PROPUESTA DE MODELO ORGANIZACIONAL DE MONITOREO DE INCIDENTES DE SISTEMAS INFORMÁTICOS EN PANAMÁ

Magister Iván Ho y Doctor Ramfis Miguelena

Universidad Tecnológica de Panamá,
Programa de Doctorado en Ingeniería de Proyectos
E-mail: Ivanhoq@gmail.com, Ramfis.miguelena@utp.ac.pa

RESUMEN

En esta investigación se describe un proyecto enmarcado en el área de prevención y respuesta a los incidentes informáticos a través del desarrollo de un modelo organizacional de monitoreo de incidentes de sistemas informáticos mediante un Centro de Investigación ubicado en la Universidad Tecnológica de Panamá. Este trabajo tiene como objetivo mostrar los beneficios que tendría para el país al proteger los principales procesos productivos de la economía nacional.

PALABRAS CLAVES

Delitos Informáticos, Auditoria Informática, Manejo de incidentes informáticos,Modelo Organizacional de Incidentes de Seguridad Informáticos.

ABSTRACT

On this research it is described a project focused on the prevention and response of computer incidents area by means the development of a organizational model for monitoring computer security incident through a research center leaded by the Universidad Tecnologica de Panama. The objective of this study is to show the benefits the country would have by protecting the main production processes of the national economy.

KEY WORDS

Cyber Crimes, Computer Audit, Computer Incidents Management, Computer Incidents Response Team, Organizational Model for Computer Security Incident.

INTRODUCCIÓN

Miles de personas caen víctimas de los delitos informáticos. Las computadoras personales y los servidores de las empresas son infectadas en forma masiva por ataques informáticos enviados desde el otro lado del mundo. Estos incidentes de seguridad informática proponen una amenaza a la habilidad de funcionamiento de los sistemas informáticos. Más aún que los sistemas cada vez crecen en complejidad y las redes informáticas van en aumento a nivel mundial.

La investigación estará orientada a la creación de un modelo organizacional de incidentes informáticos que tenga como objetivo proteger infraestructuras críticas de los sistemas informáticos en Panamá, a través de una estructura física establecida en el Centro de Investigación, Desarrollo e Innovación en Tecnologías de la Información y las Comunicaciones (CIDITIC) de la Universidad Tecnológica de Panamá. Consecuentemente, nuestro estudio se basa en la responsabilidad nacional que conlleva la implementación de un modelo organizacional de monitoreo de incidentes de sistemas informáticos para la protección de las infraestructuras criticas de nuestro país.

Este modelo organizacional de monitoreo de incidentes informáticos brindará servicios de seguridad informática a distintos sectores, los cuales pueden ser de la industria, transporte, agricultura, energía, servicios públicos, educación, la banca, las telecomunicaciones entre otros. Las vulnerabilidades de los sistemas de información pueden representar problemas graves, por eso se hace necesario la aplicación de leyes en materia de delitos informáticos para que las empresas y la comunidad en general comprendan lo indispensable que es un modelo organizacional de monitoreo de incidentes informáticos en Panamá.

Los estudios preliminares nos han indicado que no todos los equipos de respuesta de incidentes trabajan de la misma forma. Ya que varían de acuerdo a la realidad cultural, económica y legal de cada país. En Panamá, no existen modelos organizacionales internos de incidentes informáticos en ningún sector público o privado. Al proponer un modelo organizacional local contribuirá asimismo a asegurar la eficacia desde el punto de vista de la seguridad y los programas desarrollados internamente en Panamá tanto para el sector privado, público y a nivel universitario. Solo a partir del 26 de septiembre de 2011, a través del "Decreto Ejecutivo No. 709 publicado en la Gaceta Oficial No. 26880 se crea apenas la entidad para dar respuesta a incidentes de seguridad de los sistemas informáticos y de las comunicaciones del Estado Panameño".[1].

Se trata del CSIRT Panamá (Equipo Nacional de Respuesta a Incidentes de Seguridad de la Información del Estado Panameño), que realizará las acciones necesarias de prevención, tratamiento, identificación y resolución de ataques a incidentes de seguridad sobre los sistemas informáticos solamente para instituciones del Estado. En este decreto se establece que la Autoridad Nacional para la Innovación Gubernamental (AIG), será la encargada de la implementación, operación y administración del CSIRT Panamá. A su vez, se investigó que la ley existente aún no se ha ejecutado en nuestro país.

OBJETIVO

El Modelo Organizacional de Monitoreo de Incidentes de Sistemas Informáticos que proponemos desarrollar a través de esta investigación tiene dentro de sus finalidades alertar, educar y realizar análisis de riesgos, con la finalidad de proteger las infraestructuras criticas de sistemas para que no sean víctimas de delitos informáticos. En esta investigación se está en la búsqueda específica de las mejores prácticas fundamentales en los procesos de prevención, evaluación, recolección y administración de la evidencia digital que ayudaran a mejorar la eficiencia en los procesos de desarrollo de un modelo organizacional de respuesta de incidentes de seguridad informática en Panamá. La finalidad es la de incrementar los controles de

seguridad en el uso de las redes informáticas, demostrando las nuevas responsabilidades de todos los sectores públicos y privados.

En la actualidad, las tecnologías de la información y la comunicación están omnipresentes y cada vez es mayor la predilección hacia la digitalización. El internet es una de las áreas de más rápido crecimiento en el desarrollo de la infraestructura técnica. La demanda de Internet y la conectividad informática ha dado lugar a la integración de la tecnología informática en productos que normalmente funcionaban sin ella, tales como los vehículos y residencias.

Las computadoras se utilizan no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino que se presenta en casi todos los campos de la vida actual. Con este enfoque en mente se proporciona una perspectiva completa de los temas más importantes vinculados a los aspectos de prevención de los crímenes informáticos en nuestro país. Debido a la dimensión transnacional del crimen informático, los instrumentos jurídicos son los mismos para las compañías privadas como para las entidades públicas.

A nivel nacional, se trata de una responsabilidad compartida que requiere una acción coordinada para la prevención, preparación y respuesta de incidentes informáticos por parte de las autoridades como la Dirección General de Comercio Electrónico del Ministerio de Comercio e Industrias de Panamá, por el Ministerio Publico de Panamá, La Autoridad de Innovación Gubernamental (AIG), La Asamblea Legislativa de la República de Panamá y además, mundialmente por diversas entidades de seguridad sobre delitos informáticos.

ASPECTOS METODOLÓGICOS

En el desarrollo de la investigación se realizó el primer acercamiento de la Dirección General de Comercio Electrónico del Ministerio de Comercio e Industrias de Panamá, el Ministerio Publico de Panamá, La Asamblea Legislativa de la República de Panamá, La Autoridad Nacional para la Innovación Gubernamental en Panamá (AIG), la Dirección de Investigación Criminal en Panamá y la Fiscalía Especializada en Delitos contra la Propie-

dad Intelectual y Seguridad Informática y la Universidad Tecnológica de Panamá. En la cual se indagaron sus avances con respecto a un sistema de respuesta de incidentes de emergencias informáticas en nuestro país. Se procedió a la recolección de datos, aplicación del instrumento, vistas de campo y reuniones técnicas para recopilar información del proyecto seleccionado como caso de estudio de los equipos de respuesta de incidentes informáticos alrededor del mundo.

El propósito es establecer un modelo organizacional de monitoreo de incidentes de sistemas informáticos en Panamá, con una metodología práctica, y factible para convertir entornos computarizados inseguros en entornos seguros, y lograr una clara valorización de los mismos, teniendo en cuenta el objetivo y los procesos del entorno de los negocios. Ya que los modelos organizacionales de monitoreo de incidentes de sistemas informáticos varían de acuerdo con la realidad cultural, económica y legal de cada país.

ENFOQUES LEGISLATIVOS

El desafío principal de los sistemas jurídicos penales nacionales es el retraso existente entre el reconocimiento de amenazas potenciales de las nuevas tecnologías y las reformas necesarias que deben introducirse en las legislaciones nacionales. Este reto sigue siendo tan importante y fundamental como siempre, puesto que cada vez es mayor la rapidez en la innovación de las redes. Muchos países están trabajando intensamente para introducir los ajustes jurídicos pertinentes.

En Panamá, ya se cuenta con legislaciones para facilitar la evolución tecnológica y a su vez que se restringe las secuelas de los fraudes informáticos que se pueden generar en nuestro país. En tal sentido la "Ley Nº. 51, de 22 de julio de 2008, establece responsabilidades reguladoras y fiscalizadoras a la Dirección General de Comercio Electrónico del Ministerio de Comercio e Industrias de Panamá".[2], que la instituye como unidad administrativa encargada de promover las normas y regulaciones para la actividades relacionadas con el comercio electrónico, tanto para el sector público como en el privado, ésta a su vez establece las políticas y responsabilidades para la interacción entre los usuarios particulares y el gobierno.

DESCRIPCIÓN DE LA SITUACIÓN ACTUAL DE LA INVESTIGACIÓN

El peligro del terrorismo cibernético aumentará en el nuevo siglo, a medida que las posiciones de liderazgo dentro de las organizaciones extremistas las ocupen cada vez más individuos especializados en el Internet. La mayor preocupación la inspira un ataque potencial coordinado contra las infraestructuras críticas nacionales.

Si bien no se ha experimentado aún este tipo de ataque, no es difícil anticipar una amenaza tal a partir de las intrusiones que hemos presenciado. Las ofensivas cibernéticas no conocen fronteras nacionales y son realmente internacionales sus alcances. La cooperación internacional y el intercambio de información son esenciales para responder con más efectividad a esta amenaza.

El objetivo operacional es la creación de un equipo de respuesta a incidentes informáticos que tenga como foco proteger infraestructuras críticas de los sistemas informáticos, para que ningún deterioro de los sistemas puedan poner en peligros las continuidades de las operaciones tanto financieros, humanos y tecnológicos.

PROPUESTA DE LA INVESTIGACIÓN

Es inevitable que en Panamá se promuevan y divulguen los aspectos legales referentes a los crímenes cibernéticos y a su impacto en el marco jurídico nacional. Es evidente indicar que el rasgo característico de la auditoría de sistemas es demostrar que los resultados generados deben concluir con un proceso que sea legalmente aceptable; motivo por el cual el análisis forense debe realizarse cumpliendo con todos los requisitos legales. El incumplimiento de los mismos originará que la evidencia digital sea considerada inaceptable posibilitando que el proceso origine desconfianza en la presentación de evidencia forense.

El modelo organizacional de monitoreo de incidentes de sistemas informáticos propuesto, además de revisar estándares internacionales de sistemas de seguridad informática nos dará la oportunidad de crear nues-

tros propios estándares nacionales referentes a la administración de modelos organizacionales de incidentes informáticos. Bajo un modelo panameño de seguridad radica la particularidad que puede llegar a tener las mejores prácticas en el territorio nacional.

En Panamá, no existe ninguna organización que cuente con un modelo organizacional de monitoreo de incidentes informáticos, ni siquiera al menos un conjunto mínimo de procedimientos para el manejo de incidentes informático de seguridad a nivel nacional.

Se observa la total ausencia de procesos de alerta, respuesta, administración y coordinación de incidentes que indica el nivel de riesgo al que está expuesto las entidades privadas, públicas y organizaciones académicas del país.

BENEFICIOS DE LA INVESTIGACIÓN

A continuación se detallan los beneficios que en particular prestará el modelo organizacional de monitoreo de incidentes de sistemas informáticos nacional propuestos en nuestra investigación que lo hacen diferentes de los demás modelos existentes:

- Punto confiable de contacto en el caso de un incidente informático a nivel nacional.
- Desarrollar una infraestructura física y tecnológica que coordine las respuestas a los ataques informáticos del país.
- Desarrollar la capacidad de conocimiento sobre las estrategias de mitigación de incidentes informáticos con los miembros de la sociedad a nivel nacional.
- A través de este modelo propuesto se generaran investigaciones que conlleven a la aplicación del mismo para que se adecúen a su utilización en las instituciones privadas, públicas y universitarias.
- Coordinación y contacto sobre los incidentes informáticos con otras entidades a nivel internacional.
- Se presentarán modelos para el cálculo del retorno de la inversión en los sistemas informáticos.

- Se promoverá la coordinación de la presentación de las acciones penales y demandas civiles en el caso de los incidentes informáticos.
- Se promoverá la evaluación de productos de seguridad por parte de las entidades privadas, públicas y la sociedad en general.
- Se promoverá la administración de modelos organizacionales de monitoreo. de incidentes informáticos utilizando los estándares de seguridad de sistemas internacionales y estándares de procesos de mejoras continúas.

"El Centro de Investigación, Desarrollo e Innovación en Tecnologías de la Información y las Comunicaciones (CIDITIC) actualmente tiene como misión generar investigaciones de alto nivel relacionadas con el área de las TIC's que a la vez sean transferidas a la comunidad nacional e internacional a través de publicaciones científicas de reconocida trayectoria internacional y de unidades de extensión, lo cual permita coadyuvar con el desarrollo nacional".[3].

ESTRUCTURA ORGANIZATIVA CONCEPTUAL DEL MODELO ORGANIZACIONAL DE MONITO-REO DE INCIDENTES INFORMÁTICOS DENTRO DEL CIDITIC

A continuación se presenta en la figura 1, la estructura organizacional conceptual Modelo de Organizacional de Monitoreo de Incidentes Informáticos dentro del Centro de Investigación.

El desarrollo del Modelo de Monitoreo de Incidentes Informáticos comprende cuatro secciones de manera que puedan cubrir los diversos aspectos que involucra un incidente de seguridad a nivel nacional. El cual estará asignado al Departamento de Investigación y Desarrollo bajo la Unidad de Redes y Seguridad Informática del Centro.

Sección de Alertas y Advertencias se encargará de los servicios reactivos:

- Análisis de incidentes.
- Alertas y advertencias.
- Tratamiento de incidentes.
- Apoyo a la respuesta a incidentes.
- Coordinación de la respuesta a incidentes.
- Respuesta a incidentes.
- Tratamiento de la vulnerabilidad.
- Análisis de la vulnerabilidad.
- Respuesta a la Vulnerabilidad.
- Coordinación de la respuesta a la vulnerabilidad-.

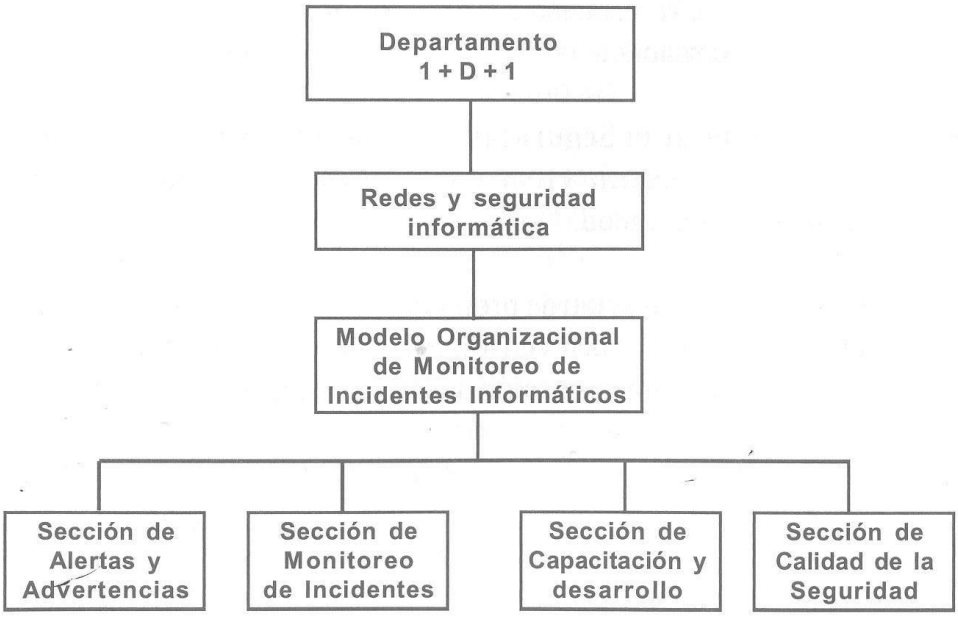

Figura 1. Estructura Organizativa Conceptual del Modelo Organizacional de Monitoreo de Incidentes Informáticos dentro del CIDITIC.

Fuente: Elaborado por el investigador. 2011.

Sección de Monitoreo de Incidentes se encargará de los servicios proactivos:

- Comunicación a las entidades privadas, públicas, educativas y a la población en general.
- Evaluaciones o auditorías de la seguridad.
- Configuración y mantenimiento de la seguridad.
- Servicios de detección de intrusos.
- Difusión de información relacionada con la seguridad.
- Análisis de infraestructura.

Sección de Capacitación y Desarrollo se encargará de los servicios de manejo de incidentes:

- Análisis de solicitudes.
- Respuesta a las solicitudes.
- Coordinación de la respuesta a las solicitudes.
- Educación / Formación.

Sección de la Calidad de la Seguridad de encargará de:

- Continuidad del negocio y recuperación tras un desastre.
- Consultoría de seguridad.
- Sensibilización.
- Evaluación o certificación de productos.
- Calculo del retorno de la inversión en los sistemas informáticos.
- Coordinación en la presentación de denuncias penales y civiles.
- Evaluación de productos de seguridad.
- Administración del modelo de mejoras continúa.
- Análisis de riesgos.

PROCESOS DE MODELO ORGANIZACIONAL DE MONITOREO DE INCIDENTES INFORMÁTICOS

El modelo organizacional de monitoreo de incidentes informáticos identifica tres niveles de los procesos de apoyo:

- **Identificación:** Identificación de alertas o necesidades de investigación y desarrollos de las entidades privadas, públicas y el público en general.
- **Gestión:** Proceso de gestión de reacción, logística y estrategias necesarias para la puesta en operación de los mecanismos de monitoreo de seguridad informática.
- **Servicios:** Proceso encargado de proporcionar la información oficial que provenga de las actividades del modelo organizacional de monitoreo de incidentes informáticos.

En base a este modelo proponemos mejorar las condiciones de seguridad informática para prevenir a la comunidad, empresas privadas y públicas que sean víctimas de delitos informáticos. Además, dentro del modelo organizacional se incluirá la forma de conducción de implicaciones legales que conllevará su aplicación dentro de la legislación panameña.

Conjuntamente, se implementarán sistemas de mejoras continuas dentro del modelo organizacional propuesto, adicionalmente se implementarán la formulación del cálculo del retorno de la inversión en los sistemas informáticos.

A pesar que existen muchos modelos organizacionales de monitoreo de incidentes de sistemas informáticos a nivel mundial estos aspectos mencionados anteriormente no están cubiertos en particular en esos modelos. Convirtiéndose en un modelo organizacional de incidentes informáticos innovador creado específicamente para nuestra geografía nacional.

CONCLUSIONES

La seguridad de la información a nivel nacional es un punto crítico y se convierte en soporte básico para la seguridad de la infraestructura de telecomunicaciones del país. Por esta razón se propone establecer un centro dedicado en la Universidad Tecnológica de Panamá en el Centro de Investigación, Desarrollo e Innovación en Tecnologías de la Información y las Comunicaciones (CIDITIC).

Siguiendo este Modelo de Monitoreo de Incidentes de Sistemas Informáticos, el cual se encargaría de coordinara los procesos de fortalecimiento de la información, para prevenir, combatir, mitigar, solucionar y protegerse los activos frente a los peligros, vulnerabilidades e incidentes de seguridad de la información de usuarios en entidades privadas, universitarias y públicas delimitándonos solo al área de infraestructura de los sistemas informáticos. Igualmente este modelo servirá como centro de entrenamiento y difusión de la información en múltiples aspectos sobre la seguridad informática en Panamá.

REFERENCIAS

[1] Decreto Ejecutivo Nº. 709, República de Panamá, publicado en la Gaceta Oficial Nº. 26880, 27-09-2011. República de Panamá.

[2] Ley Nº. 51, de 22 de julio de 2008, República de Panamá, publicado en la Gaceta Oficial Nº. 26090, (24-07-2008). República de Panamá.

[3] Estructura Organizacional del Centro de Investigación, Desarrollo e Innovación en Tecnologías de la Información y las Comunicaciones (CIDITIC), Universidad Tecnológica de Panamá, http://www.ciditic.-utp.ac.pa/organigram.

[4] Manual sobre el Ciberdelito: Guía para los Países en Desarrollo, Unión Internacional de Telecomunicaciones, abril de.2009.

[5] Como Crear un CSIRT Paso a Paso, Agencia Europea de Seguridad de las Redes y de la Información (ENISA), 2006.

[6] Informe Final Para la Constitución de un CSIRT Colombiano, Ministerio de Comunicaciones, República de Colombia, diciembre de 2008.

[7] West-Brown, Moira J.; Stikvoort, Don, Kossakowski; Klaus-Peter; Killcrece Georgia; Ruefle, Robin; Zajicek, Mark. Handbook for Computer Security Incident Response Teams (CSIRTs). First release: December 1998, 2nd Edition: April 2003.

Referencias Bibliográficas

ARDAO, A. (1986). Panamericanismo y Latinoamericanismo. En Zea, L (Ed.). *América Latina en sus ideas*. México: Siglo XXI Editores

ATKINS, P. (1979). *América Latina en el Sistema Político Internacional*. México: Ediciones Gernika

CUEVA, A. (1984). *El desarrollo del capitalismo en América Latina*. Octava Edición. México: Siglo XXI Editores.

DUQUE, M. (2006). *La Agenda Oculta Geoestratégica de la Integración USA*. Bogotá: Ediciones desde Abajo.

GALEANO, E. (1984). *Las Venas Abiertas de América Latina*. Trigésima octava Edición. México: Siglo XXI Editores.

GONZÁLEZ, B. (2008). *Más Allá del Libre Comercio: Seguridad Esencial*. Heredia: CIDCSO-UNA.

GUERRA, V. (2006). *Breve Historia de América Latina*. Universidad de Michigan: Editorial de Ciencias Sociales.

HINKELAMMERT, F. (2003). *Solidaridad o Suicidio Colectivo*. Heredia: Ambientico Ediciones.

MAGDOFF, H. (1969). *La Era del Imperialismo. Política Económica Internacional de Estados Unidos*. México: Editorial Nuestro Tiempo, S.A.

QUESADA, R. (2006). *Globalización y Deshumanización. Dos caras del Capitalismo Avanzado*. Heredia: EUNA: EUCR.

REGALADO, R. (2006). *América Latina entre Siglos. Dominación, Crisis, Lucha Social y Alternativas Políticas de la Izquierda*. La Habana: Ocean Sur.

SAXE FERNÁNDEZ, E. (1999). *La Nueva Oligarquía Latinoamericana: Ideología y Democracia*. Heredia: EUNA.

SAXE FERNÁNDEZ, E. (2005). *Colapso Mundial y Guerra*. San José: AMO AL SUR.

SAXE-FERNÁNDEZ, J y Delgado-Ramos, G. (2004). *Imperialismo y Banco Mundial*. Madrid: Editorial Popular, S.A.

SUÁREZ, L. (2006). *Un Siglo de Terror en América Latina. Crónica de Crímenes de Estados Unidos contra la Humanidad*. La Habana: Ocean Sur.

Referencias Electrónicas

RAMONET, I. (2009, abril). La nueva Suramérica. *Le Monde Diplomatique, 162*. Recuperado el 20 de abril de 2009 de http://www.mondiplo.com/isum/Direct.jsp?ISUM_Shortcut=MONDIPLO_EDITORIAL