La inevitabilidad de la falla y la transformación digital

Reflexiones de seguridad y control en un mundo digitalmente modificado

Resumen
La transformación digital es una tendencia generalizada en las empresas del siglo XXI. Su necesidad de estar más cerca de las expectativas del cliente y anticipar sus cambios, lleva a las empresas a desarrollar iniciativas de productos y/o servicios digitalmente modificados que permitan capturar mayor información con el fin de lograr experiencias excepcionales en aquellos. En este sentido, los flujos de información que se habilitan desde los objetos físicos, las interfases y las personas establecen los nuevos retos digitales para la seguridad de la información. En consecuencia, en este artículo se presentan algunas reflexiones sobre estos retos, para entender que el desafío no está en restringir, sino en habilitar una interacción confiable y flexible en la que empresa, clientes y terceros de confianza toman riesgos de forma inteligente.

Palabras clave
Seguridad de la información, transformación digital, control, valor, riesgo digital.

Jeimy J. Cano M.

Introducción

El mundo digitalmente modificado es una expresión que cada vez más está en el lenguaje de los gerentes de tecnología de información y de los ejecutivos de seguridad de la información. Mientras los primeros buscarán aumentar la presencia automatizada de los procesos empresariales y capturar toda la información posible para hacer de la experiencia del cliente algo inolvida-

ble, los segundos deberán comprender y alinear la estrategia digital de la empresa, frente al reto de proteger los activos de la empresa ahora un escenario hiperconectado, en la nube, virtualizado, de redes sociales y móvil.

Esta transformación digital toma por sorpresa a algunas organizaciones y a otras, alineadas con las exigencias de unos clientes altamente informados, demandantes de servicios novedosos y sobremanera ávidos de contenidos y apuestas emergentes que cambien su forma de hacer las cosas. En este sentido, el flujo de información corporativa y personal se incrementa, dada la convergencia tecnológica que se advierte y la modificación digital de servicios y productos que ofrece una mayor cercanía con los gustos y perfiles de sus usuarios.

En este contexto, la transformación digital no solo debe consultar los retos y apuestas estratégicas de las empresas, sino la forma como la protección de la información se traduce en fundamento básico de la interacción y la promesa de valor para el cliente que quiere aprovechar las nuevas propuestas, con la confianza y transparencia necesarias, que den cuenta del compromiso ético digital de la compañía frente al tratamiento de sus datos.

En consecuencia, la transformación digital de las empresas del siglo XXI debe indagar en los retos de la seguridad y control en un mundo digitalmente modificado, para explorar y anticipar los retos propios de la inseguridad de la información, como factor clave que permita crear y proteger el valor de las iniciativas digitales empresariales, así como motivar una práctica de aseguramiento de datos en los clientes, como efecto emergente de su participación en la nueva dinámica de los negocios.

Por tanto, adelantar una transformación digital ignorando los desafíos inherentes de la inseguridad de la información en esta nueva realidad digital, es caminar en medio de un fuego cruzado, en donde tanto empresa como cliente estarán sobre terrenos inestables, creando con cada interacción inciertos que afectarán tanto la experiencia del cliente, como los planes de negocio de la compañía.

Así las cosas, articular la transformación digital en una empresa demanda un constante aprendizaje, una interacción ágil con los productos y servicios, antes y después de su lanzamiento, así como la renovación flexible de usos y características ajustadas a los cambios de expectativas, lo cual aumenta la responsabilidad digital empresarial, para proteger los flujos de información entre la empresa y sus clientes. En este sentido, este documento plantea algunas reflexiones sobre la transformación digital y la seguridad de la información como base para repensar la práctica de seguridad y control en las orga-

nizaciones digitalmente modificadas.

Transformación digital. Una vista práctica

De acuerdo con Rogers (2016) desarrollar una transformación digital implica al menos considerar cinco elementos claves: clientes, competencia, datos, innovación y valor, los cuales en una interacción permanente logran capitalizar una lectura diferencial de la realidad, en la que se crean flujos de valor en doble vía y los datos se convierten en cada momento en activos valiosos que conectan puntos antes aislados del contexto de los clientes con la dinámica de la empresa.

La transformación digital, es una transmutación empresarial que altera la cultura organizacional y se pasa del mundo de las tecnologías de información a los productos y servicios digitalmente modificados, una apuesta de las plataformas tecnológicas para crear cooperación entre áreas, clientes, competidores y todo aquel que quiera crear activos estratégicos valiosos para el ecosistema digital de una compañía.

En este ejercicio de cambio digital, se motiva a tomar riesgos en una zona psicológicamente segura, donde fallar no es una calificación del proceso, sino un insumo que acelera la nueva práctica que la organización quiere crear para consolidar una visión renovada de sus negocios; una oportunidad, no para encontrar la solución correcta, sino para confrontar y superar el problema correcto.

Desarrollar una transformación digital implica reconocer a la organización en una dinámica de relaciones propias de un ecosistema digital, donde las conexiones definen la identidad digital de la empresa, que no es otra cosa, que la capacidad de modificar de forma anticipada su modelo de negocio para mantenerse en sintonía con la red de expectativas de los clientes y así amplificar su presencia en el entorno y confirmar su compromiso digital.

En una metamorfosis digital una empresa debe entender que se revelan comportamientos de los clientes, aquellos propios de las redes de comunicación y significados emergentes relativos a los contextos donde se encuentran inmersos. Dichas conductas apalancan los cambios digitales deseados y requeridos, para darle sentido a la estrategia digital. El acceder, el enganchar, el personalizar, el conectar y el colaborar (Rogers, 2016) son los procederes básicos que las empresas deben leer en los clientes para concretar las propuestas digitales que se desarrollen en la esfera de la realidad modificada.

A continuación, un breve resumen de las temáticas relevantes a tener en cuenta con cada uno de los comportamientos establecidos por Rogers (2016) (Figura 1).

Comportamiento	Temáticas claves que desarrolla.
Acceder	Simplicidad, conveniencia, ubicuidad y flexibilidad.
Enganchar	Conocer al cliente, crear contenido relevante, irresistible y útil, sorprender con experiencias inéditas
Personalizar	Identificar las necesidades del cliente, disponer de una plataforma de fácil uso y configuración, crear experiencias únicas.
Conectar	Motivar el uso de redes sociales para conectar los clientes con la solución de problemas, los aprendizajes de las tendencias del mercado y estar más cerca de sus gustos y expectativas.
Colaborar	Invitar a participar a sus clientes, para que desde su propio nivel de habilidad y experiencia, ofrezcan sus contribuciones y con la adecuada orientación, le den forma a su objetivo final.

Figura 1 - Nota: Tomado de: Rogers, 2016, p.29-30

Como se puede observar cada comportamiento establece la movilidad del cliente y plantea un sentido particular de su interacción. En esta lectura, lo que es transversal a todos los comportamientos detallados es el flujo de información y las emociones que se pueden crear dependiendo de la situación de negocio que se plantee en un momento específico.

En consecuencia, cada persona respecto de los comportamientos anunciados crea una dinámica de alineación o desalineación con el negocio, que debe estar asistida por las prácticas de seguridad y control, no como una tarea adicional, sino como apalancador de la relación creada entre el cliente y los servicios o productos. Lo anterior procura una madurez de la práctica de protección digital, que se traduce en confianza y transparencia, valores que ocupan mucho de la agenda de la creación de valor de aquello digitalmente modificado.

Algunas relaciones relevantes de la transformación digital y la protección de la información

Existen múltiples conexiones que se pueden revelar en el ejercicio de pensar el futuro. Los escenarios (Phadnis, Caplice & Sheffi, 2016) como fuente natural de pensamientos divergentes y como cadena de apoyo para moldear el razonamiento y las decisiones de los ejecutivos, establece una forma que sintetiza aquello que parece incierto y ambiguo en un marco de análisis de posibilidades y no de probabilidades.

Dichos escenarios revelan el potencial de las oportunidades que el ecosistema digital puede tener disponibles para todos los actores.

Dentro de las posibles contribuciones que se pueden desarrollar tenemos: (CEB, 2016)

- Integración fácil y rápida
- Incremento de la recolección de datos
- Mejoramiento del poder de cómputo y almacenamiento
- Interacción superior con la tecnología de información
- Alta movilidad

Estas posibilidades, en lectura de la infraestructura tecnológica, demandan un nivel de aseguramiento de la misma, así como de la información que va a transitar entre dispositivos móviles o productos digitalmente modificados, habida cuenta que, es de esta forma como los clientes establecen sus propios esquemas de uso y apropiación para sacarle el mayor provecho de la oferta disponible y así capitalizar el valor esperado.

De otra parte, Porter y Hoppelman (2015) confirman estos planteamientos a través de la distinción de "Niveles tecnológicos" (en inglés technology stack), donde se indica la manera como se modifica digitalmente un producto o servicio, para lo cual es necesario entender sus elementos básicos y aquellos complementarios que los modifican y nutren como son:

- Elementos básicos: a) Conectividad, b) el producto y c) el soporte en la nube
- Elementos complementarios: los elementos de seguridad y control (que afectan a todos elementos básicos), las fuentes de información externas (que afectan a b) y c)), y la integración con los sistemas de negocio.

En este modelo conceptual de los académicos de Harvard (Porter & Hoppelman, 2015), la seguridad es un elemento transversal que debe proteger la promesa de valor del producto o servicio digital e inteligente que se propone. Dada su alta conectividad y exposición en un contexto hiperconectado, es necesario validar e identificar la inseguridad de la información propia de su diseño, con el fin de aumentar la confiabilidad del producto, la seguridad de sus datos y la confianza del cliente.

En palabras de los mencionados académicos, "la seguridad de la información se convierte en una fuente clave de valor y un diferenciador potencial", palabras que confirman que toda transformación digital demanda un entendimiento de la dinámica de la información y sus flujos, para lo cual las empresas bien deben asumir los mecanismos de seguridad y control, además de ofrecer opciones particulares para que sea el mismo cliente quien configure la forma como será transmitida, recolectada o utilizada toda su información (Porter & Hoppelman, 2015).

Así las cosas, la transformación digital de las empresas supone un ejercicio previo de conceptualiza-

ción de los flujos de información que se van a desarrollar, comprender la relevancia o nivel de sensibilidad de los datos y las estrategias más adecuadas para balancear la efectividad y facilidad del uso del producto modificado, de tal forma que, tanto el cliente como la organización sean digitalmente responsables (Cooper, Siu,& Wei, 2015); esto es, asegurar una relación de confianza y transparencia que configure el valor como una propiedad emergente donde ambos se benefician.

La inseguridad de la información y la transformación digital. Una vista de retos emergentes

Sin perjuicio de lo anterior y de las conversaciones convergentes que existen entre la transformación digital y la seguridad de la información, la inseguridad establece la mirada complementaria que demanda, tanto de la organización como del cliente, una postura de riesgos, que atendiendo el contexto inestable e incierto en el que se van a usar los productos o servicios digitalmente modificados, sea capaz de aumentar la resistencia a los fa-llas o ataques de los cuales será objeto.

Por tanto, se deben revisar las actitudes y percepciones de los participantes en el diseño de la estrategia digital de la empresa, habida cuenta que es la información, la conectividad y las tecnologías de información, las que en conjunto materializan la promesa de valor para los clientes que demandan, no solamente una experiencia excepcional y sobresaliente, sino la confiabilidad y aseguramiento de su entorno digital donde él es el protagonista principal.

Ahora, el perímetro de seguridad no es ni la zona desmilitarizada o la infraestructura de contorno de las organizaciones, ni el dispositivo inalámbrico y móvil que tiene el cliente, sino la persona misma. Al tener un producto o servicio digitalmente modificado, es el ser humano el que finalmente se va a ver afectado, como quiera que su información o alguna función vital suya podrá comprometerse si algún fallo deliberado o intencional se presenta sobre aquel.

En tal sentido, la postura de riesgos, ese mínimo de paranoia debidamente administrada, deberá ser parte del entrenamiento que tanto empresa como clientes deberán construir para aumentar la resistencia a los posibles ataques sobre los productos o servicios digitalmente modificados, con el fin no sucumbir a la ansiedad por lo incierto y mantener una vigilancia y monitoreo permanente que asegure un nivel de exposición conocido y administrado.

Reflexiones finales

Hablar de transformación digital y su madurez en el contexto empresarial, es entender una serie de barreras y retos según su grado de evolución. Los temas de seguridad

y control, son propios de aquellas empresas maduras (es decir con más de cinco años con estrategia digital clara), las cuales han cubierto el camino de la falta de entendimiento de la gerencia, la insuficiencia de habilidades técnicas y las múltiples prioridades para desarrollar proyectos digitales empresariales (Kane, Palmer, Nguyen, Kiron y Buckley, 2016).

La seguridad de la información en el contexto de la transformación digital es un proceso de cambio de comportamientos, donde proteger el entorno tecnológico que concreta la ventaja competitiva significa comprender lo que es una capacidad digital: una combinación innovadora del mundo físico y el mundo lógico, donde se extrae información de los recursos físicos y se integra con los recursos digitales (Rowsell-Jones, 2013).

Así las cosas, parafraseando a los académicos del IESE (Káganer, Zamora y Sieber, 2013) los ejecutivos de seguridad de la información, en el escenario de la transformación digital, deberán ser el puente entre lo viejo y lo nuevo, gestores de lo conocido para salvaguardar las operaciones y la rentabilidad de la empresa, y custodios de las iniciativas digitales, que por ser más vulnerables, exigen una vista de un gobierno de la protección de la información para anticipar la inevitabilidad de la falla y aumentar la resiliencia organizacional ante nuevas discontinuidades de negocio.

En consecuencia y dado que se hace necesario avanzar en medio de una transformación digital, que supone un ambiente inestable e incierto, tanto las personas como las organizaciones deben tomar riesgos de forma inteligente esto es, en un continuo de confianza imperfecta, que leído en términos prácticos supone ver “los impactos estratégicos, las afectaciones tácticas, las lecciones aprendidas y los grupos de interés que se pueden ver afectados” para formular “escenarios, prototipos, simulaciones y pruebas que permitan desconectar los supuestos de los conceptos actuales para reconectarlos y crear nuevas ganancias teóricas y prácticas antes inexistentes” (Cano, 2017).

En este sentido, si bien las normas, buenas prácticas y estándares de seguridad de la información permiten un cuerpo de conocimiento base para actuar, se hace necesario repensar y reinventar las capacidades actuales de las áreas de seguridad de la información, habida cuenta que no es la reducción de la incertidumbre lo que cuenta, sino el entendimiento de los flujos continuos de certezas e inciertos que supone el riesgo digital.

Referencias

Cano, J. (2017) Riesgos inteligentes. Blog Frase de la Semana. Recuperado de: http://frasedelasemana.blogspot.com.co/2017/03/riesgos-inteligentes.html

CIO Executive Board – CEB (2016) Technology ecosystem for the digital enterprise. Infographic.

Cooper, T., Siu, J. & Wei, K. (2015) Corporate digital responsability: Doing well by doing good. Recuperado de: https://www.accenture.com/t20150521T071950__w__/us-en/_acnmedia/Accenture/Conversion-Assets/Outlook/Documents/2/Accenture-Corporate-Digital-Responsibility-Web-PDF-V2.pdf

Káganer, E., Zamora, J. y Sieber, S. (2013) Cinco habilidades del líder digital. IESE Insight. Tercer trimestre. 18.

Kane, G., Palmer, D., Nguyen, A., Kiron, D. & Buckley, N. (2016) Strategy, not Technology, Drives Digital Transformation. Becoming a digitally mature Enterprise. MIT Sloan Management Review. Research Report. In collaboration with: Deloitte University Press. Recuperado de: http://sloanreview.mit.edu/projects/strategy-drives-digital-transformation/

Phadnis, S., Caplice, C. &Sheffi, Y. (2016) How Scenario Planning Influences Strategic Decisions. Sloan Management Review. Summer.

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

Rogers, D. (2016) The digital transformation playbook. Rethink your business for the digital age. New York, USA: Columbia University Press.

Rowsell-Jones, A. (2013) Su empresa también tiene ventaja digital. IESE Insight. Tercer trimestre. No. 18.

***Jeimy J. Cano M.**, Ph.D, CFE. Profesor Asociado. Escuela de Administración, Universidad del Rosario. Ingeniero y Magíster en Ingeniería de Sistemas y Computación por 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).*