Revisión Sistemática de Literatura: Visualización de Seguridad

Glinny Mondragón Oconor, Carlos Araya Guzmán y Leonardo Martínez Saborío

Escuela de Ingeniería,
Universidad Latinoamericana de Ciencia y Tecnología,
ULACIT, Urbanización Tournón, 10235-1000
San José, Costa Rica
gmondragono958,carayag960,lmartinezs765@ulacit.ed.cr
http://www.ulacit.ac.cr

Resumen La analítica visual aplicada en los procesos de seguridad informática, está tomando cada vez más fuerza; debido a la necesidad de representar un número razonable de elementos en una sola pantalla, así logra sintetizar grandes volúmenes de datos, que son generados por diferentes equipos de seguridad de cada organización. Mediante su utilización es posible crear un ambiente de conocimiento al combinarlos con la capacidad de procesamiento de las computadoras. Se realiza un análisis basado en una revisión sistemática de la literatura relacionada con la analítica visual, se destacan los tipos de visualizaciones, con tipos de ataques, fuentes de datos de distintos orígenes, lenguajes de programación y técnicas de interacción, que han sido utilizados por las publicaciones en estudio. Todo lo anterior, con el fin de facilitar a los analistas de seguridad, la identificación y comprensión de la información para la toma de decisiones con base en las visualizaciones.

Keywords: Visualización de seguridad, análisis de ataques, patrones de ataques, validaciones de visualizaciones, fuentes de datos

1. Introducción

Todo tipo de organizaciones, gubernamentales, militares, de servicios, entretenimiento o producción, hacen uso de información para su funcionamiento y mantenimiento de la competitividad. Algunas de estas lo hacen en mayor o menor escala, pero utilizan la información. Actualmente se generan más y más datos, desde una amplia variedad de tipos de fuentes, velocidades y calidad variables (propiedades de Big Data) y registros generados en los logs de los sistemas. Existe una necesidad de generar más información, de conocerla, de transmitirla de una forma segura, según sea el interés de cada quien, a nivel regional, nacional o mundial. No se trata de generar información sólo por generarla; la idea es que esta información se mantenga para los intereses de cada organización, al considerar los principios de confidencialidad, privacidad, integridad y disponibilidad, entre otros.

El desarrollo de Big Data hace que las tareas de análisis se vuelvan más difíciles y desafiantes (Luo y Xia, 2014), debido al aumento de la complejidad. Las capacidades de percepción del ser humano facilitan la adopción de nuevas ideas para el análisis de datos, por lo que la visualización es un componente crucial en los trabajos de investigación que fueron analizados. Además posee dos ventajas principales:

1. Fusión de grandes cantidades de datos en gráficos simples y eficaces.
2. Proporcionar formas eficientes para analizar información en vivo y con formatos fáciles de entender.

Consecuentemente, la información es considerada con propiedades de Big Data por el volumen, variedad y la velocidad en la que los datos se generan, los cuales, con el apoyo de las distintas técnicas de visualización de datos, toman en cuenta la variabilidad de la producción de los registros, según la actividad de los usuarios y los sistemas, además de la calidad de la información.

De acuerdo con lo anterior, se requiere del uso de recursos tecnológicos orientados al procesamiento de grandes volúmenes de datos, que también permitan encriptar, mover y acceder a la información de forma segura; esto sin descuidar el registro de las operaciones que se realizan mediante dichos recursos, pero hay que prever que siempre existirán riesgos, los cuales gestionados de forma adecuada, pueden minimizar las posibles brechas de seguridad que se deban enfrentar.

2. Metodología de trabajo

Con el fin de determinar cómo se aplica la analítica visual en los procesos de seguridad informática, se realizó un análisis detallado que tomó como base los artículos publicados durante los años 2010-2011 en los Proceedings del International Symposium on Visualization for Cyber Security, así como varios artículos publicados durante los años 2010 - 2014 en diferentes revistas y que fueron encontrados al utilizar Google Scholar.

Las publicaciones analizadas se dividen en dos clases: las que proponen una solución a un problema (22 artículos) y las que contribuyen a la teoría (2 artículos), mediante aportes a los fundamentos teóricos sobre el uso de técnicas de visualización (Torres, 2015).

El análisis consideró los tipos de visualizaciones, los tipos de ataques y el manejo de datos, con el fin de determinar cuáles técnicas de visualización permiten la comprensión y resguardo de la información, además de orientar a quienes se encuentren interesados en aspectos de Ciberseguridad y de la visualización de seguridad.

Para realizar este análisis, se estudiaron 24 artículos completos, de los cuales se extrajo los siguientes aspectos: resumen, problema que se busca resolver, resultados, conclusiones, tipos de visualizaciones utilizadas, fuentes de datos, lenguajes de programación y técnicas de interacción.

El resultado de este análisis fue procesado y tabulado con el fin de presentar una síntesis de las características de cada una de las técnicas de visualización

utilizadas, así como su relación con las técnicas de interacción, fuentes de datos, lenguajes de programación y tipos de ataque utilizados. Lo anterior, con el fin de encontrar la tendencia en el uso y aplicación de las visualizaciones en el ámbito de la Ciberseguridad. En consecuencia, esta investigación busca responder las siguientes preguntas:

1. ¿Cómo se utiliza la visualización de datos para apoyar la comprensión de la información que se genera durante los procesos de seguridad informática?
2. ¿Cómo llevar a cabo un análisis para relacionar tipos de visualizaciones, con tipos de ataques, fuentes de datos de distintos orígenes, lenguajes de programación y técnicas de interacción, que han sido utilizados en las publicaciones bajo estudio?

De acuerdo con las preguntas anteriores, este trabajo busca determinar cómo se utiliza la visualización de datos para apoyar la comprensión de la información que se genera durante los procesos de seguridad informática, mediante una revisión sistemática de literatura; además de realizar un análisis para relacionar los tipos de visualizaciones, con tipos de ataques, fuentes de datos de distintos orígenes, lenguajes de programación y técnicas de interacción, que han sido utilizados por las publicaciones bajo estudio.

3. Resultados - Discusión

3.1. Uso de las Visualizaciones

Con el fin de responder la primera pregunta de investigación y con base en las lecturas de las diferentes publicaciones analizadas, se encontró un patrón en el uso de las técnicas de visualización. La visualización permite a los analistas de seguridad, identificar de forma más rápida las vulnerabilidades de las que son objeto, y tomar decisiones basados en este análisis.

En la Figura 1, se puede observar que tanto los grafos como los histogramas y mapas de calor, han sido las técnicas de visualización más utilizadas por los autores de los trabajos que fueron analizados. Es importante indicar que varios autores han realizado combinaciones con varios tipos de visualización. Según lo analizado, estos permiten comunicar más información a través de una imagen de la que se puede transmitir en un texto. Se comentará seguidamente cada una de ellas en forma ascendente.

1. Grafos: Son representaciones de nodos, casi siempre unidos por aristas, que buscan mostrar las relaciones que existen entre los diferentes procesos. Este tipo de visualización tiene como fin exponer posibles anomalías; muchos autores han utilizado esta técnica de visualización porque les permite, de una forma sencilla, la interpretación e identificación de ataques de los que

pueden ser objeto (Lane y cols., 2010; Wenjuan Xu y Ahn, 2013; Chang y Jeong, 2011; Li, Xia, Liu, Huang, y Luo, 2014; He, Fan, Ye, y Zhang, 2013; Yelizarov y Gamayunov, s.f.). El uso de grafos permite interpretar de forma sencilla las relaciones en los ataques y por esa razón las han adaptado con el fin de utilizarlas junto con otras técnicas, para brindar al usuario una visualización más detallada del comportamiento de la red.

2. Histogramas de tiempo: Los histogramas de tiempo, le permiten a los analistas realizar una exploración a la red con el fin de identificar falsos positivos e intrusiones. Una herramienta como la que proponen (Ying, FangFang, Xiao-Ping, Xing, y YongGang, 2013), utiliza otra herramienta llamada IDS Radar, basada en un histograma de tiempo de forma radial o circular. Dicho radar se actualiza cada cinco minutos y cada vez que detecta algún tipo de alerta y esa alerta se presenta varias veces durante un rango de tiempo, la clasifica como sospechosa y le asigna un color intenso a la misma. Esto le facilita en gran medida el trabajo al analista de seguridad, para poder detectar a tiempo los ataques de intrusión y disminuir las alertas de tipo "falsos positivos" que generan los IDS [1] en una red.
3. Mapas de Calor: Los mapas de calor o "heatmap" (por su nombre en inglés), le permiten al analista de seguridad, determinar si el color presentando se mantiene asociado a lo que se ha identificado como comportamiento normal. Los autores (M., Shawn, Douglas, Adam, y A., 2010) proponen el uso de una herramienta llamada CLIQUE [2], en donde el resumen del tráfico de red se muestra en un mapa de calor, si el analista decide detallar más la búsqueda, la herramienta le permite seleccionar distintas categorías disponibles, en donde cada una ellas, según su coloración, tiene definido lo que es un comportamiento normal y lo que no es dicho comportamiento.
4. Gráficos de barras: Este tipo de visualización ha sido utilizado para analizar el comportamiento de diferentes tipos de protocolos de red. Esta técnica ha sido mezclada con los Visual Motifs, que permitieron identificar las aplicaciones permitidas y no permitidas en un análisis de al menos 200 puertos distintos, lo que demuestra su efectividad a la hora de analizar grandes volúmenes de datos (V., Fabian, y M., 2006; Wilson, Fabian, y John, 2010).
5. Líneas de tiempo: Al igual que los histogramas de tiempo, la principal ventaja radica en mostrar el comportamiento de la red en un rango de tiempo definido por el analista, con el fin de detectar posibles ataques a tiempo.
6. Otros: En esta categoría se incluyen las demás técnicas de visualización utilizadas, aunque en menor cantidad de uso, han contribuido en la detección de diferentes tipos de ataque e intrusiones en las redes. Es importante indicar que muchas de ellas han sido mezcladas con las técnicas antes mencionadas, y han otorgado un valor mucho más importante y detallado, que le han facilitado la toma de decisiones a los analistas de seguridad. La prueba de ello se puede observar en (Peng, Chen, y Peng, 2013), en donde se detallan cada uno de los retos a los que se enfrentan los analistas, proponen una herra-

[1] Por sus siglas en inglés, Intrusion Detection System
[2] Por sus siglas en inglés, Correlation Layers for Information Query and Exploration

mienta que ayuda a los analistas a visualizar las relaciones de confianza e identificar los ataques de una forma semiautomática.

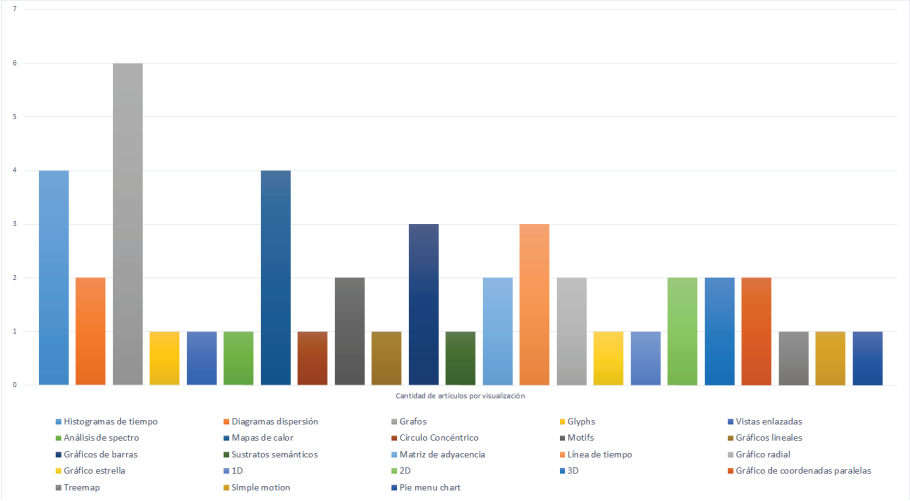

Figura 1. Tipos de Visualizaciones

3.2. Uso de las Visualizaciones y Tipos de Ataque

Se establece que la forma más segura de evitar un ataque es deshabilitar del todo los recursos tecnológicos que se deben salvaguardar; esta deshabilitación implica no utilizar del todo estos recursos, o sea, evitar que los mismos no logren funcionar de forma alguna y evitar por lo tanto, que los usuarios respectivos, tengan a su alcance el uso de dichos recursos; sin embargo, esto resulta poco práctico por los aspectos de disponibilidad, funcionalidad e incluso, ninguna de las partes interesadas, sobre todo los inversionistas, estarán agradecidos con este tipo de respuestas.

A partir del punto anterior, un aspecto importante de analizar para cualquier campo de la Ingeniería Informática y que resulta de mucha trascendencia dentro de la Visualización de Seguridad, es el de los ataques; donde es necesario que las herramientas que se diseñen, permitan identificar el tipo de ataque y la forma de resolver el mismo o por lo menos controlarlo.

De acuerdo con la tabla 1 y al tomar como referencia los artículos bajo estudio, los tipos de ataques que predominan son la Denegación de servicios o DDOS [3] y el escaneo de puertos[4], que se presentan 16 y 12 veces respectivamente

[3] Por su nombre en inglés, Distributed Denial of Service
[4] Por su nombre en inglés, Port Scanning

para los 19 tipos de visualizaciones identificadas. Aquí la tendencia si la marcan de forma muy significativa estos dos tipos de ataques, ya que aunque en la tabla 1, sí se observan otro tipo de ataques, las veces que estos se presentan realmente son poco significativas, para efectos de realizar algún análisis al respecto.

Para el ataque DDOS, el objetivo es inhabilitar ya sea un recurso dentro de la infraestructura tecnológica o el servicio que este recurso provee, lo cual se puede realizar al generar un determinado recurso dentro o fuera de dicha infraestructura, muchas peticiones a un mismo recurso o afectando la red por donde se mueve el tráfico de datos.

El ataque de Port Scanning lo que pretende es determinar cuáles puertos son vulnerables, es decir, qué puertos están "abiertos" de tal forma que se pueda ingresar a un recurso de la red y los servicios y datos que este administra, pero más importante es, ingresar del todo a la red objetivo, para afectar servicios, datos de otros recursos que forman parte de dicha red o simplemente ingresar Malware a este y afectar del todo su funcionalidad.

Los dos tipos de ataques mencionados, se presentan de forma conjunta para siete de las 23 visualizaciones bajo estudio, lo cual representa un número bastante bajo, sin embargo, aquí lo relevante no es si el número es bajo, sino que ambos ataques si se presentan a la vez, podrían dejar a cualquier organización fuera de servicio por un tiempo considerable, de ahí, la necesidad que más herramientas estén preparadas para realizar una adecuada gestión de frente a estos tipos de ataques.

Tabla 1: Tipos de Visualización y Tipos de Ataque

Tipo de ataque	**Tipo de Visualización**																			**Total**
	Histogramas tiempo	**Diagrama dispersión**	**Grafos**	**Glyphs**	**Vistas enlazadas**	**Análisis Espectro**	**Mapas de calor**	**Círculo Concéntrico**	**Motifs**	**Gráfico lineal**	**Línea de tiempo**	**Gráfico radial**	**Gráfico estrella**	**1D**	**2D**	**3D**	**Gráfico coordenadas paralelas**	**Simple motion**	**Pie menu chart**	
Sybil	**1**	**1**	**1**		**1**															**4**
MITM (man-in-the-middle)				**1**																**1**
Distributed Denial of Service (DDOS)	**1**	**1**	**3**		**1**	**1**	**1**				**1**		**1**	**1**	**2**	**1**		**1**	**1**	**16**
Bad mouthing					**1**															**1**
Bragging					**1**															**1**
New comer					**1**															**1**

Continúa en la página siguiente

Tipo de ataque	Tipo de Visualización																			Total
	Histogramas tiempo	Diagrama dispersión	Grafos	Glyphs	Vistas enlazadas	Análisis Espectro	Mapas de calor	Círculo Concéntrico	Motifs	Gráfico lineal	Línea de tiempo	Gráfico radial	Gráfico estrella	1D	2D	3D	Gráfico coordenadas paralelas	Simple motion	Pie menu chart	
Wormns	1		1			1														3
Port Scans	2		1			1	1				2	1		1	1	1	1			12
Hot Scans			1			1														2
Flash Crowds			1			1														2
Web Vulnerability Scanning								1												1
Password brute Force Insertion								1												1
Attackers position tracking								1												1
NORMAL			1																	1
PROBE		1	1										1							3
R2L	1	1	1										1							4
U2R	1	1	1										1							4
Fugas de información	1																			1
Virus	1																			1
Mailbomb							1		1	1										3
Malware propagation							1		1	1	1			1	1	1				7
Firewall policy anomaly																1				1
Low and slow scans			1								1	1								3
Total	9	5	13	1	5	5	4	3	2	2	5	2	4	3	4	4	1	1	1	74

3.3. Uso de las Visualizaciones y Tipos de Validación

Un elemento importante durante el desarrollo de software es la validación, por lo que debe ser considerado en el campo de la visualización de software. La razón es que toda herramienta de visualización de seguridad debe pasar por un proceso de validación, el cual permita demostrar que esta se comporta con la funcionalidad esperada, en otras palabras, que funciona según lo planificado y

cumple con los objetivos establecidos. Lo anterior permite que la herramienta de visualización apoye a los usuarios de forma efectiva en las tareas que realizan.

La Figura 2 muestra los 23 tipos de visualizaciones que fueron consideradas: 18 visualizaciones presentan el caso de estudio como el tipo de validación predominante, lo cual refleja la tendencia por este tipo de instrumento, al ser empleado de forma mayoritaria por los diferentes investigadores.

El Caso de Estudio representa uno de los instrumentos más complejos de implementar, debido a que requiere la definición de diferentes escenarios para realizar los diversos resultados obtenidos en cada uno de estos escenarios. El tema de los datos, al considerar una adecuada fuente de datos, implica en algunos casos, que dichos datos deban pasar por un proceso de calidad, esto con el fin de determinar cuáles datos son válidos en función de la investigación requerida, además de la selección de aquellos usuarios que realmente contribuyan con el proceso de investigación bajo observación

Parte de una adecuada estrategia para mantener el desarrollo esperado de un caso de estudio, implica el uso del software que permita y contribuya con dicha estrategia, así por ejemplo, una herramienta utilizada por (Yelizarov y Gamayunov, s.f.) es OpenGL, un "open source", que le permitió al usuario en el caso de estudio diseñado, resolver el problema de mayor severidad en el menor tiempo posible, al ser este un elemento importante por valorar, en futuros artículos, cuyo enfoque inicie definiendo el caso de uso como una de las herramientas para ser valoradas dentro de la investigación.

Después de los Casos de Estudio, la validación más utilizada corresponde a los "Test Case Scenarios", donde para las 23 visualizaciones en estudio, fue utilizada 15 veces.

Los Test Case Scenarios proponen una revisión integral del software en estudio, al considerar el flujo de datos y los diferentes procesos que intervienen en esta revisión; aquí la participación del usuario es vital, por ello, es necesario contar con usuarios expertos que son otro recurso necesario para el desarrollo de estos test case, ya que justamente estos expertos, pueden determinar en los test case scenarios, si la funcionalidad en estudio se comporta conforme lo esperado o es necesario seguir realizando ajustes hasta lograr el resultado definido.

Además de la participación de los usuarios expertos, el uso de la herramienta adecuada es importante; por ello (Ui-Hyong y cols., 2014) diseñaron una herramienta denominada Firewall Policy Checker, donde como resultado del test case escenario, se pudo detectar la presencia de servicios riesgosos como el uso del protocolo Telnet, pero que también contribuyó al análisis de políticas en un menor tiempo de duración al reafirmar en este test case, la fácil visualización de los datos procesados que pueden ser interpretados, incluso por usuarios no expertos.

Las validaciones se concentran en los Casos de Estudio y los Test Case Scenarios, pero de forma conjunta, el análisis de artículos demuestra para las 23 visualizaciones en estudio que en cinco ocasiones. Ambas validaciones se utilizaron de forma conjunta, se determina con ello, que si el uso individual de cada una de estas validaciones presenta sus respectivas ventajas, el uso de ambas, per-

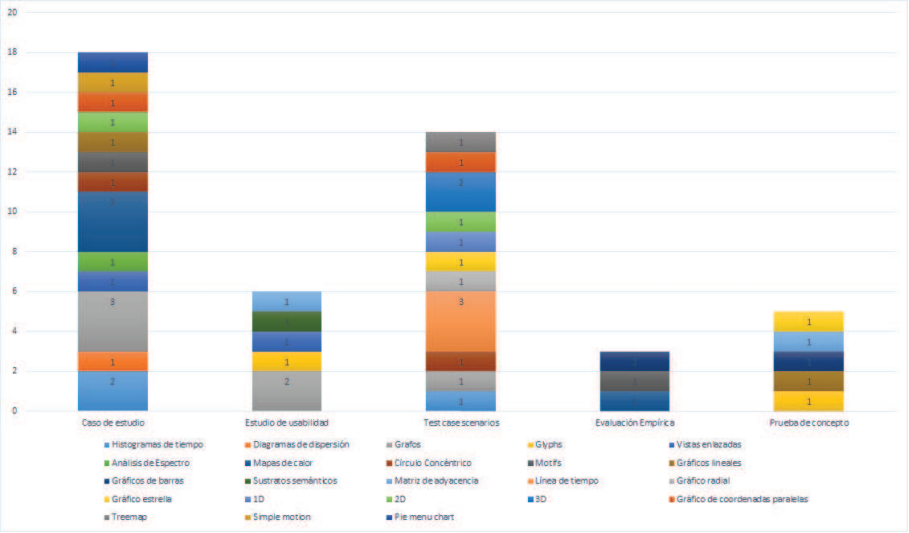

Figura 2. Tipos de Validación utilizados en las Visualizaciones

mitirá dar un enfoque integral y por lo tanto, establecer de forma más completa, si el software que se encuentra en estudio cumple conforme su funcionamiento.

Los Estudios de Usabilidad, la Evaluación Empírica y las Pruebas de Concepto también forma parte de las validaciones, aunque las mismas fueron utilizadas seis, tres y cinco veces, respectivamente, se refuerza con ello que la tendencia se orienta hacia los Casos de Estudio y los Test Case Scenarios.

3.4. Uso de las Visualizaciones y Tipos de Fuentes de Datos

El análisis de los diferentes artículos de investigación, ha demostrado que las fuentes de datos que se quieran analizar, influyen directamente en la elección del tipo de visualización. A partir de los resultados de la investigación y con base en la Tabla 2, se puede concluir que por medio del estudio de análisis de datos reales de tráficos de redes se obtienen los mejores resultados (Wilson y cols., 2010; Erbacher y Forcht, 2010; Chang y Jeong, 2011; Hu, Ahn, y Kulkarni, 2012; Li y cols., 2014; He y cols., 2013; Ui-Hyong y cols., 2014; Ying y cols., 2013; Fangfang y cols., 2013). Por lo que se puede considerar que esta es la fuente de datos utilizada para comprobar la validez de las visualizaciones de seguridad, expuestas en los artículos que fueron objeto de investigación.

De forma adicional, se encontró que los autores prefieren trabajar con datos reales; procuran que sus soluciones se encuentren lo más apegadas a la realidad. Asimismo, es importante señalar, que en el tema de las fuentes de datos, se obtuvieron aportes importantes en las investigaciones y análisis realizados en la configuración, las reglas y el comportamiento de los IDS, tales como los mencionados en (Rasmussen y cols., 2010), se convierten así en el segundo mayor

contribuyente de información para el desarrollo de este trabajo. Se obtuvo un tercer aporte proveniente de las evaluaciones ejecutadas por los expertos que desarrollaron los artículos, como las señaladas en (Peng y cols., 2013; Yu y cols., 2013), mediante las cuales se sometieron a pruebas de campo las visualizaciones y las soluciones para validar la funcionalidad de las mismas.

Tabla 2: Tipos de Visualización y Fuentes de datos

Tipo de fuente de datos	Tipo de Visualización																							Total
	Histogramas tiempo	Diagrama dispersión	Grafos	Glyphs	Vistas enlazadas	Análisis Espectro	Mapas de calor	Círculo Concéntrico	Motifs	Gráficos lineales	Gráfico barras	Sustratos semánticos	Matriz de adyacencia	Línea de tiempo	Gráfico radial	Gráfico estrella	1D	2D	3D	Gráfico coordenadas paralelas	Treemap	Simple motion	Pie menu chart	
Simulación	1	1	1	1																				4
Evaluación					1									1			1	1	1					5
IDS			2				1											1				1	1	6
Datos de reales de tráfico de red	2		2			1	2		2	2	2		1	2	1				1	1	1			20
Datos experimentales para realización de pruebas	1		1			1										1								4
Datos públicos	1						1																	2
Base de datos de logs de HTTP								1																1
Políticas de seguridad de SELinux			1									1	1											3
Total	5	1	7	1	1	2	4	1	2	2	2	1	2	3	1	1	1	2	2	1	1	1	1	45

3.5. Uso de las Visualizaciones y Lenguajes de Programación

En la actualidad existe un gran número de lenguajes de programación en el mercado. Esto permite que los desarrolladores de visualizaciones de seguridad puedan seleccionar el lenguaje que permita solucionar el problema al que se enfrentan de la mejor forma. De acuerdo con los artículos que fueron analizados,

el lenguaje más utilizando ha sido Java (Lane y cols., 2010; Peng y cols., 2013); por su versatilidad para programar visualizaciones con vistas enlazadas, y por su mejor rendimiento en la manipulación de grandes volúmenes de datos (Xia y cols., 2013), incluso de diferentes fuentes de datos. En la figura 3, se puede observar que fue el lenguaje más utilizado en 14 visualizaciones.

Con un menor nivel de uso, se encuentra MATLAB (fue utilizado únicamente en 9 visualizaciones). Es importante resaltar que MATLAB fue determinante para Xu et al. (Wenjuan Xu y Ahn, 2013) porque les permitió la elaboración de varios algoritmos y facilitó que un grupo de expertos de diferentes especialidades de computación pudieran identificar el origen de las violaciones a las políticas de seguridad y la forma cómo se propagan en los diferentes sistemas.

Es importante mencionar que ambos lenguajes mostraron sus bondades y la versatilidad ante los diferentes retos, en cuanto a volúmenes de datos, fuentes de datos, e incluyen estudios un poco más científicos dirigidos a diversos tipos de usuario.

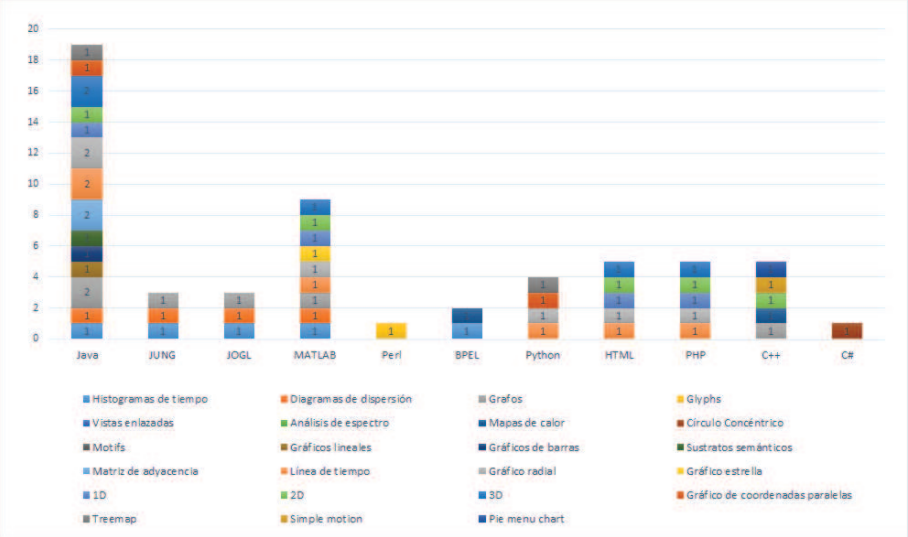

Figura 3. Lenguajes de Programación utilizados en las Visualizaciones

3.6. Uso de las Visualizaciones y Técnicas de Interacción

Las técnicas de visualización por sí solas, no pueden representar la gran cantidad de datos que se extraen de los diferentes sistemas de seguridad. Para facilitar el análisis de las visualizaciones, es necesario incorporar técnicas de interacción, que desde distintas perspectivas permitan a los analistas de seguridad, la identificación de problemas de seguridad y una oportuna toma de decisiones.

Esta investigación proporciona resultados interesantes en cuanto a la forma utilizada y la relación que existe entre el tipo de visualización y el método de interacción. A lo largo de este trabajo y como se puede ver en la Tabla 3, se puede concluir que cuando se trata de visualizaciones de seguridad, la técnica de interacción que proporciona más expectativas y es de preferencia para los expertos, se denomina Selección, la cual se puede describir como la ejecución de un clic. En (Lane y cols., 2010; Peng y cols., 2013; Wenjuan Xu y Ahn, 2013; Erbacher y Forcht, 2010; Yelizarov y Gamayunov, s.f.; Xia y cols., 2013), se muestra que con un solo clic sobre un nodo en un grafo, se obtiene más detalle de la información que se requiere visualizar.

Como segunda técnica de interacción importante, utilizada y que contribuye con aportes considerables al trabajo de investigación, se encuentra la conocida como Zoom, mencionada en (M. y cols., 2010; Rasmussen y cols., 2010; Wenjuan Xu y Ahn, 2013; Ui-Hyong y cols., 2014; Yelizarov y Gamayunov, s.f.; Ying y cols., 2013). La conducta de esta técnica, consiste en que trata de aumentar o disminuir la información visible en un rango en particular, de esta forma acerca o aleja la visualización que se puede ver con más detalle y profundiza en los datos del objeto que se encuentra en análisis.

Asímismo la interacción llamada Ampliación, indicada en (Lane y cols., 2010; Peng y cols., 2013), es la tercera técnica de preferencia en los artículos analizados ya que permite seleccionar distintos tipos de visualizaciones y profundizar en la información requerida, al combinar de esta manera todo en forma de vistas enlazadas; lo que permite obtener una visualización bastante amplia para quienes analizan la información.

Tabla 3: Tipos de Visualización y Técnica de Interacción

Tipo visualización	**Técnica de interacción**													
	Selección	**Ampliación**	**Reordenación**	**Zoom**	**Panning**	**Filtrado**	**Contracción**	**Rotación**	**Desplazamiento**	**Particionamiento**	**Drill Down**	**Cambio de ejes**	**Anotación**	**Total**
Histogramas tiempo	**1**			**2**	**1**	**1**					**1**			**6**
Diagrama dispersión	**1**													**1**
Grafos	**3**	**2**	**1**	**3**	**2**	**1**	**2**						**1**	**15**
Vistas enlazadas	**1**	**1**	**1**											**3**
Mapas de calor	**1**	**1**		**2**	**1**	**1**	**1**							**7**
Círculo Concéntrico									**1**	**1**				**2**
Sustratos semánticos	**1**		**1**	**1**	**1**								**1**	**5**
Matriz adyacencia	**1**		**1**	**1**	**1**								**1**	**5**
Línea de tiempo	**2**	**1**				**1**						**1**		**5**

Continúa en la página siguiente

Tipo visualización	Técnica de interacción													Total
	Selección	Ampliación	Reordenación	Zoom	Panning	Filtrado	Contracción	Rotación	Desplazamiento	Particionamiento	Drill Down	Cambio de ejes	Anotación	
Gráfico radial	**2**	**1**				**1**						**1**		**5**
2D	**1**	**1**		**1**			**1**							**4**
3D	**1**			**1**	**1**			**1**	**1**		**1**			**6**
Gráfico coordenadas paralelas	**1**	**1**				**1**						**1**		**4**
Treemap	**1**	**1**										**1**		**3**
Simple motion	**1**	**1**		**1**			**1**							**4**
Pie menu chart	**1**	**1**		**1**			**1**							**4**
Total	**19**	**11**	**4**	**13**	**7**	**6**	**6**	**1**	**2**	**1**	**2**	**4**	**3**	**79**

3.7. Uso de las Visualizaciones y Tipos de Enfoque

Cada artículo analizado, plantea un problema que pretende ser resuelto y que facilitará la comprensión de la solución propuesta. Entre mayor diversidad de recursos se empleen, se logrará una mejor comprensión del problema que se busca resolver. El enfoque planteado en cada artículo, considera una adecuada explicación de los eventos que promueven una apropiada investigación con el fin de mostrar, desde un punto de vista cuantitativo o cualitativo, los resultados que se analizan.

Para los 23 tipos de visualizaciones considerados; 18 de ellas se enfocan hacia la Detección anomalías en la red y esta tendencia se explica a partir de la utilidad que tienen las redes hoy en día. Se consideran desde las redes domésticas, las empresariales y las de carácter mundial, donde el flujo de datos ha crecido de forma exponencial y con ello, también los riesgos asociados a este crecimiento, como son los ataques al tráfico de la red o a los protocolos que utilizan dichas redes.

Por lo que se cita en el párrafo anterior, la detección de anomalías en la red se ha vuelto muy compleja debido al volumen de datos que circulan en la red. Por ello, es necesario no sólo la detección de estas anomalías a través de un adecuado rastreo, sino que se puedan rastrear y analizar en tiempo real y tomar decisiones que permitan mitigar dichas amenazas, también en tiempo real. El factor humano tiene gran influencia en la detección y solución temprana de dichas anomalías, esto es observado en (Erbacher y Forcht, 2010), al considerar que un tipo de visualización utilizado y unido a un usuario que tenga las capacidades requeridas para realizar el análisis del tráfico de red, son las combinaciones ideales para una clara y eficaz identificación de anomalías, al permitir, mantener un ambiente de tráfico de red, bastante seguro.

Para apoyarse en la detección de anomalías en la red, (Yu y cols., 2013), apuestan por el uso de una herramienta "open source" [5] denominada Honeypots, que permite administrar la red, determinar los ataques que sufre esta y aprender de dichos ataques a través del análisis forense, el manejo de estadísticas, aspectos de hackeo, entre otros puntos.

Después de la detección de las anomalías, el siguiente enfoque predominante es el de Análisis de Datos de IDS, donde este enfoque se repite 9 veces para las 23 visualizaciones en estudio. En el caso del primer enfoque mencionado, este trata simplemente de la detección, mientras que el enfoque de análisis de datos de IDS, implica plantear el problema del manejo de la información, ya sea porque se tiene poca información o porque existen falsas alarmas, por eso, el análisis sugerido, puede contribuir a la identificación de datos relevantes, a la categorización de los incidentes identificados y tratados de manera oportuna, con lo cual se contribuye de forma ágil y adecuada a la gestión de estos datos históricos.

Como se mencionó anteriormente, el Análisis de Datos de IDS es la segunda tendencia dentro del enfoque pero realmente, antes que pensar en IDS, los diversos artículos estudiados no hacen mención de IPS en lugar de IDS, ya que mientras IDS se enfoca en eventos pasados, IPS, lo que hace es prevenir de las posibles amenazas que podrían atacar una red. De forma muy sencilla, el IDS es un sistema pasivo y el IPS, en cambio es un sistema activo o en línea, al ser el primero, el predecesor del segundo.

Una herramienta que apoya el Análisis de Datos de IDS, es NIMBLE [6] que considera el uso de recomendaciones generadas basadas en el aprendizaje de máquinas, a partir de alertas históricas, que ayudan a los Analistas de Ciberseguridad en la toma de decisiones a partir de la información representada mediante grafos o tablas, a la vez que generan alertas asociadas a este tipo de información (Rasmussen y cols., 2010).

La detección de anomalías en la red y el Análisis de Datos de IDS fueron utilizados de forma conjunta por los autores de los artículos que constituyen la presente investigación, para cuatro de las 23 visualizaciones en lista, lo cual aunque representa un número bastante bajo, sí debe considerarse su manejo conjunto o incluir un enfoque adicional, para apoyar en las preguntas de investigación que se deseen plantear, según el tipo de artículo por resolver.

Otros enfoques observados son el de comunicaciones seguras, visualización de relaciones de confianza, análisis de datos en tiempo real y análisis de políticas de firewall, con uno, cuatro, ocho y cuatro veces observadas en los análisis realizados, lo cual refuerza que la tendencia se orienta hacia la detección de anomalías y análisis de datos de IDS. Lo anterior no implica que futuros investigadores deben considerar solo los enfoques que muestran una tendencia, también podrían realizar una combinación entre los que están dentro y fuera de dicha tendencia.

[5] En español, Software Libre

[6] Por sus siglas en inglés, Network Intrusion Management Benefiting from Learned Expertise

Tabla 4: Tipos de visualización y Tipos de enfoque

Tipo de enfoque	Tipos de visualización																							Total
	Histogramas de tiempo	Diagrama dispersión	Grafos	Glyphs	Vistas enlazadas	Análisis Espectro	Mapas de calor	Círculo Concéntrico	Motifs	Gráfico lineales	Gráfico barras	Sustratos semánticos	Matriz adyacencia	Línea de tiempo	Gráfico radial	Gráfico estrella	1D	2D	3D	Gráfico coordenadas paralelas	Treemap	Simple motion	Pie menu chart	
Detección anomalías en la red	2	1	1				2	1	2	1	1			2	1		1	1	1	1				18
Comunicaciones seguras				1																				1
Visualización relaciones de confianza			1		1							1	1											4
Análisis de Datos de IDS	1		3				1									1		1				1	1	9
Análisis de Datos en tiempo real	1		1			1	1							1	1					1	1			8
Análisis de políticas de firewalls										1	1		1						1					4
Total	4	1	6	1	1	1	4	1	2	2	2	1	2	3	2	1	1	2	2	2	1	1	1	44

4. Conclusiones

La visualización de la seguridad combina la seguridad operativa informática y la estadística aplicada en tiempo real, junto con las técnicas de interacción y las representaciones visuales en movimiento, entre otros factores. Este grupo de factores, utilizados de forma conjunta, facilitan a quienes laboran en el campo de la Ciberseguridad, ampliar o reducir el alcance de los análisis que llevan a cabo. A partir de esos análisis, se debe tomar decisiones en un menor tiempo; lo cual contribuye con una adecuada gestión de los riesgos que afectan a los recursos tecnológicos de las diferentes organizaciones cuando se presentan diversas amenazas.

El punto anterior es válido en el campo laboral, ahora, a nivel académico, la visualización de seguridad no es un tema que comúnmente se desarrolle en un salón de clases. Generalmente se hace referencia a aspectos de seguridad informática, sin hacer énfasis en herramientas específicas para el análisis de pa-

trones o ataques, como las herramientas de visualización de seguridad. Por lo tanto, este trabajo de investigación también contribuye a comprender los tipos de visualización existentes, los tipos de ataques y las técnicas de análisis de datos que se utilizan.

El análisis de los artículos permitieron determinar que aunque no todos los trabajos de investigación presentan una estructura claramente definida (por ejemplo, resumen ejecutivo, estado del arte, análisis de los resultados, conclusiones y recomendaciones), algunos artículos no son claros con respecto a varios aspectos, como son los datos que fueron utilizados, la definición del problema o si realmente el problema fue resuelto. Además, estos artículos al hacer el análisis de las valoraciones cuantitativas y cualitativas, no permiten una adecuada comprensión o solo lo permiten pero de forma parcial. Esto concuerda con la investigación realizada por González (Torres, 2015).

Este artículo recolecta una serie de valoraciones a partir de los aspectos que fueron definidos para realizar el análisis. Cada uno de esos aspectos se desarrolla de forma posterior a una breve reseña conceptual para introducirlos, y se muestran los factores relevantes que fueron observados. Debido a lo anterior, este trabajo de investigación puede ser de utilidad tanto para fines académicos como laborales, según el interés particular del lector; por lo que puede servir como complemento de futuras investigaciones, como es la orientación para los desarrolladores de herramientas de visualización, así como usuarios de estas herramientas que estén interesados en conocer las tendencias recientes, según el alcance de artículos analizados.

Referencias

Chang, B.-H., y Jeong, C. Y. (2011, oct). An efficient network attack visualization using security quad and cube. *ETRI Journal*, *33*(5), 770-779. pages 4, 9

Erbacher, R. F., y Forcht, K. A. (2010, jun). Combining visualization and interaction for scalable detection of anomalies in network data. *Journal of Computer Information Systems*, *50*(4), 117-126. pages 9, 12, 13

Fangfang, Z., Ronghua, S., Ying, Z., Huang, Yezi, y Liang, X. (2013). Netsecradar: A visualization system for network security situational awareness. En G. Wang, I. Ray, D. Feng, y M. Rajarajan (Eds.), *Cyberspace safety and security* (Vol. 8300, p. 403-416). Springer International Publishing. pages 9

He, H., Fan, G., Ye, J., y Zhang, W. (2013, aug). A topology visualization early warning distribution algorithm for large-scale network security incidents. *The Scientific World Journal*, *2013*, 1-7. pages 4, 9

Hu, H., Ahn, G.-J., y Kulkarni, K. (2012, may). Detecting and resolving firewall policy anomalies. *IEEE Trans. Dependable Secur. Comput.*, *9*(3), 318–331. Descargado de `http://dx.doi.org/10.1109/TDSC.2012.20` doi: 10.1109/TDSC.2012.20 pages 9

Lane, H., Xianlin, H., Xiaowei, Y., Aidong, L., Weichao, W., y Xintao, W. (2010, sep). Interactive detection of network anomalies via coordinated multiple views. En *Proceedings of the seventh international symposium on visualization for cyber security* (p. 91-101). New York, NY, USA: ACM. Descargado de `http://doi.acm.org/10.1145/1850795.1850806` doi: 10.1145/1850795.1850806 pages 4, 11, 12

Li, J., Xia, J., Liu, Y., Huang, Y., y Luo, B. (2014, aug). A visualization strategy with a pentacle and its application in the intrusion detection system. *Applied Mechanics & Materials*, *610*, 647-652. pages 4, 9

Luo, B., y Xia, J. (2014, jul). A novel intrusion detection system based on feature generation with visualization strategy. *Expert Systems with Applications*, *41*(9), 4139–4147. pages 2

M., B. D., Shawn, B., Douglas, L., Adam, W., y A., P. W. (2010, sep). Real-time visualization of network behaviors for situational awareness. En *Proceedings of the seventh international symposium on visualization for cyber security* (p. 79-90). New York, NY, USA: ACM. Descargado de `http://doi.acm.org/10.1145/1850795.1850805` doi: 10.1145/1850795.1850805 pages 4, 12

Peng, D., Chen, W., y Peng, Q. (2013, dec). Trustvis: visualizing trust toward attack identification in distributed computing environments. *Security and Communication Networks*, *6*(12), 1445-1459. pages 4, 10, 11, 12

Rasmussen, J., Ehrlich, K., Ross, S., Kirk, S., Gruen, D., y Patterson, J. (2010, sep). Nimble cybersecurity incident management through visualization and defensible recommendations. En *Proceedings of the seventh international symposium on visualization for cyber security* (p. 102-113). New York,

NY, USA: ACM. Descargado de http://doi.acm.org/10.1145/1850795.1850807 doi: 10.1145/1850795.1850807 pages 9, 12, 14

Torres, A. G. (2015). *Evolutionary visual software analytics* (Tesis Doctoral no publicada). Universidad de Salamanca. pages 2, 16

Ui-Hyong, K., Jung-Min, K., Jae-Sung, L., Hyong-Shik, K., Jung, y Soon-Young. (2014, jul). Practical firewall policy inspection using anomaly detection and its visualization. *Multimedia Tools and Applications*, *71*(2), 627-641. pages 8, 9, 12

V., W. C., Fabian, M., y M., M. G. (2006, nov). Using visual motifs to classify encrypted traffic. En *Proceedings of the 3rd international workshop on visualization for computer security* (p. 41-50). New York, NY, USA: ACM. Descargado de http://doi.acm.org/10.1145/1179576.1179584 doi: 10.1145/1179576.1179584 pages 4

Wenjuan Xu, M. S., y Ahn, G.-J. (2013, jun). Visualization-based policy analysis for selinux: framework and user study. *International Journal of Information Security*, *12*(3), 155-171. pages 4, 11, 12

Wilson, L., Fabian, M., y John, M. (2010, sep). Traffic classification using visual motifs: An empirical evaluation. En *Proceedings of the seventh international symposium on visualization for cyber security* (p. 70-78). New York, NY, USA: ACM. Descargado de http://doi.acm.org/10.1145/1850795.1850804 doi: 10.1145/1850795.1850804 pages 4, 9

Xia, J., Wu, F., Guo, F., Xie, C., Liu, Z., y Chen, W. (2013, apr). An online visualization system for streaming log data of computing clusters. *TSINGHUA SCIENCE AND TECHNOLOGY*, *18*(2), 196-205. pages 11, 12

Yelizarov, A., y Gamayunov, D. (s.f.). *Adaptive security event visualization for continuous monitoring.* pages 4, 8, 12

Ying, Z., FangFang, Z., XiaoPing, F., Xing, L., y YongGang, L. (2013, feb). Idsradar: a real-time visualization framework for ids alerts. *SCIENCE CHINA Information Sciences*, 1-12. pages 4, 9, 12

Yu, W., Wei, S., Shen, D., Blowers, M., Blasch, E. P., Pham, K. D., ... Lu, C. (2013, may). On detection and visualization techniques for cyber security situation awareness. *Proc. SPIE*, *8739*, 87390R-87390R-9. pages 10, 14