Arquitectura resiliente empresarial

DOI: 10.29236/sistemas.n156a6

Una visión corporativa y prospectiva al 2025.

Resumen
Comprender la evolución acelerada de las organizaciones en el contexto de un escenario digital, significa actualizar las reflexiones empresariales respecto de las promesas de valor y los retos que imponen las nuevas expectativas de los clientes y las tecnologías emergentes. En este sentido, más allá de la continuidad del negocio, es necesario desarrollar una arquitectura resiliente empresarial que les permita tomar mayores riesgos, de manera de incorporar capacidades clave para proteger el modelo de generación de valor en escenarios cada vez más inestables y volátiles. Por lo tanto, este documento desarrolla una mirada prospectiva con distintos futuros posibles para esta arquitectura, con el fin de que las compañías cuenten con un referente base para tomar las decisiones requeridas, de cara al reto de la transformación digital que ellas enfrentan en la actualidad.

Palabras clave
Resiliencia, arquitectura, prospectiva, ciberseguridad, transformación digital

Introducción

El avance acelerado de la cuarta revolución industrial y la convergencia tecnológica entre lo físico, lo lógico y lo biológico establecen un nuevo escenario de reflexión y de negocios, que demanda una lectura enriquecida de la realidad. Esta nueva realidad establece un conjunto de exigencias y retos que están más allá de las prácticas de gobierno de tecnología de información y comunicaciones actuales, las cuales ahora deben ser leídas y reinterpretadas en un escenario ciberfísico, donde existe un aumento creciente de densidad digital, flujos de información conocidos y emergentes, y una mayor conectividad en diferentes contextos (Fatima, Anjum, Malik & Ahmad, 2020).

El entorno ciberfísico plantea una ruta diferente de comprensión de los retos empresariales, comoquiera que las organizaciones, no solo deberán estar atentas a que los clientes puedan concretar experiencias novedosas y agilizar sus actividades, sino que cualquier falla en este entorno puede llegar a afectar la integridad de la persona o brindarle información inexacta que la lleve a tomar decisiones inadecuadas. En este sentido, las condiciones de seguridad y control en lo ciberfísico se mueven entre los principios básicos de confidencialidad, integridad y disponibilidad, pasando por el "*safety*" (propio de la disciplina operativa en ambientes industriales) hasta llegar a la confiabilidad del dispositivo (Avizienis, Laprie, Randell & Landwehr, 2004).

En consecuencia, los entornos ciberfísicos demandan un panorama de seguridad y control con una vista de resiliencia y confiabilidad donde la gestión de riesgos tradicional basado en "cero riesgo" y "seguridad cien por ciento", se transforma en una lectura de umbrales de operación (IIA, s.f.) donde, tanto el proveedor del producto o servicio como los clientes, están involucrados todo el tiempo para hacer realidad la expectativa del usuario en esa experiencia emergente fruto de la convergencia tecnológica.

Así las cosas, es necesario plantear una vista prospectiva que permita tanto a las organizaciones como a sus proveedores, establecer patrones de transformación de mediano y largo plazo, con el fin de consolidar una ruta de resiliencia y confiabilidad basada en al menos cuatro estrategias clave: anticipación, prevención, detección y tolerancia (Saydjari, 2018), las cuales sirvan como marco de observación y reflexión para avanzar hacia el reconocimiento y puesta en operación de una nueva cultura organizacional, ya no sólo basada en proteger, sino en defensa, anticipación y fiabilidad.

Por tanto, este documento plantea y desarrolla un escenario prospectivo para una arquitectura resiliente empresarial, que permita a las empresas visualizar un posible camino de evolución para ajustarse a los retos que le plantea la cuarta revolución industrial, y así preparar la dinámica corporativa y la cultura organizacional para romper con la inercia que se trae de los marcos conocidos y prácticas estándares, con el fin de alinear la corporación con los desafíos que impone un contexto digital acelerado, con ecosistemas digitales, distintos actores, adversarios desconocidos y exigencias que aún no llegan (Ponemon, 2020).

Marco general de la prospectiva

Al desarrollar un ejercicio de prospectiva no se busca "predecir" el futuro, sino establecer posibles futuros alternativos para visualizar y desarrollar.

Es una manera de explorar y analizar las tendencias y señales emergentes que se advierten en el entorno y con ello trazar un mapa sobre un territorio inexplorado para identificar caminos que lleven a la organización a lograr una posición estratégica anticipada desde la ventana de tiempo actual (Hines & Bishop, 2015).

Los retos prospectivos implican la revisión y análisis de diferentes tendencias políticas, económicas, sociales, tecnológicas, legales y ambientales, con lo cual no es una tarea fácil establecer el marco de trabajo base para construir la propuesta de visión de futuro. Para el desarrollo del ejercicio, el contexto es fundamental por lo que muchos detalles deben ser consolidados y simplificados para darle forma a lo que podría ser las señales más relevantes que permitan delinear algo de lo que puede ocurrir en el mediano y largo plazo (Weick & Sutcliffe, 2007).

La prospectiva es una práctica de anticipación encaminada a crear mapas de ruta para que las empresas cuenten con orientación sobre aspectos específicos de su interés, basada en información confiable, cierta y veraz, y al mismo tiempo en apuestas especulativas y exploratorias que científicos o tanques de pensamiento pueden hacer respecto de los temas de interés de la organización.

Cuando se desarrolla una prospectiva no se buscan certezas, sino respuestas parciales e incompletas, que la organización en el desarrollo mismo de sus actividades, le da forma para ir visualizando aquello que se establece en el mapa de ruta. No es un objetivo que permanece inmóvil todo el tiempo, sino que puede tener cambios por las inestabilidades que afectan el contexto.

Dichos cambios tendrán mayor o menor impacto dependiendo de nivel de la inestabilidad o volatilidad de la tendencia que se identifique

en el sector particular de negocio o a nivel global (Popper, 2008; Menon & Kyung, 2020).

Particularmente el resultado de los análisis desarrollados alrededor de la arquitectura resiliente empresarial, busca coordinar y orquestar diferentes tendencias y retos que se tienen en la actualidad desde la seguridad de la información, la ciberseguridad, la privacidad, la resiliencia, la confiabilidad y la operación de las infraestructuras, con el fin de delinear una vista enriquecida del nuevo estándar de gestión que las empresas deben asumir, para desinstalarse de las certezas y respuestas conocidas del entorno.

Los resultados que se presentan a continuación fruto de la revisión de patrones emergentes y señales débiles del ambiente, que se han identificado luego de la inmersión y correlación de diferentes documentos, reportes y artículos en las temáticas previamente mencionadas para darle forma a la visualización de la arquitectura resiliente empresarial, plantea una visión de evolución futura que permite a las organizaciones advertir los retos, riesgos y oportunidades que deben apropiar al transformar la gestión de riesgos en una práctica de umbrales, tolerancia y pronóstico distinta a la lectura vigente basada en certezas y análisis causa-raíz.

Arquitectura resiliente empresarial, una revisión conceptual

Una arquitectura resiliente empresarial no es un concepto que habla de invulnerabilidad, sino de la capacidad que tiene una organización de evolucionar y adaptarse en escenarios volátiles, inciertos, complejos y ambiguos, expuesta a amenazas y riesgos emergentes con adversarios conocidos y desconocidos, para lo cual diseña, configura y armoniza cuatro estrategias básicas: anticipación, prevención, detección y tolerancia, que definen la manera como la organización navega, entiende y da respuesta a los cambios e inestabilidades de su entorno (Saydjari, 2018).

Esta capacidad demanda desinstalarse de las certezas, asumir aquello que no sale como estaba previsto como una oportunidad de aprendizaje y explorar todo el tiempo el contexto para comprender qué es lo que hace fallar las medidas de control, y no buscar culpables en las personas, dado que la inevitabilidad de la falla es aquello que es esperado en ellas (Woods, Dekker, Cook, Johannesen & Sarter, 2010).

De esta forma, se advierte una lectura de la dinámica de la operación como un ejercicio de umbrales, que inicia con el apetito al riesgo que la compañía declara frente a su estrategia, que luego se enmarca en un nivel de tolerancia, donde la organización se mueve de forma cómoda frente al escenario adverso y que termina en una capacidad de

riesgo que declara el máximo nivel exposición que la organización puede soportar (IIA, s.f.; GAO, 2016).

La estrategia de anticipación busca establecer oportunidades y ventanas de acción previas para manejar las situaciones adversas y definir marcos de actuación concretos que habiliten a la organización avanzar en medio del evento incierto, en ese momento no conocida para el entorno, pero visualizada y analizada por adelantado en la empresa, con el mínimo de inciertos y consecuencias. La estrategia de anticipación nuevamente no es una predicción, sino un pronóstico, una lectura en contexto de las tendencias e información disponibles para avanzar donde otros no saben cómo hacerlo.

La estrategia de prevención está situada en la zona de los datos y la revelación de situaciones potencialmente agresivas contra la esencia de los objetivos empresariales. Esta estrategia se funda en propuestas basadas en analítica de datos, valoración y análisis de riesgos conocidos y latentes (Cano, 2017), identificación de patrones y prácticas concretas en las personas que movilizan esfuerzos en aquellas zonas grises que la organización tiene.

La estrategia de detección es la manera tradicional como la organización identifica que alguna situación particular no concuerda con los estándares normales. Esto se traduce en la activación de las alertas y mecanismos de bloqueo de la situación que genera la amenaza.

La detección será más efectiva mientras se cuente con mayor conocimiento del riesgo o amenaza y podrá afinarse su efectividad, en la medida que se tenga mayor información y se ajuste su operación.

La estrategia de tolerancia es la definición de los umbrales de operación permitidos frente al evento incierto. Son todos aquellos mecanismos que brindan tiempo extra a la empresa en medio de la adversidad y que no podrá sobrepasar la capacidad de riesgo definido por la organización.

Arquitectura Resiliente Empresarial. Prospectiva al 2025

Considerando los elementos conceptuales establecidos en la sección anterior, se presenta a continuación la visión prospectiva de la arquitectura resiliente empresarial al 2025, que se explicará en la Figura 1.

La prospectiva realizada se basa en la transformación digital que las empresas están desarrollando y que terminará cambiando la manera como hacen las cosas en un entorno hiperconectado, hiperautomatizado e hiperaumentado, en el cual las amenazas y tensiones emergentes mutarán y por tanto, habrá menos certezas para abor-

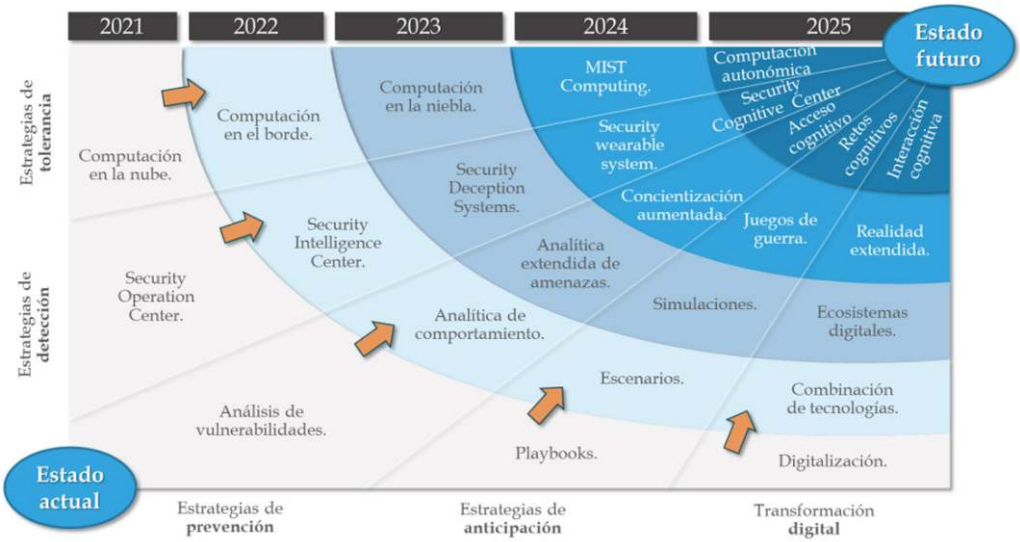

Figura 1 Arquitectura Resiliente Empresarial - Prospectiva 2025 (Elaboración propia)

dar situaciones cada vez más inesperadas (Valdez-de-León, 2019).

La presentación de la prospectiva por las estrategias definidas es acumulativa, es decir cumplir con lo establecido para un año, significa incorporarlo en el año siguiente y avanzar con la puesta en operación de la siguiente propuesta detallada. Así para la estrategia de anticipación, se inicia con los *playbooks* en el 2021 y en el 2022, la idea es madurar en la práctica anterior y evolucionar hacia los escenarios.

Estrategia de anticipación

La evolución que se plantea para las estrategias de anticipación se basa en la reducción de incierto en las actuaciones de las empresas. Los *playbooks* se configuran como los libros de trabajo permanentes donde las organizaciones se preparan para actuar frente a eventos conocidos (o semejantes) con el fin de establecer el marco de acción requerido para minimizar los posibles impactos del incidente que se tiene en la empresa, de esta forma asegura un adecuado tratamiento del evento y el marco de debido cuidado requerido frente a sus grupos de interés (Kick, 2014).

Los escenarios se plantean como el siguiente paso en esta estrategia. Los escenarios son ejercicios de construcción colectiva, basados en reflexión y análisis, que buscan establecer situaciones posibles y probables para las organizaciones con el fin de indagar en las tendencias y retos emergentes de la empresa y cómo ésta debe maniobrar en el momento que corresponda (Hines & Bishop, 2015). El caso más relevante de aplicación de es-

te ejercicio son los logros de equipo ejecutivo de Shell Corp. en la década de los sesenta cuando plantearon el escenario de la caída de precios del petróleo en 1973 y detallaron las diferentes acciones para sortear este momento, lo que les permitió actuar con claridad en medio de las inestabilidades de aquella situación.

Madurar en la práctica de *escenarios* establece la transformación de la empresa y su equipo ejecutivo para avanzar en el incierto. De igual forma, el siguiente paso propuesto es irrumpir en un mayor apetito al riesgo que necesariamente implica moverse al dominio de las simulaciones, donde lo importante es observar y determinar los comportamientos, riesgos, retos y resultados de las propuestas novedosas para la organización (Popper, 2008). Es importante aclarar, que no se tendrán todas las respuestas, sino el marco general de comprensión de lo que puede ser y los posibles impactos que se pueden presentar.

Luego de las *simulaciones*, que buscan no solamente enfrentarse al incierto, sino comprender la complejidad de las situaciones que se ven hacia adelante, se llama a una incorporación de un ejercicio denominado juegos de guerra. Los juegos de guerra son juegos de estrategia propios del entorno militar, donde se reconocen actores particulares, con capacidades específicas para movilizar acciones que puedan afectar a su contraparte (Alkire, Lingel & Hanser, 2018). En el entorno empresarial, implica conocer la dinámica de los negocios y los diferentes participantes de su sector, para que la empresa se mantenga en modo "radar" es decir, explorando e identificando aspectos de su entorno digital para capitalizar como oportunidad o reconociendo posibles amenazas para actuar de manera anticipada y aumentar su capacidad de respuesta ágil y efectiva.

El siguiente nivel en la evolución planteada para esta estrategia se funda en los recientes avances del uso de algoritmos de aprendizaje (supervisados y no supervisados) los cuales son capaces de plantear retos cognitivos, que configuran combinaciones de escenarios y situaciones basados en lógicas conocidas y aleatorias, creando contexto inciertos e inesperados para tratar de advertir situaciones que aún no se desarrollan o insinúan en las mejores estimaciones (Cano, 2020). Este tipo de rutinas de prospectiva cognitiva, asistida por algoritmos debe pasar primero por ejercicios de simulación para establecer sus posibilidades y limitaciones, y así establecer sus posibles usos y capacidades de cara a los desafíos que enfrentarán las organizaciones en la industria 4.0 y su transición hacia la sociedad 5.0

Estrategia de prevención

La prospectiva planteada en esta estrategia busca identificar en marcos de tiempo cortos aquellas si-

tuaciones que pueden desestabilizar rápidamente la organización y afectar sus operaciones. En este sentido, los temas de seguridad y control advierten momentos que pueden llegar a afectar los planes de las empresas y generar controversias que terminen afectando la estrategia de la compañía.

El *análisis de vulnerabilidades* como práctica conocida en seguridad, es un ejercicio de cierre de brechas identificadas. Las herramientas disponibles sobre este tema cuentan bien con firmas de ataques o algunas heurísticas que pueden generar condiciones de error o falla que implique revisar en detalle tanto el software como el hardware. Una práctica madura de análisis de vulnerabilidades debe estar asistida por la gestión de las fallas identificadas y el aseguramiento de los parches que se necesitan para cerrar las limitaciones que se advierten (Pillay, 2019).

Un segundo momento de la evolución es avanzar con la *analítica de comportamiento*. Este paso supone contar con sensores y formas de recoger las actuaciones de las personas, procesos o aplicaciones en la organización, de tal forma que se puedan establecer patrones de comportamiento concretos y advertir desviaciones sobre lo que inicialmente puede estar ocurriendo (Addae, Sun, Towey et al., 2019). Es importante advertir que los comportamientos pueden ser de diferente índole, desde la cadencia para escribir en el teclado, dinámica de acceso a las aplicaciones, archivos más consultados, aplicaciones más utilizadas, tráfico menos común o tendencias en utilización de procesamiento o almacenamiento en disco. La analítica de comportamiento genera alertas para atender y actuar en consecuencia.

La *analítica extendida de amenazas* es un momento de quiebre en la estrategia de prevención. Esta tendencia introduce la convergencia entre la inteligencia de amenazas y las amenazas inteligentes. Mientras la inteligencia de amenazas evalúa, integra, analiza e interpreta los datos que ha reunido, para establecer un panorama concreto al que puede enfrentarse la organización en corto y mediano plazo, las amenazas inteligentes establecen el uso adversarial de la inteligencia artificial para retar los mecanismos de seguridad y control disponibles, con el fin de crear entornos de ataque por fuera de los análisis de los datos disponibles o posiblemente alterados por algoritmos diseñados para tal fin (Yampolskiy, 2017).

La *concientización aumentada* se traduce en el uso de las experiencias del mundo aumentado por la realidad virtual, la realidad aumentada y la realidad mixta, para conectar mejor la experiencia de una persona frente al ejercicio de protección y aseguramiento de la información. Esta nueva propuesta puede bien sumergir al individuo en un

escenario completamente virtual donde puede interactuar, ver objetos simulados y los efectos de sus actuaciones, o tomar la realidad y complementarla con objetos virtualizados creando una sensación de inmersión en un escenario real donde puede ver los efectos de sus acciones, o unir los dos conceptos anteriores para facilitar una experiencia aumentada según la necesidad que se plantee por la organización (Carmigniani, Furht, Anisetti et al., 2011).

El *acceso cognitivo* es una nueva frontera donde en un contexto asistido por ecosistemas digitales, geolocalización y controles de acceso basados en biometría avanzada, una persona puede ser reconocida por un algoritmo y establecer de forma automática el perfil de acceso que requiere, cruzando los datos disponibles a la fecha. Este tipo de algoritmos de aprendizaje, por lo general supervisados, debe cuidar su fase de entrenamiento para configurar adecuadamente la estrategia de acceso bien a instalaciones físicas, aplicaciones o infraestructuras tecnológicas. La dependencia y retos que implica basar el control de acceso a este tipo de tecnologías deberán primero pasar por los ejercicios de simulación para detallar mejor las implicaciones positivas, así como sus limitaciones y retos.

Estrategia de detección

La detección supone contar con información suficiente para analizar y establecer patrones de acción que permitan levantar alertas, bien basados en firmas de ataques o vulnerabilidades conocidas, lo que actualmente desarrolla un SOC (*Security Operation Center*). Este tipo de servicios observan en tiempo real eventos, identifican desviaciones sobre patrones conocidos, que permiten reaccionar una vez confirmada la anomalía siguiendo un conjunto de reglas previamiente definidas (Jacobs, Arnab & Irwin, 2013).

La evolución de este tipo de servicios se mueve al SIC (*Security Intelligence Center*) donde se adelanta identificación de patrones emergentes, analítica de eventos inusuales en tiempo real, con una perspectiva más proactiva y basado en heurísticas. Esta nueva posibilidad permite a las organizaciones avanzar en una detección anticipada de posibles amenazas y desarrollar una capacidad de acción preventiva más eficiente y concreta de cara a los retos de nuevos productos y servicios que la organización desea desplegar en el contexto digital.

Los sistemas de engaño (*Deception Systems*) tienen como propósito crear un escenario de mayor incierto para el adversario, una estrategia que busca recrear un entorno simulado muy cercano a la realidad y sus condiciones, para que el atacante trate de ingresar y desde allí estudiar con detenimiento sus movimientos y estrate-

gias. Las tecnologías de engaño requieren un nivel de madurez y desarrollo de la infraestructura tecnológica, así como una gestión de seguridad y ciberseguridad basada en una postura defensiva, la cual se traduce en demorar al atacante antes de que tenga éxito (Wang & Lu, 2018).

La detección deberá migrar para incorporarse no solamente a la infraestructura corporativa sino al mundo físico de la ropa inteligente u objetos vestibles, con tecnologías de seguridad para vestibles (*security wearable systems*). El aumento de la densidad digital para transformar el mundo tangible y visible, establece un referente de transformación digital que buscan agregar nuevas funcionalidades a diferentes objetos del mundo real para crear condiciones aumentadas y con inteligencia que hagan más atractivos estos objetos. Camisetas, gafas, relojes, pañales, chaquetas autoajustables, zapatos deportivos, entre otros, con inteligencia artificial incorporada, establece una nueva frontera en la detección y alerta de seguridad y control. El mundo estará ahora con efectos concretos y reales de las posibles fallas del software o el hardware de forma más evidente.

En la frontera de la evolución se introduce el concepto de SCC (*Security Cognitive Center*), que ya no sólo incorpora los retos propios del SOC y del SIC, sino de los nuevos objetos vestibles, para desarrollar escenarios emergentes, ejecutar simulaciones de ataques inusuales, aprender de la dinámica del entorno y configurar pronósticos de amenazas, donde los algoritmos de inteligencia artificial son los protagonistas.

Este nuevo concepto implica reconocer las tasas de error de los algoritmos que se implementen, así como el desarrollo de una contrainteligencia cognitiva que permita validar que los programas diseñados se ajustan a los diseños establecidos y sus estrategias de aprendizaje se mantienen dentro de los parámetros programados.

Estrategia de tolerancia

La tolerancia implica poder tener opciones para responder en medio de tensiones y acciones agresivas sobre la infraestructura o procesos de la empresa. Esto es, mecanismos diseñados para recuperar y restaurar las funcionalidades críticas luego de un ataque exitoso (Jackson, 2009). En este contexto, *la computación en la nube* se ha convertido en un elemento base de las empresas del siglo XXI donde se toma una decisión informada para trasladar las capacidades de procesamiento y almacenamiento a un tercero, que generalmente con bajo costo, mantiene y asegura la información de las empresas basado en un esquema de contratación elástico que se traduce en “cobro por uso” y manejo de umbrales disponibles y acordados (Velte, Velte & Elsenpeter, 2010).

Si bien la computación en la nube se ha consolidado como un marco de trabajo base para las empresas, empieza un nuevo avance hacia la *computación en el borde*. Esta nueva computación que se incorpora por el aumento de dispositivos inteligentes conectados y enlazados con aplicaciones en la nube, los cuales serán accedidos desde dispositivos móviles (Zalewski, 2019). La *computación en el borde* no son nuevos dispositivos, es una decisión de arquitectura que busca disminuir la latencia de conexión y aumentar la capacidad de procesamiento para lograr la experiencia requerida al interactuar con un objeto con mayor densidad digital. Esta nueva apuesta, más allá de la nube, establece una vista de confiabilidad que demanda un alto nivel de tolerancia para asegurar que los datos estén más cerca de los usuarios y permitir una mayor velocidad de las aplicaciones (Overby, 2020).

La *computación en la niebla* es un concepto de una estructura de red que se extiende desde los bordes exteriores de la organización donde se crean los datos hasta dónde se almacenarán, ya sea en la nube o en el centro de datos de un cliente. Es una capa de conectividad extendida que permite acelerar la conexión con baja latencia, para luego conectarse con el sitio en la nube donde están los datos. En general se establecen diferentes nodos interconectados que mantienen la conectividad, con el fin de disminuir el ancho de banda requerido y así acelerar la respuesta de las aplicaciones para lograr una experiencia en tiempo real. Este paradigma de computación, advierte retos de seguridad y control que deberán asegurarse de cara a su incorporación y soporte en el futuro (Yahuza et al., 2020; Tozzi, 2020).

La *computación por bruma* (*MIST Computing*) es el siguiente paradigma que la organización deberá entender, comprender e incorporar. Esta computación es el extremo de una red, típicamente compuesta de microcontroladores y sensores. Utiliza microcomputadoras y microcontroladores para alimentar los nodos de computación de la niebla y potencialmente seguir adelante hacia los servicios de computación centralizados (en la nube). Dos objetivos clave de la computación por bruma son:

- Permitir la recolección de recursos mediante capacidades de computación y comunicación disponibles en el propio sensor.
- Permitir que los cálculos arbitrarios sean aprovisionados, desplegados, administrados y monitoreados en el propio sensor (Radiocrafts, 2019).

En pocas palabras, la computación por bruma está cerca de los dispositivos inteligentes de los usuarios para procesar sus flujos de información, desarrollar analítica de datos y habilitar mecanismos que aseguren su privacidad.

Finalmente, se advierte el desarrollo de una propuesta de computación que en su diseño y configuración implica materializar la resiliencia computacional de una máquina. La *computación autónoma* (o autonómica) propuesta por Paul Horn de IBM en 2001, se refiere a las características de autogestión de los recursos informáticos distribuidos, que reconocen y comprenden los cambios en el sistema, con el fin de tomar las medidas correctivas apropiadas de forma automática, con mínima intervención humana. Las características de este tipo de computación según IBM son: (Gibbs, 2002)

- Poseen un sentido de sí mismos.
- Se adaptan a los cambios en su entorno.
- Se esfuerza por mejorar su rendimiento.
- Se reparan cuando advierten un daño.
- Se defienden contra adversarios.
- Intercambia recursos con sistemas poco familiares.
- Se comunica a través de estándares abiertos.
- Anticipan las acciones de los usuarios.

Lograr configurar una computación autónoma implica reconocer inteligencia avanzada en las máquinas, que les permite mantener un nivel de monitorización y pronóstico automatizado que limita y anticipa el deterioro del mismo sistema, de tal manera que la intervención humana se limita a actividades de mantenimiento de la infraestructura en sí misma, dejando la evolución y aseguramiento del sistema a la lógica y capacidad resiliente inherente al diseño del sistema mismo.

Esta vista evolutiva de la tolerancia incorpora capacidades inteligentes tanto en la infraestructura como en el software de las máquinas para mantener la conectividad, el procesamiento y las aplicaciones en condiciones óptimas de uso y despliegue, facilitando su escalamiento y aseguramiento en mediano y largo plazo.

Si bien, muchas de estas promesas están en desarrollo y ya se cuentan con avances sustanciales, las organizaciones deberán ejecutar prototipos para aprender de las dinámicas de estos nuevos paradigmas de la computación que pronto estarán disponibles y abiertos para las empresas que se muevan hacia entornos más digitales y tecnológicamente modificados.

Reflexiones finales

Entender los nuevos entornos de negocios mediados por contextos tecnológicamente modificados y con ecosistemas digitales, es comprender que las promesas de valor se transforman y cambian de manera acelerada por las exigencias de experiencias distintas por parte de los clientes. En consecuencia, las organizaciones deberán tomar cada vez más riesgos para asegurar las capacidades requeridas que

den cuenta con los retos que implica ser cada día más digital y menos análogo (Stafford & Schindlinger, 2019).

En este escenario, las empresas estarán más interconectadas y visibles al mundo, lo cual implica mayores oportunidades para ser parte de apuestas de productos y servicios novedosos, así como parte de proyectos conjuntos que buscan crear espacios de co-creación claves para lograr innovaciones que cambien la manera de hacer las cosas. Así las cosas, la colaboración y conexión entre las diferentes organizaciones participantes, hará que se requiera un acoplamiento e interacción entre las infraestructuras, aplicaciones y datos para concretar los nuevos desarrollos esperados (Fatima, Anjum, Malik & Ahmad, 2020).

Por lo tanto, habrá una mayor exposición de las compañías y por ende un espacio de acción para actividades no autorizadas y la aparición de adversarios, que pueden capitalizar las limitaciones y riesgos propios de esta mayor conectividad, interacción y acoplamiento (Denyer, 2017). Cuanto mayor sea la apertura e interacción, el uso de tecnología abiertas y en manos de terceros, menos control se tendrá sobre el aseguramiento de las mismas y por tanto, la capacidad de respuesta ante eventos inesperados deberá ser la norma que guíe la relación con sus terceros de confianza.

La arquitectura resiliente organizacional deberá ser una norma base de las empresas en los próximos diez años, comoquiera que no hacerlo, la expone a un amplio abanico de posibilidades actuales y futuras, que pueden ser aprovechadas por agentes agresores, para impedir la exploración de oportunidades de negocio, creando un impuesto digital al desarrollo empresarial que se verá materializado en la explotación de vulnerabilidades y brechas que deteriorarán la reputación corporativa, marginando a la compañía de nuevos negocios o apuestas innovadoras (Dupont, 2019).

Contar con una arquitectura resiliente empresarial es apostarle a la viabilidad de la empresa en el contexto digital, es construir una red de protección y aseguramiento con los terceros de confianza y reconocer que, a pesar de las condiciones de operación y acuerdos clave efectuados con los proveedores, la inevitabilidad de la falla estará presente y tendrá que atender los incidentes que se manifiesten, para lo cual la mencionada arquitectura deberá dar los lineamientos y posibilidades claras para responder con claridad en medio de la incertidumbre y la inestabilidad que pueda ocasionar un evento inesperado.

La prospectiva planteada en este documento es una visión de posibles futuros que las organizaciones pueden revisar para avanzar hacia una sociedad cada vez más digital,

con distintos actores y nuevas demandas sociales, de manera que cada empresa revise las diferentes rutas y tome las decisiones que sean del caso, teniendo en cuenta cómo evoluciona su apetito al riesgo en medio de un aumento exponencial de la densidad digital en su entorno de negocio.

Referencias

Addae, J.H., Sun, X., Towey, D. et al. (2019) Exploring user behavioral data for adaptive cybersecurity. *User Model User-Adap Inter*. 29. 701–750. Doi: 10.1007/s11257-019-09236-5

Alkire, B., Lingel, S. & Hanser, L. (2018). A Wargame Method for Assessing Risk and Resilience of Military Command-and-Control Organizations. *Rand Corporation*. Doi: 10.7249/TL291

Avizienis, A., Laprie, J., Randell, B. & Landwehr, C. (2004). Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing*. 1(1). 11-33. Doi: 10.1109/TDSC.2004.2

Cano, J. (2017). The AREM Window: A Strategy to Anticipate Risk and Threats to Enterprise Cyber Security. *ISACA Journal*. 5.

Cano, J. (2020). Retos de seguridad/ciberseguridad en el 2030. Reflexión sobre un ejercicio prospectivo incompleto. *Revista SISTEMAS*. Asociación Colombiana de Ingenieros de Sistemas. 154. 68-79. Doi: 10.29236/sistemas.n154a7

Carmigniani, J., Furht, B., Anisetti, M. et al. (2011) Augmented reality technologies, systems and applications. *Multimed Tools Appl*. 51, 341–377. Doi: https:10.1007/s11042-010-0660-6

Denyer, D. (2017). Organizational resilience. A summary of academic evidence, business insights and new thinking. *BSI-Crandfield University*. De: https://www.cranfield.ac.uk/som/case-studies/organizational-resilience-a-summary-of-academic-evidence-business-insights-and-new-thinking

Dupont, B. (2019). The Cyber-Resilience of Financial Institutions: A preliminary working paper on significance and applicability of digital resilience. *Global Risk Institute*. De: https://globalriskinstitute.org/publications/the-cyber-resilience-of-financial-institutions-a-preliminary-working-paper-on-significance-and-applicability-of-digital-resilience/

Fatima, I., Anjum, A., Malik, S. & Ahmad, N. (2020) Cyber Physical Systems and IoT: Architectural Practices, Interoperability, and Transformation. *IEEE IT Professional*. May/June. 46-54. Doi: 10.1109/MITP.2019.2912604

GAO (2016). Enterprise risk management. Selected Agencies' Experiences Illustrate Good Practices in Managing Risk. De: https://www.gao.gov/assets/690/681342.pdf

Gibbs, W. (2002) Autonomic computing. *Scientific American*. De: https://www.scientificamerican.com/article/autonomic-computing/

Hines, A. & Bishop, P. (2015). *Thinking about the future: Guideline for strategic foresight*. Second Edition. Houston, TX. USA: Hinesight.

IIA (s.f.). Definición e implantación de apetito al riesgo. Fábrica de Pensamiento. *Instituto de Auditores Internos de España*. De: https://auditoresinternos.es/uploads/media_items/apetito-de-riesgo-original.original.pdf

Jackson, S. (2009). *Architecting resilient systems. Accident Avoidance and Survival and Recovery from Disruptions*. Hoboken, NJ. USA: John Wiley & Son

Jacobs, P., Arnab, A. & Irwin, B. (2013) Classification of Security Operation Centers. *2013 Information Security for South Africa*, Johannesburg. 1-7, Doi: 10.1109/ISSA.2013.6641054.

Kick, J. (2014). Cyber Exercise Playbook. *MITRE Report*. De: https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf

Menon, G. & Kyung, E. (2020). When More Information Leads to More Uncertainty. *Harvard Business Review*. De: https://hbr.org/2020/06/when-more-information-leads-to-more-uncertainty

Overby, S. (2020). Edge computing for beginners: 11 key concepts. *Enterprisers Project*. De: https://enterprisersproject.com/article/2020/7/edge-computing-beginners-11-concepts

Pillay, R. (2019). *Learn penetration testing. Understand the art of penetration testing and develop your white hat hacker skills*. Birmingham, UK.:Packt Publishing Ltd

Ponemon (2020). Digital transformation & cyber risk. What do you need to know to stay safe. *CyberGRX*. De: https://get.cybergrx.com/ponemon-report-digital-transformation-2020

Popper, R. (2008). How are foresight methods selected? *Foresight*. 10(6). 62-89. Doi: 10.1108/14636680810918586

Radiocrafts (2019) Cloud vs Fog vs Mist Computing, Which One Should You Use? De: https://radiocrafts.com/cloud-vs-fog-vs-mist-computing-which-one-should-you-use/

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

Stafford, B. & Schindlinger, D. (2019). *Governance in the digital age. A guide for the modern corporate board director*. Hoboken, N.J. USA: John Wiley & Sons

Tozzi, C. (2020). The pros and cons of adding edge computing to a cloud architecture. *TargetTec*h. De: https://searchcloudcomputing.techtarget.com/tip/The-pros-and-cons-of-adding-edge-computing-to-a-cloud-architecture

Valdez-de-León, O. (2019). How to Develop a Digital Ecosystem: a Practical Framework. *Technology Innovation Management Review*. 9(8). 43-54. http://doi.org/10.22215/timreview/1260

Velte, A., Velte, T. & Elsenpeter, R. (2010). *Cloud computing. A practical approach*. New York, USA: McGraw Hill.

Wang, C. & Lu, Z. (2018). Cyber Deception: Overview and the Road Ahead. *IEEE Security & Privacy*. 16(2). 80-85. Doi: 10.1109/MSP.2018.1870866.

Weick, K. & Sutcliffe, K. (2007). *Managing the Unexpected. Resilient Performance in an Age of Uncertainty*. Second Edition. San Francisco, CA. USA: Jossey-Bass

Woods, D., Dekker, S., Cook, R., Johannesen, L. & Sarter, N. (2010). *Behind human error*. Second Edition. Farnham, Surrey. England: Ashgate Publishing Limited.

Yahuza, M. et al. (2020). Systematic Review on Security and Privacy Require-

ments in Edge Computing: State of the Art and Future Research Opportunities. *IEEE Access*. 8. pp. 76541-76567. Doi: 10.1109/ACCESS.2020.2989456.

Yampolskiy, R. (2017). AI Is the Future of Cybersecurity, for Better and for Worse. *Harvard Business Review*. De: https://hbr.org/2017/05/ai-is-the-future-of-cybersecurity-for-better-and-for-worse

Zalewski, J. (2019). IoT Safety: State of the art. *IEEE IT Professional*. 21(1). 16-20. Doi: 10.1109/MITP.2018.2883858

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–.*