Seguridad y ciberseguridad 2009-2019

DOI: 10.29236/sistemas.n155a6

Lecciones aprendidas y retos pendientes.

Resumen
Cuando una década se cierra es natural efectuar una visión retrospectiva sobre lo ocurrido y los aprendizajes adquiridos. En la década 2009-2019 fueron múltiples los eventos y las tendencias materializados en el dominio de la seguridad y la ciberseguridad, los cuales cambiaron la forma en que las organizaciones modernas asimilan y gestionan las amenazas digitales en la dinámica de sus negocios. Este documento presenta cinco temáticas relevantes (la computación en la nube, la computación móvil, la convergencia tecnológica, las redes sociales y la asimetría de los ciberconflictos) para sustentar las bases de las prácticas y retos emergentes de seguridad y control en los próximos diez años para las empresas digitales y tecnológicamente modificadas.

Palabras clave
Seguridad, lecciones aprendidas, retos, ciberseguridad, resiliencia

Introducción

Termina una década iniciada en el año 2009 marcada por la actividad no autorizada que estuvo muy activa. En este sentido, es importante revisar los aprendizajes durante ese tiempo y las enseñanzas que dejan los eventos adversos de los últimos 365 días de ese período.

Luego de revisar diversos documentos (académicos y de proveedores) y correlacionar información basada en tendencias identificadas en cada uno de ellos, la reflexión apunta a agrupar algunas temáticas sobre las lecciones aprendidas en la última década y cómo éstas pueden ayudar a identificar y enfrentar los retos a partir del año 2020, además de realizar una mirada crítica sobre los hechos más relevantes de 2019.

Esta última mirada, más que ofrecer soluciones sobre lo observado, establece una revisión sin apasionamientos ni reclamos por lo sucedido, sino una oportunidad para avanzar en el reconocimiento de las cegueras cognitivas construidas alrededor de la experiencia previa. Experiencia que, si bien es clave y valiosa para aprender, muchas veces resulta cómoda y fácil de tomar para interpretar aspectos de una realidad que es dinámica y se reinventa en cada momento.

En consecuencia, la invitación es a encontrar una "realidad aumentada" por los datos y noticias sobre la inseguridad de la información, para decantarla y analizarla desde la perspectiva conceptual y práctica, y así buscar y conectar puntos desconectados de la realidad, además de construir conocimiento sobre las tendencias y los retos que todavía se deben resolver en la academia y en la dinámica empresarial.

¿Qué aprendimos en seguridad de la información en la década 2009-2019?

Al revisar los avances y tendencias durante la última década, se pueden advertir al menos cinco (5) temáticas relevantes para la seguridad y control, las cuales son transversales a las diferentes industrias y a las condiciones geopolíticas globales: la computación en la nube, la computación móvil, la convergencia tecnológica, las redes sociales y la asimetría de los ciberconflictos.

A continuación, se exploran tales temáticas detallando los aspectos más relevantes de cada una de ellas, para finalizar con las lecciones aprendidas y los retos pendientes en el futuro inmediato.

Computación en la nube

La introducción de terceros en la operación de la tecnología de información en las organizaciones es una realidad materializada con la computación en la nube. Es una apuesta de delegación y monitori-

zación de recursos tecnológicos en la infraestructura de un contratista que las empresas alquilan en alguna de las modalidades disponibles: infraestructura, plataforma o *software* como servicio.

Cada una de estas modalidades está asociada con el nivel de dependencia, agilidad del despliegue y valor del servicio que las empresas quieren imprimirle a la dinámica de su negocio. La computación en la nube se ha consolidado como un nuevo "commodity" que las compañías pueden usar para flexibilizar las inversiones en tecnología de información y dedicar sus recursos a temas de innovación y experiencias con los clientes (Garrison & Nova, 2018).

Con este posicionamiento empresarial de las apuestas en la nube, los temas de seguridad y control también comenzaron a migrar a este contexto. Surge el acrónimo CASB (*Cloud Access Security Broker* – cuya traducción podría ser Agente de seguridad para acceso a la nube), cuyo objetivo es proteger la información y los usuarios, con la capacidad de inspeccionar todo el tráfico que va hacia y desde las aplicaciones en la nube (Mendoza, 2014).

Este nuevo elemento de la seguridad y el control en el contexto de la nube, permite a las empresas aumentar la flexibilidad en el despliegue de sus aplicaciones, con un impacto limitado en la operación de las mismas. No obstante, se convierte en un punto único de falla que, si es comprometido, habilita posibles accesos no autorizados, desarrollo de *malware* especializado y ataques inciertos basados en las fallas no documentadas de las configuraciones previstas en este agente.

Frente a esta realidad, varias lecciones aprendidas y retos pendientes se describen a continuación:

Lecciones aprendidas

- Cada vez que el usuario sube datos a la nube, pierde control, quiera o no.
- Subir datos a la nube implica un nivel de cumplimiento distinto al contexto corporativo.
- La gestión de vulnerabilidades e incidentes debe ser la norma inherente de los terceros de confianza.

Retos pendientes

- El reto de la latencia y acceso a recursos en la nube desde dispositivos móviles y del internet de las cosas.
- Convivencia entre la "computación en el borde", la "computación en la niebla" y la computación en la nube frente a los nuevos retos de la realidad aumentada.
- La convergencia tecnológica y los nuevos ataques propios de los ecosistemas digitales de las organizaciones.

Computación móvil

Los móviles como una tendencia

que devuelve el control a los usuarios, como estrategia de acercamiento de la tecnología a las personas, se convirtió en parte natural de la dinámica social. A la fecha, en muchos países existen más teléfonos móviles que personas en el territorio. Desde los móviles diferentes dinámicas sociales se automatizaron, se aumentó el acceso a los servicios y se promulgó un acta democrática de acceso a la información, en la que los individuos están más conectados y probablemente más informados (o posiblemente desinformados o mal informados) (Cobo, 2019).

Con los teléfonos móviles se cambia la interacción inicialmente basada en la web, con páginas, servicios y accesos dirigidos a las necesidades de los ciudadanos, por una nueva realidad denominada la era de las "apps", en que la agilidad y los servicios ágiles comienzan a hacer la diferencia. Ya no es solamente la oportunidad de la atención, sino la efectividad del servicio, con una experiencia distinta que demandan los clientes. Estar conectados desde el teléfono móvil es personalizar el "control" de los individuos sobre la manera en que quieren disponer de sus productos y servicios.

Los móviles crean una gran masa de conectividad y homogeneidad (según la marca que se tenga) estableciendo una mayor superficie de cobertura y posibilidad para los negocios actuales y, al mismo tiempo, un espacio propicio para desarrollar posibles actividades no autorizadas con un impacto masivo, como quiera que las personas tienen una limitada cultura de seguridad y control (muchas veces ingenua), y que los proveedores podrían mejorar sus mecanismos sobre el aseguramiento de los sistemas operativos móviles, el desarrollo y despliegue de aplicaciones, así como frente a su conectividad vía API (*Application Program Interfase* – Interfase de Programas de Aplicación) (Brodsky & Oakes, 2017).

La seguridad y control en el tema de los móviles configura un reto conceptual y práctico para los proveedores de tecnología, las empresas y los terceros de confianza. El *malware* especializado, la gran cantidad de "apps" maliciosas, la baja confiabilidad en el desarrollo y la "confianza ingenua" de muchos usuarios, hace de esta tendencia una posibilidad concreta para desplegar acciones adversas con impactos masivos y muchas veces indeterminados, según el lugar y momento en donde se encuentren conectados (Coburn, Leverett & Woo, 2019).

Frente a esta realidad, varias lecciones aprendidas y retos pendientes:

Lecciones aprendidas

- Estar todo el tiempo conectados es virtud para los negocios y oportunidad para los adversarios.

- Toda “app” es fuente de una experiencia novedosa y posible punto de acceso para un atacante.
- La confianza en la conectividad es equivalente a una amenaza ante la vulnerabilidad.

Retos pendientes
- El balance de seguridad y funcionalidad de las “apps” que permita una interacción liviana, sencilla y efectiva.
- Conectividad entre “apps” en los nuevos ecosistemas digitales y las implicaciones de seguridad y control en estos entornos.
- La convergencia entre “apps”, internet de las cosas, vehículos no tripulados y las tecnologías emergentes como la “cadena de bloques”.

Convergencia tecnológica

Cuando se habla de convergencia tecnológica se advierte una conexión entre tecnologías informáticas y las de operaciones. Dispositivos que antes sólo funcionaban de forma aislada o con controles localizados, ahora se conectan a redes ip, donde son visibles y manifiestan nuevas posibilidades, tanto para los negocios como para los adversarios. Converger es sintonizar dos realidades y dos mundos para mejorar la experiencia de los usuarios (Ross, Beath & Mocker, 2019).

Con la convergencia tecnológica se inaugura una visión más sistémica de la realidad. Se revelan interacciones que antes estaban ocultas a los ojos de los sistemas de monitorización y control, se aumenta la densidad digital de los objetos físicos. Este aumento de conexión entre mundos inicialmente desconectados establece una nueva gama de servicios y propuestas que se traducen en nuevas oportunidades para los clientes, de contar con productos enriquecidos con datos, que les permiten aprender de sus comportamientos para brindarles cada vez la mejor experiencia.

Con la convergencia tecnológica se crean nuevas capas de flujos de información que aumentan las capacidades de los objetos físicos. Ahora no solamente cumplen con la función para la cual fueron diseñados, sino que cuentan con características inteligentes, para el monitoreo, control, optimización y autonomía (en algunos casos, cuando incluimos elementos de inteligencia artificial), con lo que ahora tenemos una vista emergente de un objeto digitalmente modificado (Porter & Heppelmann, 2014).

Bajo este nuevo paradigma de aumento de densidad digital, los elementos de seguridad y control no solamente cambian, sino que deben reinventarse. Las prácticas conocidas de seguridad y protección basadas en riesgos conocidos, no serán suficientes para reconocer las nuevas posibilidades que la convergencia habilita. Una nueva gama de amenazas emergentes estarán latentes y habrá que explorar nuevos patrones inciertos

que las conexiones y flujos configuran en los objetos.

Frente a esta realidad, varias lecciones aprendidas y retos pendientes:

Lecciones aprendidas
- A mayor densidad digital mayor innovación y mayor exposición.
- La convergencia tecnológica no implica convergencia de vulnerabilidades, sino mutación de las mismas.
- Se revelan vulnerabilidades latentes en el microcódigo del *hardware* de los objetos físicos.

Retos pendientes
- Reconocer que existen afectaciones lógicas que tienen impactos en el mundo físico.
- Analizar y atender las vulnerabilidades inherentes del *hardware* físico que afectan las infraestructuras críticas cibernéticas.
- Valorar en cada objeto físico conectado, un posible punto de acceso no autorizado.

Redes sociales

Con la democratización de la información y una mayor conectividad, las redes sociales tomaron fuerza en esta última década. Los medios sociales encontraron eco en aquellos que querían manifestarse y revelar situaciones que pasaban inadvertidas hasta ese momento. Se convirtieron en una forma de expresión natural de las personas para compartir reflexiones y posturas sobre realidades en diferentes regiones del mundo, como forma de conectar intereses y retos sin distingo de nacionalidades o fronteras (Cobo, 2019).

De igual forma, las redes sociales, con el potencial de propagación masiva, se convirtieron en estrategias de las grandes marcas y empresas, que comenzaron a capturar y analizar la información que se comparte allí, con el fin de establecer tendencias y nuevas formas de conquistar a sus clientes, con ideas o temas que son de interés para ellos, identificados casi que en tiempo real.

Los clientes de igual forma usan ahora las redes sociales para conversar y plantear ideas sobre los productos y/o servicios, así como sobre sus experiencias en el uso de los mismos. Las redes sociales no solo tienen el potencial para viralizar sus comentarios, sino de cambiar o transformar imaginarios de las personas, que sin poco escrutinio o valoración de fuentes, no logran distinguir entre lo que es confiable o no (Ellis & Mohan, 2019).

Las redes sociales son en resumen un medio de expresión y apertura de los sentimientos y percepciones de las personas. Algunas de ellas genuinas y válidas, otras manejadas o dirigidas por intereses, muchas veces oscuros, que buscan propósitos poco claros, con agendas ocultas a la realidad para lograr cambios en los imaginarios de las personas, particularmente aquellas

que poco validan o aceptan como "verdad" todo aquello que se publica por estos medios o en la red (Singer & Brooking, 2018).

En razón con lo anterior, las redes sociales establecen un foco de atención para los marcos de seguridad y control, no para tratar de regular o restringir su uso, sino para hacer conscientes a todas las personas de sus posibilidades y capacidades para transformar la realidad. En este sentido, cuando se trate de usar redes sociales, cualquiera que esta sea, es importante tomarse el tiempo para responder estas cuatro (4) preguntas: (Haidt & Rose-Stockwell, 2019)

- ¿Por qué se quiere publicar?
- ¿Está basado en hechos y datos?
- ¿Conozco y he verificado la fuente de la información?
- ¿Soy consciente que el mensaje se puede propagar de forma exponencial?

Frente a esta realidad, varias lecciones aprendidas y retos pendientes:

Lecciones aprendidas
- Los "me gusta" se han transformado en criterio de aceptación social.
- Existe mayor dependencia de la interacción digital, que debilita el encuentro personal.
- Una estrategia basada en las redes sociales es una forma de congregar y afiliar, o igualmente de dividir y enfrentar.

Retos pendientes
- Reducir el número de cuentas falsas o bots que inundan las redes sociales con propósitos oscuros.
- Disminuir la necesidad de exposición en redes sociales, para evitar el síndrome del narcisista o dependiente digital.
- Controlar la cantidad de información de baja calidad que se comparte en las redes sociales para desinformar a la audiencia.

Asimetría de los ciberconflictos

Si hay algo que haya marcado esta última década es la manifestación de los ciberconflictos entre las naciones. Actividades no autorizadas que buscan pasar desapercibidas en los medios noticiosos, como una forma de desestabilizar empresas, naciones o conglomerados de personas. El uso de la tecnología de información para crear capacidades adversas contra otros, se convierte en una de las estrategias de mayor uso por los países desarrollados generalmente (Green, 2015).

Un ciberconflicto es una confrontación, muchas veces no declarada entre dos o más intereses (que pueden o no ser naciones), con el fin de ganar una posición privilegiada en un contexto específico o debilitar una condición particular de un adversario, incluso pudiendo llevarlo al sometimiento. Este tipo de operaciones, ahora liderada por militares, mercenarios o grupos patrocinados por Estados, establece una nueva forma de agresión que no se reconocen dentro de los es-

tándares naturales de una guerra regular o cinética (Cano, 2018).

Cuando el ciberconflicto aparece, no avisa, no se conoce con claridad el adversario y menos sus capacidades para hacer daño. Es una apuesta muchas veces subversiva y subrepticia que se diseña, se prepara y se ejecuta detrás de un manto de anonimato, que termina en eventos de situaciones posiblemente identificadas, pero que no se puede establecer una atribución específica. El conflicto en el contexto ciber, no es un enfrentamiento regular, sino asimétrico y poco convencional para su tratamiento por los estados y las empresas.

Con los ciberconflictos aparecen nuevas unidades de operación en las fuerzas militares del mundo y el concepto de "acto de guerra" genera diversas tensiones y explicaciones para los académicos, los mandos militares y los organismos multilaterales. Un ciberconflicto demanda de una nación un respeto de su soberanía digital, concepto que aún permanece en las opacidades conceptuales y que poco a poco, se delinea con la experiencia que se ha venido acumulando a lo largo de los años.

Desde el punto de vista de seguridad y control, los ciberconflictos tienen un particular interés, toda vez que las infraestructuras críticas cibernéticas de las naciones como son sistemas aeronáuticos, financieros, logísticos, de emergencia, de energía, de petróleo y gas, de telecomunicaciones, gubernamentales, de la banca central, entre otros, se vuelven objetivos de las operaciones de estos nuevos adversarios para desestabilizar gobiernos o programas específicos y así minar aún más la debilidad política y social de los estados (Cano, 2018).

Basta recordar las implicaciones que se tuvieron en diferentes infraestructuras críticas en diferentes naciones del mundo y los impactos hasta en pérdidas humanas que se hicieron realidad. Si bien para algunos analistas los ciberconflictos, no pasan de ser operaciones informáticas diseñadas para desestabilizar una comunidad, para otros, sí representa una amenaza real de poder llegar a inutilizar o destruir la dinámica social, la estabilidad y prosperidad económica de las naciones. Por tanto, los ciberconflictos se constituyen en sí mismos en una nueva amenaza emergente que toda nación deben tener en su radar para entender su dinámica y por tanto, la manera para poder establecer los ejercicios de simulación requeridos para estar preparados ante esta posible eventualidad (Green, 2015).

Frente a esta realidad, varias lecciones aprendidas y retos pendientes:

Lecciones aprendidas

- La dinámica de un ciberconflicto es distinta a la forma como se materializa un conflicto regular.

- Los actores en los conflictos regulares son conocidos, mientras en los ciberconflictos pueden permanecer anónimos y ocultos.
- Los ciberconflictos pueden pasar como "verdad por negación creíble". Es decir, muchos saben que existen, pero otros niegan su existencia.

Retos pendientes

- Defender la soberanía en el ciberespacio es un nuevo reto para gobernabilidad de los estados.
- Conformar una fuerza de operaciones cibernéticas como fundamento de la soberanía en el ciberespacio es reconocer la extensión del Estado en el contexto digital.
- Transformar y reconocer los derechos humanos en el contexto digital, es habilitar la formación de los ciudadanos para cumplir nuevos deberes y exigir nuevos derechos.

Como se puede observar, la década anterior nos deja importantes aprendizajes en los temas de seguridad, nos sugiere y anticipa nuevos retos, y sobremanera nos advierte sobre las nuevas competencias y conocimientos que debemos desarrollar para afrontar los siguientes diez años. La computación en la nube, la computación móvil, la convergencia tecnológica, las redes sociales y la asimetría de los ciberconflictos se consolidaron como los nuevos normales para las organizaciones y las nuevas formas de interacción entre los ciudadanos y las empresas.

Una mirada crítica al 2019: ¿Quiénes fueron los protagonistas?

El año 2019 termina con una dinámica particular de transición de lo que se ha aprendido en la década y como anticipo de aquello que se verá en la siguiente. Este año cinco (5) temas fueron claves para tener en cuenta: aumento de ecosistemas inseguros, mayor monitorización y vigilancia a nivel global, pérdida de la integridad de la información, aumento de la extorsión con datos y la tibieza de los cuerpos ejecutivos de las empresas frente a los temas de seguridad y control.

Los ecosistemas inseguros se presentan por el aumento de la conectividad de las "cosas" con aplicaciones y sistemas previamente existentes. El incremento del uso de APIs (*Application Programa Interfase*) para conectar temáticas en el mundo físico y crear experiencias antes impensables, motiva patrones de transformación que exigen a las empresas diseñar plataformas ágiles, con componentes adaptables para mejorar el "tiempo al mercado" de sus productos o iniciativas.

Los ecosistemas como conexión de sistemas socio-técnicos: infraestructura, aplicaciones y servicios, establecen el nuevo referente tanto para las empresas como para los individuos, en el momento de

motivar propuestas alternativas o emergentes que ayuden a las personas parar resolver sus problemas de formas distintas y generadoras de valor. Así las cosas, los ecosistemas deben entender que son "inseguros por defecto" y tomar las medidas necesarias para constituir una distinción de confianza digital imperfecta en un futuro cercano (Li & Horkoff, 2014).

De otro lado, las experiencias de Edward Snowden revelan el escenario de monitorización e inteligencia permanente que los gobiernos tienen sobre diferentes aspectos de la vida humana. La necesidad de conocer los detalles de la dinámica de la vida de la persona, invita de forma arriesgada a los gobiernos a tener acceso a las conversaciones y comportamientos de los ciudadanos mancillando de forma concreta y muchas veces grosera, los derechos y libertades humanas en el contexto digital (Snowden, 2019).

De igual forma, las tensiones entre los países por el control del ciberespacio, habilita espacios de confrontación para desplegar operaciones cibernéticas encubiertas para entrar en la dinámica social de otros países y crear acciones violentas o contrarias, que logren desestabilizar a una nación o grupo específico.

En este sentido, se hace necesario desarrollar iniciativas multilaterales para darle un marco de acción y cumplimiento al uso de la información y sobremanera, entrenar a los individuos para aumentar su sensibilidad y mejorar su postura en la protección de su información en un contexto cada vez más agreste e incierto como lo es internet.

Por otro lado, se ha avanzado en el aseguramiento tanto de la disponibilidad como de la confidencialidad de la información, dejando de lado su integridad. Bajo esta indicación, es claro que las redes sociales se han aprovechado de esta ausencia para capitalizar espacios de manipulación de tendencias y posturas de las personas, usando información parcial, inexacta o falsa, para construir imaginarios que se confirman a través medios confiables o masivos como los medios digitales.

Las redes sociales como instrumento natural de reconocimiento de la dinámica social, como elemento natural y expedito para informarse de lo que está sucediendo, no han logrado controlar o asegurar la confiabilidad de la información, la difusión masiva de información falsa o inexacta, ni avanzar en la educación de las personas para su uso adecuado y disminución de la dependencia digital de aprobación de pocos o muchos. Estamos ad portas de una nueva década donde todo indica que será natural consultar cualquier red social para reconocer los cambios en el mundo y cómo éstas, cambian la dinámica de las personas y su encuentro con el otro (Singer & Brooking, 2018).

Si esta dinámica de aprobación y dependencia social se configura como un problema real, igualmente lo es el uso de la extorsión con los datos o lo que comúnmente se denomina *ransomware*. Esta realidad consolidada en 2019, establece una práctica clave de la delincuencia no sólo para obtener ganancias por acceso a la información, sino para revelar aquella que pueda ser de interés para la parte afectada. Por tanto, el *ransomware* se convierte en un "commodity" para los extorsionistas digitales como fuente base de ingresos ocasionado por ausencia de buenos hábitos de seguridad y control.

Frente a este reto, tanto empresas como individuos deben comprender que el atacante no va concentrarse en aquel punto de mayor control y seguridad, sino en esos donde existe menos atención y monitoreo, pues allí puede balancear su ecuación de trabajo, que busca lograr la mayor eficiencia de sus acciones (y por tanto mayor ganancia) con el menor esfuerzo y exposición de sus acciones (Saydjari, 2018). El *ransomware* es una realidad que se materializa cada vez que olvidamos la inevitabilidad de la falla.

Finalmente y no menos importante, se puede ver con mayor claridad cierto interés de los cuerpos ejecutivos sobre los temas de ciberseguridad. Al parecer las noticias y los eventos que afectaron la reputación de grandes empresas en diferentes sectores, llamaron la atención de estos perfiles para lograr incluir en parte de sus agendas estos temas. Sin perjuicio de esta realidad, aun no se cuenta con una decidida participación de los equipos gerenciales en los temas de ciberseguridad (Coburn, Leverett & Woo, 2019). Habrá que esperar a que, como generalmente ocurre, algo suceda para que la "reacción" se dé y no, como debe ser, "anticipar" antes de que se materialice un evento adverso.

En este sentido, es necesario actualizar y educar los imaginarios de los ejecutivos de las empresas, de tal manera que se pueda dar respuesta a sus interrogantes más frecuentes, y así concretar una inmersión en el modelo y programa de ciberseguridad que los lleve a conectar con los planes estratégicos de la empresa, y cómo construir una organización más resiliente y resistente frente los diferentes eventos conocidos y desconocidos que va a enfrentar la organización en un futuro cercano (Linkov & Trump, 2019).

Esta mirada crítica al 2019, es una oportunidad para reconocer lo que debemos aprender y descubrir de aquellas cegueras cognitivas que son relevantes para superar, habida cuenta que con un avance acelerado de nuevos sistemas sociotécnicos e incorporación de inéditas propuestas tecnológicas, cada vez más perderemos la vista global, por las nuevas distracciones y

experiencias que éstas proponen. 2019 será recordado por la versatilidad y reinvención del adversario en los sistemas socio-técnicos, así como el reconocimiento por parte del analista de la gestión de riesgos del adversario que en ningún caso es cero (Saydjari, 2018).

Reflexiones finales

Lo que ha pasado en una década en los temas de seguridad y control demanda un ejercicio de arqueología digital especializada que no es el objetivo de esta reflexión. Más bien, lo que se busca es plantear algunos puntos de interés y coincidencia con la dinámica empresarial y global, para analizar las lecciones aprendidas y los retos pendientes que se ven a futuro.

Una lección aprendida es lo que asume y capitaliza un analista con el éxito de un adversario. Con el aumento de la superficie de ataque vía la conectividad, la movilidad y la convergencia, los atacantes cuentan con un espacio de interacción y experimentación más amplio, en el que se pueden aprovechar de relaciones documentadas o no documentadas, que ponen a prueba los mecanismos de seguridad y control disponibles y desplegados en las organizaciones (Funston & Wagner, 2010).

Cada lección aprendida durante la última década para los analistas tiene algunos patrones concretos para tener en cuenta. Dichos patrones, han sido identificados en diferentes eventos que se manifestaron durante los pasados diez años bajo los siguientes parámetros:

- Mayor conectividad y flujo de datos en la nube tensiona la agilidad con la confiabilidad.
- Mayor convergencia tecnológica tensiona la eficiencia y la gestión de vulnerabilidades.
- Mayor interacción social e información instantánea tensiona la integridad de la información y la comunicación abierta.
- Mayor asimetría de la información tensiona los derechos humanos y las realidades geopolíticas.
- Menor atención ejecutiva a los retos de ciberseguridad tensiona los retos estratégicos de las empresas y las propuestas de productos/servicios innovadores.

Así las cosas, los retos estratégicos de las compañías, así como los de los responsables de la seguridad y el control en las empresas, encuentran puntos de contacto que deben comprender y analizar, no como fenómenos mutuamente excluyentes, sino como dinámicas conectadas para visualizar y comprender la complejidad inherente de estos retos, cuyo resultado no puede ser otro que una vista enriquecida de la realidad empresarial (Sridhar, 2019).

En consecuencia, las lecciones aprendidas de ésta última década

deben configurar un cuerpo de conocimiento que permita ver patrones hacia adelante y, establecer una nueva agenda conjunta entre el negocio y los ejecutivos de ciberseguridad, para anticipar y actuar con un plan de acción propositivo (Day & Schoemaker, 2019); es decir, que no espere a ser atacado, sino que descubra los movimientos del oponente en su propio terreno, creando el incierto que debilite la gestión de riesgo del adversario, generando una ganancia teórica y práctica para la seguridad y el control de la organización.

Referencias

Brodsky, L. & Oakes, L. (2017). Data sharing and open banking. *Mckinsey Insights*. Recuperado de: https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking

Cano, J. (2018). Cyberconflicts: Reflections and Implications for Today's Enterprises. *ISACA Journal*. 4.

Cobo, C. (2019). *Acepto las Condiciones: Usos y abusos de las tecnologías digitales*. Madrid, España: Fundación Santillana.

Coburn, A., Leverett, E. & Woo, G. (2019). *Solving Cyber risk. Protecting your company and society*. Hoboken, NJ. USA: John Wiley & Son.

Day, G. & Schoemaker, P. (2019). *See sooner act faster. How vigilant leaders thrive in an era of digital turbulence*. Cambridge, MA. USA: MIT Press.

Ellis, R. & Mohan, V. (Editors) (2019). *Rewired. Cybersecurity Governance*. Hoboken, NJ. USA: John Wiley & Sons.

Funston, F. & Wagner, S. (2010) *Surviving and Thriving in uncertainty. Creating the risk intelligent Enterprise*. Hoboken, NJ. USA. John Wiley & Son.

Garrison, J. & Nova, K. (2018). *Cloud Native Infrastructure. Patterns for Scalable Infrastructure and Applications in a Dynamic Environment*. Sebastopol, CA. USA: O'Really.

Green, J. (Editor) (2015). *Cyber Warfare. A multidisciplinary analysis*. New York, NY. USA: Routledge.

Haidt, J. & Rose-Stockwell, T. (2019). The Dark Psychology of Social Networks. Why it feels like everything is going haywire. *The Atlantic*. Diciembre. Recuperado de: https://www.theatlantic.com/magazine/archive/2019/12/social-media-democracy/600763/

Li T. & Horkoff J. (2014). Dealing with Security Requirements for Socio-Technical Systems: A Holistic Approach. En: Jarke M. et al. (eds) (2014) *Advanced Information Systems Engineering. CAiSE 2014. Lecture Notes in Computer Science*, vol 8484. Springer. Doi: https://doi.org/10.1007/978-3-319-07881-6_20

Linkov, I. & Trump, B. (2019) *The science and practice of resilience*. Switzerland: Springer Verlag.

Mendoza, M. (2014). Seguridad en la nube para empresas: ¿qué son los CASB? *ESET Security*. Recuperado de: https://www.welivesecurity.com/la-es/2014/09/24/seguridad-nube-empresas-que-son-casb/

Porter, M. & Heppelmann, J. (2014) How Smart, connected products are transforming competition. *Harvard Business Review*. Noviembre.

Ross, J., Beath, C. & Mocker, M. (2019*). Designed for digital. How to architect your business for sustained success*. Cambridge, MA. USA: MIT Press.

Saydjari, O. (2018). *Engineering trustworthy systems: get cybersecurity design right the first time*. New York, USA.: McGraw Hill

Singer, P. W. & Brooking, E. (2018). *Likewar. The weaponization of social media*. Boston, MA. USA: Houghton Mifflin Harcourt.

Snowden, E. (2019). *Vigilancia permanente*. Bogotá, Colombia: Editorial Planeta.

Sridhar, V. (2019). *Emerging ICT Policies and Regulations. Roadmap to Digital Economies*. Singapore: Springer Nature Singapore.

***Jeimy J. Cano M., Ph.D, CFE, CICA**. Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes. Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Ph.D en Business Administration por Newport University, CA. USA. y Ph.D en Educación por la Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista Sistemas de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*