Defensa

Administrando la Inseguridad Informática

Jeimy J. Cano 

Grado de dificultad

Este documento busca repensar la seguridad de la información desde el concepto de la inseguridad, para que, tratando de aprender de la mente del atacante, se descubra cómo diseñar y construir sistemas menos inseguros, como una estrategia para destruir la falsa sensación de seguridad y animar una postura vigilante y proactiva en la gestión de la seguridad de la información.

La única constante en el mundo de la seguridad de la información, es la inseguridad. En este sentido, las organizaciones luchan día a día para tratar de eliminar o mitigar las posibles vulnerabilidades que se presentan en sus infraestructuras tecnológicas o en sus procedimientos que apoyan el negocio.

Revisando los recientes artículos e informes de vulnerabilidades (WILLIAMS, M. 2006, MIMOSO, M. y SAVAGE, M. 2006, BEAVER, K. 2006, ROITER, N. 2006), se hace evidente que la inseguridad informática es un elemento propio de la dinámica de las organizaciones en cada uno de sus procesos. Mientras las empresas buscan alcanzar un nivel superior de seguridad, más se encuentran con la problemática de la inseguridad, pues los procesos en sí mismos, al ser redes de comunicaciones y acuerdos entre personas, tecnologías y normas, establecen relaciones y distinciones que generalmente no son distinguibles, haciendo de la labor de aseguramiento de la información más que una función tecnológica, acciones humanas y procesos administrativos y estratégicos.

Durante el 2006, los robos de información y la exposición de datos (*http://attrition.org/dataloss/*), fueron las manifestaciones más sobresalientes de la inseguridad. Si miramos con detalle estas dos consideraciones, no responden necesariamente a un problema de seguridad tecnológico, sino procedimental y de concientización. Los intrusos saben y comprenden que detrás de las infraestructuras de seguridad de la información está ese elemento que las organizaciones hoy por hoy se resisten a entrenar, a formar, a hacer parte formal de su modelo de seguridad, los usuarios. (BEAVER, K. 2006). Esta realidad, se manifiesta en importantes incrementos de robo de identidad y fraudes bancarios a través de Internet que requieren una revisión profunda de nuestra com-

En este artículo aprenderás...

- Cómo diseñar y construir sistemas menos inseguros,
- Cómo animar un apostura vigilante y proactiva en la gestión de la seguridad informática.

Lo que deberías saber...

- Concepto de la inversión y las vulnerabilidades en la seguridad informática.

prensión de la seguridad, más allá de las fallas y las vulnerabilidades.

En este sentido, repensar el discurso de administración de la seguridad exige de los profesionales y directivos de seguridad aprender a comprender el dual que combaten: la inseguridad informática. Comprender *el lado oscuro* implica reconocer que tenemos que desaprender, que nuestras actuales estrategias se limitan a mantener y utilizar más tecnologías, y no a comprender en profundidad las relaciones complejas que exhibe la organización y cómo allí se hace presente o se materializa la inseguridad. (THE HONEYNET PROJECT 2004, TAYLOR, R., CAETI, T., KALL LOPER, D., FRITSCH, E. y LIEDERBACH, J. 2006).

En consecuencia, las organizaciones deben reconocer que parte del secreto para incrementar los niveles de seguridad, está en la administración de la inseguridad informática. Expresado de otra forma, que tan seguros pueden llegar a ser, reconociendo siempre que la inseguridad de la información estará presente para desafiarlas una y otra vez.

Las implicaciones de esta propuesta exigen desarrollar un hábito que busque confrontar la inseguridad de la información y no solamente su control o mitigación. En razón a lo anterior, desarrollar un hábito requiere según Covey (2005 pág. 51) tres elementos: el conocimiento, la habilidad y la actitud.

- El conocimiento, como la capacidad de comprender en detalle los aspectos conceptuales relacionados con el área de trabajo donde se ejerce.
- La habilidad como la capacidad de hacer, desarrollar y actuar en consecuencia con ese conocimiento.
- La actitud, como la disposición del individuo frente a los retos que propone el área de conocimiento y su manera de enfrentar y motivar el desarrollo de habilidades complementarias para ir más allá de lo que su entorno le propone.

En ese contexto, desarrollar el hábito de la *Administración de la Inseguridad Informática* – ADINSI – implica hacer de ésta una pasión, una disciplina individual que permita a las organizaciones mantener una posición proactiva frente a posibles e inesperados eventos, para los cuales puede no estar preparadas, pero conscientes sobre cómo aprender de ellos.

Basado en lo anterior, se presenta este documento que examina los conceptos actuales de la seguridad de la información, algunas consideraciones de inversión en temas de seguridad, los cuales serán insumo para proponer un modelo base para la administración de la inseguridad y así ver, bajo la mirada de los intrusos, tendencias emergentes y estrategias consecuentes con este modelo.

Concepto tradicional de la seguridad de la información

La seguridad de la información desde los años 60 se ha desarrollado como una distinción formal, basada generalmente en teorías matemáticas, las cuales terminaron materializadas en implementaciones de software, hardware y productos intermedios. Como bien comentaba una persona de la industria, *en teoría la seguridad es perfecta, en la práctica no*, esta expresión nos sugiere que si bien, las especificaciones matemáticas utilizadas para darle claridad a las relaciones que se establecen entre usuarios y objetos son verificables en un escenario ideal, la realidad de las organizaciones y el desarrollo de software desbordan dichas expectativas.

Tabla 1. *Características de la Seguridad y de la Inseguridad (Tomado de: CANO, J. 2006)*

Seguridad	Inseguridad
Subjetiva	Objetiva
No tiene cota superior	Es posible establecerle cota superior
Intangible	Tangible
Es una propiedad emergente	Es una propiedad inherente
Se require modelarla	No se require modelarla

La seguridad ha estado basada todo el tiempo en la comprensión de tres elementos fundamentales y cómo alcanzarlos en cada una de las implementaciones de modelos de seguridad: confidencialidad, integridad y disponibilidad – CID. Consecuente con lo anterior, cualquier intento para vulnerar alguno de éstos elementos, se considerará un intento o ataque al activo fundamental que es la información.

Siguiendo la revisión anterior, se tiene que los ataques se presentan dado que existen escenarios y prácticas que no aseguran el cumplimiento del CID para la información a proteger, característica que en el mundo de la auditoría se denomina riesgo. Un riesgo, de manera general, es todo aquello que no me permite el logro de los objetivos; en particular, en temas de seguridad de la información, todo aquello que no me permite cumplir con CID.

Generalmente al adelantar un proceso de administración de la seguridad de la información, se establece lo que se denomina un conjunto de procesos a revisar y la información asociada con el mismo. Este proceso se basa por lo general en un programa de protección de activos de la organización (KOVACICH, G. y HALIBOZEK, E. 2006) que considera las políticas, los procedimientos, los procesos, los proyectos, los planes y las responsabilidades de cada uno de los actores de la organización frente a los activos. A través de este programa se operacionalizan las medidas requeridas para mitigar los riesgos a los cuales esta expuesta la información.

La valoración de qué tan efectivo ha sido el proceso de administración de la seguridad generalmente se

mide según el número de incidentes que se han presentado en la dinámica de la organización y su negocio. Para ello, ejercicios como las pruebas de vulnerabilidades, las evaluaciones de seguridad y las auditorías de seguridad (CANO 1997) son referentes útiles para establecer el grado en que las vulnerabilidades se hacen presentes tanto en la infraestructura como en los procesos de negocio.

Si revisamos las prácticas actuales de las organizaciones alrededor de una administración de la seguridad de la información, identificamos una fuerte tendencia al uso de tecnologías y utilización de estándares o buenas prácticas internacionales (KUPER, P. 2005), como una estrategia para avanzar en su lucha contra la inseguridad, pero pocos elementos que procuren entender esta última.

En consecuencia con lo anterior, el concepto de seguridad, como el proceso formal y riguroso para mantener un sistema de gestión orientado a la protección de la información, sustentado en las estrategias y dinámica de negocio, entra en crisis al saber que la inseguridad presente dentro del sistema atenta contra su propio objetivo. La pregunta que surge es: ¿qué hacer frente a la inseguridad o riesgos inherentes a la realidad de las organizaciones? La respuesta a este interrogante será desarrollada posteriormente.

Algunas consideraciones sobre la inversión y las vulnerabilidades en seguridad informática

Las organizaciones que reconocen en la información un activo fundamental para desarrollar negocios y sobrevivir en un mundo global, por lo general establecen presupuestos que consideran inversiones (generalmente de un dígito) en los temas de aseguramiento o protección de dicho activo. Dichas inversiones fueron revisadas por un estudio realizado por la firma Stanley Morgan durante el 2005 (KUPER, P. 2005), cuyos resultados se detallan a continuación.

La firma Stanley Morgan encontró que las mayores inversiones en seguridad se efectúan en temas de seguridad perimetral, es decir, cajas de protección de seguridad anti-spam, anti-virus, anti-spyware, las cuales generalmente viene preconfiguradas e instaladas, haciendo mucho más fácil su uso y puesta en producción. Dichas cajas generalmente poseen una interfase de administración que permite a los responsables de seguridad mirar la efectividad del control de las amenazas para las cuales han sido adquiridas.

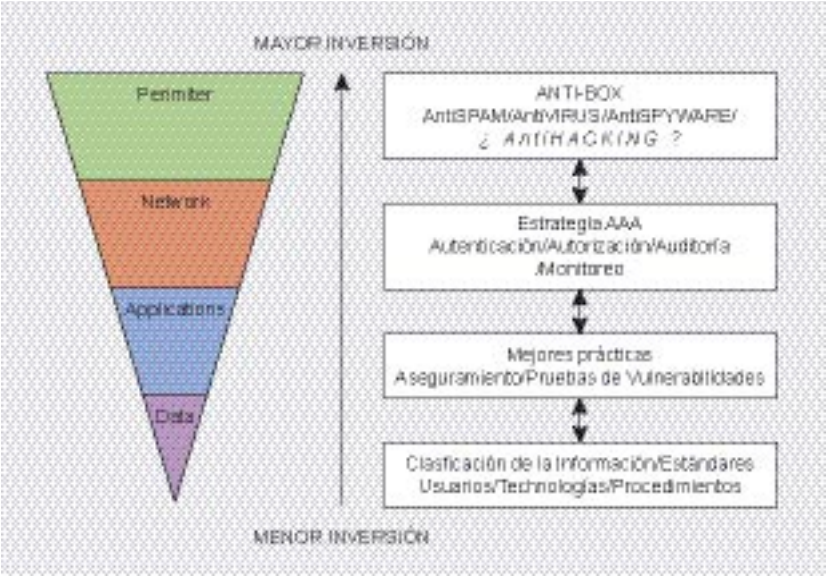

Figura. 1 *Análisis de la inversión en Seguridad Informática. [Adaptado de: KUPER, P. 2005]*

En un segundo lugar se encuentran las inversiones en tecnologías de autenticación, autorización, auditoría y monitoreo, las cuales de manera estratégica soportan y registran los eventos y el acceso a la información dentro de la infraestructura de tecnologías de información de la organización. En tercer lugar, se identifica las inversiones en el tema de aseguramiento de aplicaciones, fortalecimiento de sistemas operacionales, valoración de la seguridad, las cuales establecen buenas prácticas que permiten afianzar la distinción de gestión de la seguridad de la información

Finalmente, las inversiones sobre revisión y análisis de los datos que están residentes en la infraestructura de computación de la empresa, la clasificación de la información y las relaciones entre aplicaciones, procedimientos de operación y control de datos, uso de estándares internacionales, entre otras.

Al revisar estos resultados, es extraño ver que la menor inversión se concentra en la esencia misma de la seguridad informática, los datos, la información, y que la mayor se orienta a la adquisición de tecnologías para controlar en el exterior la aparición de amenazas contra el activo información.

Consecuente con este análisis, se adelantó una revisión paralela, siguiendo la misma estrategia del estudio de Stanley Morgan, para ver cómo evolucionan las vulnerabilidades, los resultados obtenidos establecen reflexiones que presentan en los siguientes párrafos.

Las mayores vulnerabilidades se presentan a nivel de los datos, de la información, generalmente asociadas con la falta de cultura de seguridad, la inadecuada disposición de medios de información, inadecuadas prácticas de seguridad asociadas con vulnerabilidades donde el factor humano y el incumplimiento de procedimientos se hacen presentes. Esta realidad se evidencia en todas las organizaciones en mayor o menor grado, según los esfuerzos de entrenamiento, información, capacitación y formación del personal de las áreas de negocio.

En segundo lugar tenemos las vulnerabilidades propias a las aplicaciones, las cuales frecuentemente están enraizadas en problemas con las herramientas y prácticas de programación, lo cual exige comprender que una aplicación está hecha tanto para cumplir con la especificación con la cual fue diseñada como para fallar ante un evento no esperado.

En tercer lugar, tenemos las fallas a nivel de comunicaciones. Los protocolos utilizados en las transmisiones de información tienen vulnerabilidades inherentes, las cuales con el tiempo se han venido detectando y corrigiendo, cuando es posible, o limitando la aparición de las mismas con tecnologías de seguridad que bloquean tráficos que puedan ser catalogados como sospechosos.

Finalmente, tenemos las vulnerabilidades propias de los proveedores y sus productos, los cuales constantemente están trabajando para producir los parches y actualizaciones requeridas para mitigar el riesgo que pueda comprometer la seguridad de la organización frente a las amenazas que cubre dicho software o hardware.

Como podemos observar al comparar los dos resultados, el de inversión y el de vulnerabilidades, se invierte donde existen menos vulnerabilidades. Por tanto, la seguridad, aunque reconocemos que es un proceso y no un producto, está siendo administrada en función de los recursos tecnológicos y las posibilidades que estos ofrecen. La pregunta es: ¿qué hacer para remediar esta situación?

Repensando la seguridad de la información

Basado en lo revisado hasta el momento, la seguridad de la información es una disciplina que, sustentada en la formalidad original de los años 60's, se ha fortalecido como un mundo tecnológico y normativo, donde cualquier anormalidad que se presente es una falla o vulnerabilidad que debe ser controlada o mitigada. Esta manera de razonar, ha permitido avances importantes en las tecnologías de protección, que de manera sistemática y asidua ha logrado importantes desarrollos y propuestas para enfrentar el *lado oscuro de la fuerza*, la inseguridad.

Si analizamos estos últimos 40 años de evolución de la seguridad informática, podemos ver que las investigaciones se han concentrado en revisar las limitaciones de los productos y teorías alrededor de la seguridad, es decir, hemos estado estudiando la inseguridad informática como factor base para los nuevos desarrollos (HUTCHINSON, B. y WARREN, M. 2001 Cap.4). Si esto es así, no podemos hablar de seguridad de la información, sin reconocer su dual, la inseguridad (CANO 2004).

En consecuencia, estudiar la inseguridad como estrategia para comprender la seguridad sugiere contextualizar en un escenario real la incertidumbre inherente del sistema o realidad a modelar, para revisar entre otros aspectos (SCHNEIER 2003, pag. 51):

- ¿Cómo funciona el sistema?
- ¿Cómo no funciona el sistema?
- ¿Cómo reacciona ante una falla o situación inesperada?
- ¿Cómo hacerlo fallar?

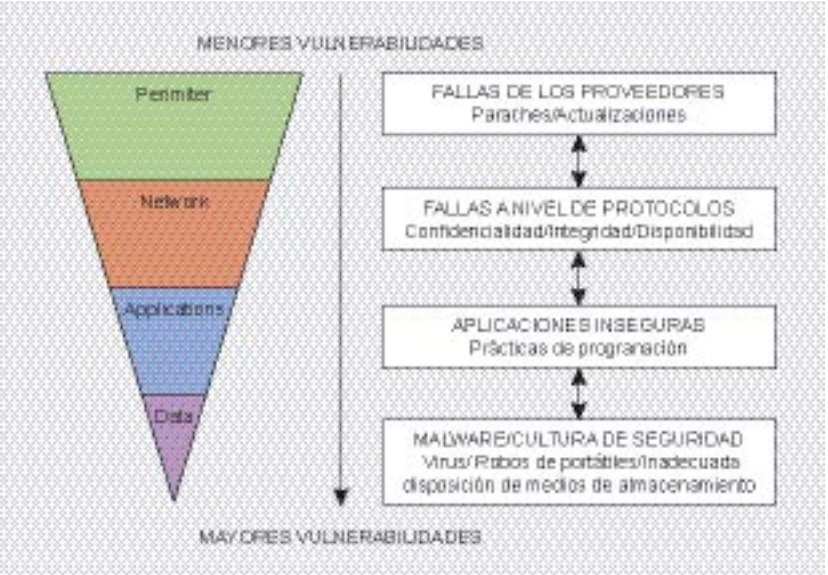

Figura 2. *Análisis de la evolución de las vulnerabilidades*

De acuerdo con una reciente investigación (CANO 2006) y considerando los elementos anteriormente presentados (Figura 1 y 2), se establecen cinco características que identifican tanto a la seguridad como a la inseguridad, las cuales serán analizadas y detalladas a continuación.

La seguridad es una realidad subjetiva, es decir propia del sujeto. Cada una de las personas tiene una manera de comprender y entender la seguridad. Es tan válida la definición de un ciudadano común, como la de un especialista en temas de seguridad, pues cada uno de ellos comprende la realidad de la seguridad según su exposición a la misma. Mientras que la inseguridad es objetiva, es decir, propia al objeto, una realidad perceptible, observable y verificable en el objeto. En este sentido, la inseguridad valida la esencia misma del análisis de riesgos, pues sólo a través de hechos cumplidos, verificables y comprobables podemos medir el nivel de exposición que tenemos y cómo podemos advertir mejores medidas de control para mitigarlo, atomizarlo, minimizarlo o transferirlo.

Agradecimientos

El autor agradece al Dr. Jorge Ramió Aguirre, a la Maestra Gabriela María Saucedo Meza y al Ingeniero Andrés Ricardo Almanza Junco por su tiempo y valiosos comentarios que permitieron afinar y ajustar las ideas expuestas en este artículo.

La seguridad no tiene cota superior, en otras palabras, siempre es posible encontrar una medida que sea más efectiva y/o eficiente que la anterior. Esto es fruto normal de la evolución de las medidas de protección, que entendiendo ¿cómo no funciona el sistema? es posible plantear estrategias que mejoren lo actualmente disponible. Si la inseguridad no tuviese cota superior como la seguridad, los seguros no existirían ni se podrían pagar. Es tal nuestra necesidad de mantener un nivel de protección, que debemos tratar de cuantificar el nivel de inseguridad que podemos administrar, siguiendo paradójicamente un nivel base de prácticas de seguridad y la dinámica de los procesos de negocio. En este sentido, podemos establecer un límite superior de exposición o riesgo que queremos asegurar, con las condiciones y precauciones que el asegurador establezca como mínimas para poder validar y pagar los daños como fruto de la materialización del riesgo, más allá de nuestro debido cuidado y diligencia para mantenerlo en los niveles establecidos.

La seguridad es intangible, no está en los mecanismos de seguridad, no está en los procedimientos, no está en las personas o en los cargos. La seguridad, complementaría al tema de la subjetividad previamente analizado, es la manifestación de que estamos ante un bien cuyo manejo no es evidente ni certero gracias a su volatilidad, fruto de la percepción de terceros. Por ejemplo, si nos detenemos a observar la variabilidad de los mercados financieros ante incertidumbres geopolíticas, nos percataremos de cómo se destruye la sensación de seguridad de los inversionistas ocasionando efectos devastadores en los movimientos financieros. En consecuencia y complementario con lo anterior, la inseguridad es tangible, es posible advertir el robo, la estafa, el accidente, la catástrofe, es una propiedad que es evidenciable y verificable, esa que se puede valorar con hechos y cifras, soportando un análisis real de los daños y efectos que ésta ha tenido.

Al ser la seguridad un intangible, necesariamente responde a una *propiedad emergente* de un sistema. Una propiedad emergente, es aquella que tienen los sistemas, fruto de la relación entre sus elementos y no particular a un objeto que lo conforma, en otras palabras, la seguridad es fruto de la relación existente entre la tecnología, los procesos y los individuos, como un todo coherente y alineado que comprende que no es posible alcanzar mayores niveles de seguridad sin un entendimiento o comprensión de las interrelaciones, muchas veces invisibles, que la seguridad sugiere cuando de protección de activos se trata.

De otra parte, la inseguridad es una propiedad inherente a los objetos, una realidad que deber ser evidenciada y explorada para ser comprendida, lo cual nos lleva necesariamente a la aparición de la administración de riesgos. Cuando entendemos que en el mundo donde nos movemos estamos expuestos a ellos, hacemos evidente que la inseguridad está presente en nuestro vivir y por tanto, es preciso advertir una serie de acciones que nos permitan mitigarlos. Es darle respuesta a la pregunta ¿Qué hacer si el sistema falla?

Cuando se habla de modelar o diseñar algo, buscamos que ese algo tenga las características que perseguimos. Si queremos que los activos gocen de seguridad, nos enfocamos en primer lugar a comprender los riesgos a los cuales está expuesto, para desarrollar las estrategias de seguridad requeridas y así lograr un nivel de exposición menor de dichos activos. Por otro lado, la inseguridad no requiere de modelos o diseños específicos o detallados, ella sabe que todos los objetos la contienen y sus manifestaciones se pueden manifestar en diferentes grados o impactos. En este sentido la inseguridad es una *propiedad inherente* a los objetos que advierte la manera de cómo establecer los mecanismos mínimos para limitar la materialización de la misma en un escenario con unos actores y variables.

Basado en esta exploración de los conceptos de seguridad e inseguridad es posible sugerir que es arriesgado afirmar que podría administrarse la seguridad cuando la inseguridad propia de los objetos nos muestra elementos reales y tangibles que ofrecen características de gestión que pueden llegar a ser analizados y cuantificados de tal forma, que se planteen métricas de inseguridad que basadas en buenas prácticas de seguridad y control, puedan alcanzar niveles mínimos permitidos

En la Red:

- BEAVER, K. (2006) Don't Spring a Leak. Information Security Magazine. Enero. Disponible en: *http://informationsecurity.techtarget.com/magItem/0,291266,sid42_gci1154838,00.html*,
- CANO, J. (1997) Auditorías de Seguridad, Evaluaciones de Seguridad y Pruebas de penetración: tres paradigmas en la seguridad informática. Disponible en: *http://www.derechotecnologico.com/estrado/estrado003.html*,
- CANO, J. (2004) Inseguridad Informática. Un concepto dual en seguridad informática. *http://www.virusprot.com/art47.html*,
- WILLIAMS, M. (2006) Security threat changing, says Symantec CEO. Disponible en: *http://www.networkworld.com/news/2006/110306-security-threat-changing-says-symantec.html*,
- MIMOSO, M. y SAVAGE, M. (2006) Today's Attackers Can Find the Needle. Information Security Magazine. Junio. Disponible en: *http://informationsecurity.techtarget.com/magItem/0,291266,sid42_gci1191313,00.html*,
- ROITER, N. (2006) That Sinking Feeling. Information Security Magazine. Octubre. Disponible en: *http://informationsecurity.techtarget.com/magItem/0,291266,sid42_gci1219723,00.html*,
- SAVAGE, M. (2006) Protect What's Precious. Information Security Magazine. Diciembre. Disponible en: *http://informationsecurity.techtarget.com/magItem/0,291266,sid42_gci1232273,00.html*.

y así mantener asegurados los bienes o activos que se tengan bajo observación y custodia.

Si la reflexión anterior es correcta se requiere repensar la administración de la seguridad, por una de inseguridad donde, haciendo evidente cada una de las características de esta última, podamos desaprender las prácticas actuales de administración del riesgo focalizadas en objetos, para reconocer en las relaciones que generan las expectativas de la gerencia (COHEN, F. 2005), los procesos de negocio y la infraestructura de computación, una fuente complementaria para el entendimiento de las vulnerabilidades en los sistemas.

Hacia un modelo de Administración de Inseguridad Informática

Los modelos actuales de administración de seguridad, generalmente buscan descubrir y corregir las fallas, pero no generan estrategias formales para entender la inseguridad; se concentran en establecer las correcciones y los controles requeridos para mejorar la efectividad y eficiencia de la gestión del modelo de seguridad (SCHOU, C. y SHOEMAKER, D. 2007). Si bien este razonamiento es útil por la manera sistemática de aprender del sistema y sus fallas, presenta limitaciones para desaprender de sus prácticas aprendidas, cuando se enfrenta a situaciones inesperadas o no contempladas en el modelo.

Para lograr materializar las ideas presentadas previamente y darle una posible respuesta a la pregunta planteada: ¿qué hacer frente a la inseguridad o riesgos inherentes a la realidad de las organizaciones?, se propone un modelo de administración de inseguridad informática basado en dos ideas principales: *descubrir la inseguridad y entender la inseguridad*.

El *descubrir la inseguridad* es utilizar el enfoque tradicional (sistemático) de administración de riesgos que se viene utilizando, donde los ejercicios de valoración de seguridad requieren un conocimiento especializado, fundado generalmente en herramientas y estrategias prácticas para identificar vulnerabilidades, orientado a resultados prácticos y concretos en cada uno de los elementos de evaluación y que exige personal especializado en el conocimiento de los objetos evaluados. Como resultado de este ejercicio tenemos la evidencia de los riesgos y controles requeridos para mitigar la presencia de la inseguridad. (KOVACICH, G. y HALIBOZEK, E. 2006)

Entender la inseguridad significa comprender las relaciones de los elementos que son objeto de evaluación. Esto implica revisar de manera sistémica e inteligente (SCHWANINGER, M. 2006, cap. 1 y 2) los resultados de la evaluación considerando, como mínimo, los aspectos de la tecnología, los individuos y los procesos, no para analizar lo que ocurre, sino para comprender porqué ocurre y efectuar un diagnóstico de la situación. En pocas palabras en términos sistémicos, administrar la variedad y complejidad que exhibe el sistema.

Cuando se aplican las consideraciones sistemáticas y sistémicas al mismo tiempo, se comprenden de manera complementaria los ejercicios tradicionales de seguridad y se posibilita un diagnóstico real de una situación anormal. Este diagnóstico puede llevarnos a desaprender lo conocido y a establecer nuevas distinciones en cualquiera de los niveles de análisis (estratégico, táctico y operacional), generando conocimiento que alimente el desarrollo de mejores estrategias de negocio, la aplicación de estándares y buenas prácticas, así como una asertiva ejecución los procedimientos de operación.

El modelo presentado (Figura 3) pretende, que la organización de manera dinámica, comprenda que cada nivel afecta a su nivel superior, esto es, lo que se evidencie en el análisis y diagnóstico del nivel operacional afecta al nivel táctico y así sucesivamente, evitando la fragmentación de la visión de seguridad y promoviendo una postura proactiva y global de la organización, que reconoce en la seguridad la propiedad emergente fruto del reconocimiento y entendimiento de los riesgos inherentes a cada uno de los objetos que la conforman.

Librería

- CANO, J. (2006) Information Insecurity: A dual concept of information security. Proceeding of 2nd Internacional Conference on E-Global Security. Londres, UK. Abril.
- COHEN, F. (2005) Security Governance: Business Operations, security governance, risk management and enterprise security architecture. ASP Press.
- COVEY, S. (2005) El octavo hábito. De la efectividad a la grandeza. Editorial Paidos.
- HUTCHINSON, B. y WARREN, M. (2001) Information warfare. Corporate attack and defense in a digital world. Butterworth Heinemann.
- KIELY, L y BENZEL, T (2006) Systemic security management. IEEE Security & Privacy. Noviembre/Diciembre.
- KOVACICH, G. y HALIBOZEK, E. (2006) Security metrics management. How to manage the cost of an assets protection program. Butterworth Heinemann.
- KUPER, P. (2005) The state of security. IEEE Security & Privacy. Septiembre/Octubre
- SCHNEIER, B. (2003) Beyond Fear. Thinking Sensibly about security in an uncertain world. Copernicus Books.
- SCHOU, C. y SHOEMAKER, D. (2007) Information Assurance for the enterprise. A roadmap to information security. McGraw Hill.
- SCHWANINGER, M. (2006) Intelligent organizations. Powerful models for systemic management. Springer Verlag.
- TAYLOR, R., CAETI, T., KALL LOPER, D., FRITSCH, E. y LIEDERBACH, J. (2006) Digital crime and digital terrorism. Pearson Prentice Hall.
- THE HONEYNET PROJECT (2004) Know your enemy. Learning about security threats. Addison Wesley.

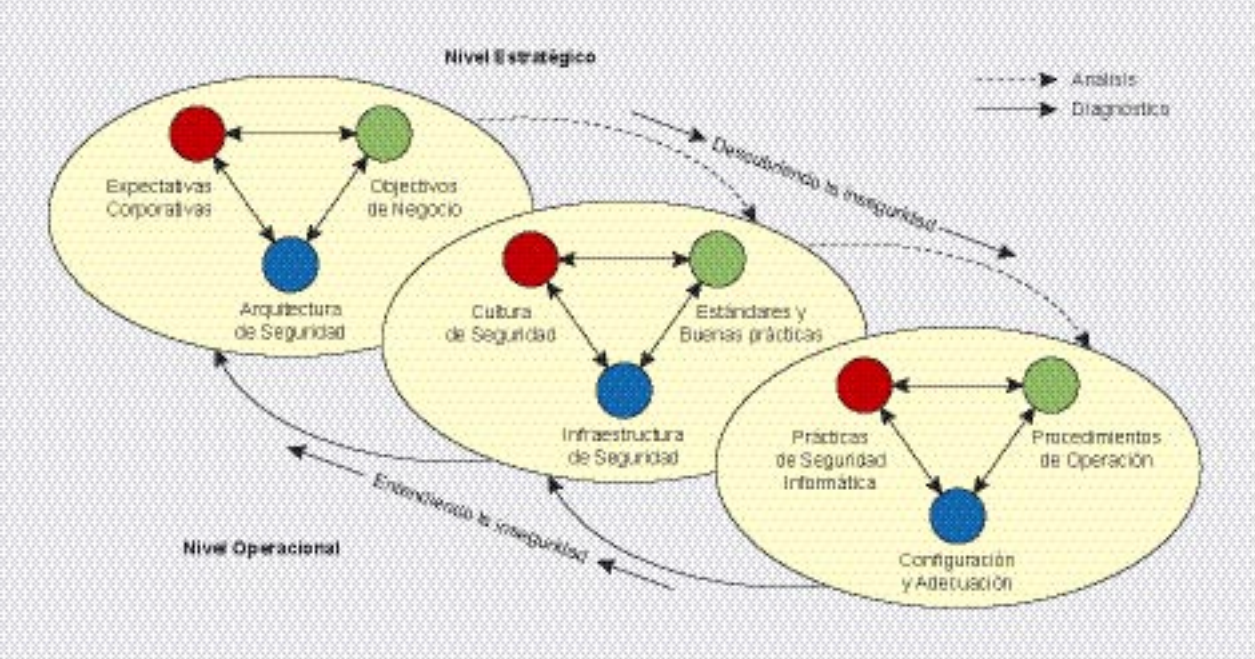

Figura 3. *Modelo de Administración de la Inseguridad Informática*

Si esto es así, la organización destruirá estructuralmente la falsa sensación de seguridad y la reemplazará por una estrategia de aprendizaje permanente sobre los incidentes que se presenten, como la norma misma de la gestión de éstos. Esto es, tomará ventaja de lo que aprende de la inseguridad de la información, para construir mejores propuestas de protección, basado en aquello que ven los intrusos y las ventajas que ofrecen las tecnologías.

Conclusión

La realidad del creciente número de vulnerabilidades reportadas, incidentes ocurridos y fallas identificadas nos invita a reflexionar sobre la forma de cómo hemos venido afrontando los riesgos que éstas generan y los impactos de las mismas. En este sentido, el paradigma actual de la seguridad de la información ha entrado en crisis, por lo que se requiere estudiar en profundidad la mente de los intrusos y sus reflexiones para comprender mejor lo que ocurre ante una falla. Por tanto, no es suficiente descubrir la falla puntal y analizar cómo se materializó, sino que se requiere una revisión relacional de lo que ocurrió para entender de manera estructural el porqué de ésta.

Por tanto, se hace necesario complementar el modelo de riesgos y controles actual, con uno basado en las técnicas de *hacking*, que más allá de estar concentrado en los activos a proteger y sus vulnerabilidades, reconoce las relaciones de los diferentes componentes del sistema para responder las preguntas planteadas anteriormente (sección repensando la seguridad de la información).

El modelo de Administración de la Inseguridad Informática (Figura 3) presentado vincula los dos paradigmas, el de riesgos y controles y el del *hacking*, como una manera efectiva de procurar una administración de la protección de la información, cuya dinámica de aplicación debe llevar a una distinción organizacional sobre la gestión de la inseguridad de la información que se denomina en la teoría *information assurance* (SCHOU, C. y SHOEMAKER, D. 2007) o aseguramiento de la información.

Finalmente, el modelo de ADINSI propuesto (Figura 3) es una manera alterna para comprender que existen tensiones entre las personas, los procesos y la tecnología (KIELY, L y BENZEL, T 2006) que deben ser objeto de revisión permanente y así evaluar el impacto de las mismas en temas como las expectativas de la alta gerencia, la arquitectura de seguridad informática y las prácticas de seguridad de las organizaciones. ●

Sobre el Autor

Jeimy J. Cano, Ph.D, CFE. Miembro investigador del *Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática* (GECTI). Facultad de Derecho. Universidad de los Andes. Colombia. Miembro Investigador de ALFA-REDI (*Red Latinoamericana de Especialistas en Derecho Informático*). Ingeniero de Sistemas y Computación, Universidad de los Andes. Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Ph.D in Business Administration, Newport University. Profesional certificado en *Computer Forensic Analysis* (CFA) del World Institute for Security Enhacement, USA. Profesional certificado como *Certified Fraud Examiner* (CFE) por la *Association of Certified Fraud Examiners*. Contacto: *jjcano@yahoo.com*.