Los CISO (Chief Information Security Officer) se Pronuncian

Sara Gallardo M.

La revista Sistemas indagó con los Directores de Seguridad de la Información de cuatro importantes organizaciones, el entorno que rodea su gestión, en términos de responsabilidad, acciones y alcance.

Las inquietudes sobre los diferentes aspectos que cobijan la gestión de los CISO, no son pocas, de ahí el interés en resolver varios interrogantes. Para ello, recurrimos a Carlos Zambrano, jefe de Seguridad Informática para Latinoamérica, en Terpel S.A.; Javier Díaz Evans, director de Seguridad de la Información, en ATH S.A.; Francisco Pacheco Alfonso, director de Seguridad de la Información, en Deceval; y, Andrés Ricardo Almanza Junco, coordinador de la Seguridad de la Información, en la Cámara de Comercio de Bogotá.

1. Es claro que la seguridad de la información sigue escalando posiciones importantes en las organizaciones, sin embargo, ¿cuáles consideran ustedes en su práctica que son los drivers (orientadores) se deben considerar para profundizar y fortalecer este tema y sus prácticas asociadas?

2. ¿En qué no se puede equivocar un CISO para tener éxito en su gestión de seguridad de la información? 3. ¿Cuáles son los riesgos emergentes que usted observa en la seguridad de la información en las empresas del país? ¿Cuál debería ser la prioridad para enfrentarlos y porqué?

4. ¿Considera usted que la seguridad de la información es un tema de negocio? ¿Qué debería hacer la función de seguridad de la información para que esto se manifieste como tal? ¿Qué limitaciones observa para que esto se dé?

5. ¿Cuáles serían sus recomendaciones para hacer de la seguridad de la información un tema de las Juntas Directivas de las organizaciones?

Carlos Zambrano
Jefe Seguridad Informática
Latinoamérica Terpel S.A.
carlos.zambrano@terpel.com

Revista Sistemas: Es claro que la seguridad de la información sigue escalando posiciones importantes en las organizaciones, sin embargo, ¿cuáles consideran ustedes en su práctica que son los drivers (orientadores) se deben considerar para profundizar y fortalecer este tema y sus prácticas asociadas?

Carlos Zambrano: Lo interesante es cautivar la importancia de la seguridad de la información como socio estratégico del negocio y su enfoque vital ante cualquier riesgo que afecte la operación y su imagen. Por ende y ante cualquier proceso de implementación de un sistema de seguridad informática, se trata de culturizar a los miembros de la organización, con el objeto de alcanzar un umbral de madurez, orientado a trazar lineamientos en los logros alcanzables y medibles de un modelo de seguridad informática.

La madurez que debe alcanzar una organización en el entendimiento de las prácticas de seguridad es la cadena del éxito en la mitigación del riesgo y el compromiso de todos los miembros de la organización en las continuas mejoras en la protección de la información. Sin este entendimiento y cultura, es difícil focalizar las estrategias de seguridad y la posición misma en la organización.

Un líder de seguridad de la información debe inclinar su balanza en un proceso de comunicación continua de cultura en la etapa inicial de implementación, con el fin único de involucrar a todos los miembros en este proyecto indefinido en tiempo, considerando que es para toda la vida organizacional mantener las estrategias.

RS: ¿En qué no se puede equivocar un CISO para tener éxito en su gestión de seguridad de la información?

CZ: Una de las equivocaciones es definir un modelo de seguridad de la información no alineada con la planeación y estrategia del negocio, así como la no existencia de un programa continuo de mejoras, acorde con la velocidad del negocio y el mercado.

Un CISO debe ser un ente estratégico, con visión sobre los procesos del negocio, a fin de concentrar sus fuerzas en la definición de acciones sobre la protección de la información, para no desviar a otros niveles en los que se pierden esfuerzo y dinero.

RS: ¿Cuáles son los riesgos emergentes que usted observa en la seguridad de la información en las empresas del país? ¿Cuál debería ser la prioridad para enfrentarlos y porqué?

CZ: La tendencia de ataques locales. En nuestro país se están desarrollando y ejecutando programas maliciosos para dirigirlos a una población estándar, a una única empresa o a una identidad focalizada, con el objeto de robar información y venderla al mejor postor. Hace unos tres años, lo más Top era negar servicios, pero en la actualidad las cosas

han cambiado y los atacantes -especialistas en su actividad-, han visto muy interesante el robo de información para venderla y generar ingresos. Desde mi punto de vista, las empresas no han tenido un programa para concienciar a sus miembros en los lineamientos de sus políticas de seguridad ni en su cumplimiento, para alcanzar la madurez que les permita reducir la brecha del riesgo.

RS: ¿Considera usted que la seguridad de la información es un tema de negocio? ¿Qué debería hacer la función de seguridad de la información para que esto se manifieste como tal? ¿Qué limitaciones observa para que esto se dé?

CZ: En los puntos anteriores he manifestado que la seguridad informática es un ente estratégico del negocio, el cual, en virtud de su palabra, es exitoso siempre y cuando cumpla con sus procesos en el logro de las utilidades. Estas pueden resultar afectadas por fallas en la disponibilidad, confidencialidad y la integridad de la información. Y, el papel de la seguridad de la información es protegerlas.

La seguridad debe definir su matriz de FCI (factores críticos de éxito) y exponerlos a las directivas dentro de un panorama y escenario de acciones tendientes a mitigar el riesgo.

RS: ¿Cuáles serían sus recomendaciones para hacer de la seguridad de la información un tema de las Juntas Directivas en las organizaciones?

CZ: En el proceso de CONCIENZAR se deben presentar ante la Junta directiva las estrategias y la planeación de seguridad de la información anual, que contemplen los lineamientos del modelo con la estrategia del negocio y los valores que aportan. Es importante que exista un comité de seguridad de la información no liderado por los profesionales del área, sino por la presidencia de la organización.

Javier Díaz Evans
Director de Seguridad
de la Información
ATH S.A.
jdiaz@ath.com.co

Revista Sistemas: Es claro que la seguridad de la información sigue escalando posiciones importantes en las organizaciones, sin embargo, ¿cuáles consideran ustedes en su práctica que son los drivers (orientadores) se deben considerar para profundizar y fortalecer este tema y sus prácticas asociadas?

Javier Díaz Evans: El ROL de oficial de seguridad de la información se fortalece de acuerdo con la sensibilización del CEO de la organización; si la cabeza de la organización ha tenido una interiorización de lo estratégico de la seguridad, se definirá el rol de CIO o CISO dentro de las organizaciones. Si la persona no tiene una experiencia importante, el rol de oficial será netamente operativo y estará bajo la responsabilidad del área de TI.

Los expertos en seguridad y responsables del tema en las organizaciones y consultores debemos garantizar que nuestra función esté soportada en un gobierno claramente definido, con el fin de:

• Orientar los objetivos de seguridad en la consecución de objetivos de la organización.

• Orientar la seguridad a una gestión de riesgos.

• Establecer recomendaciones y proyectos costo-beneficios para la organización.

• Proveer información consolidada y efectiva para la toma de decisiones.

• Mitigar el impacto de los incidentes.

• Desarrollar un modelo de inteligencia en seguridad que garantice una identificación, reacción y respuesta oportuna a los nuevos riesgos que afectan a la organización.

RS: ¿En qué no se puede equivocar un CISO para tener éxito en su gestión de seguridad de la información?

JDE: Las grandes equivocaciones se soportan no en las actividades realizadas por el CISO, sino por aquellas que deja de hacer. Las grandes equivocaciones se resumen en:

• Establecer controles, sin analizar la relación Costo-Beneficio.

• No identificar los riesgos.

• No responsabilizar al dueño de la información de los riesgos identificados.

• No establecer modelos de decisión, donde se definan claramente los roles y responsabilidades de cada integrante del modelo.

• No proveer alternativas de solución.

• No orientarse a la estrategia sino a la operación.

• No unificar los diferentes controles en un único modelo (ISO 27001, CobIT, CE 052, CE 038, PCI, etc.).

• No establecer objetivos de seguridad.

• No alinear los objetivos de seguridad con los objetivos del negocio.

• No incluir a las personas dentro del modelo de gestión de seguridad.

• Seguir instalando FW, IDS, Antivirus, IPS, sin soportarlo en algún riesgo específico.

• No medir.

• No aprender de los incidentes de seguridad.

• No registrar las actividades realizadas.

• No establecer contacto con grupos de expertos.

• No compartir sus experiencias.

RS: ¿Cuáles son los riesgos emergentes que usted observa en la seguridad de la información en las empresas del país? ¿Cuál debería ser la prioridad para enfrentarlos y porqué?

JDE: Los riesgos de seguridad siguen siendo los mismos desde hace varios años, estos sólo cambian evolucionando de acuerdo con las nuevas formas de transmisión, resguardo y procesamiento de la información.

La prioridad de las empresas debe ser primero lograr identificarlos. Este monitoreo de los riesgos de seguridad se soporta en la identificación de las fuentes de evidencia y del registro de eventos, sumado a una herramienta de correlación y de directivas de negocio, para identificar aquellas que impactan a la organización. Posteriormente, el área de seguridad debe garantizar una investigación efectiva que garantice la identificación de las fallas que tiene el modelo de seguridad. El mapa de riesgos más completo ha sido desarrollado por el ISF.

RS: ¿Considera usted que la seguridad de la información es un tema de negocio? ¿Qué debería hacer la función de seguridad de la información para que esto se manifieste como tal? ¿Qué limitaciones observa para que esto se dé?

JDE: Si la seguridad de la información no es un tema de negocio, nunca será estratégico para las organizaciones. El área de seguridad debe apalancar el cumplimiento de algunos de los objetivos definidos por la organización, un área de seguridad madura y desarrollada puede no sólo cumplir con las premisas de seguridad: confidencialidad, integridad y disponibilidad, sino incluir algunas características de la información, claves para el negocio, como son la efectividad, eficiencia y cumplimiento, entre otros.

La limitación de tener un área de seguridad orientada al negocio está en los líderes que soportan el área dentro de la organización.

RS: ¿Cuáles serían sus recomendaciones para hacer de la seguridad de la información un tema de las Juntas Directivas de las organizaciones?

JDE: La seguridad debe establecer objetivos que apalanquen el negocio. Estos objetivos deben ser medidos a través de métricas claramente definidas. La seguridad no puede seguir siendo presentada con resultados operativos o técnicos únicamente; esta debe ser presentada como el ahorro de dinero, la mitigación de riesgos, reducción de impactos y pérdidas. La junta directiva estará siempre atenta a los resultados de seguridad, si ayudan a suplir sus necesidades o a cumplir con sus objetivos.

Francisco Pacheco Alfonso
Director de Seguridad de la Información - Deceval
fpacheco@deceval.com.co
pachecoseguro@gmail.com.co

RS: Es claro que la seguridad de la información sigue escalando posiciones importantes en las organizaciones, sin embargo, ¿cuáles consideran ustedes en

su práctica que son los drivers (orientadores) se deben considerar para profundizar y fortalecer este tema y sus prácticas asociadas?

Francisco Pacheco Alfonso: Indudablemente establecer el comité de seguridad. Este es un órgano rector y orientador de las actividades que asuma la organización. Y, por encima y a través de este comité, la alta Gerencia está enterada en forma permanente. Otra condición especial es mantenerse informado sobre las diferentes debilidades o fortalezas de la infraestructura tecnológica, adoptadas por la organización. Para ello es vital ser responsable del inventario, clasificación y asignación de los responsables de los activos de información. El área de seguridad de la información debe ser partícipe en el perfeccionamiento de los contratos relacionados con IT. Así mismo, debe tener injerencia directa en la determinación y establecimiento de los roles y perfiles de los sistemas funcionales, además de los controles de seguridad que cobijarán a estos sistemas.

RS: ¿En qué no se puede equivocar un CISO para tener éxito en su gestión de seguridad de la información?

FPA: En saber reportar éxitos y fracasos a la alta dirección, pero específicamente comunicar y celebrar los primeros.

RS: ¿Cuáles son los riesgos emergentes que usted observa en la seguridad de la información en las empresas del país? ¿Cuál debería ser la prioridad para enfrentarlos y porqué?

FPA: Como los riesgos potenciales que vienen del exterior se han minimizado notablemente, los riesgos de hoy están adentro, los militares lo llaman la "Corrupción de las Filas". Para mí, la prioridad es el que al área de seguridad de la información se le permita tener injerencia en los procesos de contratación del recurso humano, en su capacitación y conciencia permanentes sobre tales asuntos. Las funciones de seguridad de la información deben ser detalladas para cada uno de los cargos en la organización.

RS: ¿Considera usted que la seguridad de la información es un tema de negocio? ¿Qué debería hacer la función de seguridad de la información para que esto se manifieste como tal? ¿Qué limitaciones observa para que esto se dé?

FPA: Si es un tema de negocio, debe ejecutarse lo descrito en el punto 3. Las limitaciones suministran la falsa creencia de que se trata de un tema prioritario sólo para empresas del sector financiero. Otra condición es subestimar el valor de los activos de la información.

RS: ¿Cuáles serían sus recomendaciones para hacer de la seguridad de la información un tema de las Juntas Directivas de las organizaciones?

FPA: Que el comité de seguridad de la información tenga un espacio para reportar.

Andrés Ricardo Almanza Junco
Coordinador de la seguridad de la información
Cámara de Comercio de Bogotá
andres_almanza@hotmail.com

RS: Es claro que la seguridad de la información sigue escalando posiciones importantes en las organizaciones, sin embargo, ¿cuáles consideran ustedes en su práctica que son los drivers (orientadores) se deben considerar para profundizar y fortalecer este tema y sus prácticas asociadas?

Andrés R. Almanza J.: Desde la perspectiva corporativa creo que son los siguientes orientadores:

Una estrategia clara dentro de la organización, que determine el rumbo de la seguridad, con unos compromisos de corto, mediano y largo plazo, encaminados a mostrar la ejecución de cualquier programa, alrededor de la seguridad de la información. Creo que esta estrategia debe resolver inquietudes tales como:

• ¿Por qué la necesidad de la seguridad dentro de la organización?

• ¿Por qué resuelve mis problemas de seguridad de la información?

Una estrategia clara debe integrar a las personas. Dentro de este conjunto de implicados estarán usuarios, entes externos y clientes. En este nivel es necesario afrontar la responsabilidad que cada uno tiene.

La estrategia debe contemplar claridad sobre cuáles son los riesgos y amenazas a los que la información se expone. Es por ello que, a través de una estrategia, se define cómo la organización debe afrontar las situaciones de difícil control.

Una estrategia debe enlazar las preguntas y sus componentes, a través de unas directrices claras (políticas), para que sean el marco de referencia que apunte a contestar las preguntas propuestas.

Una clara estrategia debe tener como uno de sus atributos la personalización de la seguridad, orientada a la necesidad de toda la organización, en el sentido de acomodar cualquier modelo y arquitectura de seguridad, a sus necesidades.

Un segundo orientador para resolver los problemas de seguridad debe planear, diseñar y establecer lo que la organización necesita, en términos de seguridad de la información; definir las responsabilidades de quienes responden por la seguridad. La planeación de proyectos en seguridad de la información sería un componente de gran importancia y un gran orientador en la búsqueda del desarrollo adecuado y sostenible. Las siguientes son algunas de las preguntas por responder:

¿Qué tipos de firewall necesitamos?

¿Qué tipo de protección de perímetro necesitamos?

¿Qué tipo de segmentación de redes?

¿Una DMZ, una red privada, una red pública?

Un tercer orientador es el soporte tecnológico que nos puede ayudar para determinar cómo resolver de manera clara, nuestros problemas de seguridad dentro de la organización. Como orientador de todo esto está el mantenimiento; no basta con montarlo,

sino revisar y actualizar, considerando que en la estrategia se ha escogido personalizar la seguridad. La organización cambia y la tecnología también. El cuarto orientador es el monitoreo, para vigilar que la estrategia se cumpla y que la tecnología sirva a los propósitos determinados. Este orientador marca la importancia de todo lo realizado dentro de la organización.

RS: ¿En qué no se puede equivocar un CISO para tener éxito en su gestión de seguridad de la información?

ARAJ: Pienso que no se debe equivocar en los siguientes elementos:

• Comunicación asertiva con los niveles superiores, para poder tener de ellos un apoyo claro, considerando los impactos que sus planes producen dentro de la organización.

• La finalización y cierre de los proyectos es la labor que sostiene su trabajo.

• El monitoreo y seguimiento no permiten equivocaciones, se trata de una tarea que en cualquier nivel, estratégico, táctico u operacional se debe realizar. Es indispensable en el mejoramiento de un proceso.

• No se debe equivocar en el entrenamiento y la conciencia en seguridad; crear esa cultura es una labor dispendiosa que requiere disciplina, esfuerzo y mucho trabajo. No permite equivocaciones y contempla entrenar y reentrenar a los usuarios.

• Es importante no exceder las expectativas de sus clientes, no debe prometer cosas que no puede cumplir.

RS: ¿Cuáles son los riesgos emergentes que usted observa en la seguridad de la información en las empresas del país? ¿Cuál debería ser la prioridad para enfrentarlos y porqué?

ARAJ: Dentro del conjunto de retos están:

• Las tecnologías móviles; debemos prepararnos para aceptar que estas tecnologías en el futuro cercano, serán una herramienta de trabajo y, por lo tanto, debemos preocuparnos por proteger que la información expuesta en los servicios soportados en esas tecnologías.

• Las redes sociales; corporativamente hablando, muchas organizaciones dentro de sus estrategias de marketing han considerado la posibilidad de proveer servicios, a través de este tipo de tecnologías, por lo tanto es indispensable diseñar una estrategia para disminuir la probabilidad de que un mecanismo que no está bajo control, utilice nuestra información.

• Tecnologías de WebServices; estamos volcados a nivel corporativo a la integración de nuestros servicios y la tecnología que nos ayuda en ese sentido está basada en WebServices. Debemos ser conscientes de que las aplicaciones soportadas en tales tecnologías no poseen mecanismos adecuados de protección.

• El cloud computing, está dando mucho de qué hablar y se está convirtiendo en una forma nueva de prestar los servicios, facilitando a las empresas no pensar en la forma y la razón de cómo invertir en tecnologías que le ayuden a proteger la información, dentro de unos parámetros de confiabilidad, por parte de la organización.

• Combatir el fraude electrónico a nivel corporativo va a ser muy importante. Estamos en la era de la información, rodeados del poder que ésta representa y es necesario protegerla a toda costa.

RS: ¿Considera usted que la seguridad de la información es un tema de negocio? ¿Qué debería hacer la función de seguridad de la información para que esto se manifieste como tal? ¿Qué limitaciones observa para que esto se dé?

ARAJ: Toda organización debe entender cuál es el propósito de la seguridad de la información. Mucho más si los objetivos de negocio giran en torno a una cadena de valor, porque ésta se convierte en un servicio de la compañía para la compañía. Es necesario entender que para que un servicio de negocio cumpla con unos niveles adecuados de inseguridad, se debe descomponer en todos sus componentes y validar para cada uno de ellos la necesidad de protección requerida.

RS: ¿Cuáles serían sus recomendaciones para hacer de la seguridad de la información un tema de las Juntas Directivas de las organizaciones?

ARAJ: Mostrar la necesidad de proveer servicios más confiables para los usuarios, no generando paranoias ni malos mensajes alrededor de los ataques, a los que puede verse expuesta una organización.

Proveer necesidad frente a la gobernabilidad de la información y qué componente importante contempla su seguridad.

Mostrar resultados medibles que reflejen la realidad de algo intangible, como la seguridad de la información. Las regulaciones en muchos casos son palancas importantes, para que las juntas directivas hablen del tema.

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas Uno y Cero, Gestión Gerencial y Acuc Noticias. Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Corresponsal de la revista Infochannel de México. Así mismo, ha sido corresponsal en Colombia de los diarios "La Prensa" de Panamá, "La Prensa Gráfica de El Salvador, de la revista IN de Lanchile. Autora del libro "Lo que cuesta el abuso del poder". Investigadora en publicaciones culturales. ex Ministra de La Palabra (gerente de comunicaciones y servicio al comensal) en Andrés Carne de Res.*