Entre Ciencia e Ingeniería, vol. 14, no. 28, julio-diciembre de 2020, páginas 46-51. DOI: https://doi.org/ 10.31908/19098367.2015.
ISSN 1909-8367 (Impreso), ISSN 2539-4169 (En línea)

Evaluación Heurística de Usabilidad utilizando Indicadores Cualitativos para Sistemas Detectores de Intrusión[1]

Usability Heuristic Evaluation Using Qualitative Indicators for Intrusion Detection Systems

C. R. Cappo y C. R. Aceval

Recibido: noviembre 25 de 2020 – Aceptado: diciembre 27 de 2020

[1]***Resumen*— La decisión de implementar en el seno de una organización un Sistema de Detección de Intrusión (IDS) puede resultar en una tarea complicada tanto del punto de vista técnico, así como de aquellos que afectan en la evaluación costo/beneficio de su uso. En este proceso de decisión/evaluación varias heurísticas combinadas con indicadores fueron propuestos focalizadas principalmente en la parte técnica de estos Sistemas. En la creación de estas heurísticas de usabilidad fuimos asistidos por un marco de trabajo (*framework*) de guías de delineamientos orientadas a los desafíos de implementación y diseño de herramientas para administrar la seguridad en tecnologías de la información (*Security Information Technology* - SIT). Expone además la experiencia de evaluar estas heurísticas en dos detectores de intrusión de tipo NIDS (*Network Intrusion Detection System*) ampliamente utilizados en el ámbito de SIT. Pretende por tanto ser una fuente de consulta para los evaluadores y profesionales de Seguridad de Tecnologías de la Información al igual que las personas encargadas de la toma de decisión de la organización.**

***Palabras clave*— heurística de usabilidad, indicadores de usabilidad, sistema de detección de intrusiones, usabilidad.**

***Abstract*— The decision to implement an Intrusion Detection System (IDS) within an organization can result in a complicated task both from a technical point of view as well as from those that affect the cost/benefit evaluation of its use. In this decision/evaluation process, several heuristics combined with indicators were proposed focused mainly on the technical part of these Systems. In creating these heuristics usability, we were assisted by a framework of guidelines of outlines oriented to the challenges of implementation and design of tools to manage security in information technology (SIT). It also presents the experience of evaluating these heuristics in two intrusion detectors of the NIDS type (Network Intrusion Detection System) widely used in the field of SIT. Therefore, it aims to be a source of consultation for evaluators and Information Technology Security professionals as well as the people in charge of decision-making in the organization.**

***Keywords*— usability heuristics, usability indicators, intrusion detection system, usability.**

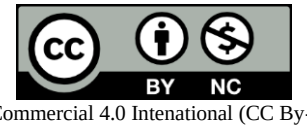
I. Introducción

La Seguridad en Tecnologías de la Información (*Security Information Technology*) en adelante SIT, es un aspecto muy importante para las organizaciones que desean proteger sus activos de amenazas internas y externas a la organización. De acuerdo con la encuesta realizada por Broadcom a varias organizaciones en el año 2019 han determinado que los *cyber* ataques son cada vez más sofisticados y han tenido un aumento considerable con relación a los últimos años. Por lo tanto, proteger la Seguridad de Información Tecnológica de una organización conlleva desafíos cada vez mayores para mitigar y proteger de estos ataques [1].

Desde el avance de la web, los usuarios han ido enfrentando dificultades de seguridad de los sistemas [2] por lo que una tarea crítica en SIT es la detección de incidentes de seguridad. Varias organizaciones dependen de tecnologías de seguridad para protegerse contra actividades maliciosas por lo que el trabajo de detectar intrusiones puede verse mejorada mediante la instalación y la puesta en marcha de sistemas que permitan facilitar y/o automatizar en alguna medida este proceso. Esto es, implementar un Sistema de Detección de Intrusión (IDS). La adopción de un IDS es motivado por varios factores tales como la presencia continua de vulnerabilidades en los sistemas de computación, el creciente número de incidentes de seguridad, la lentitud en las actualizaciones de las aplicaciones en el contexto de seguridad, los mecanismos de control de acceso que pueden ser inhabilitados o eludidos a consecuencia de malas prácticas

[1] C. R. Cappo, Universidad Nacional de Asunción, San Lorenzo, Paraguay, email:ccappo@pol.una.py.
C. R. Aceval, Universidad Nacional de Asunción, San Lorenzo, Paraguay, email:caceval@pol.una.py.

Como citar este artículo: Cappo, C. R., Aceval, C. R. Evaluación Heurística de Usabilidad utilizando Indicadores Cualitativos para Sistemas Detectores de Intrusión, Entre Ciencia e Ingeniería, vol. 14, no. 28, pp. 46-51, julio-diciembre 2020. DOI: https://doi.org/ 10.31908/19098367.2015.



en las configuraciones y, aun cuando un ataque no sea exitoso es importante conocer que existió un intento para comprometer la seguridad [3]. Un aspecto positivo obtenido del uso efectivo (mejor detección) de estos sistemas es que permiten disuadir la intención de realizar ataques a la organización [4].

Adoptar un IDS por parte de una organización no es una tarea sencilla, desde el convencimiento a las autoridades de su necesidad, la instalación y configuración, así como el mantenimiento implican muchos desafíos a los profesionales de SIT [5]. Es por ello, que este trabajo tiene como objetivo exponer las heurísticas de usabilidad aplicadas a IDS que podrían orientar a la organización en la evaluación, implementación y puesta en marcha de un IDS. En la elaboración de estas heurísticas fuimos asistidos por un marco de trabajo (*framework*) de delineamientos de diseño de herramientas de administración de SIT [5], el cual se apoya en los desafíos que enfrentan los profesionales del área de seguridad.

Este trabajo se encuentra estructurado de la siguiente forma: en la sección II presentamos los trabajos relacionados al trabajo presentado aquí. La sección III presenta los conceptos fundamentales de los IDS y el *framework* de delineamientos base utilizado. En la sección IV presentamos las heurísticas de usabilidad propuestas orientadas a la usabilidad de IDS. A fin de evaluar lo presentado en la sección anterior en V presentamos una evaluación de las heurísticas propuestas a dos reconocidos IDS para finalmente en la sección VI exponer algunas conclusiones, así como los trabajos futuros del trabajo.

II. Trabajos relacionados

Los métodos de evaluación de usabilidad han ganado una atención sustancial en las redes, particularmente en el Sistema de detección de intrusiones [6]. Las heurísticas de Nielsen [7] permiten evaluar algunos aspectos generales de usabilidad de cualquier aplicación, como la prevención de errores; control y libertad del usuario; flexibilidad y eficiencia de uso; entre otros. Sin embargo, como son “heurísticas generales”, ignoran elementos críticos de una aplicación específica. En este sentido el centro de trabajo se está moviendo hacia la usabilidad de las herramientas de seguridad [8]. Por lo tanto, es necesario desarrollar nuevas heurísticas de usabilidad específicas para evaluar características o aspectos únicos de un dominio de aplicación específico [9].

Se han encontrado algunos trabajos que describen delineamientos y recomendaciones generales de evaluación y uso de IDS [10] [11]. La mayoría de los trabajos se han enfocado en la evaluación de las características técnicas de estos sistemas, sobre todo orientado a la efectividad, por ejemplo [12]. Aunque puede decirse que la ratio de detección de los IDS es el punto fundamental de su razón de ser no puede decirse que es menos importante el proceso restante: configuración, trabajo colaborativo, emisión de reportes, documentación, visualización de alarmas entre otros. En el trabajo presentado en [2] encontramos una serie de delineamientos basados en la aplicación de evaluaciones de usabilidad [7] a fin de medir la efectividad y eficiencia de los IDS. Presenta además una evaluación de tales heurísticas a dos herramientas basadas en Snort [13]. En el trabajo presentado en [8] encontramos un conjunto de heurísticas de usabilidad considerando la sugerencia de expertos y usuarios novatos en SIT. Al igual que este trabajo presentamos una serie de heurísticas para IDS, pero a diferencia nos enmarcamos en un *framework* que intenta conjugar los desafíos organizacionales y tecnológicos que están presentes a la hora de implementar un IDS en la organización.

III. Definiciones

En esta sección se introduce conceptos fundamentales sobre usabilidad y detectores de intrusión, a fin de comprender la terminología utilizada más adelante.

A. Usabilidad.

En la literatura existen varias definiciones del concepto de usabilidad, que aportaron puntos de vista diferentes y complementarios en cada área de investigación. La norma ISO 9241-11 ha logrado proporcionar una definición aceptada internacionalmente sobre lo que es la usabilidad y su aplicación en varios campos [14].

Esta norma define la usabilidad como “la medida en que un producto puede ser utilizado por usuarios específicos para lograr objetivos específicos con *Eficacia*, *Eficiencia* y *Satisfacción* en un contexto de uso específico” [15].

Sin embargo, una definición de usabilidad generalmente aceptada todavía no existe, ya que su naturaleza compleja es difícil de describir en una definición [16].

La norma ISO 9241-11 aún está en revisión que incorpora lo aprendido sobre usabilidad desde 1998 y qué nuevos elementos han surgido en relación con el concepto de usabilidad [14].

B. Sistemas de Detección de Intrusión.

Una *intrusión* es definida como una secuencia de acciones relacionadas realizadas por una actividad maliciosa que resulta en el comprometimiento de un sistema. Una *detección de intrusión* es el proceso de identificar y responder esas actividades maliciosas. Esta definición introduce el concepto de detección de intrusión como un proceso que envuelve tecnología, personas y herramientas, y que es complementario a otros abordajes de seguridad como la encriptación y el control de acceso [3].

Un *Sistema de Detección de Intrusión* es un conjunto de herramientas de software construidas para detectar intrusiones en un sistema o en una red datos [3]. En general un IDS monitorea y registra los eventos en un sistema computacional, realiza un análisis para determinar si los mismos son incidentes de seguridad, alerta a los encargados de la seguridad de posibles amenazas y producen reportes de los eventos. Si un IDS incluye un mecanismo de bloqueo a las intrusiones detectadas entonces se denomina Sistema de Prevención de Intrusión (*Intrusion Prevention System*) o IPS [5].

Existen muchos tipos de IDS, basados en diferentes framework conceptuales. Es posible, sin embargo, reconocer

algunas estructuras comunes en ellos. Presentamos en la Tabla I los componentes básicos de los IDS y los diferentes tipos de IDS de acuerdo con varios criterios [17].

C. *Usabilidad y Framework de Guías de Delineamientos.*

La usabilidad se aplica a todos los aspectos de un sistema

TABLA I
CLASIFICACIÓN DE LOS SISTEMAS DE DETECCIÓN DE INTRUSIÓN.

Criterio	Descripción	Tipos
Método de Detección	Define la forma en como el componente de análisis opera.	SIDS: utilizan conocimiento previo a través de plantillas de ataques para detectarlos. (Signature-based Intrusion Detection System). AIDS: emiten alarmas cuando existe una desviación sustancial de lo que es normal (Anomaly-based Intrusion Detection System).
Comportamiento en la detección	Caracteriza el comportamiento del componente de respuesta.	IDS: es pasivo y se genera una alerta para el administrador en la detección. IPS: es activo y se toma una acción proactiva cuando se detecta una intrusión.
Localización de la fuente de monitoreo	Establece el lugar de donde el componente de eventos obtendrá los datos para el análisis posterior.	HIDS: los datos son generados en la misma computadora o host. (Host Intrusion Detection System). NIDS: Los datos se producen a partir del monitoreo del tráfico de red (Network Intrusion Detection System)
Frecuencia de uso	Discrimina entre sistemas en tiempo real o aquellos que lo hacen cada período de tiempo.	Online: tiempo real. Offline: por período de tiempo.

con el cual un humano puede interactuar, incluyendo procesos de instalación y de mantenimiento. Nielsen, define: "la usabilidad es un atributo de calidad que evalúa la facilidad de uso de las interfaces de usuario" y desglosa aún más el concepto en los siguientes cinco componentes de calidad [7]: *Facilidad de aprendizaje*: ¿Qué tan fácil es para los usuarios realizar tareas básicas la primera vez que encuentran el diseño? *Eficiencia*: Una vez que los usuarios han aprendido el diseño, ¿con qué rapidez pueden realizar las tareas? *Facilidad de memorizar*: cuando los usuarios regresan al diseño después de un período de no usarlo, ¿con qué facilidad pueden restablecer la habilidad? *Errores*: ¿Cuántos errores cometen los usuarios, ¿qué tan graves son estos errores y con qué facilidad pueden recuperarse de los errores? y *Satisfacción*: ¿Qué tan agradable es usar el diseño? La *International Organization for Standardization* (ISO) también define la usabilidad como una combinación de tres aspectos: *Efectividad*, *Eficiencia* y *Satisfacción* de acuerdo con el contexto de uso [15].

En este trabajo nos enfocamos en evaluar un sistema IDS, teniendo en cuenta una definición de usabilidad que considera los aspectos de *Efectividad*, *Eficiencia*, *Satisfacción*, *Facilidad de aprendizaje* y *Facilidad de memorizar*. *Efectividad* en el sentido del logro de los objetivos, *Eficiencia* teniendo en cuenta la velocidad del logro de esos objetivos, *Satisfacción* en el uso, combinando todo lo anterior con la *Facilidad de aprender* y *memorizar*.

A fin de facilitar el proceso de adopción de herramientas de SIT Jaferian *et al.* [18] proponen un *framework* de guías de delineamientos específicos para las mismas orientadas hacia la usabilidad. Este *framework* se basa en los desafíos relacionados a SIT: *Cultura y relacionamiento humano*, *Características de las organizaciones* y *Cuestiones de tecnología*.

El diseño de estos delineamientos y su agrupación se muestra en la Fig. 1, que presenta una clasificación por capas. Cada capa está focalizada hacia un conjunto diferente de desafíos (mencionados anteriormente). Las capas más bajas contienen las guías que son aplicables de forma más general, es decir a un mayor conjunto de herramientas, y las más altas establecen delineamientos que son específicos a cierto conjunto de herramientas (ejemplos: IDS, *Firewall*, etc.).

Fig. 1. Framework de guías de delineamientos de usabilidad para herramientas de SIT [18].

A continuación, presentamos una breve descripción de cada capa sugerida en el modelo de delineamientos:

1) Usabilidad General: incluye guías y recomendaciones que son aplicables a todas las herramientas para los administradores de SIT. Un ejemplo es la disponibilidad de ayuda a usuarios y documentación: disponibilidad en Internet, capacidad de búsqueda, entre otros.

2) Complejidad Tecnológica: define delineamientos relacionados al entorno de trabajo de la administración de SIT en el marco tecnológico. La estructura compleja de las redes de datos y la necesidad de varias soluciones (*firewalls*, IDS, antivirus, etc.) para el manejo de SIT crean este desafío. Los delineamientos en este desafío incluyen: herramientas combinables o integradas, soporte para compartir conocimiento y/o experiencias, múltiples métodos de presentación/interacción, múltiples niveles de abstracción de información, posibilidad de personalizar y facilidades para administrar tareas relacionadas al trabajo de seguridad.

3) Complejidad Organizacional: corresponde a otro aspecto del entorno de trabajo del administrador de SIT. Derivan de la

necesidad que el administrador pueda relacionarse con otras partes interesadas dentro de la organización. Incluye soporte para brindar facilidades en la comunicación, facilidades para mantener y guardar información de las comunicaciones con otros interesados, provisión de reportes adecuados, provisión de interfaces apropiadas para los otros interesados y delineamientos sobre trabajo distribuido (por ejemplo, soporte para trabajo colaborativo).

4) Tareas específicas: esta capa incluye delineamientos que pueden o no ser aplicables dependiendo de la naturaleza de la herramienta considerada. El primer conjunto es específico para aquellas aplicaciones o herramientas que requieren configuración intensiva, particularmente durante la implementación. El segundo conjunto es orientado a herramientas que requiere un intensivo análisis. Entre las configuraciones intensivas tenemos: facilidades para realizar configuraciones manejables, se provea soporte para analizar los resultados de aplicaciones de nuevas configuraciones y planificarlas, soporte para cambiar fácilmente las configuraciones, proveer reporte de errores comprensibles y significantes. En relación con el segundo conjunto se incluyen herramientas que permiten monitorear sistemas y generar alarmas para su posterior análisis por parte de los administradores, estos delineamientos incluyen: provisión de detección automática, de filtrado y de correlación de alarmas.

IV. Propuesta

Existen varios enfoques para desarrollar heurísticas de usabilidad, desde establecer un nuevo conjunto de heurísticas basadas en heurísticas existentes, en metodologías, en problemas de usabilidad, en teorías, en revisiones de la literatura o incluso basadas en pautas, principios o recomendaciones de diseño [9].

En este trabajo utilizamos las heurísticas de usabilidad de los IDS agrupados en categorías de acuerdo con los desafíos mencionados en el framework [18]. Una decisión importante en la confección de estas heurísticas es que no todos los delineamientos mencionados en el framework fueron tenidos en cuenta, solo aquellos que consideramos aplicables a los IDS.

A. Heurísticas de Usabilidad Propuestas.

El total de heurísticas propuestas son veintiséis (26), agrupados en seis (6) heurísticas de Usabilidad General, doce (12) heurísticas orientadas a Desafíos Tecnológicos, cuatro (4) heurísticas orientadas a la Complejidad Organizacional y cuatro (4) heurísticas de Tareas Específicas. A cada heurística se le ha asignado un código de forma a facilitar su identificación.

1) Orientados hacia la Usabilidad General.

a) H1 - Disponibilidad de CLI (Console Line Interface): una interfaz de línea de comandos es generalmente familiar para un profesional de SIT. Su presencia en un IDS solo tiene sentido cuando a partir de esta interfaz pueden ser ejecutadas tareas más complejas o visualizar configuraciones más sofisticadas.

b) H2 - Disponibilidad de GUI (Graphic User Interface) para administración y configuración: de forma a facilitar la configuración, monitoreo o análisis es conveniente que el IDS pueda tener una interfaz gráfica. Es importante que los datos que se presentan representen significativamente el funcionamiento del sistema, especialmente lo referido a la emisión de alertas y el nivel de compromiso de las mismas.

c) H3 - Documentación Técnica Disponible (en línea e impresa) incluyendo limitaciones del sistema.

d) H4 - Disponibilidad de Foros de Usuarios.

e) H5 - Disponibilidad de mecanismos de control de acceso.

f) H6 - Disponibilidad de diversas Fuentes de Evaluación de características y Capacidades: En el proceso de evaluación de un IDS es importante poseer información no solo del fabricante o constructor del mismo sino también de otras fuentes. En especial es significativo el hecho de tener claro las capacidades y limitaciones del sistema a fin de que se adecuen a las necesidades de la organización.

2) Orientados hacia la Complejidad Tecnológica.

a) H7 - Integración con otros Sistemas SIT y/o Productos relacionados.

b) H8 - Seguridad de los Componentes que integran el IDS: define la habilidad que tiene el IDS para que sus componentes (sensores, base de datos, consolas, etc.) no sean vulnerables a ataques.

c) H9 - Provisión de API de Integración con otras Herramientas: permite ampliar las capacidades del IDS utilizando otros componentes programados externamente.

d) H10 - Fácil Identificación de las Configuraciones aplicadas: define la facilidad que tiene el entorno del IDS para indicar la versión de la configuración que está en producción.

e) H11 - Facilidades para revertir los cambios aplicados.

f) H12 - Mantenimiento de versiones de las configuraciones aplicadas.

g) H13 - Disponibilidad de indicadores adecuados de funcionamiento: define la facilidad que da el entorno para brindar información sobre los indicadores de funcionamiento del IDS.

h) H14 - Mensajes y alertas en formatos estandarizados: define la facilidad del IDS para interactuar con otros productos de igual objetivo.

i) H15 - Definición de prioridades de alertas.

j) H16 - Soporte de técnicas de evasión: define la facilidad que brinda el IDS para hacer frente a técnicas de evasión, como por ejemplo la incorporación en el IDS de *encoding* recursivo.

k) H17 - Facilidades de relacionar eventos de diferentes fuentes: define las facilidades que otorga el entorno para utilizar información de otros sistemas para verificar eventos sospechosos.

l) H18 - Filtrado de alertas según criterios predefinidos o aprendidos: establece la posibilidad de ordenar con algún criterio de prioridad las alertas emitidas y

focalizarle en aquellas que realmente pueden ser de riesgo a la organización.

3) *Orientados hacia la Complejidad Organizacional.*

a) *H19 - Registro y seguimiento de incidentes de seguridad relacionados al IDS:* define la posibilidad de que pueda documentarse las amenazas a la organización de forma a aplicar medidas de seguridad para proteger los recursos de la misma.

b) *H20 - Funcionamiento distribuido de sensores y/o analizadores.*

c) *H21 - Facilidades de interactuar con otras actividades de administración:* define las facilidades del entorno para que el administrador pueda interrumpir sus tareas y volver a retomarlas sin tener que volver a empezar desde el principio.

d) *H22 - Soporte de scripting y automatización:* define las facilidades que brinda el IDS para automatizar tareas repetitivas y la posibilidad de realizar cierto grado de programación en ellas.

4) *Orientados a Tareas Específicas.*

a) *H23 - Inclusión de diferentes tecnologías para mejorar la capacidad de detección*: define las alternativas del IDS de poseer técnicas de detección híbridas al igual que posibilidades de correlación de alarmas a fin de mejorar la calidad de la detección.

b) *H24 - Facilidades para manejar configuraciones complejas:* existencia de configuraciones ejemplo, existencia de configuraciones guiadas, etc.

c) *H25 - Generación de configuraciones para prueba:* define la facilidad que brinda el entorno del IDS para generar configuraciones de prueba sin necesidad de cambiar configuraciones en producción.

d) *H26 - Ambiente de simulación para aplicar configuraciones de prueba:* aplicar configuraciones de prueba en un ambiente simulado antes de colocarlas en producción, de esta forma se reduciría el riesgo de errores en las nuevas configuraciones.

V. Evaluación

A fin de aplicar las heurísticas de usabilidad se seleccionaron dos IDS. En esta sección se explica la razón de la selección de estos, una breve descripción y un cuadro comparativo con la evaluación realizada.

A. Descripción de IDS Seleccionados.

A fin de realizarlas validaciones de usabilidad ajustadas al framework de herramientas de administración de SIT [18] se seleccionaron dos IDS de código abierto conocidos en el ámbito de los detectores de intrusión (Snort y Zeek). Por una cuestión de costos, se optó por seleccionar aquellos IDS basados en software dejando de lado aquellos que se encuentran integrados a un equipamiento (*hardware*) específico. Todos son de tipo NIDS. Actualmente este tipo de IDS son los más utilizados dentro del ámbito de seguridad de las organizaciones, debido a que un mayor porcentaje de los incidentes envuelven acceso a través de la red de datos en las organizaciones [1].

A continuación, se describen los IDS utilizados:

1) *Snort [13]:* es un IDS de código abierto también de tipo NIDS que puede actuar en modo de monitoreo pasivo (*sniffer*), como recolector de información del tráfico de red o como un NIDS con capacidad de responder a los ataques. Su configuración se basa en la detección de firmas o formas de ataques conocidos, conocido como *snort-rules*. En este último caso funcionaría como un IPS.

2) *Zeek:* anteriormente BRO [19] es un IDS de código abierto de tipo NIDS que monitorea pasivamente el tráfico de red en busca de posibles actividades sospechosas. Su esquema básico es basado en análisis de comportamientos basados en políticas previamente definidas a través de un lenguaje propio del IDS. En este sentido es un IDS que puede ser configurado para funcionar como Snort, por firmas o en su efecto puede ser utilizado para analizar anomalías en el tráfico de datos. Su propuesta fue engendrada en el *Network Research Group*, del *Lawrence Berkeley National Laboratory*.

B. Resultados.

Para la evaluación de las heurísticas de usabilidad, se utilizaron varios indicadores que se indican en la Tabla II:

Tabla II
Indicadores Cualitativos.

Indicador	Descripción
NC	No cumple
CP	Cumple parcialmente
C	Cumple

En la Tabla III se presenta un resumen de la evaluación a los sistemas detectores de intrusión mencionados en la sección V-A. Es posible observar que la cantidad de heurísticas propuestas abarcan todos los aspectos que afectan la evaluación, implementación y mantenimiento de un IDS dentro de la organización.

Tabla III
Resultados de la Evaluación para Snort y Zeek.

Categoría	Indicador	Snort	Zeek
Usabilidad General (6)	C	3	3
	CP	0	1
	NC	3	2
Complejidad Tecnológica (12)	C	5	7
	CP	2	0
	NC	5	5
Complejidad Organizacional (4)	C	0	3
	CP	1	0
	NC	3	1
Tareas Específicas (4)	C	1	3
	CP	1	1
	NC	2	0
Resumen			
IDS	C	CP	NC
Snort	9	4	13
Zeek	16	2	8

Al evaluar el cuadro de resultados, es posible observar que las mismas son bastante exigentes, ninguno pudo llegar a cumplir con todas las heurísticas de usabilidad. Aunque Snort y Zeek son de carácter libre y carecen de interfaces de configuración y visualización de datos, puede decirse que la ventaja que tienen es su facilidad de adecuación a la organización, su sencillez de aplicación y la posibilidad de extender sus capacidades con otros componentes externos.

VI. Conclusiones y trabajos futuros

En este trabajo hemos propuesto un conjunto de heurísticas enfocadas en la usabilidad de los IDS asistidas por un *framework* de delineamientos basados en desafíos. Estos desafíos no solo abarcan aspectos tecnológicos sino también aspectos humanos y organizacionales, los que en su mayoría se convierten en tareas complejas el tener que elegir, implementar, operar y mantener un Sistema de Detección de Intrusión. A fin de proponer una forma de uso de estas heurísticas, hemos evaluado dos IDS de código abierto. Queda como un trabajo futuro la evaluación a un mayor número de IDS. Como la evaluación fue realizada con IDS/IPS basados en software, una posible extensión sería realizar en otros IDS basados en hardware teniendo en cuenta que este tipo de implementación es la que se ofrece con mayor fuerza en el mercado de SIT.

Al tener disponible esta lista de heurísticas específicamente enfocadas a IDS creemos que los profesionales de SIT se verán apoyados al momento sobre todo de evaluar la implementación y puesta en marcha de un Sistema de Detección de Intrusión.

Referencias

[1] Broadcom, “Internet Security Thread Report - ISTR”, Symantec Corp., Mountain View, CA, Feb. 2019. [Online]. Available: https://docs.broadcom.com/doc/istr-24-2019-en

[2] A. T. Zhou, J. Blustein and N. Zincir-Heywood, "Improving intrusion detection systems through heuristic evaluation," Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No.04CH37513), Niagara Falls, Ontario, Canada, 2004, pp. 1641-1644 Vol.3, doi: 10.1109/CCECE.2004.1349725.

[3] Kruegel, C., Valeur, F., and Vigna, G. (2004). “Intrusion detection and correlation: challenges and solutions*”* (Vol. 14). Springer Science & Business Media.

[4] Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. *Information Systems Research*, *16*(1), 28-46.

[5] Werlinger, R., Hawkey, K., Muldner, K., Jaferian, P., and Beznosov, K. (2008, July). “The challenges of using an intrusion detection system: is it worth the effort?” In *Proceedings of the 4th symposium on Usable privacy and security* (pp. 107-118)

[6] Butt, D. S., & Gnevasheva, V. A. E. (2018). Efficiency in the Processes of Intrusion Detection System Through Usability Evaluation Methods. *Available at SSRN 3151216*.

[7] Nielsen, J. (1994). “Usability engineering”. Morgan Kaufmann.

[8] Patil, T., Bhutkar, G., and Tarapore, N. (2012). “Usability evaluation using specialized heuristics with qualitative indicators for intrusion detection system”. In *Advances in Computing and Information Technology* (pp. 317-328). Springer, Berlin, Heidelberg.

[9] Quiñones, D., and Rusu, C. (2017). “How to develop usability heuristics: A systematic literature review”. *Computer Standards & Interfaces*, *53*, 89-122.

[10] Scarfone, K., and Mell, P. (2012). “Guide to intrusion detection and prevention systems (idps)”. (No. NIST Special Publication (SP) 800-94 Rev. 1 (Draft)). National Institute of Standards and Technology.

[11] Mathew, D, (2002). Choosing an Intrusion Detection System that Best Suits your Organization. *SANS Institute.* [Online]. Available: https://www.sans.org/reading-room/whitepapers/detection/choosing-intrusion-detection-system-suits-organization-82

[12] Cárdenas, A. A., Baras, J. S., & Seamon, K. (2006, May). “A framework for the evaluation of intrusion detection systems”. In *2006 IEEE Symposium on Security and Privacy (S&P'06)* (pp. 15-pp). IEEE.

[13] Roesch, M. (1999, November). Snort: Lightweight intrusion detection for networks. In *Lisa* (Vol. 99, No. 1, pp. 229-238).

[14] Bevan, N., Carter, J., & Harker, S. (2015, August). “ISO 9241-11 revised: What have we learnt about usability since 1998?”. In *International Conference on Human-Computer Interaction* (pp. 143-151). Springer, Cham.

[15] International Organization for Standardization. (1998). *ISO 9241-11: Ergonomic requirements for office work with visual display terminals (VDTs): Part 11: Guidance on usability*.

[16] Lewis, J. R. (2014). Usability: lessons learned… and yet to be learned. *International Journal of Human-Computer Interaction*, *30*(9), 663-684.

[17] Debar, H., Dacier, M., and Wespi, A. (1999). Towards a taxonomy of intrusion-detection systems. *Computer networks*, *31*(8), 805-822.

[18] Jaferian, P., Botta, D., Raja, F., Hawkey, K., & Beznosov, K. (2008, November). Guidelines for designing IT security management tools. In *Proceedings of the 2nd ACM Symposium on Computer Human interaction For Management of information Technology* (pp. 1-10).

[19] Paxson, V. (1999). Bro: a system for detecting network intruders in real-time. *Computer networks*, *31*(23-24), 2435-2463.

Cristian Ramón Cappo Araujo. Profesor titular del Dpto. de Informática de la Facultad Politécnica (FP-UNA) de la Universidad Nacional de Asunción.
ORCID: https://orcid.org/0000-0001-7433-5733.

Cristian Rodrigo Aceval Sosa. Profesor asistente del Dpto. de Informática de la Facultad Politécnica (FP-UNA) de la Universidad Nacional de Asunción.
ORCID: https://orcid.org/0000-0002-0202-0705.