Resiliencia digital

DOI: 10.29236/sistemas.n159a5

Nuevos retos, nuevas prácticas.

Sara Gallardo M.

El Covid-19 suscita el cambio en todas las instancias de la sociedad alrededor del mundo, de ahí que el ser humano sienta ese impacto y se vea obligado a repensar su estilo de vida. Y en el ambiente empresarial y de los negocios, las organizaciones deben asumirlo enfocando sus mejores esfuerzos en una transformación.

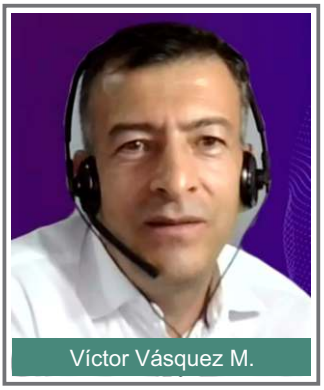
Razones para que el tema del foro en esta edición sea la resiliencia digital o la capacidad de las compañías para aceptar, sobreponerse, recuperarse y superarse. Y, en tal sentido, rediseñar los procesos comerciales y sistemas de TI, en aras de proteger su información más vulnerable y de poner en marcha estrategias claras que aseguren su funcionamiento, inclusive ante los ataques cibernéticos. Se trata de enfrentar nuevos retos e implementar nuevas prácticas.

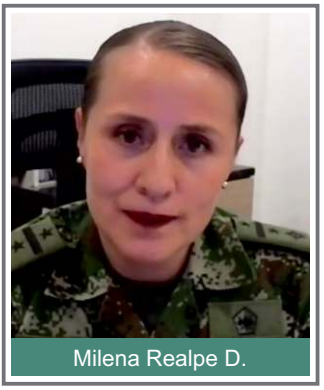
Para analizar algunos aspectos sobre esta realidad fueron invitados Armando Carvajal R., gerente arquitecto de soluciones en Globaltek; Víctor Vásquez Mejía, director de IT Advisory en KPMG; Teniente Coronel Milena Realpe Díaz, *jefe de la Maestría de Ciberseguridad y Ciberdefensa*, *Escuela Superior de Guerra, General Rafael Reyes Prieto* y Edgar Fernando Avilés Gómez, de la Oficina de Seguridad de la Información de la Dirección de Impuestos y Aduanas Nacionales (DIAN).

Jeimy J. Cano M.
Moderador
Cuando nos referimos a resiliencia digital ¿estamos hablando exactamente de qué?

Víctor Vásquez M.
Director IT Advisory
KPMG
Antes de entrar de lleno en la definición de resiliencia digital, me parece oportuno ubicar el contexto en el que se mueven los desarrollos tecnológicos y su avance en todos los ambientes de negocio. Basta citar la computación en la nube, la inteligencia artificial, *Blockchain, IoT*, entre otros, especialmente en la pandemia que aceleró la transformación digital y la convirtió en una prioridad para que las compañías puedan sobrevivir. En tal sentido, la resiliencia es la capacidad que deben tener todas las organizaciones para mantener, cambiar y recuperarse rápidamente en cualquier tipo de adversidad que atente contra su operación y la tecnología que la soporta.

Milena Realpe D.
Oficial Ejército Nacional de Colombia
Jefe de la Maestría de Ciberseguridad y Ciberdefensa
Escuela Superior de Guerra General Rafael Reyes Prieto
El entorno digital se ha convertido en el principal sistema nervioso del que hoy depende la actividad social


Víctor Vásquez M.


Milena Realpe D.


Edgar Fernando Avilés G.


Armando Carvajal R.

y económica. Las personas, las organizaciones y los países ahora penden del ciberespacio para sus actividades diarias. Adicionalmente, estamos frente a un ambiente VICA (volátil, Incierto, Complejo y Ambiguo) que nos agudiza un panorama de riesgos complejo y cambiante que pone en peligro el funcionamiento, la eficacia y la confianza que depositamos en él. Es por esto por lo que necesitamos desarrollar una buena resiliencia digital que proporcione las medidas necesarias para abordar estos riesgos de manera efectiva, brindando a las organizaciones la confianza para explotar la era digital para brindar las oportunidades de crecimiento e innovación. Recordando que siempre deberá existir un equilibrio entre la oportunidad, el costo y el riesgo. A medida que ha aumentado la dependencia de la información y las comunicaciones, los temas de seguridad también han tenido que evolucionar: de la seguridad informática a la seguridad de las TI, luego a la seguridad de la información y ahora a la ciberseguridad y luego a la Ciberresiliencia o resiliencia digital. En consecuencia, la seguridad ya no se trata solo de proteger los procesos, la información y los datos dentro del perímetro de la empresa, sino que se extiende a través de Internet a la cadena de suministro, los clientes, los socios y la sociedad en su conjunto. En este contexto, Las organizaciones deben trabajar juntas, con los gobiernos y con los ciudadanos para lograr una resiliencia cibernética efectiva. La buena resiliencia cibernética es un enfoque de colaboración completo impulsado por la junta directiva, pero que involucra a todos en la organización y se extiende a la cadena de suministro, socios y clientes. Para equilibrar los riesgos cibernéticos que enfrenta la empresa con las oportunidades y ventajas competitivas que puede obtener. También implica alejarse de las estrategias que buscan únicamente prevenir ataques a los activos y pasar a otras que incluyen la anticipación, preparación y la recuperación de un ciberataque.

Edgar Fernando Avilés Gómez
Oficina de Seguridad de la Información
Dirección de Impuestos y Aduanas Nacionales (DIAN)

Para asumir la resiliencia digital es necesario pensar en la continuidad

del negocio en términos de recuperación frente a los nuevos riesgos. Es necesario rescatar algunos temas del pasado reciente para utilizar las herramientas acordes con lo que pueda aparecer en el horizonte; desarrollar las habilidades y capacidades para enfrentarlos y contenerlos, en el marco de la recuperación para salir adelante más fortalecidos, en un entorno cambiante; ahora bien, las empresas tienen un fuerte apoyo por las áreas de gestión de servicios de Información y Tecnología (I&T); desde esta visión es indispensable contar con la habilidad de prevenir, detectar, contener y recuperarse minimizando el tiempo de exposición y el impacto de riegos cibernéticos contra los datos, aplicaciones e infraestructura.

Armando Carvajal R.
Gerente Arquitecto de Soluciones Globaltek

La pandemia nos ha obligado a transformarnos. La resiliencia digital es la capacidad de un ser humano, de una empresa, de una entidad o de un ente vivo para sobreponerse a momentos críticos. Hoy es Covid-19, mañana no sabemos qué variante será. Es necesario estar preparados para enfrentar los ciberataques y adaptarse a ese tipo de situaciones inusuales e inesperadas.

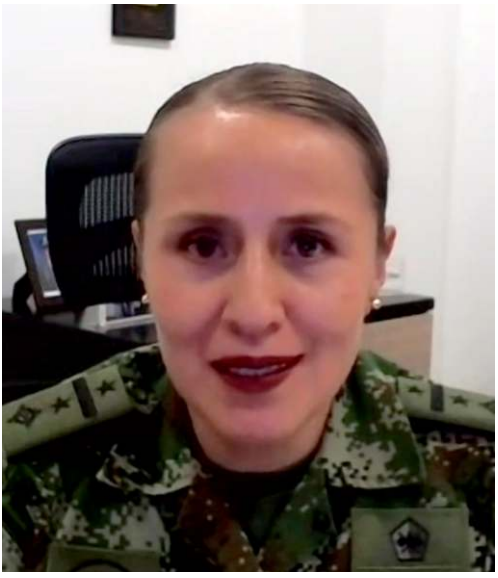
Jeimy J. Cano M.
¿Cuáles son los elementos claves que una organización debe tener en cuenta para desarrollar resiliencia digital? ¿Depende de su apetito de riesgo?

Milena Realpe D.
Los elementos claves que una organización debe tener en cuenta para desarrollar la resiliencia digital son: comprender claramente cuáles son los activos críticos de la organización, especialmente con respecto a la información. Tener una visión clara de las amenazas y vulnerabilidades de la organización que surgen de su entorno, incluido el de sus clientes, socios y cadena de suministro. La adopción de un lenguaje común utilizado por todas las partes interesadas de la empresa. Una evaluación de la madurez de la resiliencia cibernética y el diseño de planes apropiados, priorizados y proporcionados utilizando la guía de mejores prácticas. Un adecuado equilibrio de controles para prevenir, detectar y corregir. Al seleccionar el equilibrio adecuado

entre anticipación, prevención, detección, tolerancia y corrección, una organización debe considerar si la anticipación o la prevención es rentablemente viable o si, en cambio, se puede lograr una detección y corrección rápidas con un impacto aceptable a corto plazo en la resiliencia cibernética.

Jeimy J. Cano M.
¿Depende de su apetito de riesgo?

Milena Realpe D.



El apetito del riesgo es definido por COSO (*Committee of Sponsoring Organizations of the Treadway*), como el "total del riesgo que las entidades están dispuestas a aceptar al perseguir sus objetivos". En este contexto, la estrategia de resiliencia digital en una organización sí debe tomar como base el apetito al riesgo, toda vez que este establece el contexto aceptable en el que la organización va a planear la estrategia corporativa, además el apetito al riesgo sirve como parámetro para la gestión de riesgos. Considero como un elemento clave tener claro cuáles son los activos críticos, especialmente los que tienen que ver con la información. Así mismo, tener una visión clara de las amenazas y las vulnerabilidades; sabemos que no todas afectan de la misma manera, de ahí la necesidad de determinar cuáles son las más importantes que también podrían afectar las relaciones de su entorno. Se trata de desarrollar una resiliencia digital en el marco de un lenguaje común, claro que involucre todos los miembros de la empresa. De la misma manera, evaluar la madurez de resiliencia, en un proceso de seguimiento y verificación del estado de la misma.

Edgar Fernando Avilés G.
En mi opinión los cambios son profundos en toda la organización, es necesario iniciar por la cabeza, es decir, la alta dirección. Se requiere definir el "tono" de la administración enfocado en la agilidad de respuesta, en la seguridad de los activos y de la ciberseguridad. La administración debe propiciar cambios en los procesos, es necesario que sean más rápidos y deben dar el marco del apetito del riesgo que están dispuestos a aceptar. En otras palabras, las administraciones deben promover una cultura para reconocer los fallos y no castigar el error para poder aprender. Así mismo, se requieren aquellas

personas que interpreten y entiendan el nuevo entorno y que operen gestionando la incertidumbre y finalmente los riesgos, la administración debe cambiar hacia un nuevo modelo más rápido y fácil de utilizar, con criterios que incluyan los riesgos emergentes o espontáneos adicionales a los conocidos.

Víctor Vásquez M.

Sí depende del apetito de riesgo y es clave que la alta dirección participe en la definición de lo que éste significa y de las decisiones para que a lo largo de la organización funcionen las cosas. La alta gerencia debe tener una visión clara y las diferentes áreas deben lograr una alineación con la estrategia de negocio. Adicionalmente, la alta gerencia debería mostrar el compromiso e implementar las medidas requeridas para monitorear el apetito de riesgo, siempre pensando en generar una conciencia visible en la ejecución de los procesos de la compañía de lo contrario, la cultura no va a operar; todo esto sin perder de vista la tecnología y el monitoreo sobre todos los riesgos emergentes. Es necesario que todos los miembros de la empresa tengan claridad sobre unas buenas prácticas de gobierno, riesgo y cumplimiento (GRC), además de monitorear los proyectos para poder implementar GRC en la compañía.

Armando Carvajal R.

La resiliencia digital sí depende del apetito de riesgos y además de la gestión de riesgos. Vale la pena revisar los elementos clave, pues desde hace mucho tiempo se habla de este tema, pero no lo usamos con frecuencia; es como si quisiéramos empezar desde ceros y el pasado no se debe olvidar, pues éste forma e influye e. Es clave contar con un inventario de activos digitales para conocer las propiedades tales como: quién es el dueño, cual es el nombre del activo, en qué procesos se usa, quién es el custodio, cuál es su valor económico para la junta directiva, es infraestructura critica para el negocio, es crítico para el país, cuáles son sus amenazas y sobre todo cuáles son sus vulnerabilidades inherentes. Estoy de acuerdo en que los asuntos simples en general nos satisfacen y nos llevan a lo que queremos explicar, si miramos en forma holística la Figura 1.

Se puede ver que la Resiliencia Digital aumenta al cumplir normas,

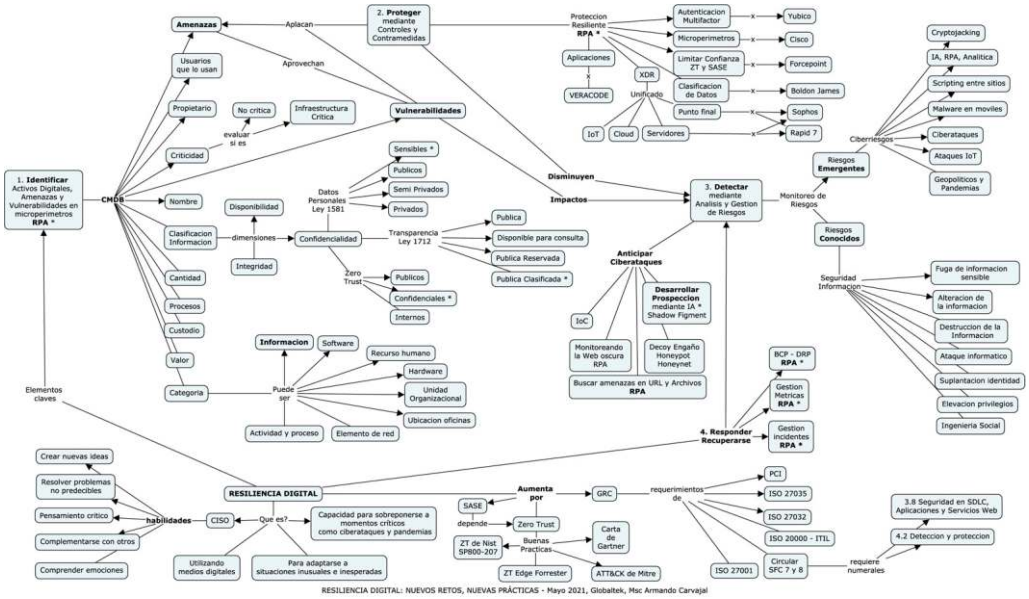


Figura 1. Mapa conceptual sobre resiliencia digital (Con autorización de uso por parte de Armando Carvajal Rodríguez)

entonces parece simple entender que debemos cumplir con la ley 1581 si el activo es de carácter personal, y debemos cumplir con la ley de trasparencia 1712 si el activo contiene información sensible o secreta.

Existe confusión en las diferencias entre vulnerabilidad y amenaza, a veces redactamos los riesgos como vulnerabilidades, o como amenazas, y olvidamos que debemos iniciar con el impacto, luego la amenaza y finalmente la vulnerabilidad como causa fundamental del riesgo.

Genera resiliencia anticipar los riesgos cibernéticos mediante técnicas de engaño, genera resiliencia prospectar, pues poder ver los riesgos emergentes nos permite defendernos y recuperarnos más fácilmente. Yo tengo esta expresión que me gusta repetirla en clases, ¨FADAS¨ o ¨FADASEI¨ para los riesgos conocidos, en la costa norte hablamos raro al usar expresiones como ¨estai" o "hacei", es un tip para no olvidar los riesgos más frecuentes, en la expresión FADASEI la letra F indica fuga de información, la letra A indica alteración de la información, la letra D destrucción de la información, la segunda letra A indica ataque informático, la letra S suplantación, la letra E indica elevación de privilegios y la letra I, indica ingeniería social, sé que estoy con expertos en riesgos y no

hay que ponerse a explicar esto, es más bien un aporte para los estudiantes afiliados de Acis que quieran profundizar en este tema de riesgos de ciberseguridad porque en general la gente no quiere ni siquiera inventarse una lista de riesgos conocidos, peor aún reconocer que vivimos en medio de los riesgos emergentes, entonces si de verdad somos resilientes deberíamos responder preguntas, como: ¿quién está mirando los riesgos que nos traen las tecnologías disruptivas como la inteligencia artificial y la robótica?, ¿quién está mirando los riesgos de la analítica predictiva basada en patrones?, ¿quién está mirando los riesgos que podrían generar los ataques de *Cripto Jacking* hacia mi organización?, será que los malandros están usando mis máquinas para minar criptomonedas, ¿quién está mirando la posibilidad de nuevas variantes de la pandemia Covid-19 y su efecto en mi organización?, finalmente creo que debemos defendernos basados en anticipación y gestión de esos riesgos, hay que usar métricas, sin métricas la alta dirección no puede saber cómo está mi resiliencia digital, pero repito es directamente proporcional uno a uno con el apetito de riesgos.

Edgar Fernando Avilés G.
En el tiempo en que yo he venido trabajando me doy cuenta de que esas buenas prácticas, sobre todo en los países latinoamericanos, chocan con la manera como se ven los procesos, y entonces surge la pregunta, ajustamos las buenas prácticas a cómo operan nuestros procesos o aplicamos las buenas prácticas modificando los procesos de operación, sugiero esta última opción.

Víctor Vásquez M.
Como ejemplo y complemento: en una compañía del sector financiero como partícipe del comité de auditoría fue complejo que sus miembros entendieran los modelos de madurez de COBIT. Por eso es importante que, en temas de cultura y conocimiento, la alta gerencia esté muy presta a aprender y a socializarlos en toda la organización.

Jeimy J. Cano M.
¿Cómo desarrollar estrategias conjuntas para que la resiliencia y la gestión de riesgo empresariales puedan interactuar? ¿Cuál es el costo beneficio entre ciberseguridad y resiliencia digital?

Edgar Fernando Avilés G.
La relación entre gestión de riesgo y resiliencia es total, es un camino para atender los incidentes. Es necesario complementar el nombre de riesgo y denominarlo “Riesgo Digital”, de manera que se incluyan los activos críticos cibernéticos y aquellos que manejan datos personales. Así mismo, la gestión de riesgos debe valorarse con más detalle en aquellos que atenten con la disponibilidad; es probable que, según la metodología, un riesgo no sea gestionado porque la calificación del mismo sea media o baja; a

pesar de tener una calificación alta en disponibilidad, esto sucede cuando la calificación de integridad y disponibilidad es baja.

El costo-beneficio lo interpreto como el valor de ciberseguridad en la organización, esto es, no debe sentirse hasta que sea necesaria; es igual que un árbitro de fútbol, no debe sentirse solo hasta que sea importante su participación.

Así las cosas, es necesario anticipar el incidente; mantener buenas relaciones y contar con credibilidad en el área que gestiona los servicios de I&T (Información y Tecnología). Y, ante un incidente, dar información de calidad (precisa, oportuna, integra, significativa y pertinente) para una rápida toma de decisiones en el "Cuarto de Guerra" o "Comité de Crisis".

Víctor Vásquez M.

Es necesario revisar cómo se están haciendo las cosas, toda vez que hoy en día uno observa islas dentro de la organización, cada una actuando por su lado. Se requiere que las compañías permeen buenas prácticas de Gobierno, Riesgo y Cumplimiento (GRC) no como una herramienta, sino como una filosofía para interactuar y disponer de un núcleo central que reúna las acciones y dejen de existir silos manejados en diferentes mecanismos manuales para alimentar los mapas de riesgos. Es necesario buscar la unidad en todos los niveles de la organización y la puesta en marcha de una sola metodología de riesgos y un área que los centralice de cara a la continuidad de negocio para tomar decisiones basadas en información dinámica, en línea y centralizadamente.

Milena Realpe D.

Todas las organizaciones tienen sistemas de gestión, formales o informales, para controlar sus actividades. El diseño y la implementación basados en el riesgo de los controles de resiliencia cibernética se lograrán solo mediante la entrega a través del sistema de gestión, impulsado por los objetivos estratégicos. Una buena resiliencia cibernética puede proporcionar beneficios significativos más allá de la mitigación de amenazas y la consiguiente reducción de la exposición al riesgo. La estrategia de resiliencia cibernética garantiza que toda la actividad en esta dirección esté basada en objetivos claramente entendidos y ayuda a lograr la intención del gobierno de la organización. El trabajo de estrategia identifica los activos críticos e identifica las vulnerabilidades y los riesgos a los que se enfrentan. Sobre el costo beneficio entre ciberseguridad y resiliencia digital, no hay un punto específico en el que se logre la ciberresiliencia absoluta, y generalmente existe una ley de rendimientos decrecientes en la resiliencia adicional que surge de la inversión adicional equilibrada con la exposición al riesgo que permanece. En este contexto, el costo beneficio depende de los resultados obteni-

dos para reducir la exposición a riesgos ciberresilientes, teniendo como base el sistema de gestión organizacional impulsado siempre en el cumplimiento de sus objetivos estratégicos.

Armando Carvajal R.

Desde mi perspectiva primero, se requiere estandarizar los riesgos sobre un único sistema integrado empresarial, toda vez que generalmente dentro de la organización cada uno va por su lado, el de riesgo operativo, el de calidad, el de ciberseguridad, el de datos personales, sería lo ideal contar con una única forma para definir riesgos. En mi caso particular de auditor, antes de hacer un análisis de riesgos en ciberseguridad, acostumbro a pasar por calidad para indagar sobre los riesgos detectados; me muestran la matriz de riesgos de calidad y por ningún lado veo las vulnerabilidades, es como si calidad no viera la vulnerabilidad como una causa de riesgo. Y, al preguntarles por qué ésta no es parte de los activos en los procesos, no hay respuesta.

Entonces se requiere unificar conceptos fundamentales, en la medida en que no es lo mismo vulnerabilidad que amenaza o el impacto. Segundo, se debe disponer de un estándar de redacción de riesgos, de unificación de conceptos. Y, como tercer punto, la sensibilización en ciberseguridad y resiliencia desde la alta dirección hasta llegar a la mensajería y hasta el suministro de café a los funcionarios. Sobre el costo-beneficio considero que el costo de los controles genera beneficios si el patrimonio de los socios no se disminuye en el ejercicio de Ciberseguridad y Resiliencia, y esto lo debemos mostrar a la junta directiva con indicadores.

Víctor Vásquez M.

En cuanto al costo-beneficio entre ciberseguridad y resiliencia organizacional, se logran cuando se tienen permeados los temas de Gobierno, Riesgo y Cumplimiento (GRC) y los beneficios se evidencian en la toma de decisiones con información más confiable y de forma dinámica. Hoy en día existen soluciones tecnológicas para apoyar los procesos de GRC que, en principio, pueden parecer costosas, pero los beneficios se ven cuando se obtienen buenas prácticas manejadas de forma centralizada. Adicionalmente, existen certificaciones de nivel internacional para los profesionales como *Certified in Risk and Information Systems Control* (CRISC), I*T Risk Fundamentals Certificate*, ISO- 31000, entre otras.

Edgar Fernando Avilés G.

Estoy de acuerdo en que se debe contemplar el costo frente a qué y en esa medida es necesario valorar las pérdidas para determinar si es o no costoso lo que se va a implementar. Nuevamente aparece una herramienta del pasado reciente, el BIA, mecanismo para determinar las pérdidas ante un incidente disruptivo en un proceso.

Jeimy J. Cano M.

¿Cuáles son las actitudes y comportamientos claves para desarrollar y fortalecer la resiliencia digital?

Milena Realpe D.

El *Oxford English Dictionary* define la resiliencia como "la cualidad o el hecho de poder recuperarse rápida o fácilmente de, o resistir ser afectado por, una desgracia, conmoción, enfermedad, robustez, adaptabilidad". En el ciberespacio, esto exige características para prevenir un incidente y recuperarse después de un incidente. En este contexto, las personas deben tener desarrolladas cuatro capacidades en particular: capacidad de aceptar, en otras palabras, aceptar a vivir de otra manera ayuda a mirar hacia un horizonte concreto. Capacidad de sobreponerse, es decir, aprender a dominar la pena, la culpa o el error y enfocarse en una nueva situación. Capacidad de recuperarse; quiere decir mantener el esfuerzo y la lucha con perseverancia y una actitud positiva para superar las situaciones traumáticas. Capacidad de superarse significa llegar al punto de hacer de la experiencia traumática un aprendizaje.

Dentro de una organización, las personas que brindan liderazgo, gobernanza y gestión tienen un papel único y vital en la mejora y el mantenimiento de la resiliencia cibernética. Entre sus principales características figuran el compromiso, el interés, el control y el desafío.

Edgar Fernando Avilés G.

Me parece oportuno agregar los siguientes planteamientos: entendimiento de negocio, creatividad y habilidad de aprender como parte de la capacidad de aceptar. Conocimiento en tecnología, autocontrol y desconfianza dentro de la capacidad de sobreponerse. Flexibilidad y manejo de incertidumbre como parte de la capacidad de superarse y toma de decisiones rápidas dentro de la capacidad de recuperarse.

Armando Carvajal R.

En mi opinión se trata de capacidades, más que de actitudes para ser resiliente. Cuando escuché mencionar la palabra innovación pensé enseguida en la era de piedra, es decir vino a mi mente los momentos cuando los cazadores miraban hacia la jungla, mirando fijamente hacia el verde de la jungla podían ver un depredador como un león o un tigre camuflados en el color verde y amarillo de la selva, por necesidad de cazar y debían estar dispuestos a atrapar a su presa para alimentarse, entonces existía la posibilidad de ser atacados por depredadores, ¿se es o no innovador por naturaleza? Yo lo llamo innovación basada en patrones, porque esto no lo hemos perdido. Es lo mismo que cuando tenemos disgustos con nuestras parejas, uno mira hacia el techo y el cerebro empieza a encontrar patrones. Cada uno es diferente y ve lo que quiere ver dependiendo de la presión y de la necesidad, pero así se da la creatividad,

mediante la búsqueda de patrones, esto es muy humano y es inherente a todos los humanos. Para ser resiliente hay que comprender las emociones de las personas con que interactuamos. En algunas oportunidades uno se encuentra con gerentes de compañías que niegan la ocurrencia de algún suceso, se molestan porque se les advierte sobre la situación de riesgos emergentes, entonces es necesario saber cuál es el interés de la alta dirección para que seamos resilientes. Debemos reconocer la transformación digital en la que los robots se están imponiendo al reemplazarnos en las tareas repetitivas, es decir debemos ser más humanos, debemos tener la capacidad de resolver problemas no predecibles y finalmente debemos tener la capacidad del pensamiento crítico.

Víctor A. Vásquez M.
Creo que son varias, pero yo resaltaría las siguientes: tolerancia a la frustración y a la incertidumbre; afrontamiento positivo de la adversidad; autoconocimiento y autoestima; conciencia de presente y optimismo, además de flexibilidad sumada a la perseverancia.

Jeimy J. Cano M.
¿Cuáles tecnologías son requeridas para desarrollar la resiliencia digital en una organización?

Víctor Vásquez M.
En mi opinión una solución tecnológica como GRC lograría integrar la metodología de riesgos en las diferentes áreas de la organización, incluyendo las de ciberseguridad y resiliencia; para esto es necesario alimentar esa herramienta y mantenerla al día en todo lo relacionado con los riesgos, cualquiera que éstos sean. De esa manera se alimenta una sola matriz corporativa.

Edgar Fernando Avilés G.
Insisto en la cuantificación de las pérdidas, las empresas deben saber cuánto van a perder ante unos eventos para saber cuánto van a invertir. Se trata de una gestión de riesgos, más rápida y proactiva, tanto como capitalizar el conocimiento del recurso humano para motivar su permanencia en la organización. Hoy en día, las nuevas generaciones duran muy poco en los trabajos y deben ser motivadas de manera diferente. En relación de tecnologías, es importante considerar software correlacionador de eventos, software para predecir tráfico anómalo, software de monitoreo de tráfico en las DB y la Red, software de Identidades, para saber a qué, cómo, cuándo y dónde las personas tienen acceso, además de un enfoque *zero trust* en los servicios; esto es, una filosofía que se basa en menos accesos privilegiados; nunca confiar, siempre verificar; y asumir una filtración. Por último, no olvidar contar con un servicio de SOC (centro de operación de seguridad).

Milena Realpe D.
La ciberresiliencia combina las mejores prácticas vinculadas a la se-

guridad de TI, la continuidad del negocio y otras disciplinas para crear una estrategia de negocio más alineada con las necesidades y objetivos de la empresa digital actual. Sin embargo, considero que se requiere una combinación de tecnologías de varios sistemas como, por ejemplo, para la seguridad cibernética-ciberseguridad; para la gestión de riesgos; para la continuidad del negocio, para la recuperación de desastres. Además de un gran sistema de analítica de datos que permita integrar esta información, correlacionarla y presentarla en cuadros de mando y control para toma de decisiones de alto nivel en tiempo real.

Armando Carvajal R.

Aunque los seres humanos somos muy, pero muy inteligentes, no somos tan sabios como parecemos, a veces, parece que no nos damos cuenta de que el futuro va a ser diferente, generalmente nos gusta la zona de confort. Hay quienes señalan que no necesitamos de las tecnologías. Y cuando recibo este tipo de cuestionamientos, mi opinión es que sí la requerimos. Basta entenderlo con el ejemplo de un rayo láser por sí mismo; éste no es malo, podría servir para eliminar un terigio o ayudar en la cirugía de un ojo; esto no lo convierte en nocivo como lo ven muchas personas que ven un enemigo, ven algo demoníaco. Relaciono mis planteamientos dentro de un marco filosófico, en la medida en que los seres humanos somos inteligentes, no somos sabios y necesitamos herramientas. Basta citar, por ejemplo, la ayuda que nos da la analítica de patrones en antimalware, o la inteligencia artificial para predecir patrones por medio del *Machine Learning* (aprendizaje de la máquina) para aprender sobre datos no estructurados, para ayudarnos a extraer datos estructurados cuando solo vemos grandes volúmenes de datos no estructurados que no sería fácil de entender para un humano promedio.

Jeimy J. Cano M.

¿Conocen ustedes modelos de madurez en resiliencia digital?, ¿cuál es su propuesta para identificar la madurez de una organización alrededor de la resiliencia digital?

Víctor Vásquez M.

He visto varios para resaltar: el BSI (http://bsigroup.com/es-MX/nuestros-servicios/Resiliencia-Organizacional/Elementos-esenciales-de-la-Resiliencia-Organizacional/), tiene un modelo interesante, manifiesto en los niveles operacionales, cadena de suministros y de información. El CMMI adquirido por ISACA hace algunos años tiene el propio para medir el nivel de madurez, muy alineado con NIST. Cobit tiene modelo de madurez y modelos de capacidad que podrían adecuarse para medir temas de resiliencia. Así mismo, el DRJ (https://drjenespanol.com/marcos-de-resiliencia/) también tiene unos componentes interesantes para revisar.

Milena Realpe D.
He leído de un modelo que propuso el Instituto Nacional de Tecnologías de Comunicación. (INTECO-CERT) CERT de seguridad e Industria como la aproximación a un marco de medición de ciberresiliencia, el cual contempla un modelo de indicadores basado en un conjunto de dominios funcionales, hasta llegar a un cuadro de mando que permita controlar y con ello realizar mejora continua, mantenimiento y su comparación en el tiempo. La propuesta para identificar la madurez de una organización alrededor de la resiliencia digital es que sea un instrumento que establezca las estrategias, metodologías y procedimientos para la protección del ciberespacio, que posibilitan de forma coordinada y metodológica anticiparse, resistir, recuperarse y evolucionar frente a las ciberamenazas. Las organizaciones, deben estar preparadas para dar respuestas rápidas a este tipo de ataques, permitiendo que los servicios que prestan no se vean interrumpidos, fortaleciendo sus capacidades de identificación, detección, prevención, contención, recuperación, cooperación y mejora continua contra las ciberamenazas.

Adicionalmente, me gustaría mencionar que, a través de la investigación formativa, en la Escuela Superior de Guerra se han realizado propuestas de modelos de medición de resiliencia cibernética, los cuales pueden ser consultados en nuestra biblioteca digital.

Edgar Fernando Avilés G.
No conozco ningún modelo de madurez para este tema, asumo que a nivel de empresa debería medirse en mantener el flujo de caja de la empresa y no perder el segmento de ventas, así como la disponibilidad de los procesos y de los servicios de la organización, además de los servicios de I&T (Información y Tecnología). El modelo debería orientarse hacia la detección temprana de eventos y la identificación de los incidentes. También la diferencia entre el tiempo en que se detecta el incidente y el tiempo que se toma la recuperación de los servicios.

Armando Carvajal R.
Sin pena manifiesto que no he experimentado todavía con ningún modelo especifico o metodología de resiliencia digital, me atraparon en la canoa buscando, investigando y curioseando, pero sí he medido la resiliencia usando análisis GAP, mediante gráficos de araña, entre otras alternativas para medir qué desea la junta directiva basados en métricas de resiliencia contra las buenas prácticas que utilizamos para ser resilientes.

Jeimy J. Cano M.
Les pido plantear sus conclusiones sobre lo aquí debatido.

Víctor Vásquez M.
En resumen, es un tema que debe ser permeado desde la alta gerencia, con el propósito de involucrar tecnologías que ayuden a adminis-

trarlo dentro de un monitoreo continuo de esa evolución.

Milena Realpe D.

Como conclusión considero que debemos preparar nuestras organizaciones para interactuar y desarrollarse en el ciberespacio, el cual se encuentra marcado por un ambiente Volátil, Incierto, Complejo y Ambiguo (VICA), en el que los riesgos requieren ser controlados a través de una estrategia general de ciberresiliencia basada en el equilibrio adecuado entre las personas, los procesos y la tecnología. Una buena estrategia de resiliencia digital debe abordar varios componentes o dominios tales como anticipar, prevenir, contener, resistir, defender, recuperar y evolucionar. Y esto solo puede darse, si tenemos personas capaces de afrontar estos nuevos desafíos, de proponer alternativas integrales que le permitan a la organización sacar el máximo provecho de la era digital.

Armando Carvajal R.

Señalo cuatro ideas que no deberíamos olvidar de esta charla: monitorear riesgos desde el estudio mínimo de la vulnerabilidad y amenazas sobre los activos críticos, para aumentar el conocimiento de los incidentes que ya tenemos hoy en

nuestras empresas y en los mercados donde vivimos; sugiero calibrar sensores simétricos para darle la bienvenida a la falla, no para asustarnos, sugiero ayudarnos de tecnologías disyuntivas como inteligencia artificial, analítica y RPA para tener un consolidado único empresarial de riesgos y de resiliencia; y, buscar apoyo de la alta dirección para estas iniciativas.

Edgar Fernando Avilés G.

Después de este debate me parece oportuno reflexionar sobre: (1) el riesgo digital, siempre está ahí y va a llegar tarde o temprano, para no crear falsas expectativas o seguridades en medio de la organización. Las organizaciones deben prepararse para su gestión y salir fortalecidas, (2) tomar nota de la necesidad de nuevas habilidades en las personas, desarrollarlas o potencializarlas en los funcionarios, (3) el apoyo de la alta gerencia, se requiere una culturización a nivel ejecutivo en este entorno, para muchos nuevo, inclusive para nosotros mismos. Y por último (4), la alineación de tecnología en esas victorias tempranas que los negocios necesitan.

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas Uno y Cero, Gestión empresarial y Acuc Noticias. Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Coautora del libro "Lo que cuesta el abuso del poder". Ha sido corresponsal de la revista Infochannel de México; de los diarios La Prensa de Panamá y La Prensa Gráfica de El Salvador y corresponsal de la revista IN de Lanchile e investigadora en publicaciones culturales. Se ha desempeñado también como gerente de Comunicaciones y Servicio al Comensal en Inmaculada Guadalupe y amigos en Cía. S.A. (Andrés Carne de Res) y editora de Alfaomega Colombiana S.A.; asesora en escritura y producción de libros; es editora de esta revista.*