Feature

Jeimy J. Cano M., Ph.D, CFE, es miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho y Profesor Distinguido en la Universidad de los Andes. Colombia. El profesor Cano se puede contactar en: *jjcano@yahoo.com.*

La función de seguridad de la información. Presiones actuales y emergentes desde la inseguridad de la información

Las tendencias internacionales manifiestan un cambio paradigmático en los modelos de negocios actuales, motivados por la dinámica y asimetría de los mercados, donde la inestabilidad es la constante y el cambio la norma. En este sentido, se advierten nuevas declaraciones empresariales estratégicas que cambian la forma de pensar en las organizaciones y ocasionan un quiebre en los supuestos fundamentales de su operación (**figura 1**).[1, 2]

Revisando las declaraciones actuales y las nuevas, vemos que las primeras están asociadas con un juego de consolidación de estrategias formalmente diseñadas, que posiblemente no evolucionan con el tiempo y su entorno, y que permanecen aún cuando su contexto dé muestras de cambios radicales e inesperados que están fuera de su capacidad de anticipación.

Las segundas son sensibles a las fluctuaciones del entorno y siguen una tendencia basada en las motivaciones y expectativas de las personas, lo cual supone una capacidad de gestión de la información, para desarrollar y capturar fuentes de valor novedosas y estacionales, las cuales son aprovechadas para tomar control de territorios emergentes y superar a sus competidores, no necesariamente en su campo de especialidad, sino allí donde las posibilidades están y hacen la diferencia.[3]

Also available in English
www.isaca.org/currentissue

Esta realidad de los negocios representa un reto de creatividad, velocidad, flexibilidad y colaboración radical para las empresas, pues no son ahora los equipos de profesionales especializados los que tienen las respuestas para hacer los pronósticos sobre las tendencias emergentes, sino la capacidad corporativa para crear esquemas de comunidad con los clientes y demás personas, para construir y desarrollar capacidades que cambien la experiencia de los clientes, apalancados en el significado y valor de los contenidos y nuevas posibilidades.

Así las cosas, las empresas que deseen permanecer en las turbulentas aguas de los cambios inesperados y retos emergentes, deberán contar con una manera distintiva de proveer valor frente a las expectativas de las personas, desarrollar capacidades exclusivas de actuación (cosas que saben hacer muy bien, que sus clientes le reconocen y los otros no pueden imitar) y mantener un ejercicio de coherencia y armonía entre las dos, con el fin de competir usando diferentes aproximaciones en múltiples categorías y mercados.[4]

Figura 1—Cambios en los modelos de negocio

Declaraciones Actuales	Declaraciones Nuevas
Desarrollo y aprovechamiento de estrategias competitivas sostenibles	Desarrollo, aprovechamiento y abandono de estrategias competitivas transitorias
Diseño de productos basado en necesidades	Diseño centrado en las personas
Desarrollo de una cultura informática a nivel organizacional	Desarrollo de una cultura digital empresarial
Desarrollo de estrategias por públicos objetivos	Desarrollo de un ecosistema de contenidos y posibilidades
Desarrollar ona posición privilegiada en su sector de negocio respecto de otros	Capturar la mayor cantidad de territorio que logre superar a los otros

Adaptado de: Gunther McGrath, R.; *The End of Competitive Advantage: How to Keep Your Strategy Moving as Fast as Your Business*, Harvard Business Review Press, 2013. Leinwand, P.; C. Mainardi; "What Drives a Company's Success? Highlights of Survey Findings," Booz & Company, 2013, *www.strategyand.pwc.com/global/home/what-we-think/reports-white-papers/article-display/what-drives-a-companys-success*

Si lo anterior es correcto, el concepto de la información clave para la empresa se enfrenta a una realidad contraria a la doctrina actual de protección de la misma, donde se entiende la gestión de este activo como residente en sitios conocidos, procesado en máquinas identificadas y accedido por personal autorizado y confiable.

Esta nueva realidad de negocios supone un mayor nivel de exposición, colaboración, entrega, intercambio y flujo de información, lo cual demanda repensar los esquemas actuales de seguridad y control, fundados en reglas y procedimientos ajustados a una entorno tranquilo y predecible, por unos que reconozcan la dinámica de la gestión de la información, las necesidades y expectativas de los clientes generalmente asociadas con movilidad, acceso y capacidad para compartir.

CAMBIO DE ENFOQUE: DE LA RESTRICCIÓN A LA FACILITACIÓN

En este nuevo contexto de los negocios y la avalancha de nuevas posibilidades tecnológicas, la seguridad de la información debe evolucionar para ajustarse a los retos que le impone la dinámica empresarial y la necesidad permanente de generar nuevas ventajas competitivas. Salir de la zona cómoda conocida de sus controles tradicionales y renovar el entendimiento de la protección de la información en una realidad abierta, móvil, con terceros y eminentemente social.

En este sentido, la transformación que se advierte en la gestión y gerencia de la seguridad de la información supone entender su modelo vigente y movilizarse hacia uno evolutivo acorde con los desafíos que impone la sociedad actual (**figura 2**).[5]

Figura 2—Modelo actual y evolutivo de la seguridad de la información

Modelo actual de la seguridad de la información	Modelo evolutivo de la seguridad de la información
Basado en mitigación del riesgo (reducción de riesgo)	Basado en gestión del riesgo (aceptación de umbral de riesgo)
Orientado a los activos de información críticos	Orientado al funcionamiento confiable de procesos críticos
Fundado en el aseguramiento del perímetro tecnológico definido	Fundado en el cambio de comportamiento de las personas frente a la información
Basado en procedimientos y guías de seguridad y control	Basado en reglas y acuerdos de uso fundados en los impactos
Soportado en acciones preventivas y sancionatorias	Soportado en acciones de monitoreo activo y de pronóstico

Fuente: Jeimy J. Cano

De acuerdo con la tabla anterior, podemos entender que el enfoque de mitigación del riesgo, es una estrategia, que si bien responde a una exigencia corporativa que guarda en su inconsciente que dicho riesgo desaparezca, es susceptible de una pérdida de confianza permanente cuando la amenaza advertida por razones que muchas veces no se pueden explicar, se materializa.

En este momento surge la pregunta natural del primer nivel ejecutivo: "¿Acaso, no hiciste un conjunto de actividades para mitigar el riesgo?" y la respuesta es por lo general, "Es que no tuvimos en cuenta estos otros escenarios".

Movilizar los esfuerzos hacia una gestión del riesgo es aceptar un umbral de riesgo conocido, que se declara de manera abierta y es aceptado por el primer nivel de la empresa. Esto es, se conocen los linderos de los riesgos en los procesos críticos de negocio, las estrategias que se aplican para mantenerlos dentro del umbral definido, las actividades que se aplican y el monitoreo del nivel de su exposición.

Aceptar el umbral de riesgo es entender igualmente que se puede materializar, así la gestión que tengamos frente al mismo es lo que hará la diferencia frente a su constante entendimiento y monitoreo activo.

A la fecha, la gerencia de la seguridad de la información insiste en un enfoque preventivo y de sanciones para motivar un cambio de comportamiento frente al tratamiento de la información. Como quiera que esta orientación ha alcanzado importantes logros en el pasado (estático, conocido y con datos en reposo), hoy se enfrenta a una realidad con alta movilidad, con propuestas audaces (generalmente para compartir información) y participación de terceros.

Nótese que ya no es formalmente el tema del acceso a la información el motivador principal de la relaciones entre las personas y las organizaciones, sino el uso de la misma, lo cual define un nuevo concepto y declaración para los ejecutivos en seguridad de la información: "Deben verse a sí mismos primero como líderes de negocio y luego como ejecutivos con especialidad en seguridad y gestión del riesgo".[6]

En consecuencia, los ejecutivos de seguridad de la información que quieran ser exitosos en las condiciones actuales de incertidumbre, asimetría de mercados y movilidad deberán:[7]

- Tomar decisiones de negocio, no de seguridad
- Trabajar con y a través de otros para alcanzar sus objetivos
- Ser un puente entre áreas y no una barrera para el negocio
- Conocer su industria y los retos propios de la misma
- Cambiar su lenguaje y comunicarse en términos del negocio

ESCENARIO DE RIESGOS: DE CONTEXTOS CONOCIDOS A VECINDARIOS Y ACTORES EMERGENTES

De acuerdo con los analistas de Gartner para el 2020 habrá múltiples posibilidades y escenarios que las organizaciones pueden enfrentar.[8] No será un momento tranquilo y habrá que explorar nuevas propuestas, nuevos caminos para descubrir las mutaciones de la inseguridad de la información en un mundo dominado por la movilidad, las operaciones con terceros, las redes sociales y las tensiones informáticas entre naciones.

Gartner advierte sobre cuatro escenarios para analizar:[9]

1. Riesgos regulados
2. Gobierno de coaliciones
3. Vigilancia del vecindario
4. Matriz de control

El escenario de riesgos regulados, advierte el incremento de regulaciones por parte de los gobiernos respecto de la protección de la información. Temas como privacidad, infraestructuras críticas, comportamientos de las personas en las redes sociales y uso de dispositivos móviles tendrán normas que ajusten los comportamientos de los individuos respectos de un adecuado tratamiento de la información. De igual forma, los ataques a infraestructuras tecnológicas podrán ser considerados actos de guerra, creando tensiones que puedan derivar en conflictos internacionales mediados por armas informáticas conocidas o desconocidas.

El gobierno de coaliciones, sugiere que los atacantes continuarán enfocados en las organizaciones, buscando nuevas formas de ataques o engaños, usando técnicas avanzadas de evasión (en inglés AET [Advanced Evasion Techniques])[10] o las conocidas amenazas persistentes avanzadas, generalmente enfocadas en las personas. Los ataques estarán organizados por colectivos, hacktivistas o mercenarios que buscarán violentar la tranquilidad de las empresas, para causar daño a las operaciones de los negocios y comprometer su modelo de generación de valor.

La vigilancia del vecindario esencialmente sugiere un momento de anarquía dominado por las personas y sus interacciones, considerando un contexto con poca regulación e intervención gubernamental. Se conformarán milicias electrónicas para enfrentar las acciones de los grupos hacktivistas, provocando una auto-organización de las empresas para generar una sociedad con prácticas de protección de información, que operan de manera coordinada. La confianza será un valor que estará comprometido de manera general tanto en las organizaciones como en las personas.

La matriz de control estará representada por los entes gubernamentales que buscarán proteger a los individuos, creando distracciones y limitando oportunidades para efectuar negocios. Será un momento donde el incremento de ataques a las personas (basados en redes oscuras y botnets), motivará la actuación de los estados para controlar este fenómeno, endureciendo su posición frente al respeto y dignidad de las personas respecto de su información. El monitoreo activo y el análisis de datos serán la norma para mantener una vista cercana de los que ocurre en desarrollo de las actividades sociales.

Ante estos análisis las empresas y personas deberán tomar nota y actuar en consecuencia. En esta medida el responsable empresarial de la seguridad de la información, deberá modelar los actores emergentes, preparar las infraestructuras tecnológicas, elaborar un plan que incremente la resistencia a los ataques en las personas y reconocer los nuevos flujos de información, con el fin de anticipar amenazas emergentes y prepararse para recibir las nuevas lecciones de la inseguridad de la información.

Figura 3—Arquetipos de la función de seguridad de la información

Énfasis	Operaciones	Gobierno	Operaciones y gobierno	Operaciones, gobierno y aspectos legales
Responsabilidades	• Seguridad informática • Monitoreo y análisis de eventos • Respuesta a incidentes y análisis forense • Gestión de vulnerabilidades y amenazas	• Establecer el nivel de apetito al riesgo • Gestión de riesgos de seguridad de la información • Cumplimiento de TI • Riesgos de TI • Protección de la información • Clasificación de la información	Adicional a los que se tiene en operaciones y gobierno: • Gestión de riesgos de seguridad con terceras partes • Gestión de identidades y accesos • Diseño de arquitecturas de seguridad	• Notificación de brechas de privacidad • Protección de la información • Descubrimiento electrónico (Soporte electrónico de litigios) • Monitoreo y análisis de eventos • Respuesta a incidentes y análisis forense • Clasificación de información • Gestión de vulnerabilidades y amenazas

Tomado y traducido de: Corporate Executive Board Chief Information Office Leadership Council, Common Archetypes of Security Functions: Implementation Tool, *www.irec.executiveboard.com*

ARQUETIPOS COMUNES PARA LAS FUNCIONES Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN

Considerando los cambios en los modelos de negocio y los escenarios desafiantes planteados por los analistas, cumplir con el reto de anticiparse a los riesgos emergentes que afecten la confiabilidad de las operaciones y proteger el modelo de generación de valor de la empresa, se hace cada vez más desafiante y por lo tanto, motivador para mantenerse alerta y atento a los cambios que se plantean en la dinámica de las organizaciones.

En este sentido, los analistas del *CEB CIO Leadership Council* han diseñado un estudio base de cuatro arquetipos de patrones relacionados con el ejercicio de la función de seguridad de la información (operaciones, gobierno, operaciones y gobierno, operaciones, gobierno y aspectos legales), que nos puede dar orientación sobre donde se encuentra ubicada la práctica actual (**figura 3**).[11]

Si revisamos el arquetipo orientado a las operaciones, es claro que el énfasis estará en los controles de tecnología, en las tecnologías de seguridad de la información, su implementación y aseguramiento como forma de responder a las expectativas de la gerencia sobre la protección de la información. Este escenario está dominado por un lenguaje técnico especializado, con una alta especialización de perfiles para la configuración y aseguramiento de la gestión de la tecnología de seguridad, gestión de incidentes, correlación de eventos y análisis forense, los cuales generalmente exigen un alto nivel de formación técnica y actualización permanente frente a los cambios de las mismas.

En el arquetipo basado en gobierno, el lenguaje dominante es de los riesgos de la información, el de la protección del modelo de generación de valor de la empresa, el de la búsqueda de estrategias de protección del valor de la empresa, el aseguramiento del cumplimiento normativo en el contexto del gobierno corporativo y en el entendimiento del umbral de riesgo conocido que la empresa declara. Este escenario requiere perfiles que comprendan las necesidades de los negocios, sus flujos de información y objetivos estratégicos para brindar orientaciones que sean livianas, sencillas y efectivas para lograr un funcionamiento confiable de la organización.

La combinación de operaciones y gobierno, mezcla dos mundos con responsabilidades algunas veces incompatibles. En las operaciones se tiene el control de los dispositivos de seguridad informática, cuyas normas de operación y control se definen desde el gobierno de la seguridad de la información, lo cual ocasiona una colisión entre quien planea y verifica y el que actúa y opera. Esta mezcla desenfoca al área de seguridad de los retos corporativos, pues estará concentrada más en una operación limpia y clara de la infraestructura tecnológica (aún más si está en manos de terceros) y menos atenta a las inestabilidades del entorno que puedan afectar la operación del negocio y por tanto, destruir el valor de la empresa.

El arquetipo que combina la vista anterior y le agrega los aspectos jurídicos, revela aún más la necesidad del área de seguridad de la información de estar atenta a los cambios legislativos y normativos, con el fin de ajustar su práctica frente al entorno regulado donde opera la organización.

No solamente se tienen las limitaciones presentadas anteriormente, sino el reto de incorporar la comprensión de un derecho como lo es la privacidad, que claramente desborda el entendimiento del área de seguridad de la información, retándola para combinar la práctica conocida de protección de la información con un objetivo corporativo, con la exigencia gubernamental y su modelo de sanciones frente al incumplimiento de las expectativas de los ciudadanos respecto de la protección de sus datos personales.

Así las cosas, cualquiera que sea el arquetipo que prevalezca en una organización o la forma como se encuentre organizada la función de seguridad de la información ésta deberá atender como mínimo los siguientes elementos:[12]

- La mutación del entorno de amenazas
- La explosión de información y de dispositivos portátiles
- El soporte electrónico a litigios jurídicos
- Las regulaciones financieras y las propias de cada industria
- La protección de la privacidad en entornos digitales

CONCLUSIÓN

Si bien la presión organizacional sobre la función de tecnología de información para apoyar la efectividad y eficiencia del negocio[13] será cada vez mayor, no menos será el interés del primer nivel ejecutivo sobre la protección de la información clave, dado el ambiente abierto y proclive a compartir donde opera.

En este sentido, se hace necesario comprender no solo el sector al cual pertenece la empresa, sino el ecosistema donde opera, con el fin de avanzar en el entendimiento de la convergencia tecnológica de los medios sociales, la computación móvil, la computación en la nube y la información[14] para proponer un modelo de seguridad de la información liviano, sencillo y efectivo que responda a la agilidad que el negocio demanda para capturar nuevos territorios y crear las nuevas tendencias.

Basados en lo anterior, el escenario de riesgos de la información será más retador para el ejercicio de protección frente a las amenazas del entorno, demandando una alta participación de las áreas y su personal, toda vez que el nuevo perímetro de seguridad y control se encuentra en cada uno de los individuos, lo cual implica diseñar y asegurar que los nuevos "cortafuegos humanos" deberán estar entrenados para hacerse resistentes a los ataques y reconfigurarse conforme el entorno cambie, aumentando su sensibilidad para detectar nuevos vectores de ataque que afecten los objetivos del negocio.

Por tanto, las técnicas orientadas por el monitoreo y respuesta activa[15] serán capacidades requeridas para mantener una postura de seguridad de la información que se arriesga a aprender de sus errores y se lanza a explorar nuevos patrones de amenaza, con el fin de provocar un pensamiento inusual, que genere quiebres en la práctica de seguridad y control vigente en la organización. Esto es, desaprender de lo conocido y vivir con la incomodidad de hacer "mejores preguntas".

Así las cosas, la función de seguridad de la información tendrá como maestra a la inseguridad de la información, como laboratorio de operaciones a las inestabilidades de los mercados y como libro texto a las expectativas de los ejecutivos de la organización, con el fin de motivar un proceso educativo acelerado, para convertirla.

NOTAS FINALES

1 Gunther McGrath, R.; *The End of Competitive Advantage: How to Keep Your Strategy Moving as Fast as Your Business*, Harvard Business Review Press, 2013

2 Leinwand, P.; C. Mainardi; "What's Drives a Company's Success? Highlights of Survey Findings," Booz & Company, 2013, *www.strategyand.pwc.com/global/home/what-we-think/reports-white-papers/article-display/what-drives-a-companys-success*

3 Vollmer, C.; M. Egol; N. Sayani; R. Park; "Reimagine Your Enterprise: Make Human-centered Design the Heart of Your Digital Agenda," Booz & Company, 2014, *www.strategyand.pwc.com/global/home/what-we-think/reports-white-papers/article-display/reimagine-your-enterprise*

4 *Op cit*, Booz & Company, 2013

5 Security for Business Innovation Council, "Transforming Information Security: Future-proofing Process," 2013, *www.emc.com/collateral/white-papers/h12622-rsa-future-proofing-processes.pdf*

6 Grimsley, H.; *The Successful Security Leader: Strategies for Success*, CreateSpace Independent Publishing Platform, 2012

7 *Ibid*.

8 Proctor, P.; R. Hunter; F. C. Bymes; A. Walls; C. Casper; E. Maiwald; T. Henry; *Security and Risk Management Scenario Planning*, 2020, Gartner Research, 2013

9 *Ibid*.

10 McAfee, "The Security Industry's Dirty Little Secret," *Research Report*, 2013, *www.mcafee.com/us/resources/reports/rp-security-industry-dirty-little-secret.pdf*

11 CEB CIO Leadership Council, *Common Archetypes of Security Functions: Implementation Tool*, *www.irec.executiveboard.com*

12 Harkins, M.; *Managing Risk and Information Security: Protect to Enable*, Apress, 2013

13 Khan, N.; J. Sikes; "IT Under Pressure: McKinsey Global Survey Results," McKinsey & Company, 2014, *www.mckinsey.com/Insights/Business_Technology/IT_under_pressure_McKinsey_Global_Survey_results?cid=other-eml-alt-mip-mck-oth-1403*

14 Howard, C.; D. C. Plummer; Y. Genovese; J. Mann; D. A. Willis; D. Mitchell Smith; "The Nexus of Forces: Social, Mobile, Cloud and Information," *Gartner Report*, 2012, *https://www.gartner.com/doc/2049315*

15 MacDonald, N.; "Prevention Is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence," *Gartner Research*, 2013

The *ISACA Journal* is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *ISACA Journal*.