Responsable de la inseguridad de la información

Andrés Ricardo Almanza J.

De una visión simplista de la seguridad, a una visión que integra el riesgo como elemento estratégico en el cumplimiento de los objetivos del negocio.

La importancia de la inseguridad de la información en los ambientes organizacionales ha tomado mayor fuerza y relevancia, no solo como un plus, sino por la necesidad de proteger los volúmenes de información que día a día se producen al interior de las empresas; estos crecimientos desmedidos no poseen unas directrices y políticas claras con las cuales se puedan afrontar los retos acordes al crecimiento de la organización y la forma como la información es protegida.

Las organizaciones han venido transformando el concepto acerca de la inseguridad informática, por un enfoque más integral, en el cual ven la inseguridad como un proceso que cubre la información de la organización; la tecnología como fuente de su procesamiento; y, el recurso humano, encargado de manipular y responder por la misma. Es decir, se ha pasado de una visión simplista de la seguridad a una visión que integra el riesgo como elemento estratégico en el cumplimiento de los objetivos del negocio.

Este nuevo panorama requiere de mayores esfuerzos dentro de la organización por el cumplimiento de un programa estructurado, con una forma y un contenido, buscando su puesta en marcha de la mejor manera por esa nueva visión integral del la inseguridad, enfocada a la protección de los activos de información de la organización.

En este orden de ideas se requiere de alguien capaz de poder dirigir y dar marcha al programa creado y diseñado de manera específica para la organización; alguien que con esfuerzo, disciplina y una convicción clara pueda realizar la ardua labor de orquestar el panorama desmedido de inseguridad, al que la organización se ve expuesta en su constante crecimiento.

El ambiente corporativo

El documento "The Global State of Information Security 2007", investigación publicada entre PricewaterhouseCoopers, CIO y CSO, presenta los resultados de la encuesta global, en la cual se realiza un análisis acerca de la seguridad en lo transcurrido del año 2007, y muestra elementos interesantes.

En primer lugar, muestra un incremento sorprendente sobre la forma como la organización percibe la seguridad y la forma como día a día incrementa la creación de una estrategia corporativa de seguridad (57%).

De igual manera, dicho estudio evidencia un aumento considerable a la hora de hablar de los responsables de la seguridad de la información dentro de la organización; hoy se habla de un CSO (Chief Security Officer's) (28%), o CISO (Chief Information Security Officer's) (32%).

Según Garthner, más del 65% de las empresas más grandes del mundo tendrán una cabeza visible encargada de manejar en forma centralizada la seguridad y protección de las organizaciones; y, sobre todo, alguien que no solo vele por la inseguridad tecnológica de la organización, sino un profesional con una visión de negocios que le facilite el manejo de la seguridad.

Dentro de este panorama surgen algunas dudas: ¿Quién es ese responsable de la seguridad y protección de la información?, ¿cuáles son sus funciones básicas?, ¿a quién debe entregar reportes?, ¿por qué debe preocuparse?, ¿dónde debe estar ubicado?, ¿cuál será su interrelación con las distintas áreas?

Responsable de la seguridad

Para hablar de quién es el responsable de la seguridad de la información, es necesario hacer una retrospectiva sobre la forma como ha evolucionado la seguridad dentro de las organizaciones. En primer lugar, se podría decir que en el transcurso de los últimos ocho años, la seguridad ha tenido una visión netamente operacional; las organizaciones se han preocupado por proteger su perímetro, las estaciones de trabajo de los empleados; por tener sistemas adecuados de control de acceso, y demás mecanismos que impidan a intrusos afectar la operación de las plataformas tecnológicas, con las cuales prestan los diferentes servicios sobre las redes que utilizan.

Dentro de ese gran período, se pueden ver los cambios de los últimos tres años hacia la época actual, en la cual se observa como se busca mejorar la protección del perímetro interno, el desarrollo de las aplicaciones y algunos otros elementos operacio-

nales; ese cambio significativo se ha presentado sobre la inclusión de la protección de la información, ya no como un aspecto netamente técnico y operacional, sino con una perspectiva más corporativa, en donde la organización determina cuáles pueden ser las fuentes de riesgo que afecten al negocio, y así involucrar la seguridad en beneficio de prestar el servicio y/o producto de la mejor manera posible.

Vemos entonces que estos personajes presentan la seguridad de la información como un servicio de negocios, en el cual se pueden contemplar las siguientes actividades:

• Protección del perímetro de trabajo definido.

• Permitir que la organización pueda aumentar de la manera menos insegura posible, su perímetro de acción.

• Validar que los servicios dentro de la organización sean ejecutados de la mejor manera posible por parte de los miembros de la organización.

• Facilitar que la interacción empresa, empleados, proveedores y clientes, sea realizada de la manera menos insegura posible.

CISO vs. CSO

En la actualidad, muchas organizaciones están utilizando siglas como el CSO (Chief Security Officer) o CISO (Chief Information Security Officer) y en la realidad nacional se denomina OSI (Oficial de Seguridad Informática) o incluso algunos lo llaman (Oficial de Seguridad de la Información). Lo importante de su definición es pensar en cuál es el contexto en que está concebida esta posición, dentro de las empresas.

Para definir su contexto, las organizaciones deben evaluar paradigmas de protección tales como:

• Qué es lo que se pretende abordar: seguridad en la infraestructura de IT o seguridad de la información, en la cual se contemplan elementos como (seguridad física, seguridad de los empleados, seguridad de los procesos).

• Visión de la seguridad desde el punto de vista técnico, o servicio de apoyo a los servicios de negocio de la organización.

• Enfoque y orientación a procesos y procedimientos.

• Arquitecturas de servicios orientadas a la seguridad y protección de los activos de información de la organización.

• Entrenamiento y conciencia organizacional sobre la seguridad de la organización, o si solo las áreas de

tecnología deben poseer dicha conciencia.

• Gobierno corporativo en torno a la seguridad de la organización.

Para cualquiera de los enfoques previstos, debe describirse al responsable de seguridad como el líder con las habilidades necesarias para manejar de manera clara y de acuerdo con las necesidades de la organizaciones, la seguridad y protección de la organización; bien sea que su enfoque esté direccionado a TI o tenga una visión más amplia del mismo, su labor será la de crear una postura de seguridad para la organización. En la creación de dicha postura debe utilizar todas las herramientas que considere necesarias para incorporar de la manera más exacta posible, la seguridad en el negocio.

Roles funciones y responsabilidades

Los roles y responsabilidades pueden ser vistos desde tres enfoques o perspectivas, los cuales pueden ser considerados como marco de actividades, dentro de las cuales están:

Marco Estratégico:

En esta perspectiva tenemos como campo de acción la preocupación que tiene el responsable, de velar por el marco corporativo de seguridad, además de hacer ver a la organización la importancia de la seguridad como un componente estratégico en la prestación de los servicios de la organización.

Es indispensable que piense en el diseño de los productos y o servicios de la organización, buscando incluir la seguridad como elemento importante. Así mismo, mostrar las ventajas y desventajas de tener o no contemplada la seguridad.

Dentro del conjunto de actividades de este nivel se encuentran las siguientes, sin ser las únicas.

• Diseñar, plantear, desarrollar la estrategia y visión corporativa de la seguridad de la información.

• Ser punto de contacto y miembro asesor del equipo directivo, frente al riesgo y las implicaciones que este tiene dentro de la organización.

• Diseño de la arquitectura de seguridad y protección de la información para la organización.

• Definición de indicadores de medición de la seguridad al interior de la organización.

• Diseñar, planear y seguir el plan estratégico de seguridad de la información, alineado a la organización.

• Participar en la creación del programa de continuidad de la organización.

• Ser un asesor para las unidades de negocio de la organización en los temas de seguridad y protección de la información.

• Sustento de presupuestos en temas de seguridad y protección para la organización.

Marco Táctico:

Desde ese punto de vista, el responsable de la seguridad de la organización, debe velar por la ejecución de las tareas de mediano plazo dentro de la empresa y que soportan la gestión de su función. En ella está la creación de controles de gestión, objetivos y resultados específicos en la consecución de su trabajo, entre otros figuran:

• Creación de la política organizacional de seguridad de la información, así como el marco procedimental y de estándares a aplicar dentro de la compañía.

• Diseño del programa de concientización y entrenamiento.

• Preocuparse por el cumplimiento de normativas, legislaciones y leyes que cubran a la organización, en la prestación de sus servicios.

• Ser el líder del grupo de trabajo de seguridad (Comité de Seguridad de la Información) dentro de la organización.

• Creación de procesos necesarios para la gestión y respuesta ante incidentes.

• Monitoreo continuo del proceso de gestión de seguridad de la información.

• Punto de contacto con entes externos de la organización, en temas relacionados con la seguridad que afecte a la organización.

• Unión estrecha con las áreas de seguridad física, en procura de velar por la visión corporativa de seguridad de la información.

• Cooperación con las auditorías externas.

Marco Operacional:

Este enfoque involucra las actividades de corto plazo relacionadas con el día a día. Entre otras están:

• Análisis de vulnerabilidades y amenazas a activos de información.

• Preocupación por la protección de los perímetros de la organización.

• Entrenamiento de las áreas de TI en temas de seguridad, concientización a la empresa en temas de seguridad de la información.

• Monitoreo y revisión de la infraestructura de eventos de seguridad de la organización.

• Investigaciones y trabajo forense.

• Pruebas de vulnerabilidades e intrusiones.

Competencias

Cuando se habla de competencias para el desempeño de este tipo de cargos, es necesario revisar las competencias técnicas, así como las conductuales para que el profesional que va a desempeñar dicho cargo, lo pueda hacer de la mejor manera. Entre ellas, están:

Competencias conductuales:

Son las competencias inherentes a la persona y dentro de las cuales deben estar entre otras:

• Facilidades para la comunicación, poseer las habilidades de comunicación necesarias para interactuar en los niveles de la organización (estratégico, técnico, de usuario final).

• Debe tener una clara orientación estratégica y táctica.

• Perspectiva global.

• Madurez emocional, para afrontar los momentos de crisis y responder ante las mismas.

• Agente generador de cambio.

• Alto compromiso organizacional.

• Un negociador por excelencia, con el ánimo de integrar las necesidades de las unidades de negocio y motivarlos en la utilización e inclusión de los servicios de seguridad que su área presta.

• Inteligente y audaz, para saber actuar en el momento oportuno.

• Autónomo para la toma de decisiones.

• Habilidad para la interrelación e interacción con grupos de trabajo.

• Honestidad e integridad.

Competencias técnicas:

No son otra cosa que el soporte y experiencia de la persona que se encargará de desempeñar dicho rol. Son, entre otras:

• Formación profesional en seguridad de la información, a nivel técnico, y estratégico, para validar su experiencia.

• Experiencia en continuidad de negocios, gestión del riesgo y auditoría.

• Conocimiento acerca de las normativas de gestión de seguridad de la información del mercado y su forma de aplicación en la organización.

• Experiencia en el desarrollo de pruebas técnicas de seguridad (Pen-Test / Valoración de Seguridad).

• De 2 a 4 años de experiencia en el campo de la seguridad informática y/o seguridad de la información, que pueda ser demostrable.

• Habilidad y destreza para el manejo de simultaneidad en la ejecución de proyectos.

Ubicación del responsable de seguridad de la información

Este aspecto es de alta relevancia, dado que define la forma como el responsable de seguridad de la información interactúa con la organización; así mismo define la forma en cómo es visto para la misma.

La posición del responsable de seguridad de la información puede estar sujeta a la forma como la organización se comporta. Con base en tal apreciación, es posible que se encuentren las siguientes estructuras para el desempeño de sus funciones:

Responsable de seguridad dependiendo del área de TI. En la mayoría de los casos, esta posición refleja una clara orientación hacia la seguridad informática y su visión puede ser sesgada por el alcance del área a la que pertenece.

Responsable de seguridad dependiendo del área de Auditoría y Control Interno. En esta posición se nota una clara independencia con las áreas de TI; su enfoque es un poco más amplio, pero puede estar limitado a las funciones de auditoría y cumplimiento de acuerdo con los lineamientos del área a la que pertenece.

Responsable de seguridad como grupo de apoyo a la alta gerencia. Posición ideal que muestra el grado de madurez de la organización, frente a la seguridad de la información; en ella se puede ver que las empresas no solo contemplan la seguridad, sino que ven en dicha persona un asesor que le ayude a entender de manera clara los riesgos a los que el negocio está expuesto. Cada una de las posiciones anteriormente descritas, tiene sus pros y sus contras; lo importante es que se visualice como un proceso de evolución por el cual las organizaciones deben pasar, de tal manera que alcancen un nivel adecuado de madurez frente a la seguridad y protección de la organización.

Conclusiones

La complejidad de la inseguridad de la información, plantea la necesidad de un responsable de la seguridad dentro de la organización; su asesoría se hace indispensable en pro del cumplimiento de los objetivos del negocio; y, a la vez, permite proteger sus activos de información.

Se considera necesario que las organizaciones empiecen a visualizar la necesidad de involucrar una persona con estas características, de tal manera que vayan incluyendo la seguridad no solo como un panorama netamente tecnológico, sino desde una visión más amplia, en la cual se consideren otros escenarios que desde la concepción tecnológica no pueden ser tenidos en cuenta. Dentro de sus cualidades, habilidades y destrezas estarán entonces la disciplina, el autoestudio, la autocrítica, y por sobre todas las cosas, unas excelentes facilidades de comunicación e interrelación con todas las áreas, unidades de negocio, y miembros de la organización, a quien deba hacerles llegar el mensaje.

La seguridad de la información como se ha mencionado es "personalizable"; es decir, cada organización posee su propia realidad y por ende tiene sus propias necesidades. En ese orden de ideas, es necesario responder el cuestionamiento acerca de cuál es el rol que debe desempeñar el oficial de seguridad y protección de la información. La respuesta ideal será "el que la organización desde su personalización demande". Lo que sí puede ser claro a la hora de definir su rol es que debe cumplir con varios componentes generales, pero claves a la hora de desempeñar su función:

1) Tener claro la postura de seguridad que se debe crear para la organización, visualizando los riesgos como una realidad inherente al negocio y la forma como mitigarlos al prestar los servicios.

2) Todo lo planeado, diseñado, estructurado, debe ser medido; así se observa si la postura es funcional para la organización o si requiere ajustes en su operación.

3) Procurar realizar un seguimiento adecuado de la implementación, bien sea desarrollada por el responsable de seguridad o delegada en otras personas (responsables de activos de información, áreas de TI).

4) Buscar de la manera más independiente posible, la validación de que lo realizado esté bien hecho; con ello se garantizan los resultados de lo planeado, y ejecutado.

Así mismo, es importante resaltar que como la realidad de las organizaciones puede ser tan variada, es posible que alguno de estos puntos clave no existan en la organización; por lo tanto, se tendría que trabajar en los otros aspectos, a sabiendas de que la organización es débil y los costos de la operación pueden aumentar.

Es necesario que el responsable de la seguridad maneje una posición privilegiada dentro de la organización, dado que debe interactuar con los diferentes niveles de la empresa.

Su primer grado de interacción será con las directivas de la organización, de tal manera que pueda hacerles ver que los servicios prestados por la empresa, pueden ofrecerse de una mejor manera si es involucrada la seguridad dentro de los mismos. Por otro lado, un lenguaje técnico para interactuar con las áreas de TI, transmitiendo la necesidad de unas plataformas y unas operaciones que involucren la seguridad y la importancia de ellas en la operación del negocio. Y, por último, debe interactuar de una forma paciente con los usuarios de la organización, explicándoles las razones por las cuales es vital la seguridad en la operación del negocio.

Referencias

[1] ASIS: "Chief Security Officer Guideline", ASIS, Agosto 2004. www.asisonline.org/guidelines/guidelineschief.pdf

[2] NASCIO: "Born of Necesity: The Ciso Evolution – Bringing the Technical and the Policy Together", NASCIO, July 2006. www.nascio.org/publications/documents/NASCIO-CISO_Brief_071006.pdf
"A Current View of the State CISO: A National Survey Assessment"
NASCIO, September 2006
www.nascio.org/publications/documents/NASCIO-CISOsurveyReport.pdf

[3] Educause: "Safeguarding Information Assets in Higher Education: The Role of the CSO", Educause, Octubre 2006. http://net.educause.edu/ir/library/pdf/erm0655.pdf

[4] Wylder J. (2004) Strategic Information Security. Addison Wesley.

[5] Kovacich G. (2003) The Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program, Second Edition.

[6] Butterworth Heinemann. PwC: "The Global State of Information Security – 2007", PwC, September 2007. http://www.pwc.com/extweb/pwcpublications.nsf/docid/114E0DE67DE69653852573410 05AED7B/$FILE/PwC_GISS2007.pdf

Andrés Ricardo Almanza Junco Ms(c). *Ingeniero de Sistemas, Universidad Católica de Colombia; especialización de Seguridad en Redes de la misma Universidad. Master en Seguridad de la Información de la Universidad Oberta de Cataluña. Ha sido docente de postgrados en las Universidades Pontificia Bolivariana, Rosario de Colombia y Externado de Colombia. Es miembro de la Red Iberoamericana de Cristología y Seguridad de la Información –CriptoRED (http: //www.criptored.upm.es)-. En la actualidad, es Jefe de Seguridad y Protección de la Información de la Cámara de Comercio de Bogotá.*