Convergencia de la seguridad

Andrés Ricardo Almanza Junco Ms(c)

En la actualidad, han surgido nuevas tecnologías de protección como resultado del incremento no predecible de las amenazas y su mayor complejidad. Cada vez más, es necesario mezclar tales alternativas en la organización.

Las organizaciones de hoy buscan incrementar a toda costa su productividad y de la forma más eficientemente posible, los recursos disponibles, de tal manera que sus productos y/o servicios sean ofrecidos de la mejor manera. En este sentido es que la seguridad y la protección de la información han visto la necesidad de evolucionar, de ver más allá, de buscar una manera integral para garantizar su protección.

Este escenario cambiante y dinámico de la inseguridad de la información ha direccionado los esfuerzos de la organización a entender que la protección de la información debe contemplar un contexto completo, ver cómo la información circula a través de empresa y cómo se deben implementar las respectivas medidas de protección, sin discriminar el ambiente del que se esté hablando.

Por la misma evolución de la seguridad y la protección de la información, que ha venido desarrollándose, ya no sólo se ve a la inseguridad como un camino que integra procesos, gente y tecnología, sino que ahora se integra con otros elementos propios de protección, respondiendo a la necesidad de ver a la inseguridad de manera total alrededor de la información, donde inclusive el riesgo que se ha vuelto un elemento estratégico para el desarrollo natural de la organización, ahora se puede ver por su evolución natural como un riesgo de valor corporativo y así como la seguridad se ve como un elemento transversal a la organización, y no de manera individual por cada unidad de negocio por donde circula información.

Este nuevo panorama hace que se requieran mayores esfuerzos dentro de la organización por el cumplimiento de un programa estructurado, con una forma y un contenido, buscando cumplir 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 llevar a acabo la ardua labor de orquestar el panorama desmedido de inseguridad, al que la organización se ve expuesto, en su constante crecimiento.

Convergencia

Convergencia es un término que ha existido desde los años 70, y al que se le han atribuido muchas definiciones y diferentes connotaciones.

Al momento de revisar la definición de convergencia encontramos lo siguiente. Según diccionarios *online* se define la convergencia como "… Unión de dos o mas cosas que confluyen en un mismo punto..."

Según la Real Academia de la Lengua. "Acción y efecto de convergir" y en los términos matemáticos se entiende por convergencia, cuando una sucesión de número tiene un limite definido.

Al analizar la definición se nota que se está hablando de que las tendencias se unen o se encuentran en algún punto del tiempo y del espacio, de tal manera que conjuran sus esfuerzos en pro de algo; que si bien al principio no poseen características similares, tienden a entrelazarse por la misma naturaleza de la situación o porque encuentran que sus esfuerzos mancomunados los llevan al mismo objetivo.

Cuando se habla de convergencia de la seguridad, se hace referencia a un todo como un elemento que integra las visuales de seguridad, desde todos sus puntos de vista. Se trata de ver los servicios de seguridad no operando de manera independiente; por un lado la seguridad física y por otro la seguridad lógica, como un primer enfoque. Es ir más allá, para presentar la seguridad como un todo, un elemento universal, un elemento único que contempla todas las aristas posibles, en pro de un propósito: proteger un servicio de negocio.

Hablando puramente de seguridad, la convergencia en términos de compartir, cooperar, colaborar parte de un propósito, la defensa; por lo tanto, es posible definirla como todos aquellos esfuerzos mancomunados de seguri-

dad de las organizaciones, para compartir el propósito de "la defensa" y todo lo que a ella le corresponda.

Desafíos actuales

En la actualidad las organizaciones presentan algunos panoramas de crecimiento en torno a su avance sobre el tema de protección frente a sus amenazas; es por ello que las empresas tienen la seguridad cubierta a través de sus diferentes áreas, en lo que se refiere a la seguridad física. Es decir, las medidas que buscan proteger a las personas, las infraestructuras físicas, y demás elementos tangibles.

Por otro lado, encontramos la seguridad lógica, como aquel conjunto de medidas que buscan proteger sistemas de información, redes de comunicaciones; en definitiva, todas las medidas enfocadas a la protección de los activos de información que se soporten de alguna manera, en una medida tecnológica.

Desde otra arista encontramos los que se preocupan por la continuidad del negocio, como un conjunto de medidas que ayudan a la organización en pro de saber cómo responder ante una eventual catástrofe.

De igual manera, encontramos otro grupo que se preocupa por cosas menos tangibles, como los temas de propiedad intelectual o el cumplimiento ante algún tipo de regulación, norma o ley que exista y no llegar a incumplir. Y, por último y no menos importante, los que se encargan de planear en las organizaciones la gestión del riesgo, unidades en muchos casos aisladas que ven el riesgo desde cada una de las perspectivas posibles.

En este panorama normal y actual se nota una realidad, un esfuerzo orientado a proteger la información de la organización, pero con algún reto importante, el esfuerzo mancomunado. Por lo tanto, si se aplicara la definición anteriormente expuesta de convergencia en seguridad, se tendría un esfuerzo común desde las distintas áreas de la empresa, que busca proteger los activos de la mejor manera posible, evitando que las amenazas de cualquier índole se puedan presentar, sin importar su razón, índole, origen, característica, o tipo. En este orden de ideas podría decirse que la seguridad es una cadena, en donde se ve de forma lineal la implementación de los mecanismos de protección necesarios para proteger el proceso o servicio de negocio que atravesará de manera transversal la compañía.

El marco de la convergencia en seguridad no pretende que se unan departamentos porque si, sin un fin, sin un propósito.

Tampoco buscan que unos empleados de la organización adquieran un nuevo rol; por ejemplo, que los ingenieros se conviertan en vigilantes y salgan de sus oficinas a ofrecer servicios de tal naturaleza. De ahí que el término divergencia, también está involucrado dentro de la convergencia, puesto que su trabajo es recolectar esfuerzos teniendo para la organización, propósitos diferentes como roles o responsabilidades, pero enfocadas en un claro objetivo: proteger y brindar apoyo a los servicios de negocio de la organización.

Razones para converger

Existirán muchas razones por las que se pueda definir la convergencia; es más, para muchos podrán existir razones totalmente diferentes. Al realizar las revisiones de los distintos grupos de estudio, encontramos las siguientes razones para que la convergencia se de por motivos organizacionales.

• **Crecimiento corporativo:** En la actualidad las organizaciones son más complejas, existen más interdependencias entre las mismas áreas. A esto se suma la interrelación fortalecida con los terceros y sus clientes. Cada vez más se pierde la diferencia entre proveedores, clientes y organización; se entremezclan por la misma complejidad de los negocios y los servicios ofrecidos, razón por la cual se requiere de un esfuerzo para integrar la mayor cantidad de estos ambientes. Es necesario construir entre todos los involucrados unas relaciones ampliamente confiables, para garantizar que sus operaciones se realicen de tal forma que se basen en la confianza para poder ejecutar de manera íntegra la operación o conjunto de operaciones que se están estableciendo entre las partes interesadas.

• **Transformación de los activos:** En las décadas anteriores, las organizaciones se han preocupado por proteger sus activos físicos, de tal manera que se han venido implementando controles para ello. En la actualidad se ve una realidad totalmente diferente, cada vez más y como premisa se repite que los activos de la información, así como los intangibles están tomando mayor fuerza, lo que motiva esfuerzos importantes encaminados a su protección. Temas como la compu-

tación forense y la misma seguridad de la información, muestran cómo emerge la importancia de proteger la información y para muchos casos los sistemas y tecnología que la respalda, eso sin dejar de lado la protección física de los mismos, que hace que se requieran esfuerzos en integrar los sistemas. Esto si bien presenta grandes retos referentes a la forma en cómo debe ser abordados los riesgos y con ellos la forma en como debe minuciosamente ser visto el problema, también muestra un panorama para abordar los problemas identificados y con ellos definir la forma en como deben ser tratados de una forma consistente con los objetivos del negocio.

• **Límites de protección:** Se plantea esta como una de las razones importantes para pensar en la integración de los diferentes sistemas de protección a trabajar en conjunto, de tal forma que se logre en primera instancia la protección y como segundo propósito, ahorros significativos en las inversiones de TI que la organización pueda llevar a acabo en esa dirección.

• **Regulaciones y Cumplimiento:** Cada vez es más notorio ver cómo las regulaciones, sean del país o de carácter internacional, aplican a cada una de las organizaciones de hoy, sin importar su distribución y localización geográfica. En muchos casos se hace más complejo seguir este cumplimiento de manera independiente, de acuerdo a quién le corresponda dentro de la organización, haciendo necesario ver desde dónde se puede tener el control del cumplimiento. Así mismo, se debe tratar de garantizar el gobierno, a través de un claro cumplimiento de las normas, leyes, reglas y/o regulaciones que existan

• **Reducción de costos:** Las organizaciones con mayor apuro y precisión, sin distorsionar su realidad, se reinventan para manejar de manera eficiente los recursos existentes, sobre los temas corporativos. Dentro de ellos el manejo de riesgos y las inversiones en TI, de tal forma que realizando inversiones adecuadas y acordes con las necesidades de la organización, se pueda lograr un ambiente de confianza razonable que refleje niveles adecuados, en términos de la inseguridad corporativa.

Enfoques de convergencia

La convergencia de seguridad de la información, puede darse de distintas formas, según la siguiente perspectiva: a nivel tecnológico, a nivel de estructuras corporativas, y, a nivel de organización y su visión de negocios.

El primer enfoque se relaciona con una convergencia entre la seguridad física y la seguridad lógica; y se presenta porque las amenazas de nuestro

tiempo son cada vez más complejas y buscan afectar la información sin importar las formas en como esta se pueda manifestar. Hoy vemos amenazas que van desde dispositivos móviles, hasta malware y amenazas que se manifiestan en los cajeros electrónicos. Desde esa perspectiva se plantea la convergencia de primer nivel, donde los sistemas de seguridad física han dejado de ser máquinas aisladas e independientes que son en primera medida sistemas IP-enable, y posterior a ello sistemas totalmente integrados con las redes convencionales.

En este escenario vemos que la convergencia es en ambas vías. Cada vez es más común observar cómo los proveedores de seguridad electrónica integran dentro de sus sistemas componentes de información y tecnología (bases de datos, soporte de redes inalámbricas, reportes, métodos de procesamiento de información, entre otros). Particularmente se ve en soluciones tales como las de control de acceso físico, en temas de reporteadores, así como en los sistemas de vigilancia soportados en repositorios como bases de datos para almacenar la información.

Así mismo, encontramos con más frecuencia las tecnologías de información y sobre todo, los conceptos que ellas encierran, las cuales recurren a los soportes de la seguridad física. Principalmente, podríamos decir que encontramos esta situación en cuatro grandes conceptos. 1) Gestión de Identidad (Identity Managment), donde lo que se busca es tener la identidad de una persona a través de todos sus ambientes físico y lógicos, inclusive en algunos casos y con algunas soluciones encontramos su registro visual a través de cámaras IP. 2) Control de acceso, en este tipo de soluciones es común ver que se controla a través de medios físicos y las formas como se tiene acceso a la información soportada en medios digitales; como por ejemplo, los sistemas de biometría, junto con temas como Smart Card. 3) Gestión de usuarios, son soluciones que buscan definir los niveles de autorización de los usuarios en ambos ambientes tanto físico como lógico. 4) Monitoreo, tal vez uno de los más desarrollados hasta el momento, sin suponer que los otros no lo estén; en este tipo de soluciones se busca la centralización, correlación y seguimiento de todos los posibles eventos que se puedan presentar en ambos mundos. Vemos cómo han emergido los conceptos de SIEM, para dar vida a sistemas de información que se encargan de poder monitorear los eventos de seguridad previamente definidos y con ello hacer un seguimiento y monitoreo, desde un solo punto de recolección o través de diferentes puntos, pero todos reportados a un único repositorio, donde existen los algoritmos de co-

rrelación con los cuales se muestran los resultados en una única consola.

El segundo nivel nos habla de la convergencia de las estructuras organizacionales y más exactamente sobre los roles de quien se encarga de esta función. En este nivel se trata de ver cómo la organización asigna un responsable de los temas de convergencia, con la capacidad de ver el negocio como tal para entender sus funciones orientadas a la protección de la información, como un objetivo estratégico de la organización.

Lo importante que no debe perderse de vista sin importar el tipo de organización, es que dentro de sus competencias debe estar la visión holística (negocio, tecnología, seguridad). Este rol se ha denominado CSO (Chief Security Officer), un nuevo rol que en muchos casos difiere del CISO por el enfoque que manejan, mientras que el CISO está orientado a trabajar la información y la tecnología como componentes principales el CSO; es un poco más global porque ve temas como: 1) Desarrollo de una estrategia corporativa de seguridad, para mostrar la necesidad a los niveles directivos la necesidad de la protección ante cualquier evento. 2) Gobierno de Riesgo y Cumplimiento (GRC), donde ve el riesgo como lo que es, una amenaza que puede presentarse desde cualquier escenario. 3) Prevención Corporativa, donde debe ocuparse de preparar a la organización a través de los diferentes planes frente a las amenazas. 4) Aseguramiento intangible, en este tópico debe velar por otros tipos de protecciones y su integración con otros escenarios, protección de recurso humano, protección del core de negocio, la reputación. 4) GRI, refiriéndose a que debe ser quien coordine los esfuerzos necesarios para realizar la gestión, respuesta y recuperación ante un incidente. 5) Cumplimiento, en este tópico debe tener claro que es el responsable por visualizar las posibles afectaciones que puedan generar las normativas, regulaciones, normas, leyes y demás que puedan estar cobijando a la organización, de igual manera debe estar presto para ver el panorama de las buenas practicas del mercado en temas de protección de los activos de la organización y ver como de acuerdo a un plan detallado, ordenado y estructurado se pueden llevar a cabo. 6) Integrador, esto es más una cualidad y habilidad, tener la capacidad de integrar esfuerzos de muchos frentes, estar preparado para que muchos puedan rechazar sus ideas, opiniones y planes.

En la última visión de nivel corporativo, se tiene en cuenta el riesgo como un componente totalmente global; es decir, no detenerse a ver el riesgo desde una sola óptica, como elementos que afectan a la organización, a través de la prestación de sus servicios. En este nivel lo que se busca a través de la visión integral de los riesgos es propender por poseer un buen gobier-

no alrededor del tema de la seguridad de la información, buscar observar, analizar, y seguir los planes propuestos; busca concertar los esfuerzos que el CSO debe realizar para integrar su propósito cumplir con el deber de proteger, de las amenazas que se puedan materializar al respecto.

En este aspecto es importante que se pase de una visual que ve a la gestión de activos independientes y no relacionados, donde cada esfuerzo de gestión de riesgo se concentra de acuerdo con el grado de especialidad (riesgo financiero, de operación, de tecnología, etc.), a un escenario donde se identifique el riesgo sin importar el área funcional que afecte; por lo tanto, la integración de esfuerzos es válida para lograr poder coordinar los esfuerzos, en pro de una sola visual de riesgo.

En este mismo concepto se podría decir que nuestra definición de convergencia de la seguridad cambia, evoluciona en donde podría decirse que la convergencia de seguridad serían todos los esfuerzos mancomunados que buscan identificar todos aquellos riesgos que afectan a los activos y la interdependencia que estos tienen dentro de la función de negocio, y/o proceso, con el propósito de poder controlar dichos riesgos que puedan llegar a afectar a la organización. Este nivel reta al responsable a hacer visible el gobierno a través de todas sus acciones, debe propender por la proactividad del gobierno de seguridad de la información. Es de vital importancia que el responsable, en este nivel plantee un modelo de madurez al respecto de la gestión y gobierno de riesgo, basado en las prácticas de la industria, alineándolo con las necesidades de la empresa.

Conclusiones

La convergencia es un nuevo panorama que muestra una realidad, que se puede leer como una tendencia que vendrá o existe en la actualidad, pero que en el futuro cercano podría llegar a convertirse en una consideración y recomendación para muchos tipos de organizaciones.

Es necesario que cada organización de sus pasos en el tema, sin dejarse presionar por factores externos; lo importante podría ser reconocer su estado y si de alguna manera es beneficioso llegar a una convergencia total, proceso, tecnología y gente como marco de trabajo.

Existen en la actualidad algunos Framework de trabajo para adaptarse a los modelos de convergencia; lo esencial de todos ellos es tener clara la visión de negocio como elemento importante, de tal manera que pueda apalancar los procesos de cambio que requiera la organización al acercarse a cualquier modelo.

Es necesario que el líder o responsable de una visión corporativa de seguridad cambie su posición de una postura funcional y experta, a una persona con visión de negocio, que vea de manera transversal la información y en ella lo que puede afectar de manera integral a la misma.

La colaboración, trabajo en equipo y esfuerzo conjunto serán piezas claves, de tal forma que se pueda trabajar en pro de un propósito corporativo común, "objetivo estratégico".

Es posible que las organizaciones definan un modelo de madurez, para poder cubrir los escenarios propuestos de convergencia presentados, una convergencia a TI, como un primer nivel que nos permite tener una visión de riesgos de TI unificada entre lo físico y lo lógico, después reordenar la responsabilidades, y competencias del responsable de este rol; y, por último, una visión global del riesgo, en donde desde un punto unificado y con los recursos y esfuerzos adecuados se pueda gestionar y gobernar los riesgos de la organización, teniendo en cuenta la visión del negocio y no las áreas funcionales.

Referencias

[1] ASIS:
"Convergence of Enterprise Security Organizations"
ASIS ISSA ISACA, November 2005
www.asisonline.org/newsroom/alliance.pdf
[2] USBX:
Convergence and the Security Industry
www.usbx.com/industries/security/Advance Convergence in Security.pdf
[3] ASIS:
"The Convergence of Phisical and Information Security in the Context of Enterprise Risk Management"
[3] ASIS, DELOITE 2005.
www.isaca.org/ContentManagment/ContenDisplay.cfm?ContentID=43023
[4] CSO Fundamentals: Phisical and IT Security Convergence: The Basics. CSO Magazine 2005.
[5] Chief Security Office (CSO) Guideline. ASIS International, 2008.
[6] Wylder J. (2004) Strategic Information Security. Addison Wesley.
[7] Contos B., Crowell W., DeRodeff C., Dunkel D. (2007) n. Phisical and Logical Security Convergence

Andrés Ricardo Almanza Junco Ms(c). *Ingeniero de Sistemas de la Universidad de Católica de Colombia, graduado de la Especialización de Seguridad en Redes de la Universidad Católica de Colombia; Master en Seguridad de la Información de la Universidad Oberta de Cataluña. Se ha desempeñado como profesor de postgrados de la Universidad Pontificia Bolivariana en el área de la seguridad en redes, y sistemas de detección de intrusiones, de igual manera se desempeña como docente de postgrado de la Universidad Rosario de Colombia, en el área de seguridad en redes, así como de la Universidad Externado de Colombia en el área de Fraude Electrónico. Es miembro de la Red Iberoamericana de Cristología y Seguridad de la Información – CriptoRED (http: //www.criptored.upm.es). Se desempeña actualmente como Jefe de Seguridad y Administración de la Información de la Cámara de Comercio de Bogotá.*