UNIVERSIDAD Rafael Belloso Chacín

Revista Electrónica de Estudios Telemáticos

TÉLÉMATIQUE

LAS MÉTRICAS, ELEMENTO FUNDAMENTAL EN LA CONSTRUCCIÓN DE MODELOS DE MADUREZ DE LA SEGURIDAD INFORMÁTICA

(Metrics, a fundamental element in the construction of informatics security maturity models)

Recibido: 02/02/2011 **Aceptado:** 28/07/2011

Villegas, Marianella
Universidad Simón Bolívar, Venezuela
nellavillegas@usb.ve

Meza, Marina
Universidad Simón Bolívar, Venezuela
mmeza@usb.ve

León, Pilar
Universidad Simón Bolívar, Venezuela
pleon@usb.ve

RESUMEN

En las organizaciones se requiere gestionar la seguridad informática para asegurar un entorno informático institucional, mediante la administración del recurso humano y tecnológico, para ello es necesario emplear dispositivos reguladores de las funciones y actividades desarrolladas por el personal de la institución. El propósito de este trabajo fue construir métricas de seguridad que permitan cuantificar, tomar decisiones y mejorar el desempeño de los sistemas de seguridad informática en las universidades de la Región Capital. Para esta investigación, en primer lugar, se realizó una revisión bibliográfica que sustenta los referenciales conceptuales acerca de métricas de seguridad, sus tipos e indicadores, y en segundo, se establecen los niveles de seguridad informática. A partir de estos niveles se elaboró y validó un cuestionario que fue aplicado a los administradores o encargados de la seguridad de las universidades seleccionadas en la Región Capital. Posteriormente, se analizaron los datos y se identificó un conjunto de indicadores que permitieron la construcción de métricas para cada nivel. Las métricas resultantes permiten medir el desempeño institucional frente a los retos que plantea la preservación y el resguardo informático, así como identificar el origen de los desempeños no satisfactorios y las áreas informáticas que requieren ser mejoradas. Asimismo, éstas facilitan el establecimiento de renovadas políticas de seguridad informática, donde se lleva a cabo una redefinición de metas y objetivos que vayan a la par de los cambios tecnológicos para enfrentar amenazas y vulnerabilidades que pudieran surgir en el futuro.

Palabras clave: Métricas, Indicadores, Modelos de madurez de la seguridad informática, Controles.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 10 Edición No 1 – Año 2011

ABSTRACT

In organizations, information security is required to guarantee institutional information environment, through human resources and technological management, to do so, it is necessary to use regulatory devices for functions and activities developed by institution personnel. The purpose of this paper was to construct security metrics that allow measuring, making decisions and improving information security systems performance in Capital District universities. In order to carry out this research, a literature review was done which supported conceptual references about security metrics, their types and indicators, and information security levels were established. From these levels, a questionnaire was designed and validated; it was applied to information security administrators or managers at selected Capital District universities. Then, the data was analyzed and a set of indicators which permitted metrics construction for each level. Resulting metrics made possible to measure institutional performance against challenges for preservation and protection of information, as well as identifying the origin of not satisfactory performance and informatics areas which require being improved. Likewise, metrics facilitate the establishment of new information security policies, where goals and objectives redefinition is carried out at the same time with technological changes to face threats and vulnerabilities that would arise in the future.

Keywords: Indicators, Metrics, Information security management models, Controls.

INTRODUCCIÓN

A partir de los años cincuenta, se han utilizado diferentes términos para denominar y comunicar los fenómenos relacionados con la convergencia de la cibernética, la computación científica, la automatización, el procesamiento automático de datos, los sistemas de computación de datos, la telemática y la robótica.

Es indudable que luego del año 2000 se ha iniciado una nueva era en lo concerniente a la inserción, innovación y gobernabilidad de las nuevas tecnologías de la información y la comunicación, caracterizada por las necesidades y acciones referidas a la seguridad en general (social, jurídica y económica, entre otros) en particular a la seguridad informática, ya que es ésta la que permite el entrecruzamiento y la trazabilidad de todas ellas para asegurar las demandas cruciales de estos tiempos: confiabilidad, transparencia y accesibilidad en la gestión de las instituciones.

Durante la década de los setenta y ochenta, la formulación de políticas de información e informática estaban signadas por sus implicaciones en el desarrollo organizacional. A partir de los noventa, surgen modelos más liberales y el foco pasó a la disponibilidad de plataformas tecnológicas para soportar “modelos de negocios”, tanto en lo público como en lo privado.

A partir del año 2001, la situación ha cambiado totalmente. La seguridad se transformó de una razón de Estado a una “cultura de la seguridad” y se generaron programas para la sensibilización y concientización de cada ciudadano, con el fin de revertir los efectos de la

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 10 Edición No 1 – Año 2011

"ingeniería social" realizada por entes interesados en vulnerar el "orden social e institucional" de naciones, corporaciones y/o instituciones científicas.

El concepto de "seguridad informática" se ha popularizado a nivel mundial a través de las Normas ISO 17799 y BS 7799-2, utilizadas por las empresas e instituciones. Actualmente en Venezuela se están utilizando mecanismos de control como la Ley de Habeas Data (Enmienda Nº 1 de la CRBV de fecha 15 de febrero de 2009, Gaceta Oficial Extraordinaria Nº 5.908, artículos: 28 y 60, entre otros), la Firma Digital (Decreto con Fuerza De Ley de 2.001 sobre Mensajes de Datos y Firmas Electrónicas) y la Ley Especial contra los Delitos Informáticos (Gaceta Oficial 37.313 del 30 de octubre de 2001).

En una investigación previa se evidenció la vulnerabilidad de los sistemas informáticos y del personal a cargo en una muestra de universidades de la zona metropolitana de Caracas (Villegas, 2008), entre los hallazgos se puede mencionar: la falta de especialistas en seguridad de la información y de instancias formales para atender situaciones de ataques a los activos informáticos, políticas de seguridad poco difundidas, carencia de normas, procedimientos y auditorías, no se aplican de manera sistemática las metodologías formales y el análisis de gestión de riesgo, no se elaboran planes estratégicos bajo la perspectiva de la seguridad informática, no se le da suficiente importancia y se invierten pocos recursos para mejorarla.

Ante estos resultados se pretende contribuir a mejorar la seguridad informática en instituciones de educación superior, aportando algunas métricas e indicadores que faciliten el cumplimiento de objetivos y metas en el área de gestión de la seguridad informática, a través de la implantación de controles de seguridad, eficacia y eficiencia de los mismos. Asimismo se plantean algunas consideraciones sobre el impacto que pueda generar la implantación de estos controles en las universidades del país.

ANTECEDENTES

Existen investigaciones que establecen las reglas, normas, controles y procedimientos que regulan la forma en que las instituciones tratan de asegurar la prevención, la protección y el manejo de los riesgos de seguridad en diversas circunstancias. Tal es el caso del Manual de Normas y Políticas de Seguridad Informática que elaboró la Universidad de Oriente de El Salvador (UNIVO, 2006).

En este manual se considera que las métricas de seguridad son la medida de la efectividad de los esfuerzos de seguridad en el tiempo de la organización. Así como considera que lo ideal es desarrollarlas de manera sencilla y que provean información útil para la gestión. En este sentido, la clave para las métricas es obtener medidas que tengan las siguientes características:

- Medir cosas significativas para la organización
- Ser reproducible

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 10 Edición No 1 – Año 2011

- Ser objetivas y sin sesgo
- Capaces en el tiempo de medir algún tipo de progreso hacia una meta.

Este documento señala que las métricas tradicionales presentan problemas en su diseño, aunque se logra el mejor valor posible de la métrica, no se garantiza la seguridad. Por lo tanto, el objetivo de desarrollar métricas o mediciones es poder conocer lo que se busca medir.

De esta manera, se obtiene un conocimiento científico (demostrable) del objeto en cuestión y se le puede controlar. Es en este sentido que las métricas son aplicables y no son importantes en sí mismas, sino en la información que nos transmiten. En el caso de la Seguridad informática, si se eligen métricas inadecuadas (difíciles de implementar o que brindan información incompleta) pueden ocurrir efectos desastrosos.

El establecimiento de métricas es un tema controvertido, algunos autores como Chapin & Akridg (2005) afirman que las métricas de seguridad tradicionales son, en el mejor de los casos, fortuitas y dan una falsa sensación de seguridad, que lleva a una implantación ineficiente o insegura de medidas de seguridad. De igual manera, Gómez & Quintero (2008) consideran que el concepto de seguridad en la informática es utópico, porque no existe un sistema 100% seguro, y establecen que para que un sistema informático se pueda definir como seguro, debe tener estas cuatro características:

- **Integridad:** la información sólo puede ser modificada por quien esté autorizado.
- **Confidencialidad:** la información sólo debe estar legible para los autorizados.
- **Disponibilidad:** debe estar disponible cuando se necesite.
- **Irrefutabilidad:** que no se pueda negar su autoría.

LA PROBLEMÁTICA

En los actuales momentos, la seguridad informática es un tema de dominio obligado para cualquier usuario de internet que no esté dispuesto a que su información sea vulnerada. Aunque a simple vista se puede entender que “riesgo” y “vulnerabilidad” se pueden englobar en un mismo concepto, una definición más precisa es que “vulnerabilidad” está ligada a una amenaza y “riesgo” se refiere a un impacto.

Las organizaciones son entidades sociales compuestas por dos o más individuos con la finalidad de cumplir metas y objetivos (Vásquez, 2003). Uno de sus objetivos es el de preservar y conservar la información que constituye un activo esencial que les proporciona posicionamiento y competitividad.

Asimismo, las universidades son también sistemas psicosociales complejos que funcionan como organizaciones que tienen como finalidad: crear, asimilar y difundir el saber mediante la investigación y enseñanza a los estudiantes para completar la formación integral iniciada en los ciclos educacionales anteriores, formar los equipos

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 10 Edición No 1 – Año 2011

profesionales y técnicos que necesita la Nación para su desarrollo y progreso (Congreso de la República de Venezuela, 1970).

En lo que se refiere a las universidades venezolanas, se consideran como sistemas abiertos y no son una excepción. Éstas requieren, necesariamente, un proceso de adaptación que les permita evolucionar y realizar los cambios indispensables que van a permitir desenvolverse de manera eficiente ante las exigencias de la sociedad actual, llamada sociedad informática para unos y sociedad del conocimiento para otros. (Vásquez, 2003).

Por lo tanto, las universidades venezolanas necesitan adquirir, desarrollar y mantener Sistemas de Información (SI), aplicaciones, Bases de Datos (BD) y Tecnologías de información y Comunicación (TIC), además de implementar medidas de salvaguarda que protejan los activos existentes de las posibles amenazas internas o externas.

Estas acciones contribuyen a reducir el riesgo de ataques sobre los bienes informáticos y a minimizar el impacto económico que ocasionaría la costosa inversión que haría la institución, para recuperar sus sistemas informáticos en caso de resultar dañados o destruidos por no estar protegidos adecuadamente.

En el caso de las universidades venezolanas, han ocurrido diversos ataques hacia los activos informáticos, como son: el robo de computadoras personales (PC) y portátiles (laptop), de video beams, de periféricos y componentes internos de estos equipos; así como el acceso no autorizado a información confidencial, la eliminación de sitios web y de aplicaciones.

También se encuentra la denegación de servicio de correo electrónico y de sitios web de departamentos críticos, la alteración de información sensible almacenada en servidores de los departamentos académicos por agentes externos a ellos (hackers, crackers y otros). Cualquiera de estos ataques a los servicios críticos puede afectar severamente el logro de los objetivos institucionales.

En la actualidad se viene reportando una serie de ataques informáticos a diferentes organizaciones, entre ellas las universitarias. Existen referencias de ataques a los activos informáticos en algunas universidades españolas, los cuales señalan que durante el año 1998 el número de incidentes denunciados a los organismos españoles encargados de la seguridad en internet, IRIS-CERT y CERT-UPC, subió y, como dato interesante, reportan un aumento de ataques en las universidades y un descenso en las empresas.

Las universidades y centros de investigación son, desde siempre, el punto débil de la seguridad en internet porque aquí se flexibilizan las medidas de seguridad ya que existen muchos estudiantes que tienen cuentas de correo y disponen del servicio de internet.

Por ejemplo: .as estadísticas del IRIS-CERT, mencionadas por Molist (1999) muestran que los ataques e intentos (escaneos de puertos, telnet, etc) a instituciones universitarias españolas habían subido en un 250%, entre 1997 y 1998, ataques informáticos realizados desde ordenadores ubicados fuera de España en más de un 50%.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 10 Edición No 1 – Año 2011

En el caso venezolano los ataques informáticos a instituciones son silenciados por razones estratégicas, ya que pondrían en evidencia sus vulnerabilidades y en consecuencia perderían la confianza de los usuarios.

Esto es particularmente cierto en las universidades donde se presume que los registros de datos de los estudiantes están seguros y son confiables para consultas futuras. De hecho, Villegas (2008) encontró muchas dificultades para obtener información sensible y tuvo que acudir a mediciones indirectas para identificar vulnerabilidades en las instituciones investigadas.

Esta carencia de seguridad institucional es lo que ha inducido a plantear una investigación que permita proponer indicadores y métricas que contribuyan a mejorar la gestión de la seguridad informática, a través de la implantación de controles de seguridad y de la eficacia y eficiencia de los mismos, así como el impacto que va generar la implantación de éstos en las universidades venezolanas.

DESARROLLO

La seguridad informática de las tecnologías y de los sistemas de información se ha convertido en un factor clave para el éxito y la rentabilidad de las organizaciones. Passarello (2006) sostiene que es necesario contar con profesionales que posean competencias y conocimientos que permitan desarrollar políticas de seguridad las cuales garanticen la aplicación de salvaguarda contra las pérdidas económicas graves; el deterioro de la imagen pública de la organización; el incumplimiento legal o la fuga de información.

En este mismo orden de ideas, las organizaciones, al igual que las universidades, requieren personas competentes y con conocimientos para reconfigurar la manera de trabajar, lo cual exige reflexionar sobre la situación actual, saber hacia dónde se quiere llegar, proveer los recursos necesarios para alcanzarlos y dar la oportunidad de cambiar.

Asimismo, el objetivo de la construcción de estas métricas es comprender el estado actual en que se encuentra la seguridad informática en las universidades venezolanas de la Región Capital, y contribuir a la formulación de las estrategias que las ayuden a mejorar la seguridad con la adopción de las mejores prácticas.

Por consiguiente, las métricas se convertirán en una guía para saber cómo llegar a los objetivos y metas que se desean alcanzar en cuanto a la seguridad informática en las universidades, por lo que su aplicación y seguimiento permitirán minimizar los niveles de inseguridad.

La construcción de las métricas de seguridad de esta investigación son preceptos y reglas necesarios para poder medir de forma real el nivel de seguridad de una universidad (Corletti & De Alba, 2008.)

Por lo anterior, las métricas ayudan a mejorar los niveles de seguridad y también proporcionan algunos otros beneficios dentro de las organizaciones, como lo afirma Cano (2007), algunas de estos son:

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 10 Edición No 1 – Año 2011

(a) Comprender mejor sus riesgos, (b) Identificar problemas emergentes, (c) Comprender las debilidades de la infraestructura tecnológica, (d) Medir el desempeño de los controles implantados, (e) Actualizar las tecnologías y mejorar los procesos actuales, (f) Evidenciar la evolución de la cultura de seguridad de la información.═En esta investigación se usan los criterios de Schneier (2002), quien plantea la necesidad de responder las siguientes interrogantes:

(a) ¿Dónde queremos estar?

Esta interrogante se refiere a la Misión y Objetivos de Negocio de las instituciones. En relación a esta investigación se ha considerado que las universidades venezolanas tienen como misión y visión el mejorar la gestión de la Seguridad informática, a través de la implementación de distintas políticas y normas.

(b) ¿Dónde estamos hoy?

Se evaluó la situación actual de la seguridad informática a partir de los resultados de la aplicación de un cuestionario y de entrevistas realizadas a los distintos encargados de la Seguridad informática en universidades de la Región Capital, y otros especialistas del área.

La información fue recopilada en una investigación previa realizada por Villegas (2008) la cual permitió determinar que, en la mayoría de estas instituciones venezolanas, se aplican políticas netamente correctivas y no preventivas.

De igual forma, los entrevistados coinciden en considerar que el personal técnico es el único responsable del problema de inseguridad y el factor humano no es considerado como elemento crucial para tomar conciencia del problema y mejorarlo y aunado a lo anterior, señalan que existe poca inversión en el resguardo de los activos informáticos de las instituciones universitarios.

(c) ¿Cómo podemos llegar?

Los resultados de la investigación realizada en 2008 permiten establecer algunas estrategias para lograr cambios relativos a la seguridad informática en las instituciones universitarias, entre los cuales podemos mencionar los siguientes:

- Cada universidad debe realizar un estudio a profundidad de cómo se encuentra la seguridad informática que posee.

- Se requiere, de acuerdo a los resultados de cada estudio particular, que se analice la creación y operatividad de una Unidad Organizacional o Departamento de Seguridad informática para así tener una estructura responsable que enfrente el problema.

- Es necesario que se invierta en mejorar la infraestructura técnica y se ofrezca capacitación al personal encargado del área.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 10 Edición No 1 – Año 2011

- Es imprescindible desarrollar manuales que contengan normas, políticas, funciones del personal responsable de la Seguridad Informática de cada institución, entre otros.

(d) ¿Cómo saber que llegamos?

Para medir avances en el logro de los objetivos de cada institución se necesita utilizar métricas ya que, según Chew et al (2003), las métricas son herramientas para facilitar la toma de decisiones, mejorar el desempeño y la responsabilidad:

Las métricas son herramientas diseñadas para facilitar la toma de decisiones y mejorar el desempeño y eficiencia a través de la recolección, análisis, y el reporte de datos relevantes relativos al desempeño (…) las métricas de seguridad se pueden obtener a diferentes niveles en la organización. Las métricas detalladas, recopiladas a nivel de sistema, pueden ser agregadas y elevadas progresivamente a niveles más altos, dependiendo del tamaño y complejidad de una organización (p. 9)[1]

En este mismo orden de ideas, Chalico & Saucedo (2008), señalan que "en seguridad informática es más común el término "métrica" la cual se define como una medida o conjunto de medidas que permiten caracterizar, conocer, estimar o evaluar un atributo especificado; para realizar y conocer su desempeño y estado actual" (p.4).

Asimismo, Cano (2007) afirma que una buena métrica de seguridad es aquella que provee mediciones o valores concretos, como respuestas a preguntas concretas. Las características más sobresalientes son: (a) No deben tener criterios subjetivos, (b) Deben ser fáciles de recolectar, (c) Detalladas con respecto a sus unidades de medida, (d) Relevante para la toma de decisiones (p.23).

Por otra parte, Cano (2007) también expresa que los errores más frecuentes al definir las métricas y que debemos evitar al construir las mismas son: (a) Querer ajustarse a los dominios o variables definidas en los estándares de la industria, (b) Ignorar la dinámica propia de la seguridad en la organización.

(c) No comprender los riesgos de la organización y la percepción de los mismos, (d) Querer abarcar toda la gestión de seguridad en el primer ejercicio, (e) Ignorar las expectativas de alta gerencia sobre el tema, (f) Desconocer las características de la cultura organizacional, (g) Ignorar que es un ejercicio de evaluación y diagnóstico (p.26).

Tomando en cuenta lo anteriormente planteado, las métricas son un conjunto de instrumentos que nos guían hacia la obtención de los objetivos y metas que se han planificado lograr con respecto a la seguridad informática de las instituciones universitarias, es por ello, que es fundamental explicar cómo se construyen ya que éstas nos ayudaran a medir la eficiencia y eficacia de la seguridad informática, así como aminorar los riesgos que pueden existir.

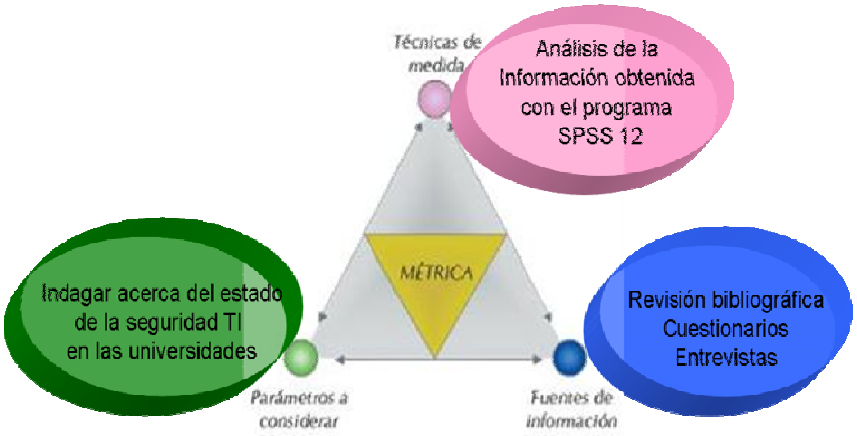
[1] Traducción de las autoras

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 10 Edición No 1 – Año 2011

PROCESO DE CONSTRUCCIÓN DE LAS MÉTRICAS

En esta investigación se utiliza el modelo contextualizado de Colado & Franco (2003), citado por Anabalón (2008) (Ver Figura 1), el cual considera los aspectos de triangulación donde cada uno de sus vértices expresa tres condiciones que deben tomarse en cuenta al construirlas, éstas son: ¿Para qué?, ¿Qué? y ¿Cómo?

Figura 1: Contextualización de los elementos propuestos



Fuente: Anabalón (2008)[2].

A este modelo se le incorpora y define la funcionalidad de las condiciones en relación a lo investigado, es decir, se adapta al contexto de acción de la seguridad informática en las universidades de la región capital. A continuación se explican cada una de estas condiciones:

¿Para qué? se refiere a la indagación del estado de la seguridad informática en las universidades.

¿Qué? se refiere a las fuentes de información utilizadas y se destacan la revisión bibliográfica, el cuestionario y las entrevistas.

¿Cómo? tiene que ver con el análisis de los datos obtenidos de las fuentes de información

Aunado a lo anterior se realizó un sondeo que permitió identificar los parámetros más relevantes para determinar el estado de la seguridad informática de las universidades en la región capital. En este contexto se establecen los principales indicadores de seguridad informática, a saber:

- Funcionamiento de un departamento o unidad especializada en el área.

[2] Adaptado por las autoras

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 10 Edición No 1 – Año 2011

- Disponibilidad de, al menos, un conjunto de herramientas básicas de hardware y software que garanticen un mínimo de seguridad informática.

- Actualización sistemática del software de seguridad.

- Medidas de seguridad: encriptación informática, acceso controlado, respaldo informático (backups) en diversas ubicaciones, software para la recuperación de datos y cuarentena automática para archivos infectados.

- Detección de procedimientos informales, no sujetos a los estándares de la institución.

- Instalación anárquica de herramientas de hardware y software.

- Planificación estratégica enfocada a la seguridad informática, entre otros.

Una vez detectados estos indicadores se procedió a la búsqueda de las posibles fuentes de información, entre las cuales se tiene: revisión bibliográfica, cuestionarios y protocolos de entrevistas.

La información obtenida fue agrupada en niveles de análisis, cada uno de ellos por indicadores y métricas. Los indicadores y métricas fueron organizados en cuatro niveles de análisis:

a) **Estado Inicial de Seguridad Informática**: etapa inicial en la que se hace el diagnóstico del estado de seguridad de las universidades estudiadas.

b) **Detección de Necesidades**: etapa en la que se describen e identifican los elementos necesarios para mejorar la seguridad informática.

c) **Planificación Estratégica**: trabajo en equipo para afinar el diagnóstico, establecer un plan estratégico para crear políticas de seguridad informática.

d) **Inteligencia Organizacional**: etapa en la que aplica el plan estratégico y se hacen correcciones sobre la marcha para optimizar la seguridad informática.

La metodología utilizada para desarrollar los indicadores y las métricas descritas en las tablas 1,2, 3 y 4 forman parte de un modelo para determinar niveles de madurez en la gestión y administración de la seguridad informática en instituciones que manejan información sensible (Villegas, 2008).

Este modelo ha resultado particularmente útil para medir el desempeño institucional frente a los retos que plantea la preservación y resguardo informática, por lo tanto permite identificar el origen de los desempeños no satisfactorios y las áreas que requieren ser mejoradas.

Adicionalmente, facilita mantener la consistencia de las políticas de seguridad informática, realizar cambios en las mismas, redefinir metas y objetivos y apoyar la evolución de estas

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 10 Edición No 1 – Año 2011

políticas para permitir los cambios tecnológicos y enfrentar amenazas y vulnerabilidades que pudieran surgir en el futuro. A continuación, se presentan las tablas 1, 2, 3 y 4 en las cuales se especifican los niveles mencionados anteriormente:

TABLA N° 1: Estado Inicial de Seguridad Informática

Nivel	Definición	Indicadores	Métricas
Estado inicial de Seguridad Informática	Diagnóstico de las condiciones iniciales de la seguridad informática en las instituciones investigadas	Responsables o Unidad Organizacional de la Seguridad informática	Existencia de un Responsable o Departamento de Seguridad informática
			Responsables de la Seguridad informática: técnicos, afines y otros
		Medidas básicas de Seguridad	Calificación profesional de los responsables de la seguridad informática
			Experticia de los responsables en el área de Seguridad informática
			Procedimientos informales y/o instalación anárquica de herramientas de Hardware o Software
			Encargados de la seguridad física de Hardware y Software existentes
			Actualización permanente del Software de seguridad instalado en los equipos de la institución
		Herramientas de Hardware y Software	Instalación de Hardware en los equipos.
			Instalación de software: Programas antivirus, antispyware, firewall y otros programas contra espías.
		Respaldo y recuperación de datos (Backups)	Frecuencia (diaria/semanal/mensual) de la data e información de la universidad
			Digitalización de documentos
			Ubicación física de los respaldos: dentro de la universidad, fuera en el país o fuera del país.

Fuente: elaboración propia.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 10 Edición No 1 – Año 2011

TABLA N° 2: Detección de Necesidades

Nivel	Definición	Indicadores	Métricas
Detección de necesidades	Se describen e identifican los elementos que permitirían mejorar la seguridad informática	Existencia de documentos de Seguridad informática	Documento donde se especifiquen los procedimientos, funciones, medidas, normas, políticas y obligaciones de los usuarios
		Funciones y obligaciones del personal	Documento que explique cómo llevar procesos, hardware y software de la universidad, así como las responsabilidades del personal y de los usuarios
		Difusión de políticas de seguridad	Información sobre: Confidencialidad , Integridad, Disponibilidad, Autenticación, Autorización, Firmas Electrónicas, Certificados Digitales, etc.
		Registro de eventos que afectan la seguridad informática	Bitácora con registro de usuarios que acceden a los datos u otra información, accidentes de seguridad y otros eventos relevantes para mejorar la seguridad.
		Medidas de Seguridad Intermedia.	Uso de la Bitácora para planificar mantenimiento preventivo y correctivo.
		Valores y conductas éticas	Definición y difusión de valores éticos asociados a la seguridad informática
			Conductas éticas asociadas al manejo informática.
			Charlas, cursos, seminario y reuniones para crear una cultura de Seguridad informática

Fuente: elaboración propia.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 10 Edición No 1 – Año 2011

TABLA N° 3: Planificación Estratégica

Nivel	Definición	Indicadores	Métricas
Planificación estratégica	Trabajo en equipo para afinar el diagnóstico, se establece un plan estratégico dirigido a crear políticas de seguridad informática para las universidades	Trabajo el equipo	Promover aprendizaje y el trabajo en equipo.
		Visión compartida	Establecer acuerdo entre los miembros de la Unidad encargada de la seguridad informática
		Auditorías	Realizar Auditorias, tanto externas como internas
		Plan estratégico	Desarrollar un Plan Estratégico donde su visión, misión y políticas incluyan la seguridad informática
		Medidas de Seguridad Avanzadas	Incluir a profesores, personal administrativo y estudiantes como agentes importantes para garantizar las políticas de seguridad informática
			Promover el desarrollo de capacidades y destrezas relativas a la seguridad informática
			Controlar el acceso al software de quienes usan datos y recursos en el desarrollo de sus funciones.
			Llevar control de acceso físico para algunos sitios de la universidad según el cargo que se desempeñe
			Asegurar que operadores y usuarios no puedan modificar programas ni archivos
		Adopción y cumplimiento de las Políticas de Seguridad informática	Adoptar y cumplir las políticas relativas a confidencialidad, integridad, disponibilidad, autenticación, autorización firmas electrónicas , certificados digitales y cualquier otra medida de seguridad que se considere necesaria
		Observación de valores y conductas éticas	Identificar en el personal y los usuarios las conductas relacionadas con los valores y la ética de la Seguridad informática.

Fuente: elaboración propia.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 10 Edición No 1 – Año 2011

TABLA N° 4: Inteligencia Organizacional

Nivel	Definición	Indicadores	Métricas
Inteligencia Organizacional	Se ejecuta el plan estratégico tratando de lograr el estado máximo de seguridad posible que garantice el resguardo de datos e información sensible	Responsables de que se cumplan las políticas y medidas de Seguridad informática	Informar periódicamente a la comunidad universitaria sobre las políticas de seguridad
			Designar un responsable o departamento que haga cumplir las políticas de Seguridad informática
			Instaurar políticas propias para la Seguridad informática
			Aplicar en la Comunidad Universitaria las políticas de Seguridad informática
			Hacer notar a todos que la Seguridad informática es un problema que compete a todos los miembros de la Comunidad universitaria
			Hacer cumplir las políticas cada usuario
		Cultura organizacional	Instaurar una cultura organizacional de la Seguridad informática
			Exigir valores éticos como parte d e la cultura organizacional de la universidad
		Cumplimiento de la misión y visión compartida	Mantener la misión y la visión compartida con respecto a la Seguridad informática
			Incentivar a los grupos de trabajo para que actúen de acuerdo a la misión y visión compartida enfocada a la Seguridad informática
Inteligencia Organizacional	Se ejecuta el plan estratégico tratando de lograr el estado máximo de seguridad posible que garantice el resguardo de datos e información sensible	Desarrollo de actitudes y aptitudes en las personas que forman los grupos de trabajo	Consolidar los Grupos de Seguridad como equipos de trabajo
			Incrementar la experticia técnica de los grupos de trabajo en la Seguridad informática
			Promover una actitud proactiva en los miembros de los grupos de trabajo.
			Fomentar la comunicación entre los equipos de desarrollo de sistemas informáticos y los encargados de la Seguridad informática
		Análisis y Gestión de Riesgo de los Sistemas Informáticos	Aplicar con frecuencia metodologías de análisis y gestión de riesgo
			Realizar análisis y gestión de riesgo a los nuevos activos incorporados a la organización
		Monitoreo de la red estadísticas y descripción de ataques	Monitorear permanentemente la red
			Controlar los registros de ataques ocurridos
			Llevar estadísticas y gráficos para planificar medidas preventivas y correctivas
			Modificar permanentemente las contraseñas de acceso al sistema.
		Ejecución del Plan Estratégico	Desarrollar en conjunto la planificación estratégica, los sistemas y la adopción de las TIC con la programación de la Seguridad informática
			Ejecutar el plan estratégico, evaluarlo permanentemente, hacer correcciones sobre la marcha y repetir el ciclo.

Fuente: elaboración propia.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 10 Edición No 1 – Año 2011

CONCLUSIONES

Para toda institución pública o privada que maneje información sensible se considera que la adopción de políticas de Seguridad informática es vital. El modelo de madurez para la gestión y administración de la seguridad informática aquí utilizado (Villegas, 2008) permitió construir un conjunto de indicadores y métricas específicas para el grupo de universidades analizadas para dar respuesta a cuan efectivo es el Sistema General de Seguridad informática de instituciones universitarias y otras similares como los centros de investigación científica.

Asimismo, se pudo comprobar, tal y como lo plantea Corletti & De Alba (Ob.cit.), que en todas las organizaciones así como en las universidades se deben medir los niveles de seguridad informática (todo aquello que no se puede medir, no se puede mejorar). Las métricas irán madurando y cambiando en función del nivel de madurez que vaya adquiriendo la universidad. Igualmente, las métricas permiten a los responsables de seguridad demostrar la eficiencia del cumplimiento de las mismas y el valor que aportan a la institución universitaria.

Si bien los resultados aquí obtenidos no son generalizables a todas las universidades del país, sí pueden constituir un punto de partida para aquellas instituciones, universitarias o no, que deseen iniciar un trabajo más sistemático sobre la Seguridad de sus Sistemas de Información. Adicionalmente, estos resultados permiten guiar la toma de decisiones en cuanto a la orientación de nuevas inversiones, reubicación de personal para obtener un óptimo desempeño y, en general, mejorar el clima organizacional.

Se espera que esta contribución pueda ser usada como herramienta para identificar áreas que requieren ser mejoradas, facilitar la consistencia de la implementación de políticas relacionadas con la plataforma informática, realizar cambios en las mismas, redefinir metas y objetivos y apuntalar la evolución hacia la madurez de las instituciones universitarias en cuanto a su Seguridad informática.

REFERENCIAS BIBLIOGRÁFICAS

Anabalón, J. (2008). Desarrollo de métricas de seguridad SOX. ISSA. Documento en línea. Disponible en: http://anabalon.clan.su/papers/metricas_de_seguridad.pdf Consulta: 15/12/2009.

Cano, J. (2007). Métricas en seguridad informática: una revisión académica. VII Jornada de Seguridad Informática ACIS. Documento en línea. Disponible en: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/07-MetricasSeguridadInformaticaUnaRevisionAcademica.pdf. Consulta: 27/02/2011.

Chalico, C. y Saucedo, E. (2008). Indicadores de gestión aplicados a los procesos de administración de riesgos y seguridad. Documento en línea. Disponible en: http://ebookbrowse.com/6-chalico-saucedo-ppt-d59398282. Consulta: 13/02/2009.

Chapin, D. y Akridg, S. (2005). ¿Cómo Puede Medirse la Seguridad? Information Systems Control Journal. Volumen 2. Documento en línea. Disponible en:

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 10 Edición No 1 – Año 2011

http://www.iso27000.es/download/HowCanSecurityBeMeasured-SP.pdf. Consulta: 15/10/2007.

Chew, E.; Swanson, M.; Stine, K.; Bartol, N.; Brown, A. & Robinson, W. (2008). Performance Measurement Guide for Information Security. Computer Security. NIST National Institute of Standars and Technology. Technology Administration U.S Department of Commerce. Documento en línea. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf Consulta: 09/01/2009.

Corletti, A. y De Alba, C. (2008). Métricas de Seguridad, Indicadores y Cuadro de Mando. Normas y Estándares. Las métricas permiten a los responsables de seguridad demostrar la eficiencia del programa de seguridad y el valor que aporta a la compañía. Documento en línea. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m292p.htm. Consulta: 22/02/2009.

Congreso de la República de Venezuela (1970). Ley de Universidades. Gaceta Oficial No. 1429, Extraordinario, del 8 de septiembre de 1970. Venezuela.

Gómez, D. y Quintero, M. (2008). Seguridad Informática**.** Servicio Nacional de Aprendizaje (SENA). Técnico Profesional en Administración del Talento Humano Recurso Humano. Documento en línea. Disponible en: http://www.scribd.com/doc/6317119/Seguridad-a-Doc-Word1. Consulta: 26/02/2009.

Molist, M. (1999). Aumentan los Ataques a Universidades y bajan en las Empresas, según las Estadísticas del CERT. Documento en línea. Disponible en: http://ww2.grn.es/merce/1999/estadistiques.html. Consulta: 15/03/2008.

Passarello, E. (2006). Convergencia de prácticas. Reflexiones y Tendencias. Consejo Profesional de Ingeniería en Electrónica, Telecomunicaciones y Computación (COPITEC). Documento en línea. Disponible en: http://www.scribd.com/doc/3796594/PASSARELLO-ESPEITO-Convergencia-de-Practicas. Consulta: 30/03/2009.

Schneier, B. (2002). Secrets and Lies. Digital Security in a Networked World. EE.UU. John Wiley & Sons.

Universidad de Oriente (UNIVO) (2006). Manual de Normas y Políticas de Seguridad Informática. Documento en línea. Disponible en: http://www.scribd.com/doc/2023909/manual-de-politicas-y-normas-de-seguridad-informatica#document_metadata. Consulta: 30/03/2009.

Vásquez, J. (2003). ¿Qué son las Organizaciones? Teoría y pensamiento administrativo. Documento en línea. Disponible en: http://www.gestiopolis.com/canales/gerencial/articulos/56/orgsqueson.htm. Consulta: 30/04/2008.

Villegas, M. (2008). Modelo de Madurez para la Gestión y Administración de la Seguridad Informática en las Universidades. Tesis de Maestría no publicada. Universidad Simón Bolívar, Venezuela.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 10 Edición No 1 – Año 2011