Inseguridad de la información

Una visión estratégica

JEIMY J. CANO M.

Alfaomega

INSEGURIDAD DE LA INFORMACIÓN: UNA VISIÓN ESTRATÉGICA

JEIMY J. CANO M.

Alfaomega

CATALOGACIÓN EN LA PUBLICACIÓN

Cano Martínez, Jeimy José
Inseguridad de la información : una visión estratégica / Jeimy J. Cano M. – Bogotá : Alfaomega, 2013.
p. 198

ISBN 978-958-682-844-4

1. Seguridad en computadores 2. Seguridad en bases de datos I. Título

CDD: 005.8 ed. 20 CO-BOBN– a823764

INSEGURIDAD DE LA INFORMACIÓN: UNA VISIÓN ESTRATÉGICA

ISBN 978-958-682-844-4
ISBN E-book 978-607-707-681-0

Edición Alfaomega Colombiana S.A.
Corrección de estilo Francisco Díaz-Granados
Diseño Ana Paula Santander

ALFAOMEGA COLOMBIANA S.A

Empresas del Grupo
Colombia: Alfaomega Colombiana S.A.
Calle 62 n°. 20 - 46 Esquina, Bogotá
PBX (57-1) 210 0122
FAX (57-1) 746 0102
cliente@alfaomegacolombiana.com

México: Alfaomega Grupo Editor S.A. de C.V.
Pitágoras 1139, Col del Valle de México D.F.
C.P. 03100 · Tel. (52-55) 5089 7740
FAX (52-55) 5575 2420 - 5575 2420
Sin costo 01-800-020-4396
libreriapitagoras@alfaomega.com.mx

Argentina: Alfaomega Grupo Editor Argentino S.A.
Paraguay 1307 P.B. of. 11, Buenos Aires,
Tel./Fax: (54-11) 4811 7183 / 8352 /0887
ventas@alfaomegaeditor.com.ar

Chile: Alfaomega Grupo Editor S.A.
Dr. Manuel Barros Borgoño 21 Providencia, Santiago,
Tel.: (56-2)2354248 · Fax: (56-2) 2355786
agechile@alfaomega.cl

www.alfaomega.com.co

AGRADECIMIENTOS

Lograr una contribución única demanda el reconocimiento de un trabajo colectivo y de esfuerzos particulares, conjugar la pasión por un resultado y hacer que las cosas pasen. En este sentido, esta publicación que tiene en sus manos ha sido consecuencia de muchas horas de trabajo, múltiples contradicciones, grandes retos personales y colectivos.

Hablar de inseguridad de la información, en un mundo eminentemente causal (seguridad vs. controles), y no morir en el intento ha sido viable gracias a que muchas personas han comprendido que es posible, desde la inevitabilidad de la falla, entender por qué han sucedido los eventos y qué tan seguros podemos llegar a estar. En este contexto, las reflexiones de destacados profesionales, como José Isaías Martínez Gutiérrez, Luis Francisco Rivas Dueñas, Iván Reyes Gómez, Juan Carlos Huertas Amaya (Q.E.P.D.), Beatriz Caicedo Rioja, Manuel Dávila Sguerra, Fredy Bautista García, Andrés Almanza Junco, Armando Carvajal Rodríguez, Alberto León Lozano, Samuel Pinzón Barrios, Daliris Maldonado Gómez, Mauricio Luna Salguero, Aris González Rodríguez, Amanda Trujillo Mora y otros colegas y amigos, que bien saben ellos quiénes son, me han permitido cuestionarme una y otra vez, para afinar en cada momento las implicaciones prácticas de un modelo de gestión de seguridad basado en la inseguridad.

No puedo olvidar agradecer a los maestros y profesores que han sumado con sus posturas científicas y académicas para forjar esta línea de pensamiento basada en la inseguridad como una perspectiva diferente con que destruir la falsa sensación de seguridad y revelar la asimetría de la vulnerabilidad. En línea con lo anterior, gracias a los doctores Alfonso Reyes Alvarado, Raúl Espejo Ballivián, Ángela Espinosa, Álvaro Galvis Panqueva, Eugene Schultz (Q.E.P.D.), Fred Cohen, José de Jesús Vásquez Gómez, Jorge Ramió Aguirre, Mattew Bishop, Gurpreet Dhillon, entre otros, quienes me han ofrecido desafiantes visiones de la realidad, para repensar y confirmar que solo en el entendimiento de las relaciones entre las personas, la tecnología y los procesos podemos observar aquello que comúnmente está más allá de los modelos causa-efecto.

Un agradecimiento especial a todos mis estudiantes de cursos de pregrado, especialización y maestría, cuya notable inquietud académica

y científica me permite continuar creyendo que es posible transformar la manera de construir el mundo y lanzarnos a crear el futuro que queremos. Gracias por mantenerme en forma y activo, fuera de la zona de *confort* y alerta a las posibilidades que quiebran la inercia y hacen evidente nuestro deseo de desaprender, como supuesto base para escribir "derecho con letras torcidas".

Todo esto no pudo ser posible sin el concurso de mi padre y madre, que con su ejemplo de perseverancia, generosidad y entrega me han marcado el camino de la fe, la virtud y el amor, como pilares fundamentales de una vida centrada en la espiritualidad, el aprendizaje y el dominio de sí. Gracias por "darle el sí a la vida" y hacerme parte de la historia de la humanidad.

No quiero concluir este breve espacio de agradecimientos sin dedicar un momento para un ser maravilloso y lleno de luz; una dama entusiasta y altamente creativa que me ha permitido continuar en el descubrimiento de mi vocación científica y conocimiento personal, una mente inquieta que ha sabido entender mi pasión por escribir y enseñar, a quien va mi gratitud y todo mi amor. Gracias, mi corazón bello, esposa mía, por ser esa plataforma para continuar retando el futuro.

De otra parte, gracias a Martha Edna Suárez, Gerente General de Alfaomega; Francisco Díaz-Granados, corrector de estilo, y demás personas del equipo editorial, cuyo apoyo, especial dirección y acierto han hecho posible que esta nueva publicación sea una realidad. Finalmente, gracias a todos ustedes por su tiempo para encontrarnos a través de las meditaciones sobre la inseguridad de la información, pues allí podemos construir una forma alterna para reconocer la realidad y descubrir la esencia de la estrategia de seguridad: la inevitabilidad de la falla.

JEIMY J. CANO M.
PH.D., CFE.

PRÓLOGO

La consolidación de la Web 2.0 ha fomentado la proliferación de blogs de todos los tipos, con mayor o menor acierto y con mayor o menor fortuna, en especial ante un parámetro de vital trascendencia en este nuevo escenario como es el impacto alcanzado en la red y la credibilidad de sus contenidos y de su autor.

Como era lógico esperar, la seguridad de la información no se ha quedado atrás en esta nueva tendencia de la difusión masiva de información en la red, y es así como en los últimos cinco años hemos visto nacer infinidad de blogs en Latinoamérica, en donde destaca de forma notoria el blog del amigo, colega y compañero Dr. Jeimy Cano, quien ha acuñado y popularizado el término inseguridad de la información para hacer notar que nuestro problema como ingenieros preocupados de la seguridad de la información es, precisamente, su inseguridad.

Y tiene sentido hablar de inseguridad de la información, como nos dice Jeimy, en vez de seguridad, porque, aunque seamos capaces de cuantificar cuán inseguros nos encontramos, al no tener implementados adecuadamente políticas, prácticas, métodos e infraestructuras de seguridad no podremos, sin embargo, plantearnos una seguridad de la información al cien por cien, en tanto está demostrado que ello es una quimera, un objetivo inalcanzable.

En este contexto, la inseguridad se convierte en una excusa estratégica y práctica para pensar, desde la sabiduría del error, una forma de alcanzar sistemas más confiables, es decir, resistentes a los errores y vigilantes de los efectos de borde. Cuando adoptamos la inseguridad como referente para comprender la seguridad de la información, allanamos el camino para ver en medio de las vulnerabilidades y enfrentar lo inesperado.

Como compañero que he sido de él en campañas de difusión de la seguridad de la información en Iberoamérica, las cuales, de manera coloquial, hemos definido como evangelización, guardando las distancias, hago partícipe al amigo Jeimy de unas palabras mías expresadas en más de alguna entrevista y en una Lección Magistral reciente presentada en mi universidad: quienes tenemos el privilegio de ser generadores de información deberíamos asumir, además, la obligación moral de darla a conocer de una manera gratuita a quienes no tienen posibilidad alguna de obtenerla de otra forma.

Y eso es precisamente lo que viene haciendo desde hace años el Dr. Jeimy Cano, quien seguirá con esa labor aportando día a día, *post* a *post*, su grano de arena para el conocimiento y la difusión de la seguridad (o insegu-

ridad) de la información, hasta convertir ese aporte en una extensa playa de finísima y blanca arena, donde se confronta la realidad de la práctica de la operación de la seguridad con las reflexiones estratégicas para su gobierno.

Agrupadas sus reflexiones en tres partes bien definidas, forman un libro de amena lectura. Dada la excelente escritura y exposición de sus ideas, el resultado no puede ser otro que una interesante presentación del estado del arte sobre la inseguridad de la información en este último lustro, de obligada lectura por responsables, técnicos, gerentes y amantes de la protección de la información.

DR. JORGE RAMIÓ AGUIRRE

Canet d'en Berenguer, Valencia (España)
agosto de 2012

Profesor de la Universidad Politécnica de Madrid; director de los proyectos Criptored, Intypedia y Crypt4you.

JEIMY J. CANO

PH.D.

Ingeniero de Sistemas y Computación; Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes; y Ph.D. en Business Administration por la Newport University, California. Profesional certificado en: Computer Forensic Analysis (CFA) por el World Institute for Security Enhacement, EE.UU.; Certified Fraud Examiner (CFE) por la Association of Certified Fraud Examiners (ACFE); Certified Master Antiterrorist Specialist (CMAS), con especialidad en *Cyber Terrorism* por la Anti Terrorism Accreditation Board; y Executive Certificate in Management and Leadership por la Sloan School of Management del Instituto Tecnológico de Massachusetts (MIT). Egresado del Global Change Agent de la Harvard Kennedy School. Fundador e investigador del Grupo de Estudios de Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho de la Universidad de los Andes; investigador de la Red Iberoamericana de Criptología y Seguridad de la Información (CriptoRED), en España, y miembro de la Red Latinoamérica de Especialistas en Derecho Informático (Alfa-Redi). Miembro activo de: Association for Information Systems (AIS), ACM, IEEE, ISACA ACFE y HTCIA. Es autor y coordinador de los libros *Computación forense. Descubriendo los rastros informáticos* , Alfaomega, 2009, y *El peritaje informático y la evidencia digital en Colombia*, Uniandes en 2010. Ha realizado más de 100 publicaciones internacionales en revistas y conferencias académicas, entre otras: Sistemas de ACIS, *ISACA Information System Control Journal*, Conferencia Latinoamericana de Informática-CLEI, *Revista Electrónica de Derecho Informático*, Red Seguridad, Novática.

CONTENIDO

INTRODUCCIÓN

Anualmente se publica una nutrida literatura relacionada con temas de seguridad tecnológica, la evolución de sus buenas prácticas y cómo ella afecta la gestión de las organizaciones. De igual forma, son muchos y múltiples los informes que año tras año nos muestran las novedosas formas como los atacantes informáticos nos revelan las fallas inherentes de los productos o servicios que utilizamos a través de las redes o sistemas de información. En este contexto, se presentan muchos interrogantes frente a la forma como venimos enfrentando la inseguridad de la información: ¿por qué no estamos anticipando las nuevas amenazas?, ¿por qué sentimos que los "chicos malos" generalmente están un paso adelante?, ¿no estamos invirtiendo lo suficiente en medidas tecnológicas, culturales o procedimentales?, ¿las personas son cada día más abiertas a compartir información?

Estas preguntas y otras que el lector puede inferir son la mejor excusa para meditar sobre la realidad de los responsables de la seguridad de la información, esos profesionales que a diario se someten al ejercicio de comprender y anticipar la inseguridad de la información en las organizaciones buscando establecer sus mejores análisis y propuestas para desafiar la realidad evidente de la inevitabilidad de la falla. En este ejercicio los directores o gerentes de seguridad de la información saben que deberán estar preparados para enfrentar efectos inesperados de la materialización de las vulnerabilidades tanto técnicas como procedimentales e individuales, y poner a prueba su capacidad de respuesta y la "cuota de confianza" que los altos ejecutivos tienen en ellos.

El libro que tiene en sus manos detalla un conjunto de reflexiones propias del reto de "gobernar la inseguridad de la información", como una ruta aprendizaje que nos recuerda la humildad requerida por los ejecutivos de la seguridad de la información para enfrentar situaciones extremas, así como la renovación permanente de su conocimiento en los procesos de negocio y sus flujos de información. Los temas propuestos y las posiciones descritas en esta publicación son el resultado de la experiencia compartida de muchos profesionales, académicos y apasionados independientes por la seguridad de la información. Parte de los errores cometidos en el reconocimiento de la inseguridad y del encuentro con nuestras limitaciones y tentaciones, no para ver aquello que ha pasado, sino para reconocer sabiamente la enseñanza del error como una forma de reinventar el *statu quo* de la práctica y destruir la falsa sensación de seguridad.

SECCIÓN 1

ENTENDER LA INSEGURIDAD: CONCEPTOS Y GUÍAS

FUNCIÓN Y PROPÓSITO DE LA SEGURIDAD DE LA INFORMACIÓN

Revisando algunas reflexiones elaboradas por R. Ackoff en su libro *Differences that make a difference* respecto de qué es una función y qué es un propósito, encontramos muchas ideas que pueden ser de utilidad para el responsable de la seguridad de la información. Mientras una función es el uso de algo que puede tener alguna cosa, tener un propósito implica hacer selecciones y tomar opciones para lograr que ese algo se movilice. En este sentido, desarrollar una función de seguridad de la información en la empresa es establecer los mecanismos, estrategias y acciones que nos permitan hacer realidad las metas operativas de la seguridad de la información, representadas en prevención de ataques, control del *spam*, revisión y control antivirus, aseguramiento de *firewalls*, entre otras temáticas, que buscan medir la efectividad y eficiencia de las implementaciones de hardware y software para proteger la infraestructura tecnológica de riesgos que atenten contra la confidencialidad, la integridad y la disponibilidad.

Todo lo anterior se podría implementar exclusivamente desde la óptica operativa y funcional, aún sin un propósito específico, y tendría efectos positivos en la exigente labor de administración de la seguridad de una organización. Sin embargo, esta postura no respondería a la necesidad de anticipación requerida y demandada por las organizaciones para movilizar la transformación de las empresas e incrementar el nivel de protección de la información requerido por los negocios ahora y en el futuro.

Cuando la seguridad de la información tiene un propósito y un fundamento, un sueño que lograr y unas metas para cumplir es capaz de movilizar elementos organizacionales como tiempo, personas y finanzas, para cambiar la percepción de las personas y renovar lo que ellas "hacen", con lo que se hace visible un cambio de paradigma en el tratamiento de la información, es decir, que se pasa de "algo" que alguien hace por mí a "algo que es parte inherente de mí".

Materializar este tipo de paradigmas implica no solamente entender la función de seguridad de la información *per se*, sino encontrar un sentido práctico a la protección de los activos de información, como una manera de hacernos responsables reales en el tratamiento de la misma y tomar las opciones y selecciones conscientes que incrementen la percepción de tranquilidad y seguridad de los activos identificados, clasificados y puestos a disposición de una organización y sus metas grandes y ambiciosas.

Cuando hablamos de la función de seguridad de la información en una organización sin tener en cuenta su propósito nos referimos a una serie de actividades y acciones que no tienen claramente un sentido o direccionamiento, a pesar de que estas funcionen de la manera prevista. De igual forma, contar con el propósito motivador de la seguridad en una organización, pero no tener acceso a los recursos suficientes para movilizarlo, se convierte en un buen ejercicio académico que motiva a pocos y no convence a muchos. En este sentido, cada vez que nos hacemos "de mayor edad" y más pausados en nuestras reflexiones, debemos renovar nuestro niño interior, ese que está libre de autorrestricciones y dejarnos sorprender con las nuevas lecciones de la inseguridad de la información.

Adicionalmente, si agregamos un símil sobre lo que venimos reflexionando y para ello utilizamos el concepto de "caja de herramientas", podemos notar que la función de aquella, entre otras que le podemos asignar, es poder custodiar y mantener funcionales los elementos disponibles allí. Si esto es cierto, el poder de la caja de herramientas (en este caso, de la seguridad de la información) no está en su diseño ni en su funcionalidad, está en el propósito que alguien le ha asignado, en las decisiones y

opciones que se han tomado para continuar entendiendo las acciones de la inseguridad de la información, teniendo como referente base las declaraciones y protocolos legales propios que las brechas de seguridad de la información imponen a la empresa.

Tener propósitos en la vida y vivirlos con intensidad cada día es encontrar la fuente de la disciplina, la energía para hacer que las cosas pasen, y es hallar el libro de la sabiduría para tomar las opciones requeridas y necesarias que permitan elevar nuestro potencial. Si lo anterior es cierto, el responsable de la seguridad de la información, entendiendo el valor propio de las implementaciones tecnológicas y la realidad de las mediciones, podrá responder de manera ágil y contundente a las preguntas políticas que exigen los ejecutivos de la empresa, preguntas que no son otra cosa que una expresión de las necesidades y expectativas que ellos tienen para proyectarse en su mercado o sector de negocio.

Así las cosas y como quiera que aún debemos cruzar el umbral de las decisiones de presidencia y/o junta directiva, es importante recorrer el camino del propósito desde la realidad interna de la empresa, para formular estrategias operativas que, reconociendo el valor estratégico de la información, sean capaces de cautivar las metas de negocio y sus decisiones estratégicas, desde las prácticas diarias de protección de la información.

SEGURIDAD DE LA INFORMACIÓN: UNA ESTRATEGIA DE APRENDIZAJE

Russell Ackoff y Daniel Greenberg en su libro *Turning learning right side up*, publicado por Wharton School Publishing en 2008, hacen una serie de reflexiones respecto de la educación tradicional que bien se pueden aplicar al desarrollo de la función de seguridad de la información en una organización:

1. La educación tradicional se concentra en la enseñanza y no en el aprendizaje.
2. El objetivo de la educación es el aprendizaje y no la enseñanza.
3. La inteligencia es la habilidad para aprender, no es una medida de cuánto has aprendido.

La función de seguridad de la información tradicional se concentra en la información y cómo esta deber ser protegida. Es decir, estudia sus detalles y sus medios de difusión o almacenamiento para establecer las medidas tecnológicas (en el amplio sentido de la palabra y no solamente como

elementos computarizados) requeridas que permitan un acceso confiable y controlado. En esta dirección, la seguridad hace énfasis en la forma como deben hacerse las cosas para obtener el comportamiento deseado y evitar sorpresas en el futuro que impacten el nivel de confianza del usuario en el acceso a los medios donde se encuentre registrada o almacenada la información.

En consecuencia con lo anterior, una función de seguridad de la información planteada de esta forma trata de encontrar e impartir una manera de entender la protección de los activos de información orientada claramente por los controles conocidos y aplicados. En este sentido, las personas reconocerán la seguridad de la información como la atención a las medidas de restricción que le permiten conocer el nivel de confiabilidad del acceso y uso de los datos y su procesamiento, haciendo de estas una rutina básica y propia que cada persona debe memorizar y aplicar.

Entender la función de seguridad de esta manera es cerrarle la posibilidad a la organización para descubrir en su función de negocio nuevas formas de construir confianza en el acceso y uso de la información; es negarle la posibilidad de reconocer nuevos valores y comportamientos que se pueden desarrollar para confirmar una estrategia de protección basada en las personas; es perder el potencial de acción y conocimiento de cada individuo en los procesos de negocio, para revelar las intenciones de los atacantes.

Si el objetivo de la educación es el aprendizaje, el de la seguridad son los riesgos y no los controles. Parece una herejía lo que se plantea en esta reflexión, pero no lo es; es realmente el resultado de comprender que la seguridad es una propiedad emergente de un sistema, que no viene de impartir clases sobre cómo fluye y se asegura la información, sino más bien de buscar constantemente respuestas en los inesperados comportamientos que el mismo sistema presenta, fruto de la interacción entre sus componentes.

Si no existieran los riesgos o pudiésemos tener situaciones sin riesgos, la seguridad sobraría, no sería elemento sensible a considerar. Pero como no existe tal condición y la constante es que estamos expuestos a los riesgos, se hace necesario aprender de la incertidumbre y de las "fallas de control" para comprender que en la sabiduría del error está la fuente del aseguramiento permanente de la información de las empresas.

Si el secreto de la educación es el aprendizaje, entonces la inteligencia de la función de la seguridad estará en su capacidad de aprender de la dinámica de los flujos de la información en los negocios, comprender las

condiciones inseguras a las cuales está expuesta la información y detallar y moderar las expectativas de los responsables de la información, con el fin de actuar como asociado y consultor interno, de modo que pueda acompañarlos en la valoración permanente del nivel de seguridad requerido; no para hacer invulnerable el tratamiento de la información, sino para encontrar nuevas formas de responder a la inevitabilidad de la falla.

En este sentido, el encargado o responsable de la seguridad (en inglés, el *Chief Information Security Officer*, CISO) deberá entender su función como una estrategia permanente de aprendizaje y no de enseñanza, que le permita descubrir y afinar en la práctica que no se trata de transmitir, instruir, enseñar o usar la seguridad, sino más bien de construir una comprensión conjunta, tangible y concreta de los riesgos de la información desde la dinámica del negocio que de manera natural sugiera sus estrategias de aseguramiento.

ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN: UNA LECCIÓN PENDIENTE PARA LOS CISO

¿Quiénes son los arquitectos?

Frecuentemente se habla de arquitecturas, arquitectos, elementos y personalidades que poco a poco han tomado forma en medio de diferentes temáticas, como tecnología de información, seguridad de la información, talento humano, liderazgo, entre otros campos. Cuando revisamos la etimología de la palabra arquitectura encontramos que proviene del griego αρχ (*arch*, cuyo significado es "jefe", "quien tiene el mando") y τεκτων (*tekton*, es decir, "constructor" o "carpintero"), que de manera combinada podría leerse como "jefe constructor", esa persona que orienta, dirige y mantiene el rumbo para asegurar que cada pieza sea la requerida y mantenga la vista general y articulada de todo cuanto se tiene.

El arquitecto es quien de manera sistemática y sistémica define y mantiene las relaciones entre los elementos, le da forma a la estructura y define su propio funcionamiento. Ser un arquitecto es encontrarle el sentido a cada unión de los componentes, entendiendo su función en el conjunto de su obra, una forma de conjugar a los diferentes participantes e interesados para ser luz en medio de las "turbas" de los diferentes entendimientos. *Ser un "maestro constructor" es traducir la complejidad y la visión de un diseño en la sencillez de una expresión, en la cotidianidad de una explicación y en la contundencia de una declaración.*

Avanzar en el *diseño de una arquitectura*, es decir, de una forma de articular y entender una realidad, es sumar en la reconstrucción de una verdad vista por múltiples actores, planteando una serie de patrones y parámetros para hacer de la visión de la estructura final una ruta concreta y desafiante que permite a cada uno de sus participantes sentirse orgulloso de un logro colectivo. El arquitecto no puede permitirse "errores de interpretación" o la tentación de "tener la verdad", pues corre el riesgo de encontrarse con su propio reflejo, que no es otra cosa que su limitado entendimiento del enfoque final del proyecto.

En este sentido, tener la responsabilidad de *ser un arquitecto* de tecnología de información, de seguridad de la información, de la estrategia corporativa de una organización, *requiere ir más allá del entendimiento de su propia área de conocimiento y forzarse a cruzar sus dominios y descubrir aquellas relaciones que antes no había visto, encontrarse con la esencia misma de la incertidumbre, para trazar un camino evolutivo que lo lleve de una vista particular a una colectiva, enriquecida con las reflexiones de otros.*

Un arquitecto que se niegue a vivir la realidad de su misión: ser facilitador de una visión colectiva de un equipo, sabrá que será responsable de las consecuencias de las inconsistencias que se planteen en el desarrollo de sus planes, pues el que debiendo ser luz se vuelve tiniebla corrompe la sal que "da sabor" a la fuente de la perspectiva y limita el desarrollo del potencial de la comunidad, de la cual es mentor.

Así las cosas, los arquitectos, esos jefes de construcciones técnicas, deben ver en profundidad sus propias limitaciones, para que, haciéndolas evidentes en cada una de sus actuaciones, puedan ser ocasión de descubrirse a sí mismos. Por tanto, avanzar en el reconocimiento de principios básicos de arquitectura es recabar en la historia reciente de la humanidad que, desafiante de la obra divina, es capaz de vivir la humildad de su propio conocimiento.

Finalmente y sabiendo que todos somos responsables de lograr la "maestría del constructor", es necesario reconocernos finitos y limitados, para encontrar el camino que nos lleva a la *veritas*, esa promesa divina y búsqueda humana que se esconde en cada uno de nuestros pensamientos, en cada disciplina científica, en cada esfuerzo humano y técnico que hace de cada día la experiencia más exigente y desafiante que podemos experimentar: vivir en plenitud y sin límites.

Reflexiones para los arquitectos de seguridad de la información

En este sentido, un *arquitecto de seguridad de la información*, con todo su conocimiento, deberá servir de "tapete" para que sea mancillado y puesto a prueba por las "huestes" de la inseguridad de la información y así aprenda a cada paso de sus maestros la exigencia que comporta el reto de encontrar sentido y valor, para ver más allá de lo evidente y "escribir derecho con las letras torcidas".

Todo aquel que en seguridad de la información acepte el reto de ser un arquitecto deberá apartar la vista de la infraestructura tecnológica y sumergirse en el mar de las relaciones de los negocios, no para saber cómo alcanzar mayor reconocimiento corporativo, sino para descubrir en la esencia misma de cada estrategia corporativa cómo apalancar la diferencia desequilibrante, en un mercado altamente competitivo y dinámico.

Los arquitectos de seguridad de la información deben encontrar en su organización el mejor laboratorio conceptual y arquitectónico para poner a prueba su entendimiento de los negocios y las promesas de valor basadas en la confianza corporativa, con el fin de esbozar con mayores detalles las estructuras más adecuadas para anticiparse a los ataques propios de la inseguridad de la información replegada en la articulación de la tecnología, las personas y los procesos.

En consecuencia, avanzar en una vista empresarial de la *arquitectura de seguridad de la información* es reconocer en las capacidades del negocio fuerzas y mecanismos anticipatorios que permitan proteger los flujos de información que alimentan la estrategia. Es buscar en la sabiduría de los incidentes de seguridad el conocimiento requerido para blindar las respuestas de la organización frente a sus amenazas. *Es comprender las expectativas de los interesados como retos y sugerencias de transformación que hacen de las estrategias de seguridad de la información un insumo real y evidente del logro de las metas empresariales.*

Cuando el gerente, director o ejecutivo de seguridad de la información reconoce en la arquitectura empresarial cómo se hace parte de la dinámica de la corporación misma revela los disparadores escondidos del programa de seguridad de la información, amplía la visión del modelo de negocios y es consciente del impacto de sus decisiones frente a la protección de la información.

Si bien existen múltiples formas de aproximarse al diseño de una arquitectura de seguridad, cualquiera que se escoja deberá tener en cuenta al menos cuatro elementos fundamentales: *la información, las estrategias y*

metas de negocio, los fundamentos de seguridad y la administración de los riesgos. Estos cuatro elementos, vistos de manera sistémica, revelan las necesidades propias de una organización frente al reto de hacer de la información un activo valioso y de su protección una práctica sistemática inmersa en cada elemento que la constituye.

Por tanto, los arquitectos de seguridad de la información deberán compartir y alinear la agenda interna de la alta gerencia con la agenda interna del área de seguridad de la información, no para estar enterados de los retos y ajustes empresarial, sino para afinar y ajustar sus acciones frente a las amenazas empresariales del entorno y, desde el entendimiento de los riesgos de la información, generar escenarios predictivos y preventivos que custodien la forma como la empresa genera valor para sus accionistas y empleados.

Para dar cumplimiento a esta promesa del arquitecto de seguridad se deben considerar algunas declaraciones de diseño que no pueden ser negociables, y menos hoy, en un ambiente móvil de sobrecarga de información y de servicios extendidos. Las declaraciones sugeridas son:

- La *inseguridad de la información es una propiedad inherente de un sistema*, por tanto, es deber de la arquitectura descubrirla y entenderla.
- La arquitectura de seguridad de la información deberá ser *flexible y adaptable* como la inseguridad de la información (resiliente).
- El arquitecto debe entender que *la seguridad es una propiedad emergente de un sistema* y, por tanto, deberá *generar la variedad requerida* para enfrentar sus amenazas internas y del entorno.
- Cualquier diseño que se proponga para enfrentar la inseguridad de la información deberá privilegiar la *autorregulación*, la *autoadaptación* y el *aprendizaje*, como apalancadores de valor de la información, las estrategias y metas de negocio, los fundamentos de seguridad y la administración de los riesgos.

Si bien no será fácil materializar esta disciplina arquitectónica en los diseños actuales de seguridad de la información, será un reto tratar de hacerlos realidad en las nuevas iniciativas que den paso a un entendimiento de la seguridad –más allá de un ejercicio de protección de información y aseguramiento del cumplimiento normativo– cuyos fundamentos sean parte de la construcción de modelos de negocio confiables y productivos y la información sea el eje fundamental de nuestra relación con accionistas y grupos de interés.