Modelo de Evaluación Cuantitativa de Riesgos en Seguridad Informática

Quantitative Model in Security Informatics Risk Assessment

*Andrés Casanova**

Resumen

El artículo presenta el desarrollo de un proyecto orientado hacia la evaluación de un modelado que permita a los profesionales en seguridad informática, fundamentar la evaluación de riesgos de seguridad sobre bases de estimación cuantitativas, soportándose para ello en herramientas tales como: Regresión logística, Diagramas de Influencia y Network Forensic, que permitan capturar datos de volúmenes de transacciones (archivos tipo LOG), garantizando su integridad y seguridad de dicha información [20], con el fin de llegar a cálculos de probabilidad numérica, sobre escenarios de riesgo detectados en los logs transaccionales y en las trazas que dejan los registros en un IDS SNORT.

Palabras clave: Análisis Forense Logs, Seguridad informática – Evaluación de riesgos- regresión logística – diagramas de influencias.

Abstract

This paper shows the importance of approaching in security Risk Assessment (RA) about Quantitative model in Risk Management. The RA has been calculated with qualitative method by different framework, for example: RISK IT FRAMEWORK (COBIT Component) [7], OCTAVE – ALLEGRO [8], MAGERIT V3 [9], FAIR [4], ISO 27005 [11], NIST800-30 [3]. All frameworks included in the scope the Risk Assessment; however this is more qualitative than quantitative. In this work, we propose a methodology to support the implementation and execution risk management, using quantitative risk assessment method. The methodology is based on three components: secure capture logs (apply networks forensic technical), likelihood risk or log analysis with logistic regression and risk assessment with influence diagrams.

Key words: Risk Assessment, Information security, logistic regression statistics model, influence diagrams, IDS, and Network forensic.

Fecha Recibido:
Fecha Aceptado:

* Ingeniero de Sistemas Universidad Nacional de Colombia, Especialista en Teleinformática, Magister en Ciencias de la Información y las Comunicaciones, Universidad Distrital Francisco Jose de caldas, Docente Facultad de Contaduría, Universidad Antonio Nariño, jcasanova@uan.edu.co.

I. INTRODUCCIÓN

La evaluación cuantitativa de riesgos en seguridad informática es una necesidad para poder estimar alternativas o estrategias de seguridad, las cuales, permitan minimizar de la manera más efectiva riesgos de seguridad existentes o potenciales. El tratamiento detallado en la evaluación de riesgos en seguridad informática, ha sido un tema generalmente tratado a partir de la experiencia o basado en hechos conocidos por parte de un experto; quienes aplican metodologías de origen cualitativo para estimar la probabilidad de ocurrencia y el grado del impacto asociado.

II. GESTIÓN DE RIESGOS EN SEGURIDAD INFORMÁTICA

La Gestión de Riesgos (RM) es en principio identificar medir y controlar los eventos de riesgo en seguridad informática [2], en razón, que toda causa de riesgo identificada y medida será controlada. Por lo tanto, todas las acciones, decisiones y/o medidas tendientes a mitigar las causas de riesgos, están orientadas a reducir el impacto de las mismas, a tal punto que el riesgo sea administrable o aceptable. Por lo anterior, la gestión de riesgos en seguridad informática debe incluir la fase de evaluación y aseguramiento riesgos.

La gestión de riesgos RM (Risk Management) incluye dos puntos muy importantes: el análisis de las causas de riesgos y la implementación de controles para mitigar los mismos [11]. El primero también denominado el proceso de evaluación de riesgos (Risk Assessment RA), el cual, tiene como principal propósito identificar, clasificar y cuantificar la amenaza sobre escenarios potenciales [5], estimando el impacto de la materialización de las causas de riesgo y su gravedad. El segundo proceso, habitualmente denominado mitigación de riesgos (Risk mitigation Rm), consiste en implementar planes de acción tendientes a gestionar los riesgos potenciales, con el propósito de minimizar el efecto si se llegasen a materializar las causas de riesgos [25].

Actualmente, las metodologías de evaluación de riesgos de amplio uso en las organizaciones a nivel mundial corresponden a marcos de referencia (Frameworks), tales como; IT RISK [7], ISO 27005, ISO 31010, OCTAVE [9], MAGERIT V3 [8] o FAIR [4] entre otras. Cada marco de referencia emplea métodos de análisis de riesgos y usan clasificaciones descriptivas, subjetivas para evaluar los impactos del riesgo [3]. Estos métodos por lo general, dependen del nivel de experiencia del experto que realiza la evaluación.

Un análisis de riesgos cuantitativo ofrecerá una mejor medida aproximada de la evaluación del impacto [2]. Este método también emplea el uso de herramientas matemáticas o estadísticas [1] para efectuar cálculos que permitan hacer una aproximación de la probabilidad de ocurrencia de una causa de riesgos [10].

III. MODELO DE EVALUACIÓN CUANTITATIVA DE RIESGOS

El modelo propuesto está compuesto de tres componentes: recolección segura de logs, análisis de probabilidades con regresión logística y análisis de riesgos con diagramas de influencias.

El análisis nace desde la recolección de las trazas o logs de auditoria, el cuales, son tratados de manera segura mediante una práctica de Network Forensic [15]. Los logs, registran posibles escenarios de vulnerabilidades materializados o potencialmente materializarles [12], que son analizadas según los atributos de prioridad de cada traza.

Cada traza, contienen atributos que pueden de cierta manera dar mayor peso a un registro de auditoria que a otro. El volumen de las trazas de auditoria, puede ser tratado de manera estadística, llegando a una aproximación de probabilidad de riesgo numérica cuantitativa [13], donde la función de densidad de probabilidad es calculada a partir de un modelo de regresión logística [1]. El propósito de la Regresión logística es obtener una función lineal de las variables independientes de tal manera que sea posible clasificar los individuos en una subpoblación de las variables dependientes [22].

Finalmente el modelo, concluye el análisis de riesgo con el uso de diagramas de influencias [6],

Paso	Actividad	Resultado
1	Inicio	Fecha de inicio
2	Configuración de log de auditoria elemento de seguridad	Auditorias activas
3	Captura de trazas de auditoria	Archivos de trazas (logs) del elemento de seguridad
4	Extracción y custodia de las trazas de los logs con prácticas de forensia en redes NF	Archivo de log Extraído de manera segura
5	Análisis de los elementos que contienen la traza y definición de campos clave	Definición de campos clave
6	Cosntrucción de archivo formateado	Archivo log formateado con campos claves eliminando redundancia
7	Análisis de probabilidades con el uso de regresión logística	Construcción algoritmo de regresión logística
8	Conclusión de resultados con Software estadístico	Definición de función de regresión logística
9	Definición de costos de activos informáticos impactados	Tabla de costos por activo impactado
10	Construcción de diagramas de influencias	Diagrama de influencias
11	Análsis de resultados de criticidad	Conclusiones y resultado del análisis de riesgos cuantitativos
	Fin	

Figura 1. Esquema metodológico propuesto.

la cual, es una herramienta que permiten hacer un análisis de sensibilidad por cada escenario de vulnerabilidad evaluado. Los riesgos más sensibles, son aquellos que representan mayor probabilidad de ocurrencia y costo de materialización.

IV. CONSTRUCCIÓN DEL MODELO

Se evaluaron y analizaron los incidentes de seguridad, sobre la base de una población de datos procedentes de un IDS (Intrusion Detection Systems), el cual, recopiló una base poblacional de ataques donde se analizaron las variables de peso que se consideraron podían asignar mayor o menor criticidad al ataque.

El IDS SNORT [16] por ser una herramienta libre, que permite una configuración robusta y que se adapta a las necesidades del ejercicio

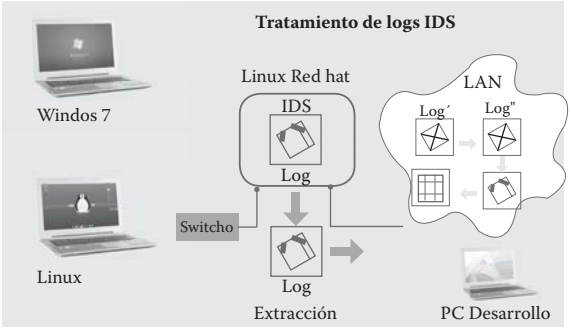

Figura 2. Laboratorio implementado

académico. El propósito fue tomar las trazas (registros LOGS) del IDS y realizar un análisis detallado de las mismas bajo un esquema seguro de captura de los logs de auditoria del IDS SNORT [20]. A continuación se detalla el laboratorio implementado:

Todas las trazas registran que hubo una alerta de ataque o una intención de ataque y todas las trazas están clasificadas por orden de prioridad 1,2 o 3. Para las trazas que tienen prioridad 2 y están marcadas con bandera MF se clasificaron con más peso que las trazas prioridad 2 que no tienen dicha bandera. Para las trazas que tienen prioridad 3 y un TOS [17] con valor superior de 0x0 (0 en decimal) tienen un mayor peso que las trazas que tienen prioridad 3 con TOS 0x0. La razón por la cual se asignó mayor peso a las trazas antes citadas, indica que estos ataques están asociados a inundación de datagramas IP, los cuales no fueron re ensamblados y se excedió el tiempo de re ensamble [26].

V. RECOLECCIÓN Y ANÁLISIS DE DATOS

La normalización de los datos es un elemento fundamental, en razón que los datos registrados por las trazas de los logs se constituyen en el insumo (materia prima) para el análisis de riesgos en la red [18]. Por lo anterior, se formateo un archivo cuyos campos dieran mayor significancia o relevancia criterio de prioridad a las trazas del IDS SNORT [21]. Cada traza viene clasificada y calificada por tipo de ataque y relevancia, además, existen otros elementos dentro de la traza, que pueden afectar de menor o mayor manera

la calificación de la misma. Los campos que se definieron en nuestro archivo de análisis fueron los siguientes:

- Fecha: contiene la fecha del ataque en formato mes día año
- Hora: contienen hora en que se realiza el ataque
- Nombre: Descripción del ataque asignada por IDS SNORT
- Clasificación: Clasificación asignada por IDS SNORT
- Prioridad: Criticidad del ataque calificada por IDS SNORT
- Ip_origen: dirección IP desde donde se originó el ataque
- puerto_origen: Puerto de origen de ataque
- Ip_destino: dirección IP de destino donde se atacó
- puerto_destino: Puerto destino ataque
- TOS: Campo tipo de servicio TOS del datagrama IP
- DF: Bandera de control de fragmentación
- MF: Bandera de control de más fragmentación
- Len: Longitud datagrama IP
- frag_offset: Fragmento de compensación

Para el análisis de los datos almacenados en el archivo normalizado proveniente del IDS SNORT, se empleó análisis estadístico mediante el uso de Regresión Logística.

VI. REGRESIÓN LOGÍSTICA

A partir de la regresión logística es posible estimar la probabilidad de que un individuo pertenezca a uno de los grupos diferenciados en la variable dependiente. En este caso ataques no malignos (0) ó ataques malignos (1).

Dichos modelos presentan las siguientes ventajas para el cálculo de la probabilidad:

- Se obtiene un modelo estadístico con la combinación de variables que marcan la mayor diferencia entre los grupos de la variable dependiente (0,1).
- A partir de esta fórmula se estima directamente la probabilidad de ataques malignos a un sistema.
- Permite la clasificación de un nuevo individuo en uno de los subgrupos de la variable dependiente.
- Es posible modelar a partir de variables cualitativas.

El modelo de regresión logístico multivariado se define de la siguiente forma [1]:

$$P(X) = \frac{1}{1+ e^{-(\beta_0+\beta_1 x_1+\beta_2 x_2+ \ldots. +\beta_n x_n)}} \qquad (1)$$

Fórmula 1. Regresión Logística

Donde los estimadores β_0, β_1, $\beta_2 \ldots \beta_n$ son los parámetros del modelo

Con la regresión logística se procura expresar la probabilidad de que ocurra el evento de interés como función de algunas variables, que desde la teoría (o la experiencia) se asumen como influyentes [23].

Dado que una variable Y_i se supone sigue una distribución tipo Bernoulli al tratarse de un modelo de regresión logística, la solución a las ecuaciones implicadas en este proceso de optimización suministran los estimadores de los parámetros del modelo. La variable dependiente de RL, se define como una variable categórica tipo dicotómica "ataque Maligno" (ataq_maligno), que asume los siguientes valores:

0: ataque no maligno o falso positivo
1: ataque maligno

Para el presente modelo se definió como ataques no malignos aquellas trazas que cumplen de manera simultánea con los siguientes requisitos: Pertenece al grupo prioridad 3 y nombre de ataque es diferente de

- "SCAN SSH brute force login attempt"
- "PROTOCOL-ICMP Destination Unreachable Port Unreachable"
- "PROTOCOL-ICMP Fragment Reassembly Time Exceede"

El modelo de regresión logística es desarrollado en R [19], sigue un proceso estadístico de análisis de variables y su peso, desarrollado en R presenta los resultados de la ejecución del algoritmo y los resultados de la ejecución en el cálculo de los significativos y la relevancia de los mismos para el modelo.

Del resultado de las validaciones estadísticas se observó que las variables con más significancia estadística dentro del proceso de evaluación, fueron las siguientes:

Criticidad: afecta la calificación de la traza reportada por el IDS. Esta variable viene ordenada.

Longitud Datagrama Len: Esta variable también puede considerarse de peso en la fórmula de cálculo de probabilidad para ataques nocivos, por cuanto, si la longitud del datagrama excede su longitud estándar 1500 Bytes (MTU para Ethernet) o es de longitudes cercanas [26], el ataque tiene una orientación hacia un intento DoS. Por lo tanto en la media que la longitud de datagrama se incremente, el modelo de regresión logística lo interpreta como una probabilidad de ataque.

El modelo resultado del estudio de regresión logística es el siguiente:

$$P(X) = \frac{1}{1+ e^{-(11.63 - 1.653X_1 + 0.014X_2)}} \qquad (2)$$

Fórmula 2. Regresión Logística bivariada

Dónde:

X_1: variable Criticidad
X_2: variable len = longitud datagrama

Se interpreta que la variable independiente que tiene mayor peso es Criticidad y la variable Longitud presenta valores significativos a valores grandes de Longitud.

VII. USO DE DIAGRAMAS DE INFLUENCIAS

El diagrama de Influencias, por ser una estructura matemática conceptual que permite abstraer un problema y representarlo de manera compacta en un problema de decisión, se convierte en una herramienta que facilita el cálculo cuantitativo de variables de decisión y variables aleatorias [14].

Por lo anterior, el cálculo cuantitativo de riesgos se apoya con el uso de Diagramas de influencias, por cuanto dicha herramienta permite integrar de manera simultánea variables aleatorias y variables de decisión para calcular estadísticamente su desempeño. Para el ejercicio del diagrama de influencia, fue necesario definir el costo del activo informático que se va afectar por causa de la materialización de un riesgo (materialización de un ataque), este valor, estará sujeto exclusivamente al impacto o daño que ocasiona la vulnerabilidad explotada sobre el activo informático de una organización [22].

El activo informático se puede definir como la información crítica, sensible o de alto impacto para una organización, la cual, representa el objeto de mayor valor para la misma y debe ser altamente resguardada; sin embargo, lograr valorar en términos cuantitativos el activo informático [23], se convierte en una ejercicio particular de cada organización, en razón, que solo cada una de ellas conoce y determinará la criticidad de su información [25]. Por lo anterior, la metodología que se desarrolle en el diagrama de influencias, requiere que se determine de manera a priori una tabla de costes por vulnerabilidad, donde estos valores serán asignados por los expertos de la organización y son variables fundamentales para el cálculo del análisis de riesgo de vulnerabilidades [24].

Debido a que los ataques vienen clasificados desde IDS SNORT, se etiqueta cada uno de los ataques de la siguiente como se muestra en la tabla 1, con el propósito de construir el diagrama de influencias de manera resumida.

Posteriormente en el desarrollo de la metodología, se asignan costos para cada una de las vulnerabilidades, los cuales deben ser asignados por un experto dependiendo del grado de sensibilidad del activo informático impactado.

Tabla 1. Clasificación de ataques etiquetados por vulnerabilidad explotada

Clasificación	Etiqueta	Nombre del ataque	Etiqueta
Web Application Attack	A	COMMUNITY SQL-INJECTION Sql Injection attempt	A1
		POLICY-OTHER PHP uri tag injection attempt	A2
		POLICY-OTHER script tag in URI - likely cross-site scripting attempt	A3
Attempted Denial of Service	B	COMMUNITY SIP TCP/IP message flooding directed to SIP proxy	B1
Attempted Information Leak	C	SNMP AgentX/tcp request	C1
		SNMP request tcp	C2
Misc activity	D	SCAN SSH brute force login attempt	D1
		PROTOCOL-ICMP Fragment Reassembly Time Exceede	D2
		PROTOCOL-ICMP Destination Unreachable Port Unreachable	D3
		PROTOCOL-ICMP PING BSDtyp	D4
		PROTOCOL-ICMP PING *NIX	D5
		PROTOCOL-ICMP PING	D6
		PROTOCOL-ICMP Echo Reply	D7

Tabla 2. Clasificación de ataques con costos asociados

Grupo de Variable	Variable	Costos
A	A1	5
	A2	4
	A3	4
B	B1	5
C	C1	3
	C2	3
D	D1	4
	D2	3
	D3	3
	D4	0
	D5	0
	D6	0
	D7	0
Costo Total		34

Toda Vulnerabilidad Vi tiene asociado un costo Ki pesos; sin embargo, cuando la vulnerabilidad es un Warning (advertencia) y corresponde a un ataque no declarado, en este caso el K = 0 pesos, por cuanto no corresponde a un ataque propiamente dicho y no existen impactos o costos asociados a pérdidas por activo informático afectado.

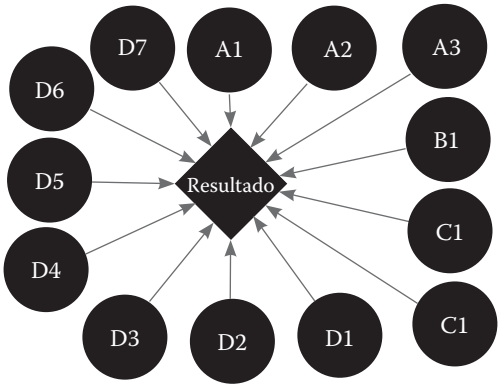

Figura 3. Diagrama de influencias por vulnerabilidad explotada

Donde Vi → Ki

El Diagrama de Influencia se presenta de la siguiente manera, donde se incluye en el sistema las probabilidades ya calculadas y los costos por cada vulnerabilidad explotada.

Tal como se presenta en el diagrama de influencias, podría suponer que todos los ataques pueden ocurrir de manera recurrente o en diferentes combinaciones y no son excluyentes. Cada ataque materializa una vulnerabilidad, que a su vez tiene una probabilidad de ocurrencia y una consecuencia o un impacto asociado.

La gráfica de probabilidad del perfil de riesgo muestra la información de cada posible resultado como una distribución de densidad discreta. Cada línea del gráfico muestra la probabilidad de que el resultado sea igual a un cierto valor.

Tabla 3. Resultados estadísticos
Diagrama de influencias

Estadística	Resultados
Media	29,025
Mínimo	0
Máximo	34
Modo	28
Desviación estándar	2,411985696
Índice de asimetría	-0,4433
Curtosis	3,7117

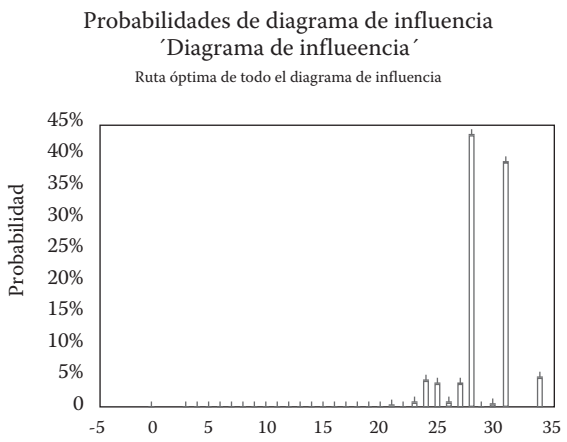

Figura 4. Gráfico de probabilidad

Como se puede ver en el gráfico las probabilidades versus costos, indica que la mayoría de probabilidades se concentran entre los costos 25 y 31. Se interpreta que la combinación de ataques con mayores probabilidades de ocurrencia suma costos entre 25 y 31. Es de aclarar, que en la representación de un diagrama de influencias, cada vulnerabilidad explotada tiene un costo asociado y en principio los ataques pueden ocurrir en diferentes combinaciones. Además, los ataques que explotan las vulnerabilidades no son excluyentes y pueden ocurrir en diferente orden y/o momentos, es así, como puede ocurrir solamente uno o pueden ocurrir todos al mismo tiempo. Por lo anterior, el diagrama de influencias en su estructura, concluye un análisis estadístico de riesgo cuantitativo, donde se concentran los escenarios más críticos del perfil de riesgo evaluado.

Los ataques que se materializaron de manera combinada y presentan mayor probabilidad de ocurrencia y costo para la organización son:

- Community SQL – Injection
- Policy Other PHP – uri tag injection attempt
- Policy Other script Tag Uri.
- Community SIP/TCP
- SNMP AGENT/Tcp request
- SNMP request TCP
- SCAN SSH Brutal Force

Escenarios de riesgo de mayor impacto, con su cálculo de probabilidad, según la fórmula 2 de regresión logística bivariado:

$$P(X) = \frac{1}{1+ e^{-(11.63 - 1.653X_1 + 0.014X_2)}} \qquad (2)$$

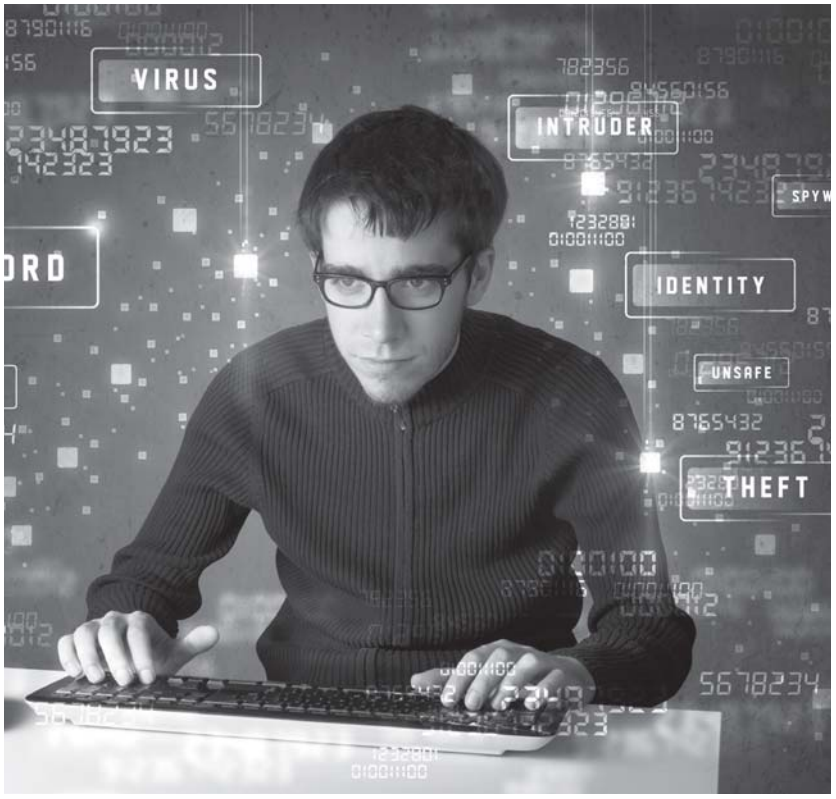

Tabla 4. Resultados de análisis de riesgos de mayor impacto

Calificación	Etiqueta de Grupo	Descripción	Etiqueta subgrupo	Probabilidad	Costo afectado	Costo Impacto	Mayor Impacto
Web Application Attack	A	COMMUNITY SQL-INJECTION Sql Injection attempt	A1	0,999	5	5	X
		POLICY-OTHER PHP uri tag injection attempt	A2	0,999	4	4	X
		POLICY-OTHER script tag in URI - likely cross-site scripting attempt	A3	0,999	4	4	X
Attempted Denial of Service	B	COMMUNITY SIP TCP/IP message flooding directed to SIP proxy	B1	0,998	5	5	X
Attempted Information Leak	C	SNMP AgentX/tcp request	C1	0,986	3	3	X
		SNMP request tcp	C2	0,93	3	3	X
Misc activity	D	SCAN SSH brute force login attempt	D1	0,93	4	4	X
		PROTOCOL-ICMP Echo Reply	D2	0,445	3	0	
		PROTOCOL-ICMP Fragment Reassembly Time Exceede	D3	0,129	3	0	
		PROTOCOL-ICMP PING	D4	0,075	0	0	
		PROTOCOL-ICMP PING *NIX	D5	0,846	0	0	
		PROTOCOL-ICMP Destination Unreachable Port Unreachable	D6	0,001	0	0	
		PROTOCOL-ICMP PING BSDtyp	D7	0	0	0	
	Total				34	28	

Conclusiones

La modelo metodológica propuesta permite evaluar riesgos de seguridad informática de manera cuantitativa aplicable a un esquema de red.

Es necesario depurar cada traza del elemento generador de logs de Auditoria, en razón que las trazas generan un volumen de información que podría generar valor en la variable de decisión a evaluar o en el conjunto de ellas.

La predicción del modelo depende en gran medida de la preparación de los datos o de la base a ataques, los cuales deben contemplar múltiples escenarios de riesgo. Esto permite crear un modelo general que permita predecir el comportamiento de cualquier base de ataques, lo anterior, evitaría crear modelos particulares para distintas bases de ataques cada vez que estas ocurren.

Los log por ser fuentes generadoras de evidencia digital, contienen información sensible, la cual, debe ser tratada con procedimientos y/o práctica de forensia en redes [18], que garantice la integridad y seguridad de la misma y permita evaluarse de manera confiable.

La metodología expuesta fortalece y complementa los esquemas o marcos de referencia en evaluación de riesgos de seguridad informática, en razón que ofrece una herramienta práctica y aplicable a los profesionales que se apoyan en dichos marcos de referencias.

El análisis del diagrama de influencias, permite una concepción más amplia y real a un problema de análisis de riesgo que un árbol de decisión, por cuanto el diagrama contempla múltiples ocurrencias de n eventos de riesgo de manera simultánea. Lo que hace más real el planteamiento del modelo y su respectivo cálculo, así como la

combinación de las variables de decisión y las variables aleatorias.

La variable costo de activo impactado se constituye en una variable de peso para el análisis de criticidad en el modelo con el uso de diagramas de influencias; sin embargo, no es posible asignar una metodología estándar para la estimación del costo del activo informático, por cuanto este es nativo y/o particular a la naturaleza de cada organización.

Referencias

[1] *M. V. C. Juan Caros Correa Morales, La Separación en Regresión Logística, una solución y aplicación, Bogotá: Universidad Nacional de Colombia, 2003.*

[2] *ACIS, Cultura en seguridad informatica retos y cambios, ISSN 0120-5919 ed., BOGOTA, 2014.*

[3] *R. L. K. a. R. D. Vines, The CISM Prep Guide: Mastering the Five Domains of Information Security Management, ISBN 978-1-60420-215-1 ed., Indianapolis: John Wiley & Sons, 2012, p. 90.*

[4] J. A. Jones, An Introduction to Factor Analysis of Information Risk, http://riskmanagementinsight.com/media/documents/FAIR_Introduction.pdf, 2008

[5] *R. L. K. a. R. D. Vines, The CISM Prep Guide: Mastering the Five Domains of Information Security Management, ISBN 978-1-60420-215-1 ed., Indianapolis: John Wiley & Sons, 2012, p. 90.*

[6] *J. S. Ortiz, Análisis de Decisiones estratégicas en entornos inciertos cambiantes y complejos, ISBN 978-987-1486-12-0 ed., Buenos Aires: Cengage, 2010, p. 58.*

[7] *ISACA, The Risk IT Framework, Rolling Meadows: ISACA, 2009.*

[8] *http://administracionelectronica.gob.es/ctt/, Magerit, "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información", 2010.*

[9] C. A. a. A. Dorofee, Managing information Security Risks. The OCTAVE Approach, Addison Wesley, 2003.

[10] *P. Meyer, Probabilidades y aplicaciones estadísticas, Addision Wesley, 2010, p. 15.*

[11] *M. Sahinoglu, Quantitative Risk Assessment for Dependent Vulnerabilities, IEEE.*

[12] *Y. K. M. O. H. Alhazmi, Quantitative Vulnerability Assessment of Systems Software, IEEE, 2005.*

[13] *M. Sahinoglu, Security Meter- A Probabilistic Framework to Quantify Security Risk, 2008.*

[14] *Analisis de desiciones estrategicas, ISBN 978-987-1486-12-0 ed., Buenos Aires: CENGAGE, 2009.*

[15] *L. Z. G. C. Chen Lin, Automated Analysis of Multi-source Logs for Network Forensics. 978-0-7695-3557-9/09 © 2009 IEEE, 2009.*

[16] *«www.snort.org/downloads/#rule-downloads» [En línea].*

[17] *J. Postel, http://www.rfc-es.org/rfc/rfc0791-es.txt.*

[18] *J. C. M., Peritaje informático y la evidencia digital en Colombia, Universidad de los Andes, 2010.*

[19] «www. «http://cran.r-project.org/,» [En línea].

[20] *N. Nisiblat, El manejo de la prueba electrónica en el proceso civil colombiano, Universidad de los Andes, 2010*

[21] *ACIS, «http://www.acis.org.co/fileadmin/Base_de_Conocimiento/XII_JornadaSeguridad/PresentacionJairoCasanovaDECEVAL-LogEventosEvidenciaDigital.pdf.,» [En línea].*

[22] *D. W. Hosmer, Applied logistic regression / David W. Hosmer, Stanley Lemeshow., New York : John Wiley & Sons.*

[23] *D. W. Hosmer, Applied logistic regression / David W. Hosmer, Stanley Lemeshow, New York: John Wiley, 1989.*

[24] *S. M. B. A. D. R. William R. Cheswick, Repelling the Wily Hacker, Boston: Lumeta Corporation, 2003.*

[25] *A. D. Chistopher Alberts, Managing Information Security Risk: The Octave Approach, Albuquerque: Addison Wesley, 2002.*

[26] *J. A. Casanova, Implementación de un prototipo de sistema de control de acceso para la red autónomo del laboratorio de redes, Universidad Nacional, 1998.*