El profesional de seguridad de la información

Un análisis de su evolución: 1960-2030+

DOI: 10.29236/sistemas.n147a6

Resumen

La rápida evolución del entorno de negocios y el advenimiento de otra revolución industrial revelan nuevos retos para el área de seguridad de la información. En este sentido, analizar el desarrollo de esta área a lo largo del tiempo, permite observar los desafíos para los profesionales de seguridad de la información en un contexto gobernado por la inestabilidad y la incertidumbre. Por tanto, este documento busca reflexionar sobre las variaciones en sus competencias y proyectar el ejercicio de una práctica de protección, consolidada con los requerimientos de las organizaciones y los negocios del siglo XXI.

Palabras clave

Seguridad de la información, perfil, capacidades, prácticas, ciber

Jeimy J. Cano M.

Introducción

Entender la evolución de los profesionales de seguridad de la información y los retos que vienen en el mediano y largo plazo, es comprender el nuevo entorno de las organizaciones. En la medida en que las compañías cambian y se reinventan, el área de seguridad se articula para proteger la promesa de valor de la empresa.

Es claro que, ante una mayor conectividad e interacción entre individuos y las máquinas, mayores se-

rán los retos que el área de seguridad de la información deba enfrentar. En este contexto, las habilidades y saberes de sus profesionales, deberán ser ajustados y reinventados, para dar cuenta de la complejidad que supone un entorno digitalmente modificado, en el que la inseguridad de la información puede camuflarse de diferentes formas.

Así las cosas, revisar cómo ha evolucionado la función de seguridad de la información establece un escenario de análisis de los retos, que tanto el ejecutivo del área, como su equipo de trabajo deben entender, asumir y superar, para construir una hoja de ruta de reinvención de sus puestos de trabajo, para acompañar a los negocios y navegar en medio de tensiones y tormentas inesperadas que puedan y quieran comprometer la promesa de valor de la empresa.

En este contexto, se revisa la evolución del perfil del profesional de seguridad de la información, de la mano con la evolución del área de seguridad de la información, analizando en cada uno de sus momentos, los focos estratégicos de su gestión y los retos que implica el entorno digital, tecnológicamente modificado, móvil e hiperconectado de forma acelerada y con sobrecarga de información.

Seguridad de la información: una perspectiva evolutiva del área y sus perfiles

1960-1970 – Controles tecnológicos

Una primera fase de la evolución inicia en los años 60 y 70, cuando la seguridad de la información estaba concentrada en el ***desarrollo y aplicación de acciones tecnológicas basadas en el control de acceso***, las cuales permanecen en la actualidad. Este desarrollo técnico ubicaba a la función de seguridad en las áreas de tecnologías de información y comunicaciones, asociada con los especialistas del tema, que conocían bien la manera de configurar dichos controles para asegurar el acceso de las personas a la información y la ejecución de sus programas autorizados (Department of Defense, 1970).

Esta vista eminentemente tecnológica convierte a los profesionales de seguridad de la información en especialistas con lenguaje técnico y estudios profundos en ciencias de la computación. La esencia de la práctica de estos profesionales era conocer en detalle los controles, su diseño, efectividad y la manera de efectuar seguimiento a su implementación. Sus reflexiones y aportes buscan disminuir la exposición de la empresa a las amenazas del momento y proteger el acceso a la información.

1980-1990: Riesgos y procesos

Con la llegada de internet, durante los años 80 y 90, la seguridad de la información se observa desde ***la vista de procesos y riesgos***, es decir, la comprensión de la inevita-

bilidad de la falla se incorpora en la dinámica de las actividades de la empresa, ubicando a la información en un lugar visible y con impactos particularmente claves, motivando reflexiones adicionales que sacan a la seguridad de un lindero eminentemente tecnológico, para leerlo a la luz de los resultados propios de la realización de las funciones del negocio.

Ahora no es solamente qué tan bien está configurado el control de acceso, sino comprender los impactos de una gestión inadecuada de los riesgos identificados en los procesos, lo cual ubica al área de seguridad en la lectura de los dominios de los sistemas de gestión y de riesgo empresariales.

En este escenario, los profesionales de seguridad de la información no solamente tienen un lenguaje tecnológico, sino de procesos. Sus perspectivas y reflexiones contemplan nuevos saberes desde la realidad de las actividades del negocio, reconociendo cómo la información fluye y permite que se alcancen los objetivos empresariales.

2000-2010: Cumplimiento y objetivos estratégicos

Entrado el nuevo milenio y su primera década, el tema de la seguridad y control evoluciona hacia un lugar más corporativo. Ahora se incorpora dentro de las ***exigencias de cumplimiento regulatorio***, como quiera que el ejercicio empresarial en el contexto de una sociedad de la información y el conocimiento, demanda una serie de condiciones básicas para aumentar la confianza de los clientes y proteger el valor de los inversionistas. La proliferación de normas con exigencias de protección y aseguramiento de información, elevan la discusión de la seguridad al escenario de satisfacer requerimientos por los cuales las empresas pueden o no pertenecer a un grupo particular (por ejemplo, la OCDE –Organización para la Cooperación y el Desarrollo Económico–) o cotizar en bolsas de valores nacionales e internacionales (p.e. la bolsa de valores de New York, en los Estados Unidos de América).

En este sentido, no son sólo los controles tecnológicos y la gestión del riesgo sobre el inadecuado tratamiento de la información, sino ahora se trata de las sanciones que imponen los reguladores por incumplimientos de las normas y estándares que generan confianza a los terceros interesados, llevando a la función de seguridad a los dominios de las áreas de cumplimiento.

Los profesionales de seguridad de la información de este momento, deben ser hábiles lectores e intérpretes de las normas de cumplimiento nacional e internacional, que articuladas con las prácticas vigentes, tanto en controles tecnológicos como de riesgos empresariales, sean capaces de enviar un mensaje claro a los ejecutivos sobre sus deberes de cumplimiento

normativo para darle profundidad a la naciente cultura organizacional de seguridad de la información (Cano, 2016), ahora vista desde el ejercicio de buenas prácticas de protección de la información y aseguramiento de los procesos.

2020-2030+: Ecosistema digital

Con la modificación acelerada del mundo a través de la tecnología y en el marco de una sociedad digitalmente modificada hacia 2020, en la que el flujo de información se percibe con mayor claridad en los ***nuevos productos y servicios de las "cosas conectadas"***, se observa una nueva revolución industrial que, en forma instantánea, permite obtener información sobre el estado de las cosas y las personas. Una realidad que experimenta cambios y se ajusta conforme las personas actúan y se relacionan con otras.

En este escenario, la seguridad de la información se convierte en un valor fundamental, en una exigencia necesaria y obligatoria que permite a las personas mantenerse conectadas con la tranquilidad de que su "realidad digital", representada en todo lo que recibe y transmite, se mantiene dentro del dominio de experiencia que ellas han declarado compartir (Porter y Heppelmann, 2015).

Así las cosas, la protección de la información no sólo se traduce en medidas tecnológicas dentro de la organización, orientadas por una gestión de riesgos y controles propios de los procesos, que asisten las exigencias de cumplimiento normativo nacionales e internacionales, sino que ahora deben concretar elementos de protección más allá de los límites empresariales y asegurar que los productos y servicios que consumen sus clientes funcionen de tal manera, que no permitan que una falla de los mismos, comprometa o afecte la esfera personal y familiar de sus usuarios. Por tanto, se pasa de una distinción de protección de afectaciones que vienen del exterior a mantener una operación interna de productos y servicios confiable, que funcione y sobreviva a pesar de los ataques externos (Bughin, Lund y Manyika, 2016).

En consecuencia, la función de seguridad de la información adquiere mayor visibilidad y sensibilidad por parte de los clientes y, por tanto, entre los ejecutivos de la empresa, generando mayor necesidad de conocimiento de los avances y prácticas de protección dentro de la operación de la compañía, como en los procesos de producción y fabricación de los productos y servicios, habida cuenta de que una falla generalizada en uno de ellos, no sólo tiene alcances técnicos, sino repercusiones económicas, sociales, políticas y administrativas. En pocas palabras, se evidencian las relaciones sistémicas que la empresa mantiene con su entorno y cómo éste afecta la manera en que la compañía desarrolla su actividad económica (De Geus, 2011).

Bajo este escenario, la función de seguridad y control se especifica a través de lo que se denomina riesgo "ciber", una categoría que no sólo concreta lo tecnológico como tal, sino la integración o convergencia entre lo físico y lo lógico, que cambia la forma como se configura la relación entre la empresa y los clientes, así como la manera en que se conciben los impactos dentro y fuera de la organización. Lo "ciber" conecta a la empresa en un espacio de relaciones hacia el exterior, para entender cómo sus operaciones afectan a otros y cómo los otros y sus actividades concretan efectos en su desarrollo de negocio, es decir, un ecosistema digital (Frappolli, 2015).

Luego, la función de seguridad de la información modifica su postura de cumplimiento normativo, por una lectura de valor para el negocio, de implicaciones políticas para los miembros del directorio, de impactos en las expectativas de los clientes y, sobre manera, en la supervivencia de la empresa en un entorno digital.

Con esta lectura, el ejecutivo de seguridad deberá madurar y desarrollar un discurso políticamente correcto, que, asistido por su conocimiento del entorno, como buen estratega que debe ser, ilustra la forma para superar el laberinto de las amenazas emergentes, comprometiendo las voluntades de los directores de la junta para concebir una lectura conjunta de la estrategia corporativa digitalmente responsable (Cano, 2015; Choudhary, 2015).

Por tanto, un profesional de seguridad de la información competente en un mundo como el propuesto, siguiendo las reflexiones de Echeverría et al (2014, p.77) "*no puede reducirse ni a un saber específico ni a una capacidad específica. La competencia exige pasar del saber hacer al saber actuar, ir más allá de lo prescrito*".

Lo anterior en perspectiva sistémica, significa comprender la seguridad de la información como un "*darnos cuenta de nuevas posibilidades… lo que implica cuestionarse los supuestos, significados, valores y normas que generalmente damos por sentados*" (Espejo y Reyes, 2016, p.63), con el fin de hacer nuevas distinciones que se conviertan en acciones prácticas incorporadas, las cuales no sólo permiten construir el mundo y desempeñarse en él, sino actuar como profesionales únicos y particulares (ídem, p.64).

En consecuencia, como afirma Echeverría (2014 et al, p.78) "*el profesional competente se caracteriza predominantemente por saber innovar, más que por los saberes rutinarios. Es decir, por poner en práctica conductas y actos pertinentes en situaciones inéditas*". Esto es, en la lectura sistémica, un entendimiento de la seguridad de la información en un contexto particular

que revela una red de interacciones, para hacer frente a los desbalances de complejidad propios de aquella, rediseñando las prácticas actuales o clasificando y agrupando las inestabilidades de la situación observada (Espejo y Reyes, 2016).

En tal sentido, la función de seguridad de la información no estará atada a las connotaciones técnicas de los dispositivos tecnológicos ni a las normas o riesgos particulares de las plataformas, sino a las lecturas ejecutivas que definen el futuro de las empresas. Las discontinuidades del entorno, particularmente basadas en estrategias digitales, se transforman en eventos relevantes que alteran la realidad empresarial y que son leídos por los miembros de la junta como eventos para revisar alrededor de las oportunidades o amenazas, en las que el ejecutivo de seguridad y control, forma parte de la vista valiosa que define el posicionamiento de la empresa entre los clientes (Kaplan, Bailey, O'Halloran, Marcus & Rezek, 2015; Veltos, 2016).

Reflexiones finales

Revisar la evolución del área de seguridad de la información, desde el mundo de los controles de tecnología, hasta su visión digitalmente modificada, en la cual las relaciones y sus impactos son evidentes; se trata de caminar por un sendero retador de aprendizaje/desaprendizaje para los profesionales de seguridad de la información en el que, como anota Morin (2011), abundan las incertidumbres con algunos pocos archipiélagos de certezas.

Es un proceso en el que se cambia un aprendizaje mecanicista fundado en repetir una fórmula probada y validada en un entorno medianamente conocido y cierto, a uno sistémico, sensible al contexto, en el que diferentes interacciones de los actores del escenario pueden cambiar las condiciones de operación de los productos y servicios de las empresas. En este sentido, los profesionales de seguridad de la información deben incorporar prácticas y reflexiones claves que les permitan equivocarse rápido, capitalizar lecciones aprendidas, generar controversias y vencer sus sesgos cognitivos, de tal forma que puedan anticipar riesgos y amenazas emergentes que afecten los nuevos activos digitales de las empresas.

En pocas palabras, lo anterior significa ejercer un “CiberLideraXgo” digitalmente confiable, que les permita:

- *Actuar de forma rápida*. Caminar con los retos empresariales y contar con los escenarios dispuestos para experimentar y simular soluciones de forma ágil y efectiva. Equivocarse es una virtud y no un defecto. Aprender rápido, es superar las barreras cognitivas de aquello que se conoce para tomar riesgos de forma inteligente.

- *Experimentar mucho*. Contar con entornos psicológicamente seguros, donde la contradicción y la experimentación sean parte natural de las reflexiones. Aprender, desaprender, desconectar y reconectar, son palabras que definen la manera como el profesional de seguridad de la información conoce y descubre su propio entorno y la realidad de los negocios.
- *Adoptar de forma temprana*. Utilizar plataformas y ecosistemas de despliegue rápido, con terceros de confianza, que permitan concretar grupos de pruebas, con el fin de desarrollar y consolidar las nuevas competencias digitales requeridas para articular los retos empresariales con las nuevas experiencias de los clientes.

- *Reinventar siempre*. Anticipar tendencias, comprender los riesgos y amenazas digitales inherentes al entorno digital y tecnológicamente modificado, con el fin de defender la promesa de valor para los clientes, consolidando acciones encaminadas a asegurar una confianza digital que proporcione profundidad y transparencia a los productos y/o servicios entregados a los consumidores.

En resumen, el profesional de seguridad de la información deberá ser una persona que construye relaciones de largo plazo, que crece con las organizaciones, creando espacios como afirmaba Steve Jobs, "*donde las ideas ganen las discusiones, no las jerarquías*". Un ejercicio de disciplina, colaboración y confianza que erige puentes para deconstruir el pasado, reinventar el presente y hacer realidad el futuro; es decir, una transformación de prácticas que buscan inicialmente proteger y asegurar la información clave de una empresa, para construir capacidades orientadas a defender y anticipar los retos y las amenazas emergentes, como una manera de custodiar la promesa de valor de las empresas.

Referencias

Bughin, J., Lund, S. & Manyika, J. (2016) Five priorities for competing in an era of digital globalization. Mckinsey Quarterly. Mayo. Recuperado de: http://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/five-priorities-for-competing-in-an-era-of-digital-globalization

Cano, J. (2015) Juntas directivas. Descifrar e influenciar su imaginario vigente sobre la seguridad de la información. *Blog IT-Insecurity*. Recuperado de: http://insecurityit.blogspot.com.co/2015/08/juntas-directivas-descifrar-e.html

Cano, J. (2016) Modelo de madurez de cultura organizacional de seguridad de la información. Una visión desde el pensamiento sistémico-cibernético. *Actas XIV Reunión Española sobre Criptología y Seguridad de la Información*. ISBN: 978-84-608-9470-4. Octubre. pp 24-29.

Choudhary, U. (2015) This Might Be The Next Coveted Leadership Position Of 2015. *F@stcompany Magazine.* Recuperado de: https://www.fastcompany.com/3043376/how-to-earn-respect-from-the-hottest-seat-in-leadership-today

De Geus, A. (2011) *La empresa viviente. Hábitos para sobrevivir en un ambiente de negocios turbulento*. Buenos Aires, Argentina: Editorial Gránica.

Department of Defense (1970) Security controls for computer systems (U). *Report of Defense Science Board Task Force on Computer Security*. Febrero. Recuperado de: http://seclab.cs.ucdavis.edu/projects/history/papers/ware70.pdf

Echeverría, B. (Coordinador), Isus, S. Martínez, M. P. y Sarasola, L. (2014) *Orientación profesional*. Segunda reimpresión. Barcelona, España: Editorial UOC.

Espejo, R. y Reyes, A. (2016) *Sistemas organizacionales. El manejo de la complejidad con el modelo del sistema viable*. Bogotá, Colombia: Ediciones Uniandes–Universidad de Ibagué.

Frappolli, M. (2015) *Managing cyber risk*. Malvern, Pennsylvania.USA: American Institute for Chartered Property Casualty Underwriters. https://www.fastcompany.com/3043376/how-to-earn-respect-from-the-hottest-seat-in-leadership-today

Kaplan, J., Bailey, T., O'Halloran, D., Marcus, A. y Rezek, C. (2015) *Beyond cybersecurity. Protecting your digital business*. Hoboken, New Jersey. USA: Editorial John Wiley & Sons.

Morin, E. (2011) *Los siete saberes necesarios para la educación del futuro*. Madrid, España: Editorial Paidós.

Porter, M. y Heppelmann, J. (2015) How Smart, connected products are transforming companies. *Harvard Business Review*. Octubre.

Veltsos, C. (2016) Is Your CISO Out of Place? *IBM Security Intelligence*. Recuperado de: https://securityintelligence.com/is-your-ciso-out-of-place/

***Jeimy J. Cano M., Ph.D, CFE**. Profesor Asociado. Escuela de Administración, Universidad del Rosario. Ingeniero y Magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Especialista en Derecho Disciplinario de la Universidad Externado de Colombia. Ph.D in Business Administration por Newport University, CA. USA. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners. Director de la Revista Sistemas de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*