

Innovación, Cambio y Estrategia: Tres elementos claves para potenciar la función de seguridad de la información

Jeimy J. Cano, Ph.D

Introducción

Durante estos días de múltiples noticias sobre balances de mitad de año, de revelación de indicadores de gestión, surgen muchas inquietudes sobre qué deben hacer las organizaciones para lograr lo que se han propuesto para este periodo de 365 días. En este sentido, luego de revisar tres libros, uno sobre **innovación**, otro sobre el **cambio** y un tercero sobre **estrategia**, se advierte con claridad que son estas tres palabras las que deben marcar el paso de todos aquellos que se atreven a hacer sus sueños realidad y que han decidido dejar una huella profunda en el mundo.

En este contexto, los responsables de la seguridad deberán hacer lo propio, pues la magia de la inseguridad de la información, como maestra de aquellos, nos recuerda a cada instante que debemos caminar por la ruta del desaprender, como requisito de la estrategia, la base para el cambio y la fuente de la innovación. Cada vez que nos enfrentemos al reto de la inseguridad, son los tres elementos antes mencionados los que deben animar nuestra reflexión para avanzar y desafiar los movimientos de nuestra maestra.

La innovación

La innovación en seguridad de la información supone una mente creativa, que constantemente se pregunta el porqué de las cosas, nunca está satisfecha con las explicaciones de los proveedores y demanda de ellos, formas diferentes de enfrentar los retos de la inseguridad. De igual forma, busca de manera constante combinar dominios y fuentes de análisis, como la incorporación de prácticas de otras disciplinas como el derecho, la seguridad física, las matemáticas, las ciencias sociales, entre otras, pues sabe que allí encontrará elementos que le permitirán ver mejor o replantear el reto mismo de las fallas de seguridad. (Adaptado de: PONTI 2010, pág. 72 y 73)

Todo esto lleva al responsable de la seguridad de la información a una meditación irreverente, que le permite enfrentar y desafiar a su maestra y plantear alternativas novedosas o ingenuas, que potencien la intuición y el pensamiento lateral (romper pautas y patrones habituales de comportamiento), para crear una distinción fuera de lo común, que alineada con las exigencias del negocio, le permita una posición privilegiada frente a los referente actuales de la seguridad. Todo esto siempre y cuando, se involucren y comprometan, los interesados, pues sólo allí tiene sentido el reto de la innovación en seguridad de la información.

El cambio

De otro lado, el innovar supone un cambio. Un cambio que debe estar apalancado en una movilización de esfuerzos alrededor de una visión compartida, que permita a la creatividad, encontrar terreno fértil para que sus semillas germinen. Mientras el responsable de la seguridad no sea el abono natural para pensar de manera diferente la seguridad de la información, ésta no estará en la zona de impacto que la organización necesita para ser diferente y hacer de sus procesos de negocio una zona confiable para gerencia y sus grupos de interés.

El cambio de acuerdo con la publicación de Harvard (2009 Cap.2), se adelanta en una estrategia de siete pasos a saber:

1. Movilice la energía y el compromiso a través de la identificación de problemas y sus soluciones.
 - ✓ En pocas palabras, anime la identificación de retos y logros en el tema de seguridad y provoque que las personas se “enganchen” con ellos, sólo así tiene la energía base requerida para iniciar la conquista de la su maestra: la inseguridad de la información.

2. Desarrolle una visión compartida de cómo organizarse y administrar la competencia desmedida.
 - ✓ La invitación en este punto nos lleva a que la competencia no es la forma de avanzar en la transformación de una visión. La competencia es un espejismo de los mercados, que sólo busca una confrontación de egos y no una suma de voluntades. Así las cosas, cuando de cambios se trate en seguridad, busque la colaboración de personas, que compartan la visión de un reto de protección de activos diferentes, novedoso y sobre manera, ajustado con la realidad de la empresa.

3. Identifique el liderazgo.
 - ✓ Los líderes son los individuos que inspiran, que motivan, que atraen, que conmocionan y sobre manera, que vibran con sus ideas. En seguridad, sus responsables deberán ser el ejemplo de esto, contagiando a sus aliados en los procesos de negocio para que en ellos germine la vida de la seguridad, la conciencia de los riesgos asociados con la información personal y corporativa.

4. Concéntrese en los resultados, no en las actividades.
 - ✓ Esta sugerencia nos dice que nuestro foco debe estar en aquello que queremos lograr, visualizarlo y creer que es posible realizarlo. Mantener el foco en aquello que deseamos nos ensancha el camino de la transformación, nos define las actividades que queremos realizar y nos libera de las distracciones que se puedan presentar. La seguridad de la información como foco, destruye la sensación de confort y anima una postura vigilante y alerta sobre los amenazas frente a la información.

5. Inicie el cambio en la periferia, luego a otras unidades, sin presionarlo desde la gerencia.
 - ✓ Harvard nos dice que iniciemos el proceso de cambio allí donde está nuestra zona de control, donde nuestra influencia es conocida y apoyada. Luego, con la firmeza y perseverancia del ejercicio, se irá irradiando por el ejemplo a todos aquellos, que han visto que algo diferente se hace. En seguridad de la información, podríamos hablar de “zona seguras”, esas zonas donde a pesar de los riesgos que se advierten en esas áreas, son capaces de asumir prácticas que hacen más difícil el actuar de la inseguridad.

6. Institucionalice el éxito a través de políticas, sistemas y estructuras formales.
 - ✓ Ya en este punto se le dice al responsables de la iniciativa de cambio, particularmente en los temas de seguridad, que se hace necesario mantener y

validar bitácoras del proceso que se lleva, donde se muestren con hechos y datos, cómo la organización ha venido transformando sus prácticas de seguridad de la información, no como una exigencia de la gerencia, sino como un reconocimiento propio de la forma particular como la gestión segura información hace la diferencia en los procesos de negocio.

7. Monitorizar y ajustar las estrategias en respuesta a los problemas en el proceso de cambio.

- ✓ Recuerde que en todo proceso de cambio muchos inician y pocos terminan. En este sentido la novedad de la seguridad de la información, puede hacer que muchos animadores iniciales se retiren y que las “fuerzas oscuras” del no cambio aparezcan para impactar el proceso. En seguridad de la información, la novedad y el ejemplo aplicado en cada uno de sus participantes, es la savia que alimenta y fortalece el proceso mismo de institucionalización del proceso. No desfallezca ante los ataques premeditados de terceros frente a su agenda en la gestión segura de la información, pues ellos lo que le darán son mejores y finos argumentos para mantener la flexibilidad y atención sobre lo realmente importante de la transformación: las personas y la información.

Seguir la ruta propuesta por Harvard para el cambio, no es una receta que se construye con ingredientes y mezclas precisas, es una combinación especial ajustada para cada persona y organización que se lance a desafiar el statu quo de una realidad y se someta al escrutinio público de aquellos que aún se encuentran en la zona de confort. En este sentido, los responsables de la seguridad deberán superar su temor al fracaso y a la rutina que supone la vigilancia de la seguridad y, desafiar el hecho de que la seguridad de la información es más que productos y servicios para alcanzar un nivel de protección, para convertirse en un motor estratégico de la gerencia que encuentre en ella, una manera para hacer las cosas diferentes.

La estrategia

En consecuencia con lo anterior, surge todo el discurso estratégico de la seguridad de la información que les permita a los responsables de la seguridad de la información revisar sus acciones y actividades de cara al reto mismo de la inseguridad dentro de los procesos de negocio. Para ello, la doctrina actual sobre pensamiento estratégico nos muestra tanto a Porter como a Hax, como los referentes básicos que nos permitan distinguir visiones renovadas para hacer de la seguridad una componente más que vincule al negocio, con la información y sus estrategias.

Mientras Porter funda sus estrategias de posicionamiento de los negocios basado en la competencia entre diferentes actores, buscando deferenciación por costo y producto, Hax, hace lo propio y expande dicho concepto hacia los clientes y relaciones entre complementarios en el mercado, lo cual hace que la función de visión estratégica se funde en el amor y no en la lucha de egos. Así las cosas, la seguridad de la información deberá trascender su visión eminentemente técnica por una más de negocio, que le permitan surtir el proceso estratégico evolutivo necesario para mantenerse activa como eje transversal de las conversaciones directivas.

Siguiendo lo establecido por Hax en su Modelo Delta (HAX 2010), las opciones estratégicas de las organizaciones deberán estar fundadas en tres distinciones a saber: el mejor producto, servicio integral al cliente y consolidación del sistema. Cada una de ellas como forma de generar el valor requerido para posicionarla en su propio entorno de negocio. De igual manera, la seguridad de la

información se debe valer de esta propuesta estratégica para repensarse día a día frente a sus retos corporativos y propios de la inseguridad de la información.

La opción del mejor producto, que la fuente de la competitividad de Porter, es una estrategia que en seguridad se ha consolidado a lo largo del tiempo. El liderazgo basado en tecnologías de protección y aseguramiento de equipos informáticos y las redes asociadas, establece una visión de la seguridad fundada en aseguramiento tecnológico que enfatiza y caracteriza a los profesionales de la seguridad como una personas altamente técnica y especializada que busca las mejores opciones en precio y desempeño que le permitan a la organización tener un ejercicio de seguridad tecnológica ajustado a las condiciones y expectativas de protección técnica del negocio.

Esta visión de liderazgo en costos o diferenciación tecnológica, se agota rápidamente dada la alta estandarización de las plataformas y servicios requeridos desde el aseguramiento técnico de las infraestructuras, lo que lleva indefectiblemente a la seguridad como un “commodity”, que es el escenario que se advierte hoy en las organizaciones modernas. Es una advertencia que se hace a los responsables de la seguridad en cuanto a la visión de la organización frente al tema, como algo que no requiere más elementos que los tecnológicos conocidos, desconociendo otros aspectos claves de la gestión segura de la información, que no se ven desde ésta opción estratégica.



Fuente: Arnoldo C. Hax & Dean L. Wilde; The Delta Project, 2001

Tomado de: Presentación de Juan Pablo Armas. Bacon Hill. Management Consulting. Disponible en:

http://intrawww.ing.puc.cl/siding/public/ingcursos/cursos_pub/descarga.phtml?id_curso_ic=2028&id_archivo=69507 (Consultado: 05-07-2010)

Tomar la opción estratégica del servicio integral al cliente, supone un giro estratégico crítico para los ejecutivos de la seguridad de la información. Es comprender en los mismos procesos de sus clientes las necesidades y “dolores” que hagan del negocio una nueva forma de generar valor para la empresa. En este sentido, la seguridad de la información deberá avanzar de manera profunda y detallada sobre el entendimiento de los flujos de información del negocio y advertir los riesgos y los costos de su materialización, para lo cual la tecnología será un medio y no la razón de ser de las acciones que se definan.

Asumir esta posición estratégica en seguridad de la información, posiciona al área misma como un aliado estratégico de la protección de la información en la empresa y fortalece la función de seguridad como ente asesor y de apoyo, que genera valor y diferencia frente a las expectativas y condiciones particulares de cada negocio. Así las cosas, el reto del responsable de la seguridad es hacerse uno con los dueños de los procesos para mitigar los riesgos propios de las actividades del negocio que permita reducir sus costos y aumentar los beneficios de su operación.

Nuevamente si los encargados de la seguridad de la información se mantienen en este ritmo de asesoría y acompañamiento, sin una renovación clara y concreta que le permita al negocio advertir el valor y posicionamiento de sus procesos, la función de seguridad de la información, sabrá que su posición se debilitará y comenzará el cliente a exigir nuevas formas de hacer diferente las cosas, que le permitan evolucionar de acuerdo con las necesidades de los negocios y los riesgos emergentes de la información en ese contexto.

Finalmente Hax, propone un escenario u opción estratégica más, que supone el conocimiento y complementariedad de los actores del mercado, para lograr una consolidación del sistema. Esto es, sintonía y alineación con empresas complementarias, exclusión y barreras de entrada a competidores y desarrollo de estándares y prácticas propietarias.

Aplicar esta propuesta a la seguridad de la información es realmente un desafío importante. Esto presume un alto grado de conocimiento del mercado y sus socios, el desarrollo de alianzas estratégicas de largo plazo, basadas en una fuerte dosis de innovación y cambio, así como desarrollo de prácticas empresariales muy propias y especiales, que se no se puedan identificar en el mercado o que de identificarse, la mejor opción para hacerlo se encuentra dentro de la organización.

Esta opción estratégica sugerida por Hax, hace que la seguridad de la información defina su propuesta de madurez organizacional, que le permitan hacer de su práctica una revisión estratégica de cara a la consolidación de la misma en las agendas directivas. Lograr un grado de conocimiento e innovación como el exigido en la estrategia de consolidación del sistema, nos demanda la generación permanente de sinergias y acciones concretas con terceros e internos que permitan una fuente permanente de rentabilidad corporativa, creación de barreras significativas que limiten el ingreso de nuevos competidores y la habilidad de crear estándares propietarios que transformen la industria de la seguridad de la información.

Lograr este nivel estratégico, es consolidar a la seguridad de la información como una ventaja competitiva de la organización, un activo negocio que hace la diferencia y en la forma misma como la empresa se relaciona con sus terceros. Si esta consideración se indica en los planes de desarrollo de las áreas de seguridad de las empresas, otro será el futuro de los Chief Information Security Officers, pues no estarán buscando razones para justificar la importancia de la seguridad en los negocios, sino haciendo parte de la búsqueda de nuevos horizontes y escenarios de crecimiento de las corporaciones, una forma novedosa de comunicar el valor a sus clientes y grupos de interés.

Reflexiones finales

Innovación, cambio y estrategia son tres elementos que todo responsable de la seguridad de la información debe tener en su mesa de trabajo. Son tres condiciones necesarias y suficientes para

destruir la inercia de la función de seguridad anclada en la tecnología, soportada en las prácticas y asistida por una función de servicio.

Cuando somos capaces de innovar, de retirar nuestras propias autorestricciones y lanzarnos a experimentar las consecuencias de este acto, es posible liberar la energía potencial de ideas y acciones que la seguridad requiere para enfrentar a la inseguridad. Esta connotación, exige de los diseños organizacionales de la función de seguridad espacios seguros para pensar diferente y traducir en la práctica, empoderamiento de los profesionales del área y sobre manera mucha alineación con los objetivos de negocio, para que el impacto de lo que se proponga maximice su competitividad y la fuerza de la función de seguridad.

Cambiar, deja de ser un proceso de las organizaciones, para convertirse en una necesidad permanente de las mismas. El cambio generalmente se indica cuando se desarrolla una crisis, un momento de verdad. En seguridad de la información el cambio es una crisis permanente, gracias a que la inseguridad todo el tiempo está generando nuevas formas de hacernos ver que tenemos mucho que aprender. Así las cosas, el cambio en la función de seguridad de la información es una exigencia permanente que evita a toda costa la zona de confort para los profesionales del área y la tentación de “la falsa sensación de seguridad”.

Pensar de manera estratégica, requiere tener una visión intuitiva e irreverente de lo que vemos y queremos de nuestro futuro. Bien se dice que planear, es lanzarnos a experimentar las corrientes inesperadas y propias de los vientos en las alturas como lo hacen las aves, pues de la misma forma en seguridad se exige que busquemos fuera del statu quo opciones y alternativas para disparar las rentabilidades de los negocios. La seguridad de la información más allá de un servicio, debe transformarse en una realidad de las expresiones y declaraciones de las juntas directivas, que vean en esta función un proceso de madurez organizacional, que crea estándares de industria que diferencia y posicionan a la organización más allá de sus propuestas de negocio.

Hablar de innovación, cambio y estrategia en seguridad de la información es declarar que estamos dispuestos a dar la batalla permanente y efectiva a la inseguridad de la información, que estamos atentos y alertas para conocer y confrontar las consecuencias de lecciones de las fallas, errores y vulnerabilidades de la tecnología y sobremanera, que nuestra decisión para alcanzar la madurez y evolución en el gobierno de la seguridad de la información, estará soportada en la visión estratégica, sistémica y de futuro que la organización quiere alcanzar.

Referencias

- PONTI, F. (2010) *Los siete movimientos de la innovación*. Editorial Norma
- HARVARD BUSINESS (2009) *Surviving Change. A manager's guide*. Harvard Business Press.
- HAX, A. (2010) *The Delta model. Reinventing your business strategy*. Springer Verlag

Autor:

Jeimy J. Cano, Ph.D, CFE. Ingeniero y Magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Ph.D en Administración de Negocios de Newport University, CA. USA. Profesor Distinguido y miembro del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática de la Facultad de Derecho de la Universidad de los Andes. Examinador Certificado de Fraude – CFE, IEEE Senior Member y Miembro de varios consejos editoriales como la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas, IEEE Transactions Latinoamerica, Fraud Magazine de la ACFE, entre otros. Contacto: jjcano at yahoo.com