Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1521

(04/2011)

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

Intercambio de información de ciberseguridad – Intercambio de estados/vulnerabilidad

---

Sistema común de puntuación de vulnerabilidades

Recomendación UIT-T X.1521

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

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

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

Recomendación UIT-T X.1521

Sistema común de puntuación de vulnerabilidades

Resumen

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

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio
1.0	ITU-T X.1521	2011-04-20	17

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 2012

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 esta Recomendación	1
4	Abreviaturas y acrónimos	2
5	Convenios	2
6	Utilización de CVSS	3
6.1	Descripción del CVSS	3
6.2	Funcionamiento del CVSS	4
6.3	¿Quién realiza la puntuación?	4
6.4	¿Quién utiliza el CVSS?	4
6.5	Grupos de métricas: métricas base	5
6.6	Métricas temporales	9
6.7	Métricas relacionadas con el entorno	11
6.8	Vectores básico, temporal y del entorno	13
6.9	Directrices para realizar la puntuación	14
6.10	Ecuaciones	15
7	Recursos adicionales	17
Apéndice I – Ejemplos de uso de CVSS		18
I.1	CVE-2002-0392	18
I.2	CVE-2003-0818	19
I.3	CVE-2003-0062	21
Apéndice II – Recursos adicionales		23
Bibliografía		24

Introducción

Sin el CVSS, los gestores de las TIC se enfrentan a identificar y evaluar vulnerabilidades en numerosas plataformas hardware y software diferentes. A continuación, deben priorizar las vulnerabilidades y remediar las que conlleven mayores riesgos. Cuando son muchas las correcciones de software necesarias, y cada una se valora mediante una escala diferente, los gestores de las TIC sólo pueden utilizar metodologías propias para, de alguna forma, comparar las distintas vulnerabilidades y, a partir de dicha información, tomar las medidas oportunas.

Puesto que el CVSS normaliza el enfoque para la caracterización de vulnerabilidades, los usuarios del CVSS pueden invocar métricas temporales y dependientes del entorno para aplicar la información contextual que refleje con la mayor exactitud el riesgo para sus entornos específicos. Ello les permite tomar decisiones mejor informadas para intentar mitigar riesgos de vulnerabilidades independientes del suministrador y en el contexto de su entorno específico.

Esta Recomendación es técnicamente equivalente y compatible con el documento "Common Vulnerability Scoring System (CVSS) version 2", 20 de junio de 2007 que puede encontrarse en el sitio web: http://www.first.org/cvss.

Recomendación UIT-T X.1521

Sistema común de puntuación de vulnerabilidades

1 Alcance

Esta Recomendación proporciona un enfoque normalizado para la comunicación de características e impactos de vulnerabilidades de las tecnologías de la información y las comunicaciones (TIC) utilizando métricas temporales y del entorno que aplican información contextual para reflejar con la mayor exactitud el riesgo que dichas vulnerabilidades suponen para el entorno específico de cada usuario.

Esta Recomendación es técnicamente equivalente y compatible con el documento "Common Vulnerability Scoring System (CVSS) version 2", 20 de junio de 2007 que puede encontrarse en el sitio web http://www.first.org/cvss.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de esta Recomendación. A la fecha de esta publicación, las ediciones citadas están en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios a que estudien la posibilidad de utilizar 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 actualmente en vigor. En la presente Recomendación, la referencia a un documento no confiere a este último, como documento autónomo, la categoría de una Recomendación.

[CVSS Guide] CVSS (2007), *A complete Guide to the Common Vulnerability Scoring System Version 2.0*.
<http://www.first.org/cvss/cvss-guide.pdf>

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los términos siguientes:

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

3.2.2 disponibilidad: Acceso fiable y oportuno en el tiempo a datos y recursos realizado por individuos autorizados.

3.2.3 confidencialidad: Principio de seguridad destinado a asegurar que la información no se pone a disposición de sujetos no autorizados.

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

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

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

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las abreviaturas y acrónimos siguientes:

A Impacto en la disponibilidad (*availability impact*)

AC Complejidad del acceso (*access complexity*)

AR Requisito de disponibilidad (*availability requirement*)

Au Autentificación (*authentication*)

AV Vector de acceso (*access vector*)

C Impacto en la confidencialidad (*confidentiality impact*)

CDP Potencial daño colateral (*collateral damage potential*)

CR Requisito de confidencialidad (*confidentiality requirement*)

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

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

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

E Impacto en la explotabilidad (*exploitability impact*)

I Impacto en la integridad (*integrity impact*)

IM Mensajería instantánea (*instant messaging*)

IR Requisito de integridad (*integrity requirement*)

JVN Notas de vulnerabilidades de Japón (*Japan Vulnerability Notes*)

NVD Base de datos nacional de vulnerabilidades (*national vulnerability database*)

RC Confianza de la información (*report confidence*)

RL Nivel de remedio (*remediation level*)

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

SLA Acuerdo de nivel de servicio (*service level agreement*)

TD Distribución del objetivo (*target distribution*)

TIC Tecnologías de la información y las comunicaciones

USB Bus universal serie (*universal serial bus*)

5 Convenios

Ninguno.

6 Utilización de CVSS

Actualmente, los gestores de las TIC tienen que identificar y evaluar las vulnerabilidades en numerosas plataformas hardware y software diferentes. Necesitan priorizar dichas vulnerabilidades y encontrar soluciones para las que conllevan los mayores riesgos. Cuando son muchas las correcciones de software necesarias, y cada una se valora mediante una escala diferente, resulta difíciles para los gestores de las TIC convertir tal cantidad de datos sobre vulnerabilidades en información útil para tomar las medidas oportunas. El sistema común de puntuación de vulnerabilidades (CVSS) es un marco abierto que permite abordar este asunto. Ofrece los beneficios siguientes:

- Puntuaciones normalizadas de vulnerabilidades: cuando una organización normaliza las puntuaciones de vulnerabilidades de sus plataformas hardware y software, puede aprovechar las ventajas de una política única de gestión de vulnerabilidades. Dicha política puede ser similar a un acuerdo de nivel de servicio que establezca la rapidez con que una vulnerabilidad concreta debe ser validada y remediada.
- Marco abierto: la asignación de una puntuación de valoración arbitraria a una vulnerabilidad puede confundir a los usuarios. "¿En virtud de qué se le asignó dicha puntuación? ¿Cuál es la diferencia respecto a la que se publicó ayer?". Mediante el CVSS, cualquiera puede conocer las características individuales utilizadas para obtener una puntuación.
- Riesgo priorizado: cuando se calcula la puntuación de valoración relacionada con el entorno, se pone en contexto la vulnerabilidad. Es decir, las puntuaciones de las vulnerabilidades pasan a ser representativas del riesgo real para una organización. Los usuarios conocen cuán importante es una vulnerabilidad en relación con otras vulnerabilidades.

6.1 Descripción del CVSS

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

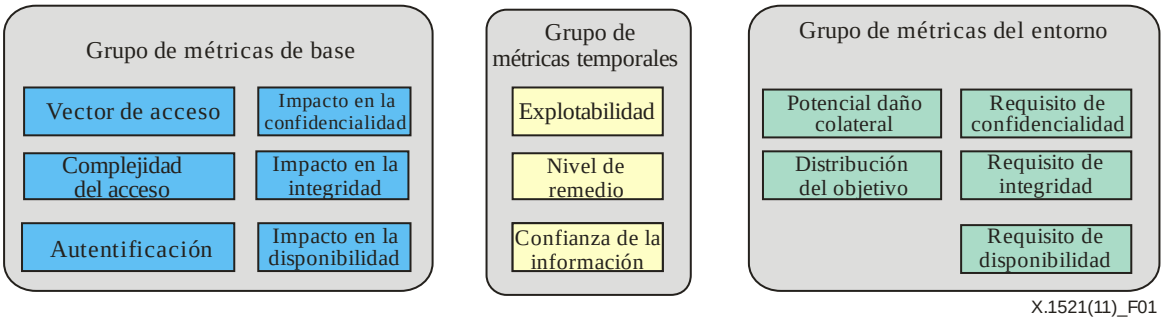

Figura 1 – Grupos de métricas del CVSS

Los grupos de métricas se describen de la forma siguiente:

- Base: representa las características intrínsecas y fundamentales de una vulnerabilidad que son constantes a lo largo del tiempo y en los distintos entornos de usuario. Las métricas base se analizan en 6.5.
- Temporal: representa las características de una vulnerabilidad que cambian con el tiempo, pero no en función del entorno de usuario. Las métricas temporales se analizan en 6.6.
- Del entorno: representa las características de una vulnerabilidad que son relevantes y singulares para un entorno de usuario determinado. Las métricas del entorno se analizan en 6.7.

El objetivo del grupo de métricas base del CVSS es definir y comunicar las características esenciales de una vulnerabilidad. Este enfoque objetivo para la caracterización de vulnerabilidades proporciona a los usuarios una representación clara e intuitiva de una vulnerabilidad. Los usuarios pueden entonces invocar los grupos de métricas temporales y del entorno para obtener información de contexto que refleje más exactamente el riesgo para su entorno específico. Ello les permite tomar decisiones mejor informadas cuando tratan de mitigar los riesgos de las vulnerabilidades.

6.2 Funcionamiento del CVSS

Cuando las métricas base son valores asignados, la ecuación base calcula un rango de valores de puntuación entre 0 y 10 y se crea un vector, tal como se muestra en la figura 2. El vector facilita la naturaleza "abierta" del marco. Es una cadena de texto que contiene los valores asignados a cada métrica y se utiliza para indicar con exactitud cómo se obtiene la puntuación de cada vulnerabilidad. Por tanto, el vector debería mostrarse siempre con la puntuación de vulnerabilidad. Los vectores se explican con más detalle en 7.4.

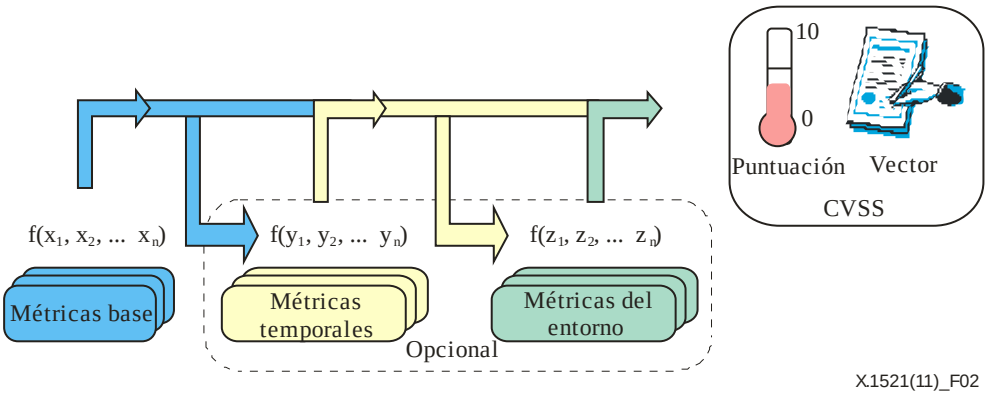

Figura 2 – Métricas y ecuaciones del CVSS

Opcionalmente, la puntuación base puede refinarse mediante la asignación de valores a las métricas temporal y de entorno. Ello es de utilidad para proporcionar información de contexto adicional sobre una vulnerabilidad, al reflejar más exactamente el riesgo que supone la vulnerabilidad para el entorno del usuario. No obstante, no es obligatorio y en función del objetivo, la puntuación y vector base pueden ser suficientes.

Si se necesita puntuación temporal, la ecuación temporal combina las métricas temporales con la puntuación base para obtener un rango de puntuación temporal entre 0 y 10. Igualmente, si se necesita puntuación del entorno, la ecuación del entorno combina las métricas del entorno con la puntuación temporal para obtener un rango de puntuación del entorno entre 0 y 10. Las ecuaciones base, temporal y del entorno se describen con detalle en 8.2.

6.3 ¿Quién realiza la puntuación?

En general, las métricas base y temporal son especificadas por analistas que elaboran boletines de vulnerabilidades, vendedores de productos de seguridad o vendedores de aplicaciones, que normalmente tienen más información que los usuarios sobre las características de una vulnerabilidad. Sin embargo, las métricas del entorno son especificadas por usuarios puesto que éstos pueden hacer la mejor evaluación del impacto potencial de una vulnerabilidad sobre sus propios entornos.

6.4 ¿Quién utiliza el CVSS?

Numerosas organizaciones utilizan el CVSS, y cada una de ellas aprecia el valor del mismo de forma diferente. A continuación se describen algunos ejemplos:

- Proveedores de boletines de vulnerabilidades: organizaciones sin ánimo de lucro y organizaciones comerciales publican puntuaciones y vectores base y temporales CVSS en los boletines de vulnerabilidades que publican gratuitamente. Dichos boletines ofrecen mucha información incluida la fecha del descubrimiento, sistemas afectados y enlaces a vendedores para obtener recomendaciones sobre los parches a implantar.
- Vendedores de aplicaciones software: los vendedores de aplicaciones software proporcionan puntuaciones y vectores base CVSS a sus clientes. Ello les ayuda a comunicar de forma adecuada la gravedad de las vulnerabilidades de sus productos y ayudar a sus clientes a gestionar de forma efectiva los riesgos por utilización de las TIC.
- Organizaciones de usuarios: muchas organizaciones del sector privado utilizan internamente el CVSS para tomar decisiones de gestión sobre vulnerabilidades debidamente informadas. Utilizan sistemas de exploración o tecnologías de supervisión para localizar las vulnerabilidades en equipos anfitriones y aplicaciones. Combinan dichos datos con puntuaciones CVSS base, temporales y del entorno a fin de disponer de más información de carácter contextual del riesgo y remediar aquellas vulnerabilidades que conlleven los mayores riesgos para sus sistemas.
- Exploración y gestión de vulnerabilidades: las organizaciones de gestión de vulnerabilidades exploran las redes para detectar vulnerabilidades de las TIC. Proporcionan puntuaciones CVSS base para cada vulnerabilidad en cada anfitrión. Las organizaciones de usuarios utilizan este flujo de datos críticos para gestionar de forma más efectiva sus infraestructuras TIC reduciendo las interrupciones del servicio y protegiéndose de amenazas maliciosas y accidentales que se ciernen sobre las TIC.
- Gestión (de riesgos) de la seguridad: las empresas que se dedican a la gestión de riesgos de la seguridad utilizan el CVSS como parámetro de entrada para calcular el riesgo o nivel de amenaza para una organización. Dichas empresas utilizan aplicaciones sofisticadas que a menudo se integran en la topología de la red, datos de vulnerabilidades, y base de datos de activos de la organización para ofrecer a sus clientes una perspectiva mejor informada de su nivel de riesgo.
- Investigadores: el marco abierto del CVSS permite a los investigadores realizar análisis estadísticos de las vulnerabilidades y de sus propiedades.

6.5 Grupos de métricas: métricas base

El grupo de métricas base permite obtener las características de una vulnerabilidad que son constantes con el tiempo y en distintos entornos de usuario. Las métricas basadas en el vector de acceso, la complejidad del acceso y la autentificación determinan cómo se accede a la vulnerabilidad y si son necesarias condiciones especiales para explotarla. Las tres métricas de impactos miden cómo afecta la explotación de una vulnerabilidad a un activo TIC, definiéndose como impactos mutuamente independientes el nivel de pérdida de confidencialidad, de integridad y de disponibilidad. Por ejemplo, una vulnerabilidad podría causar la pérdida parcial de la integridad y la disponibilidad, pero no de la confidencialidad.

6.5.1 Vector de acceso (AV)

Esta métrica refleja cómo se explota una vulnerabilidad. En el cuadro 1 se enumeran los valores posibles de esta métrica Cuanta mayor sea la distancia a la que un agresor puede atacar a un anfitrión, mayor será la puntuación de la vulnerabilidad.

Cuadro 1 – Evaluación de la puntuación del vector de acceso

Valor de la métrica	Descripción
Local (L)	Una vulnerabilidad que sólo pueda explotarse a través de acceso local requiere que el agresor tenga acceso físico al sistema vulnerable o una cuenta local (*shell*). Ejemplos de vulnerabilidades explotables en local son los ataques a través de elementos periféricos, tales como ataques a través de cortafuegos /USB DMA y ataques con escalado basado en privilegios locales (por ejemplo, sudo).
Red adyacente (A)	Una vulnerabilidad que pueda explotarse mediante el acceso desde una red adyacente requiere que el agresor tenga acceso al dominio de difusión o de colisión del software vulnerable. Son ejemplos de redes locales las subredes IP, Bluetooth, IEEE 802.11 y el segmento local Ethernet.
Red (N)	Una vulnerabilidad que pueda explotarse mediante el acceso a través de la red significa que el software vulnerable está asociado a la capa de red, no requiriendo el agresor acceso a través de red local o de acceso local. Dicha vulnerabilidad se denomina a menudo "explotable a distancia". Un ejemplo de ataque de red es el desbordamiento de la memoria intermedia RPC.

6.5.2 Complejidad del acceso (AC)

Esta métrica mide la complejidad del ataque requerido para explotar la vulnerabilidad una vez que el agresor ha ganado acceso al sistema objetivo. Por ejemplo, es el caso del desbordamiento de la memoria intermedia en un servicio de Internet: una vez se ha localizado y accedido al sistema objetivo, el agresor puede lanzar sus ataques a voluntad.

No obstante, otras vulnerabilidades pueden requerir pasos adicionales para poder ser explotadas. Por ejemplo, una vulnerabilidad en un cliente de correo electrónico sólo se explota después de que el usuario haya descargado y abierto un anexo infectado. En el cuadro 2 se recogen los posibles valores para esta métrica. Cuanto menor sea la complejidad requerida, mayor será la puntuación de la vulnerabilidad.

Cuadro 2 – Evaluación de la puntuación de complejidad del acceso

Valor de la métrica	Descripción
Alto (H)	Las condiciones de acceso son especiales. Por ejemplo: • En la mayoría de las configuraciones, la parte agresora debe tener un elevado nivel de privilegios o actuar con una identidad falsa en otros sistemas, además de atacar el sistema objetivo (por ejemplo, apropiación de DNS). • El ataque se basa en métodos de ingeniería social que serían fácilmente detectados por personas con suficientes conocimientos. Por ejemplo, cuando la víctima lleva a cabo actuaciones sospechosas o atípicas. • La configuración vulnerable es muy poco frecuente en la práctica. • Si se produce un estado de carrera, la ventana es muy estrecha.

Cuadro 2 – Evaluación de la puntuación de complejidad del acceso

Valor de la métrica	Descripción
Medio (M)	Las condiciones de acceso son en cierta medida especiales; por ejemplo: • La parte agresora se limita a un grupo de sistemas o usuarios con un determinado nivel de autorización, posiblemente no fiable. • Es necesario recopilar determinada información antes de lanzar un ataque con éxito. • La configuración afectada no es la utilizada por defecto ni la que se configura normalmente (por ejemplo, una vulnerabilidad que se produce cuando un servidor realiza la autentificación de la cuenta de un usuario mediante un esquema especial, pero que no está presente para otros esquemas de autentificación). • El ataque exige una cierta dosis de ingeniería social que puede ocasionalmente engañar a usuarios cautelosos (por ejemplo, ataques de suplantación que modifican la barra de estado de los navegadores para mostrar enlaces falsos o utilizar la lista de contactos de alguien para enviar mensajería instantánea maliciosa).
Bajo (L)	No existen condiciones de acceso especiales o circunstancias atenuantes. Por ejemplo: • El producto afectado requiere típicamente el acceso a una amplia gama de sistemas y usuarios, posiblemente anónimos y no fiables (por ejemplo, una web accesible desde Internet o un servidor de correo). • La configuración afectada es la establecida por defecto o la que es ubicua. • El ataque puede realizarse manualmente y requiere pocas habilidades o recopilar información adicional. • El estado de carrera tiene una ejecución lenta (es decir, técnicamente es una situación de carrera pero puede contrarrestarse fácilmente).

6.5.3 Autentificación (Au)

Esta métrica mide el número de veces que un agresor debe autentificarse ante un objetivo para explotar una vulnerabilidad. Esta métrica no mide la fortaleza o complejidad del proceso de autentificación, sino el hecho de que el agresor deba presentar credenciales antes de explotar la vulnerabilidad. En el cuadro 3 se enumeran los posibles valores de esta métrica. Cuantas menos instancias de autentificación sean necesarias, más alta será la puntuación de vulnerabilidad.

Cuadro 3 – Evaluación de la puntuación de autentificación

Valor de la métrica	Descripción
Múltiple (M)	Explotar la vulnerabilidad requiere que el agresor se autentifique dos o más veces, incluso si cada vez se utilizan las mismas credenciales. Por ejemplo, un agresor que se autentifique ante un sistema operativo además de presentar sus credenciales para acceder a una aplicación que aloje dicho sistema.
Sencillo (S)	La vulnerabilidad requiere que el agresor se registre en el sistema (por ejemplo, en una línea de instrucción o a través de una sesión o una interfaz web).
Ninguno (N)	No se requiere autentificación para explotar la vulnerabilidad.

La métrica debería aplicarse basada en la autentificación que se exige a un agresor antes de lanzar un ataque. Por ejemplo, si un servidor de correo es vulnerable a una instrucción que puede ser ejecutada antes que el usuario se autentique, la métrica debería tomar el valor "Ninguna", pues el agresor puede lanzar su ataque antes de que sean necesarias credenciales. Si la instrucción vulnerable sólo está disponible después de una autentificación exitosa, la puntuación de

vulnerabilidad debería ser "Sencilla" o "Múltiple", en función de las instancias de autentificación necesarias antes de la ejecución de la instrucción.

6.5.4 Impacto sobre la confidencialidad (C)

Esta métrica mide el impacto sobre la confidencialidad de una vulnerabilidad explotada con éxito. La confidencialidad conlleva limitar el acceso a la información y su divulgación exclusivamente a usuarios autorizados, así como a impedir el acceso o descubrimiento a usuarios no autorizados. En el cuadro 4 se enumeran los posibles valores de esta métrica. Un mayor impacto en la confidencialidad aumenta la puntuación de vulnerabilidad.

Cuadro 4 – Evaluación de la puntuación del impacto sobre la confidencialidad

Valor de la métrica	Descripción
Ninguno (N)	No hay impacto sobre la confidencialidad del sistema.
Parcial (P)	Se produce un descubrimiento considerable de información. Aunque es posible acceder a algunos ficheros del sistema, el agresor no tiene control de lo que consigue o el ámbito de la pérdida está limitado. Un ejemplo de ello es la vulnerabilidad que divulga sólo algunas tablas de una base de datos.
Completo (C)	Toda la información queda al descubrimiento, como consecuencia de lo cual todos los ficheros del sistema son revelados. El agresor puede leer todos los datos del sistema (memoria, ficheros, etc.).

6.5.5 Impacto sobre la integridad (I)

Esta métrica mide el impacto sobre la integridad de una vulnerabilidad explotada con éxito. La integridad hace referencia al grado de confianza y garantía de veracidad de la información. En el cuadro 5 se enumeran los posibles valores de esta métrica. Un mayor impacto en la integridad aumenta la puntuación de vulnerabilidad.

Cuadro 5 – Evaluación de la puntuación del impacto sobre la integridad

Valor de la métrica	Descripción
Ninguno (N)	No hay impacto en la integridad del sistema.
Parcial (P)	Es posible modificar algunos ficheros o información, pero el agresor no controla lo que ha modificado o el ámbito del ataque es limitado. Por ejemplo, el sistema o los ficheros de una aplicación pueden ser sobrescritos o modificados, pero el agresor no controla los ficheros afectados, o bien, sólo puede modificar ficheros en un contexto o ámbito limitado.
Completo (C)	La integridad del sistema está completamente en riesgo. La pérdida de protección del sistema es total. El agresor puede modificar cualquier fichero del sistema objetivo.

6.5.6 Impacto sobre la disponibilidad (A)

Esta métrica mide el impacto sobre la disponibilidad de una vulnerabilidad explotada con éxito. La disponibilidad hace referencia al acceso a recursos de información. Los ataques que consumen anchura de banda, ciclos de proceso o espacio en el disco, afectan a la disponibilidad de un sistema En el cuadro 6 se enumeran los posibles valores de esta métrica. Un mayor impacto en la disponibilidad aumenta la puntuación de la vulnerabilidad.

Cuadro 6 – Evaluación de la puntuación del impacto sobre la disponibilidad

Valor de la métrica	Descripción
Ninguno (N)	No hay impacto en la disponibilidad del sistema.
Parcial (P)	Se reducen las prestaciones o se producen interrupciones en la disponibilidad del recurso. Un ejemplo de ello es un ataque desde la red por inundación que permita mantener activas un número limitado de conexiones a un servicio de acceso a Internet.
Completo (C)	Se produce una caída completa del recurso afectado. El agresor puede hacer que el recurso quede completamente indisponible.

6.6 Métricas temporales

La amenaza de una vulnerabilidad puede cambiar con el tiempo. Los tres factores que contempla el CVSS son: confirmación de la información técnica disponible sobre una vulnerabilidad, estado del remedio de la vulnerabilidad y disponibilidad de código o técnicas de explotación de la vulnerabilidad. Dado que las métricas temporales son opcionales, cada una de ellas incluye un valor de métrica que no afecta a la puntuación y que se utiliza cuando el usuario considera que una métrica concreta no es aplicable y no desea tenerla en cuenta.

6.6.1 Explotabilidad (E)

Esta métrica mide la situación actual de disponibilidad del código o técnicas de explotación maliciosas. La disponibilidad pública de un código de explotación maliciosa de fácil utilización aumenta el número de potenciales agresores, incluidos los no expertos e incrementando la gravedad de la vulnerabilidad.

Inicialmente, la capacidad de explotación real de una vulnerabilidad puede ser sólo teórica. Ulteriormente, puede hacerse público un código de prueba de concepto, un código que permita la explotación funcional o incluso información técnica suficiente para la explotación de la vulnerabilidad. Además, el código para la explotación maliciosa inicialmente existente puede pasar de ser prueba de concepto a código con capacidad para una explotación consistente de la vulnerabilidad. En casos graves, el código puede ser distribuido mediante un gusano o un virus a través de la red. En el cuadro 7 se enumeran los posibles valores de esta métrica. Cuanto más fácil sea la explotación de una vulnerabilidad, más alta será la puntuación de la misma.

Cuadro 7 – Evaluación de la puntuación del impacto sobre la explotabilidad

Valor de la métrica	Descripción
Sin pruebas (U)	No existe código de la aplicación maliciosa, o ésta es completamente teórica.
Prueba de concepto (POC)	Existe un código de aplicación maliciosa que es una prueba de concepto o una demostración que no es aplicable en la práctica a la mayoría de los sistemas. El código o técnica no es funcionalmente operativo en todas las situaciones y puede requerir ser sustancialmente modificado por un agresor suficientemente capacitado.
Funcional (F)	Hay disponible un código de aplicación maliciosa que funciona en la mayoría de las situaciones en las que existe la vulnerabilidad.
Alto (H)	La vulnerabilidad es explotable mediante un código autónomo móvil y funcional, o bien, no requiere de una aplicación maliciosa (activación manual), estando la información técnica detallada ampliamente disponible. El código funciona en cualquier situación o es distribuido activamente mediante un agente autónomo móvil (como un gusano o un virus).
No definido (ND)	La asignación de este valor a la métrica no influye en la puntuación. Es una indicación para que la ecuación no tenga en cuenta esta métrica.

6.6.2 Nivel de remedio (RL)

El nivel de remedio o subsanación de una vulnerabilidad es un factor importante para la priorización. Normalmente, en el momento de la publicación de una vulnerabilidad se carece de parche para la misma. Las soluciones temporales alternativas o parches en caliente pueden ser remedios interinos hasta la disponibilidad de un parche o una mejora oficial de la aplicación afectada. Cada una de dichas etapas reduce la puntuación temporal, que refleja así una urgencia decreciente cuando el remedio pasa a ser el definitivo. En el cuadro 8 se enumeran los posibles valores de esta métrica. Cuanto menos oficial y permanente sea una solución, más alta será la puntuación de vulnerabilidad.

Cuadro 8 – Evaluación de la puntuación del nivel de remedio

Valor de la métrica	Descripción
Parche oficial (OF)	Hay disponible una solución completa del vendedor. El vendedor dispone de un parche oficial o hay disponible una mejora de la aplicación.
Parche temporal (TF)	Hay disponible una solución oficial pero temporal. Ello incluye instancias para las que el vendedor dispone de un parche en caliente, herramienta o solución alternativa temporal.
Rodeo (W)	Hay disponible una solución no oficial, no creada por el vendedor. En algunos casos, los usuarios de la tecnología afectada crean un parche propio como solución alternativa o para mitigar la vulnerabilidad.
Indisponible (U)	No hay una solución disponible o ésta es imposible de aplicar.
No definido (ND)	La asignación de este valor a la métrica no influye en la puntuación. Es una indicación para que la ecuación no tenga en cuenta esta métrica.

6.6.3 Confianza de la información (RC)

Esta métrica mide el grado de confianza en la propia existencia de la vulnerabilidad y la credibilidad de la información técnica conocida. Algunas veces sólo se publica la existencia de una vulnerabilidad sin más detalles específicos. La vulnerabilidad puede ser corroborada ulteriormente y confirmada por el diseñador o vendedor de la tecnología afectada. La urgencia frente a una vulnerabilidad es mayor si hay certeza de su existencia. Esta métrica también indica el nivel de conocimiento técnico que deben tener los potenciales agresores. En el cuadro 9 se enumeran los posibles valores de la misma. Cuanta más validez otorgue el suministrador u otras fuentes reputadas a la existencia de la vulnerabilidad, mayor será la puntuación.

Cuadro 9 – Evaluación de la puntuación de Confianza de la información

Valor de la métrica	Descripción
No confirmado (UC)	Existe una única fuente no confirmada o posiblemente múltiples informes contradictorios. Existe poca confianza en la validez de los informes. Un ejemplo es un rumor surgido del mundo de los piratas informáticos.
No corroborado (UR)	Existen múltiples fuentes no oficiales, que posiblemente incluyan a empresas de seguridad independientes u organizaciones de investigación. Pueden existir informaciones técnicas contradictorias o ambigüedades persistentes.

Cuadro 9 – Evaluación de la puntuación de Confianza de la información

Valor de la métrica	Descripción
Confirmado (C)	El vendedor o diseñador de la tecnología afectada ha reconocido la existencia de la vulnerabilidad. La existencia de la vulnerabilidad también puede ser confirmada por un evento externo tal como la publicación de un código de aplicación maliciosa que sea una prueba de concepto funcional o una amplia difusión de la aplicación maliciosa.
No definido (ND)	La asignación de este valor a la métrica no influye en la puntuación. Es una indicación para que la ecuación no tenga en cuenta esta métrica.

6.7 Métricas relacionadas con el entorno

El riesgo que supone una vulnerabilidad para una organización y partes interesadas está muy relacionado con la existencia de distintos entornos en la organización. El conjunto de métricas CVSS relacionadas con el entorno recoge las características de una vulnerabilidad asociadas al entorno específico de las TIC del usuario. Dado que las métricas relacionadas con el entorno son opcionales, cada métrica incluye un valor que hace que ésta no influya en la puntuación. Dicho valor se utiliza cuando el usuario considera que la métrica en concreto no es aplicable y desea obviarla.

6.7.1 Potencial daño colateral (CDP)

Esta métrica mide la potencial pérdida de vidas o activos físicos causado por el daño o robo de propiedades o de equipos. La métrica también mide la pérdida económica, en términos de productividad o de ingresos. En el cuadro 10 se enumeran los posibles valores de esta métrica. Naturalmente, cuanto mayor sea el daño potencial, más alta será la puntuación de la vulnerabilidad.

Cuadro 10 – Evaluación de la puntuación del potencial daño colateral

Valor de la métrica	Descripción
Ninguno (N)	No existe una potencial pérdida de vidas, activos físicos, productividad o ingresos.
Bajo (L)	Una aplicación maliciosa exitosa de la vulnerabilidad puede producir un ligero daño físico o a la propiedad, o bien, una ligera pérdida de ingresos o de productividad de la organización.
Bajo-Medio (LM)	Una aplicación maliciosa exitosa de esta vulnerabilidad puede producir un moderado daño físico o a la propiedad, o bien, una pérdida moderada de ingresos o de productividad de la organización.
Medio-Alto (MH)	Una aplicación maliciosa exitosa de esta vulnerabilidad puede producir un significativo daño físico o a la propiedad, o bien, una pérdida significativa de ingresos o de productividad.
Alto (H)	Una aplicación maliciosa exitosa de esta vulnerabilidad puede producir un daño físico o a la propiedad que sea catastrófico, o bien, una pérdida catastrófica de ingresos o de productividad.
No definido (ND)	La asignación de este valor a la métrica no influye en la puntuación. Es una indicación para que la ecuación no tenga en cuenta esta métrica.

Cada organización debe determinar el significado preciso que para ella tienen los términos "ligero, moderado, significativo y catastrófico."

6.7.2 Distribución del objetivo (TD)

Esta métrica mide la proporción de sistemas vulnerables. Tiene el significado de indicador específico del entorno para estimar de forma aproximada el porcentaje de sistemas que podrían ser afectados por la vulnerabilidad. En el cuadro 11 se enumeran los posibles valores de esta métrica. Cuanto mayor sea la proporción de sistemas vulnerables, más alta será la puntuación.

Cuadro 11 – Evaluación de la puntuación de la distribución del objetivo

Valor de la métrica	Descripción
Ninguno (N)	No existe un sistema objetivo, o los objetivos son tan especializados que sólo existen en un entorno de laboratorio. Puede decirse que, de forma efectiva, el 0% del entorno está en riesgo.
Bajo (L)	Existen objetivos en el entorno, pero a pequeña escala. Entre el 1% y el 25% del entorno está en riesgo.
Medio (M)	Existen objetivos en el entorno, pero a mediana escala. Entre el 26% y el 75% del entorno está en riesgo.
Alto (H)	Existen objetivos en el entorno a una escala considerable. Entre el 76% y el 100% del entorno está en riesgo.
No definido (ND)	La asignación de este valor a la métrica no influye en la puntuación. Es una indicación para que la ecuación no tenga en cuenta esta métrica.

6.7.3 Requisitos de seguridad (CR, IR, AR)

Estas métricas permiten al analista diseñar a medida la puntuación CVSS en función de la importancia que para la organización del usuario tenga el activo TIC afectado, medido en términos de confidencialidad (CR), integridad (IR) y disponibilidad (DR). Es decir, si un activo TIC soporta una función de negocio para la que la disponibilidad es de la máxima importancia, el analista puede asignar un valor superior a la disponibilidad que a la confidencialidad o a la integridad. Cada requisito de seguridad tiene tres valores posibles: bajo, medio o alto.

El efecto total de la puntuación del entorno está determinado por las correspondientes métricas base de impacto (nótese que no se modifican las métricas base del impacto en confidencialidad, integridad y disponibilidad). Es decir, dichas métricas modifican la puntuación del entorno al ponderar de nuevo las métricas (base) del impacto sobre confidencialidad, integridad y disponibilidad. Por ejemplo, la métrica del impacto sobre la confidencialidad (C) tiene un peso mayor si el requisito de confidencialidad (CR) es elevado. Asimismo, la métrica del impacto sobre la confidencialidad reduce su peso si el requisito de confidencialidad es bajo. La ponderación de la métrica del impacto sobre confidencialidad es neutral si el requisito de confidencialidad es medio. La misma lógica se aplica a los requisitos de integridad y disponibilidad.

Nótese que el requisito de confidencialidad no afectará a la puntuación del entorno si el impacto (base) sobre la confidencialidad se fija en el valor ninguno. Asimismo, un aumento del requisito de confidencialidad desde medio a alto no cambiará la puntuación del entorno si la métrica del impacto (base) se ha fijado en completo. Ello se debe a que la subpuntuación del impacto (parte de la puntuación base que calcula impacto) ya tiene un valor máximo de 10.

En el cuadro 12 se enumeran los posibles valores de los requisitos de seguridad. Por brevedad, se utiliza el mismo cuadro para las tres métricas. Cuanto mayor sea el requisito de seguridad, mayor será la puntuación (recuérdese que el valor por defecto es medio). Estas métricas modificarán la puntuación en ±2,5 como máximo.

Cuadro 12 – Evaluación de la puntuación de requisitos de seguridad

Valor de la métrica	Descripción
Bajo (L)	Es probable que la pérdida de [confidencialidad | integridad | disponibilidad] sólo tenga un efecto adverso limitado en la organización o en individuos ligados a la organización (por ejemplo, empleados, clientes)
Medio (M)	Es probable que la pérdida de [confidencialidad | integridad | disponibilidad] sólo tenga un efecto adverso grave en la organización o en individuos ligados a la organización (por ejemplo, empleados, clientes)
Alto (H)	Es probable que la pérdida de [confidencialidad | integridad | disponibilidad] sólo tenga un efecto adverso catastrófico en la organización o en individuos ligados a la organización (por ejemplo, empleados, clientes)
No definido (ND)	La asignación de este valor a la métrica no influirá en la puntuación. Es una indicación para que la ecuación no tenga en cuenta esta métrica.

En numerosas organizaciones, los recursos de las TIC se clasifican según su criticidad en base a la ubicación en la red, función de negocio y potencial para producir pérdida de ingresos o vidas. Por ejemplo, el gobierno de los EE.UU. asigna cada activo TIC no secreto a una agrupación de activos denominada sistema. A cada sistema se le deben asignar tres valoraciones de "impactos potenciales" para reflejar el impacto potencial sobre la organización si el Sistema se encuentra en situación de riesgo según tres objetivos de seguridad: confidencialidad, integridad y disponibilidad. Por tanto, cada activo TIC no secreto del gobierno de los EE.UU. tiene una clasificación del impacto potencial que puede ser bajo, moderado o alto en relación con los objetivos de seguridad de confidencialidad, integridad y disponibilidad. Este sistema de clasificación se describe en la norma Federal Information Processing Standards (FIPS) 199. El CVSS sigue este modelo general de la FIPS 199, pero no requiere que las organizaciones utilicen un sistema en particular para la asignación de valoraciones de impacto bajo, medio y alto.

6.8 Vectores básico, temporal y del entorno

Cada métrica del vector consta del nombre abreviado de la misma, seguido de ":" (dos puntos) y del valor abreviado de la métrica. El vector enumera dichas métricas en un orden predeterminado, utilizando el carácter "/" (barra oblicua) para separar las métricas. Si no se utiliza métrica temporal o del entorno, ésta toma el valor "ND" (no definido). En el cuadro 13 se muestran los vectores base, temporal y de entorno.

Cuadro 13 – Vectores base, temporal y del entorno

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

Por ejemplo, una vulnerabilidad con los valores de métrica base siguientes: "vector de acceso: bajo; complejidad del acceso: medio; autentificación: ninguna; impacto sobre la confidencialidad: ninguno; impacto sobre la integridad: parcial; impacto sobre la disponibilidad: completo", tendría el vector básico: "AV:L/AC:M/Au:N/C:N/I:P/A:C".

6.9 Directrices para realizar la puntuación

En esta cláusula se presentan directrices destinadas a ayudar a los analistas en su labor de puntuación de vulnerabilidades.

6.9.1 General

RECOMENDACIÓN de PUNTUACIÓN #1: la puntuación de vulnerabilidad no debería tener en cuenta ninguna interacción con otras vulnerabilidades. Es decir, cada vulnerabilidad debería puntuarse de forma independiente.

RECOMENDACIÓN de PUNTUACIÓN #2: cuando se puntúe una vulnerabilidad, sólo debe considerarse el impacto sobre el anfitrión objetivo. Por ejemplo, en el caso de una vulnerabilidad de tipo "cross-site scripting" o interpretación de scripts en un sitio diferente al objetivo original, el impacto sobre un sistema de usuario podría ser muy superior al impacto sobre el anfitrión objetivo. No obstante, éste es un impacto indirecto. Las vulnerabilidades de tipo "cross-site scripting" deberían puntuarse sin impacto sobre la confidencialidad o disponibilidad, y con un impacto parcial sobre la integridad.

RECOMENDACIÓN de PUNTUACIÓN #3: numerosas aplicaciones, como los servidores Web, pueden ejecutarse con diferentes privilegios y para puntuar el impacto deben hacerse hipótesis sobre qué privilegios se utilizan. Por tanto, las vulnerabilidades deberían puntuarse de conformidad con los privilegios más comúnmente utilizados. Ello puede no reflejar necesariamente las prácticas idóneas en materia de seguridad, especialmente para aplicaciones cliente que a menudo se ejecutan con privilegios a nivel raíz. Cuando existan incertidumbres sobre qué privilegios son los más comunes, el analista que realice la puntuación debería asumir una configuración por defecto.

RECOMENDACIÓN de PUNTUACIÓN #4: cuando se puntúe el impacto de una vulnerabilidad que puede explotarse de múltiples formas (vectores de ataque), el analista debería elegir el método que tenga un mayor impacto en lugar del método más común o más fácil de ejecutar. Por ejemplo, si existe un código de aplicación maliciosa que funcione sobre una plataforma pero no sobre otra, la explotabilidad debe fijarse en el valor "Funcional". Si dos variantes diferentes de un producto se encuentran en desarrollo paralelo (por ejemplo, PHP 4.x y PHP 5.x) y existe un parche para una variante pero no para otra, el nivel de remedio debería ser "Indisponible".

6.9.2 Métricas base

6.9.2.1 Vector de acceso

RECOMENDACIÓN de PUNTUACIÓN #5: cuando una vulnerabilidad pueda explotarse tanto localmente como desde la red, debería elegirse el valor "red". Cuando una vulnerabilidad pueda explotarse localmente y desde redes adyacentes, pero no desde redes a distancia, debería elegirse el valor "red adyacente". Cuando una vulnerabilidad pueda explotarse desde una "red adyacente" y desde redes a distancia, debería elegirse el valor "red".

RECOMENDACIÓN de PUNTUACIÓN #6: numerosas aplicaciones y utilidades de cliente tienen vulnerabilidades locales que pueden explotarse a distancia mediante actuaciones que precisan de la complicidad del usuario o mediante procesos automáticos. Por ejemplo, las utilidades de descompresión y los analizadores de virus exploran automáticamente los correos electrónicos de entrada. Asimismo, las aplicaciones de apoyo (conjuntos de tipo Office, visores de imágenes, reproductores de medios, etc.) están expuestas a ataques cuando se intercambian ficheros maliciosos vía correo electrónico o cuando se realizan descargas desde sitios web. Por tanto, el analista debe asignar el valor "red" al vector de acceso de dichas vulnerabilidades.

6.9.2.2 Autentificación

RECOMENDACIÓN de PUNTUACIÓN #7: si la vulnerabilidad está presente en un esquema de autentificación (por ejemplo, PAM, Kerberos) o en un servicio anónimo (por ejemplo, un servidor FTP público), la métrica debería tomar el valor "Ninguno", puesto que el agresor puede explotarla sin suministrar credenciales válidas. En caso de existencia de una cuenta de usuario por defecto, el valor de Autentificación puede ser "Sencillo" o "Múltiple" (según sea el caso), pero puede tener como valor de explotabilidad "Alto" si las credenciales se hacen públicas.

RECOMENDACIÓN de PUNTUACIÓN #8: es importante señalar que la métrica de autentificación es diferente del Vector de Acceso. En este caso, los requisitos de autentificación se tienen en cuenta una vez que se ha accedido al sistema. Por ejemplo, en el caso de vulnerabilidades explotables localmente, el valor de esta métrica no debe ser "Sencillo" o "Múltiple" si se precisa autentificación adicional a la necesaria para registrarse en el sistema. Un ejemplo de vulnerabilidad localmente explotable que requiere autentificación es la del motor de una base de datos que escuche un conector o socket de un dominio Unix (o alguna otra interfaz que no sea de red). Si para poder explotar la vulnerabilidad el usuario debe autentificarse como usuario válido de la base de datos, el valor de la métrica debe ser "Sencillo".

6.9.2.3 Impactos en la confidencialidad, integridad y disponibilidad

RECOMENDACIÓN de PUNTUACIÓN #9: las vulnerabilidades que permiten acceso a nivel raíz deberían puntuarse con pérdida completa de confidencialidad, integridad y disponibilidad, mientras que las vulnerabilidades que den acceso a nivel de usuario deberían puntuarse sólo con pérdida parcial de confidencialidad, integridad y disponibilidad. Por ejemplo, una vulneración de la integridad que permita a un agresor modificar un fichero de palabras clave del sistema operativo debería puntuarse con impacto completo sobre confidencialidad, integridad y disponibilidad.

RECOMENDACIÓN de PUNTUACIÓN #10: las vulnerabilidades con pérdida parcial o completa de integridad también pueden tener impacto en la disponibilidad. Por ejemplo, un pirata informático que pueda modificar registros probablemente también pueda suprimirlos.

6.10 Ecuaciones

En esta cláusula se describen las ecuaciones y algoritmos de puntuación para grupos de métricas base, temporales y del entorno. En el sitio http://www.first.org/cvss está disponible el origen y la prueba de estas ecuaciones. En el apéndice I se muestran tres ejemplos de casos de uso de dichas ecuaciones.

6.10.1 Ecuación base

La ecuación base es el elemento fundamental de la puntuación CVSS. La ecuación base (versión 2.10) es la siguiente:

```
BaseScore = round_to_1_decimal(((0.6*Impact)+(0.4*Exploitability)-1.5)*f(Impact))
Impact = 10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact))
Exploitability = 20*AccessVector*AccessComplexity*Authentication
f(impact) = 0 if Impact=0, 1.176 otherwise
AccessVector     = case AccessVector of
                        requires local access: 0.395
                        adjacent network accessible: 0.646
                        network accessible: 1.0
AccessComplexity = case AccessComplexity of
                        high: 0.35
                        medium: 0.61
                        low: 0.71
Authentication   = case Authentication of
                        requires multiple instances of authentication: 0.45
                        requires single instance of authentication: 0.56
                        requires no authentication: 0.704
ConfImpact       = case ConfidentialityImpact of
                        none:             0.000
                        partial:          0.275
                        complete:         0.660
IntegImpact      = case IntegrityImpact of
                        none:             0.000
                        partial:          0.275
                        complete:         0.660
AvailImpact      = case AvailabilityImpact of
                        none:             0.000
                        partial:          0.275
                        complete:         0.660
```

6.10.2 Ecuación temporal

Si se utiliza la ecuación temporal, ésta combinará las métricas temporales con la puntuación base para obtener una puntuación temporal comprendida entre 0 y 10. Además, la puntuación temporal generará una puntuación temporal no superior a la puntuación base y no menor de un 33% inferior que la puntuación base. La ecuación temporal es la siguiente:

```
TemporalScore = round_to_1_decimal(BaseScore*Exploitability
                *RemediationLevel*ReportConfidence)
Exploitability   = case Exploitability of
                        unproven:             0.85
                        proof-of-concept:     0.90
                        functional:           0.95
                        high:                 1.00
                        not defined:          1.00

RemediationLevel = case RemediationLevel of
                        official-fix:         0.87
                        temporary-fix:        0.90
                        workaround:           0.95
                        unavailable:          1.00
                        not defined:          1.00

ReportConfidence = case ReportConfidence of
                        unconfirmed:          0.90
                        uncorroborated:       0.95
                        confirmed:            1.00
                        not defined:          1.00
```

6.10.3 Ecuación del entorno

Si se utiliza la ecuación del entorno, ésta combinará las métricas del entorno con la puntuación temporal para obtener una puntuación del entorno comprendida entre 0 y 10. Además, esta ecuación generará una puntuación no superior a la puntuación temporal. La ecuación del entorno es la siguiente:

```
EnvironmentalScore = round_to_1_decimal((AdjustedTemporal+
(10-AdjustedTemporal)*CollateralDamagePotential)*TargetDistribution)
AdjustedTemporal = TemporalScore recomputed with the BaseScores Impact
sub-equation replaced with the AdjustedImpact equation
AdjustedImpact = min(10,10.41*(1-(1-ConfImpact*ConfReq)*(1-IntegImpact*IntegReq)
                 *(1-AvailImpact*AvailReq)))
CollateralDamagePotential = case CollateralDamagePotential of
                                none:            0.0
                                low:             0.1
                                low-medium:      0.3
                                medium-high:     0.4
                                high:            0.5
                                not defined:     0.0

TargetDistribution        = case TargetDistribution of
                                none:            0.00
                                low:             0.25
                                medium:          0.75
                                high:            1.00
                                not defined:     1.00
ConfReq                      = case ConfReq of
                                low:             0.5
                                medium:          1.0
                                high:            1.51
                                not defined:     1.0
IntegReq                  = case IntegReq of
                                low:             0.5
                                medium:          1.0
                                high:            1.51
                                not defined:     1.0
AvailReq                  = case AvailReq of
                                low:             0.5
                                medium:          1.0
                                high:            1.51
                                not defined:     1.0
```

7 Recursos adicionales

El apéndice II contiene una lista de recursos que pueden resultar útiles a quienes desee utilizar el CVSS. La lista contiene enlaces a boletines de vulnerabilidad y a diversas calculadoras de CVSS. Estos boletines sirven de ayuda cuando se desea obtener información detallada sobre una determinada vulnerabilidad. Las calculadoras de CVSS son útiles para quien desea calcular puntuaciones base, temporales o del entorno.

Apéndice I

Ejemplos de uso de CVSS

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

A continuación se muestran ejemplos de cómo puede utilizarse el CVSS para tres vulnerabilidades diferentes.

I.1 CVE-2002-0392

Caso CVE-2002-0392: Apache Chunked-Encoding Memory Corruption Vulnerability (Vulnerabilidad de corrupción de memoria con codificación segmentada en Apache). En junio de 2002 se identificó una vulnerabilidad que se produce cuando el servidor web Apache trata solicitudes codificadas en segmentos (*chunked-encoding*). La Fundación Apache informó de que en determinados casos un programa agresor puede tener éxito y producir denegación de servicio, y en otros puede permitir la ejecución de código arbitrario con los privilegios propios del servidor web.

Puesto que la vulnerabilidad puede explotarse a distancia, el vector de acceso es "Red". El valor de la complejidad de acceso es "Bajo" porque no es necesario que existan circunstancias adicionales para que el programa malicioso tenga éxito; el agresor solo necesita diseñar un mensaje adecuado dirigido al elemento de escucha web Apache. No se requiere autentificación para poner en marcha esta vulnerabilidad (cualquier usuario de internet puede conectarse al servidor web), por lo que el valor de la métrica de autentificación es "Ninguno".

Puesto que la vulnerabilidad puede explotarse con múltiples métodos con resultados variados, es necesario generar puntuaciones para cada método y utilizar el más elevado.

Si la vulnerabilidad se explota para ejecutar código arbitrario con los permisos del servidor web, alterando por tanto el contenido de la web y posiblemente dando acceso a información de usuario o configuración local (incluyendo parámetros y contraseñas de acceso a bases de datos internas), las métricas del impacto en confidencialidad e integridad se fijan en "Parcial". Conjuntamente, dichas métricas alcanzan una puntuación base de 6,4.

Si la vulnerabilidad se explota para causar denegación del servicio, el valor del impacto sobre la disponibilidad debe ser "Completo". Conjuntamente, dichas métricas alcanzan una puntuación base 7,8. Puesto que esa es la puntuación base más elevada posible de las opciones de explotación, se utiliza como la puntuación base.

Por tanto, el vector básico para esta vulnerabilidad es: AV:N/AC:L/Au:N/C:N/I:N/A:C.

Dado que se conoce la existencia de código del programa malicioso, el parámetro Explotabilidad se fija en "Funcional". La Fundación Apache ha publicado parches para esta vulnerabilidad (están disponibles las versiones 1.3 y 2.0) y el nivel de remedio o subsanación es "Solución oficial". Naturalmente, el valor de confianza de la información es "Confirmada". Estas métricas ajustan la puntuación base de forma que la puntuación temporal sea de 6,4.

Si para los sistemas objetivo la disponibilidad es más importante de lo habitual, en función de los valores de Potenciales daños colaterales y de la Distribución del objetivo, la puntuación del entorno puede oscilar entre 0,0 ("Ninguno", "Ninguno") y 9,2 ("Alto", "Alto"). A continuación se resumen los resultados.

```
-------------------------------------------------------
BASE METRIC                 EVALUATION              SCORE
-------------------------------------------------------
Access Vector               [Network]              (1.00)
Access Complexity           [Low]                  (0.71)
Authentication              [None]                 (0.704)
Confidentiality Impact      [None]                 (0.00)
Integrity Impact            [None]                 (0.00)
Availability Impact         [Complete]             (0.66)
-------------------------------------------------------
BASE FORMULA                                   BASE SCORE
-------------------------------------------------------
Impact = 10.41*(1-(1)*(1)*(0.34)) == 6.9
Exploitability = 20*0.71*0.704*1 == 10.0
f(Impact) = 1.176
BaseScore = ((0.6*6.9) + (0.4*10.0) - 1.5)*1.176 == (7.8)
-------------------------------------------------------
-------------------------------------------------------
TEMPORAL METRIC             EVALUATION              SCORE
-------------------------------------------------------
Exploitability              [Functional]           (0.95)
Remediation Level           [Official-Fix]         (0.87)
Report Confidence           [Confirmed]            (1.00)
-------------------------------------------------------
TEMPORAL FORMULA                            TEMPORAL SCORE
-------------------------------------------------------
round(7.8 * 0.95 * 0.87 * 1.00)                  == (6.4)
-------------------------------------------------------
-------------------------------------------------------
ENVIRONMENTAL METRIC        EVALUATION              SCORE
-------------------------------------------------------
Collateral Damage Potential [None - High]       {0 - 0.5}
Target Distribution         [None - High]       {0 - 1.0}
Confidentiality Req.        [Medium]                (1.0)
Integrity Req.              [Medium]                (1.0)
Availability Req.           [High]                 (1.51)
-------------------------------------------------------
ENVIRONMENTAL FORMULA                ENVIRONMENTAL SCORE
-------------------------------------------------------
AdjustedImpact = min(10,10.41*(1-(1-0*1)*(1-0*1)
         *(1-0.66*1.51))                         == (10.0)
AdjustedBase =((0.6*10)+(0.4*10.0) - 1.5)*1.176
                                                 == (10.0)
AdjustedTemporal == (10*0.95*0.87*1.0)            == (8.3)
EnvScore = round((8.3+(10-8.3)*{0-0.5})*{0-1})
                                            == (0.00 - 9.2)
-------------------------------------------------------
```

I.2 CVE-2003-0818

Caso CVE-2003-0818: Microsoft Windows ASN.1 Library Integer Handling Vulnerability. En septiembre de 2003 se detectó una vulnerabilidad de la biblioteca ASN.1 de todos los sistemas operativos de Microsoft. La explotación exitosa de esta vulnerabilidad produce el desbordamiento de la memoria intermedia, lo cual permite al agresor ejecutar código arbitrario con privilegios administrativos (del sistema).

Se trata de una vulnerabilidad explotable a distancia y que no requiere autentificación; por tanto, el vector de acceso es "Red" y el valor de autentificación es "Ninguno". El valor de la complejidad de acceso es "Bajo" porque no es necesario un acceso adicional ni circunstancias especiales para una explotación exitosa del programa malicioso. Cada una de las métricas de impacto toma el valor "Completo" por la posibilidad de poner en riesgo todo el sistema. Conjuntamente, estas métricas tienen una puntuación base máxima de 10,0.

Por tanto, el vector base de esta vulnerabilidad es: AV:N/AC:L/Au:N/C:C/I:C/A:C.

Existen programas maliciosos conocidos que atacan esta vulnerabilidad y, por tanto, la Explotabilidad tiene el valor "Funcional". En febrero de 2004 Microsoft liberó el parche MS04-007, pasando el nivel de remedio a "solución oficial" y la Confianza de la información a "Confirmado". Estas métricas ajustan la puntuación base de forma que la puntuación temporal sea de 8,3.

Si la disponibilidad es menos importante de lo habitual para los sistemas objetivo, en función de los valores de Potencial daño colateral y de Distribución de objetivo, la puntuación del entorno podría oscilar entre 0,0 ("Ninguno", "Ninguno") y 9,0 ("Alto", "Alto"). A continuación se resumen los resultados.

```
-------------------------------------------------------
BASE METRIC                 EVALUATION              SCORE
-------------------------------------------------------
Access Vector               [Network]              (1.00)
Access Complexity           [Low]                  (0.71)
Authentication              [None]                 (0.704)
Confidentiality Impact      [Complete]             (0.66)
Integrity Impact            [Complete]             (0.66)
Availability Impact         [Complete]             (0.66)
-------------------------------------------------------
FORMULA                                         BASE SCORE
-------------------------------------------------------
Impact = 10.41*(1-(0.34*0.34*0.34)) == 10.0
Exploitability = 20*0.71*0.704*1 == 10.0
f(Impact) = 1.176
BaseScore =((0.6*10.0)+(0.4*10.0) - 1.5)*1.176  == (10.0)
-------------------------------------------------------

-------------------------------------------------------
TEMPORAL METRIC             EVALUATION              SCORE
-------------------------------------------------------
Exploitability              [Functional]           (0.95)
Remediation Level           [Official-Fix]         (0.87)
Report Confidence           [Confirmed]            (1.00)
-------------------------------------------------------
FORMULA                                     TEMPORAL SCORE
-------------------------------------------------------
round(10.0 * 0.95 * 0.87 * 1.00) ==                 (8.3)
-------------------------------------------------------
-------------------------------------------------------
ENVIRONMENTAL METRIC        EVALUATION              SCORE
-------------------------------------------------------
Collateral Damage Potential [None - High]       {0 - 0.5}
Target Distribution         [None - High]       {0 - 1.0}
Confidentiality Req.        [Medium]                (1.0)
Integrity Req.              [Medium]                (1.0)
Availability Req.           [Low]                   (0.5)
-------------------------------------------------------
FORMULA                                 ENVIRONMENTAL SCORE
-------------------------------------------------------
AdjustedImpact = 10.41*(1-(1-0.66*1)*(1-0.66*1)
         *(1-0.66*0.5))                          == (9.6)
AdjustedBase =((0.6*9.6)+(0.4*10.0) - 1.5)*1.176
                                                 == (9.7)
AdjustedTemporal == (9.7*0.95*0.87*1.0)          == (8.0)
EnvScore = round((8.0+(10-8.0)*{0-0.5})*{0-1})
                 ==                          (0.00 - 9.0)
-------------------------------------------------------
```

I.3 CVE-2003-0062

Caso CVE-2003-0062: Buffer Overflow in NOD32 Antivirus (Desbordamiento de la memoria intermedia del antivirus NOD32). NOD32 es un programa antivirus desarrollado por Eset. En febrero de 2003 se detectó una vulnerabilidad que provocaba el desbordamiento de la memoria intermedia en las versiones Linux y Unix anteriores a la 1.013 que podría permitir que usuarios locales ejecutasen un código arbitrario con los privilegios del usuario que ejecuta NOD32. Para provocar el desbordamiento de la memoria intermedia, el agresor debe esperar a que otro usuario (posiblemente raíz) explore un trayecto del directorio con una longitud excesiva.

Puesto que sólo un usuario registrado localmente en el sistema puede explotar la vulnerabilidad, el Vector de acceso es "Local". El valor de Complejidad del acceso es "Alto" porque el agresor no puede explotar la vulnerabilidad a su voluntad. Existe una capa adicional de complejidad porque el agresor debe esperar a que otro usuario ejecute el software de exploración del virus. La autentificación toma el valor "Ninguno" porque el atacante no precisa autentificarse ante un sistema adicional. Si un usuario administrativo quisiera explorar el virus y causar el desbordamiento de la memoria intermedia, podría ponerse en riesgo todo el sistema. Dado que debe tenerse en cuenta el caso más perjudicial, cada una de las tres métricas de impactos se pone al valor "Completo". Conjuntamente, estas métricas producen una puntuación base de 6,2.

Por tanto, el vector básico de esta vulnerabilidad es: AV:L/AC:H/Au:N/C:C/I:C/A:C.

Dado que se ha liberado parcialmente el código del programa malicioso, la métrica de la Explotabilidad toma el valor "Prueba de concepto". Éste ha publicado software actualizado, lo implica que el nivel de remedio es "solución oficial" y el valor de la confianza de la información es "Confirmado". Estas tres métricas ajustan la puntuación base de forma que la puntuación temporal sea de 4,9.

Si la confidencialidad, integridad y disponibilidad son, en líneas generales, de igual importancia para los sistemas objetivos, en función de los valores de Potencial daño colateral y de Distribución de objetivo, la puntuación del entorno podría variar entre 0,0 ("Ninguno", "Ninguno") y 7,5 ("Alto", "Alto"). A continuación se resumen los resultados.

```
-------------------------------------------------------
BASE METRIC                 EVALUATION              SCORE
-------------------------------------------------------
Access Vector               [Local]                (0.395)
Access Complexity           [High]                 (0.35)
Authentication              [None]                 (0.704)
Confidentiality Impact      [Complete]             (0.66)
Integrity Impact            [Complete]             (0.66)
Availability Impact         [Complete]             (0.66)
-------------------------------------------------------
-------------------------------------------------------
FORMULA                                         BASE SCORE
-------------------------------------------------------
Impact = 10.41 *(1-(0.34*0.34*0.34)) == 10.0
Exploitability = 20*0.35*0.704*0.395 == 1.9
f(Impact) = 1.176
BaseScore =((0.6*10)+(0.4*1.9) - 1.5)*1.176      == (6.2)
-------------------------------------------------------
```

```
-------------------------------------------------------
TEMPORAL METRIC             EVALUATION              SCORE
-------------------------------------------------------
Exploitability              [Proof-Of-Concept]     (0.90)
Remediation Level           [Official-Fix]         (0.87)
Report Confidence           [Confirmed]            (1.00)
-------------------------------------------------------
FORMULA                                   TEMPORAL SCORE
-------------------------------------------------------
round(6.2 * 0.90 * 0.87 * 1.00) ==                  (4.9)
-------------------------------------------------------
-------------------------------------------------------
ENVIRONMENTAL METRIC        EVALUATION              SCORE
-------------------------------------------------------
Collateral Damage Potential [None - High]       {0 - 0.5}
Target Distribution         [None - High]       {0 - 1.0}
Confidentiality Req.        [Medium]                (1.0)
Integrity Req.              [Medium]                (1.0)
Availability Req.           [Medium]                (1.0)
-------------------------------------------------------
FORMULA                                 ENVIRONMENTAL SCORE
-------------------------------------------------------
AdjustedTemporal == 4.9
EnvScore = round((4.9+(10-4.9)*{0-0.5})*{0-1})
                                          == (0.00 - 7.5)
-------------------------------------------------------
```

Apéndice II

Recursos adicionales

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

A continuación se presenta una lista de recursos que pueden ser útiles para quienes implementen el CVSS. Estos boletines sirven de ayuda cuando se desea obtener información detallada sobre una determinada vulnerabilidad. Las calculadoras de CVSS son útiles para quien desea calcular puntuaciones base, temporales o del entorno.

Boletines de vulnerabilidad:

- El Instituto Nacional de Normas y Tecnología [de los EE.UU.] (*National Institute of Standards and Technology*, NIST) mantiene la base de datos denominada National Vulnerability Database (NVD) y un boletín de vulnerabilidades en un sitio web que incluye puntuaciones CVSS base. El NIST proporciona dichos boletines en su web además de notas XML de uso gratuito. Pueden encontrarse en http://nvd.nist.gov/nvd.cfm, y http://nvd.nist.gov/download.cfm#XML, respectivamente.
- IBM Internet Security Systems (ISS) publica gratuitamente los boletines de vulnerabilidad X-Force. Incluyen puntuaciones CVSS base y temporales y pueden encontrarse en http://xforce.iss.net/xforce/alerts.
- Qualys publica referencias de vulnerabilidades que incluyen puntuaciones CVSS base y temporales. Pueden encontrarse en http://www.qualys.com/research/alerts/.
- Los boletines de vulnerabilidades de Cisco, incluyendo puntuaciones CVSS base y temporales pueden encontrarse en http://tools.cisco.com/MySDN/Intelligence/home.x. (NOTA – Se exige una cuenta Cisco Connection Online.)
- Tenable Network Security publica programas asociables (*plugins*) a la herramienta de exploración de vulnerabilidades Nessus. Dichos programas, que incluyen puntuaciones CVSS base, pueden encontrarse en http://www.nessus.org/plugins/.
- JPCERT/CC e IPA mantienen las Japan Vulnerability Notes (JVN), un boletín de vulnerabilidades en un sitio web que incluye puntuaciones CVSS base. JVN proporciona dichos boletines además de notas XML de uso gratuito. Pueden encontrarse en http://jvndb.jvn.jp/en/, y http://jvndb.jvn.jp/en/apis/, respectivamente.

Calculadoras CVSS:

- Calculadora del NIST CVSSv2:
  http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2
- Information-Technology Promotion Agency de Japón:
  http://jvndb.jvn.jp/en/cvss/index.html

Bibliografía

[b-1] Mike Schiffman, Gerhard Eschelbeck, David Ahmad, Andrew Wright, Sasha Romanosky, "*CVSS: A Common Vulnerability Scoring System*", National Infrastructure Advisory Council (NIAC), 2004.

[b-2] Microsoft Corporation. *Microsoft Security Response Center Security Bulletin Severity Rating System*. November 2002 [cited 16 March 2007]. Available from URL: http://www.microsoft.com/technet/security/bulletin/rating.mspx.

[b-3] United States Computer Emergency Readiness Team (US-CERT). US-CERT Vulnerability Note Field Descriptions. 2006 [cited 16 March 2007]. Available from URL: http://www.kb.cert.org/vuls/html/fieldhelp.

[b-4] SANS Institute. SANS Critical Vulnerability Analysis Archive. Undated (cited 16 March 2007).

[b-ITU-T X.1500] Recomendación X.1500 (2011), *Técnicas para el intercambio de información en materia de ciberseguridad.*

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
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	Construcción, instalación y protección de los cables y otros 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	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
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 y redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2012