Ingeniería de sistemas

CIBERSEGURIDAD EMPRESARIAL

Reflexiones y retos para los ejecutivos del siglo XXI

Jeimy J. Cano M.

2da Edición

edU®

Ingeniería de sistemas

Ciberseguridad empresarial

Reflexiones y retos para los ejecutivos del siglo XXI

Jeimy J. Cano M.
Ph.D., Ed.D., CFE, CICA

2da Edición

edU®
Conocimiento a su alcance
Bogotá - México, D.F.

Cano Martínez, Jeimy J.

Ciberseguridad empresarial / Jeimy J. Cano Martínez -- 2a. edición. Bogotá: Ediciones de la U, 2023
330 p. ; 24 cm.
ISBN 978-958-792-483-1 e-ISBN 978-958-792-484-8
1. Ingeniería de sistemas 2. Seguridad informática 3. Riesgos informáticos 4. Seguridad informática empresarial I. Tít.
658.38 cd 24 ed.

Área: Ingeniería de sistemas
Primera edición: Bogotá, Colombia, febrero de 2022
Segunda edición: Bogotá, Colombia, marzo de 2023
ISBN. 978-958-792-483-1

Ediciones de la U es una empresa editorial que, con una visión moderna y estratégica de las tecnologías, desarrolla, promueve, distribuye y comercializa contenidos, herramientas de formación, libros técnicos y profesionales, e-books, e-learning o aprendizaje en línea, realizados por autores con amplia experiencia en las diferentes áreas profesionales e investigativas, para brindar a nuestros usuarios soluciones útiles y prácticas que contribuyan al dominio de sus campos de trabajo y a su mejor desempeño en un mundo global, cambiante y cada vez más competitivo.

Coordinación editorial: Adriana Gutiérrez M.
Diagramación: Oscar Javier Avendaño Yossa
Carátula: Ediciones de la U
Impresión: DGP Editores SAS
Calle 63 No. 70 D - 34, Pbx. (+57-601) 7217756

Impreso y hecho en Colombia
Printed and made in Colombia

Dedicatoria

Este ejercicio académico y de pensamiento gerencial está dedicado a todos aquellos que han compartido sus experiencias, logros y lecciones aprendidas con este servidor, así como a la academia (Facultad de Derecho de la Universidad de los Andes, Facultades de Contaduría Pública y de Derecho de la Universidad Externado de Colombia, Departamento de Ingeniería de Sistemas de la Pontificia Universidad Javeriana, Escuela Superior de Guerra "Rafael Reyes Prieto") y a las asociaciones profesionales (Asociación Colombiana de Ingenieros de Sistemas [ACIS], ISACA Internacional e ISACA capítulos de Latinoamérica) que me han permitido explorar posibilidades sobre la ciberseguridad empresarial como una apuesta para intentar construir sobre las bases de un dominio que aún se encuentra en construcción.

Quiero agradecer en particular al doctor Jesús Vázquez Gómez, académico y destacado profesional de la banca central de México, que generosamente ha revisado y cuidado los detalles de cada uno de los capítulos de la presente publicación; a él le doy gracias por su tiempo, consideración y disposición para afinar las reflexiones propuestas en esta obra.

Una dedicación especial a mi compañera de viaje y de votos matrimoniales perpetuos, por su apoyo y complicidad en el ejercicio de aportar y construir mapas parciales sobre territorios volátiles, inciertos, complejos y ambiguos. Gracias, mi corazón bello, por estar allí siempre para ayudarme a crecer y a descubrir mi potencial, en medio de mis luces y mis sombras.

Contenido

Índice de tablas

Índice de figuras

Prólogo segunda edición

Desde la publicación de la exitosa primera edición de "Ciberseguridad Empresarial: Reflexiones y retos para los ejecutivos del siglo XXI", el escenario se ha transformado: las tensiones e inestabilidades globales, acompañadas de una emergencia sanitaria internacional, no solo han cambiado la naturaleza de los riesgos y la dimensión de las amenazas, sino que han dejado en evidencia vulnerabilidades ya existentes que no habían sido contempladas ni atendidas. Los actores de la ciberseguridad empresarial se enfrentan a nuevos retos al diseñar e implementar estrategias y controles que respondan al contexto actual.

En esta segunda edición, el Dr. Jeimy Cano logra nuevamente una propuesta intelectual efectiva y una guía práctica adaptada a este escenario. Pone en evidencia la importancia de una formación ejecutiva que sea sensible a las amenazas que son parte "de la nueva realidad digital y tecnológicamente modificada", y que estreche la relación entre la ciberseguridad y las líneas de negocio.

Sobre todo, propone un modelo atinado para repensar las estrategias de seguridad y control, orientado a identificar el tipo de adversario y el tipo de amenaza para definir, con mayor precisión, el tipo de ataque frente al que se está. En esta nueva reflexión, el autor invita al analista no sólo a mantener la operación en caso de un ataque, sino a "descubrir y anticipar al adversario" mediante una construcción estratégica de tecnologías.

Estas reflexiones, entre muchas otras expuestas en el libro, se suman a una primera edición que ya mostraba la relevancia de la ciberseguridad en el ámbito empresarial. Esta edición revisada y, sobre todo, adaptada al contexto actual de la agenda global, se vuelve un compendio único de

fundamentos claves que todo ejecutivo debe conocer para hacer frente a los retos que se presentan en el día a día en materia de seguridad.

Auguro que esta segunda edición se convierta en un manual de referencia no sólo para el ejecutivo del siglo XXI, sino para los profesionales de toda industria y para los estudiantes y personas en formación, futuros actores de la ciberseguridad empresarial.

Dra. Erika Mata Sánchez
Cyber and Information Security Executive
México, Enero 2023

Introducción

La rápida evolución de la tecnología, las tensiones geopolíticas y la desinformación permanente se convierten en tres elementos fundamentales para tratar de comprender los cambios que suceden todo el tiempo en el mundo. En este sentido, estar al día en lo que ocurre y enfocarse en los temas más relevantes se convierte en una tarea titánica, habida cuenta del tsunami digital de información permanente al cual nos exponemos cada día.

Frente a este escenario, comprender la evolución de un tema como la ciberseguridad empresarial demanda no solo capacidad para observar patrones y advertir tendencias, sino también permanecer con una vista ecosistémica que les permita a los ejecutivos de las organizaciones comprender que ahora la dinámica corporativa no está solamente en los esfuerzos particulares que hacen las empresas para sobresalir en su entorno de negocio, sino en la forma como se crean alianzas y aliados estratégicos para construir capacidades antes inexistentes.

En consecuencia, se presenta esta publicación, que es fruto de al menos diez años de investigación y experiencia práctica en un dominio de conocimiento interdisciplinario por definición, que demanda salir de la zona de confort de los estándares y las prácticas, para ubicarse en el desarrollo de capacidades en las que el reto es concretar nuevos patrones de aprendizaje y desaprendizaje. Esto significa problemas nuevos, complejos y cambiantes, marcados por la incertidumbre y la inestabilidad de un entorno cada vez más digitalmente modificado.

Las seis secciones en que está dividido el libro se basan en reflexiones académicas y prácticas que no buscan dar respuesta a los retos actuales de la ciberseguridad empresarial, sino ayudar al lector a hacerse mejores preguntas que le permitan avanzar de forma decidida y documentada sobre sus desafíos actuales, con el fin de desarrollar capacidades que le ayuden a diseñar y desarrollar organizaciones digitalmente resilientes y orientadas a

reinventarse de manera anticipada cada vez que una tecnología disruptiva hace su aparición y plantea nuevos retos y riesgos cibernéticos.

A lo largo de esta obra se hará énfasis, particularmente, en la perspectiva del adversario como una forma de avanzar en el territorio de lo incierto que plantean los ecosistemas digitales sobre los cuales funcionan las organizaciones modernas, teniendo en cuenta la participación de los terceros de confianza, quienes son claves en la manera como las organizaciones del siglo XXI les dan forma a las promesas de valor para sus clientes y cómo son capaces de concretar experiencias distintas a través de sus productos y servicios.

Finalmente, en este proyecto editorial se establece un marco de trabajo y de pensamiento sobre la ciberseguridad empresarial que busca posicionar este tema en el imaginario de los ejecutivos de las empresas como la nueva normalidad del ejercicio de gobierno corporativo, que va más allá de los reportes y planes estratégicos para hacer las preguntas incómodas, entender la dinámica del adversario y proponer opciones poco convencionales.

Jeimy J. Cano M., Ph.D., Ed.D., CFE, CICA
Bogotá, D.C., Colombia
Diciembre 2022

I. Fundamentos de ciberseguridad empresarial

1. Ciberseguridad empresarial. Primeras aproximaciones prácticas

Introducción

La evolución acelerada de la tecnología y las comunicaciones en todas las esferas de la vida, particularmente en las empresas, demanda entender ahora una realidad interconectada, en la que los productos y servicios se definen en medio de lo que se llama un ecosistema digital.

Las empresas deben comprender que el escenario de operación ya no es del todo conocido y que se requiere superar la distinción vigente del concepto de seguridad de la información como ejercicio de práctica interna, con el propósito de proteger la organización de vulnerabilidades y fallas de seguridad y control que puedan comprometer tanto la dinámica de negocio como la de sus terceros, en los cuales la empresa es custodio de sus datos, por una nueva y complementaria que se ha denominado ciberseguridad.

La ciberseguridad, desde el punto de vista empresarial, es una realidad que prepara a la organización para comprender un escenario de amenazas digitales propias del ecosistema en el que opera y establece un conjunto de nuevas prácticas de defensa, anticipación y resiliencia, antes desconocidas y poco nombradas. La ciberseguridad empresarial no se puede ni se debe confundir con el ejercicio que se hace a escala nacional para proteger y defender las infraestructuras críticas de la nación, comoquiera que dicho ejercicio escapa a las disposiciones que un país hace para reconocer su ecosistema digital de gobierno y cómo se mantiene su operación a pesar de los posibles ataques.

En tal sentido, la ciberseguridad se enmarca en el contexto de lo empresarial, más allá de una nueva exigencia de cumplimiento, como una responsabilidad de marca mayor que implica a los miembros de la junta directiva

para entender y construir una estrategia corporativa orientada a proteger y asegurar la resiliencia de las operaciones y la reputación de la empresa, dado que, al estar expuesta en su ecosistema, se hace vulnerable a las tendencias y posiciones en las redes sociales y demás expresiones digitales disponibles a la fecha.

Así las cosas, la ciberseguridad desempeña un papel relevante en las empresas del siglo XXI, habida cuenta de que los impactos de los posibles ciberataques, bien enfocados sobre la infraestructura tecnológica o a través de campañas mediáticas de desprestigio, o que provocan la pérdida de propiedad intelectual o sanciones legales, establecen una nueva realidad que las empresas modernas deben asumir ahora como la nueva frontera del precio que se debe pagar por estar interconectados y formar parte de una red de contactos y conexiones, muchas de ellas compartidas por terceros con los cuales otras industrias igualmente contratan, para crear cadenas de suministro cada vez más complejas.

Esta reflexión sirve como preámbulo para presentar una breve revisión del concepto de ciberseguridad desde la perspectiva de las empresas, como una primera aproximación para ilustrar los conceptos, prácticas y retos que las organizaciones deben asumir por ser parte de un entorno hiperconectado, con relaciones asimétricas, abundancia de propuestas y servicios novedosos, que en cualquier momento tiene la capacidad de cambiar la historia y motivar cambios hasta el momento inimaginados.

La ciberseguridad en la empresa. Algunas precisiones conceptuales

Si bien es cierto que un ciberataque puede ocurrir en cualquier momento y de cualquier forma, los especialistas en ciberseguridad de las empresas no están para reducir este tipo de riesgo, sino para que las organizaciones tomen riesgos de manera inteligente. Para esto se requiere dar respuesta, al menos, a las siguientes preguntas (Kaplan, Bailey, O'Halloran, Marcus & Rezek, 2015, p. xvi):

- ¿Cuáles son los riesgos asociados con esta nueva iniciativa tecnológica del negocio? ¿El negocio está informado sobre el incremento del nivel de exposición de la empresa con esta iniciativa?

- ¿Cómo se diseñará esta iniciativa tecnológica del negocio para generar la mejor experiencia en el cliente y el menor riesgo de pérdida (daño o inaccesibilidad) de datos por un ciberataque?

- ¿El negocio conoce con claridad la dinámica y amenazas del ecosistema digital donde se enmarca la iniciativa tecnológica que se quiere desarrollar?

Responder a estas preguntas establece en la empresa un entendimiento extendido de lo que significa operar en un entorno interconectado, en el que las compañías no pueden protegerse ellas solas, sino que requieren conectar y desarrollar cooperación interempresarial para construir una distinción de defensa y anticipación completamente distinta de lo que se tiene en el ejercicio interno de seguridad de la información.

En este contexto, el primer ejercicio para movilizar esfuerzos hacia la ciberseguridad empresarial es reconocer y construir su ecosistema digital para enumerar sus proveedores de servicios y tecnología, las expectativas de los posibles clientes, las agencias gubernamentales y sus capacidades de acción, la sociedad civil y sus grupos relevantes, los aseguradores con sus propuestas de cobertura frente a ciberataques, así como los principales adversarios en este ecosistema.

Una vez recreado el mapa de actores y relaciones propios del ecosistema digital, la empresa, sabiendo que no puede eliminar de sus análisis la materialización de un ciberataque, debe fundamentar sus acciones para alcanzar lo que en la bibliografía especializada se llama resiliencia digital, donde (Kaplan, Bailey, O'Halloran, Marcus & Rezek, 2015, pp. xvii-xviii):

- La empresa comprende los riesgos de los ciberataques y puede tomar decisiones en que los retornos de las iniciativas tecnológicas planteadas justifican el incremento del riesgo.

- La compañía confía en que los riesgos de los ciberataques son manejables, más que los estratégicos, los cuales no ponen en riesgo la posición competitiva de la empresa o su existencia.

- Los clientes y los negocios tienen confianza en la economía en línea, en la que los riesgos sobre los activos de información y los fraudes en línea no son un freno para el crecimiento del comercio digital.

- El riesgo de ciberataques no limita a las empresas a la hora de continuar tomando ventaja de las innovaciones tecnológicas.

El ejercicio de resiliencia digital debe procurar la continuidad de los negocios, fundada en la capacidad de la empresa para gestionar los incidentes de seguridad y asegurar la disponibilidad de los sistemas, con base no solamente en sus posibilidades técnicas y operacionales, sino con el apoyo de sus socios estratégicos en el ecosistema digital en el que participa.

La ciberseguridad en la empresa y su nueva normalidad

Las empresas entienden que las prácticas básicas de seguridad de la información, sustentadas en los estándares conocidos (ISO 27002, NIST SP800-53), determinan los elementos que articulan las estrategias que se desarrollen para asegurar la nueva función de ciberseguridad de la organización.

Esto supone que se debe pasar de un enfoque basado en *proteger y asegurar*, el cual moviliza las actividades dentro de la organización para cultivar un adecuado tratamiento de la información y soportar las exigencias propias del cumplimiento regulatorio, a otro basado en *defender y anticipar*, en el que la organización *censa y responde* de acuerdo con su lectura del ambiente, las tendencias identificadas y los retos de negocio que crean entornos disruptivos que afectan su posición estratégica y competitiva (Cano, 2014).

Lo anterior significa que las prácticas que conocemos de la seguridad de la información, asociadas con autenticación, autorización, auditabilidad y no repudio, se deben complementar con otras que den cuenta de las exigencias de anticipación que las empresas requieren para mantener ahora su nivel de "ciberriesgo" (Frapolli, 2015, p. 13).

Las prácticas complementarias, que podemos llamar propias de la ciberseguridad de las compañías, deben estar fundadas en actividades relacionadas con:

- **Análisis de escenarios.** Una práctica que establece y proyecta contextos posibles de amenazas y riesgos emergentes, con el propósito de motivar reflexiones y acciones que preparen a la organización frente a situaciones imprevistas y eventos no esperados.

- **Ciberinteligencia.** Una función de monitoreo y valoración de información sobre amenazas, que desarrolla pronósticos sobre vectores de ataques y objetivos que los atacantes pueden materializar en el contexto del ecosistema digital en que opera la organización.

- **Juegos de guerra.** Se diferencian de las pruebas de vulnerabilidades tradicionales, en las que se contratan terceros para identificar fallas en la infraestructura que habilitan una fuga o pérdida de información, en cuanto a que en los juegos de guerra se busca comprender la información que hay que proteger, sabiendo las fallas de seguridad que el atacante puede concretar y así poder ver las limitaciones que la empresa tiene para enfrentar un ciberataque, particularmente en la forma de establecer su estrategia de comunicaciones y su proceso de toma de decisiones (Kaplan, Bailey, O'Halloran, Marcus & Rezek, 2015, p. 150).

- **Defensa activa.** Esto implica pasar de una postura pasiva de respuesta frente a ataques del exterior a una reflexión que modela y anticipa los nuevos movimientos de los atacantes (Kaplan, Bailey, O'Halloran, Marcus & Rezek, 2015, pp. 134-135), para lo cual:

    - Establece los perfiles de actividades que son consideradas normales en la organización, para poder ver los cambios inusuales y así alertar y actuar en consecuencia.

    - Integra los resultados de la ciberinteligencia para plantear hipótesis de posibles intrusiones peligrosas y emergentes.

    - Consulta y afina los resultados del Centro de Operaciones de Seguridad (en inglés *Security Operation Center*, SOC), que luego de filtrar los posibles falsos positivos y de descifrar los nuevos patrones o vectores de ataque, permite enfocar las acciones que son decisivas para enfrentar y tratar de contener a los posibles atacantes.

La ciberseguridad en la empresa y sus nuevos retos

La ciberseguridad en el contexto empresarial tiene un enfoque completamente distinto de las connotaciones del concepto en el escenario de la protección de la gobernabilidad de una nación, a menos que la empresa en cuestión tenga a cargo infraestructuras críticas del orden nacional.

Mientras en un país la ciberseguridad adquiere una distinción de práctica transversal que conecta los sistemas de protección de cada una de las entidades que forman parte del sistema de gobierno nacional para hacer más resiliente la operación gubernamental, en el ámbito empresarial se revelan las conexiones propias de la corporación y la sensibilidad de estas frente a su capacidad de resistencia a ciberataques que comprometen su modelo de operaciones.

En razón de lo anterior, se requiere formular una nueva función de protección del modelo de negocio, basado en la lectura del ecosistema digital, que incorpore nuevas habilidades y capacidades para defender y anticipar nuevos escenarios de ciberataques, las cuales deben responder a retos empresariales como los siguientes (Kaplan, Bailey, O'Halloran, Marcus & Rezek, 2015, p. 163):

- Priorizar los activos de información basados en los riesgos de negocio.
- Integrar las prácticas complementarias previamente enunciadas en el entorno de la tecnología de información empresarial.
- Incorporar el concepto de ciberriesgo dentro del sistema de riesgos empresariales y los procesos de gobierno corporativo.
- Establecer estrategias de protección diferenciadas, de acuerdo con el nivel de sensibilidad de los activos identificados.
- Mantener y sostener la capacidad de respuesta a incidentes, que permita incorporar y asegurar las lecciones aprendidas e incrementar la resiliencia corporativa.
- Reconocer, construir y actualizar su ecosistema digital.

Estos retos se deben traducir en planes de acción y estrategias concretas que permitan asegurar la incorporación de la nueva normalidad, para así cambiar no solamente la estrategia de participación de la empresa en su entorno digital, sino activar un nuevo conjunto de habilidades y recursos que construyan un nivel de resiliencia mayor dentro de su ecosistema digital, para lo cual es clave tener en cuenta esto (Kaplan, Bailey, O'Halloran, Marcus & Rezek, 2015, p. 191):

- Las definiciones de política pública nacional e internacional vigente.

- Los aportes de la sociedad civil, así como de las comunidades académicas y de investigación.

- La dinámica de los mercados y cambios en internet, que hablen de acciones coordinadas para estabilizar y normalizar operaciones comprometidas.

Finalmente, pero no menos importante, se hace necesario incorporar dentro de la agenda empresarial, en lo que respecta a la junta directiva (Rai, 2014), la lectura de algunos deberes claves de los miembros del directorio, como práctica de gobierno corporativo que reconoce las amenazas externas y las volatilidades propias del ecosistema digital en el que se encuentra la organización.

En este escenario, los miembros de la junta deben asegurar que sus actuaciones son coherentes con esta realidad y dar cuenta de sus acciones respecto de estos eventos, para movilizar y asegurar su debido cuidado y diligencia frente a los intereses de la empresa y el cuidado de la imagen corporativa. Por consiguiente, cada miembro de la junta debe asegurar el cumplimiento de al menos cinco deberes (Frappolli, 2015, pp. 316-317) frente a la dinámica de las tensiones que provoca un ciberataque y las exigencias que la ciberseguridad demanda tanto para la organización como para sus ejecutivos de primer nivel:

Deber de cuidado. Cada miembro de la junta debe mantenerse informado de los eventos y noticias relevantes sobre ciberseguridad o ciberataques, con el propósito de asegurar un tono adecuado de las discusiones en el contexto de los objetivos y estrategias de la organización.

Deber de lealtad. Cada miembro de la junta no debe tener negocios o participar en negocios que compitan con la organización para la cual sirve, y más aún, comunicar situaciones adversas que conozca, las cuales afecten las condiciones de seguridad y control que tenga la empresa de la que es miembro en su directorio ejecutivo.

Deber de divulgación (transparencia). Los miembros de la junta están obligados a revelar los hechos que son relevantes para los grupos de interés

de la empresa para la cual trabajan. En particular, establecen el mecanismo y la estrategia que permiten dar cuenta de eventos desafortunados de seguridad de la información, con impactos en alguno de sus grupos de interés.

Deber de obediencia. Los miembros de la junta deben ceñir sus actuaciones a la Constitución y la ley, así como frente a los fundamentos del gobierno corporativo. En otras palabras, asegurar las prácticas y los estándares requeridos para aumentar la resistencia de la empresa frente a ataques informáticos, así como motivar y apoyar comportamientos adecuados en el tratamiento de la información de la compañía.

Deber de verificación. Los miembros de la junta deben contar con mecanismos para validar las acciones que sobre el tema de seguridad de la información se llevan a cabo en la empresa, motivar los planes de mejora que sean del caso y asegurar los recursos necesarios para incorporar las buenas prácticas en personas, procesos y tecnología.

Reflexiones finales

Si bien a lo largo de este texto se han enunciado algunas ideas sobre la ciberseguridad en el contexto empresarial, es importante anotar algunos de los retos legales propios de la tensión existente entre el uso abierto y libre del ciberespacio y su protección como espacio de estrategias competitivas e innovación (García, 2013, pp. 87-90):

- La neutralidad de la red.
- La regulación del ciberespacio.
- Las amenazas para derechos y garantías individuales.
- La responsabilidad de los proveedores de los servicios.
- Los problemas de la jurisdicción sobre los alcances de las conductas punibles en internet.
- Las tecnologías emergentes estructurales, como computación en la nube, computación móvil, las redes sociales, los grandes datos y su analítica, la inteligencia artificial y el internet de las cosas.

Estos retos completan el escenario volátil, incierto, complejo y ambiguo (Johansen, 2009) que configura la realidad de las organizaciones modernas, enmarcadas en un ecosistema digital en permanente movimiento y evolución. Así las cosas, la ciberseguridad empresarial debe prepararse para las nuevas amenazas digitales, derivadas ahora de su relacionamiento con cada uno de los actores del ecosistema en el que participa:

- Las agencias de regulación.
- Los proveedores de servicios y productos.
- Los vendedores de tecnologías de información y comunicaciones.
- Las asociaciones industriales.
- Los clientes corporativos y los consumidores.
- El Gobierno y sus agencias de seguridad y control.
- Los atacantes.
- La sociedad civil.

Lo anterior implica entender con claridad qué significa ser una empresa digital (Dörner & Edelman, 2015) o con maestría digital (Westerman, Bonnet & McAfee, 2014), esto es:

- Lectura y análisis de los comportamientos y expectativas de los clientes que se desarrollan dentro y fuera del contexto de negocio, así como fuera de su sector, para identificar las tendencias que pueden entregar o destruir valor.
- Uso de nuevas capacidades para optimizar la forma como se atiende a los clientes y se mejora su experiencia como usuario.

En pocas palabras, los procesos tecnológicos y organizacionales que permiten que una compañía sea ágil y rápida para responder y anticipar los cambios disruptivos del entorno, al igual que capitalizar las oportunidades que se derivan de estos (Dörner & Edelman, 2015).

En consonancia con lo anterior, la ciberseguridad empresarial debe apoyar y movilizar a la organización para establecer su nivel de exposición al ciberriesgo, entendiendo sobre qué parte de la cadena de valor tendrá control y cuánto desea invertir en conocer a sus clientes finales (Weill & Woerner, 2015). Esto significa que deberá desarrollar escenarios de análisis en los que se desconecten los puntos de la realidad conocida, se incorporen los resultados de la ciberinteligencia realizada, para conectarlos nuevamente (De Jong, 2015) y así expandir el entendimiento de su ecosistema y revelar aspectos ocultos de futuros inciertos o riesgos inesperados (Roxburgh, 2009).

La ciberseguridad empresarial, por tanto, es una novedosa práctica corporativa que demanda explorar, por debajo de la superficie institucional y en medio de la vorágine de propuestas emergentes, aspectos novedosos de la realidad que motiven y descubran agentes de riesgo inéditos o renovados que puedan comprometer la dinámica de los negocios y establecer condiciones adversas que limiten su participación en las oportunidades de su sector.

Si lo anterior es correcto, la ciberseguridad empresarial se convierte en un nuevo estándar de las operaciones de las compañías con presencia global, que reconocen que no existen límites geográficos para que un atacante, o actor no identificado, pueda concretar un ciberataque y crear un escenario de inestabilidad e incertidumbre que comprometa sus virtudes corporativas y sus alianzas estratégicas.

Referencias

Cano, J. (2014). Transformando la función de la seguridad de la información. Anticipando el futuro, entendiendo el presente. Blog *IT-Insecurity*. http://insecurityit.blogspot.com.co/2014/11/transformando-la-funcion-de-la.html.

De Jong, R. (2015). *Anticipate. The art of leading by looking ahead*. Amacon.

Dörner, K. & Edelman, D. (2015). *What 'digital' really means*. McKinsey Digital. http://www.mckinsey.com/insights/high_tech_telecoms_internet/what_ digital_really_means.

Frappolli, M. (2015). *Managing cyber risk*. American Institute for Chartered Property Casualty Underwriters.

García, P. (2013). El derecho de internet. En A. Segura y F. Gordo (coords.) (2013). *Ciberseguridad global. Oportunidades y compromisos en el uso del ciberespacio* (pp. 69-90). Editorial Universidad de Granada.

Johansen, B. (2009). *Leaders make the future: ten new leadership skills for an uncertain world*. Berrett-Koehler Publishers.

Kaplan, J., Bailey, T., O'Halloran, D., Marcus, A. & Rezek, C. (2015). *Beyond cybersecurity. Protecting your digital business*. Wiley.

Rai, S. (2014). *Cybersecurity: what the board of directors needs to ask*. Isaca-IIA. http://www.theiia.org/bookstore/downloads/freetoall/5036.dl_GRC%20Cyber%20.

Roxburgh, C. (2009). The use and abuse of scenarios. *McKinsey Quarterly*. https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/the-use-and-abuse-of-scenarios.

Weill, P. & Woerner, S. (2015). Thriving in an increasingly digital ecosystem. *Sloan Management Review*, *56* (4), 27-34.

Westerman, G., Bonnet, D. & McAfee, A. (2014). *Leading digital. Turning technology into business transformation*. Harvard Business Review Press.

2. La inevitabilidad de la falla y la transformación digital. Reflexiones de seguridad y control en un mundo digitalmente modificado

Introducción

El mundo digitalmente modificado es una expresión que está cada vez más 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 captar toda la información posible para hacer de la experiencia del cliente algo inolvidable, los segundos deberán comprender y alinear la estrategia digital de la empresa frente al reto de proteger los activos de la compañía ahora en 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 ávidos sobremanera de contenidos y apuestas emergentes que cambien su forma de hacer las cosas. En tal sentido, el flujo de información corporativa y personal se incrementa, debido a la convergencia tecnológica que se advierte y la modificación digital de servicios y productos, la cual 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 también la manera 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 la 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, al igual que motivar una práctica

de aseguramiento de datos en los clientes, como efecto emergente de su participación en la nueva dinámica de los negocios.

Por consiguiente, llevar a cabo una transformación digital desconociendo los desafíos inherentes a la inseguridad de la información en esta nueva realidad digital es caminar en medio de un fuego cruzado, en el que tanto empresa como cliente estarán sobre terrenos inestables, creando con cada interacción actos 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, al igual que la renovación flexible de usos y características ajustados a los cambios de expectativas, lo cual aumenta la responsabilidad digital empresarial para proteger los flujos de información entre la compañía y sus clientes. En tal sentido, a lo largo de este texto se plantean algunas reflexiones sobre la transformación digital y la seguridad de la información como base para repensar la práctica de seguridad y control en las organizaciones 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. Estos elementos logran capitalizar, en una interacción permanente, 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 compañía.

La transformación digital es una transmutación empresarial que altera la cultura organizacional, en la que 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 vista renovada de sus negocios; una oportunidad para confrontar y superar el problema correcto, no para encontrar la solución correcta.

Desarrollar una transformación digital implica reconocer a la organización en una dinámica de relaciones propias de un ecosistema digital, en la que las conexiones definen la identidad digital de la empresa, que no es otra cosa que la capacidad de modificar anticipadamente su modelo de negocio para mantenerse en sintonía con la red de expectativas de los clientes y así ampliar 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 compañías deben leer en los clientes para concretar las propuestas digitales que se desarrollen en la esfera de la realidad modificada.

A continuación (Véase tabla 1), un breve resumen de los temas relevantes que hay que tener en cuenta con cada uno de los comportamientos establecidos por Rogers (2016):

Como se puede observar, cada comportamiento establece la movilidad del cliente y plantea un sentido particular de su interacción. En esta lectura, lo 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 crea una dinámica de alineación o desalineación con el negocio respecto de los comportamientos anunciados, la cual ha de estar asistida por las prácticas de seguridad y control, no como una tarea adicional, sino como una labor apalancadora 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 gran parte de la agenda de la creación de valor de aquello digitalmente modificado.

Tabla 1. Comportamientos claves para la transformación digital

Comportamiento	Temas 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 a 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 le den forma a su objetivo final, con la orientación adecuada.

Fuente: tomado de Rogers (2016, pp. 29-30).

Cómo entender 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 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 (Phadnis, Caplice & Sheffi, 2016).

Dichos escenarios revelan el potencial de las oportunidades que el ecosistema digital puede tener disponibles para todos los actores. Entre las posibles contribuciones que se pueden desarrollar están (CEB, 2016):

- Integración fácil y rápida.