Información Tecnológica
Vol. 29(1), 27-38 (2018)
http://dx.doi.org/10.4067/S0718-07642018000100027

Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas

Diego J. Parada*, Angélica Flórez y Urbano E. Gómez
Universidad Pontificia Bolivariana seccional Bucaramanga, Facultad de Ingeniería de Sistemas e Informática, Autopista a Piedecuesta Km 7, Edificio L, Oficina 301, Bucaramanga, Colombia
(e-mail: diego.parada@upb.edu.co; angelica.florez@upb.edu.co; urbano.gomez@upb.edu.co)

* Autor a quien debe ser dirigida la correspondencia

Recibido Jul. 6, 2017; Aceptado Sep. 1, 2017; Versión final Nov. 7, 2017, Publicado Feb. 2018

Resumen

Este artículo presenta el análisis sistémico de los componentes de la seguridad utilizando los lenguajes de la dinámica de sistemas tales como la prosa, el diagrama de influencias, de flujo-nivel, las ecuaciones y los comportamientos. La dinámica de sistemas permite el análisis de la complejidad de los elementos de la seguridad mediante la caracterización de los ciclos de realimentación presentes para el entendimiento, explicación y pronóstico de la misma. Se muestra la utilidad del modelo propuesto a través de la simulación de escenarios hipotéticos, permitiendo con ello medir la seguridad de la información.

Palabras clave: dinámica de sistemas; seguridad informática; seguridad de la información; ciberseguridad

Analysis of the Components of Security from a Systemic System Dynamics Perspective

Abstract

This article presents the systemic analysis of the components of security with the use of the languages of systems dynamics such as the prose, influence diagram, flow-level, equations and behaviors. Systems dynamics allows the analysis of the complexity of security's elements through the characterization of the existing feedback cycles, for the perception, explanation and prediction of security. The usefulness of the proposed model is shown through the simulation of hypothetical scenarios, allowing in this way measuring information security.

Keywords: system dynamics; information technology security; information security; cyber security

INTRODUCCIÓN

La evolución de las comunicaciones en el mundo cambió el paradigma de las transacciones comerciales enmarcadas en concepciones tecnológicas, tales como: comercio electrónico (*e-commerce*); intercambio electrónico de Datos (EDI – *Electronic Data Interchange*); B2B (*Business to Business*); colaboración abierta distribuida (*Crowdsourcing*); la web 2.0 (redes sociales); almacenamiento de grandes cantidades de datos (*Big Data*), entre otros; concepciones tecnológicas que tienen su soporte en las Tecnologías de la Información (TI) que permiten su funcionamiento (Calvo *et al*., 2013). El reconocimiento del papel de las TI en la evolución de las comunicaciones se considera fundamental, así como el hecho que ellas pueden ver comprometido su trabajo o normal funcionamiento debido a sus vulnerabilidades inherentes, bien sea por omisión o por fallas de configuración del responsable de su administración, ello conlleva una probabilidad intrínseca para la materialización de amenazas la cual puede desencadenar en fugas, pérdidas, alteraciones, destrucción, entre otras anomalías que recaen sobre la información (Chinchilla, 2012). Para mitigar el riesgo, esto es, la relación existente entre las vulnerabilidades y las amenazas de las organizaciones (Hernández & Vásquez, 2013), corresponde un proceso continuo de aseguramiento de las TI cuyo objetivo sea establecer mecanismos que garanticen la confidencialidad, la integridad y la disponibilidad de la información.

Las organizaciones se encuentran conformadas por tres elementos genéricos: los actores involucrados tales como los directivos, jefes, empleados, clientes y demás interesados en el negocio (Recurso Humano); los métodos, actividades o políticas que la orientan (Procesos del Negocio); la infraestructura tecnológica que soporta la operación del negocio (Tecnologías de Información) (Rahimi *et al*, 2016); esta triada se encuentra regida dentro de un marco regulatorio que conlleva al cumplimiento de las normas y leyes asociadas a la protección de la información (Marco Jurídico). Estos componentes coexisten, se interrelacionan y son parte fundamental del funcionamiento del negocio, ya que ante cualquier evento inesperado se genera un impacto negativo que puede conllevar a pérdidas o interrupciones en su operación (Calvo et al., 2013), en el caso de Colombia, las empresas se clasifican según el avaluó de sus activos y el personal contratado en micro, pequeña, mediana y grande y por operación se dan tipos de organización en financieras, comerciales, de servicios, educación y transformación, este estudio contempla de manera general las vulnerabilidades y por ende los ataques que podría tener cualquier organización.

Hay evidencias de trabajos que buscan integrar aspectos de la ciberseguridad. Tal es el caso de experiencias como el *framework* para la Ciberseguridad que tiene en cuenta lo relacionado al Internet de las Cosas como un servicio de la computación en la nube, en donde los autores plantean que el funcionamiento depende de la eficiencia de las comunicaciones en los dispositivos perimetrales que las soportan (*switch, router y gateway*), debido a que son necesarias las transacciones en tiempo real. El trabajo está soportado en un modelo de Markov que utiliza procesos estocásticos para simular el comportamiento de la computación en la nube, sin embargo, el *framewok* presentado se puede tener en cuenta para observar las ecuaciones estadísticas con las que cuenta el modelo de Markov, que podrían mejorar el modelo con DS (Amandeep et al., 2017).

Además, con el objeto de proteger la infraestructura de información crítica (Brechbühl et al., 2010) propone una estrategia que involucra prácticas de seguridad de la información obtenidas de la investigación de la literatura y otras que se dan en las empresas de los Estados Unidos y plantea que deben ser adoptadas en los países emergentes. Los autores presentan ejemplos de los nodos de comunicación en las organizaciones en su interacción con otras organizaciones y los representa en un esquema similar al que propone el diagrama de influencias de este artículo. Los aspectos principales son: -1- la necesidad de compartir información entre sus pares, -2- el establecimiento de los canales de comunicación especialmente en emergencias y -3- la habilitación de herramientas de evaluación como oportunidad de mejoramiento. En el texto se manifiesta que la responsabilidad compartida en los ámbitos corporativo, nacional e internacional -entre entidades del sector público y privado- basada en la confianza que se de en la interacción entre las instituciones, lo que podría generar los mecanismos que le den efectividad a los programas que buscan proteger la infraestructura crítica disminuyendo el riesgo cibernético de las relaciones.

Adicionalmente (Nagurneyet.al., 2017) presenta la problemática global que existe a nivel mundial en cuestiones de ciberseguridad cuyas cifras económicas en pérdidas rondan miles de millones de dólares que anualmente pierden los países debido a los ataques que afectan la infraestructura crítica de los gobiernos y empresas, por ejemplo: gasoductos, sistemas eléctricos, suministro de agua y servicios financieros. La preocupación más grande es el incremento de la tecnología en el Internet de las Cosas pues representa un aumento en las distintas vulnerabilidades por el aumento de los dispositivos indefensos ante posibles ataques de los cibercriminales y manifiestan la necesidad de mejorar la planificación y asignación adecuada de los recursos para mitigar el daño probable y las consecuencias catastróficas no solo económicas. Los autores citan otras fuentes que han estudiado esta área y analizan modelos que sintetizan el

comportamiento de los ataques y expresan que el dominio de la seguridad en las redes de computadoras tiene una literatura limitada pero útil que emplea. Por ejemplo, la teoría de juegos, aplicando juegos de suma cero, dinámicos, estocásticos, estáticos y de coalición a redes informáticas y de comunicación. Los autores presentan tres nuevos modelos de inversiones en ciberseguridad que no están restringidos al número de empresas, sus ubicaciones o los sectores a los que pertenecen: -1- El primero es un modelo de Nash de equilibrio de no cooperación y competencia, que se formula, se analiza y se resuelve utilizando la teoría de la desigualdad que sirve para encontrar el punto de desacuerdo sobre el cual tiene lugar la negociación en el segundo modelo. -2- Un Modelo de cooperación, en donde utilizan la teoría cooperativa de juegos, para argumentar a favor del intercambio de información sobre los niveles de ciberseguridad de las empresas en donde se da una negociación para decidir los niveles de seguridad que estarían dispuestos a implementar con respecto a sus funciones de costos de inversión, riqueza y daños en el caso de un ciberataque y restricciones. -3- El tercer modelo en este documento también se centra en la cooperación entre las empresas en términos de sus niveles de ciberseguridad, pero desde una perspectiva de optimización del sistema en la que se maximiza la suma de las utilidades esperadas de las empresas.

El proceso fundamental que las organizaciones deben contemplar para afrontar los eventos inesperados es la seguridad; cuyo propósito es crear estrategias que permitan asegurar la información y el conocimiento de la organización (*Know How*) bajo la gestión de un proceso sistemático, lógico y continuo, que se muestre como un indicador positivo que da valor agregado a los procesos misionales (Skopik *et al.*, 2016). Adicionalmente, se concibe la seguridad como una herramienta valiosa para cualquier negocio lo cual conlleva a cuestionarse sobre la manera en la cual se puede formalizar la intensión que tiene la misma en las organizaciones. En el contexto actual cuando se habla de seguridad sobre las TI se definen o establecen desde diversas áreas, tales como la seguridad informática, la seguridad de la información y la Ciberseguridad (Flake, 2017). La seguridad informática es reconocida como el proceso que vela por la protección de los activos de información, es decir, se establece en el nivel operativo del negocio, pues su fin es brindar soporte al negocio mediante el establecimiento de los controles o buenas prácticas de configuración y el manejo o uso de los diferentes dispositivos que conforman la infraestructura de TI (Calvo *et al*., 2013).

La seguridad de la información, según la norma ISO 27002:2013 como un proceso que busca proteger la confidencialidad, integridad y disponibilidad de la información, contra un compendio de amenazas, en pro de asegurar la continuidad del negocio, disminuir los posibles daños y maximizar el retorno de la inversión en la organización (ISO/IEC, 2012). La Ciberseguridad entendida en la norma ISO 27032 como la “preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio” (ISO/IEC, 2012); el ciberespacio es entendido como el ambiente virtual que en el que confluyen las personas, los usuarios, las infraestructuras tecnológicas y las organizaciones en la Internet (Flórez *et al.*, 2016). Adicionalmente se presenta el concepto de la Ciberdefensa, en el cual se amplía el campo de estudio de la Ciberseguridad o la seguridad informática al incluir las infraestructuras y redes industriales donde se soportan servicios esenciales o estratégicos, tales como el transporte, tránsito, energía, petróleo y gas, nuclear, entre otros, los cuales al estar interconectados al Ciberespacio se encuentran expuestos a las vulnerabilidades y amenazas inherentes en el mismo (Skopik *et al.*, 2016). Esto conlleva a la necesidad de brindar las condiciones necesarias de seguridad para el normal funcionamiento y convergencia de las redes de datos (TCP/IP) y las redes industriales (SCADA, sensores, entre otros), además de otros conceptos emergentes como el Internet de las Cosas, el *Big Data*, *Smart Cities*, entre otros, hecho que amplía el espectro de aplicación de la seguridad.

A partir de estos análisis se desarrolla el modelo de los componentes de la seguridad mediante la formalización de los lenguajes de la Dinámica de Sistemas, que se presenta como un lenguaje de representación del conocimiento e ilustra la complejidad dinámica de los sistemas mediante la identificación de los elementos y las relaciones que se dan entre ellos (Gómez, et al., 2015). La identificación de los componentes de la seguridad sugirió un estudio para la comprensión de la complejidad de sus elementos a través de la caracterización de los ciclos de realimentación presentes, que conllevara a la utilidad del modelo propuesto con el entendimiento, explicación y pronóstico del comportamiento de la seguridad a través de la simulación de escenarios hipotéticos. El modelo fue desarrollado en la herramienta *PowerSim Studio 10 Professional*, la cual permite que a través de los parámetros definidos se puedan manipular las variables del modelo especificando las condiciones de simulación, proceso denominado escenario, el cual parte de una hipótesis desde la cual se realiza la variación de los parámetros del modelo y se obtiene un comportamiento que permite su validación o análisis.

Este artículo se desarrolla como resultado del proyecto de investigación “Análisis Sistémico de los Observatorios de Ciberseguridad – OCi” desarrollado con apoyo de la Universidad Pontificia Bolivariana Seccional Bucaramanga, en el cual se hizo necesario la revisión del estado del arte en torno a la Ciberseguridad y la Dinámica de Sistemas, con el fin de identificar y describir los elementos que

caracterizan la Ciberseguridad basado en los *frameworks*, estándares o normas internacionales de agentes reconocidos, tales como: la Organización Internacional de Estándares (ISO), la Unión Internacional de Telecomunicaciones (ITU), la Agencia Europea de Seguridad de la Información y de las Redes (ENISA), and others (Bruin *et al.*, 2016); el modelo de componentes de la seguridad se define como el eje central del Modelo Estructural de los Observatorios de Ciberseguridad – MEOCi definido en la investigación (Parada *et al.,* 2017).

RESULTADOS

Con el fin de dar respuesta a la inseguridad en el ciberespacio se procede a plantear un modelo de la seguridad. La norma ISO 27032 plantea una guía que permite observar la seguridad de manera funcional u operativa denominado: Contexto General de Seguridad (CGS) que propone la guía de relaciones de los diferentes elementos que lo conforman. De acuerdo a la norma ISO 27032, la seguridad está compuesta de siete elementos fundamentales: los interesados (*Stakeholders*), los activos, las vulnerabilidades, el riesgo, los controles, las amenazas y los agentes de amenaza (atacantes o intrusos), los cuales se relacionan de la siguiente manera (ISO/IEC, 2012):

Se parte de la premisa o el hecho de la existencia de unos interesados, los cuales poseen unos activos que inherentes a su existencia tienen valor; los interesados pueden estar conscientes de las vulnerabilidades que conllevan al riesgo de los activos; aunado a ellos existen los agentes de amenaza quienes a través de las mismas pueden explotar las vulnerabilidades y con ello materializar el riesgo sobre los activos; a su vez, los agentes de amenaza desean abusar y/o poder dañar los activos; como éstos se encuentran expuestos al riesgo, los interesados desean reducirlo, para ello definen e implementan controles con los cuales lo reducen; finalmente, los controles pueden tener vulnerabilidades los cuales se logran reducir a través de los mismos controles. Se realizó un análisis de referentes en seguridad lo que conllevó a evidenciar la existencia de normas, *framewoks* o estándares tales como: CoBIT 5.0, ISO 27001:2013, ITIL v3, NIST SP800, entre otras, las cuales permiten al interesado conceptualizarla con base en definiciones, los elementos que la conforman, entre otros (Jaramillo, *et al.*, 2015); sin embargo, no se encontraron evidencias suficientes sobre modelos que permiten analizar el comportamiento de dichos elementos y sus relaciones con su respectiva complejidad.

Con el fin de estudiar el fenómeno de la seguridad y sus componentes a través de un análisis sistémico, se procede a utilizar la metodología de la dinámica de sistemas, partiendo del lenguaje de la prosa que permitió identificar las variables del sistema, sus relaciones y sus ciclos de realimentación; posteriormente se definió a través del diagrama de influencias el esquema que permitió la integración de todas las variables y las influencias que existen o afectan el sistema; consecuentemente, se desarrolla el diagrama flujo-nivel para la representación del modelo matemático del sistema y las ecuaciones que permiten analizar los datos y la relación matemática de las variables del modelo; finalmente, a través del lenguaje de los comportamientos se generan los resultados luego de la simulación del modelo, a partir de hipótesis planteadas como puntos iniciales, que conllevan a la aceptación o rechazo de las mismas y con ello entender el fenómeno en estudio.

Lenguaje en Prosa y Lenguaje de Influencias

Para la comprensión de la explicación dada en el lenguaje en Prosa de la DS es necesario comprender dos elementos fundamentales: los Activos y los Controles. Los Activos, según la Asociación Española de Normalización y Certificación, son el componente operacional de un sistema de información, el cual tiene una probabilidad de ser atacado accidental o deliberadamente, de forma externa o interna, lo cual acarrea una consecuencia para la organización. Dentro de un sistema de información puede ser considerado como activo: la información, los datos, los servicios, las aplicaciones (software), los equipos (hardware), las comunicaciones, los recursos administrativos, los recursos físicos y los recursos humanos (AENOR, 2008). Los Controles, según la metodología de análisis y gestión de riesgos MAGERIT, son las contramedidas, mecanismos o procesos que al ser aplicados tienen como objetivo disminuir o mitigar el riesgo que existe de la relación entre las vulnerabilidades y amenazas (Portal de Administración Electrónica de España, 2012).

A partir de los elementos definidos como componentes de la seguridad en la norma ISO 27032 se conlleva al análisis de la seguridad a través del lenguaje de la prosa en el cual se describe el sistema en estudio y, se procede a presentarlo en el lenguaje de influencias en donde se pueden apreciar las relaciones entre los elementos y los ciclos de realimentación que conllevan a definir la situación como dinámica. El diagrama es presentado en la Fig. 1 y posteriormente se explican los ciclos de realimentación (Parada *et al.,* 2017): i) Los Activos conllevan al surgimiento de Atacantes quienes fabrican Amenazas y las materializan al explotar el Riesgo aumentando el Impacto y depreciando los Activos; ii) Los Activos tienen, inherente a su función, Vulnerabilidades que, de materializarse, con la explotación del Riesgo, aumentan el Impacto y deprecian los Activos; iii) Los Activos tienen inherentemente Riesgos que generan Impacto sobre los Activos; iv) Sobre los

Activos es necesario aplicar Controles para mitigar la Materialización de explotar el Riesgo y a su vez el Impacto sobre los Activos; v) A mayor probabilidad de Riesgo, mayor será el Impacto, por ello se genera la necesidad de invertir en Controles para disminuir la afectación que acarrea la Materialización del Riesgo.

Fig. 1: Diagrama de Influencias de los Componentes de la Seguridad

Lenguaje de Flujo-Nivel

Mediante el lenguaje Flujo – Nivel, se da consistencia al resultado obtenido en el lenguaje de influencias al formalizar el modelo matemático precisando el contenedor de las ecuaciones en los símbolos que se presentan en la Tabla 1. En la Tabla 1 se muestran las convenciones con las cuales se construye un diagrama Flujo – Nivel, además se hace una breve explicación de su función. En la Fig. 2 se muestra una estructura básica del diagrama Flujo-Nivel donde el nivel Activo, almacena la variación del flujo *Ingreso de Activos* (*ActIng*), la cual se calcula por medio de la auxiliar *Relación del Valor del Activo respecto a su Existencia* (*RelValActExt*) a partir de la operación de las contantes *Valor Promedio de Activos* (*ActValPro*) y la *Existencia de Activos* (*ActExt*), la replicación de esta muestra en todo el modelo facilitará la comprensión de la metodología que propone la DS.

En la Fig. 3 se presenta el diagrama de Flujo-Nivel de los Componentes de la Seguridad, en el cual los parámetros (rombos) permiten determinar los valores iniciales de las ecuaciones que afectan el comportamiento de los niveles (rectángulos) en relación con los flujos de entrada y salida. En el diagrama de Flujo-Nivel de la Fig. 3, se trató que cada un elemento del diagrama de influencias, representara un nivel o acumulador, sin embargo, los elementos Riesgo y Materialización son auxiliares, teniendo en cuenta que su función es determinar si hay daño (materialización) y la proporción del mismo (riesgo); además, estos elementos repercuten como variación, es decir, flujos de salida de los niveles Activos y Controles.

Tabla 1: Lista de parámetros y sus condiciones iniciales

Símbolo	*Definición*
	Nube: representa la fuente del flujo, cuando este es de entrada o el sumidero cuando es de salida.
	Flujo: permite el cálculo de la variación de las unidades de los elementos acumulables.
	Nivel: almacena los cambios o la variación de los flujos para los elementos que se acumulan.
	Auxiliar: permite el cálculo de los estímulos generados como respuesta a un paso de simulación.
	Parámetro: representa las constantes que definen un escenario o situación específica de simulación.

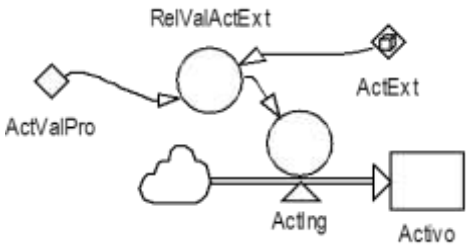

Fig 2: Estructura Básica de Flujo-Nivel

Lenguaje de las Ecuaciones

Según (Gómez, et al., 2015) "la ecuación indica cómo evoluciona la variable de estado en función del flujo que determina su variación". Para el modelo, la variable *ActIng (Ingreso a Activo*, el Flujo) y la variable Activo (el nivel), equivale a la expresión diferencial en la ecuación 1 que el software de modelado asume en términos de una ecuación en notación de Euler.

$$\frac{\mathrm{d}(\mathrm{Activo})}{\mathrm{dt}} = F(t)$$
$$Activo(t+1) = Activo(t) + ActIng(t) \quad (1)$$

La evaluación es realizada por el software en cada paso de simulación generando el comportamiento de cada variable como indica la ecuación 1: el nivel *Contro* en un instante de tiempo t+1 se obtiene sumando al nivel que existía en el tiempo t, con el flujo *ConIng* calculado en t y asumido constante durante el período de tiempo. Además de Flujos y Niveles, en un modelo de DS están presentes otros elementos y relaciones que se describen en términos de Parámetros, Variables Auxiliares y Exógenas, Retardos, Multiplicadores, Clones y Sectores presentados en la Fig. 3. Con el fin de comprender situaciones o hipótesis posibles de presentarse al analizar el comportamiento de la Ciberseguridad, son asignados valores en los parámetros del diagrama flujo-nivel, definidos como escenarios y se procede a analizar el comportamiento de las variables a través del tiempo con el fin de encontrar un pronóstico, que conlleve al análisis e interpretación de los resultados.

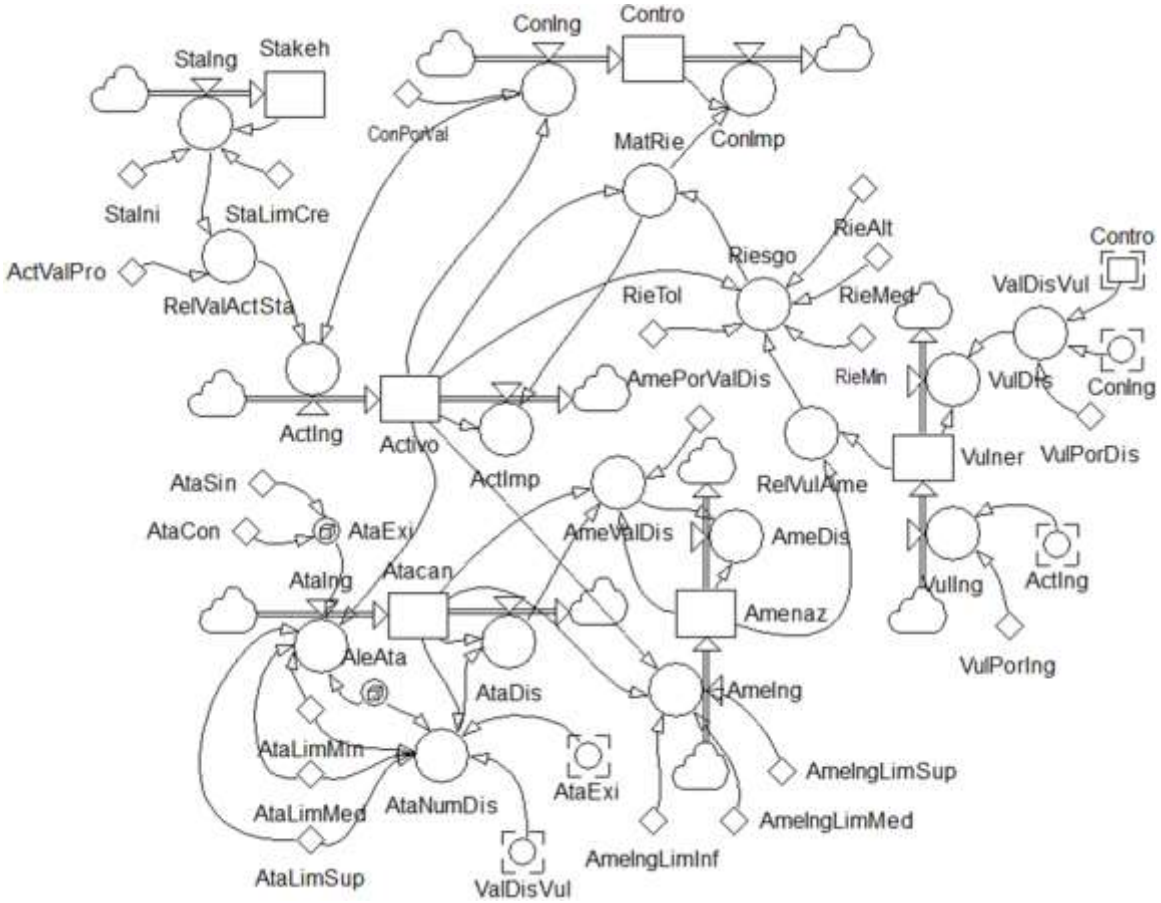

Fig. 3: Diagrama de Flujo-Nivel de los Componentes de la Seguridad

Lenguaje de los Comportamientos

En este artículo serán presentados los Comportamientos (quinto lenguaje de la DS) de dos Escenarios: i) en el primero se considera que los *Stakeholder* invierten el 30% del valor de sus activos en controles, los cuales tendrán una efectividad en su aplicación del 50%, con la premisa que se puede tolerar el 90% del Riesgo; y ii) en el segundo escenario se plantea que el Stakeholder no hace inversión controles, por lo tanto, no existe preocupación por disminuir vulnerabilidades, pese a ello quiere ser tolerante al riesgo en el porcentaje mínimo, es decir, el 10%.

En las Tabla 2 y 3 se presentan los valores definidos para los parámetros del modelo de la Fig. 3 y las unidades de medida definidas para su simulación (Parada *et al.*, 2017). En la Tabla 2 muestra el valor y las unidades de los parámetros generales del modelo. En la Tabla 3 se presenta el resumen del valor y las unidades con las cuales se configuró la simulación de los dos escenarios.

Tabla 2: Lista de parámetros y sus condiciones iniciales

Nombre	*Parámetro*	*Valor*	*Unidades*
Stakeholders Inicio	StaIni	1	Cantidad
Stakeholders Limite Crecimiento	StaLimCre	30	Cantidad
Activos Valor Promedio	ActValPro	500	Millones de Pesos
Atacantes Límite Mínimo	AtaLimMin	1000	Millones de Pesos
Atacantes Límite Medio	AtaLimMed	10000	Millones de Pesos
Atacantes Límite Superior	AtaLimSup	20000	Millones de Pesos
Amenazas Límite Inferior	AmeLimInf	1000	Millones de Pesos
Amenazas Límite Medio	AmeLimMed	10000	Millones de Pesos
Amenazas Límite Superior	AmeLimSup	20000	Millones de Pesos
Vulnerabilidades Porcentaje de Ingreso	VulPorIng	0.25	Porcentaje
Riesgo Alto	RieAlt	0.9	Porcentaje
Riesgo Medio	RieMed	0.5	Porcentaje
Riesgo Mínimo	RieMin	0.1	Porcentaje

Tabla 3: Condiciones Iniciales de los Escenarios propuestos

			Valores	
Nombre	*Parámetro*	*Unidades*	*Escenario 1*	*Escenario 2*
Valor Porcentual de la inversión en controles (Controles Porcentaje Valor)	*ConPorVal*	Porcentaje	0.3	0.0
Efectividad de la aplicación de los controles (Vulnerabilidad Porcentaje Disminución)	*VulPorDis*	Porcentaje	0.5	0.0
Riesgo Tolerable	*RieTol*	Porcentaje	0.9	0.9

Escenario 1: Con controles

Hipótesis: existirán *Stakeholders* que están haciendo un proceso proactivo al estar invirtiendo el 30% del valor de sus activos en controles, los cuales al ser implementados tienen una efectividad del 50%, es decir, que con dicha efectividad se pueda tratar la materialización del riesgo con un impacto alto, alienado a la alta tolerancia del riesgo que está dispuesto a asumir, definida del 90%; esto quiere decir que se espera ser altamente resistente a ataques, pero con tan alto nivel de tolerancia al riesgo, esto en el tiempo hará que la efectividad de la inversión en controles pueda no ser lo suficiente para mitigarlo. Las Fig. 4, 5 y 6 muestran los comportamientos del modelo de los componentes de la seguridad a través de la simulación de lo propuesto en la hipótesis, con las condiciones del escenario 1 (definido con controles).

Los resultados encontrados en la Fig. 4 son los siguientes: i) Los Activos se valorizan exponencialmente; ii) La inversión en Controles (*ConIng*) crece exponencialmente a partir de un valor porcentual de los Activos; iii) La materialización del riesgo (*MatRie*) tiene una tendencia exponencial en su mínima expresión, en razón a que el Riesgo es del 10% del valor de los Activos; y iv) La relación entre las amenazas y las vulnerabilidades (*RelVulAme*) tienen tendencia a crecer, pero se mantienen por debajo del valor de los Activos.

En la Fig. 5 se muestra que los *Stakeholders* aumentan linealmente hasta el mes 30, cuando alcanza su límite de crecimiento, a partir de allí permanece constante; los atacantes (Atacan) oscilan, suben y bajan, no tienen una tendencia clara a la efectividad de los controles; las amenazas (Amenaz) oscilan, no muestran

una tendencia marcada, esto debido a la dependencia de los Atacan quienes tampoco tienen tendencia, aunado que la disminución de vulnerabilidades (*VulDis*) tampoco tiene tendencia. En la Fig. 6 se encuentra que el Riesgo a partir del cuarto mes es constante y se mantiene en el 10%.

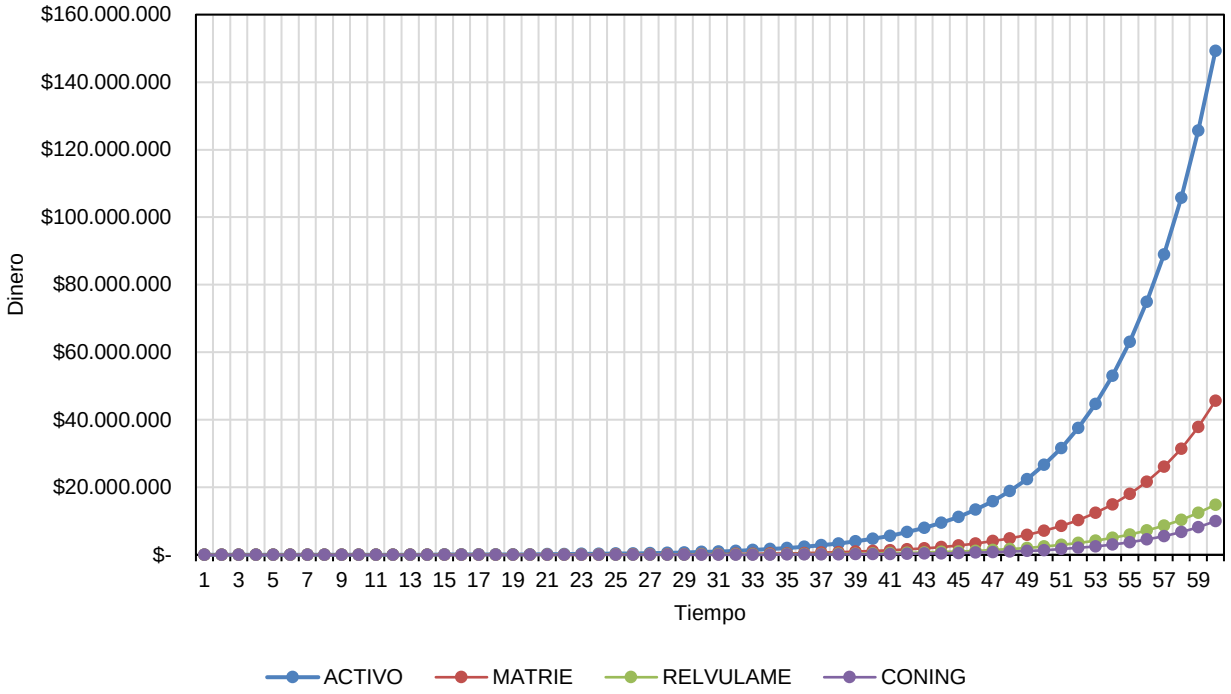

Fig. 4: Comportamientos de las variables Activos – Materialización del Riesgo – Relación Vulnerabilidades y Amenazas – Inversión en Controles en el Escenario 1

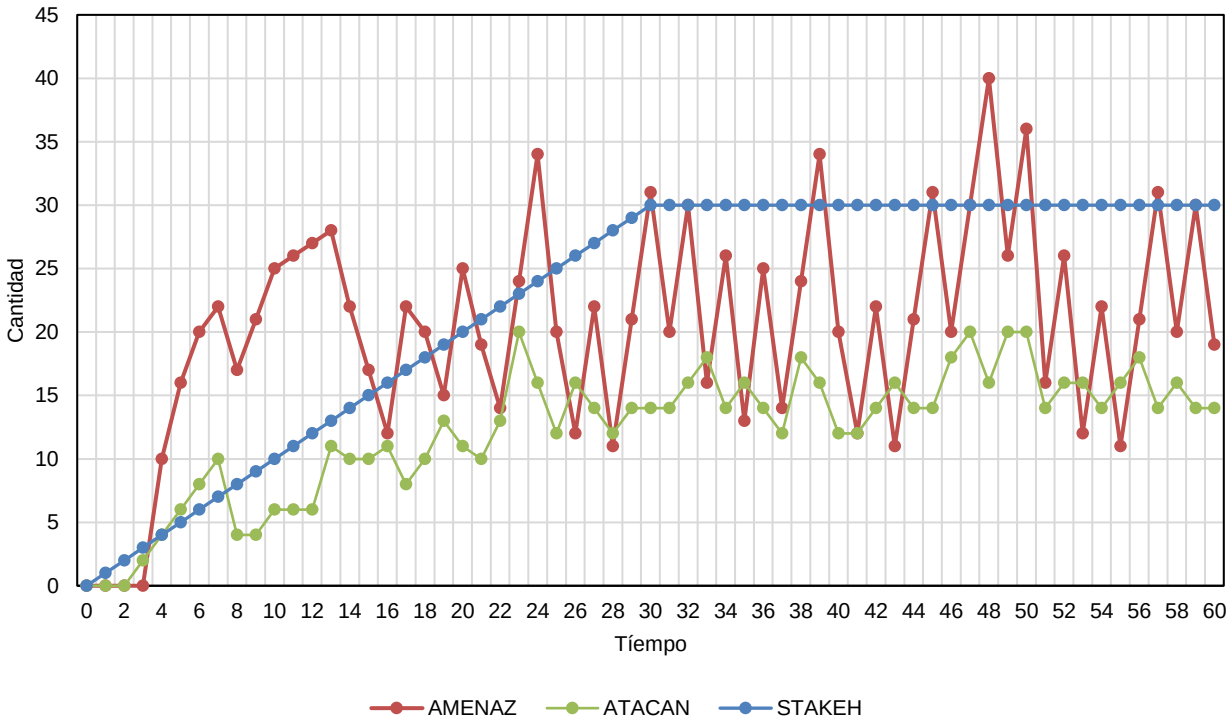

Fig. 5: Comportamientos de las variables Amenazas – Atacantes – *Stakeholders* en el Escenario1

De acuerdo a los resultados encontrados, se concluye que la hipótesis se rechaza, pues el comportamiento no es el esperado; se observa que pese al alto nivel del riesgo (*RieTol*) asumido por el *Stakeholder*, la inversión en controles (*ConPorVal*) es efectiva, con ello se muestra que mientras se monitorice la relación que hay entre amenazas y vulnerabilidades (*RelVulAme*) con el apoyo de los controles (*Contro*), la materialización del riesgo (*MatRie*) se mantiene en niveles por debajo del valor de los activos (*Activo*). En este escenario se encuentra una relación importante que determina lo que se tiene que invertir en controles

(*ConPorVal*) y la efectividad que debe lograrse al aplicarlos (*VulPorDis*), luego se puede concluir que la inversión ideal en controles (*Contro*) es del 30% y que se debe velar porque tengan efectividad (*VulPorDis*) en el orden del 50%; con la parametrización de estos valores los activos se mantienen por encima de la relación de amenazas y vulnerabilidades (*RelVulAme*) y de la misma materialización del riesgo (*MatRie*).

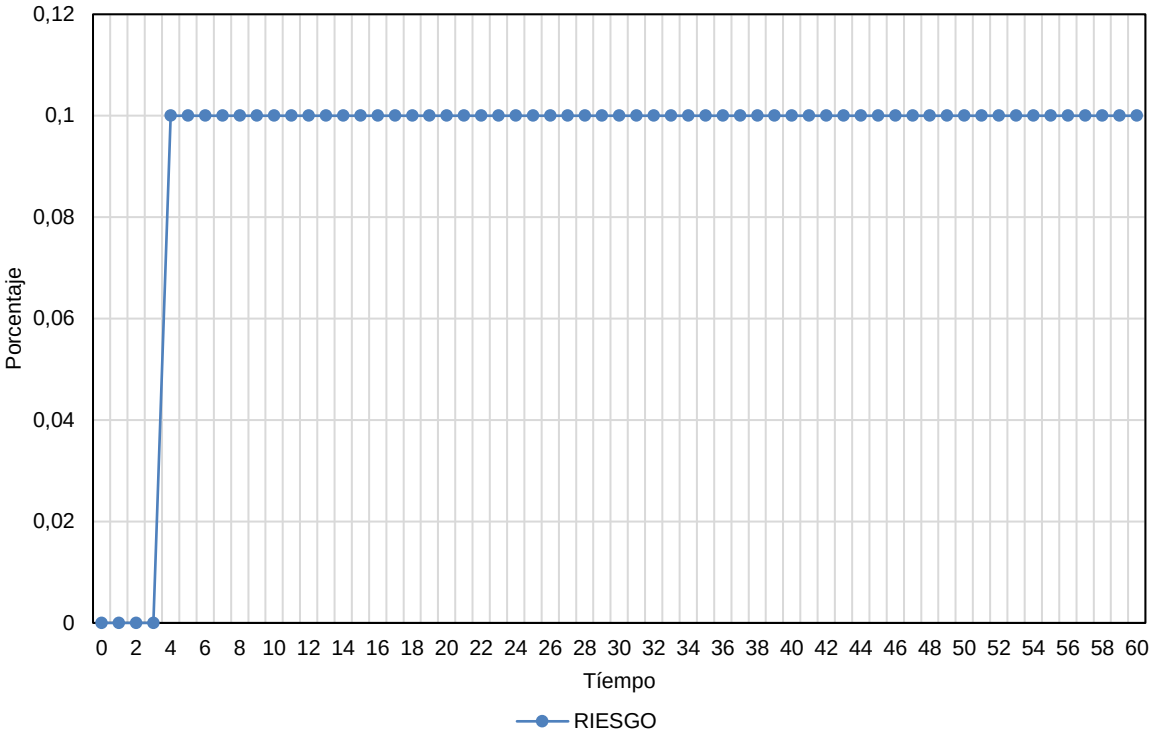

Fig. 6: Comportamientos de la variable Riesgo del Escenario 1

Escenario 2: Sin controles

Hipótesis: los *Stakeholders* confiados en el hecho en que no han tenido afectaciones en sus activos y que por ello no les afectará en el futuro, demuestran su poco o nulo interés en la seguridad de sus activos y por ello no invierten en controles; pretenden manejar un nivel de riesgo en lo máximo tolerable; es de esperar que bajo estas condiciones en el tiempo los *Stakeholders* vean en los niveles más bajos sus activos. Las Fig. 7, 8 y 9 muestran los comportamientos del modelo de los componentes de la seguridad a través de la simulación de lo propuesto en la hipótesis, con las condiciones del escenario 2 (sin controles).

Los resultados encontrados en la Fig. 7 son los siguientes: i) Se valorizan los activos (Activo) hasta el mes 4 y alcanza su máximo valor; en los meses 5 al 7 inicia su depreciación debido a la materialización del riesgo (MatRie); del mes 8 al 30 permanece constante sin valorización ni depreciación, esto debido a la continua llegada de *Stakeholders*, pero cuando estos llegan a su límite de crecimiento, en el mes 31, se deprecian hasta llegar a cero; ii) Por condición inicial, no hay inversión en controles (ConIng) luego su valor permanece en 0. La materialización del riesgo (MatRie) se estimula hasta el mes 4 debido al Riesgo, a partir de allí su presencia es persistente y no permite la valorización de los activos; y iii) Pese a que no hay controles (ConIng), las amenazas y vulnerabilidades (*RelVulAme*) los tres primeros meses no se manifiestan, pero a partir del mes 4, estás crecen como manifestación de los atacantes que fabrican amenazas; en el mes 8 superan el valor de los activos y se muestran como un antecedente, que confirma la falta de controles.

En la Fig. 8 se evidencia la existencia de *Stakeholders* los cuales crecen linealmente hasta el mes 30 cuando alcanza su límite de crecimiento; adicionalmente, se evidencia la existencia de atacantes (Atacan) con un crecimiento lineal hasta el mes 8, pues hay un valor en activos atractivo para ellos, pero a partir del mes 9 estos permanecen constantes debido a que los activos no se valoran lo suficiente y por ello dejan de ser apetecidos por los atacantes; así mismo, hasta el mes 3 no se fabrican amenazas (Amenaz) hasta que no existan suficientes atacantes (Atacan); del mes 4 al 8 se empieza a reflejar la existencia de amenazas, asociado a la aparición de los atacantes, pero a partir del mes 9 se dejan de fabricar, pues con las existentes se está logrando el objetivo, degradar los activos del *Stakeholder.* En la Fig. 9 se muestra que pese a que no hay controles se evidencia Riesgo hasta el mes 4 donde se manifiesta en su escala media, pero luego lo hace en su máxima expresión, 90%, y permanece constante, haciendo que el riesgo se materialice en igual proporción y los activos se degraden hasta llegar a su mínimo.

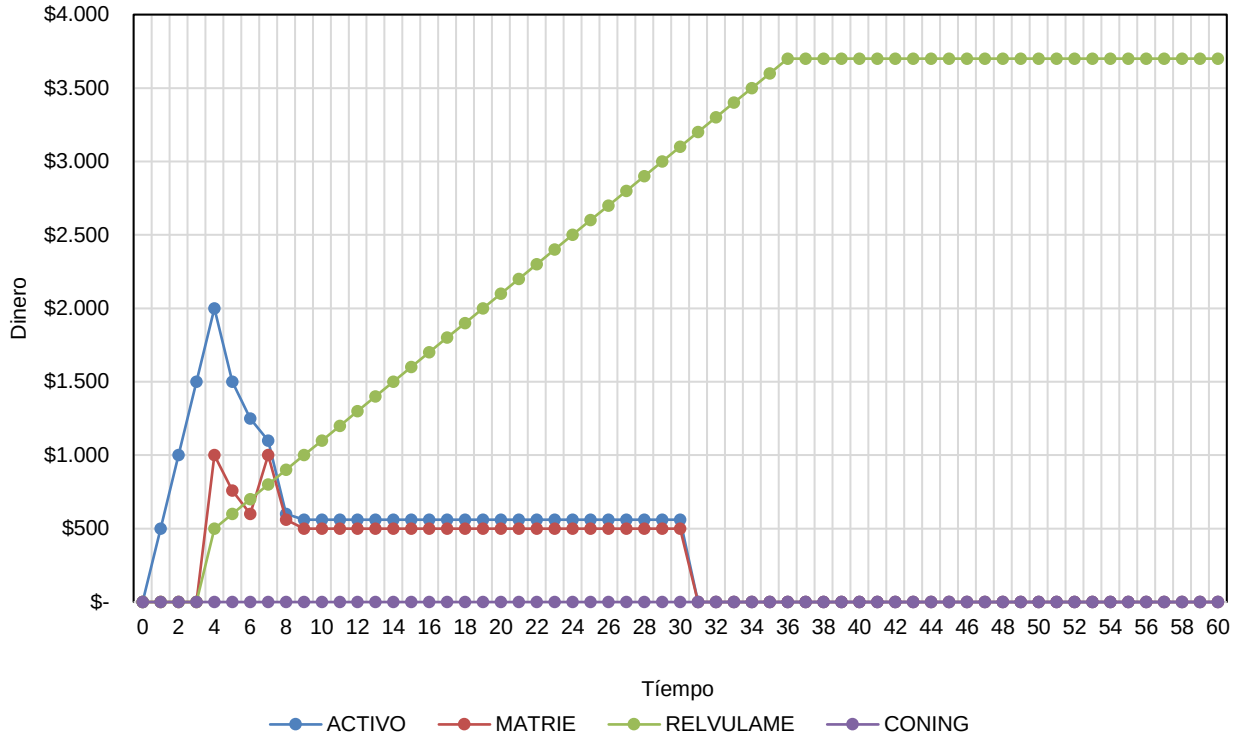

Fig. 7: Comportamientos de las variables Activos – Materialización del Riesgo – Relación Vulnerabilidades y Amenazas – Inversión en Controles del Escenario 2

Respecto a la hipótesis planteada, los comportamientos permiten concluir la aceptación de la misma, ya que al no existir controles (*Contro*) por la falta de inversión en los mismos (*ConPorVal*) se hace insostenible la operación del *Stakeholder*, y la materialización del riesgo (*MatRie)* es inminente, llevando el valor de los Activos a niveles críticos sin importar el aumento en la cantidad de *Stakeholders*; además, pretender manejar condiciones de nivel de riesgo tan altas (*RieTol*) que es pretencioso al no hacer inversión, pues ello hará que las amenazas (*Amenaz*) usen las vulnerabilidades (*Vulner*). Algo que resulta curioso de este escenario es el hecho, que pese de no tener controles (*Contro*), llevó un tiempo considerable (34 meses) para que los activos (*Activo*) lograran niveles críticos, esto denota la influencia que tiene la llegada de nuevos *Stakeholders.*

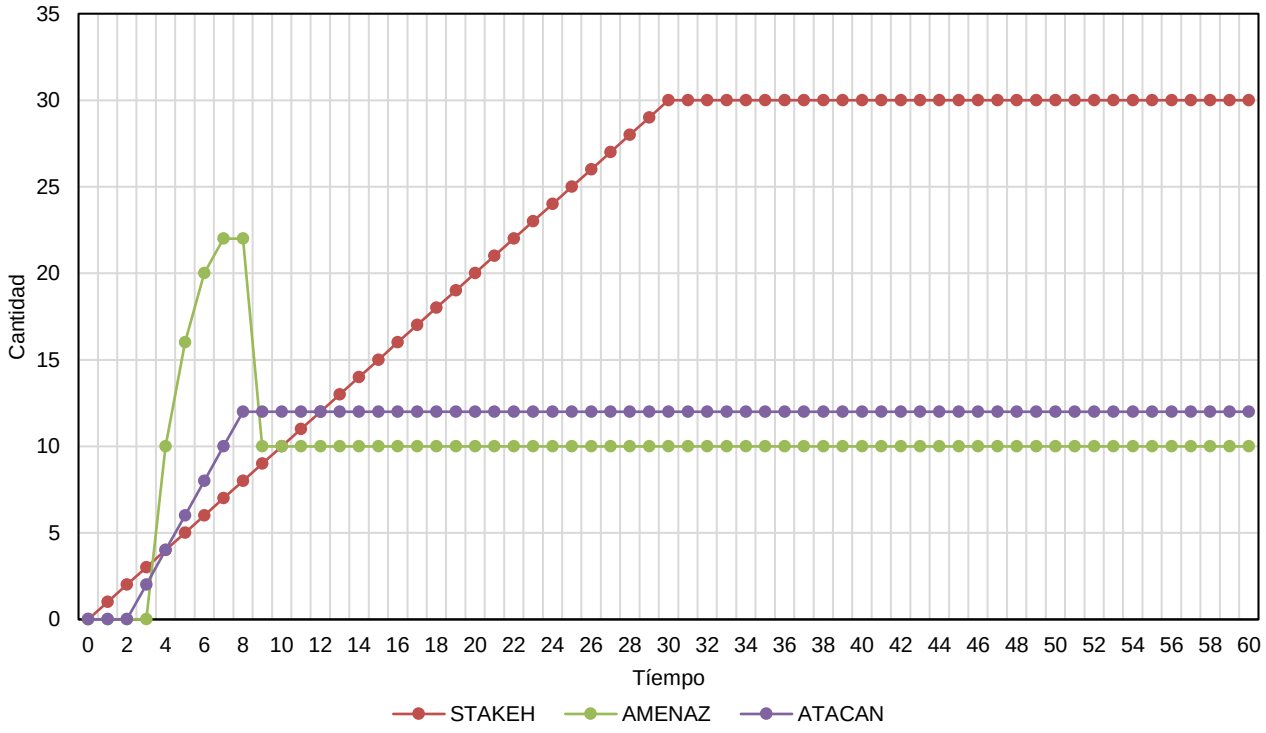

Fig. 8: Comportamientos de las variables Amenazas – Atacantes – *Stakeholders* del Escenario 2

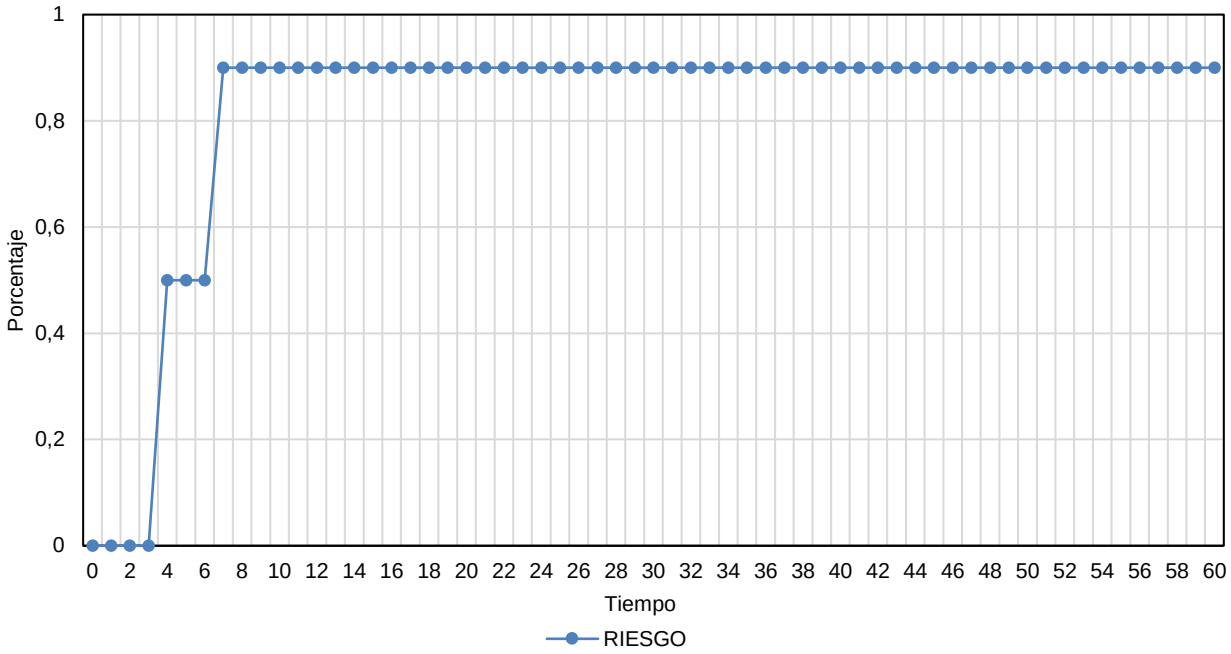

Fig. 9: Comportamientos de la variable Riesgo del Escenario 2

CONCLUSIONES

El análisis sistémico de los componentes de la seguridad es una propuesta útil, pues permite cumplir con el propósito que tiene la DS de poder entender, explicar y pronosticar (a través de escenarios) un fenómeno; para el caso particular, la norma ISO 27032 plantea una cobertura (elementos) los cuales a través del diagrama de influencias se propuso analizar su complejidad con base en la formalización de relaciones y ciclos de realimentación para entender el fenómeno, por medio del diagrama de Flujo – Nivel y de las ecuaciones explicar su funcionamiento mediante la consistencia matemática del modelo; finalmente la simulación permitió pronosticar el comportamiento de los componentes de la seguridad.

Como resultado de las simulaciones, con base en la configuración de parámetros específicos, se observa que los controles juegan un papel fundamental en la valoración de los activos, en el escenario 1 donde se hizo inversión en controles, estos se valoraron, a diferencia del escenario 2 donde los activos al no tener con que salvaguardase de la materialización del riesgo, llegan un punto en el cual se deprecian hasta llegar cero. De acuerdo a los resultados de las simulaciones, se puede observar que el valor de la relación de las amenazas y vulnerabilidades en un escenario sin controles, en el cual se considera nula la inversión en controles, crece linealmente, conllevando a depreciar el valor de los activos, de tal manera que luego de 30 pasos de simulación estos toman el valor de cero, lo que evidencia la materialización del riesgo en dichos activos. Por lo tanto, con las amenazas fabricadas fue suficiente para aprovechar las vulnerabilidades conllevando a la degradación o depreciación de los activos; dichas amenazas continúan constantes, lo cual no permite durante el resto de pasos de simulación la recuperación del valor de los activos. El análisis sistémico de los componentes de la seguridad es un intento por medir la seguridad, aunque de manera subjetiva pues no hay consideraciones claras, es decir, estudios que permitan tener datos de, por ejemplo: cómo medir la materialización del riesgo, cómo relacionar el número de amenazas por atacantes, cómo se valoran los activos y los controles, entre otros.

La DS permite realizar simulaciones que pueden considerarse como experimentos en un sistema para su comprensión o pronóstico. La aplicación de la DS para modelar el comportamiento de la seguridad permite reconocer la complejidad del mismo, además, puede considerarse novedoso al ser representado con esta metodología, aunque requiere que los resultados sean contrastados con la realidad (para lo cual se requiere la definición de datos en un trabajo futuro) y aumentar el grado de certeza que se brinda en las simulaciones. Se recomienda analizar situaciones como las presentadas con los escenarios en donde se puede sugerir, en el caso particular, un margen de inversión en controles con respecto a los activos para su efectividad.

REFERENCIAS

AENOR, UNE 71504:2008: Metodología de análisis y gestión de riesgos para los sistemas de información. (En la web: goo.gl/5XjkQr), 11 octubre de 2012. Acceso: 6 de octubre de 2017 (2012)

Amandeep, S., Rajinder-Sandhu R., Sood, S., Chang, V., A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments, Computers & Security, ISSN: 0167-4048 (2017)

Brechbühl, H., Scott, D., Johnson. E., Protecting Critical Information Infrastructure: Developing Cybersecurity Policy, Information Technology for Development, 16(1), 83–91 (2010)

Calvo, J., D. Parada y A. Flórez, Actualización del Modelo de Arquitectura de Seguridad de la Información - MASI v2.0. Actas del VII Congreso Iberoamericano de Seguridad Informática CIBSI2013, 72-79, Ciudad de Panamá, Panamá, 29 al 31 de Octubre (2013)

Cano, J., Fundamentos de la ciber defensa. Reflexiones sobre la estrategia. (En la web: https://goo.gl/Md2fxi), 8 de marzo de 2015. Acceso: 24 de Julio de 2016 (2015)

Chinchilla, S., Aseguramiento del Gobierno TI. (En la web: goo.gl/w3zwcB), 29 de agosto de 2012. Acceso: 6 de Junio de 2016 (2012)

De Bruin, R. y S.H. Von Solms, Cybersecurity Governance: How can we measure it?, doi: 10.1109/ISTAFRICA.2016.7530578, 2016 IST-Africa Week Conference, Durban, 1-9 (2016)

Flake, F., Industry Specific Q&A: Information Security, Information Tecnhnology Security, and Cybersecurity, Women in the Security Profession: A Practical Guide for Career Development, ElSevier, 95-105 (2017)

Flórez, A., L. Serrano, U. Gómez, L. Suárez, A. Villarraga y H. Rodríguez, H., Analysis of Dynamic Complexity of the Cyber Security Ecosystem of Colombia, doi:10.3390/fi8030033, Future Internet, 8(3), 33 (2016)

Gómez, U., H. Andrade y C. Vásquez, Lineamientos Metodológicos para construir Ambientes de Aprendizaje en Sistemas Productivos Agropecuarios soportados en Dinámica de Sistemas, doi:10.4067/S0718-07642015000400016, Información Tecnológica, 26(4), 125-136 (2015)

Hernández, D. y Vásquez M., La Seguridad de la Información,1ª Ed., Limusa, México D.F., México (2013)

ISO/IEC. International Standard ISO/IEC 27032. Information Tecnhology - Security techniques - Guidelines for Cybersecurity, First Edition, ISO/IEC, Switzerland (2012)

Jaramillo D., A. Cabrera, M. Abad y A. Torres, Definition of Cybersecurity Business Framework based on ADM-TOGAF, CISTI (Iberian Conference on Information System & Tecnologies) 1, 562-567 (2015)

Nagurney, A., Shukla, S., Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability, European Journal of Operational Research, 260, 588–600 (2017)

Parada, D., A. Flórez, A. y U. Gómez, Modelo Estructural del los Observatorios de Ciberseguridad, Documento Interno, Bucaramanga, Colombia (2017)

Portal de Administración Electrónica de España. MAGERIT v.3: “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – Versión 3. (En la web: goo.gl/vruxyu), octubre de 2012. Acceso: 6 de octubre (2017)

Rahimi, F., C. Moller y L. Hvam, Business process management and IT management: the missing integration, International Journal of Information Management, 36(1), 142-154, Gran Bretaña (2016)

Skopik, F., G. Settanni y R. Fiedler, A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing, Computers & Security, doi: 10.1016/j.cose.2016.04.003, 60, 154-176 (2016)