Common Vulnerability Score System (CVSS) para calcular la severidad de una vulnerabilidad en los Sistemas de Información

Common Vulnerability Score System (CVSS) to calculate the Severity of a vulnerability in the Information Systems

Common Vulnerability Score System (CVSS) ao fin de calcular a severidade que pode apresentar uma vulnerabilidade em Sistemas de Informação

Pedro Henry Quintero Vivas[1], Helena Alemán Novoa[2]
Grupo de Investigación MUISCA, Facultad de Ingeniería, Especialización en Seguridad Informática, Fundación Universitaria Juan de Castellanos, Tunja, Colombia.
[1]Henquintero100@hotmail.com, [2]haleman@jdc.edu.co

Recibido / Received: 09/09/2015 – Aceptado / Accepted: 09/12/2015

Resumen

En la actualidad, en el ámbito de la seguridad informática se presentan vulnerabilidades que afectan los activos o controles implementados y que pueden ser explotadas por amenazas externas o internas, lo cual configura un riesgo de seguridad que expone a las organizaciones en su activo más importante, la información. En el presente documento, se realiza una descripción detallada del CVSS (Common Vulnerability Score System) como estándar abierto y de uso libre para estimar el impacto generado por la presencia de vulnerabilidades en un sistema informático, cuantificando su severidad y permitiendo la toma de decisiones por parte de la organización, para el tratamiento del riesgo a un nivel aceptable.

Palabras clave: Vulnerabilidades en empresas u organizaciones, CVSS (CommonVulnerability Score System), Métricas.

Abstract

Currently in the field of information security vulnerabilities are found affecting the assets or implemented controls and which can be exploited by external or internal threats, which set a security risk that exposes organizations in its most important asset, information. In this paper, a detailed description of the CVSS (Common Vulnerability Score System) as an open standard and free use to estimate the impact generated by the presence of vulnerabilities in a computer system by quantifying the severity and allowing decision making from the organization for the treatment of risk to an acceptable level.

Keywords: Vulnerabilities in Companies or Organizations, CVSS (Common Vulnerability Score System) metrics.

Resumo

Atualmente no campo de segurança da informação, vulnerabilidades são encontrados afetando os ativos ou controles implementados e que podem ser exploradas por ameaças externas ou internas, que definem um risco de segurança que expõe as organizações em seu ativo mais importante, a informação. Neste trabalho, uma descrição detalhada do CVSS (Common Vulnerability Score System) como um padrão aberto e de livre utilização para estimar o impacto gerado pela presença de vulnerabilidades em um sistema de computador por meio da quantificação da gravidade e permitindo a tomada de decisão da organização para o tratamento do risco para um nível aceitável.

Palavras-chave: Vulnerabilidades em empresas ou organizações, CVSS (Common Vulnerability Score System), Métrica.

I. Introducción

A través del tiempo, el avance de las tecnologías globalmente, se ha convertido en una constante que las personas han adoptado en sus pensamientos y cotidianidad, pues el intento de hacer más fácil la vida de la humanidad es latente [1]. Pero así como esta evolución ha traído una serie de ventajas, también se han presentado una serie de desventajas, dentro de las cuales encontramos la problemática en torno a la seguridad de la información, la cual es susceptible de muchas vulnerabilidades. Punto clave donde la información desempeña un papel muy importante, ya que es un activo valioso y de suma importancia en cualquier tipo de organización o empresa [2]. La continua exposición en la que se encuentran, hace que existan amenazas tanto internas como externas, las cuales pueden ocasionar falta de credibilidad y daños financieros, entre otros.

Para lograr una acorde protección en los sistemas de información, es necesario ceñirse a una disponibilidad en tiempo real y de manera inmediata, siendo confidencial e integral a su vez [3]. Por consiguiente, al llevar a cabo esta tarea, es importante conocer el impacto de la vulnerabilidad en los sistemas de información, la cual se debe someter a la cuantificación de los tres tipos de métricas que el sistema Common Vulnerability Scoring System (CVSS**)** ofrece [4]. Dentro de los cuales, encontramos métricas base, métricas temporales y métricas ambientales, su función consiste en identificar y evaluar las vulnerabilidades, a través de muchas plataformas de hardware y software. Cada uno de estos grupos se compone de un conjunto de métricas, diseñadas de tal forma que son esenciales para la obtención de un resultado total y preciso, el cual puntúa y determina cuantitativamente el impacto final de una vulnerabilidad [5]. En esta oportunidad, a través de un análisis documental investigativo, se presenta el proceso a seguir ante la presencia de una vulnerabilidad, partiendo desde su sometimiento para ser calificada por las diferentes métricas, hasta la obtención de un resultado que conlleva a la inmediata y apropiada implementación del mecanismo más idóneo o política de instalación, con el fin de proteger y salvaguardar los activos de información, garantizándose así la continuidad de la organización o empresa [6]. Razones por las cuales es importante la utilización del sistema CVSS, siendo este un modelo primordial para la toma de decisiones ante la presencia de una vulnerabilidad en los sistemas de información.

II. Common Vulnerability Scoring System (Cvss)

CVSS es un sistema de puntaje, diseñado con el fin de proveer un método abierto y estándar, el cual permite estimar el impacto derivado de una vulnerabilidad identificada en las tecnologías de la información, se encuentra bajo la custodia del foro de respuesta a incidentes y equipos de seguridad (FIRST). Además, se trata de un estándar completamente abierto, es decir su acceso no es limitado, se

puede utilizar libremente [7]. Dentro de sus características principales, encontramos:

Puntuación estándar: posición neutra desde el punto de vista de las aplicaciones, aceptando la participación autónoma de diferentes organizaciones o empresas, es decir, permite calificar sus vulnerabilidades de acuerdo a un único esquema previamente establecido.

Puntuación contextualizada: cada puntuación asignada por la organización o empresa, se define o establece de acuerdo a la gravedad de la misma y, por consiguiente, al riesgo que acarrea.

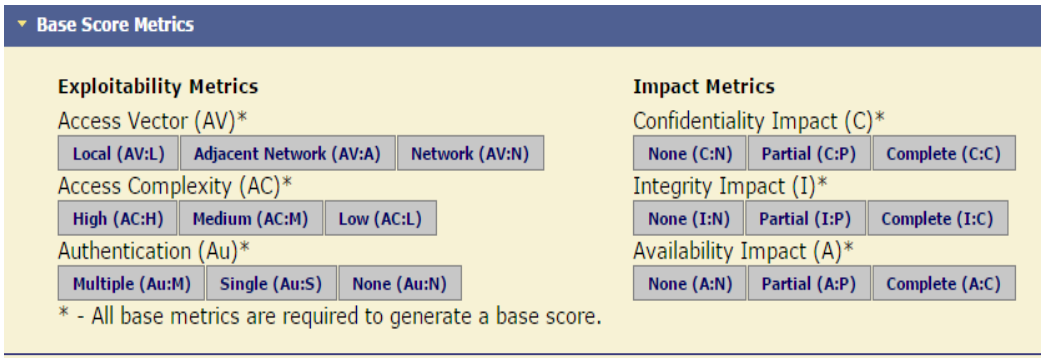
Sistema abierto: todos aquellos parámetros que permiten deducir la puntuación de una vulnerabilidad, se sustentan en un razonamiento lógico del cual se desprende una fácil diferenciación de puntuaciones [8].

Para iniciar el proceso de funcionalidad de la CVSS, se somete la vulnerabilidad encontrada a una base de datos estandarizada de vulnerabilidades públicamente reconocidas, como: National Vulnerability Database (NVDB), Common Vulnerabilities and Exposures (CVE) u Open Source Vulnerability Database (OSVDB). Las puntuaciones a continuación obtenidas se basan en una serie de mediciones (llamadas métricas), definidas así en base a la evaluación de expertos [9]. Dichas puntuaciones, van en una escala del 0 hasta 10, la cual permite clasificar las vulnerabilidades, así: el nivel alto va en el rango de 7 a 10, el nivel medio va en el rango de 4, 0 a 6, 9 y el nivel bajo va en el rango de 0 a 3, 9 [10].

El sistema CVSS está compuesto de tres grupos de métricas: métricas base, métricas temporales y métricas ambientales, cada una consistente de un conjunto de métricas [11]. El propósito del grupo de métricas base CVSS es definir y comunicar las características fundamentales de una vulnerabilidad. Este enfoque objetivo a las vulnerabilidades, permite proporcionar a los usuarios una representación clara e intuitiva de una vulnerabilidad. De igual forma, los usuarios pueden invocar los grupos temporales y ambientales para proporcionar información contextual que refleja con mayor precisión el riesgo a su entorno único, situación que conlleva al usuario a tomar decisiones más informadas, dirigidas a mitigar los riesgos que plantean las vulnerabilidades [12].

A. Métrica Base

Representa las características intrínsecas y fundamentales de una vulnerabilidad, constantes en cuanto al entorno de tiempo y de usuario. El vector Access, Acceso Complejidad, y las métricas de autenticación captan cómo se accede a la vulnerabilidad, infiriendo si se requieren o no de condiciones adicionales para explotarla [13]. Dentro de esta métrica, hay tres indicadores de impacto, los cuales miden cómo una vulnerabilidad explota o afecta directamente a un activo de TI. Dichos impactos se definen independientemente, como el grado de pérdida de confidencialidad, integridad y disponibilidad, por ejemplo, una vulnerabilidad podría provocar una pérdida parcial de la integridad y la disponibilidad, pero sin pérdida o afectación de confidencialidad [14].



Fuente: https://nvd. nist. gov/cvss. cfm?calculator&version=2

Fig. 1. Calculadora métricas base.

Según la Fig. 1, podemos encontrar el conjunto de métricas cuantitativas integrantes de la métrica base:

Acceso Vectorial (AV). Esta métrica tiene como función reflejar cómo se explota la vulnerabilidad, teniendo en cuenta unos valores posibles, previamente establecidos a través del sistema estandarizado. Para la aplicación de esta métrica, la mayor puntuación es reconocida como la más remota de un atacante, es decir, puede atacar directamente a un anfitrión de una vulnerabilidad [15].

Las puntuaciones obtenidas se ubican dentro de un margen de evaluación, posicionando el grado de gravedad de la vulnerabilidad. Para este proceso, existen tres posibles ubicaciones, denominadas así: Local (L), corresponde a aquellas vulnerabilidades explotables por medio de accesos locales, es decir, que el componente no está obligado a la pila de red, requiriendo que el atacante tenga el acceso físico al sistema vulnerable o a una cuenta Shell local, desarrollando ampliamente sus capacidades de lectura y escritura. Ejemplos de ataques periféricos como DMA Firewire/USB y escaladas de privilegios locales SUDO [16], son los siguientes: Red (A), son aquellas vulnerabilidades explotables con acceso a la red adyacente, requieren que el atacante tenga acceso a la red, es decir, a cualquier dominio de la colisión del software vulnerable, Bluetooth, IEEE 802. 1, o a un segmento de internet local. Por ejemplo, el ataque a un ARP (IP v4), conduciendo a una denegación de servicio en el segmento LAN local [17]; Red (N), corresponde a aquellas vulnerabilidades explotables con acceso a la red, significando entonces que el componente vulnerable debe estar unido a la pila de la red. Sitio donde el atacante toma la ruta de un ataque dirigido a la capa OSI 3, no siendo necesaria la conexión a una red local. Una vulnerabilidad de este tipo se denomina a menudo "explotable remotamente". Por ejemplo, un desbordamiento de búfer de RPC [18].

Complejidad de Acceso (AC). Esta métrica contiene las condiciones de complejidad del ataque, requiriendo para la explotación de la vulnerabilidad que el acceso al sistema objetivo esté a disposición del atacante. Por ejemplo, considerar un desbordamiento de buffer en un servicio de Internet da paso a ubicar un sistema objetivo, favoreciendo dicha situación para el atacante, el cual podrá lanzar exploit cada vez que lo decida [19]. La puntuación derivada de este proceso, oscilará entre la siguiente calificación: Alto (H), es necesaria la existencia de un requisito previo para los métodos de ingeniería social, conllevando a que se puedan detectar fácilmente, por personas con conocimientos en el área de estudio; Medio (M), la existencia de un requisito previo para el sistema vulnerable, cuando se encuentre en ejecución, obedece a una configuración poco común, no predeterminada por el sistema [20]; Baja (L), no existen condiciones especiales para el acceso a la vulnerabilidad, puede ser visto como cuando el sistema está disponible para un gran número de usuarios.

Autenticación (AU). La siguiente métrica mide el número de veces que un atacante accedió al sistema, debiendo autenticarse hacia un objeto para explotar una vulnerabilidad. Por consiguiente, esta métrica no mide la complejidad del proceso de autenticación, sino el requerimiento por parte del atacante de facilitar las credenciales ante la ocurrencia de un exploit [21]. A continuación, encontramos los valores para esta métrica: Varios (M), explotar la vulnerabilidad requiere la autenticación del atacante dos o más veces; Individual (S), el atacante debe autenticarse una vez, con el fin de aprovechar la vulnerabilidad; Ninguno (N), no hay ningún requisito para que el atacante se autentique [22]. Estas métricas deben ser aplicadas basándose en la autenticación requerida por el atacante antes de lanzar un ataque.

Métricas de Impacto. Esta clase de métricas mide el impacto que sufrió la confidencialidad de una vulnerabilidad explotada satisfactoriamente, tiene en cuenta que la confidencialidad limita el acceso a la información, y su presentación únicamente es viable a usuarios autorizados [23].

Impacto de Confidencialidad (C). Esta métrica mide el impacto de la confidencialidad de las fuentes de información gestionados por un componente de software, debido a una vulnerabilidad explotada con éxito [24]. Ninguno (N), no existe impacto en la confidencialidad del sistema; Parcial (P), existe una considerable exposición de información, por consiguiente es posible el acceso a algunos archivos del

sistema; Completo (C), existe una exposición total de información. Asimismo, el atacante está libre para leer todos los archivos del sistema, incluyendo la memoria [25].

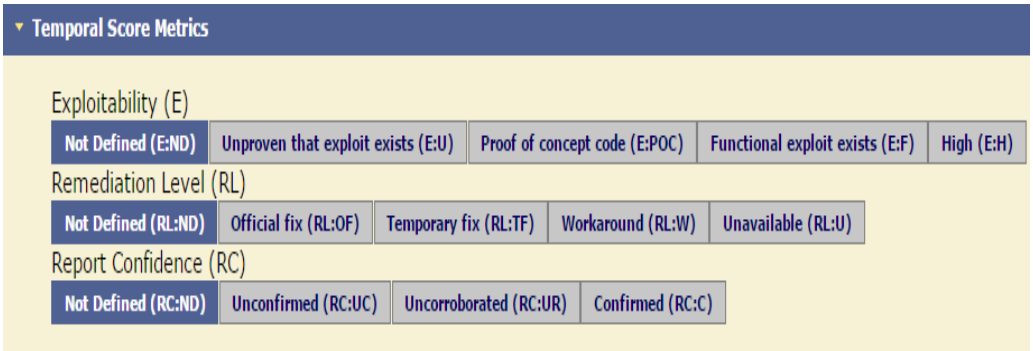
Impacto de Integridad. Esta métrica mide el impacto sobre la integridad de una vulnerabilidad explotada satisfactoriamente. La integridad se refiere a la confiabilidad y garantía de veracidad de la información [19]. Los valores posibles para esta métrica están a continuación: Ningún (N), no existe impacto a la integridad del sistema; Parcial (P), es posible la modificación de algunos archivos del sistema o información; Completo (C), existe un compromiso total de la integridad del sistema. Existe una completa pérdida de protección del sistema [26].

Impacto de Disponibilidad. La métrica mide el impacto a la disponibilidad del componente afectado como resultado de una vulnerabilidad explotada con éxito. La disponibilidad se refiere a la accesibilidad de los recursos de información, por ejemplo los ataques que consumen ancho de banda, ciclos de procesador, o espacio en disco, que impactan la disponibilidad de un sistema [27]. Ningún (N), no existe impacto en la disponibilidad del sistema; Parcial (P), existen interrupciones o desempeño reducido en la disponibilidad del recurso. Un ejemplo es un ataque de inundación basado en red, el cual permite un limitado número de conexiones exitosas hacia un servicio de Internet [28]; Completo (C), existe un reinicio total del recurso afectado. El atacante puede hacer el recurso completamente no disponible [29].

B. Métricas de Puntuación Temporales

Este segundo grupo corresponde a las métricas temporales, las cuales representan las características de una vulnerabilidad que puede cambiar en el tiempo, pero que son constantes en el ambiente de un usuario [30]. Debido a que los riesgos planteados por una vulnerabilidad pueden cambiar a lo largo del tiempo, se consideran tres factores que influyen en ello: confirmación de los detalles técnicos de la vulnerabilidad (explotabilidad), el nivel de remediación y el reporte de confianza, referido a la disponibilidad del código o técnicas que permitan la explotación. Estas métricas son opcionales e incluyen un valor que no afecta a la evaluación cuando un usuario cree que la métrica en particular no existe y quiere omitirla [31].

Con la captura de este pantallazo, podemos apreciar el conjunto de métricas cuantitativas integrantes de la métrica temporal (ver Fig. 2):



Fuente: https://nvd. nist. gov/cvss. cfm?calculator&version=2

Fig. 2. Calculadora métricas temporales.

Explotabilidad (E). Esta métrica mide la probabilidad de la vulnerabilidad de ser atacada, y se basa normalmente en el estado actual de explotación de técnicas o disponibilidad de código, igualmente la existencia de los parches o soluciones, o la confianza que uno tiene en la descripción de una vulnerabilidad [32]. No probada (U), sin código de explotación se encuentra disponible; Prueba de concepto (p), explotar ataques de código o de demostración están disponibles; Funcional (F), el código funcional del exploit está disponible [33]; Alto (H), la vulnerabilidad es explotable por código, ningún exploit se requiere, y los detalles están ampliamente disponibles, se requiere (disparador manual), también los

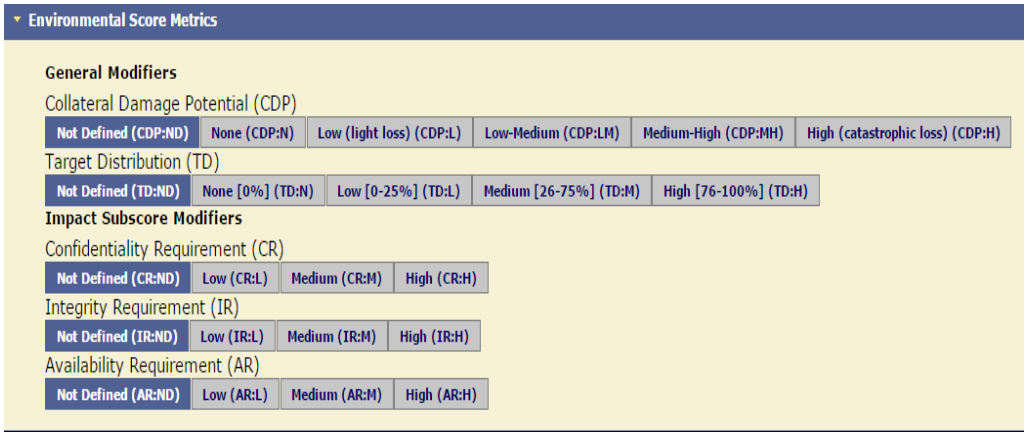
sistemas que están conectados a la red, es probable que encuentre exploración o intentos de explotación [34].

Nivel Remediación (RL). Es el nivel de saneamiento de una vulnerabilidad, es considerado un factor importante para el establecimiento de prioridades. Unas de las soluciones provisionales o revisiones se pueden ofrecer hasta que un parche oficial o actualización se establezca [35]. A continuación, encontramos la lista de los posibles valores: Arreglo temporal (T), hay una solución de mitigación oficial, temporal disponible del proveedor; Solución (W), no existe proveedor disponible, en este caso el usuario proporcionará pasos para mitigar la vulnerabilidad; No disponible (U), no hay una solución disponible, o es imposible aplicar una solución sugerida; No definido (ND), esta es una señal de ignorar o saltarse esta métrica [36].

Informe de Confianza (RC). Esta métrica mide el grado de confianza presente en una vulnerabilidad, así mismo la credibilidad de los detalles técnicos conocidos de la misma, por ejemplo, un impacto puede ser reconocido como indeseable, pero la causa raíz de ese impacto no puede ser reconocida, es decir, la vulnerabilidad puede confirmarse mediante el autor o el proveedor de la tecnología afectada [37]. A continuación, encontramos la lista de los posibles valores: Sin confirmar (UC), existen informes de huellas que nos indican que la vulnerabilidad está presente; No corroborada (UR), múltiples fuentes que en términos generales están de acuerdo y señalan que puede haber cierto nivel de incertidumbre que queda sobre la vulnerabilidad [38]; Confirmado (C), reconocido y confirmado por el proveedor o fabricante del producto afectado; No definido (ND), esta es una señal de ignorar [39].

C. Métricas Ambientales

Las métricas ambientales usan la base y la puntuación temporal actual para evaluar la gravedad de una vulnerabilidad en el contexto de la forma en que el producto o software vulnerabilidad se despliega, permitiendo al analista personalizar la puntuación de la importancia de un activo de una organización o empresa en la TI [40]. Esta medida se calcula subjetivamente, por lo general, por las partes afectadas. Las métricas ambientales son opcionales, incluyen cada una un valor de métrica, el cual no tiene ningún efecto, no se aplica y si se desea, se puede pasar por alto [41].



Fuente: https://nvd. nist. gov/cvss. cfm?calculator&version=2

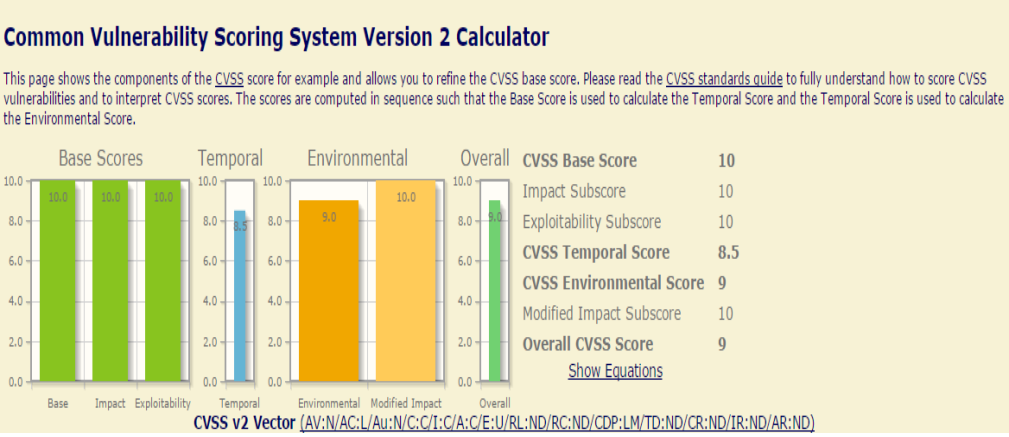
Fig. 3. Calculadora métrica ambiental.

Con la captura de este pantallazo (ver Fig. 3), podemos apreciar el conjunto de métricas cuantitativas integrantes de la métrica ambiental, las cuales son: Daño Potencial Colateral (CDP), esta métrica es la pérdida potencial de un impacto o en cualquiera de los activos físicos, tales como equipos y la vida, o el impacto financiero de la organización, que afectada de la vulnerabilidad, es explotada[42]; Daño Colateral Potencial, hace referencia al daño que puede ocasionar a terceros, como a personas, bienes físi-

cos, la productividad o beneficios[43]. Distribución de Objetivos, aquí medimos la proporción de sistemas vulnerables en el entorno, se suele dar valor numérico entre 0 y 10; y se expresa en intervalos de mínimo y máximo [44]. Modificadores de las subpuntuaciones de impacto, tienen como función identificar el grado de afectación dentro de los objetivos de la seguridad, como son: la confidencialidad, integridad y disponibilidad. Es decir, mediante estos valores podemos medir cuán importante es para esta vulnerabilidad cada uno de estos parámetros [45].

D. Cálculo CVSS

Finalmente, una vez evaluados todos los parámetros a seguir y explicado cada uno de ellos, podemos recalcular el CVSS de la CVE-2014-7169 usando el propio sistema de cálculo que nos facilita NVD (CVSS v2 calculadora), y obtendremos el siguiente resultado [46], como muestra la Fig. 4.



Fuente: https://nvd.nist.gov/cvss.cfm?calculator&version=2

Fig. 4. Cálculo con CVSS v2 de una vulnerabilidad.

Con la captura de este pantallazo, podemos a preciar el cálculo de una vulnerabilidad en sus diferentes entornos a que está expuesta la vulnerabilidad [47]. Al finalizar las medidas de los tres vectores de métricas para analizar la vulnerabilidad, teniendo en cuenta los diferentes entornos donde se encuentra la misma, la calculadora CVSS nos muestra los resultados del promedio de ponderados y puntuaciones del riesgo que puede ocasionar los diferentes tipos de vulnerabilidad [48]. El vector completo para CVE-2014-7169 quedaría de la siguiente forma:

CVSS v2=(AV: N/AC: L/Au: N/C: C/I: C/A: C/E: U/RL: ND/RC: ND/CDP: LM/TD: ND/CR: ND/IR: ND/AR: ND) [49].

Esta fórmula proporciona todas las aproximaciones matemáticas de las combinaciones métricas clasificadas en un orden de gravedad, mediante la asignación de las posibles combinaciones métricas clasificadas en un orden de gravedad [50].

III. Discusión

La constante evolución de las tecnologías de la información, desde el punto de vista empresarial u organizacional, se enfoca en dar respuesta a las necesidades de los clientes y, por ende, a marcar un factor diferenciador de competencia. Este escenario de alta conectividad ha conllevado a la existencia de mayores riesgos en el manejo de la seguridad de la información, convirtiéndose esta en el motor esencial tanto para su funcionamiento como para la toma de decisiones estratégicas. En ocasiones, la pérdida de información obedece a factores accidentales o malintencionados, los cuales traen consigo daños económicos, desprestigio e incluso consecuencias irremediables.

Como se puede apreciar, es fundamental para la seguridad de la información tener claro el modelo que se va a implementar para las vulnerabilidades existentes, puesto que el fin principal de las organi-

zaciones no solo radica en ser más productivas sino en la protección ante cualquier tipo de ataque. Por esta razón, el sistema CVSS participa de una manera eficiente en este proceso, demostrando ser la base esencial que la industria de seguridad necesita, su característica principal radica en medir con una puntuación estándar, contextualizada y un sistema abierto, y soportado en métricas ofrece la posibilidad de conocer las características individuales de cada vulnerabilidad. Lo cual permite crear criterios de certeza para la gestión de las mismas, acudiendo de forma prioritaria, oportuna y consciente a las medidas de seguridad que se desean implementar.

Finalmente, el sistema CVSS clasificará la vulnerabilidad en función de si está afectada la disponibilidad, la fiabilidad y seguridad de los sistemas de información. Así mismo, su diseño está estructurado de tal forma que es de fácil entender para un público en general, permitiendo a cualquier organización o empresa priorizar el orden en que se deben abordar las diferentes vulnerabilidades presentes en las tecnologías de la información (TI).

IV. Conclusiones

Frente a los ataques que puede sufrir un sistema de la información, debido a la presencia de una vulnerabilidad, existen varios mecanismos para poder mitigar el riesgo. De acuerdo a la anterior investigación documental, se ofrece la posibilidad de adquirir conocimiento sobre la calculadora CVSS, información que suministra la utilización de la misma como una buena elección.

En la calculadora CVSS, en el vector de acceso, nos da detalles de la ubicación de un atacante en un instante de llevar a cabo una explotación en diferentes contornos de los sistemas de información.

Con esta calculadora CVSS, definimos un estándar de ponderaciones para obtener una puntuación exacta de la vulnerabilidad.

En este análisis documental, obtenido a través de la calculadora CVSS, se logró deducir que es muy útil para calcular el impacto de una vulnerabilidad, así como también para poder generar políticas de seguridad en los sistemas de información. Se puede controlar la metodología adoptada en el análisis de la vulnerabilidad CVSS y ayuda a las organizaciones a tener un mayor control sobre sus activos, minimizando las amenazas.

Referencias

[1] P. Mell, K. Scarfone, andS. Romanosky, Una guía completa al Common Vulnerability Scoring System Version 2. 0, Foro de Respuesta a Incidentes y Equipos de Seguridad. [Online]. Available: http://www.first.org/cvss/cvss-guide.html.

[2] R. Welive security, Vulnerabilidades: qué es CVSS y cómo utilizarlo, 2014. [Online]. Available: http://www.welivesecurity.com/la-es/2014/08/04/vulnerabilidades-que-es-cvss-como-utilizarlo/.

[3] H. Holm, and M. Anderson, Análisis empírico del sistema de nivel de métrica de vulnerabilidad a través de ataques reales, computación confiable y seguro, IEEE Transaction. [Online]. Available: http://ieeexplore.ieee.org/xpl/abstractCitations.jsp?reload=true&tp=&arnumber=5591391&url=http%3A%2F%2Fieeexplore. ieee. org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5591391

[4] PCI Security Standards Council, Data Security Standard. [Online]. Available: https://www.pcisecuritystandards. org/documents/pci_dss_v2.pdf.

[5] S. H. Houmba, N. L. Virginia Franqueirab, and E. A. Engumc, "Quantifying security risk level from CVSS estimates of frequency and impact", Journal of Systems and Software, vol. 83, no. 9, pp. 1622–1634, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0164121209002155

[6] M. Schiffman, Common Vulnerability Scoring System (CVSS). [Online]. Available: https://www.first.org/cvss/specification-document

[7] H. Jara, andF. G. Pacheco, Ethical Hacking: implementación de un sistema para la gestión de seguridad. [Online]. Available: https://books.google.com.co/books?id=joMlAU-4seLYC&pg=PA135&lpg=PA135&dq=cvss+hacking&source=bl&ots=soDd2cGVdE&sig=XRbGSEp9QcjvBzP_764L1dbBHBk&hl=es&sa=X&ved=0ahUKEwiVwevl7avKAhWDHB4KHVGjD0UQ6AEIMDAD#v=onepage&q=cvss%20hacking&f=false

[8] FIRTS, Políticas de privacidad. [Online]. Available: http://www.usfirst.org/.

[9] P. Mell, K. Scarfone, and S. Romanosky, A Complete Guide to the Common Vulnerability Scoring System Version 2. 0. [Online]. Available: https://www.first.org/cvss/cvss-v2-guide.pdf

[10] OpenBSD, AnonCVS. [Online]. Available: http://www.openbsd.org/anoncvs.html.

[11] A. Caballero, Introducción A CVSS. [Online]. Available: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc112/p533528_A1b.pdf.

[12] FIRST, Common Vulnerability Scoring System v3. 0: Specification Document. [Online]. Available: https://www.first.org/cvss/v2/meetings.

[13] FIRST, Métricas SIG. [Online]. Available: https://www.first.org/meetings/nm-sig.

[14] FIRST, Métricas SIG. [Online]. Available: https://www.owasp.org/images/1/19/Owasp-ciso-guide_es.pdf.

[15] INSIBE Instituto Nacional de Ciberseguridad de España, Métricas de evaluación de CVSS 3. 0. [Online]. Available: http://www.incibe.es/blogs/cat/Seguridad/BlogSeguridad/Articulos_seleccionados/?categoryID=1000080657.

[16] J. Jiménez Unzueta, Auditoría de Sistemas y Código. [Online]. Available: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/2736/Tesina.pdf?sequence=1

[17] M. A. Hernández, CVSS, Calculadora de métricas y vulnerabilidades, 2012. [Online]. Available: https://seguinfo.wordpress.com/2012/10/10/cvss-calculadora-de-metricas-y-vulnerabilidades/

[18] Richrumble, Stoned boot DIDN'T work that way (at first). [Online]. Available: https://codex.wordpress. org/Theme_Development

[19] JVNRSS, CVSSv2, Feasibility Study Team. [Online]. Available: http://jvnrss. ise.chuo-u.ac.jp/jtg/cvss/es/CVSSv2.html.

[20] IPA, Reporting Status of Vulnerability-related Information about Software Products and Websites. [Online]. Available: http://www.ipa. go. jp/files/000033082.pdf

[21] Vulnerability Chaser, Herramienta para la gestión de vulnerabilidades. [Online]. Available: http://ibrapk.github.io/Vulnerability-Chaser/

[22] C. Rincón, Análisis de vulnerabilidades - Seguridad Informática. [Online]. Available: https://seguridadinformaticaufps.wikispaces.com

[23] Highsec, Cómo Valorar Nuestras Vulnerabilidades en nuestra Auditoría – parte I - Calcular CVSS Base Score. [Online]. Available: http://highsec.es/.../como-valorar-las-vulnerabilidades-en-nuestra-auditoria-par.

[24] CLCERT-ED07-006, El Common Vulnerability Scoring System (CVSS). [Online]. Available: http://www.clcert. cl/show. php?xml=xml/editoriales/doc_07-06.xml&xsl=xsl/editoriales.xsl.

[25] IBM, Puntuaciones CVSS, IBM Security AppScan Enterprise 9. 0. [Online]. Available: http://www.ibm.com/developerworks/ssa/xml/tutorials/x-epubtut/

[26] IBM, Valores CVSS. [Online]. Available: http://www.01. ibm.com/support/knowledgecenter/SSPH29_9.0.1/com.ibm.help.common.infocenter.aps/r_CVSSSettings014.html?lang=es.

[27] Docplayer, Recomendación UIT-T X.1521 - Sistema común, Sistema común de puntuación de vulnerabilidades. [Online]. Available: http://docplayer.es/1874436-Seguridad-informatica-y-proteccion-de-datos.html

[28] M. A. Sánchez, Priorización de vulnerabilidades técnicas con CVSS2.0, 2015. [Online]. Available: https://technologyincontrol2.wordpress.com/2015/01/23/priorizacion-de-vulnerabilidades-tecnicas-con-cvss-2-0.

[29] Seguridad Apple, Criticidad de un Bug: Common Vulnerability Scoring System, 2012. [Online]. Available: http://www.seguridadapple.com/2012/03/criticidad-de-un-bug-common.html

[30] H. Jara, and F. G. Pacheco, Ethical Hacking 2. 0, 2009, p. 353. [Online]. Available: https://books.google.com.co/books?id=joMlAU4seLYC&pg=PA136&lpg=PA136&dq=impacto+de+integridad+cvss&source=bl&ots=soCkX6M_5E&sig=D2yWkWZtPqSlkDS1-mVJniV87LI&hl=es-

[31] Asset, CVSS Calculator - French Version, CVSS 2.0. [Online]. Available: http://asset.rue89.com/files/AmbroiseBouleis/Microsoft%20Security%20Intelligence%20Report%20volume%206%20-%20Key%20Findings%20Summary%20-%20French.pdf

[32] RedHat, Clasificación de severidad e impacto de los parches de seguridad de JBoss. [Online]. Available: https://access.redhat.com/documentation/es-ES/JBoss_Enterprise_Application_Platform/6.2.

[33] Magazcitum, Retomando el valor de un análisis de vulnerabilidades. [Online]. Available: http://www.magazcitum.com.mx/?p=1805#.Vl-yzHYvfIU.

[34] Scribd, Una Guía para Construir Aplicaciones y Servicios Web Seguros, 2nd ed. (Black Hat), OWASP, 2005. [Online]. Available: https://es.scribd.com/doc/284988164/OWASP-Development-Guide-2-0-1-Spanish

[35] INTECO, Qué son las vulnerabilidades del software. [Online]. Available: http://www.egov.ufsc.br/portal/sites/default/files/vulnerabilidades_notasobs.pdf.

[36] DarFe, Proceso de hacking Ético. [Online]. Available: http://149.62.170.30/joomla/index.php/2-uncategorised/15-presentacion-he

[37] L. E. Ramírez, and W. G. Rodríguez, Seguridad informática, 2012. [Online]. Available: http://seguridadinformaticaufps.wikispaces.com/.../Actividad+en+Clase.doc

[38] Eleventphats, Ocho siglas relacionadas con las vulnerabilidades (III): CVSS. [Online]. Available: http://blog.elevenpaths.com/2014/04/ocho-siglas-relacionadas-con-las.html.

[39] Qualys, CVSS Escoring-Qualys, CVSS y su puntuación, 2013. [Online]. Available: https://qualysguard.qualys.com/.../cvss_scoring.htm

[40] FIRTS, Preguntas frecuentes de FIRTS, 2014. [Online]. Available: https://www.first.org/cvss/specification-document.

[41] CVSS-CISCO, Common Vulnerability Scoring Systems, 2014. [Online]. Available: http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html.

[42] CVSS-CISCO, Métricas Temporales, 2014. [Online]. Available: http://www.cisco.com/web/about/.../cvss-qandas.html.

[43] BLACKBERRY, Sistema de Calificación de Vulnerabilidades Comunes Temporales, 2015. [Online]. Available: http://global.blackberry.com/es/.../common-vulnerability-scoring.html.

[44] Tenable Network Security, CVSS Relación Temporal, 2014. [Online]. Available: https://www.tenable.com/sc-dashboards/cvss-temporal-ratio.

[45] J. A. Wang, F. Zhang, and M. Xia, Temporal Metrics for Software Vulnerabilities, 2009. [Online]. Available: http://www.cs.wayne.edu/fengwei/paper/wang-csiirw08.pdf.

[46] P. Mell, K. Scarfone, and S. Romanosky, Una complete Guía de la Common Vulnerability Scoring System (CVSS), Versión 2.0, 2006. [Online]. Available: http:// firts.org/cvss/cvss-gude.html.

[47] J. A. Wang, Modelos de seguridad de la información y métricas, Actas de ACM, Conferencia Sudeste, vol. 2, pp. 178-184.

[48] Highsec, Cómo valorar las vulnerabilidades en nuestra auditoría, 2013. [Online]. Available: http://highsec.es/2013/11/como-valorar-las-vulnerabilidades-en-nuestra-auditoria-parte-i-calcular-cvss-base-score/

[49] Oracle Corporation, La actualización crítica. [Online]. Available: http://www.oracle.com/technology/deploy/security/critical-patch.

[50] CISCO, Asesor de Seguridad, Vulnerabilidad de Inspección Aplicación en CISCO: Módulo de Servicios de Firewall. [Online]. Available: http://www.cisco.com/en/US/products/products_security_advisory09186a008091b11d.shtm.