Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas

Informatic organizational security: a simulation model based on systems dynamic.

Víctor Daniel Gil Vera[1], Juan Carlos Gil Vera[2]
[1]*Facultad de Ingeniería y Arquitectura, Fundación Universitaria Luis Amigó, Bogotá, Colombia.*
[2]*Ingeniero de Sistemas e Informática, Universidad Nacional de Colombia, Bogotá, Colombia.*
victor.gilve@amigo.edu.co
jhoancarl@gmail.com

***Resumen*— La seguridad informática permite a las organizaciones proteger sus recursos financieros, sistemas de información, reputación, situación legal, y otros bienes tangibles e intangibles. El objetivo principal de este trabajo es desarrollar un modelo de simulación que permita evaluar el nivel óptimo de seguridad que deben tener las organizaciones considerando aspectos relacionados con la reducción del riesgo y la obtención de beneficios empresariales. La técnica empleada para la construcción del modelo fue dinámica de sistemas, la cual permite modelar y analizar el comportamiento de sistemas complejos en el corto, mediano y largo plazo. El modelo fue construido con el software "POWERSIM", que es un ambiente integrado para la construcción y utilización de modelos de simulación de negocios. Con el desarrollo del modelo se concluye que si las organizaciones no cuentan con un plan director que guíe los esfuerzos de protección de los activos, por mucho dinero que inviertan en seguridad nunca alcanzarán niveles de seguridad satisfactorios.**

***Palabras clave*—Dinámica de Sistemas, Gestión de la Información, Modelos de Simulación, Seguridad Informática, Organizaciones.**

***Abstract*— The computer security enables organizations to protect their financial resources, information systems, reputation, legal situation, and other tangible and intangible properties. The main objective of this paper is to develop a simulation model to evaluate the optimal level of security that must have the organizations, considering aspects related to the reduction of the risk and the acquisition of business benefits. The technique used for the construction of the model was dynamic systems, which allows analyze the behavior of complex systems in the short, medium and long term. The model was built with the software "POWERSIM", which is an integrated environment for the construction and use of simulation models of business. With the development of the model it concludes that if the organizations do not have a master plan to guide efforts to protect the assets, by a lot of money to invest in security never reach satisfactory levels of safety.**

***Key Word* —Dynamic Systems, Information Management, I.T Security, Simulation Models.**

I. INTRODUCCIÓN

En los últimos años, el uso de la informática se ha extendido a la mayoría de actividades profesionales y humanas a nivel mundial. Las redes de comunicación y los sistemas de información (SI) se han convertido en un factor esencial para el desarrollo económico y social de las naciones. Debido a lo anterior, garantizar la seguridad de la información se ha convertido en una tarea de vital importancia y preocupación para empresas, organizaciones e instituciones públicas y privadas.

En la actualidad, día a día se incrementa el uso de ordenadores y dispositivos móviles con acceso a internet para almacenar información: documentos, cartas, hojas de cálculo, imágenes, música, bases de datos de clientes, nóminas, pedidos, facturación, cuentas bancarias y demás [1]. Paralelamente al crecimiento del uso de la informática y de las redes de comunicación se ha incrementado el número de incidentes de seguridad. A mayor volumen de información procesado y transferido informática y telemáticamente, mayor riesgo derivado de su pérdida, alteración o revelación [1].

La seguridad de la información tiene por objeto proteger a los sistemas informáticos de las amenazas a los que están expuestos [2]. Debido a lo anterior, la aplicación de medidas de seguridad debe realizarse de manera planificada y racional, para evitar dirigir esfuerzos e invertir recursos en áreas que no lo requieren [2]. Para que las medidas y mecanismos de protección resulten eficaces, deben integrarse dentro de un sistema más amplio de gestión de la seguridad de la información [2].

Fecha de Recepción: 14 de noviembre de 2015
Fecha de Aceptación: 20 de abril de 2017

La dinámica de sistemas es una técnica de modelado de sistemas complejos cuya filosofía gira en torno al concepto de retroalimentación, o causalidad circular entre variables observables [3]. Es utilizada ampliamente para modelar sistemas en diferentes áreas del conocimiento: agronomía [4], energías renovables [5], ingeniería [6], sanidad pública [7], entre otras.

Para el desarrollo del modelo se empleó el software "POWERSIM". Se simuló una empresa que no cuenta con medidas de seguridad informáticas, la cual tiene que ir atendiendo las posibles eventualidades de ataques a medida que se presentan. El contenido del trabajo se divide como sigue: en primer lugar se presenta una contextualización general de la seguridad informática, el planteamiento del problema, el diagrama causal y el de flujos y niveles, el análisis de resultados y por último las conclusiones obtenidas. Con el desarrollo del modelo se concluye que, si las organizaciones no cuentan con un plan director que guíe los esfuerzos de protección de los activos, por mucho dinero que inviertan en seguridad nunca alcanzarán niveles de seguridad satisfactorios.

II. SEGURIDAD INFORMÁTICA ORGANIZACIONAL

La seguridad informática, de igual manera a como sucede con la seguridad aplicada a otros entornos, trata de minimizar los riesgos asociados al acceso y utilización de determinados sistemas de forma no autorizada y en general malintencionada [8]. El objetivo de la seguridad informática es proteger los recursos informáticos valiosos de la organización, tales como información, hardware o software [8]. A través de la adopción de las medidas adecuadas, la seguridad informática ayuda a una organización a cumplir sus objetivos, permite proteger los recursos financieros, sistemas de información, reputación, situación legal, y otros bienes tanto tangibles e intangibles [8]. En efecto, gestionar la seguridad informática organizacional es una tarea exigente y evaluar el valor de las tecnologías de seguridad es esencial para gestionar eficazmente la seguridad de la información [9].

La Tecnología de la Información (TI) se está extendiendo constantemente a más y más áreas en las organizaciones y es un factor crítico para tener éxito en la economía mundial [10]. La pérdida, manipulación, divulgación, o simplemente la falta de disponibilidad de información causada por incidentes en la seguridad de la misma, pueden dar lugar a gastos, pérdida de beneficios o inclusive consecuencias legales [10]. Los incidentes en la seguridad de la información pueden ser originados por diferentes actores y diferentes motivos [10].

Hackers, profesionales, aficionados, empleados maliciosos, espías industriales, o inclusive terroristas, tratan de introducirse en los sistemas para obtener acceso a la información o simplemente para crear daños [11]. Estas personas buscan vulnerabilidades y utilizan cualquier eslabón débil en la cadena de seguridad de una organización [11]. En la constante lucha para hacer que los sistemas de información sean más seguros, las organizaciones siempre están tratando de encontrar nuevas formas de abordar adecuadamente las cuestiones de seguridad [10].

I. PLANTEAMIENTO DEL PROBLEMA

Existen empresas que no se preocupan por implementar medidas de seguridad informática o si lo hacen, solo consideran externalidades y no tienen en cuenta los riesgos que se puedan presentar al interior de las mismas. El modelo desarrollado en este trabajo hace referencia a una empresa que no cuenta con medidas de seguridad informáticas, y que tiene que ir atendiendo las posibles eventualidades de ataques cuando se presenten. En el modelo se establece que cuando la empresa es víctima de un ataque que se convierte en un incidente, esta aplica una contramedida para responder y solucionarlo, para lo cual debe hacer una inversión en recursos económicos y tecnológicos. Esta estrategia de solución no es óptima, ya que redunda en nuevas vulnerabilidades porque se está tomando medidas para solucionar los eventos a medida que surgen y no se hacen de una forma planificada ni con políticas de seguridad adecuadas. En este escenario, la situación de seguridad no mejora o lo hace muy poco y el costo de invertir en seguridad es muy elevado y se incrementa en términos inmediatos.

II. MODELO DINAMICO CON DIAGRAMA CAUSAL

El modelo presenta el diagrama causal de una empresa sin medidas de seguridad, la cual actúa únicamente en caso de que un ataque se convierta en un incidente. Las variables consideradas en este escenario son: tasa_información, vulnerabilidades, ataques, nuevos_incidentes, e inversión. Ver Figura 1:

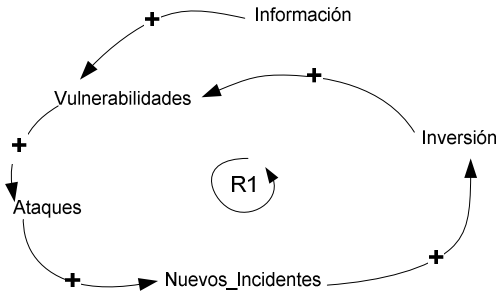


Figura 1. Empresa sin medidas de seguridad. Fuente: Elaboración Propia

Si se invierte en solventar el ataque, no se resuelve el problema porque se descuida otro donde sí se debería invertir, ya que no se tiene un plan definido y no se conocen las necesidades de seguridad, lo que aumenta la vulnerabilidad porque se invierte en algo que no requería mayor atención y se deja de hacer en otra que sí. En la Figura 1, se presenta el ciclo de refuerzo R1, en donde se acentúa el problema de la vulnerabilidad.

III. MODELO DINAMICO CON DIAGRAMA DE FLUJOS Y NIVELES

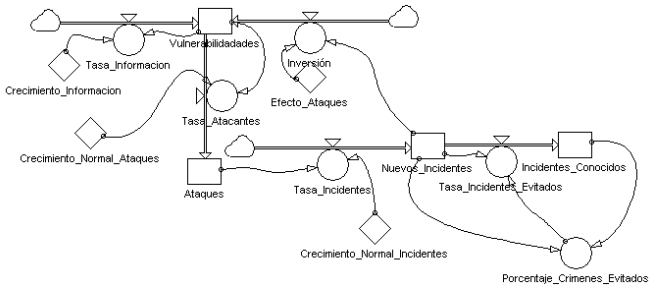


Figura 2. Diagrama de Flujos y Niveles. Fuente: Elaboración Propia

En la Tabla 1, se presenta el resumen de las variables presentadas en la Figura 2, el tipo y las unidades de medición.

TABLA I
VARIABLES, TIPOS Y UNIDADES

Variables	Tipo	Unidades
Crecimiento_Información	Constante	1/mes
Tasa_Información	Flujo	Vulnerabilidades /mes
Vulnerabilidades	Nivel	Vulnerabilidades
Inversión	Flujo	Pesos
Efecto ataques	Constante	Adimensional
Tasa atacantes	Flujo	Atacantes/mes
Crecimiento_Normal Ataques	Constante	1/mes
Ataques	Nivel	Ataques
Tasa_Incidentes	Flujo	Incidentes/mes
Crecimiento_Normal Incidentes	Constante	1/mes
Nuevos_Incidentes	Nivel	Incidentes
Tasa_Incidentes_Evitados	Flujo	Incidentes/mes
Incidentes_Conocidos	Flujo	Incidentes
Porcentaje_Crimenes Evitados	Constante	Incidentes

Tabla 1. Variables, Tipos y Unidades.

A continuación, se presentan las ecuaciones de cada una de las variables establecidas en la Figura 2:

(1) Crecimiento_información = 0.9 *(Constante)*

(2) Tasa_Información = *Crecimiento_Información* Vulnerabilidades*

(3) Vulnerabilidades = *100 + dt * (Tasa_Información) + dt * (Inversión) - dt * (Tasa_Atacantes)*

(4) Inversión = *Nuevos_Incidentes * Efecto_Ataques / 5000*

(5) *Efecto ataques = 0.75*

(6) *Tasa atacantes = Vulnerabilidadades* Crecimiento_Normal_Ataques*

(7) Crecimiento_Normal_Ataques = 0.4

(8) *Ataques* = 100 + dt* (Tasa_Atacantes)

(9) *Tasa_Incidentes* = Ataques*Crecimiento_Normal_Incidentes

(10) Crecimiento_Normal_Incidentes = 0.3

(11) Nuevos_Incidentes = 100

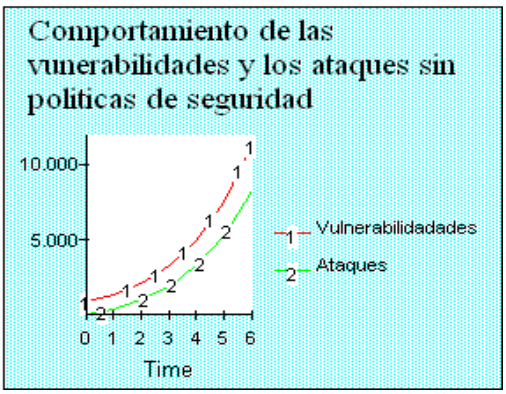
(12) Tasa_Incidentes_Evitados = *Nuevos_Incidentes* % Crimenes_Evitados*

(13) Incidentes_Conocidos = 10

(14) Porcentaje_Crimenes_Evitados = *Incidentes_Conocidos / Nuevos_Incidentes*

IV. ANÁLISIS Y RESULTADOS

El período de tiempo considerado en el modelo, estuvo comprendido de cero a seis meses con una periodicidad mensual. En primer lugar, se analizó el comportamiento de las vulnerabilidades, los ataques y la seguridad. La Figura 3, presenta el comportamiento semestral de las vulnerabilidades, ataques y de la seguridad.

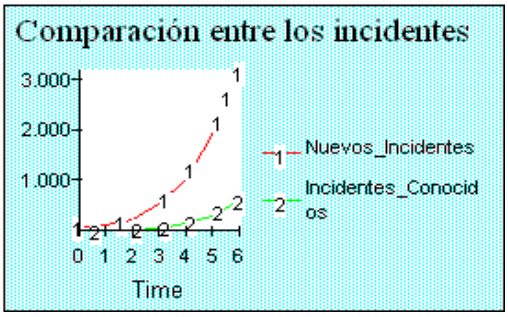


Evolución en seis meses de las vulnerabilidades y los ataques

Time	Ataques	Vulnerabilidadades
0	100,00	1.000,00
1	500,00	1.500,02
2	1.100,0	2.250,04
3	2.000,0	3.375,10
4	3.350,1	5.062,73
5	5.375,2	7.594,25
6	8.412,9	11.391,66

Figura 3. Comportamiento semestral

En la figura 3, se observa que el comportamiento de las vulnerabilidades sigue siendo mayor que los ataques, ya que se simuló el comportamiento con un factor de crecimiento acelerado de la información de 0.9, mientras que el factor de crecimiento normal de ataques fue de 0.4 (conservador). Tanto las vulnerabilidades y los ataques siguen un comportamiento de crecimiento, que es lo que se esperaba del ciclo de refuerzo positivo, que acentúa el problema de la vulnerabilidad al ir invirtiendo en seguridad a medida que surgen los ataques que se convierten en incidentes.

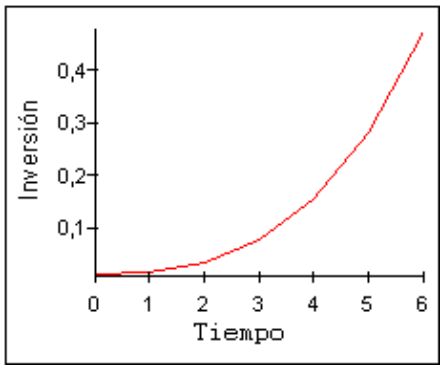


Comportamiento de los incidentes

Time	Nuevos_Incidentes	Incidentes_Conocidos
0	100,00	10,00
1	120,00	20,00
2	250,00	40,00
3	540,00	80,00
4	1.060,01	160,00
5	1.905,03	320,00
6	3.197,57	640,00

Figura 4. Diferencia de los nuevos incidentes frente a los incidentes conocidos.

En la figura 4, se presenta el comportamiento de los incidentes en donde es claro que los nuevos incidentes superan a los incidentes conocidos. El conocimiento por experiencia de incidentes no asegura la seguridad en la organización, la cual sigue siendo igual o más vulnerable.



Tiempo	Inversión
0	0,015
1	0,018
2	0,0375
3	0,081
4	0,159
5	0,286
6	0,48

Figura 5. El comportamiento de la inversión en seguridad

En la Figura 5, se presenta el comportamiento de la inversión en seguridad, la cual muestra que la organización se ve obligada a invertir continuamente.

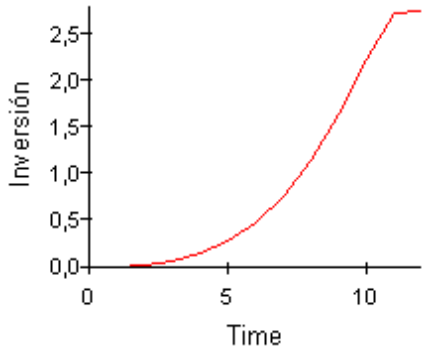


Figura 6. Comportamiento de la inversión en 12 meses.

En la Figura 6, se muestra que la inversión en seguridad se estabiliza a partir de los 12 meses y sigue siendo constante a medida que pasan los meses, posiblemente porque los incidentes conocidos superan a los incidentes nuevos tal y como se presenta en la Figura 7.

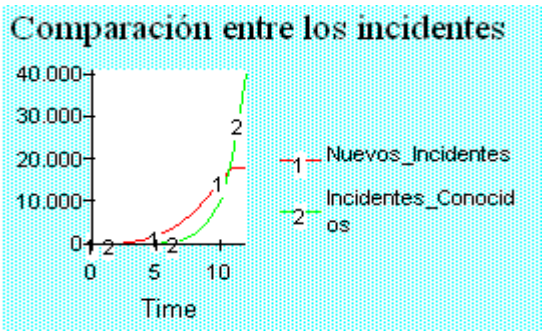


Figura 7. Comportamiento de los incidentes.

V. CONCLUSIONES

Si las organizaciones no cuentan con un plan director que guíe los esfuerzos de protección de los activos, por más dinero que inviertan en seguridad nunca alcanzarán niveles de seguridad satisfactorios.

Debido al alto costo de la seguridad de la información y al hecho de que una organización ciento por ciento segura es una meta casi imposible de alcanzar, los agentes encargados de la seguridad informática deben cuestionarse constantemente si están realizando las inversiones necesarias que garanticen la seguridad de la información.

Las organizaciones deben aprender a determinar la cantidad óptima de inversión en seguridad, tomando como base modelos financieros o basados en análisis económicos de costo-beneficio.

Para futuras investigaciones se recomienda desarrollar modelos de simulación que permitan evaluar el nivel óptimo de seguridad de las organizaciones, teniendo en cuenta no solo aspectos relacionados con la reducción del riesgo, sino también variables macroeconómicas.

REFERENCIAS

[1] O. Delgado and G. Alvaréz, “Seguridad con PGP,” 2008. [Online]. Available: http://www.pcworld.es/archive/seguridad-con-pgp. [Accessed: 04-Nov-2015].

[2] Wikipedia, “Seguridad Informática,” 2015. [Online]. Available: https://es.wikipedia.org/wiki/Seguridad_informática. [Accessed: 04-Nov-2015].

[3] L. Izquierdo, J. Galán, J. Santos, and R. Olmo, “simulación basada en agentes y mediante dinámica de sistemas,” *EMPIRIA. Rev. Metodol. Ciencias Soc.*, vol. 16, pp. 85–112, 2008.

[4] F. Abaunza, S. Arango, and Y. Olaya, “Estrategias de inversión para pequeños caficultores colombianos: una aproximación con dinámica de sistemas,” *Rev. Fac. Nac. Agron.*, vol. 64, no. 2, pp. 6277–6290, 2011.

[5] O. Vásquez, “Modelo de simulación de gestión de residuos sólidos domiciliarios en la Región Metropolitana de Chile,” *Rev. dinámica Sist.*, vol. 1, no. 1, pp. 27–52, 2005.

[6] V. Gil, “Modelo de Simulación de Estrategias de Inversión para Papicultores Colombianos,” *Lampsakos*, vol. 13, pp. 81–87, 2015.

[7] J. B. HOMER and G. B. HIRSCH, “System Dynamics Modeling for Public Health: Background and Opportunities,” *Am. J. Public Health*, vol. 96, no. 3, pp. 452–458, 2006.

[8] P. Galdaméz, “Seguridad Informática.” Actualidad TIC, pp. 1–4, 2011.

[9] C. Huseyin, B. Mishra, and S. Raghunathan, “A Model for Evaluating IT Security Investments,” *Commun. ACM*, vol. 47, no. 7, pp. 87–92, 2004.

[10] A. Schilling and B. Werners, “Optimal selection of IT security safeguards from an existing knowledge base,” *Eur. J. Oper. Res.*, vol. 248, no. 1, pp. 318–327, Jun. 2015.

[11] R. Werlinger, K. Hawkey, and K. Beznosov, “An integrated view of human, organizational, and technological challenges of IT security management,” *Inf. Manag. Comput. Secur.*, vol. 17, no. 1, pp. 4–19, Mar. 2009.