4,0`
  - `= 84,0`
- SubpuntuaciónSuperficieAtaque:
  - `[ 20*(RP + RL + AV) + 20*SC + 15*IN + 5*AS ] / 100,0`
  - `= [ 20*(0,7 + 1 + 1) + 20*1,0 + 15*1,0 + 5*0,9 ] / 100,0`
  - `= [ 54,0 + 20,0 + 15,0 + 4,5 ] / 100,0`
  - `= 93,5 / 100,0`
  - `= 0,94 (0,935)`
- SubpuntuaciónContexto:
  - `[ (10*BI + 3*DI + 4*EX + 3*P) * f(BI) * EC ] / 20,0`
  - `f(BI) = 1`
  - `= [ (10*0,3 + 3*1,0 + 4*1,0 + 3*1,0) * f(BI) * 1 ] / 20,0`
  - `= [ (3,0 + 3,0 + 4,0 + 3,0) * 1,0 * 1,0 ] / 20,0`
  - `= [ 13,0 * 1,0 ] / 20,0`
  - `= 0,65.`

La puntuación final es:

`84,0 * 0,935 * 0,65 = 51,051 == 51,1`

7.7.3 Otros métodos para la portabilidad de la puntuación CWSS

En lugar de registrar cada ponderación mediante un vector CWSS, podrían adoptarse otros métodos.

Una posibilidad sería incluir metadatos en los vectores CWSS para indicar la versión u otra información importante sin afectar a la puntuación. Los metadatos no tienen necesariamente que indicar las ponderaciones. Por ejemplo, la versión del CWSS podría registrarse mediante un "factor" denominado "V" junto con un valor que represente la versión del CWSS, por ejemplo "V:1.1". El tamaño del vector CWSS aumentaría en 4 bytes aproximadamente. Ahora bien, si la versión se codifica dentro del vector, deja de ser necesario registrar las ponderaciones asignadas (salvo para los valores cuantificados), por lo que los vectores resultantes podrían ser mucho más cortos.

Otro método diferente sería adjuntar metadatos a un conjunto de puntuaciones CWSS generadas (como la tarjeta de puntuación del impacto técnico, si se utiliza el CWRAF), pero estos metadatos podrían desvincularse demasiado fácilmente de sus puntuaciones/vectores. Por otra parte, seguirá siendo necesario representar los factores cuantificados en un vector, dado que podrían varias para cada punto débil hallado.

Otro método consiste en transferir las puntuaciones CWSS de una parte a otra y que la parte receptora vuelva a calcular las puntuaciones partiendo de los vectores CWSS recibidos y compare las puntaciones recalculadas con las originales. Una diferencia entre las puntuaciones indicaría que el proveedor y el receptor utilizan mecanismos distintos, por ejemplo una versión del CWSS diferente.

Bibliografía

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

[b-UIT-T X.1520] Recomendación UIT-T X.1520 (2014), *Vulnerabilidades y exposiciones comunes*.

[b-UIT-T X.1521] Recomendación UIT-T X.1521 (2011), *Sistema común de puntuación de vulnerabilidades*.

[b-UIT-T X.1524] Recomendación UIT-T X.1524 (2012), *Lista de puntos débiles comunes*.

[b-UIT-T X.1544] Recomendación UIT-T X.1544 (2013), *Enumeración y clasificación de pautas de ataques comunes*.

[b-CWRAF] Common Weakness Risk Analysis Framework, http://cwe.mitre.org/cwraf/.

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, 2020