



Las organizaciones de cara a la seguridad informática

Jeimy J. Cano, Ph.D, CFE

La inseguridad informática [CANO 2004] es la constante en el mundo actual. Las permanentes advertencias de fallas, las diferentes alternativas de penetración de sistemas y la creciente explotación de vulnerabilidades técnicas, procedimentales y humanas, nos alertan sobre la creciente complejidad que exhibe cada uno de los elementos que conforman o dan sentido a la distinción de seguridad de la información en las organizaciones.

En este contexto, las corporaciones modernas, comprometidas en aumentar su nivel de seguridad de la información deben desarrollar elementos conceptuales y prácticos que les permitan satisfacer las expectativas de la gerencia, los objetivos de los programas de seguridad y la con-

fiabilidad de los servicios de seguridad de la información.

Por tanto, se abre paso un nuevo concepto extendido de los temas de gobierno corporativo que denominamos Gobierno de la Inseguridad Informática (GI2). Ver figura 1.



Figura No.1 Gobierno de la Inseguridad Informática

Gobierno de la Inseguridad Informática (Gobierno de la ISI)

El GI2 es el escenario donde se establecen las expectativas de la gerencia en torno a la administración de la

seguridad de la información. Para ello, define en sí mismo la arquitectura de seguridad informática, la cual constituye la materialización de las inquietudes de la gerencia en riesgos de negocio, objetivos de negocio, vulnerabilidades, amenazas, requerimientos de seguridad, inversiones de seguridad informática, entre otros aspectos. Todo ello, como una manera de establecer los niveles de inseguridad que deberá gobernar a la luz de esta arquitectura.

De cara a lo anterior, es necesario operacionalizar esta distinción de gobierno, manifestada en una arquitectura, para lo cual surge el concepto de administración de la inseguridad informática (administración de la ISI). Esta administración, considerando los lineamientos de la arquitectura, deberá desarrollar los programas de seguridad informática y la infraestructura de seguridad soporte de la misma. En este sentido, los directores o encargados de la seguridad informática tienen que velar por una adecuada operacionalización de la arquitectura en la infraestructura, para procurar la confiabilidad de los servicios y generación de confianza en los usuarios, además de validar y satisfacer las expectativas de la gerencia en este tema.

En forma paralela, se tiene en el último nivel la operación de la inseguri-

"... las corporaciones modernas, comprometidas en aumentar su nivel de seguridad de la información deben desarrollar elementos conceptuales y prácticos que les permitan satisfacer las expectativas de la gerencia".

dad informática (operación de la ISI), como la materialización plena del uso de los procedimientos, tecnologías y comportamiento de los individuos en el contexto organizacional. De esta manera, las interacciones entre estos elementos y la infraestructura ofrecerán elementos de valoración del estado de la inseguridad reinante en las organizaciones.

Nivel de aseguramiento de la información

Si todo este conjunto de distinciones fruto de un gobierno de la inseguridad se presentan, es decir se mantiene un nivel de satisfacción de las

"El GI2 es el escenario donde se establecen las expectativas de la gerencia en torno a la administración de la seguridad de la información".

expectativas de la alta gerencia, una adecuada implementación de programas e infraestructura de seguridad y un importante nivel de confiabilidad en los servicios de seguridad, estaremos abriendo la puerta a una propiedad emergente propia de este gobierno, que los expertos denominan "information assurance" [BISHOP 2003, IATF] o que podríamos parafrasear como nivel de aseguramiento de la información.

En la medida en que los elementos anteriormente expuestos se conjungen y se ordenen para mantener un nivel aceptable de inseguridad en la organización, podemos decir que esta madura en su gestión de la seguridad y en este sentido, exhibe una propiedad fruto de esta interacción que llamaremos nivel de aseguramiento de la información, el cual

deberá ser evaluado y revisado por el oficial de cumplimiento, quien será la autoridad para establecer los niveles de gobierno y aseguramiento en cada uno de los niveles establecidos: gobierno, administración y operación.

EL GI2 es la respuesta natural de la gerencia del área de seguridad informática, no para decirle a la alta gerencia el nivel de seguridad con que se cuenta, sino el nivel de confiabilidad y confianza alcanzado en las funciones de negocio y por ende de sus clientes.

Es una estrategia corporativa de protección de los activos, que reconoce las vulnerabilidades inherentes de los elementos de los sistemas de las empresas, para promover una administración y operación de la inseguridad como sistema preventivo y activo, frente a las cambiantes realidades de la organización, la tecnología y las personas.

Madurez permanente

Al reconocer el GI2 como esa estrategia que destruye la falsa sensación de seguridad, las falsas pretensiones de sistemas seguros y la perfecta conjunción entre comportamientos humanos y operaciones tecnológicas, es posible avanzar en mejores

"... comprender que el proceso de madurez exige alinear la confiabilidad de los servicios de seguridad, los programas e infraestructura y las expectativas de negocio en un solo sentido".

niveles de madurez de la función de seguridad de la información. Se pasaría rápidamente de una concentración en aplicaciones o proyectos de infraestructura a fortalecimiento de arquitecturas de seguridad de la información, no como proyectos conceptuales o estratégicos en sí mismos, sino como realidades con-

cretas en la operación de la inseguridad por parte de todos los participantes de la organización.

Visualizar el GI2 como la ruta para crecer en la relación entre objetivos de negocio, valor agregado y generación de confianza en las diferentes áreas de la organización y sus clientes, es comprender que el proceso de madurez exige alinear la confiabilidad de los servicios de seguridad, los programas e infraestructura y las expectativas de negocio en un solo sentido, aquel que le da forma a la organización en un contexto globalizado.

Referencias

CANO, J. (2004) Inseguridad Informática. Un concepto dual en seguridad informática.

Disponible en:

<http://www.virusprot.com/Art47.html>

BISHOP, M. (2003) Computer Security. Art and Science. Addison Wesley.

Information Assurance Technical Framework - IATF - USA.

http://www.iatf.net/framework_docs/ve rsion-3_1/index.cfm

Jeimy J. Cano, Ph.D, CFE. Es egresado del Programa de Ingeniería y Maestría en Sistemas y Computación de la Universidad de Los Andes. Cuenta con un doctorado en Filosofía de la Administración de Negocios, título otorgado por Newport University en California, Estados Unidos. Además de una certificación como Examinador Certificado de Fraude - en inglés CFE. Es profesor e investigador a nivel nacional y latinoamericano en temas de seguridad informática, computación forense y sistemas de información. Actualmente, es Presidente de la Asociación Colombiana de Ingenieros de Sistemas (ACIS).