No. 159 Abril - Junio 2021 DOI: 10.29236/sistemas ISSN 0120-5919

SISTEMAS

Tarifa Postal Reducida Servicios Postales Nacional S.A. No. 2017-186 4-72, vence 31 de Dic. 2021

Resiliencia digital

La nueva frontera para las organizaciones del siglo XXI

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS
Calle 93 No. 13 - 32 of. 102
Bogotá, D.C.
www.acis.org.co

ISACA®
Bogotá Chapter

CISM Certified Information Security Manager®
An ISACA® Certification

CGEIT Certified in the Governance of Enterprise IT®
An ISACA® Certification

CET Certified in Emerging Technology
An ISACA® Certification

CSX CYBERSECURITY
FUNDAMENTALS CERTIFICATE

COBIT® 2019

Mayor Información
www.isaca.org/credentialing

Los miembros de ISACA pueden beneficiarse del acceso, ahorros y conocimiento para impulsar su éxito en auditoría, control, seguridad, ciberseguridad y gobernanza de SI / TI en una multitud de industrias. Member Advantage abarca el conjunto de beneficios que los miembros de ISACA reciben para avanzar profesionalmente y ser recompensados personalmente a lo largo de toda su carrera.

¡Sé parte de **ISACA Bogotá**!

www.isacabogota.org | Teléfono 3007498689

ISACA® Bogotá Chapter

LUMU

NADA BUENO SUCEDE
CUANDO ESTÁS EN CONTACTO
CON EL ADVERSARIO

Tanto en la naturaleza como en **ciberseguridad**, el resultado de estar en contacto con el adversario es catastrófico. **Lumu te ayuda** a identificar las conexiones entre tu empresa y criminales **en tiempo real**.

www.lumu.io


Microsoft

En esta edición

Publicación de la Asociación Colombiana de Ingenieros de Sistemas (ACIS)
Resolución No. 003983 del Ministerio de Gobierno
Tarifa Postal Reducida Servicios Postales Nacional S.A. No. 2015-186 4-72
ISSN 0120-5919
Apartado Aéreo No. 94334
Bogotá D.C., Colombia

Abril - Junio 2021
Calle 93 No.13 - 32 Of. 102
Teléfonos 616 1407 - 616 1409
A.A. 94334
Bogotá D.C.
www.acis.org.co

AWS ENTERPRISE

amazon.com/enterprise

Cloud Computing en Amazon Web Services

Ofrecemos un sólido conjunto de servicios diseñados específicamente para satisfacer las necesidades exclusivas de seguridad, conformidad, privacidad y gobernanza de grandes empresas. Con una plataforma tecnológica amplia y sólida, AWS puede ayudarle a avanzar más rápido y a hacer más.

Céntrese en las necesidades de la empresa y no en la infraestructura

- Confianza y seguridad
- Plataforma más completa
- Innovación rápida
- Presencia global

Conozca más sobre las soluciones de AWS en nuestro sitio web

Resiliencia digital: más allá de la continuidad del negocio

DOI: 10.29236/sistemas.n159a1

En un contexto volátil, incierto, complejo y ambigüo (VICA) lo normal es enfrentar "eventos inesperados"; en este sentido, la resiliencia digital se configura como el nuevo referente para vivir atentos y vigilantes en procura de mantener las operaciones a pesar de la inevitabilidad de la falla y las acciones exitosas de agentes adversos.

Jeimy J. Cano M.

Las organizaciones hoy se enfrentan a una dinámica de cambios permanentes que demandan una mirada distinta al entorno y a las tendencias que allí se advierten. La incertidumbre como elemento natural para los ejecutivos de las empresas e insumo base de la innovación, establece dos puntos de análisis que exponen a las compañías a tomar acciones sobre un escenario que se transforma con las diferentes posturas que pueden aparecer desde cualquier mercado o sector (Day & Schoemaker, 2019).

En este contexto, la tecnología juega un papel fundamental como ha-

bilitador de posibilidades, servicios o productos que terminan capitalizando nuevas experiencias para los individuos y cambiando muchas veces la forma de hacer las cosas. Por tanto, los conceptos de digitalización (digitalizar) y transformación digital (ser digital) adquieren una relevancia estratégica para las empresas, habida cuenta que permite preparar los componentes de infraestructura requeridos para fundar una estrategia digital y, además, transforma el modelo de negocio y la cultura organizacional para crear apuestas novedosas que reten los saberes previos (Ross, Beath & Mocker, 2019).

Así las cosas, ya no es suficiente con reconocer y asegurar los activos de información claves que se generan en la organización por cuenta de las estrategias digitales, sus productos y servicios, sino que es necesario centrarse en la experiencia del cliente, en el reconocimiento y desarrollo de la confianza digital, para desde allí habilitar las opciones de seguridad y control, basadas en su apetito al riesgo, a de fin crear entornos con umbrales de operación y tolerancia que conecten las capacidades empresariales y los acuerdos claves cuando las cosas no salen como estaban previstas (Zongo, 2018).

Es por esto que la resiliencia digital, como una nueva capacidad organizacional, se consolida como el nuevo horizonte y reto corporativo, que exige a las empresas alcanzar por lo menos cinco objetivos claves: (Robinson, 2020)

- **Anticipar disrupciones**: detección temprana y patrones de ataques emergentes.
- **Resistir interrupciones**: establecer niveles de defensa para mantener la operación.
- **Recuperarse de los ataques**: ejecutar las estrategias control y restauración frente a los ataques.
- **Aprender de los riesgos**: incorporar la inteligencia y cacería de amenazas.
- **Adaptar y modificar las capacidades vigentes**: desarrollar simulaciones y prototipos frente a escenarios inciertos y emergentes.

Es por esto que esta edición de la revista *Sistemas*, de la Asociación Colombiana de Ingenieros de Sistemas −ACIS−, apunta a revisar, explorar y analizar los retos y oportunidades de la resiliencia digital, con el fin de traer al escenario actual diferentes posturas y comprensiones sobre el tema, como insumo para plantear alternativas y opciones en un entorno VICA. Con ese propósito fueron convocados profesionales especialistas, quienes desde su experiencia proponen reflexiones para seguirle la pista al desarrollo de las tendencias y prácticas vigentes, capitalizando lecciones aprendidas, repensando las dinámicas de los negocios y retos actuales, así como al futuro que se avizora en el horizonte.

El ingeniero Mario Ureña Cuate, columnista invitado, establece desde su práctica de consultoría un marco base para reflexionar sobre la ciberresiliencia, en el marco de la capacidad empresarial demostrada para anticipar, resistir, recuperar y adaptarse ante eventos disruptivos que pongan en riesgo la actividad de las organizaciones en el ciberespacio. En esa dirección presenta una serie de propuestas en el campo empresarial y técnico que orienta a los ejecutivos y profesionales de TI para asumir el reto de permanecer a pesar de los eventos adversos.

En la entrevista el ingeniero Andrés Mauricio Bolívar Arias nos comparte sus reflexiones acerca de la resiliencia digital, desde la perspectiva de los negocios y los retos empresariales, además de afirmar que la resiliencia es más que seguridad e implica agilidad y velocidad para cambiar y adaptarse a las nuevas condiciones de los mercados.

Por su parte, el ingeniero Andrés Almanza Junco presenta el análisis de los resultados de la versión número veintiuno de la encuesta nacional de seguridad de la información, realizada cada año por ACIS, estudio que revela las tendencias más representativas de las empresas colombianas en los temas de protección de la información y la evolución del líder digital de seguridad, así como sus respectivos contrastes con la realidad internacional. En esta ocasión, se presentan los aspectos más representativos de las tendencias y algunos contrastes frente a patrones identificados en los datos acumulados.

El foro de esta revista fue un espacio para compartir visiones desde diferentes ángulos sobre la resiliencia digital. Los ingenieros Víctor Vásquez Mejía, Édgar Fernando Avilés, Milena Realpe Díaz y Armando Carvajal Rodríguez desarrollaron un diálogo abierto y nutrido para contrastar y complementar sus posturas desde la práctica de consultoría, la visión de defensa y seguridad nacional, la dinámica del sector público y los estándares disponibles a la fecha. Ellos advierten sobre la necesidad de incorporar los nuevos retos que impone la resiliencia digital y cómo avanzar en una perspectiva interdisciplinaria que permita a los profesionales y ejecutivos de seguridad y control enfrentarse a un escenario cada vez más disruptivo, inestable e hiperconectado, ambiente que demanda una mayor anticipación y capacidad de aprendizaje.

Así mismo, nuestros lectores dispondrán de dos artículos para reflexionar sobre la ciberresiliencia como integración entre seguridad de la información y continuidad, y por otra parte, sobre el reto de superar la falsa sensación de seguridad. En un primer documento el ingeniero Norman Ramírez se ocupa de explorar y analizar cómo es el ejercicio de convergencia entre las prácticas de seguridad de la informa-

ción y los retos de la continuidad de negocio y contrastar algunos marcos de trabajo para avanzar en la configuración de una organización ciberresiliente.

El segundo artículo, escrito por este servidor, aborda una revisión y análisis del reto de la falsa sensación de seguridad, esa zona cómoda y engañosa en la que se materializan y concretan sesgos y puntos ciegos en los modelos de seguridad y control; en que la necesidad de certezas enfrenta la cultura de productividad con la de aprendizaje. Frente a esta realidad, el artículo plantea una propuesta de un modelo de gestión que pase del tradicional "Planear, Hacer, Verifica y Actuar", a otro que privilegie las inestabilidades basado en "Arriesgar, Anticipar, Responder y Monitorizar.

En resumen, se trata de un panorama renovado y provocador de nuevas prácticas y desafíos alrededor de la resiliencia digital, que tensiona las certezas de los saberes y prácticas existentes. Su contenido invita a todos los profesionales en las diferentes áreas a explorar las nuevas realidades de un mundo digital y tecnológicamente modificado, sin perjuicio de los nuevos desafíos políticos, económicos, sociales, tecnológicos, legales y ecológicos, que los diferentes grupos de interés buscan para darle forma a las incertidumbres del entorno y desarrollar capacidades de negocio inexistentes, de cara a los riesgos que aún no aparecen en sus mapas estratégicos.

Referencias

Day, G. & Schoemaker, P. (2019). *See sooner act faster. How vigilant leaders thrive in a era of digital turbulence*. The MIT Press.

Robinson, C. (2020). Are We Cyber-Resilient? The Key Question Every Organization Must Answer. *IDC Market Spotlight*. Noviembre. https://www.bankinfosecurity.com/whitepapers/are-we-cyber-resilient-key-question-every-organization-must-answer-w-7136

Ross, J., Beath, C. & Mocker, M. (2019). *Designed for digital. How to architect your business for sustained sucess*. The MIT Press.

Zongo, P. (2018). *The five anchors of cyber resilience. Why some enterprises are hacked into banksruptcy while other easily bounce back*. Broadcast Books.

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–.*

Ciberresiliencia organizacional

DOI: 10.29236/sistemas.n159a2

Afrontando la incertidumbre para sobrevivir y prosperar en un mundo digital. Solamente las organizaciones ciberresilientes tendrán la capacidad de sobrevivir ante los frecuentes ciberataques y frente al próximo gran evento disruptivo que enfrente la humanidad.

Mario Ureña Cuate

La pandemia por COVID-19 ha representado retos de gran impacto durante 2020 y 2021 para la sociedad y las organizaciones a nivel mundial, permitiendo renovar la importancia de la resiliencia organizacional a nivel individual y colectivo. La necesidad de implementar acciones y soluciones de continuidad del negocio, transformación y adaptación en respuesta a la emergencia sanitaria ha probado la capacidad de las empresas para sobrevivir y prosperar en un contexto global que presenta grandes cambios y retos.

La resiliencia organizacional es definida por BSI (*British Standards Institution*) en el estándar BS 650-00 como "la habilidad de una organización para anticipar, prepararse, responder y adaptarse al cambio incremental y las disrupciones repentinas con el fin de sobrevivir y prosperar" (BSI, 2014).

En este sentido, desde el punto de vista del ciberespacio como ese ambiente complejo que resulta de la interacción de personas, aplicaciones y servicios en internet a través de dispositivos tecnológicos y redes de comunicación que los conectan, hemos sido testigos de dos cambios profundos. Por una parte, la aceleración de la transformación digital en las organizaciones y, por otra, el incremento en los ciberriesgos que enfrentan.

La transformación digital se ha convertido en una estrategia primordial para mejorar las capacidades de resiliencia de las organizaciones al habilitar la posibilidad de adaptación en su forma de operar y el entendimiento de su rol y valor en la sociedad actual (Siebel, 2019).

Esta transformación digital va más allá del concepto común asociado a la digitalización, el cual es un elemento muy importante para lograr esta transformación; sin embargo, requiere de un cambio mucho más profundo que contempla: (Rogers, 2016)

- El entendimiento de los **clientes** como una red dinámica que exige una comunicación bidireccional y que representa la influencia principal sobre las decisiones de la organización

- Una búsqueda de **valor** hacia los clientes que permita descubrir dinámicamente las nuevas propuestas de valor encaminadas a una evolución antes de estar obligados al cambio.

- El reconocimiento de la **innovación** que acepte los fracasos como una fuente de aprendizaje y que permita el entendimiento y la resolución de los problemas correctos a través de la experimentación constante e inclusiva.

- La eliminación de los silos de **datos** con el objetivo de convertirlos en información valiosa para la toma de decisiones

- El entendimiento de la **competencia** como la implementación de redes externas que permitan la cooperación en áreas clave con socios que intercambian valor.

Este incremento en el uso del ciberespacio para habilitar nuevas formas de interacción en la sociedad conlleva riesgos que se han intensificado sustancialmente durante este tiempo de pandemia, debido al incremento sostenido en el uso de la tecnología y las consecuencias sociales asociadas al desempleo, impactos económicos y cambios culturales, que en ocasiones demuestran una degradación de los principios éticos y morales de grupos y personas a nivel internacional.

En consecuencia, los ciberriesgos han tenido una escalada preocupante con datos que confirman el estado de urgencia que debe ser

atendido. De acuerdo con datos del FBI (*Federal Bureau of Investigation*) se reporta un incremento del 300% en ciberataques a partir del inicio de la pandemia por COVID-19. Así mismo, la compañía de tecnología Verizon indica que, en 2020, el 86% de los ciberataques fueron motivados por aspectos financieros y el 10% por espionaje (Walter, 2021).

Un dato preocupante es el que presenta la asociación internacional en seguridad de sistemas de información ISSA (*Information Systems Security Association International*), la cual reporta que el 70% de los profesionales en ciberseguridad considera que su organización ha sido impactada debido a la falta de una calificación adecuada del personal de ciberseguridad para el desempeño de sus funciones (Oltsik, 2020).

Por lo que tomando en consideración el contexto en el que vivimos, respecto a la búsqueda de resiliencia mediante el uso de la tecnología y el incremento en ciberriesgos, es necesario asegurar una capacidad de ciberresiliencia demostrada para anticipar, resistir, recuperar y adaptarse ante eventos disruptivos que pongan en riesgo la actividad de las organizaciones en el ciberespacio, tomando en consideración las siguientes características:

- Una organización ciberresiliente asume que el adversario comprometerá o vulnerará sus sistemas en cualquier momento y que dicho adversario mantendrá una presencia en el sistema.

- Enfoca sus esfuerzos de ciberresiliencia en la misión y funciones del negocio, no sólo en aspectos técnicos.

- Se enfoca en los efectos de las amenazas persistentes avanzadas (APTs).

Para lograrlo, las organizaciones deben implementar las soluciones estratégicas, tácticas, operativas y técnicas orientadas a **prevenir o evitar** la ejecución exitosa de un ataque o la materialización de condiciones adversas; **preparar** un conjunto de cursos de acción en caso de que estos eventos se materialicen; asegurar la **continuidad** de la misión y funciones principales del negocio durante la adversidad; **limitar los daños** en la medida de lo posible, privilegiando siempre la vida humana por sobre todas las cosas; **reconstruir** la misión o funcionalidad de negocio tanto como sea posible después de la adversidad; **entender** el estado de los recursos involucrados; **transformar** la misión, funciones y/o procesos con la finalidad de atender los cambios en el ambiente y **rediseñar** arquitecturas para manejar esta y las futuras adversidades.

Finalmente, desde el punto de vista técnico, la atención de los riesgos ha requerido la creación y adopción de nuevas técnicas para mejorar

las prácticas de seguridad de la información y ciberseguridad, de manera de lograr una mayor capacidad de ciberresiliencia.

Algunas de las opciones técnicas que permiten mejorar esta capacidad de ciberresiliencia incluyen, pero no se limitan a la implementación de mecanismos de **monitoreo analítico** de las operaciones a través de sistemas de detección y respuesta que aprovechan los recursos de inteligencia artificial; **respuesta adaptativa** en la infraestructura tecnológica y procesos de operación; **protección coordinada** entre grupos y sectores de industria; mejora de la comunicación para asegurar la **concientización contextual** que involucra conocer el estatus de la situación conforme se va desarrollando entre las partes interesadas; **uso del engaño** como una forma de protección; **diversidad** en la infraestructura tecnológica para evitar que una sola vulnerabilidad pueda existir en todo el sistema de forma simultánea; **posicionamiento dinámico** que dificulte a un posible atacante la identificación de objetivos de ataque y la predicción de la operación; además de reducir la **persistencia** de información buscando que esta se encuentre disponible sólo cuando se requiere y se asegure su resguardo, ocultamiento y/o destrucción una vez aprovechada con fines legítimos (Verizon, 2021).

En conclusión, la ciberresiliencia debe formar parte de la agenda ejecutiva de las organizaciones y su atención requiere implementar modelos de trabajo que consideren, tanto los aspectos estratégicos como los elementos técnicos que sean soportados por una adecuada gestión de ciberriesgos, de acuerdo con el contexto interno y externo propio de cada empresa y en consideración de su rol en la sociedad. Solamente las organizaciones ciberresilientes tendrán la capacidad de sobrevivir y prosperar día con día ante los frecuentes ciberataques y frente al próximo gran evento disruptivo que enfrente la humanidad.

Referencias

Siebel, T. (2019). *Digital Transformation Survive and Thrive in an Era of Mass Extinction*. USA: RosettaBooks.

Roger, D. (2016). *The Digital Transformation Playbook: Rethink Your Business for the Digital Age*. USA: Columbia Business School Publishing.

BSI. (2014). Guidance on organizational resilience. UK: BSI. https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2014/november/Organizational-resilience-standard-published/

Verizon. (2021). Data Breach Investigations Report. USA: Verizon. https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

Oltsik, J. (2020). The impact of the COVID-19 Pandemic on Cybersecurity. USA: ESG & ISSA. https://www.issa.org/the-impact-of-the-covid-19-pandemic-on-cybersecurity/

Walter, J. (2021). COVID-19 News: FBI Reports 300% Increase in Reported Cybercrimes. https://www.imcgrupo.com/covid-19-news-fbi-reports-300-increase-in-reported-cybercrimes/

Mario Ureña Cuate. *CISSP, CISA, CISM, CGEIT, CDPSE. Es presidente de la firma de consultoría "Secure Information Technologies", y reconocido especialista en Gestión de Riesgos, Continuidad del Negocio, Seguridad de la Información, Resiliencia Organizacional y Auditoría. Con BSI (British Standards Institution) es instructor certificado y vocero para normas relacionadas con gestión integral de riesgos, continuidad del negocio, resiliencia organizacional y ciberseguridad. Ha participado como miembro de los comités CISA QAT (Quality Assurance Team) y EAC (External Advocacy Committee) de ISACA internacional, participó como miembro del comité de la conferencia internacional de ISACA y de la conferencia latinoamericana de seguridad y administración del riesgo, redactor de preguntas para las certificaciones CISA y CISM y colaborador en el desarrollo del material de estudio para la certificación CISM. Conferencista recurrente en eventos de Gestión de Riesgos, Seguridad de la Información, Auditoría de TI, Gobierno de TI y Resiliencia Organizacional. Participó como jurado para el Premio Nacional de Innovación y Buenas Prácticas en la Protección de Datos Personales del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).*

aruba
a Hewlett Packard Enterprise company

AL BORDE DEL CAMBIO

A medida que aumenta el volumen de datos de la red, deben procesarse, almacenarse y analizarse más cerca de su fuente – en Edge. ¿Qué piensan los Tomadores de Decisiones de TI (ITDM) sobre este cambio y cómo se están preparando?

Frente a una avalancha de datos

33% de los ITDM dicen que ya existen demasiados datos para que sus sistemas los manejen

28% dicen que no pueden procesar datos lo suficientemente rápido como para tomar acciones

Líderes de TI se están moviendo a Edge

82%
de los ITDM describieron la necesidad de un **sistema integrado en Edge** como **urgente**

72%
ya está utilizando **tecnologías Edge** para **entregar nuevos resultados**

88%
están **extrayendo y analizando datos** desde los **dispositivos en su red**

En caso de querer agendar una reunión para hablar más acerca de la solución, por favor escríbenos a **contacto.aruba@hpe.com**

Resiliencia digital es más que seguridad

DOI: 10.29236/sistemas.n159a3

Así lo plantea Andrés Mauricio Bolívar Arias, alrededor de otras inquietudes que circulan en la actualidad.

Sara Gallardo M.

En las actuales circunstancias por las que atraviesa la humanidad es fundamental generar conciencia sobre la situación para disponer de las medidas suficientes de protección, seguridad y bienestar. Y, en términos empresariales, la resiliencia digital se ubicó en el escenario de los negocios, en el marco de un protagonismo inusitado.

En ese contexto, Andrés Mauricio Bolívar Arias ingeniero de sistemas de la Universidad Piloto de Colombia con Especialización en Gerencia de Proyectos de la Universidad del Rosario y MBA del Colegio de Estudios Superiores de Administración (CESA), comparte su experiencia de más de 15 años en la creación de nuevos productos y servicios ciudadanos digitales y la comercialización de otros basados en la tecnología.

A ese recorrido le suma su gestión como CEO de ReconoSER ID, con la "responsabilidad de planificar, organizar y dirigir la estrategia de soluciones para empresas 100% digi-

tales, que requieren perfilamiento y conocimiento de sus clientes en todo el territorio latinoamericano a través de sistemas biométricos", como él la define.

Su concentración en lo laboral no lo distrae de su tiempo en familia, de la buena mesa, del interés por conocer nuevas culturas, de jugar fútbol y de su pasión por los automóviles.

Revista Sistemas: *El concepto de resiliencia es bien conocido en el entorno personal del ser humano, cuando se trata de resiliencia digital ¿cuál es el alcance?, ¿qué contempla?*

Andrés Mauricio Bolívar A. La resiliencia digital de una organización es la capacidad de recuperarse de cualquier dificultad del negocio, identificando el nivel de debilidad digital que consideran acepta-

ble y su nivel de innovación. Contempla el análisis del negocio, procesos y personas, para identificar las consecuencias que traería una falta de resiliencia digital y construir escenarios sobre cómo estas pueden evolucionar.

RS: *¿Cómo debe prepararse una organización para el desarrollo de una infraestructura que cobije la resiliencia digital? ¿Cuáles son los elementos fundamentales en esa dirección? ¿De qué dependen?*

AMBA: La resiliencia digital es más que seguridad. Abarca agilidad y velocidad. Volverse más ágil con una capacidad más rápida para adaptarse a las condiciones cambiantes del mercado. Aplicar datos y gobernanza digital en toda la organización para una respuesta rápida a las interrupciones. Construir seguridad a través del cumplimiento automatizado de privacidad de datos y acceso de confianza cero. Mejorar y reforzar las experiencias de clientes, empleados y socios. Mejora continua de la velocidad y el tiempo de comercialización para aplicaciones innovadoras

RS: *¿En qué forma los directivos de una empresa deben prepararse para orientar los pasos a seguir basados en resiliencia digital? ¿Cómo definen esa estrategia?*

AMBA: Es importante que los directivos de las empresas comiencen a pensar en el POSCOVID, reconociendo que la normalidad que teníamos no regresará y para ello, es necesario analizar si los activos digitales y físicos implementados y en funcionamiento, son los adecuados. Algunos autores como McKinsey mencionan la adopción de las "5R": resolución, resiliencia, retorno, reinvención y reforma.

RS: *Considerando que es una labor especializada ¿cuál función debe desempeñar el área de tecnología y cómo la debe ejercer? ¿Es un trabajo en conjunto?*

AMBA: Es preciso revisar varios aspectos. Para las organizaciones en las que los ingresos y las utilidades vienen a la baja es necesario que las áreas de tecnología y TI revisen la reducción de costos en sus departamentos. La transformación digital en las empresas es vital, pero deben corresponder a un equilibrio entre las opciones de bajo costo y los servicios/soluciones *premium.* Es importante asegurarse de contar con los expertos adecuados dentro de la organización. Frente a la ausencia de habilidades y conocimientos, establecer unos planes de trabajo con el talento. Estar rodeados de los proveedores y socios apropiados, lo que implica ampliar el ecosistema para obtener más valor colaborativo.

RS: *¿Cómo se enmarca la resiliencia digital dentro de la ciberseguridad? ¿Se confunden? ¿En qué se diferencian? ¿Cuál es su costo-beneficio?*

AMBA: Es la capacidad de una organización en recuperarse de cualquier dificultad del negocio manteniendo metodologías de trabajo de

manera segura, por ello es necesario entender cuánto dependen de la tecnología digital y ser suficientemente conscientes de las oportunidades y riesgos que esto conlleva.

El enfoque resiliente de la ciberseguridad es defender los datos de forma dinámica y activa y, al mismo tiempo, hacer que funcionen para la organización; sin embargo, la resiliencia digital abarca mucho más, hablamos del negocio, los procesos y las personas.

RS: *Desde la perspectiva del ser humano, de sus actitudes y comportamientos ¿cómo se desarrolla una cultura empresarial orientada a la resiliencia digital?*

AMBA: Hay que asegurar que toda la organización incorpore el pensamiento de resiliencia con respecto a las amenazas y las oportunidades. Alentar y empoderar a las personas para que discutan críticamente las amenazas existenciales, con mecanismos de gestión adecuados para recopilarlas y analizarlas en combinación. Promover una cultura de comunicación temprana frente a los impactos potenciales de la debilidad digital. Esto conlleva a crear oportunidades al interior de la organización. Fortalecer la respuesta de la organización y su dirección, para establecer en dónde existen brechas en la toma de decisiones y la capacidad. Fomentar un empoderamiento del capital humano que se centre en un fuerte liderazgo empresarial y un equipo colaborativo y bien conectado. Controlar los efectos emocionales con un buen sistema de liderazgo empresarial y una cultura resiliente para que la plantilla de trabajo sea capaz de gestionar los cambios sin niveles altos de ansiedad y estrés.

RS: *Desde el punto de vista de la tecnología, ¿qué se requiere para desarrollar la resiliencia digital en una organización?*

AMBA: Las siguientes tecnologías son necesarias para desarrollar resiliencia digital: identidad digital, firma digital y electrónica, pagos en línea y factura electrónica. Todas estas tecnologías deben estar acompañadas de analítica de datos y de inteligencia artificial para mejorar la toma de decisiones.

RS: *Con base en su experiencia ¿cuáles modelos deben tenerse en cuenta para considerar una compañía madura en términos de resiliencia digital?*

AMBA: El primer paso para asegurar que una compañía es madura en términos de resiliencia digital, es que conozca sus fortalezas, debilidades, brechas y vulnerabilidades de su propia infraestructura digital. Así mismo, es necesario que la empresa presente una clara definición, planeación y ejecución de los siguientes desafíos de la resiliencia digital: privacidad y seguridad; capacidad de respuesta; capacidad de recuperación; confiabilidad y flexibilidad.

RS: *Imposible dejar de lado su opinión personal sobre el momento que vive la humanidad, los riesgos a los que está expuesta y la preparación para salir adelante.*

AMBA: Es claro que vivimos un momento difícil a causa del COVID-19 que deja millones de personas fallecidas alrededor del mundo (cerca a los cuatro millones de víctimas) y con ello, el confinamiento obligatorio que provocó la desaceleración económica de los países, dejando a su paso la quiebra de muchas compañías, la pérdida de empleo y mucha pobreza. Mientras la vacunación avanza, con mayor rapidez en algunos países que en otros, la virtualidad parece el único camino para que las oportunidades y los negocios no se detengan. Es aquí, en donde incorporar al ciclo de negocio herramientas que promuevan la *confianza digital* con clientes, aliados y proveedores, será la clave para generar un factor diferencial en el mercado.

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.*

XXI Encuesta Nacional de Seguridad Informática

Resiliencia un aspecto clave en la ciberseguridad

DOI: 10.29236/sistemas.n159a4

Resumen

La encuesta de seguridad informática, capítulo Colombia, soportada por la Asociación Colombiana de Ingenieros de Sistemas (ACIS) y realizada a través de Internet, entre los meses de abril y junio de 2021, contó con la participación de 173 encuestados, quienes con sus respuestas permiten conocer la realidad del país en esta temática. La distribución se hizo a través de las diferentes redes sociales, comunidades y grupos, y contó con la cooperación de otras asociaciones como ISACA Capítulo Bogotá, Tacticaledge, CISOS.CLUB, CISObeat (Perú) entidades y comunidades que colaboraron también con el diligenciamiento del instrumento. Sus resultados muestran la transformación de las prácticas de seguridad y control en el país, los cuales se contrastan con los referentes internacionales seleccionados para esta versión de la encuesta.

Palabras clave

Seguridad de la información, encuesta, líder, perfil profesional, riesgos de información.

Introducción

Entender la realidad nacional en materia de seguridad de la información y ciberseguridad, permite visualizar los retos a corto, mediano y largo plazo, además de construir mejores posiciones en las organizaciones. Ese entendimiento, sumado a conocer el contexto internacional, proporciona una proyección al entorno nacional para enfrentar los retos y desafíos en ambientes cada vez más permeados por la realidad digitalmente modificada.

De la misma manera que en otras versiones, la Encuesta Nacional pretende medir las dinámicas y lógicas de las empresas del país, ver otros referentes mundiales en la búsqueda y construcción de los propios.

Año tras año, este estudio ha reflejado cómo ha venido desarrollándose en Colombia la protección de la información en los entornos digitales y cómo en los diferentes sectores (industrial y empresarial), la seguridad y la resiliencia digital se convierten en un valor dentro de las organizaciones.

Es de resaltar el análisis longitudinal realizado sobre los últimos 10 años de la encuesta, sobre la variable incidentes que fue publicado en 2020 denominado “Evolución de los incidentes de Seguridad de la Información en Colombia: 2010-2020” (Cano & Almanza, 2020), como un registro analítico y documentado del pasado y una prospectiva sobre el futuro de la seguridad en Colombia.

Como todos los años, se revisan para la realización de este informe, algunos de los reportes más representativos de la industria, afines con los datos analizados de este instrumento.

Estructura de la encuesta

El estudio contempla 40 preguntas repartidas en varias secciones sobre diferentes asuntos.

Demografía: Describe la información del encuestado, cuáles son las tareas que realiza, la visión de la seguridad, además de los roles que en tal sentido puedan existir dentro de su organización. Datos que permiten ubicar el sector al que pertenece, el tamaño y tipo de empresa.

Presupuestos: Relaciona todos los aspectos asociados con los recursos financieros destinados en materia de seguridad y, sobre todo, en qué se concentra la inversión de dichos recursos.

Incidentes de seguridad: Muestra los detalles y tipos de incidentes presentados, un barrido por las prácticas más importantes en el manejo y diligencia de la evidencia digital, como herramienta en la persecución de los ciberdelincuentes.

Herramientas y prácticas de seguridad: Se refiere a las prácticas comunes en materia de seguridad, ese conjunto de acciones que permite a las organizaciones definir una postura clara en materia de protección.

Políticas de seguridad: Busca conocer el estado de las políticas de seguridad, la práctica de la gestión de riesgos y su integración en el contexto organizacional.

Capital intelectual: Busca definir cómo son las áreas de seguridad y las características básicas en materia de experiencia, formación y capacitación de los profesionales de seguridad. Muestra también la relación de las instituciones de educación superior frente a una realidad tan cambiante.

Temas emergentes: En esta sección se analizan varios aspectos, entre ellos: la percepción del futuro en materia de ciberseguridad; la vinculación de los directivos de la organización en la ciberseguridad empresarial, además de la responsabilidad y el papel del líder de seguridad en el desarrollo de la dinámica de protección de la empresa.

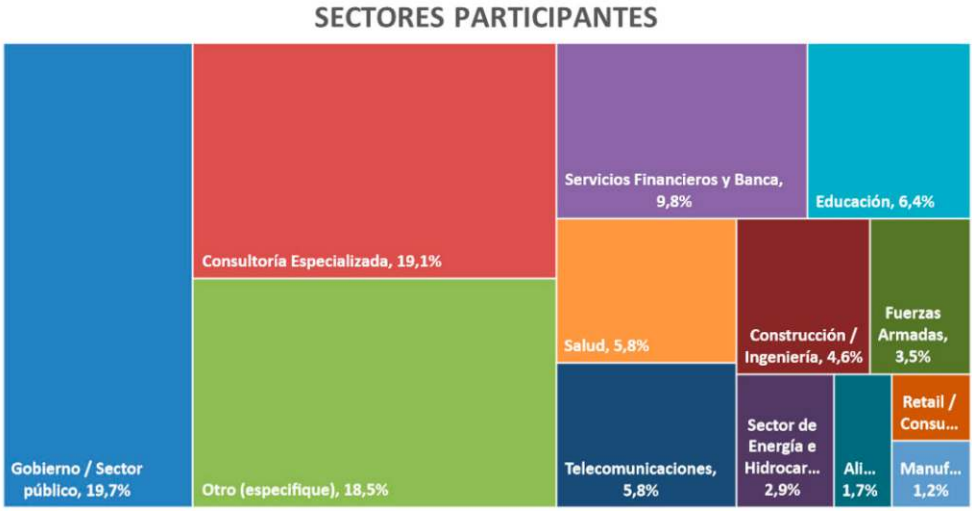
Cambios: Cada año luego de revisados los resultados de la encuesta, las opciones y los análisis correspondientes de pertinencia y relevancia, se cambian, adicionan, o modifican opciones. Este año no fue la excepción y tienen unas pequeñas variaciones en cuanto a la cantidad, pasando de 43 en el 2020 a 40 en el 2021.

Hallazgos principales

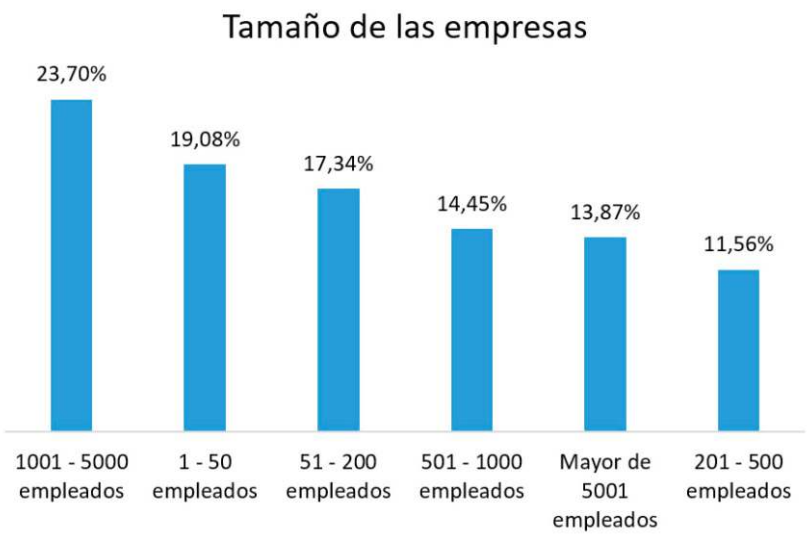
Demografía

Sectores participantes

La gráfica 1 refleja la participación de 13 sectores de la economía colombiana. Los tres segmentos con



Gráfica 1: Sectores participantes



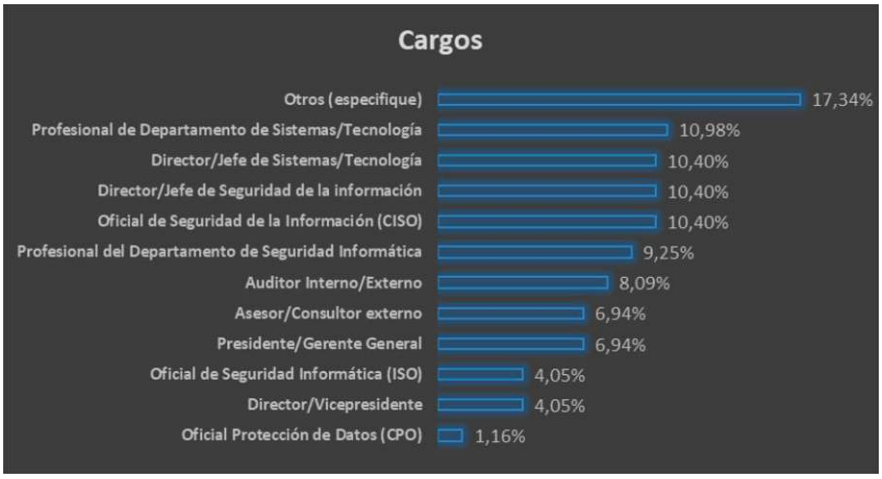
Gráfica 2: Tamaño de las empresas participantes

mayor participación de la encuesta para este año fueron Gobierno, Sector Financiero y la Consultoría Especializada.

En este año Gobierno, Consultoría, Otros sectores, Servicios financieros y Educación, son los principales grupos que participan en la encuesta.

La gráfica 2 muestra el tamaño de las empresas en Colombia, de acuerdo con el número de empleados y se puede observar la participación de empresas de todos los tamaños y cómo la ciberseguridad ha impactado sus operaciones.

La gráfica 3 muestra los cargos de los encuestados, entre los que se



Gráfica 3: Cargos de los encuestados

cuentan profesionales de las áreas de TI, oficiales de Seguridad, auditores internos y directores de Seguridad de la Información.

Así mismo, figuran otras clasificaciones para los profesionales de seguridad digital en el país, tales como analistas y profesionales de planta de seguridad, docentes de cátedra y planta de las áreas de seguridad como los más relevantes. Es importante considerar que existe una gran gama de roles que responden la encuesta y dan sus distintas visiones acerca de lo que representa la ciberseguridad en sus organizaciones.

En la gráfica 4 se observan las tareas realizadas por los profesionales de seguridad dentro de las organizaciones. Para este año, el porcentaje más alto está representado por la *definición de controles de TI en materia de seguridad de la información*, luego la *creación de programas de entrenamiento* y, en tercer lugar, *establecer e implementar un modelo de políticas*.

La gráfica está expresada con relación a los cambios que sufren las funciones del profesional de seguridad. Para este año se agregaron tres nuevas funciones: Definir, diseñar y velar por el programa de

Gráfica 4: Funciones del responsable de seguridad

privacidad de la información; definir o diseñar escenarios/simulaciones/Playbooks en relación con ciberriesgos y definir programas de resiliencia digital.

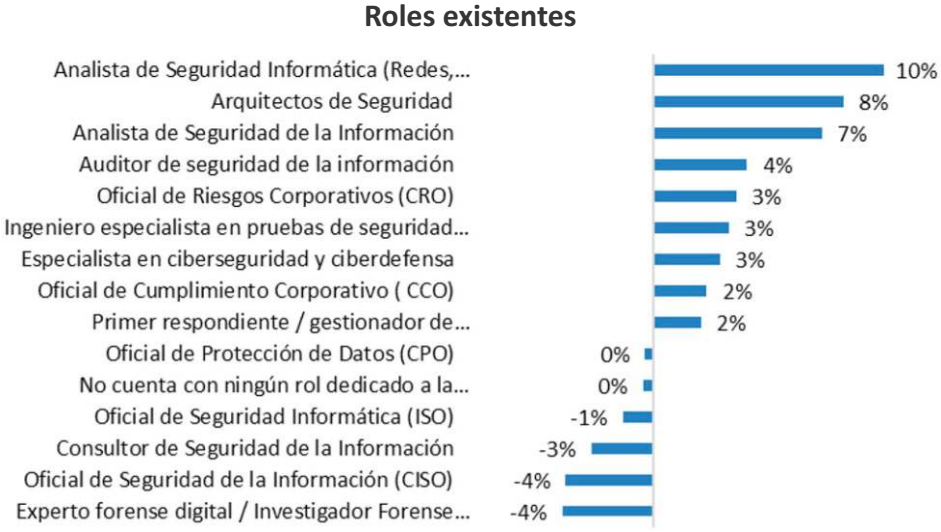
Frente al año anterior, las funciones que reflejan un incremento tienen que ver con la creación del programa de gobierno y gestión, la supervisión de los procesos de cumplimiento, además de velar por la protección de la información personal.

Los que tuvieron decrecimiento en comparación con el año anterior son la supervisión y gestión de los procesos de investigaciones forenses, la interacción con las diferentes áreas del negocio y el más bajo está relacionado con informar a la alta gerencia sobre el avance de los programas de seguridad en la organización.

Esto refleja la dinámica de lo que los profesionales de seguridad en tiempos disruptivos, como los actuales, deben atender y repensar frente a un programa de seguridad de la información: asegurar que se cumpla lo mínimo, para seguir en ese proceso de construir resiliencia digital.

La gráfica 5 muestra de quién depende el área de seguridad. Los datos indican que el área de seguridad depende de una dirección propia, Director/Jefe de Seguridad de la Información, seguido por la Vicepresidencia/Director Departa-

Gráfica 5: Dependencia del área de Seguridad



Gráfica 6: Roles de Seguridad

mento de Tecnologías de la Información y en tercer lugar del Director/Jefe de Seguridad Informática.

En la gráfica 6 se observan los roles dentro de una organización en materia de seguridad digital. En este año los analistas de seguridad de la información, de seguridad informática y el Oficial de Riesgos Corporativos (CRO) son los primeros roles presentes en las organizaciones.

Al comparar con el año anterior encontramos que las posiciones de analistas y arquitectos son las que mayor variación y presencia tienen en las organizaciones. Entre los roles que decrecieron figuran el consultor de seguridad, el CISO y el experto en forensia digital.

Consideraciones de los datos

Según El *Data Breach Report* (2021) de la Firma Verizon, el tamaño de las empresas sí importa. En su metodología señala que las empresas de menos de 1000 empleados son consideradas (SMB) (*Small, Medium Business*) y por encima de 1000 empleados grandes empresas.

Según este informe, se evidencia que a las empresas grandes y pequeñas las vienen afectando los fenómenos de ciberseguridad a nivel global. Si bien, los grandes titulares de la industria muestran los casos complejos como Solarwinds, Colonial, JBS, Fireeye, entre otros, han ocupado las primeras planas de los medios; no significa que la ciberseguridad en las empresas pequeñas no tenga relevancia.

Los roles y las responsabilidades de los profesionales de seguridad varían, y se mueven de acuerdo con los tiempos que actualmente son turbulentos, inciertos, novedo-

sos y ambigüos (Tessore, 2020). Según F-Secure en su reporte The CISOs' New Dawn (2021), los profesionales de seguridad tanto en Europa (57%) y en los Estados Unidos (59%) ven un claro incremento de responsabilidades en rol. Las temáticas adicionales están relacionadas con la privacidad (tendencia igualmente marcada en Colombia); hecho que confirma al no existir una persona responsable de la protección de los datos personales, lo que termina ubicando esta actividad como parte de las responsabilidades de los profesionales de seguridad.

Así mismo, la pandemia ha cambiado la realidad y ha definido nuevas normas para la protección de los activos digitales de las organizaciones; algunos inclusive empiezan a entender la dinámica del trabajo remoto como una realidad que llegó para quedarse y que significa repensar la forma en cómo las funciones de las áreas de seguridad deben rediseñarse; así lo muestra el informe de la firma Ivanti, titulado How the Pandemic Has Shifted CISO Priorities (2021).

El 93% de los profesionales de seguridad según Ponemon-LogRythm (2021) no reportan directamente al CEO, manifestando que hay al menos tres niveles para que la información llegue a quienes toman decisiones; en consecuencia, es necesario que la dependencia de la seguridad tenga impacto en el proceso de decisiones de la organización; entre más distancia existan entre el Líder de Seguridad Digital, su equipo y los cuerpos directivos, menos agilidad y fluidez en la toma de decisiones claves y mayor será el esfuerzo en el desarrollo de la ciberresiliencia de la organización.

En Colombia, si bien hay un director de seguridad nombrado o CISO como posición, esto no significa que esté reportando directamente a quienes toman decisiones; se ha avanzado en el tema, pero se requieren mayores esfuerzos en la materia.

Por tanto, esta realidad presenta nuevos aprendizajes en las funciones, roles y responsabilidades de los profesionales de seguridad que seguro en la realidad de Colombia no es distinta y que crea nuevas oportunidades para repensar lo que el profesional de seguridad hace, y hará según evolucionan los tiempos.

Presupuestos

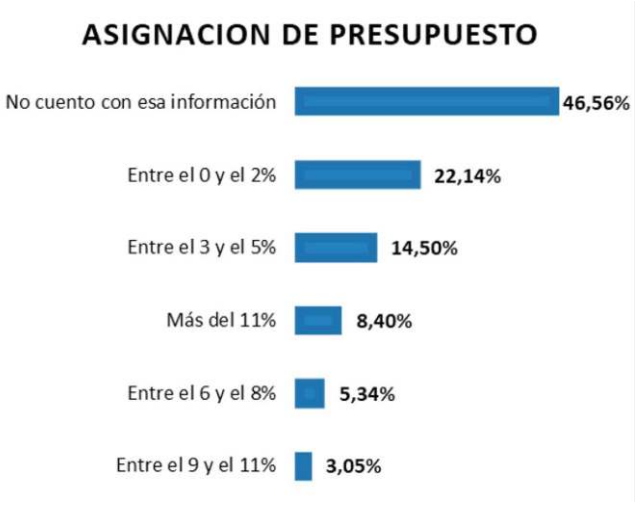
Continúa la asignación de presupuestos para la ciberseguridad; en esta oportunidad el 80% manifiesta tener asignado un presupuesto de seguridad en la organización. Gráfica 7.

La gráfica 8 muestra el monto del presupuesto en relación con el presupuesto global; cerca del 53% de los encuestados lo conoce, mientras que el 47% dice no conocer o no tener la información. Con rela-

Gráfica 7: Presupuesto de Seguridad

ción al año anterior, también incrementa el conocimiento del presupuesto asignado del total de la organización. De quienes conocen los montos asignados se puede observar que los montos inferiores al 5% del presupuesto global de la compañía representan el 69%, mientras que el 31% están para los montos superiores al 5%.

La gráfica 9 refleja la distribución de los presupuestos en dólares. Para este año cerca del 52% tiene un monto asignado para la seguridad; que aumenta, comparado con el año pasado cerca de un 7%, mientras el 48% restante manifiesta no conocer dicha información. Algunos movimientos interesantes al revisar y comparar con el año ante-



Gráfica 8: Porcentaje del presupuesto Global

Gráfica 9: Presupuesto de Seguridad

Gráfica 10: Inversión de Seguridad

rior. Aumenta en todos los rangos establecidos con excepción de las franjas de los $US110.000 a $US 130.000 y $US70.000 a $US 90.000 donde disminuye. No obstante, el mayor incremento en términos porcentuales es la franja de mayor de $US130.000, esto es claramente explicable por el hecho que las inversiones en seguridad cada vez son más especializadas y por tanto tienen mayores valores de inversión.

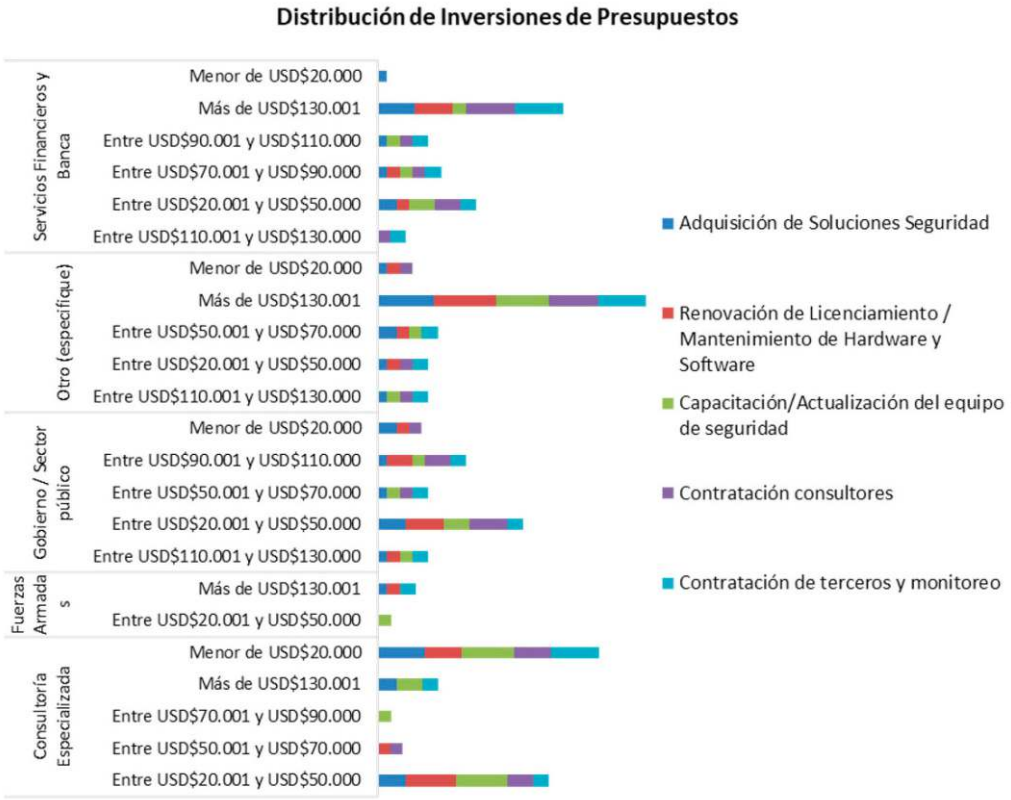
La gráfica 10 muestra la forma cómo se está invirtiendo el dinero en materia de ciberseguridad. Sigue creciendo la inversión en tecnologías de seguridad informática. Renovación de licenciamiento, Sensibilización, Contratación de consultorías y el Monitoreo son en su or-

den la forma en cómo se invierten estos presupuestos asignados.

En la gráfica 11 se puede observar la forma en cómo cada sector de la industria hace sus respectivas distribuciones de las inversiones en seguridad. Hay datos interesantes a observar, el sector financiero invierte en todas las franjas, llama la atención que las inversiones en la franja de más de $US130.000 dólares, es la que involucra a todos los tipos de inversiones, el mismo comportamiento lo mantienen otros sectores, y el sector de Fuerzas Armadas en menor proporción.

El sector de Gobierno mantiene su distribución de inversiones en la franja entre $US20.000 y $US-50.000 y $US90.000 y $US-110.000 dólares, como la distribución más alta; en el sector de la consultoría especializada las franjas más altas son todas las que están por debajo de $US50.000.

Al revisar la destinación de estas franjas se encuentra que la adquisición de soluciones de seguridad no es el primer destino de ninguno de los sectores de la industria principalmente, es solo la destinación de segunda importancia en el Go-



Gráfica 11: Montos en dólares de las inversiones de seguridad. Sectores vs. inversiones

bierno, Fuerzas Armadas, y otros sectores.

La renovación de licenciamiento y mantenimiento de *hardware* y *software* es la destinación primaria del sector de Fuerzas Armadas y otros sectores, mientras que es la segunda destinación de inversiones en sectores como la Consultoría especializada.

La Capacitación/Actualización del personal de seguridad de la información solo es la destinación primaria del sector de Consultoría y de ningún otro sector en segundo lugar. La Contratación de servicios de asesoría/consultoría es la destinación primaria de inversiones del sector Financiero, de otros sectores no lo es.

Los Servicios de monitoreo y gestión de seguridad con terceros, es de la destinación en primaria instancia del sector de Gobierno, mientras que la segunda destinación de inversiones del sector Financiero.

Consideraciones de los datos

Los reportes internacionales ratifican la tendencia de Colombia sobre los aumentos en los presupuestos de seguridad en las organizaciones de todos los tamaños y sectores. Sin embargo, al revisar el informe ISACA (2021) se muestran leves descontentos por la disminución de los presupuestos afectados por la situación disruptiva de la pandemia a nivel global. No obstante, en el mismo estudio se ve un optimismo al ver un incremento de los presupuestos en términos históricos, y en la misma línea se observa un optimismo moderado hacia los próximos 12 meses en relación con el incremento de estos.

En el informe de Ponemon-IBM (2020) el desafío se mantiene con relación a las inversiones de ciberseguridad, mientras que la sofisticación de los ataques incrementa. Son necesarias mayores inversiones en tecnologías, procesos y personas en la búsqueda de organizaciones más resilientes frente a los ciberataques, igual se considera en el informe que si bien los presupuestos mejoran, cerca del 40% considera como gran desafío la consecución de presupuestos acordes con la situación actual.

Todos los informes revisados durante el 2021 (ISACA, 2021; Ponemon-IBM, 2020, Vanti, 202x; Verizon, 2021) y otros son concluyentes en afirmar que el modelo de seguridad ha cambiado por las condiciones disruptivas de la pandemia, y sobre todo por los posibles escenarios del trabajo que vendrán en los próximos tiempos (CISOs. CLUB, 2021), lo que hará que los presupuestos en materia de seguridad cambien y las inversiones en seguridad se ajusten con estos nuevos escenarios.

Sin perjuicio de lo anterior, las inversiones en seguridad se consideran insuficientes para invertir en las

tecnologías más avanzadas requeridas para atender escenarios disruptivos, como lo manifiesta el 63% de los encuestados del informe de Ponemon-LogRhytmn (2021).

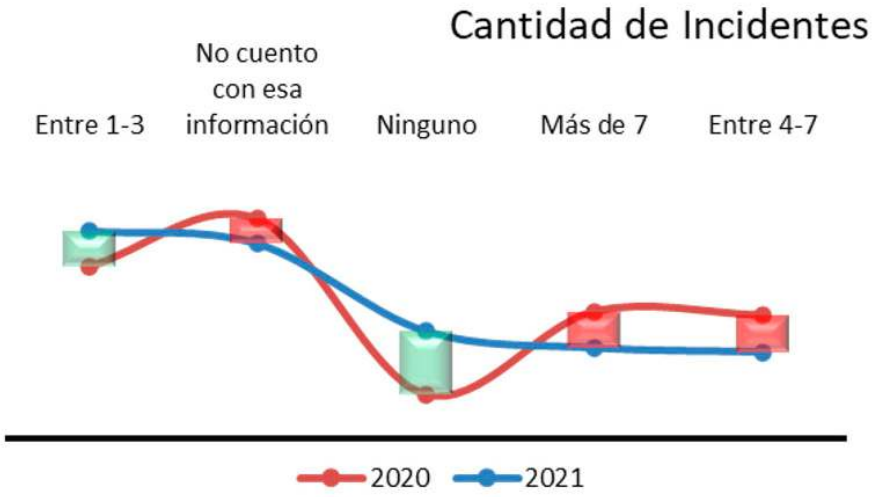
Incidentes

En Colombia se mantiene la tendencia en materia de incidentes de seguridad en concordancia con las tendencias internacionales. Tales desafíos, en términos de preparación y atención son una exigencia para las organizaciones.

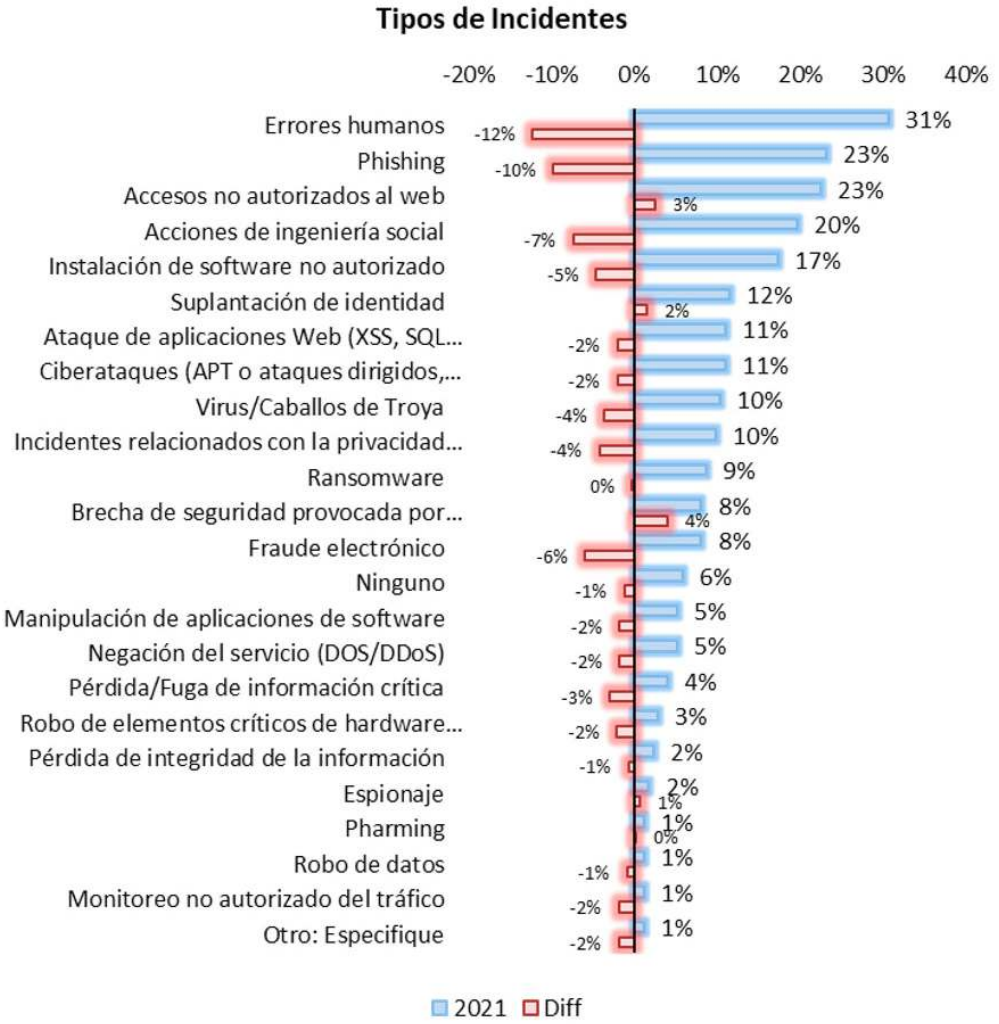
La gráfica 12 muestra la cantidad de incidentes que se presentan en Colombia, según los participantes. Para este año el 72% de los encuestados manifiesta que ha estado en contacto con algún incidente de seguridad en su empresa, en comparación con el año inmediatamente anterior, donde el 68% lo ha manifestado.

En este año, en comparación con el anterior, hay una disminución de las personas que manifiestan no tener conocimiento sobre los incidentes de seguridad, pasando del 32% en el 2020, al 28,31% en el 2021. Llama la atención que hubo un incremento del 9% de aquellos que manifiestan no tener incidentes de seguridad, y la disminución de un 5% en las franjas de incidentes entre 4 y 7 y más de 7 respectivamente. Por el otro lado, se incrementa un 5% de quienes manifiestan tener entre 1 y 3 incidentes en sus organizaciones.

La gráfica 13 relaciona los tipos de incidentes que se presentaron en las organizaciones, así como su variación con relación al año anterior. Para este año hay datos interesantes, se mantienen los errores humanos como el tipo de incidente más reportado; sin embargo, de-



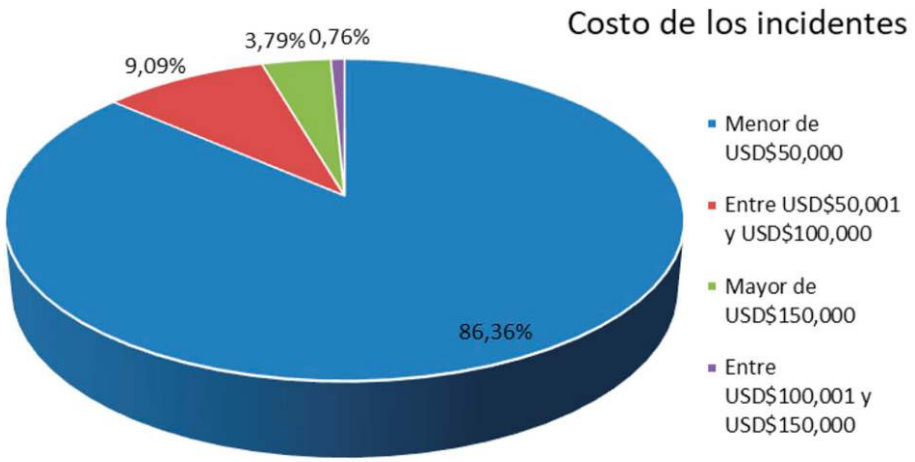
Gráfica 12: Cantidad de Incidentes. Incidentes



Gráfica 13: Tipos de Incidentes de Seguridad

crece un 12% frente al año anterior. Las brechas de seguridad provocadas por terceros es el tipo de incidente que mayor crecimiento con un 4%, seguido de acceso no autorizados en la web (3%) y suplantación de identidad (2%).

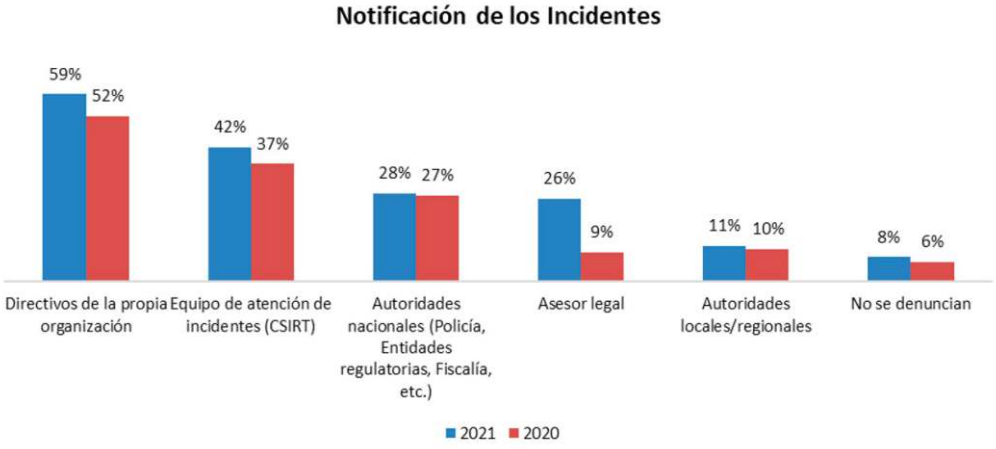
La gráfica 14 representa el costo promedio de los incidentes. Al igual que el año anterior los datos reflejan que hay costos involucrados en relación con los incidentes de seguridad; cerca del 86% manifiesta que sus incidentes cuestan menos de $US50.000, cerca del 9% entre $US50.000 y $US100.000, el 4% manifiesta que le cuesta más de $US150.000 y solo el 1% manifiesta que está en la franja de los $US100.001 hasta los $US150.000 dólares.



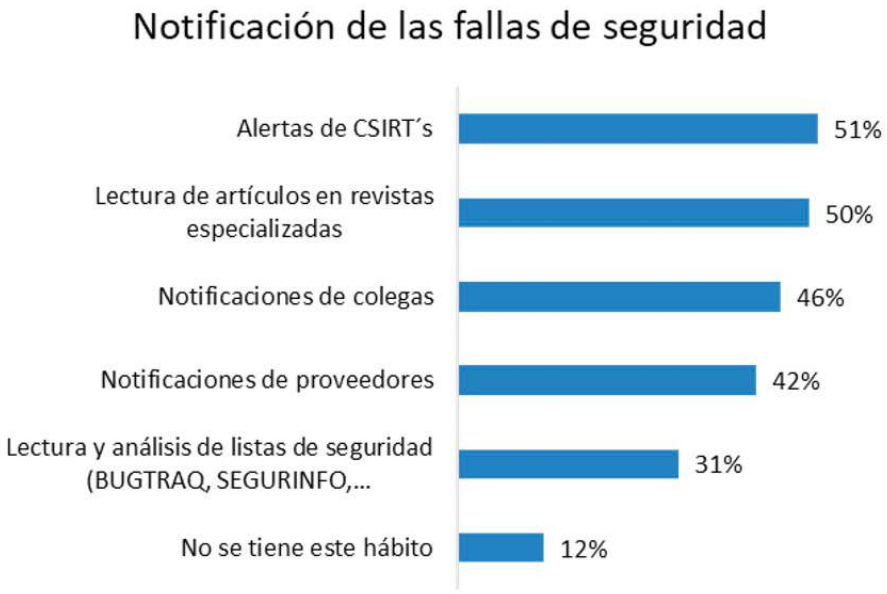
Gráfica 14: Costos de los Incidentes

La gráfica 15, muestra ante quién se reportan los incidentes de seguridad. El 59% lo reporta directamente a los directivos de la organización, el 42% lo reporta al equipo de atención de incidentes (CSIRT), el 28% a las autoridades nacionales, el 26% a los asesores legales, el 11% a autoridades locales o regionales y solo el 8% manifiesta que no se denuncian.

La gráfica 16, muestra las razones, como se mantienen los profesionales de seguridad informados acerca de las vulnerabilidades y fallas de los sistemas. Se encuentra que el 51% de los profesionales de



Gráfica 15: A quien se reportan los incidentes



Gráfica 16: Razones para no denunciar los incidentes

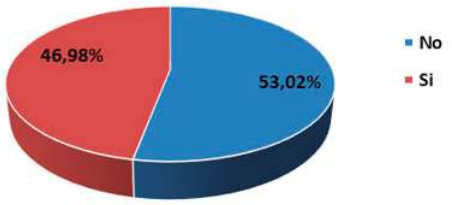
seguridad se enteran o están conectados con CSIRTs, las revistas especializadas son el segundo recurso usado con un 50%, seguido por la notificación con los colegas 46%, luego el contacto con los proveedores (42%), listas de seguridad el 31% y solo el 12% manifiesta no tener ese hábito.

La gráfica 17 resalta que el 61% mantiene algún tipo de contacto con autoridades del orden local o regional, mientras que el 39% no lo hace

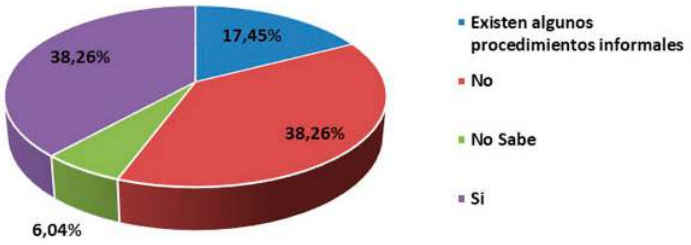
La evidencia digital y su uso dentro del proceso de gestión de incidentes es pieza fundamental para un

Gráfica 17: Mecanismos para denunciar/compartir

Gráfica 18: Consciencia de la Evidencia Digital



Gráfica19: Procedimiento de Gestión de Evidencia Digital



Gráfica 20: Implementación de procedimientos de evidencia digital

adecuado mejoramiento. La gráfica 18, resalta la importancia y consciencia en relación con el adecuado manejo de la evidencia digital. El 73% resalta que es consciente de ello, el 14% no lo es y el 13% restante no sabe del tema. La gráfica 19 muestra que el 53% manifiesta tener un procedimiento aprobado para manejo de la evidencia digital y el 47% no lo tiene. La gráfica 20 para este año quiso revisar qué tan

implementados están dichos procedimientos, el 38% manifiesta que existe un procedimiento formal al respecto y el 17% manifiesta que existe informalidad en dichos procedimientos. El 38% indica no tenerlos y solo el 6% no sabe si existe algún procedimiento implementado.

Consideraciones de los datos

Los reportes internacionales como Verizon (2021) señala que al menos ellos han podido analizar cerca de 29.207 incidentes y que de ellos 5.258 se confirmaron como brechas de seguridad. Algunos datos interesantes indican que el 85% de las brechas involucran a las personas, el 61% a las credenciales y el robo de estas, confirmando la tendencia en Colombia.

El mismo informe advierte que la media del costo de un incidente está en $US21.659; sin embargo, el rango total de los incidentes está entre $US865 y $US653,587. Si bien en Colombia estamos en el rango de la media, hay que resaltar que puede haber mediciones inexactas frente a los costos, toda vez que los incidentes como el *Ransomware* generan un costo adicional, que a lo mejor no se ha considerado.

Ransomware definitivamente ha sido el incidente del año 2020; si bien en Colombia es un incidente que se mantiene con niveles bajos en su ejecución, puede no estar en el radar de los profesionales de seguridad, toda vez que desde el año 2020 y hasta la fecha en el 2021, se han visto muchos casos de este tipo, en donde el promedio de pago es de $US170.404 según Sophos (2021). Lo mismo se puede evidenciar en el informe del FBI (2021) que resalta la importancia que ha cobrado el *ransomware* como el incidente que hoy se está considerando a nivel de los estados como un ataque terrorista, con el fin de darle toda la atención de acuerdo con las exigencias de esa clasificación.

Los incidentes cada vez son más serios y complejos de investigar afirma el reporte de CyberEdge Group (2021). En este sentido, se aumentan las iniciativas, cerca del 70%, que permitan mejorar la capacidad de las organizaciones para responder a incidentes, según lo manifiestan IDG (2021). Estos datos confirman los resultados de Colombia, donde el proceso de atención de incidentes es esencial, y por lo tanto debe mejorarse continuamente pese a las presiones propias de dicho proceso: dar respuesta al incidente, investigar el incidente y hacer un manejo adecuado de la evidencia digital.

Definitivamente manejar evidencia, poseer un proceso y tenerlo implementado es indispensable si se quiere tener un proceso de gestión de incidentes robusto y que apalanque la resiliencia digital de las empresas. En el informe de CyberEdge Group (2021), el 13% de los

encuestados no considera usar alguna solución de esta naturaleza, el resto o ya las tiene en uso, o planea usarlas. Por tanto, ratifica lo que está sucediendo en Colombia en este aspecto, es importante y hay que trabajar más en dirección a fortalecer la implementación de este tipo de procedimientos.

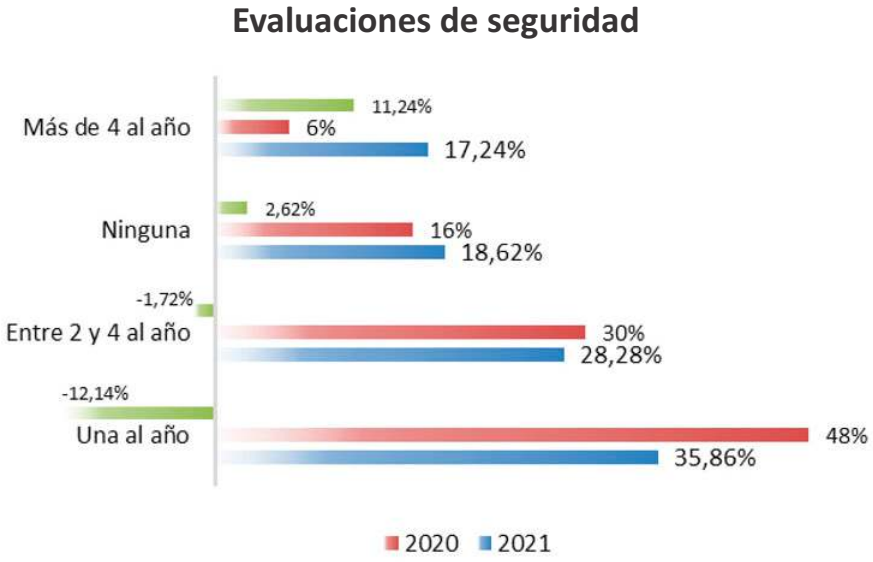
Accenture (2020), indica que la respuesta de incidentes como proceso de la organización se ha incrementado en términos de las inversiones de seguridad, al menos un 25%. Estos datos soportan y ratifican lo que sucede en Colombia, los incidentes tienen presencia, tienen costos y tienen impacto. Accenture (2020) igualmente muestra que el 79% de las empresas bajo estudio están de acuerdo con la colaboración y cooperación entre empresas, como mecanismos para estar mejor preparados para enfrentar los ciberataques, ratificando la tendencia de Colombia en ese sentido.

Los profesionales de seguridad se mantienen informados y usan la práctica de leer artículos y publicaciones especializadas, tendencia que se ratifica a través del informe de Verizon (2021), el cual señala que las investigaciones de seguridad son las formas más utilizadas para descubrir brechas de seguridad.

En Colombia, la práctica de la gestión de incidentes se identifica como una práctica no desarrollada, pero con avances importantes, resultado que ratifica los hallazgos del informe de IDC (2021), según el cual las inversiones en seguridad están orientadas a fortalecer la gestión de incidentes, toda vez que se considera una práctica que necesita mejorar su madurez en las organizaciones para así fortalecer la resiliencia digital.

Todos los grandes informes de la industria concuerdan en confirmar la tendencia de Colombia, en el sentido de que la gran mayoría de organizaciones sufrieron, sufren y sufrirán de un ciberataque; por tanto, la premisa del cuándo, cómo, el porqué, son innecesarias de responder, hoy estamos más ante la necesidad de saber que hacer en el momento de la crisis.

La ciberresiliencia es una capacidad de las organizaciones, que debe ser desarrollada de manera integral en las organizaciones, aquellos tiempos en donde los incidentes de seguridad son atendidos solo por el área de seguridad y de tecnologías de la información están desapareciendo, tal vez pueda darse para incidentes básicos (EY & IIA, 2021); sin embargo, en incidentes complejos en los que la recuperación y la respuesta demandan mayores esfuerzos e involucran a muchas partes, la gestión de incidentes demanda un proceso multidisciplinario; tener planes claros, con ejercicios probados puede ser la clave para que este proceso sea de utilidad en los momentos de crisis.



Gráfica 21: Evaluaciones de Seguridad

Herramientas

La gráfica 21 muestra el uso de las evaluaciones de seguridad como una de las prácticas más usadas. Un 81% de los participantes manifiesta hacer uso de esta práctica como instrumento clave para validar el estado de la seguridad digital de la organización. El 36% de los participantes usa esta práctica una vez al año; el 28% entre dos y 4 veces al año; el 17% manifiesta usa más de 4 veces al año y el 19% dice no usarla.

La gráfica 22 indica cómo los sectores están usando las evaluaciones de seguridad para evaluar y valorar su postura de seguridad; en tal sentido se observa que en pro de mejorar su ciberresiliencia, quien más usa una evaluación de seguridad al año es el sector gobierno con un 10,34%, seguido del sector de la consultoría especializada con un 9,66%. Entre dos y cuatro valoraciones al año se ubican la consultoría especializada con un 6,90%, seguido los servicios financieros con un 6,21%. Ninguna evaluación de seguridad al año está dentro de otros sectores; el segundo lugar es para el sector salud con un 2,76%. Más de cuatro evaluaciones de seguridad al año están dentro de otros sectores, seguido de la consultoría especializada con un 4,14%.

Cabe resaltar que los servicios Financieros y el sector de *Retail* no dejan de hacer pruebas de seguridad durante un período de un año. Por lo demás, los restantes sectores no ejecutan pruebas de seguridad.

La gráfica 23, muestra cuáles son los mecanismos de seguridad co-

Gráfica 22: Evaluaciones de Seguridad por Sectores

múnmente usados en las organizaciones. VPNs 53%, el cifrado de datos con un 49% seguido de las soluciones *antimalware*; sin embargo, comparado con el año inmediatamente anterior, son los servicios de inteligencia de amenazas el 7% las soluciones de seguridad con Inteligencia Artificial (IA) 5% y el cifrado de datos con 4% los que tienen un incremento en su uso frente al año 2020.

La gráfica 24 muestra la forma como los sectores principales de la industria usan los diferentes tipos de tecnologías con relación a la ciberseguridad. El sector financiero se concentra en la tercerización de la seguridad, seguido de las soluciones de monitoreo de redes sociales y luego herramientas que le permitan dar cumplimiento a los marcos normativos. El sector Gobierno por su parte se concentra en herramientas de denegación de servicio, seguido de las tecnologías tradicionales de firewall y las vpns. La consultoría especializada tiene como herramientas primarias, las soluciones de seguridad con IA, seguido de los sistemas de contraseña y las soluciones con enfoque de zero trust.

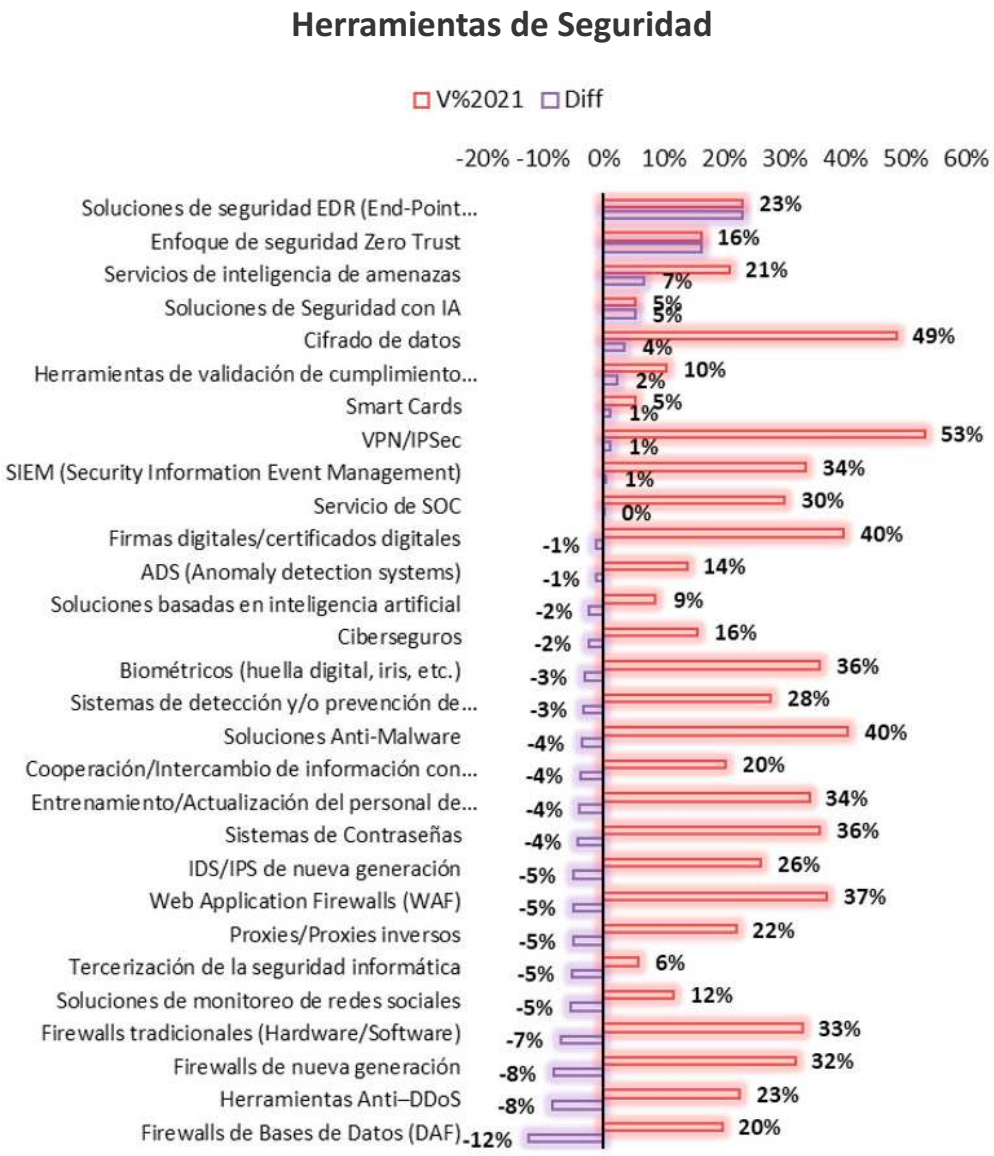
Llama la atención que el sector salud y otros sectores, también han estimado que las primeras soluciones de seguridad sean aquellas que usan la IA.

Consideraciones de los datos

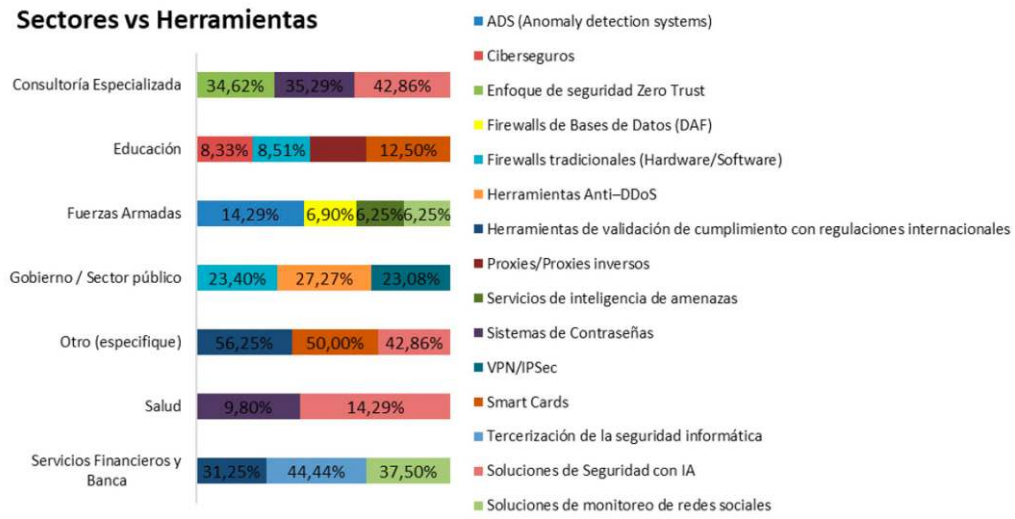
La tendencia en el uso de mecanismos de seguridad se mantiene al compararse con los años anteriores, sin perjuicio de algunas pequeñas variaciones en los mecanismos tradicionales. Para este

año se agregaron nuevas soluciones, como el enfoque de Zero Trust, las soluciones de EDR, las cuales ya se reporta su uso en el sector de la Consultoría especializada, otros sectores, el sector de Gobierno, y los servicios Financieros.

En el estudio de Ponemon-IBM (2020), se resalta que las empresas están tendiendo a usar herra-



Gráfica 23: Mecanismos de Seguridad usados



Gráfica 24: Mecanismos de seguridad en Sectores

mientas de automatización para la seguridad, tales como herramientas de inteligencia artificial y máquinas de aprendizaje, movimiento que también se ve como tendencia de Colombia.

La tendencia de seguir invirtiendo en tecnologías y servicios de seguridad se confirma, no solo son las soluciones actuales, sino en todo aquello que tiene enfoque de nube también muestra un profundo interés. Según CyberEdge Group (2021), el incremento en soluciones de seguridad orientadas a la red como IDS/IPS, Firewall de nueva generación, soluciones de Data Loss Prevention (DLP), están en los principales rubros de inversión.

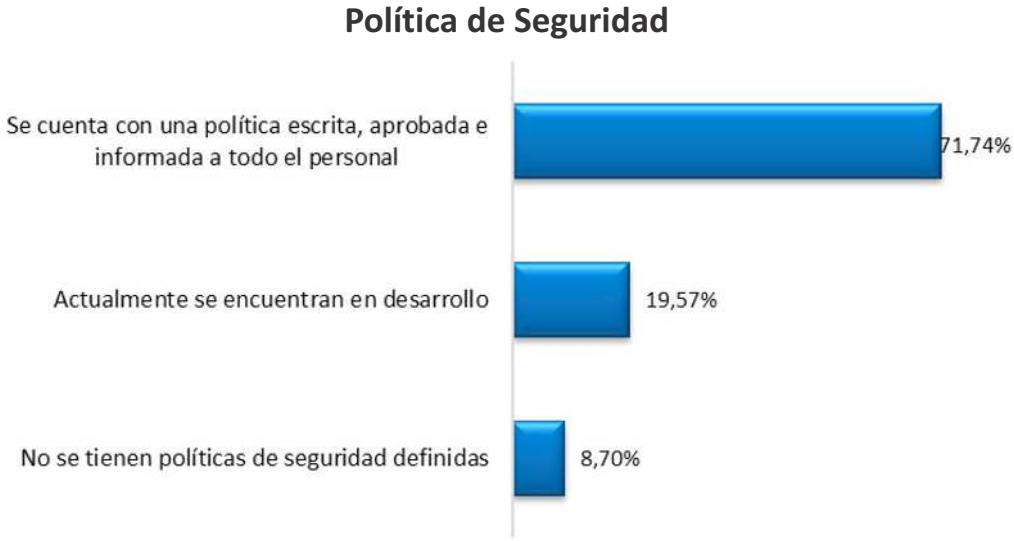
En relación con la protección de estaciones de trabajo el mismo informe resalta que las soluciones *antimalware*, cifrado de discos, antivirus avanzados basados en inteligencia artificial también están considerados.

En cuanto a la protección de la capa de aplicaciones, los *Firewalls Web*, de bases de datos la protección de APIs son los controles que más se están usando y se tiene proyectado utilizar.

Políticas

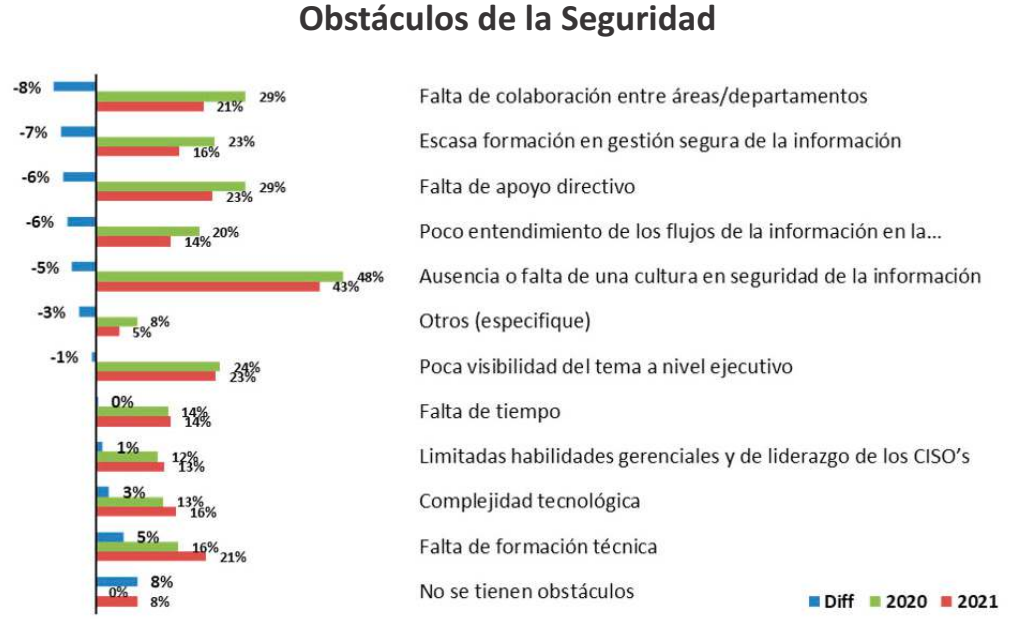
La gráfica 25 refleja el estado de las políticas de seguridad en las organizaciones colombianas; el 72% de los encuestados manifiesta que tienen formalizada sus políticas de seguridad, el 20% actualmente en desarrollo y solo el 8,7% señala no tener políticas de seguridad de la información.

La gráfica 26, muestra lo que manifiestan los participantes al indagar por los obstáculos por los cuales no

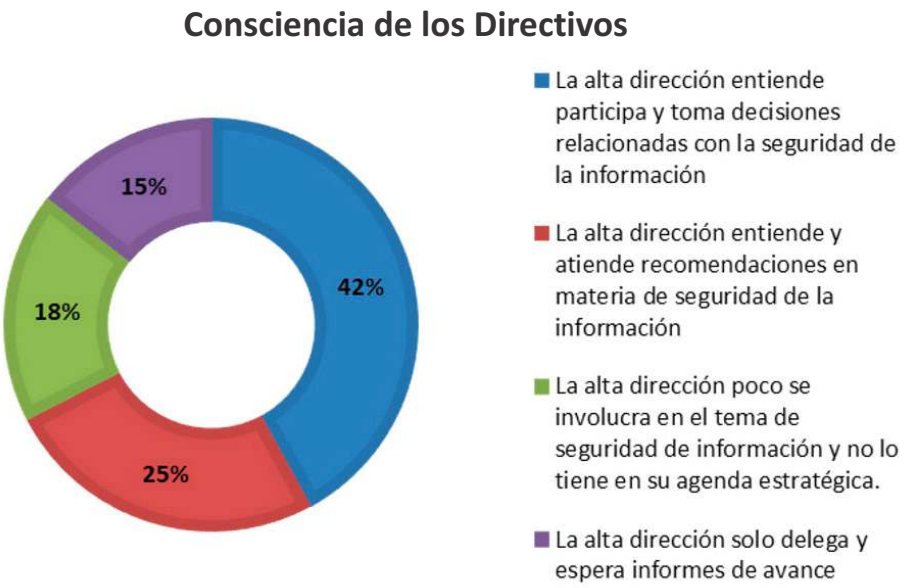


Gráfica: 25 Estado de las Políticas

hay una postura adecuada de seguridad en sus empresas. Ausencia o falta de cultura de seguridad 43%, la poca visibilidad a nivel ejecutivo 23% y la falta de apoyo directivo 23% son los tres principales motivos del año 2021. Sin embargo, al comparar con el año inmediatamente anterior estos tres elementos principales decrecen de



Gráfica 26: Obstáculos de la Seguridad



Gráfica 27: Consciencia de los directivos

manera interesante. Lo que más crece frente al año anterior es la falta de formación técnica 5%, la complejidad tecnológica 3% y las limitadas habilidades gerenciales de los CISOs con un 1% en total, todos los demás criterios descienden en comparación con el año inmediatamente anterior.

La gráfica 27 refleja el nivel de consciencia de los directivos en materia de seguridad, encontrando que la alta dirección entiende participa y toma decisiones relacionadas con la seguridad de la información en 42%, la dirección entiende y atiende las recomendaciones en materia de seguridad de la información 25%, la dirección poco se involucra en el tema 18% y la alta dirección solo delega y espera avances de informes un 15%; al revisar con el año inmediatamente anterior, se tiene una mejora significativa en este aspecto, crece cerca de un 10% el involucramiento de las altas direcciones y su activa participación en la toma de decisiones, y decrecen los demás criterios.

La gestión de riesgos como parte estructural de las funciones y tareas de los responsables de seguridad y sus organizaciones es otro de los componentes claves.

En la gráfica 28, el 79% de los participantes hace una evaluación de riesgos de seguridad digital y la incluyen en sus ejercicios globales de gestión de riesgos, mientras que solo el 21% no lo hace. La gráfica 29 muestra la frecuencia de ejecución de las evaluaciones de riegos, el 50% manifiesta que al menos la ejecuta 1 vez al año, el 26% más de dos y solo dos el 24%.

Gráfica 28: Evaluaciones de Riesgos

La gráfica 30, muestra las razones de por qué no es realizada la gestión de riesgos. El primer motivo que resaltan los participantes está relacionado con no tener un proceso formal de gestión de riesgos (28%), seguido del desconocimiento del tema 28%, así como informar que ya está incluido en el proceso de gestión de riesgo empresarial 28%, la falta de presupuestos 14% y la última consideración se relaciona con no tener asociados riesgos al tratamiento de la información con un 3%

La Gráfica 31 muestra el tipo de metodologías usadas al realizar los ejercicios de gestión de riesgos de seguridad; la ISO 31000, con un 39%, es la metodología más usada; comparado con el año anterior es la que mejor crecimiento tiene. ERM (*Enterprise Risk Management*) como metodología sigue en segundo lugar y para Colombia SARO (Sistema de Administración de Riesgo Operativo) es el tercer escaño.

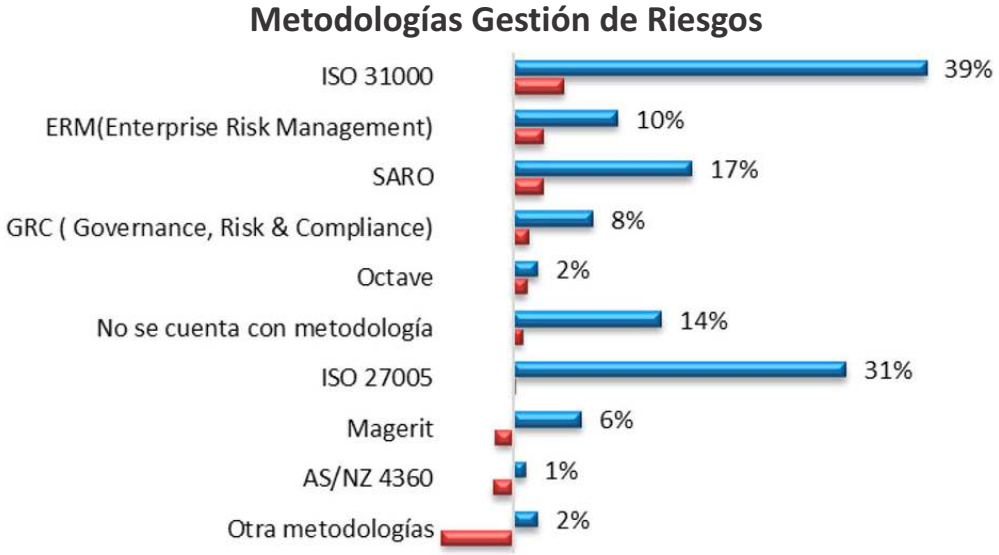
La Gráfica 32 muestra el tipo de riesgo usado para representar los

Gráfica 29: Evaluaciones de Riesgos

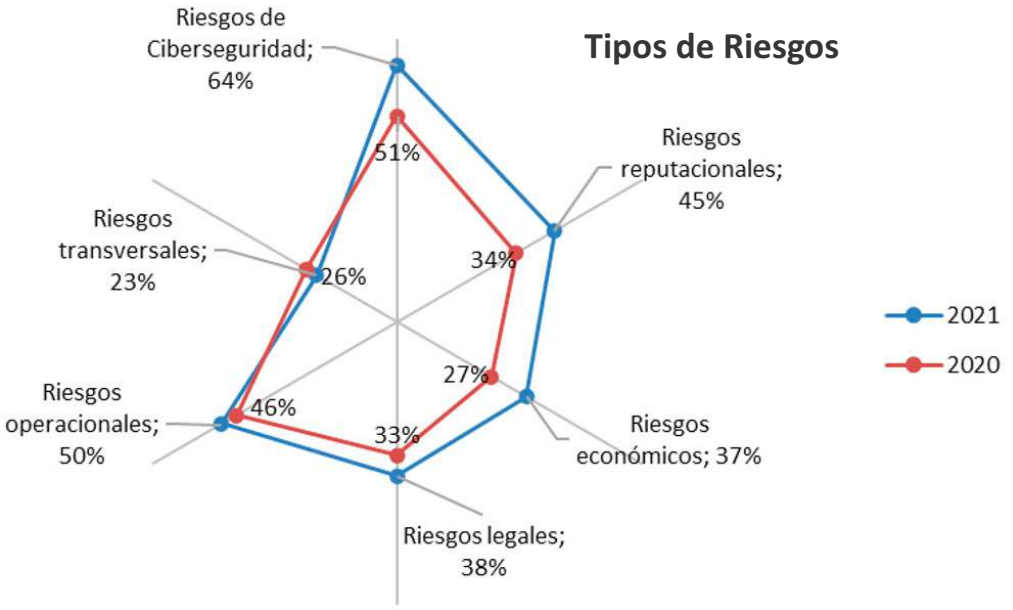
Gráfica 30 Razones para no realizar la gestión de riesgos

incidentes de seguridad en las organizaciones. Todas las categorías tienen incrementos importantes; al revisar los detalles vemos que los riesgos de tipo económico tienen un crecimiento del 37%, los riesgos reputacionales 33%, los riesgos de ciberseguridad 25%, riesgos legales 16%, riesgos operacionales 9%, los riesgos transversales decrecen el 11%

La gráfica 33 ilustra el uso de los distintos marcos de trabajo (*frame-*



Gráfica 31: Tipos de Metodología

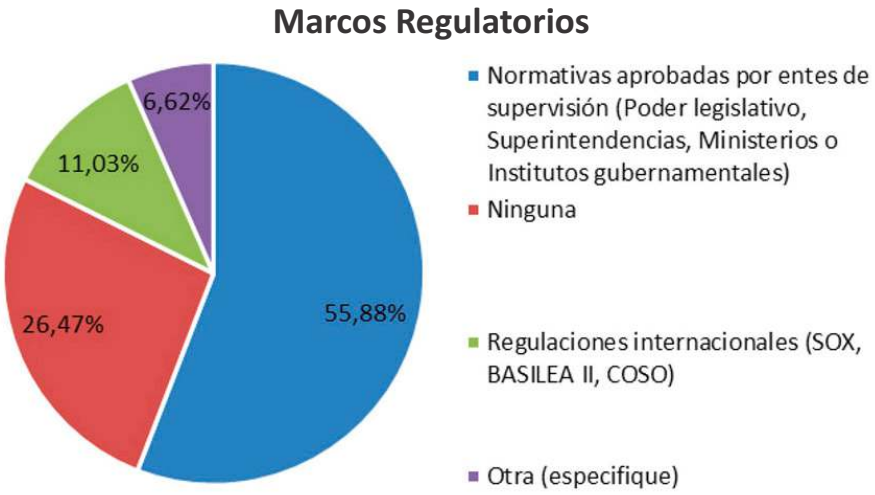


Gráfica 32: Tipos de Riesgos

works) usados en las organizaciones colombianas: ISO/IEC 27001, NIST, ITIL y COBIT son los más usados. Disminuye contra el año anterior el no usar ningún marco de buenas prácticas.

La gráfica 34 refleja las regulaciones que las organizaciones deben asegurar. En el caso colombiano, el 74% de los participantes manifiesta que sí existen regulaciones que se deben cumplir, bien sea en un mar-

Gráfica 33: Marcos de trabajo usados



Gráfica 34: Regulaciones o normativas

co nacional o internacional al que estén sometidos, mientras que el 26% considera que no está sujeto a cumplir ningún marco regulatorio o normativos.

Consideraciones de los datos

Los riesgos de seguridad de la información y ciberseguridad en definitiva son una realidad como lo es ratificado en el informe del Foro Económico Mundial (WEF, 2021), el cual manifiesta que la prioridad de estos tipos de ataques es alta en las organizaciones del mundo.

La confianza en los entornos digitales y la construcción de la capacidad de ciberresiliencia se fundamenta en una estructura de gobierno de la seguridad, en la que las políticas, la gestión de riesgos y el conjunto de buenas prácticas se convierten en elementos centrales para dirigir los programas de ciberseguridad. La conexión entre una estrategia de seguridad y los objetivos de seguridad que sean claros ayudaran a construir y fomentar la ciberresiliencia (World Goverment Summint – EY, 2020).

Confianza digital, va más allá de las tecnologías que puedan ser de utilidad para protegerse del adversario digital, implica componentes como la gestión de riesgos, como la ética en el manejo de los datos, el uso de buenas prácticas, y la participación de todos los actores de un ecosistema digital que cada vez es más complejo (Deloitte,2021).

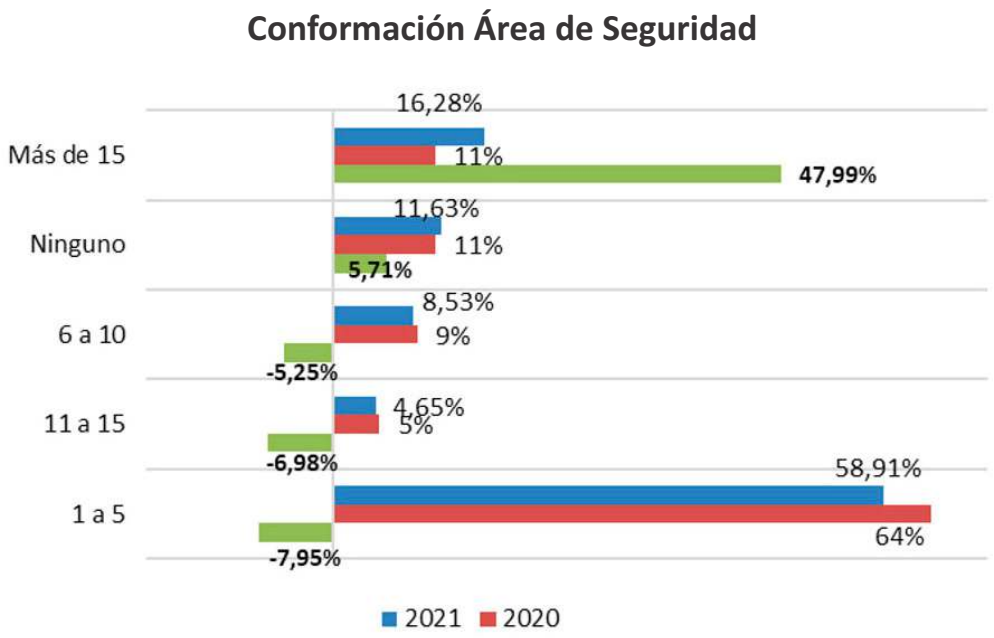
Así mismo, el informe de Deloitte (2019) resalta que el 50% de los participantes usan metodologías de riesgos y la cuantificación de estos como instrumentos y prácticas sólidas para la atención de los ciberataques de seguridad en las empresas.

Con relación a las políticas y su adopción, la tendencia en Colombia

para contar con un modelo fortalecido de políticas de seguridad y control es ratificado con el informe de CISCO (CISCO, 2020), el cual muestra que las compañías que se adhieren a sus prácticas, políticas de seguridad tienen costos menores por brechas relacionadas con los datos en comparación con quienes no lo hacen, lo cual puede apoyar el comportamiento de Colombia en este sentido.

Cada vez más toda la organización como un organismo vivo, desde sus niveles directivos deben entender desde lo más profundo lo que significa gobernar los riesgos en el contexto digital, es imperativo para desarrollar mejores modelos sostenibles en los ambientes digitales disruptivos en los que se desenvuelven las organizaciones de hoy y del futuro. (EY & IIA, 2021)

Situaciones como la evolución de los adversarios, la pandemia y la realidad digital de las organizaciones han cambiado la forma de ver la ciberseguridad, y así mismo la necesidad de repensar las prácticas de gestión de riesgos, de solo entender que es necesario proteger una infraestructura a defender y anticiparse de un adversario digital, para ello se requiere que lo fundamental se consolide en las organizaciones y así poder dar pasos más importantes que permitan evolucionar en la práctica de la ciberseguridad, que desarrolle mejores posturas de seguridad y que repercutan en una adecuada ciberresiliencia.



Gráfica 35: Tamaño del área de seguridad.

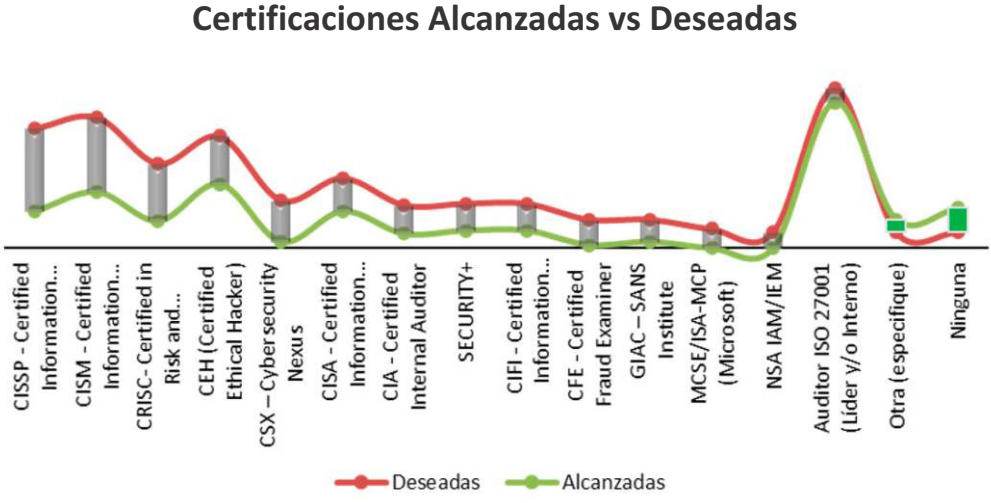
Capital intelectual

La gráfica 35 relaciona los recursos dedicados a la seguridad en las empresas, cerca del 88%, manifiesta tener recursos dedicados a la seguridad, la predominancia es de 1 a 5 con un 59%. Sin embargo, al revisar los datos contra el año 2020, encontramos que hay una variación importante, crecen las áreas de seguridad en un 48% en el rango de más de 15 personas, crece un 5% no tener recursos asignados a la seguridad, y decrecen las demás franjas.

La gráfica 36, representa la comparación de las certificaciones que los profesionales de seguridad han alcanzado en la actualidad y que desean alcanzar en el tiempo. CISSP, CISM, CRISC y CEH y CSX, son las certificaciones que mayor variación tienen entre lo que se tiene actualmente y lo deseado en el futuro. Resaltar que cada vez más son menos personas las que no están en el grupo de no poseer alguna certificación

Para este año se ha decidido incluir una nueva variable en relación con la preferencia que tienen los profesionales de seguridad sobre su formación. La gráfica 37, indica que las certificaciones son la primera opción con un 60% y el 49% la educación formal como segunda opción, entendida como todos los programas ofrecidos por la universidad como (pregrado, postgrado).

Al revisar los datos en profundidad se encuentra que los CISOs prefieren en primera instancia las charlas especializadas con un 42% y los programas de formación ejecutiva con el 38%, mientras que los directores de seguridad prefieren la educación formal en primer lugar 30,30% seguido de los cursos cortos con el 30%. El profesional de



Gráfica 36: Certificaciones alcanzadas vs deseadas

Gráfica 37: Preferencias de formación

seguridad prefiere para su formación los diplomados (33%) seguido de las charlas especializadas (32%). El Oficial de Seguridad Informática para desarrollar sus competencias y habilidades, prefiere los cursos cortos 20% y los diplomados (17%). Los profesionales con el cargo de privacidad prefieren los programas de formación ejecutiva (8%) seguido de las certificaciones con un 2%.

La Gráfica 38, muestra las brechas que se identifican para los profesionales de seguridad en la actuali-

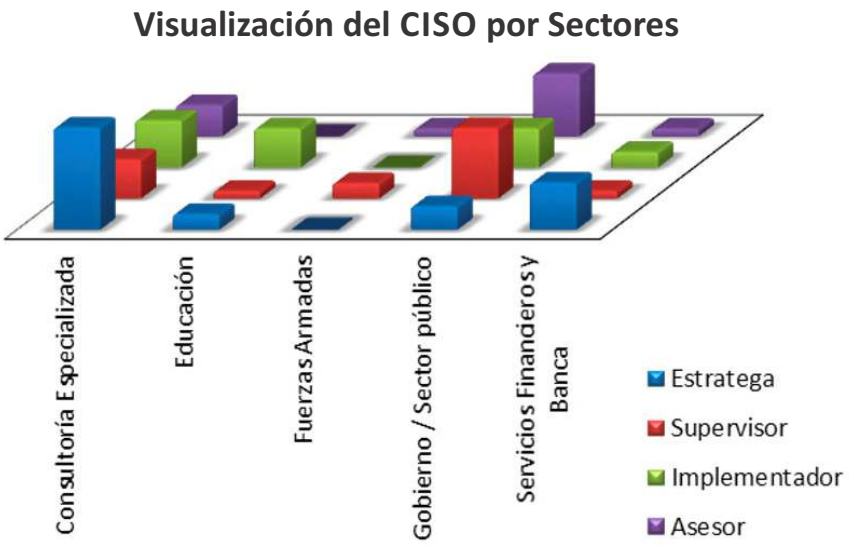
Gráfica 38: Brechas del profesional de seguridad

Gráfica 39: Tipo de CISO

dad y en dónde pueden mejorar. De acuerdo con los resultados se observa que las capacidades estratégicas son el primer lugar 47%, seguido de las capacidades intelectuales (37%), las capacidades de gestión (36%), las capacidades humanas (36%), la experiencia profesional el 25% y otras consideraciones el 1%. Comparado con el año anterior hay variaciones importantes, las capacidades intelectuales tienen un incremento del 12%, capacidades estratégicas tiene un incremento del 3%, es decir que es necesario cerrar las brechas en esos aspectos, mientras que las capacidades de gestión decrecen un 30% y la experiencia profesional decrece un 42%, lo que significa que en dichos aspectos se ha mejorado.

El CISO, es la figura más representativa como cabeza visible para guiar y orientar la ciberseguridad en las organizaciones. La Gráfica 39 muestra la forma en que las organizaciones ven o identifican el tipo de CISO que existe en ellas, el 28% ven al CISO como un supervisor, el 28% lo ven como un estratega, el 22% lo ven como un asesor, y el 22% restante como un implementador. Frente al año anterior hay un incremento significativo del 63% en el tipo estratega, 18% de incremento en la vista supervisor, mientras que decrece un 22% el implementador y un 28% como asesor.

En la Gráfica 40, se explora la forma en cómo los sectores principales de la industria ven la posición del CISO, el sector de la consulto-



Gráfica 40: Tipo de CISO x Sectores

ría especializada y los servicios financieros ven al ciso como una posición estratégica, el sector del gobierno y las fuerzas armadas ven al rol del ciso como un supervisor, mientras que el sector de la educación lo visualiza como un implementador.

La Gráfica 41, muestra el tipo de información que el CISO entrega en la organización, el 44% entrega

Gráfica 41 Tipo de información que entrega el CISO

información relacionada con la gestión para la toma de decisiones, el 40% entrega información relacionada con los riesgos en seguridad de la información, el 34% información relacionada con vulnerabilidades, el 32% entrega información relacionada con las brechas de seguridad existentes, el 17% no entrega información, y el 1% relaciona otros puntos.

En relación con el año inmediatamente anterior tenemos variaciones importantes, crece en un 24% que el CISO no está entregando información, seguido de la entrega de información con la gestión de la seguridad para la toma de decisiones 10%, mientras que todos los demás valores tienen disminuciones importantes. Decrece en primer lugar la entrega de información de las brechas de seguridad un 19%, seguido de la información técnica de vulnerabilidades 22% y 23% decrece la entrega de información relacionada con los riesgos en seguridad de la información y ciberseguridad.

Consideraciones de los datos

En Colombia se ratifica que las organizaciones piensan en tener áreas de seguridad de un tamaño pequeño, sin embargo, los fenómenos disruptivos como la pandemia, hicieron que para el año 2020 las áreas de seguridad tuvieran que incrementar su tamaño y capacidades. Esto reflejado en el incremento del 50% en tener precisamente este tipo de áreas de seguridad.

Existe una tendencia macada a hablar de una brecha de talento de ciberseguridad, todos los informes coinciden en que cada vez más es necesario tener una fuerza de trabajo en las áreas de seguridad entrenada de diferentes formas, lo que implica, una fuerza entrenada que tiene mayores posibilidades para enfrentar los desafíos actuales (ISACA, 2021).

El reporte de MarlinHawk (2020) muestra que el promedio de los profesionales estudiados del mundo de la seguridad tiene 4 años en una posición en esta área. Desde el mismo informe resalta que el 94% de los profesionales de seguridad tienen un grado obtenido en la universidad, que el 84% está relacionado con ciencias de la computación, que cerca del 44% surgen de las áreas de TI.

El estudio de ISACA (2021) muestra que los perfiles de seguridad buscados apuntan a algún grado de formación formal en ciberseguridad; sin embargo, el mismo estudio muestra que tener el grado no necesariamente significa un grado alto de preparación para enfrentar los roles en materia de seguridad.

Para (ISC2, 2021) un profesional de seguridad es una amalgama de muchas variables en cuanto a su formación, indicando que estos profesionales en su mayoría, cerca del 76%, poseen algún tipo de grado entre el pregrado y un estudio formal de postgrado.

En relación con las certificaciones, CISSP, CISM, CRISK y CEH, muestran ser las certificaciones con mayor relevancia en el mundo de los profesionales de seguridad digital, son inclusive las que más desean los profesionales, en comparación con lo que más tienen en la actualidad. Estos datos son igualmente ratificados por el informe de Kaspersky (2019), con relación a las certificaciones.

El valor de la educación en seguridad y control es muy alto, y no dista de la función que cumplen los entes de certificación, consideraciones efectuadas por el informe de ENISA (2020). Definitivamente formarse en ciberseguridad es importante, y los datos muestran que las preferencias son variadas en esta materia, todos los informes consultados muestran las fortalezas de todas las formas de educación, y relacionan que ninguna es enemiga de la otra, por el contrario, se debe trabajar por inclusive incentivar el usar marcos de trabajo generales como el modelo del NIST (INFOSEC, 2021).

Este estudio indica que todos los actores como el gobierno, la academia y la industria deben trabajar de la mano para ir cerrando las brechas estimadas de profesionales de seguridad que existen en la actualidad. De igual manera el informe indaga sobre cómo las universidades pueden trabajar y ayudar en la creación tanto de formación como de soluciones para enfrentar los desafíos en materia de ciberseguridad y concluye que el sector de la educación juega un papel fundamental en ambos sentidos.

Las nuevas capacidades son elementos esenciales en la vida de los profesionales de ciberseguridad. (ISACA, 2021; ISC2, 2021). Capacidades de liderazgo, comunicación y capacidades humanas son necesarias para desarrollar cualquier función en materia de ciberseguridad (F-Secure, 2021). Marlin Hawk (2020) resalta que una de las actividades fundamentales de los Líderes de Seguridad (25%) está asociada con el desarrollo de talentos de ciberseguridad, y por tanto de las capacidades de gestión y liderazgo que son indispensables en el desarrollo de la función de seguridad.

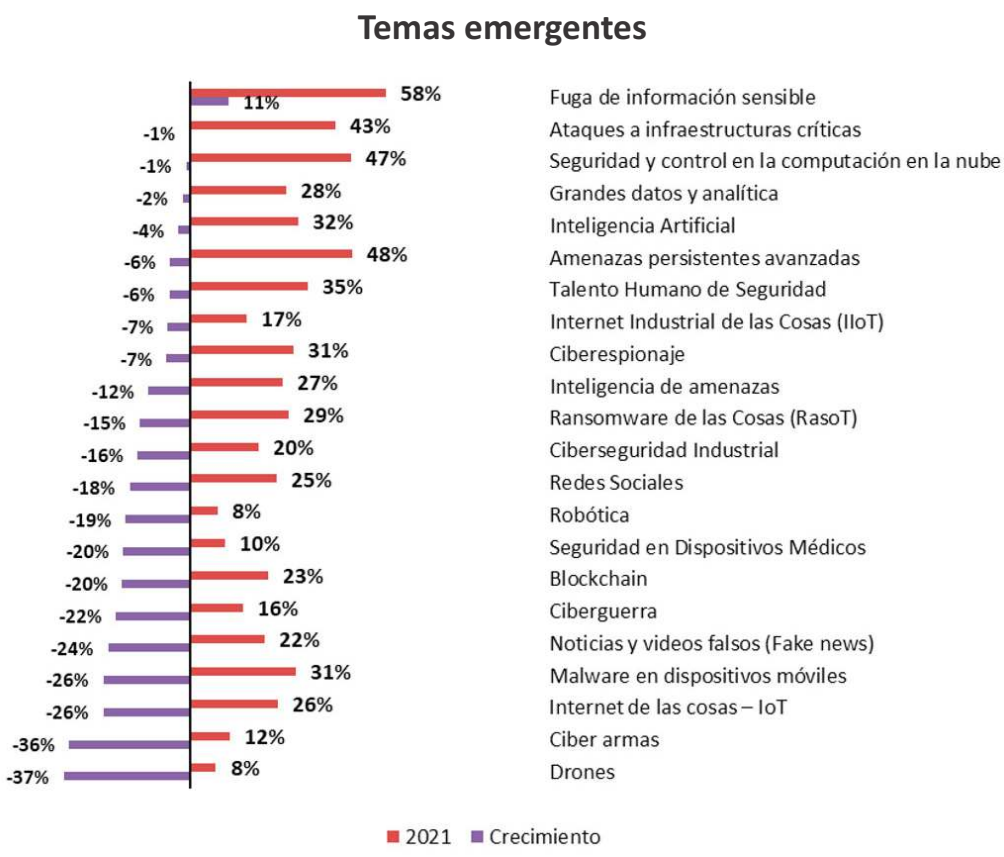
La forma en cómo puede avanzar un profesional de seguridad en otros cargos y generar mayor visibilidad, es a través del desarrollo de nuevas capacidades y habilidades: capacidades de liderazgo, capacidades para entender el negocio y de comunicación son claves para ello (ESG-ISSA, 2020).

Todos estos datos ratifican la situación de Colombia en relación con el desarrollo del profesional de seguridad, sus capacidades, competencias y habilidades que deben ser desarrolladas continuamente y más ahora que los entornos cambiantes requieren de una acelerada capacidad para ser abordados.

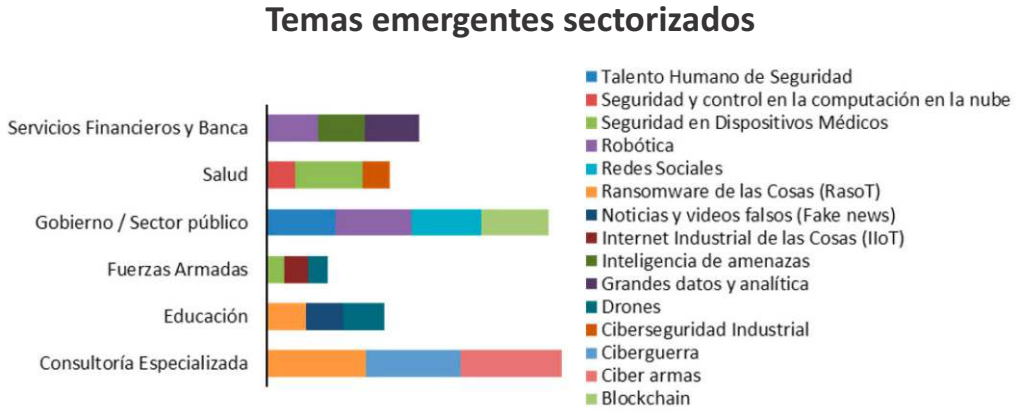
Temas emergentes

La gráfica 42 muestra los temas relevantes y emergentes que tienen en la mira los profesionales de seguridad. El más relevante, la fuga de información sensible, las amenazas persistentes avanzadas y la seguridad de la computación en la nube son los de más alto valor. Sin embargo, con relación al año anterior el único que tiene un incremento, es decir sigue siendo un tema que está en el radar y las inquietudes de los profesionales de seguridad es la fuga de información sensible que incrementa un 11%, todos los demás valores tienen una disminución en algún grado.

Al revisar directamente lo que inquieta a los sectores de la industria, se observan aspectos interesantes en la Grafica 43; primero se seleccionan los temas más importantes por sectores, encontrando que para el sector financiero los tres temas principales son grandes datos y analítica, la robótica y automatización, la inteligencia de amenazas. Para el sector de gobierno, la robótica aparece en primer lugar, seguido las redes sociales y por úl-



Gráfica 42: Temas emergentes



Gráfica 43: Temas emergentes por sectores

timo el talento de seguridad y *blockchain*. En el sector de salud, los temas son seguridad en los dispositivos médicos, la seguridad en la nube y ciberseguridad industrial. En las fuerzas armadas, el internet industrial de las cosas, los drones, y la seguridad en dispositivos médicos, así mismo el sector educativo tiene en su radar tienen los drones, el *ransomware* de las cosas y *las fake news*, por último, para la consultoría especializada están las ciberarmas, el *ransomware* de las cosas y la ciberguerra.

Consideraciones de los datos

Los profesionales de seguridad de Colombia ven el panorama de los desafíos de la ciberseguridad y sus consideraciones ponen de manifiesto la inquietud latente de lo que vendrá. Informes como el de Fireeye (2021) soportan las consideraciones locales, en el sentido de observar al *ransomware* y su evolución que se ha venido desarrollando alrededor del globo.

Booz Allen Hamilton (2020) en su informe de tendencias de la ciberseguridad, resalta que el *malware* evoluciona y en sus consideraciones ve a los drones como una fuente para que ello se desarrolle movilizando el mundo de las ciberoperaciones y las tensiones militares que esto ocasiona.

El mundo OT (Tecnología de Operación), ha tenido grandes impactos por diferentes anomalías, no por nada está en las preocupaciones de sectores como el de las fuerzas armadas, tendencia que también se puede ver advertir en el informe de IBM (2021) y que muestra que este es un escenario complejo que debe ser protegido por las implicaciones que tiene en las múltiples industrias.

Reflexiones finales

Año tras año, el estudio muestra un afianzamiento de la seguridad digital como un instrumento corporativo en las empresas colombianas.

En este contexto, cada vez más incierto, son necesarias perspectivas más incluyentes que involucren a los actores y los lleven a repensar o pensar de manera distinta la protección de la información, sin perder de vista lo ya alcanzado, y así enfrentar y superar la realidad del mundo en que se desenvuelven.

Este último período evaluado ha venido cargado de un fenómeno denominado pandemia que definitivamente ha revolucionado y cambiado la forma en cómo la seguridad se tiene que plantear en las organizaciones.

En un primer momento vimos a las empresas volcadas al contexto digital y aprendiendo de muchas maneras lo que significaba entrar por completo en una realidad virtual. Luego un período de afianzamiento en el mundo digital que ha empezado a mostrar un poco de lo que vendrá en ambiente postpandemia, donde los entornos de trabajo, las fuerzas laborales y los procesos organizacionales serán diferentes (Davis, 2021).

Cada vez más, las organizaciones se enfrentan a una realidad digitalmente modificada, en la que las nuevas tecnologías permean cada uno de los ambientes organizacionales y personales. Este contexto crea nuevos y desafiantes escenarios que se transforman en riesgos para las organizaciones, así como en una invitación para desarrollar nuevos, continuos y creativos esfuerzos en procura de proteger y crear valor como la confianza, la confiabilidad y la resiliencia en un mercado cada vez más competitivo y exigente.

Definitivamente los directivos de las organizaciones colombianas están interesados en los temas de ciberseguridad, en un informe reciente de Nominet (2020) se resalta que más del 84% de los niveles directivos y ejecutivos incluyen los temas de seguridad en sus reuniones.

Lo mismo menciona el documento de PwC (2021) donde resalta que el 47% de los CEO de su estudio global están preocupados por los temas relacionados con las ciberamenazas. Lo anterior, ratifica para Colombia que los directivos, y ejecutivos de la seguridad están interesados en estas temáticas, y esperan que los Líderes de Seguridad Digital, los orienten sobre estos riesgos.

Mejorar la resiliencia digital, pasa por gobernar y establecer cultura de ciberseguridad en las organizaciones, pasa porque toda la organización y sus miembros se adhieran a la buena práctica. Esto demanda que sus máximos líderes asuman las responsabilidades y entiendan con claridad lo que significa el ciberriesgo, de tal manera que le permita manejarlo en la realidad actualmente modificada y en los nuevos normales que se exigen (Dobrygowski & Vadala, 2020).

Por lo tanto, los ejecutivos de seguridad de esta nueva era se enfrentan de una manera más directa a otros escenarios dinámicos que demandan reacciones rápidas y prospectivas arriesgadas. Estos implican desarrollar espacios para anticiparse y observar los entornos cambiantes y superpuestos, en procura de la protección de la información y los nuevos activos digitales.

Esta nueva realidad por tanto hace que los líderes de seguridad necesiten evolucionar, no solo por desarrollar nuevas habilidades, a su vez capacidades y competencias que los posibiliten para enfrentar los desafíos actuales. Los Líderes de seguridad seguirán siendo líderes de niveles medios (Elliot, 2021), que deben poder actualizar el conjunto de herramientas como la comunicación para que puedan interactuar con más determinación con sus equipos de trabajo.

En la realidad colombiana, los datos muestran que los esfuerzos se vienen haciendo y las demandas de la realidad digitalmente modificada aceleran la transformación de la visión de la seguridad de la información. El contexto internacional confirma la misma tendencia.

En la realidad nacional se pueden concluir los siguientes aspectos:

1. En las organizaciones colombianas, las áreas de seguridad y ciberseguridad tienen dos posiciones marcadas. Algunas cuentan con una dirección propia y definida, mientras otras dependen formalmente de las áreas de tecnología. Pero eso no significa en ninguno de los dos casos que esté llegando su mensaje a los tomadores de decisiones.
2. Las compañías de gran tamaño, con más de 1000 empleados, son las que tienen mayor claridad en torno a un área independiente y a un director de seguridad. En tales empresas grandes, el área de seguridad depende de las direcciones como la de gestión de riesgos. Es interesante observar entre las organizaciones de todos los tamaños, el bajo porcentaje que no tiene un cargo o responsabilidades definidas.
3. La posición del profesional de seguridad continúa su proceso de afianzamiento dentro de las organizaciones, cada vez se ven más plazas creadas de profesionales de seguridad como CISOs y directores de seguridad en las organizaciones, estos movimientos demandan la creación de nuevas y actualizadas conjunto de competencias, capacidades y habilidades que le permitan desarrollar mejor sus nuevas funciones
4. Entre más disruptivos son los entornos de trabajo, las nuevas capacidades como las capacidades estratégicas, humanas y técnicas necesitan ser desarrolladas de manera integral para

atender la demanda de nuevas responsabilidades.

5. Los datos de Colombia muestran la importancia del profesional de seguridad, su relevancia para mantener un negocio con los niveles de confianza digital adecuados pensando en las dinámicas digitales. Así mismo, se invita al profesional a seguir expandiendo y ampliando tanto sus saberes como sus prácticas. Hay muchos desafíos y se requiere del crecimiento del profesional de una manera rápida, oportuna y con altos niveles de adaptabilidad para afrontar los desafíos actuales y futuros como Líder de Seguridad.
6. La formación del profesional de seguridad es variada y puede darse de múltiples maneras, ninguna de ellas resta a las demás, por tanto, es importante que en el radar del profesional de seguridad existan todas las opciones que le permitan desarrollar su plan de crecimiento y carrera profesional.
7. La experiencia, los conocimientos y sus adicionales (como las certificaciones) en la vida del profesional de seguridad en la realidad de Colombia son importantes, se complementan y no se oponen, por el contrario, alimentan el camino para tener un mayor potencial en el mercado laboral colombiano.
8. La realidad digital hace que todos los sectores e industrias lleven su mirada al tema de ciberseguridad. A los sectores como el financiero, la consultoría especializada y el gobierno les interesa participar y conocer la realidad de la seguridad, tendencia observada en diferentes informes publicados sobre seguridad y ciberseguridad.
9. Los riesgos es el lenguaje común de los negocios y a su vez es un instrumento catalizador de un programa de seguridad. Los Líderes de seguridad digital están considerando este instrumento como una valiosa oportunidad para elevar su interlocución con los niveles directivos y ejecutivos, para poder tomar caminos acordes a la realidad digital de la empresa.
10. La confianza digital y la ciberresiliencia se convierten en un generador de nuevos negocios; tendencias internacionales también sostienen que dicha confianza es una fuente que motiva a cultivar las relaciones entre consumidores y quienes ofrecen los servicios, para configurar un activo valioso a la hora de manejar y maniobrar en los ecosistemas digitales actuales.
11. A nivel nacional, se mantiene la sólida tendencia de usar mecanismos tecnológicos como las principales herramientas de protección. Si bien las tendencias internacionales dan esto por sentado, se debe hacer un llamado tanto a los responsables de seguridad como a las organizaciones para que vean a la seguridad como un tema inherente a la dinámica empresarial. Las

tendencias internacionales ratifican que es necesario extender la visión de la seguridad como una fuente generación de valor para la organización y los objetivos de su negocio.

12. El poder de las anomalías digitales, de los adversarios y de la realidad digital se entiende cada vez más en el marco de las organizaciones colombianas. Más allá de lo técnico, se registran los errores humanos y, en tal sentido, es necesario pasar de procesos de sensibilización al cambio de comportamientos, liderado por los responsables de la seguridad, con el ánimo de crear una nueva cultura alrededor de entornos digitalmente modificados. Así mismo, es necesario gestionar un programa de seguridad que permee todos los niveles organizacionales basados en prácticas dirigidas a los diferentes grupos de interés, y orientadas a construir posturas de seguridad diferenciadas y articuladas desde los desafíos que debe asumir el talento humano.
13. Las nuevas tecnologías como Cloud, IoT, IA, *machine learning* Zero Trust y otras, están cambiando la concepción del mundo, la forma de interactuar y los retos a los que se enfrentan las organizaciones a nivel nacional e internacional. De ahí que los profesionales de seguridad deban tener claridad para profundizar en estas nuevas tendencias y su uso.
14. Los resultados de la encuesta reflejan que, a la hora de implementar modelos de seguridad, las organizaciones usan algún estándar, hecho motivado más por las regulaciones que por una intención de proteger, lo que genera el debate nacional e internacional alrededor de tales asuntos. La meta de la protección organizacional no debe estar sujeta al cumplimiento.
15. Es claro que el cisne negro (o ¿sorpresa predecible?) denominado Covid-19, ha cambiado por completo no solo la forma de ver la vida, sino ha resaltado la importancia de la ciberseguridad y la gestión de las tecnologías de la información. Hoy más que nunca se observa a la ciberseguridad como una capacidad empresarial, que ofrece y aporta en el desarrollo de negocios digitales, y que se enfrenta y enfrentará las tensiones geopolíticas y de cumplimiento con mucha más profundidad. Esta capacidad deberá apalancar la confianza digital necesaria para ofrecer servicios y desarrollar modelos de negocio en el ecosistema digital de hoy como fundamento del nuevo normal que empezamos a construir.

En resumen, el panorama general de la seguridad en Colombia muestra cambios importantes, grandes movimientos y desafíos emergentes. La realidad llamada Covid-19 ha creado una ventana de oportu-

nidad para que la ciberseguridad se afiance como herramienta indispensable para apalancar los negocios.

El año 2021 está marcado por el desarrollo del "nuevo normal", que, si bien no hay consensos a la fecha, sí ha empezado a dar lineamientos de posibles futuros, en los que no existe una sola opción, sino múltiples escenarios que permitan diseñar posibles alternativas, cosas que se han venido aprendiendo sobre la marcha, donde la ciberseguridad no es la excepción.

En este ejercicio, es necesario repensar lo ya conocido y concebido como verdades definidas para reescribir nuevas prácticas tendientes a apoyar a las empresas para que caminen por la constante de la incertidumbre, que no es otra cosa que entender la dinámica de los ecosistemas digital en los cuales las organizaciones se mueven hoy.

Referencias

Booz Allen Hamilton (2020). 2020 CYBERSECURITY THREAT TRENDS OUTLOOK. https://content.fireeye.com/m-trends/rpt-m-trends-2020

Cano, J. & Almanza, A. (2020) Estudio de la evolución de la Seguridad de la Información en Colombia: 2000 - 2018. *Revista Iberoamericana de Sistemas y Tecnologías de Información*. E27. Marzo. 470-483. https://www.researchgate.net/publication/339629757_Estudio_de_la_evolucion_de_la_Seguridad_de_la_Informacion_en_Colombia_2000_-_2018

CISCO (2020). Securing What's Now and What's Next. Recuperado de: https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-ciso-benchmark-cybersecurity-series-feb-2020.pdf

CISOS.CLUB (2021). Modelos Post Pandemia de Entornos de Trabajo (Infografía). https://www.linkedin.com/feed/update/urn:li:activity:6809142558334214145/

CyberEdge Group (2021). Cyberthreat Defense Report. https://www.herjavecgroup.com/wp-content/uploads/2021/04/CyberEdge-2021-CDR-Report-v1.1.pdf

David. D. (2021). 5 Models for the Post-Pandemic Workplace. HBR. https://hbr.org/2021/06/5-models-for-the-post-pandemic-workplace

Deloitte (2019). The Future of Cyber Sphere 2019. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-sphere.pdf

Deloitte (2021). Building The Resilient Organization. https://www2.deloitte.com/content/dam/insights/articles/US114083_Global-resilience-and-disruption/2021-Resilience-Report.pdf

Dobrygowski, D. & Vadala, D. (2021). Does Your Board Really Understand Your Cyber Risks?. HBR. https://hbr.org/2020/09/ does-your-

board-really-understand-your-cyber-risks

Eliot, B. (2021). It's Time to Free the Middle Manager. HBR. https://hbr.org/2021/05/its-time-to-free-the-middle-manager

ENISA (2020). Cybersecurity skills development in the eu. https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union/at_download/fullReport

ESG-ISSA (2020). The Life and Times of Cybersecurity Professionals 2020. https://www.esg-global.com/esg-issa-research-report-2020

EY (2020). How does security evolve from bolted on to built-in? https://www.ey.com/Publication/vwLUAssets/2020_GISS_pdf/$FILE/ey-global-information-security-survey-2020-report.pdf

EY & IIA. (2021). The risky six. https://global.theiia.org/knowledge/Public%20Documents/EY-The-Risky-Six-Board-Disconnections.pdf

FBI. (2021). Internet Crime Report 2020. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

F-Secure (2021). The CISOs' New Dawn. https://www.f-secure.com/content/dam/f-secure/en/business/cisos-new-dawn/collaterals/mdr-the-cisos-new-dawn.pdf

Fireeye (2021). M-Trends 2021. https://www.fireeye.com/content/dam/collateral/en/rpt-mtrends-2021.pdf

IBM (2021). X-Force Threat Intelligence Index 2021. https://www.ibm.com/downloads/cas/M1X3B7QG

IDG (2021). Cybersecurity at a Crossroads. https://www.insightcdct.com/getattachment/40ff5ebd-03f2-4d4d-8f4e-b7871c00fd5f/Complete-2021-IDG-survey-results.aspx

INFOSEC (2021). 2021 Cybersecurity Role & Career Path Clarity Study. https://www.infosecinstitute.com/form/2021-role-clarity-study/

ISACA (2021). State of Cybersecurity 2021, Part 1: Global Update on Workforce Efforts, Resources and Budgets. https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpsc211

$(ISC)^2$. (2021). Cybersecurity Professionals Stand Up to a Pandemic. https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

Ivanti (2021). How the Pandemic Has Shifted CISO Priorities. https://www.ivanti.com/resources/v/doc/pr-survey-report/ivi-2459-emea-ciso-survey-en

Kaspersky (2019). What It Takes to Be a CISO: Success and Leadership in Corporate IT Security. https://kas.pr/4sw6

Marlin Hawk (2020). Global Snapshot: The CISO in 2020. Recuperado de: https://www.marlinhawk.com/docs/Marlin-Hawk-Global-CISO-Research-Report.pdf

Nominet (2020). THE CISO STRESS REPORT. Recuperado de: https://media.nominetcyber.com/wpcontent/uploads/2020/02/Nominet_The-CISO-Stress-Report_2020_V10.pdf

Ponemon-IBM (2020). The Cyber Resilient Organization. https://www.ibm.com/downloads/cas/VR9E8AKM

Ponemon-LogRhytmn (2021). Security and the C-Suite: Making Security Priorities Business Priorities. https://gallery.logrhythm.com/analyst-reviews-and-reports/na-report-ponemon-security-and-csuite.pdf

PwC (2021). 24nd Annual Global CEO Survey. A leadership agenda to take on tomorrow. https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2021/report.html

Sophos. (2021). The State of Ransomware 2021. https://news.sophos.com/en-us/2021/04/27/the-state-of-ransomware-2021/

Tessore, C. (2020). Vuca y tuna abordaje conceptual cambios de paradigma en contextos vuca y tuna. Changes of paradigm in vuca and tuna a conceptual approach. https://www.academia.edu/41717050/VUCA_Y_TUNA_ABORDAJE_CONCEPTUAL_CAMBIOS_DE_PARADIGMA_EN_CONTEXTOS_VUCA_Y_TUNA

Verizon (2021). Data Breach Investigation Report. https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

WEF - World Economic Forum (2021) The Global Risk Report 2020. Recuperado de: https://www.weforum.org/reports/the-global-risks-report-2021

World Government – EY. (2020) Cyber Resilience in the Digital Age. https://www.worldgovernmentsummit.org/api/publications/document?id=24717dc4-e97c-6578-b2f8-ff0000a7ddb6

***Andres R. Almanza J., Ms.C, CISM**. Chief Growth Officer en CISOS.CLUB, Investigador en Ciberseguridad SegInfo y Liderazgo. | Executive Certificate in Cybersecurity Leadership & Strategy by FIU University | Certificado como ISO 27001 Lead Implementer and 27005 Lead Manager from PECB | CISM, ITILv3, LPI| Certificado como Coach Profesional Internacional, Master in Leadership and Organizational Development with Coaching, Executive Master's in Leadership Skills Developed in Harvard, & Coach Profesional avalado por International Coach Federation| Profesional en Ingeniería de Sistemas | especialista en seguridad en redes y máster en seguridad de la información. Docente del programa de maestría de la Universidad Externado de Colombia y de la Universidad de las Américas en Ecuador. Creador de la Comunnidad CISOS.CLUB, CISOS-COL y CISOS-LATAM (Linkedin) y Miembro del comité editorial de la revista sistemas de ACIS.*

¡ESCRÍBANOS!

REVISTA SISTEMAS

Asociación Colombiana de Ingenieros de Sistemas (ACIS)

Diríjase a la editora de la revista:

Sara Gallardo M.

saragallardo@acis.org.co

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

Calle 93 No. 13-32 Of. 102
Bogotá, D.C.
www.acis.org.co

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.

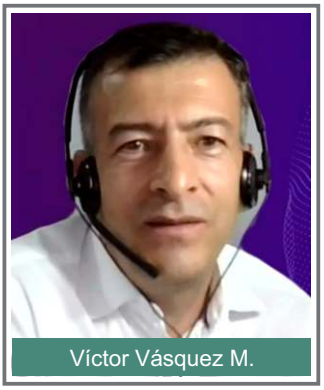
Razones para que el tema del foro en esta edición sea la resiliencia digital o la capacidad de las compañías para aceptar, sobreponerse, recuperarse y superarse. Y, en tal sentido, rediseñar los procesos comerciales y sistemas de TI, en aras de proteger su información más vulnerable y de poner en marcha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

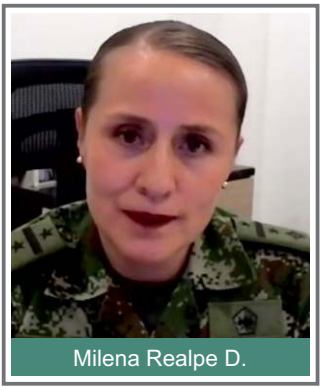
Para analizar algunos aspectos sobre esta realidad fueron invitados Armando Carvajal R., gerente arquitecto de soluciones en Globaltek; Víctor Vásquez Mejía, director de IT Advisory en KPMG; Teniente Coronel Milena Realpe Díaz, *jefe de la Maestría de Ciberseguridad y Ciberdefensa*, *Escuela Superior 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.

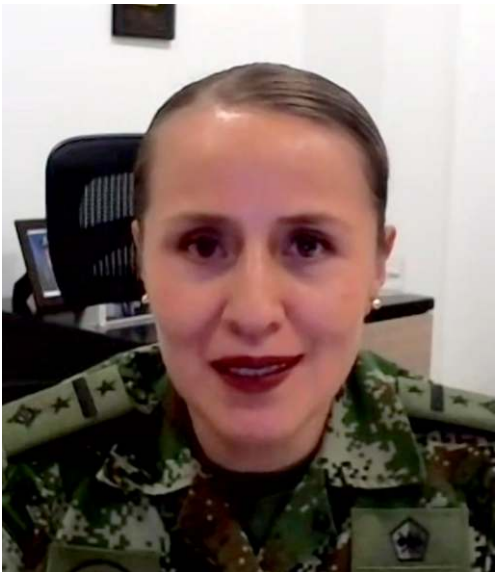
Jeimy J. Cano M.
¿Cuáles son los elementos claves que una organización debe tener en cuenta para desarrollar resiliencia digital? ¿Depende de su apetito de riesgo?

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,

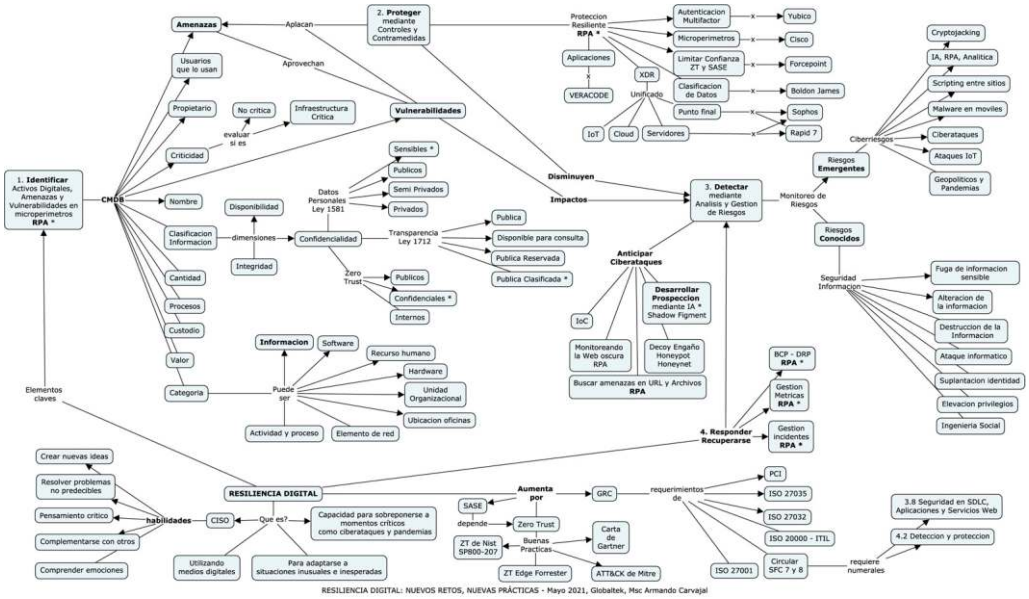


Figura 1. Mapa conceptual sobre resiliencia digital (Con autorización de uso por parte de Armando Carvajal Rodríguez)

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.*

La “falsa sensación de seguridad”

DOI: 10.29236/sistemas.n159a6

El reto de incomodar las certezas de los estándares y tratar de “domesticar” los inciertos.

Resumen
Las prácticas actuales de seguridad/ciberseguridad de las organizaciones modernas han estado fundadas en la aplicación de estándares y buenas prácticas que les han permitido alcanzar importantes niveles de aseguramiento y control en sus procesos e iniciativas de negocio. Sin perjuicio de lo anterior, con un entorno de cambio permanente, de inestabilidades e inciertos políticos, económicos, sociales, tecnológicos y legales que alteran la dinámica de los mercados y las tendencias internacionales, es necesario actualizarlas para habilitar a la empresa para navegar en escenarios de volatilidad e incertidumbre y mantenerla fuera de la zona cómoda y engañosa de la “falsa sensación de seguridad”. En este sentido, este artículo propone algunas estrategias y alternativas para retar las prácticas actuales y habilitar espacios de reflexión desde la resiliencia y la antifragilidad como fundamentos claves para la función de seguridad/ciberseguridad en las organizaciones del siglo XXI.

Palabras clave
Ciberseguridad, estándares, resiliencia, antifragilidad, inseguridad de la información

Introducción

Con el avance acelerado de la puesta en operación de tecnologías emergentes y disruptivas las organizaciones crean escenarios de nuevas experiencias para sus clientes, y al mismo tiempo motivan nuevas zonas grises de seguridad y control que pueden terminar aprovechadas por vulnerabilidades conocidas modificadas y otras emergentes, fruto de la convergencia tecnológica vigente. Esta realidad de conectividad exponencial, revela con mayor claridad el acoplamiento y la interacción que se tienen entre los objetos físicos y las implementaciones lógicas, temáticas que terminan definiendo la dinámica de operación y su confiabilidad (Perrow, 1999).

En este escenario las organizaciones deben comprender que la inevitabilidad de la falla se convierte en el nuevo normal que deben atender y enfrentar comoquiera que una mayor conexión entre los objetos físicos y las implementaciones lógicas, tendrá necesariamente puntos opacos de control, los cuales podrán ser capitalizados por los adversarios ahora o en el futuro. Así las cosas, la mecánica actual de seguridad y control que se funda en riesgos conocidos y métricas específicas, deberán actualizarse para dar cuenta con esta nueva realidad aumentada de "cosas" digitalmente conectadas (Cano, 2021).

Movilizar los esfuerzos corporativos en esta vía descubre algunas tensiones que generan diferencias y lecturas distintas entre los cuerpos de gobierno, los ejecutivos de riesgos y los directivos de seguridad/ciberseguridad, que van desde posturas que acentúan la necesidad de certezas y la productividad de la empresa, hasta las implicaciones claves de eventos adversos y sus impactos para el negocio y sus grupos de interés. En consecuencia, se advierten desencuentros entre la cultura de la productividad y la cultura del aprendizaje, así como asimetrías en la confianza entre las herramientas y las prácticas de seguridad y control.

Lo anterior crea una zona de inestabilidad estratégica que tiene el riesgo inherente de crear en una "falsa sensación de seguridad", la cual termina privilegiando la necesidad de certezas y productividad, para lo cual las inversiones en herramientas tecnológicas terminan siendo la respuesta a los retos de la inevitabilidad de la falla. Por tanto, cuando esto ocurre, la organización se debilita en su postura resiliente frente a los eventos inesperados, reaccionando a estas situaciones de formas no coordinadas, lo que no permite un mayor margen de maniobra por parte de los atacantes que buscan desestabilizar la empresa y sus negocios (Mckinsey-IIF, 2020).

En este sentido, este artículo busca explorar algunos elementos claves de la "falsa sensación de seguridad" con el fin de establecer puntos relevantes que muestren su manifestación e impactos, así como plantear un marco general de apoyo para movilizar a las organizaciones fuera de esa zona "cómoda y engañosa" donde muchas de ellas pueden estar sin percatarse de ello y así, plantear estrategias de resiliencia y antifragilidad que aumenten la capacidad de respuesta y anticipación de las empresas frente a la inevitabilidad de la falla y los adversarios digitales emergentes.

Cultura de productividad y cultura de aprendizaje. Dos mundos convergentes

En el mundo empresarial la necesidad de producir resultados es la norma base para desarrollar cualquier actividad de negocios. En la medida que se puedan superar con celeridad y confianza los retos que la organización requiere para alcanzar sus objetivos estratégicos, podrá avanzar explorando nuevas formas y estrategias que la habiliten para consolidar su posición estratégica en un segmento de mercado.

En esta línea, los ejecutivos de las empresas privilegiarán toda actividad que produzca resultados de forma eficiente y efectiva, manteniendo a la corporación en cumplimiento de las exigencias regulatorias, las indicaciones propias de la auditoría y los mandatos éticos y legales con los que cuente ella cuente. De esta forma, los planes de desarrollo de la organización tomarán forma desde la estructura general del modelo de negocio y las expectativas de los clientes.

Esta forma de operar responde por lo general al modelo de Planear, Hacer, Verificar y Actuar (PHVA) (Ver figura 1), el cual permite asegurar un resultado de forma repetible todo el tiempo. Cuando en la ejecución alguna situación no sale como estaba previsto, se activa el procedimiento de análisis causa-raíz, con el fin de entender, evaluar y cerrar aquello que no corresponde a lo esperado.

Este modelo permite automatizar la producción de los bienes y servicios con la calidad esperada y respondiendo a los estándares de operación que la empresa tiene.

Sin perjuicio de lo anterior, en un escenario cada vez más volátil e incierto, las condiciones cambian y se hace necesario analizar y explorar nuevas oportunidades que se presentan para concretar opciones antes inexistentes. En consecuencia, el modelo PHVA diseñado para entornos ciertos, comienza a ceder terreno para darle paso a una postura renovada que busca conectar los momentos inciertos con ventanas de aprendizaje que habiliten a la organización para repensar sus propios procesos y formas de hacer las cosas (Denyer, 2017).

Figura 1. Ciclo PHVA (Elaboración propia con ideas de Denyer, 2017)

Considerando lo anterior se introduce el modelo A2RM (ver figura 2), que se traduce en Arriesgar, Anticipar, Responder y Monitorizar, en el cual se pasa de un PHVA que busca "hacer mejor lo que sabemos hacer", al reto de "hacer mejores cosas". Esta nueva apuesta conceptual busca motivar a la organización a navegar en el incierto, no de cualquier manera, sino declarando su apetito al riesgo (tomar riesgos para crear disrupciones y oportunidades), proponiendo futuros alternos (para anticipar escenarios), interpretando y analizando las tendencias actuales (para responder de forma ágil al presente), y finalmente monitorizando los cambios del entorno (para aprender y ajustarse rápidamente a ellos).

Cuando una empresa adopta el A2RM, se embarca en el reto de construir una cultura de aprendizaje, donde la norma es que se sabe que no se sabe, se duda de las prácticas existentes y se mantiene una curiosidad permanente acerca de nuevas rutinas y propuestas que se pueden intentar. En este contexto, se busca crear una zona psicológicamente segura, donde la idea no es relajar los estándares vigentes, o mantener a las personas en una zona cómoda, o acceder a todas las solicitudes y ser complacientes, sino más bien establecer

Figura 2. Ciclo A2RM (Elaboración propia con ideas de Denyer, 2017)

un clima de respeto, confianza y apertura donde se pueden poner sobre la mesa las preocupaciones, sugerencias y propuestas sin temor a represalias o juzgamientos (Edmondson, 2018).

Cuando se acentúa la cultura de la productividad o rendimiento, esto es, el énfasis en los resultados medibles, el entorno psicológicamente seguro se deteriora, dado que se advierte la cultura del castigo del "error", lo que necesariamente hace retroceder a las personas para no exponer sus propias capacidades y proteger sus carreras. En la cultura de la productividad se motiva el surgimiento de los expertos los cuales por lo general tienen todas las respuestas, particularmente en aquellas áreas donde no se tiene la competencia particular (Grant, 2021).

Cuando se privilegia una cultura de aprendizaje, los errores se convierten en oportunidades para ver puntos ciegos, comprender el entorno donde ocurren y cómo ocurren, tomando distancia del hecho en sí mismo (De la Torre, 2004). En este entorno de confianza, las personas tienden a revelar aquello que los llevó a esa situación y ubican nuevos puntos del contexto donde es posible ver otros elementos para entender la situación inesperada que se ha verificado. Por tanto, cuando es posible crear equipos

que se enfrentan al reto de “no saber” y tienen dispuesto un escenario psicológicamente seguro para abordarlo, no hay otro resultado de oportunidades para encontrar “feed-forward”, es decir, acciones proactivas, propositivas y centrada en las fortalezas y así, entender que es aquello que se debe dejar de hacer, que es eso que distingue al equipo y qué cosas no se han hecho antes y que es clave desarrollar ahora.

Ciberseguridad: Prácticas y herramientas ¿Cuánto creemos en unas y otras?

Cuando se encuentran las dos culturas la de productividad y la de aprendizaje, es posible encontrar una zona de movimiento que habilite la puesta en marcha de propuestas que terminen aumentando la capacidad de anticipación de la organización. En este sentido, la ciberseguridad debe ubicar esos espacios creados por estas dos culturas con el fin de fundar su nicho de negocio concreto, que permita capitalizar sus iniciativas en favor de la empresa, sus iniciativas innovadoras y sus grupos de interés.

No obstante lo anterior, mantiene un desafío permanente para establecer su marco de referencia y revisión en el contexto ejecutivo de la empresa, toda vez que muchas veces queda atrapada entre las dos culturas, lo que le impide desarrollar prácticas o apuestas resilientes de forma adecuada, dada las exigencias permanentes de resultados concretos, sobremanera por el nivel de inversión que la organización ha hecho particularmente en herramientas tecnológicas.

Así las cosas, el ejecutivo de seguridad/ciberseguridad se encuentra en la encrucijada de saber cuánto confiar en las herramientas tecnológicas que tiene desplegadas y en las prácticas y estándares actualmente utilizados en el desarrollo de la gestión y el gobierno de la seguridad/ciberseguridad. Este sentimiento mantiene en una tensión permanente a este directivo, comoquiera que sabe que en cualquier momento una brecha de seguridad puede ocurrir y traer como consecuencia una inestabilidad para la organización, lo que necesariamente significa que todos los ojos serán puestos en él.

Encontrar el lugar común que permita un postura resiliente para la organización frente a evento inesperados o adversarios emergentes, implica reconocer cuánto se cree en las herramientas (sabiendo que todas tienen vulnerabilidades conocidas y ocultas) y cuánto en las prácticas y estándares vigentes (sabiendo que todas ellas tienen limitaciones) (Abraham, Sims & Gregorio, 2020). Para lograrlo, es necesario que el director de seguridad/ciberseguridad habilite una cultura de aprendizaje fundada en el defender y anticipar, mientras mantiene y valida los riesgos conocidos a través del proteger y asegurar.

Defender y anticipar implica reconocer que siempre el atacante en algún momento tendrá éxito y por lo tanto la organización debe estar preparada, para "ver" cuando esa situación se esté manifestando, para tratar de demorar al adversario y tomar tiempo para la respuesta que se requiere en ese instante (Pillay, 2019).

Esto es, crear una confianza imperfecta que permite una zona de simulaciones y aprendizajes, que rápidamente se incorporan a las prácticas vigentes, y permiten actualizar las amenazas latentes y emergentes de la organización.

Lo anterior exige una postura vigilante que se traduce en algunas preguntas que el equipo de seguridad/ciberseguridad debe hacerse de manera permanente: (Day & Schoemaker, 2019)

Al interior:

- ¿Cómo podemos **mejorar** y **aumentar** la identificación de nuevos patrones de amenazas?
- ¿Qué **más podemos hacer** con nuestras capacidades actuales?
- ¿En **qué somos buenos** actualmente?
- ¿Qué **nuevas capacidades** necesitamos?

Al exterior:

- ¿Cómo han venido **evolucionando** las técnicas y tácticas de los adversarios?
- ¿Qué **adversarios** están anticipando y usando estás nuevas técnicas y tácticas?
- ¿Qué **nuevos ataques** pueden afectar a la organización?
- ¿Cómo nos podemos **anticipar y defender** de los nuevos ataques?

Cuando el equipo de ciberseguridad/seguridad se mantiene en este nivel de reflexión permanente, es capaz de superar la "falsa sensación de seguridad". Esto es, confiar en la capacidad para crear y alcanzar un entorno de operación confiable en el futuro y, al mismo tiempo, enfrentar el reto de la inevitabilidad de la falla y mantener la humildad para cuestionar si se tienen las herramientas y prácticas adecuadas en el presente. Esta duda razonable es lo que habilita una comprensión de las vulnerabilidades, no por su aprovechamiento, sino por la lectura y comprensión de su contexto.

Resiliencia y antifragilidad. Dos conceptos para superar la "falsa sensación de seguridad"

Cuando en el ejercicio de comprensión de una falla de control se concentra la atención en el hecho como tal, olvidando el contexto donde ocurrió, lo más fácil es buscar un culpable, una persona que termina siendo la responsable de un evento (Reason, 2000). Lo que en la lectura tradicional de la seguridad se denomina el eslabón más débil de la cadena, la acción "errada" de un humano al enfrentarse a

una situación conocida o desconocida.

Si en lugar de fijar la mirada en el evento y sus impactos, se toma distancia y se visualiza el contexto en el cual ocurrieron los eventos, las situaciones circundantes, las relaciones visibles e invisibles que se manifestaron, es posible comprender mejor por qué el evento sucedió, y cómo podemos hacer más resistente el sistema en una siguiente ocasión. Esto implica desarrollar umbrales de operación, tolerancia y capacidad de riesgo que buscan aumentar la resiliencia del sistema que se modela o analiza (Woods, Dekker, Cook, Johannesen & Sarter, 2010).

De acuerdo con documentos recientes del NIST existen algunas definiciones de resiliencia que se mencionan a continuación:

- D1 - La capacidad de un sistema de información para continuar: (i) operando en condiciones adversas o de estrés, incluso si se encuentra en un estado degradado o debilitado, manteniendo las capacidades operativas esenciales; y (ii) recuperarse a una postura operativa efectiva en un marco de tiempo consistente con las necesidades de la misión (NIST SP 800-39).
- D2 - La capacidad de un sistema de información para continuar operando mientras es atacado, incluso si se encuentra en un estado degradado o debilitado, y recuperar rápidamente sus capacidades operativas para las funciones esenciales después de un ataque exitoso (NIST SP 800-30 Rev. 1).
- D3 - La capacidad de adaptarse y recuperarse rápidamente de cualquier cambio conocido o desconocido en el entorno a través de la aplicación holística de la gestión de riesgos, la contingencia y la planificación de la continuidad (NIST SP 800-34 Rev. 1).

Estas tres definiciones hablan de palabras claves que se deben tener en cuenta al hablar de atender eventos adversos, ataques o cambios conocidos o desconocidos: (Clédel, Cuppens, Cuppens & Dagnas, 2020)

- *Capacidad* – Desarrollo de patrones de aprendizaje frente a eventos inciertos.
- *Adaptación* – Ajuste de prácticas y actualización de saberes previos frente a eventos inesperados.
- *Recuperación* – Volver a poner al servicio un sistema o proceso luego de haberse materializado una situación o condición no prevista.

Son estas tres palabras las que se requieren comprender en profundidad para mantener una postura atenta, vigilante y de aprendizaje permanente con el fin de preparar a la organización para atender situaciones de tensión que pueda sugerir cualquier agente externo o interno. En la medida que se cuente con

una postura de falla segura, que es aquella que se dispara cuando los umbrales previstos de operación se superan, los sistemas de información, podrán mantener niveles funcionamiento que les permita aumentar su capacidad para atender condiciones no estándar, adaptarse rápidamente mientras se opera con los mínimos y sobretodo, aprender lo ocurrido para recuperarse de forma eficiente y en condiciones mejoradas (Australian Government, 2011).

Lo que inicialmente se conocía de la realidad de los riesgos empresariales, se desdibuja rápidamente hoy, dejando de lado las certezas, para darle paso a la incertidumbre, como el nuevo insumo de las estrategias corporativas, donde se introduce la "idea peligrosa" de la "antifragilidad" (Taleb, 2013) como ese proceso de entender y alimentarse de la aleatoriedad, el azar, los errores y las fallas como forma de fortalecer una posición en el entorno de negocios y sobrevivir aún las amenazas se materialicen en el ejercicio y aplicación de su modelo de generación de valor.

La antifragilidad consiste entonces en navegar en los eventos inesperados, con el fin de "domesticar" la incertidumbre, lo que se traduce en: "reducir los riesgos perjudiciales y mantener el beneficio de las posibles ganancias" (Idem, pág. 214), un ejercicio retador de aprendizaje permanente, que invita a las organizaciones y los responsables de seguridad/ciberseguridad a elaborar un modelo de seguridad y control, basado en el reconocimiento del incierto como base, esto es en el azar, los errores, la imprevisibilidad, los comportamientos no lineales y manejar los impactos de la combinación de éstos, para alimentar la curiosidad, la capacidad de aprendizaje y resistencia del modelo, que claramente será contrario a lo que espera un ejecutivo de alto nivel de una empresa.

En este sentido la condición antifrágil que debe asumir la función de seguridad/ciberseguridad en las organizaciones modernas, es aquella que incorpora la inevitabilidad de la falla como parte natural de las prácticas de defensa y anticipación, que promueve la generación de escenarios de riesgo como parte se preparación y gestión, y que se prepara para superar las situaciones críticas e inesperadas incorporando la resiliencia como parte fundamental de su acción y operación (Weick & Sutcliffe, 2007).

Cuando convergen la postura antifrágil y las capacidades resilientes, el ejecutivo de seguridad/ciberseguridad no tendrá que decidir en qué confiar (prácticas o herramientas), sino que mantiene una dinámica de reto permanente sobre ambas cosas, que le permite desarrollar una competencia que lo mantiene fuera de la zona cómoda, sin experimentar superávit de futuro ni déficit de presente, sino navegando en medio de aguas profundas ab-

sorbiendo nuevas ideas, actualizando las vigentes y sobremanera experimentando para sorprender al adversario en su mismo terreno (Bodeau, Graubart, Heinbockel & Laderman, 2015).

Marco general para superar la "falsa sensación de seguridad". Algunas reflexiones

Con el fin de mantener a las organizaciones fuera de la zona cómoda de la "falsa sensación de seguridad", es necesario actualizar la mentalidad vigente de los estándares y las certezas, que es propia de la cultura de la productividad, por una que se sienta cómoda con la vulnerabilidad, con la ambigüedad y aceptar que "no sabe", y lo más importante abierta a los errores, que es propia de la cultura de aprendizaje.

Para ello, es necesario introducir el modelo A2RM: Arriesgar, Anticipar, Responder y Monitorizar, como base del nuevo modelo de gestión y desarrollo de la organización, y particularmente del área de seguridad/ciberseguridad. Lo anterior implica desarrollar una mentalidad de aprendizaje ágil que busca aumentar la colaboración, mejorar y habilitar ciclos de aprendizaje, focalizarse en la entrega de valor y la habilidad para adaptarse al cambio.

Esta mentalidad tiene como base cuatro elementos claves: (McGowan & Shipley, 2020)

- *Agencia* – Capacidad de actuar de forma independiente y hacer elecciones por sí mismo. Donde el aprendizaje es una responsabilidad propia de cada individuo.
- *Agilidad* – Es la habilidad para aprender y desaprender. Es el ejercicio de tomar nueva información, crear nuevo conocimiento y lanzarse a cambiar aquello que requiere actualizarse.
- *Adaptabilidad* – Capacidad para navegar en situaciones ambiguas y asumir los retos aun cuando no toda la información es clara o conocida. Esto es, desaprender lo conocido, diseñar una nueva propuesta, conectar los nuevos puntos y cambiar la lectura actual.
- *Atención* – Entender las acciones conscientes que cada persona hace, que definen su identidad para darle sentido a sus aportes en un contexto individual y empresarial.

En segundo lugar, comprender que la viabilidad de la práctica de seguridad/ciberseguridad "no es solamente mitigar los riesgos, ni evitarlos (si eso es viable), sino avanzar en la comprensión del entorno, profundizar en la construcción de confianza, concretar la identificación de las incertidumbres claves que afecten el negocio y desarrollar la capacidad de respuesta frente a un incidente" (Cano, 2020). En este sentido, se hace necesario conectar tres ciclos de operación que vinculan tanto la cultura de productividad como la de aprendizaje: el ciclo de regulación (productividad y aseguramiento de lo conocido), el ciclo

de adaptación (prospectiva y tendencias identificadas) y el ciclo de memoria y aprendizaje (sinergia que se genera al interior de la dinámica empresarial que habilita un aprendizaje colaborativo, para construir y conectar puntos aparentemente sueltos en el engranaje empresarial) (Cano, 2020).

En tercer lugar, entender que la ciberseguridad/seguridad es un "deporte colectivo" y de "contacto", por lo tanto se hace necesario mantener una cultura de aprendizaje que todo el tiempo rete y confronte las buenas prácticas, configure un entorno psicológicamente seguro para preguntar, tensionar y desafiar el statu quo de la dinámica de la ciberseguridad/seguridad, y defina zonas y lugares para desarrollar experimentos inteligentes, que permitan concretar cada vez más errores brillantes, que son aquellos que en los que se invierte poco y se obtiene mucho beneficio (Hepfer & Powell, 2020).

Estas tres condiciones básicas a nivel de gestión, a nivel individual y a nivel funcional, se convierten en la base para movilizar los esfuerzos del área de seguridad/ciberseguridad fuera de la zona cómoda de la "falsa sensación de seguridad", lo que implica una transformación de la dinámica de un concepto inicialmente estático y conocido, por uno que evoluciona, que es cambiante y se reinventa conforme los retos del entorno le plantean nuevas propuestas.

Reflexiones finales

Estudios recientes indican que mientras la tecnología crece exponencialmente la productividad de los negocios lo hace de forma lineal, lo que genera una brecha de adaptación, que de alguna forma define el potencial que tienen las empresas para lograr y cambiar la forma de hacer las cosas, lo que se traduce en nuevas oportunidades de negocio (McGowan & Shipley, 2020).

De igual forma ocurre con la seguridad/ciberseguridad, mientras crece y avanza rápidamente la capacidad de los adversarios para sorprender a las organizaciones con diferentes apuestas y estrategias novedosas, la respuesta de las áreas de seguridad y control se hace de forma más lenta y con dificultades para atender a los retos inciertos que los atacantes plantean (Pillay, 2019). Esto define una brecha de adaptación y aprendizaje, que tienen éstas áreas como una oportunidad para repensar lo que conocen y expandir sus reflexiones más allá de los estándares y buenas prácticas.

En este sentido, superar la "falsa sensación de seguridad" crea la crisis necesaria en los modelos de seguridad y control vigentes, que permite incomodar los saberes previos y romper la vitrina de los logros alcanzados, para entender la ciberseguridad/seguridad como un proceso inacabado que no termina con las métricas de efectividad de los

controles para los riesgos conocidos, sino que es parte de la ruta del nuevo territorio que se crea y actualiza con una mayor conectividad, acoplamiento e interacción de objetos conectados fruto del incremento de la densidad digital.

Este nuevo referente digital hace evidente que la seguridad/ciberseguridad sea un ejercicio de confianza imperfecta, donde tanto los clientes, como los objetos conectados y los servicios implementados, podrán tener puntos ciegos de seguridad y control, que tarde o temprano serán aprovechados por los adversarios.

En consecuencia, se hace necesario establecer las bases de una relación resiliente entre los diferentes participantes, para diseñar un entorno de operación basado de umbrales, tolerancias y capacidades que permitan actuar de forma coordinada cuando las cosas no salen como estaban planeadas (Fiskel, 2015).

Así las cosas, tanto la cultura de productividad como la de aprendizaje tendrán que converger para habilitar los nuevos espacios de cooperación, colaboración y coordinación para absorber la complejidad y la incertidumbre que puede generar la materialización de una brecha de seguridad/ciberseguridad, comoquiera que sus impactos van más allá del evento mismo, y revelan la característica sistémica del riesgo cibernético: se conoce dónde inicia la acción pero no dónde termina o cómo se propagan sus efectos.

Superar la "falsa sensación de seguridad" deberá ser el mantra permanente de los ejecutivos de seguridad/ciberseguridad, así como la motivación para mantener una conversación estratégica con los consejos de administración o junta directivas en términos de la resiliencia del negocio y la manera de asumir la antifragilidad como fundamento de unas relaciones simétricas, transparentes y reciprocidad con los diferentes grupos de interés, para así, capitalizar una postura vigilante que desequilibre e interrogue los planes de los atacantes en sus mismos fundamentos: incertidumbre, volatilidad y ambigüedad.

Referencias

Abraham, C., Sims, R. & Gregorio, T. (2020). Develop Your Cyber Resilience Plan. Sloan Management Review. https://sloanreview.mit.edu/article/develop-your-cyber-resilience-plan/

Australian Government (2011). Organisational resilience. Position paper for critical infrastructure. De: https://www.organisationalresilience.gov.au/Documents/organisational-resilience-position-paper-for-critical-infrastructure-australian-case-studies.pdf

Bodeau, D., Graubart, R., Heinbockel, W. & Laderman, E. (2015). Cyber

Resiliency Engineering Aid –The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques. MITRE Corporation. De: https://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf

Cano, J. (2020). Repensando la práctica de la seguridad y la ciberseguridad en las organizaciones. Una revisión sistémico-cibernética. Global Strategy. Global Strategy Report 58. https://global-strategy.org/repensando-la-practica-de-la-seguridad-y-la-ciberseguridad-en-las-organizaciones-una-revision-sistemico-cibernetica/

Cano, J. (2021). Ciberseguridad empresarial. Reflexiones y retos para los ejecutivos del siglo XXI. Bogotá, Colombia: Lemoine Editores.

Clédel T., Cuppens N., Cuppens, F. & Dagnas R. (2020). Resilience properties and metrics: how far have we gone? Journal of Surveillance, Security and Safety. 1. 119-139. http://dx.doi.org/10.20517/jsss.2020.08

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

De la Torre, S. (2004). Aprender de los errores. El tratamiento didáctico de los errores como estrategia de innovación. Buenos Aires, Argentina: Editorial Magisterio del Río de la Plata.

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

Edmondson, A. (2018). The fearles organization. Creating psychological safety in the workplace for learning, innovation, and growth. Hoboken, New Jersey. USA: John Wiley & Sons

Fiskel, J. (2015). Resilient by design. Creating Businesses That Adapt and Flourish in a Changing World. Washington, D.C., USA: Island Press

Grant, A. (2021). Think again. The power of knowing what you don't know. New York, USA: Viking.

Hepfer, M. & Powell, T. (2020). Make Cybersecurity a Strategic Asset. Sloan Management Review. 62(1). 40-45.

McGowan, H. & Shipley, C. (2020). The adaptation advantage. Hoboken, NJ. USA: John Wiley & Son

Mckinsey-IIF (2020). Cyber Resilience Survey. Cybersecurity posture of the financial services industry. https://www.iif.com/Portals/0/Files/content/cyber_resilience_survey_3.20.2020_print.pdf

Perrow, C. (1999). Normal accidents. Living with High-Risk Technologies. Princeton, NJ. USA: Princeton University Press.

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

Reason, J. (2000). Human error: models and management. BMJ. 320-768 doi:10.1136/bmj.320.7237.768

Taleb, N. (2013). Antifrágil. Las cosas que se benefician del desorden. Barcelona, España: Paidos

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

***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–.*

Ciberresiliencia

DOI: 10.29236/sistemas.n159a7

La integración entre Seguridad de la Información y continuidad de negocio

Resumen
Así como la ambigüedad del concepto de Resiliencia Organizacional, la Ciber Resiliencia se debate en confusiones, por lo que el objetivo del presente escrito es proporcionar con claridad una versión encaminada a entender su importancia y alcance, en términos de Seguridad, Ciber Seguridad, Gestión de Crisis y Continuidad.

En esencia, la clave es la integración del escenario de ciberataque al Programa de Continuidad de Negocio, que suena simple, pero tiene muchas repercusiones, partiendo del Análisis de Riesgos que puede llevar a la interrupción del negocio y finalizando con el impacto operativo, reputacional y financiero, así como la implementación de alternativas tendientes a disponer de una estrategia funcional.

Adicionalmente, es necesaria la revisión de la Gestión de Crisis y del Plan de Comunicaciones, pues los mismos han cambiado debido a factores como el tipo de escenario de interrupción, los actores involucrados, los medios de comunicación (principalmente redes sociales) y las audiencias objetivo.

Palabras claves
Resiliencia, Ciberseguridad, Continuidad, Crisis

Introducción

Comenzando por lo básico, ¿sabían ustedes que la palabra resiliencia viene de latín, *resilio* usada por el ejército romano para describir la táctica de dar pasos hacia atrás o replegarse, para luego avanzar hacia adelante, en el sentido de cambio? Un concepto se trasladó a la física y se refiere a la propiedad de algunos materiales de "volver a su forma original" después de que por alguna razón la han perdido, o a la capacidad de deformarse sin romperse (un buen ejemplo es el bambú).

Este concepto se ha venido usando de diferentes maneras y con connotaciones poco entendibles. En cuanto al nivel de las personas, afirman Torres & Ramírez (2019), en psicología es usual hablar de la "capacidad de los seres humanos para adaptarse positivamente a situaciones adversas, superando el trauma ocasionado por estas".

Sin embargo, puede ir más allá y no limitarse a eventos puntuales, empero es una competencia en las personas que les permiten, por ejemplo, tomar decisiones correctas en la forma de ver la vida diaria y manejar cada una de las situaciones bajo presión y también en situaciones límite o eventos de desastres a la que nos enfrentamos.

En el ámbito de las organizaciones, este concepto es refinado y apunta a conectar la estrategia de negocios con la gestión de riesgos sistémicos, la cual plantea el entorno en el que se mueve; tiene que ver con percibir adecuadamente este entorno (conciencia situacional), con la coherencia en la gestión de riesgos y en la implementación de la estrategia, eliminando el trabajo por silos y enfocándose en una gestión integral. En este punto comenzamos a entender, por qué es necesario incluir el manejo adecuado de los riesgos derivados de los ciberataques, como parte de los riesgos sistémicos más preponderantes en la actualidad, bajo la nueva realidad impuesta por la pandemia del COVID-19, dado el incremento del uso de la tecnología en todos los ámbitos.

Existen varias definiciones del concepto de ciber resiliencia, por ejemplo:

- Instituto Nacional de Ciberseguridad de España - INCIBE (INCIBE, 2021), según el cual la ciber resiliencia es "la capacidad para resistir, proteger y defender el uso del ciberespacio de los atacantes".

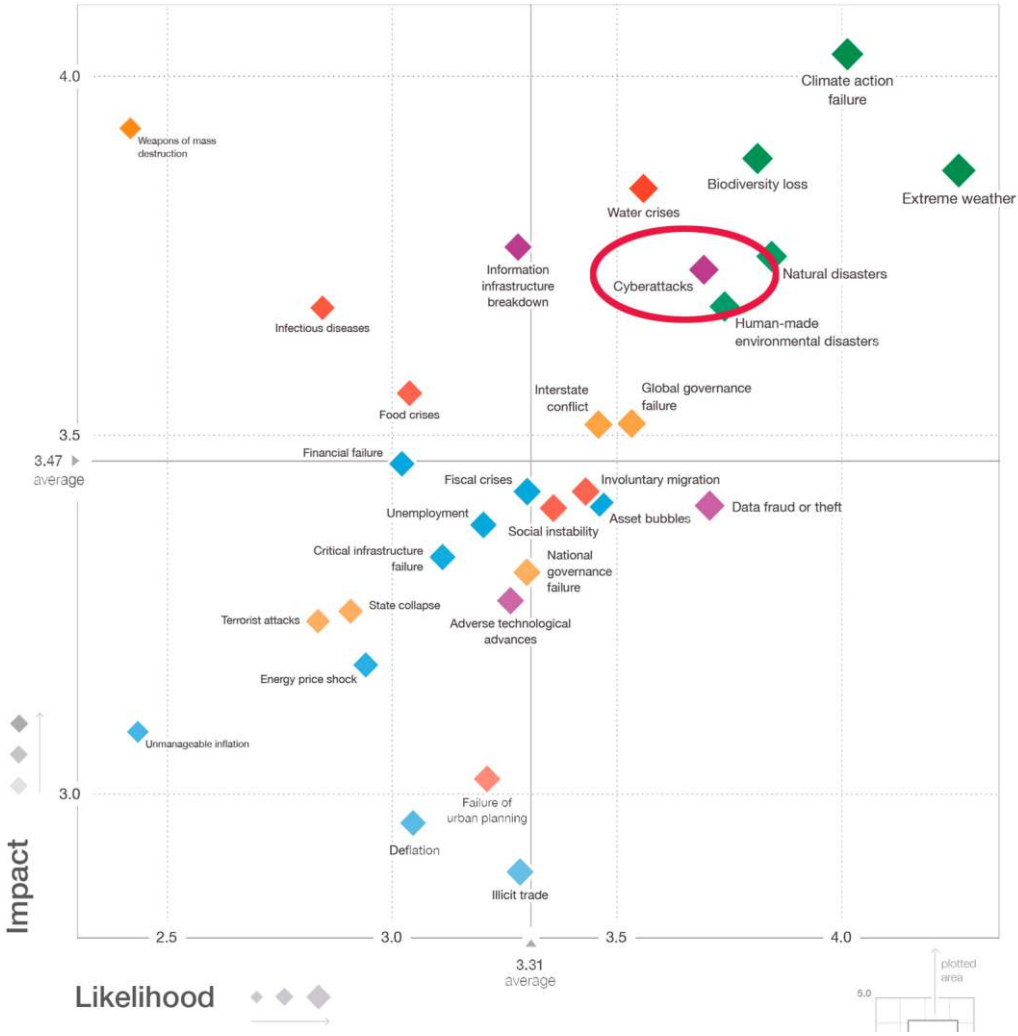
- Disaster Recovery Institute International - DRII (DRII, 2019), afirma que la Resiliencia Cibernética (*Cyber Resilience*) es "la capacidad de una entidad para entregar continuamente el resultado previsto a pesar de los eventos cibernéticos adversos".

• SGSI Blog de ISOTools Excellence (2019), “es la capacidad de las organizaciones de recuperarse de forma rápida de los ciberataques”.

• Así mismo, la habilidad de prepararse, reponerse y recuperarse de un posible incidente cibernético, la ciber resiliencia es una práctica que permite a una organización estar preparada ante posibles ataques, manejar la severidad de estos, y asegurar la continuidad del negocio en caso de que sucedan (The One Brief Aon, 2019).

En varios estudios realizados en los últimos años, el riesgo de ciberataques se ha posicionado como

Figura 1. Paisaje de los riesgos globales 2020



Nota. Matriz de impacto y probabilidad de riesgos. Tomado de Foro Económico Mundial (WEF, 2020).

uno de los de más alto impacto y también en probabilidad de ocurrencia; un ejemplo de esto es el Foro Económico Mundial (WEF, 2020) que califica a los ciberataques dentro del Top 10 de riesgos a nivel Global (Figura 1).

Desde una perspectiva proactiva, ser resiliente implica tomar acciones para desarrollar la capacidad para esa adaptación o incluso transformarse. Por supuesto, para lograrlo el primer paso es innovar, tener conciencia respecto a qué se requiere y contar con los riesgos emergentes que podrían impedir dicho propósito; existen maneras comprobadas que funcionan para manejarlos y sacarles provecho. Cuando se involucra el uso de tecnología de información en las organizaciones en su innovación y operación, también se registra un nuevo ámbito de riesgos, en ocasiones desconocidos y evolucionan más rápido que la capacidad para su entendimiento y manejo.

En este contexto, si una organización quiere ser ciber resiliente, debe empezar por tener personas resilientes en todos los niveles, iniciando con la conciencia de los directivos respecto al entorno global y la actitud, en cuanto a su total convicción para asumirlo. Más allá de las declaraciones vacías de valores corporativos y del cumplimiento de regulaciones, se demanda tomar acciones reales para contar con la capacidad adecuada de protección y respuesta en la recuperación de tecnología, en el instante que sea preciso.

Además, es importante tener en cuenta que hay múltiples factores que afectan la capacidad de una organización de ser resiliente, los cuales se pueden entender desde diferentes marcos de Resiliencia Organizacional existentes:

- ICOR - *International Consortium for Organizational Resilience* (ICOR) de EE.UU.
- BSI – *British Standards Institute* del Reino Unido.
- *The Resilience Institute* de EE.UU.

En todos ellos, se evidencia la necesidad de tener en cuenta múltiples disciplinas en la organización, para desarrollar la capacidad de recuperarse mediante la adaptación; además, entender que no es una práctica en sí misma, sino un resultado de hacer las cosas bien en cada uno de esos aspectos.

A continuación, una breve referencia de cada uno de los marcos mencionados (Figura 2).

Para ICOR la Resiliencia Organizacional se obtiene al conjugar las doce disciplinas que plantea, sin un orden específico y con la necesidad de revisar cómo debe ser el desarrollo específico de cada una y la integración con las demás.

En este modelo prima un enfoque holístico, en el que la Resiliencia

Figura 2. Marco de la Resiliencia Organizacional

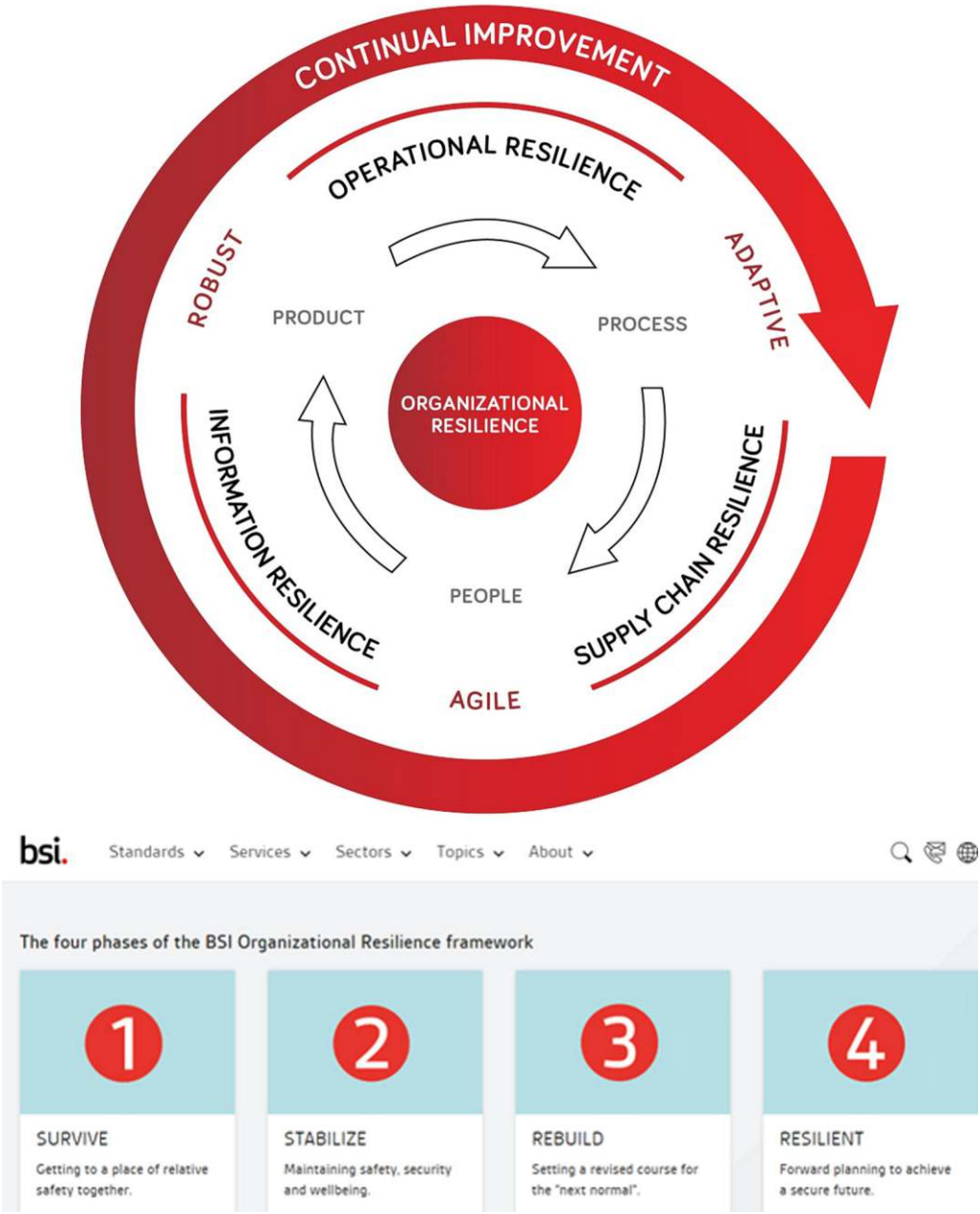
Nota. Marco de la Resiliencia Organizacional. (Tomado de ICOR, 2021, Traducción y adaptación al español iteam).

Organizacional es un resultado de hacer bien las cosas en cada una de las disciplinas y de manera integrada; es decir, teniendo cuidado sobre cómo el desarrollo en cada una de ellas va de la mano con las demás, pues enfocarse en sólo una o algunas, al final no va a permitir la evolución completa como organización. Es necesario balancear los esfuerzos y asignar las responsabilidades de manera adecuada. En este sentido, ser resiliente como organización es una decisión que va absolutamente ligada a la estrategia de negocio establecida. Para finalizar, cabe nombrar que este marco tiene un vínculo a la Resiliencia Comunitaria, es decir, de las ciudades o países, en el que se establecen unos principios y definiciones requeridas para el bienestar de la comunidad a partir de las organizaciones que la conforman (Figura 3).

Para el BSI Group (*British Standards Institution*), la Resiliencia Organizacional se enfoca en dar respuesta operacional a eventos de gran magnitud o crisis, como la Pandemia COVID-19 y para ello establece un antes y un después en las acciones que la organización debe tomar, con un enfoque proactivo en los procesos y en las personas, pero alineado a la estrategia de negocio.

En este caso, el enfoque en lo operacional significa inicialmente definir el manejo a la situación, en ciertos casos dirigir sus esfuerzos a establecer un ambiente seguro para su operación con antelación, cono-

Figura 3. Three essential elements of Organizational Resilience

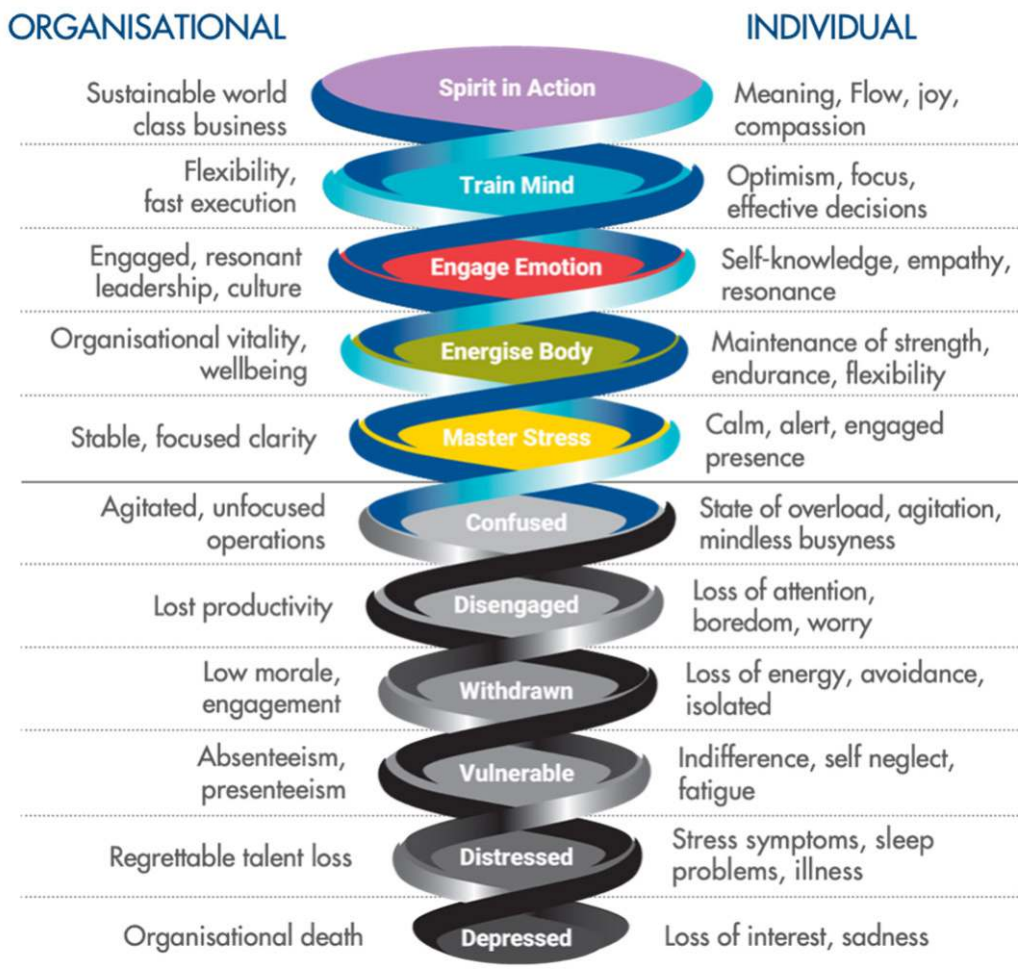


Nota. Three essential elements of Organizational Resilience. (Tomado de BSI)

ciendo su ambiente y su funcionamiento. El siguiente paso, es la estabilización para funcionar con las medidas implementadas anteriormente, ciertas restricciones y cambios que usualmente requieren esfuerzos importantes para asegurar el bienestar de los colaboradores, el manejo de la cadena de suministro y la información.

Posteriormente, en la reconstrucción se induce al cumplimiento de estándares en los ámbitos de Gestión de Riesgo, Ambiental, Continuidad de Negocio, Ocupacional, Calidad y Seguridad de la Información, como prácticas probadas que aportan a esa estabilización de la operación y al funcionamiento en la nueva normalidad. Incluso puede

Figura 4. Resilience Spiral



Nota. Resilience Spiral. (Tomado de The Resilience Institute, 2021)

llevar a cambiar su modelo de negocio e industria, para adaptarse y estar preparado para posibles eventos futuros que requieran de la Resiliencia Organizacional (Figura 4).

Para el *Resilience Institute*, la capacidad resiliente de las organizaciones parte de las personas y crea un paralelo en diferentes niveles de evolución, estableciendo un punto de inflexión entre el deber ser (positivo) y lo no aceptable (negativo), en la medida que se cumple con los 60 factores de resiliencia que están organizados en 11 categorías. La meta es evolucionar y sostener dicha evolución en la medida que se reconoce las debilidades y riesgos y se trabaja para resolverlos.

Esta orientación, viene influenciada desde el desarrollo de lo personal y el potencial del ser humano, para luego extrapolar a las organizaciones y también a las comunidades. Utiliza una herramienta de diagnóstico para establecer un punto de partida y un plan de trabajo, para aprender a vivir y superar los factores que limitan actualmente su desarrollo y para adaptarse a lo necesario para crecer a la resiliencia, sabiendo que no hay soluciones mágicas y que se requiere de esfuerzo para la evolución deseada. Utiliza la figura de la espiral como concepto para avanzar, con base en lo existente, sin olvidar los pasos anteriores, aprendiendo, adaptándose y creciendo. Aceptando que siempre existen retos, aún en la prosperidad y que representan siempre una posibilidad de aprender.

Realizando una comparación de los tres modelos marco de Resiliencia Organizacional, encontramos en resumen que **ICOR** establece una visión global y holística, con diversas disciplinas que conllevan al resultado y se integra con la resiliencia comunitaria. Por otra parte, **BSI** se enfoca en lo operacional y en la organización, protegiendo y adaptando el funcionamiento propio, la cadena de suministro y la información. Por último, el **Resilience Institute** tiene un enfoque más filosófico que permea desde lo personal a las organizaciones y las comunidades, con la noción de crecimiento y evolución.

Los tres marcos tienen en común los conceptos de adaptación y gestión de riesgos, como parte fundamental de la capacidad de ser una organización resiliente, cada cual con diferentes formas para lograrlo.

¿Por qué es importante gestionar la ciber resiliencia?

El aumento de los vectores de ataque que significa la amplia implementación de nuevas Tecnologías de Información, es la principal razón que conlleva la necesidad de gestionar de manera eficaz este importante riesgo, aplicable prácticamente a cualquier tipo de organización; ya no es único en grandes y conocidas corporaciones, más bien se ha encontrado que es asunto de

las pequeñas y medianas empresas, toda vez que son más vulnerables por estar menos protegidas y poseer una menor conciencia de los riesgos en general.

Algunos datos para tener en cuenta:

• Más del 50% de la población mundial, ahora está en línea; aproximadamente un millón más personas se unen a internet cada día. Dos tercios de la humanidad poseen un dispositivo móvil. La cuarta revolución industrial (4IR) de la mano de las nuevas tecnologías atraen grandes beneficios económicos y sociales a gran parte de la población mundial[1].

• Quinta generación (5G) redes, computación cuántica y la Inteligencia artificial están creando oportunidades y a su vez, nuevas amenazas propias en ciberseguridad.

• Ciberataques a la infraestructura crítica, ha sido el enfoque inicial de los delincuentes.

• El robo de datos, permite la manipulación de comportamiento individual y colectivo, liderando a daño físico y psicológico.

La integración de Seguridad de la Información y Continuidad de Negocio

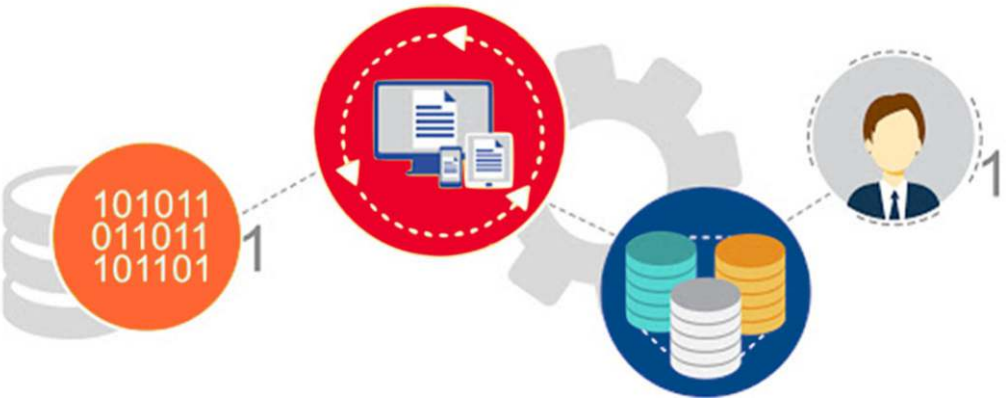
Un enfoque sobre la integración es el que nos brinda el NIST Cyber Resilience Framework 1.1[2], en el que se establece cómo en los pasos ini-

[1] The Global State of Digital 2020 (2020). https://www.hootsuite.com/pages/digital-2020
[2] NIST Cyber Resilience Framework 1.1 https://www.nist.gov/cyberframework/framework

Figura 5. Cyber Resilience Course

Nota. Cyber resilience course. (Tomado de DRII. CRLE 2000 material, 2019)

Figura 6. Identificación de Amenazas



Nota. Identificación de amenazas. (Elaboración propia).

ciales la Seguridad de la Información y Ciber Seguridad son responsables de la protección, y la Continuidad de Negocio es la responsable de la recuperación, combinando manejo de crisis y específicamente la respuesta del DRP para la infraestructura de tecnología. Ambas disciplinas son responsables en conjunto de la gestión de incidentes (Figura 5).

Lo primero, es identificar correctamente las ciberamenazas del entorno en el que opera la organización. Es un proceso estructurado que consulta diferentes fuentes para identificar y proveer información sobre amenazas cibernéticas y sus tendencias (Figura 6).

Este proceso suele llamarse Ciber Inteligencia[3], puesto que es un término acuñado a partir de las estructuras gubernamentales; consta de varias etapas que serán revisadas más adelante y sus salidas vendrán determinadas por la naturaleza de la amenaza, si es conocida o no, activando otros procesos que forman parte de la gestión de ciberseguridad (Figura 7).

La planificación de la gestión de ciberamenazas incluye:

- Definir qué fuentes van a ser incorporadas a la investigación.
- Establecer las responsabilidades que tendrá el equipo.
- Establecer el método y las herramientas de identificación de amenazas.
- Conocer la frecuencia en que se realizarán las investigaciones y se presentarán los resultados.

[3] Ciber Inteligencia: Se define como la adquisición y el análisis de información para identificar, rastrear y predecir las capacidades, intenciones y actividades cibernéticas que apoye la toma de decisiones. ASOSEC – Asociación Colombiana de Seguridad. Recuperado de https://asosec.co/ciberinteligencia/

La recolección de datos tiene como objetivo obtener la información en bruto, establecer los atributos de la información y contar con un repositorio de los datos.

El análisis de los datos consiste en la aplicación de diversas técnicas para poder convertir los datos en información. El resultado final del análisis de ciberamenazas deberá determinar qué acciones realizar con ella.

La conclusión de este proceso es la difusión a la organización de los hallazgos, para:

- Alineación de los equipos.
- Fortalecimiento de controles o desarrollo de nuevos.
- Preparación preventiva de los usuarios.
- Llamado a la acción.

Es decir, tomar medidas que realmente fortalezcan la capacidad de protección de la organización, mediante una gestión adecuada de los incidentes que sean amenazas de ciberataques. No obstante, puede ser insuficiente y es por ello que se necesita una capacidad de recuperación, desde la Continuidad de Negocio, esto implica una integración, la cual se aprecia en la figura 8.

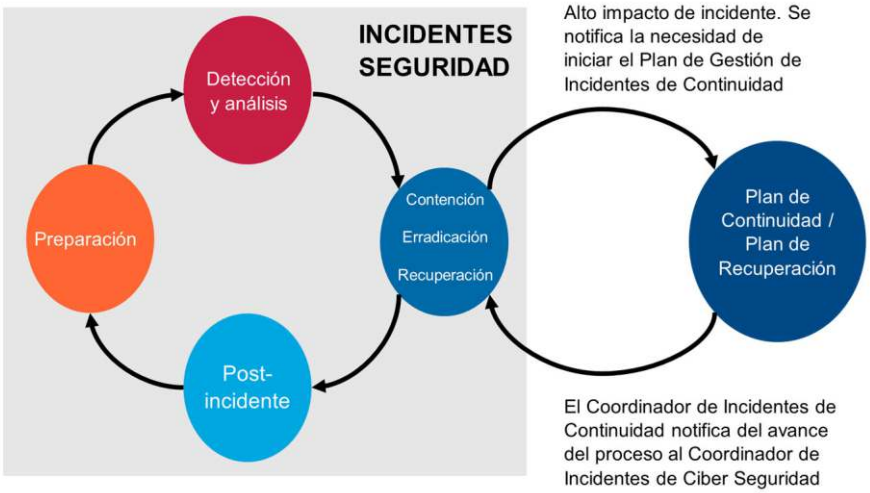
Recuperación de tecnología y lo que se requiere hoy

Desde que comenzó la disciplina de *Disaster Recovery*, en los tiem-

Figura 7. Modelo de gestión de Ciber amenazas

Nota. Modelo de gestión de Ciber amenazas. (Elaboración propia).

Figura 8. Integración del proceso de atención de incidentes de seguridad con el proceso de continuidad de negocio y recuperación ante desastres



Nota. Integración del proceso de atención de incidentes de seguridad con el proceso de continuidad de negocio y recuperación ante desastres. (Elaboración propia).

pos de los primeros mainframes, la dependencia de un solo sitio de cómputo concentrando todo el procesamiento y el riesgo de perderlo, la estrategia siempre fue crear una capacidad redundante, para recuperar los datos y el procesamiento en otro sitio similar, equivalente o algunas veces superior.

Lo clásico es establecer lo más claro posible qué es lo más crítico para el negocio (entendiendo negocio, como la razón de ser de la organización, no sólo para empresas comerciales) usualmente, mediante un Análisis de Impacto al Negocio (BIA por sus siglas en inglés, *Business Impact Analysis*), para definir los procesos críticos y todos los recursos que requieren para una recuperación adecuada, así como los tiempos en que deberían estar de nuevo operativos; uno de los recursos más importantes ha sido la tecnología, las aplicaciones y cómo funcionan para la operación del negocio y qué tantos datos se deben conservar. También se identifican los riesgos del sitio de cómputo y de los sitios donde funciona el negocio. Con estos insumos se diseña una Estrategia de Continuidad, dentro de la cual la recuperación de la tecnología de información es una parte crucial, a la que se le conoce como DRP (por sus siglas en inglés, *Disaster Recovery Plan*). Al final se documentan los planes (procedimientos para las diferentes

áreas de TI) y se hacen ejercicios incluyendo pruebas, para asegurarse de que todo ello funciona.

Han evolucionado diferentes tecnologías para realizar estas tareas, replicar más rápido y de manera eficiente e incluso hasta lo que se conoce como Disponibilidad Continua (*Continuos Availability* por sus siglas en inglés), que permite tiempos de recuperación cercanos a cero.

Inicialmente el DRP consistía en tener un centro de datos alterno, pero ante el escenario de ciberataque eso no es suficiente, simplemente porque el daño causado al centro de datos principal se replicaría tan rápido como sea la eficacia de la estrategia implementada, que puede ser en segundos o en minutos, por lo cual no es una defensa apropiada, toda vez que el resultado sería tener en corto tiempo dos o más centros de datos atacados y probablemente inservibles.

Es por esto, que se requiere implementar otras estrategias y nuevas tecnologías, tampoco procedimientos y trabajo en conjunto con las áreas responsables de seguridad de la información, y otros departamentos de TI. Algunos ejemplos son:

- Air GAP y Bóveda segura (vault), que en esencia establece una conexión aislada y controlada, física y lógicamente, para evitar que el ataque se replique, pero no los datos más esenciales del DRP que se guardan de manera segura cada vez que se activa y asegura la conexión.

- Regreso en el tiempo, a múltiples puntos de recuperación hacia atrás, lo que se logra a partir de tecnologías de virtualización e hiperconvergencia.

Conclusiones

Atender esta nueva realidad de ciberataques aumentados, que evolucionan muy rápido y son difíciles de manejar, requiere de un enfoque diferente, en el que se combinan varias disciplinas, siendo las principales la Seguridad de la Información y la Continuidad de Negocio.

Cabe considerar que no se debe realizar de manera independiente, por el contrario, implica trabajo en conjunto con el objetivo en común de gestionar este riesgo de la mejor manera para la organización.

La integración de las disciplinas es la clave, primero con trabajo preventivo, implementando las soluciones tecnológicas y procedimientos que obstaculicen la realización de los ataques (Seguridad de la Información), sin creer que se es completamente infalible; también es necesario implementar las soluciones para tratar el riesgo del ciberataque una vez se presenta, para poder restaurar los datos y el procesamiento desde fuentes seguras y aisladas.

En paralelo, activando la gestión de crisis para este caso tan especial, que tiene tanto potencial de dañar la reputación, por negligencia (permitir que suceda el ataque a los datos propios o de los clientes) o por mala actuación una vez sucede. En este sentido, es preciso revisar el Plan de Manejo de Crisis y el Plan de Comunicaciones, para hacerlos más asertivos, toda vez que requieren una atención más rápida que otros escenarios y exigen la capacidad de ajuste, cambio y toma del rumbo a la misma velocidad de los acontecimientos del ataque cibernético, que puede ser caprichoso de acuerdo con lo que el atacante pueda decidir durante o desde antes, muchas veces dejan acciones del código malicioso para más adelante contar con una reserva en su actuación y así tomar ventaja.

Desde la perspectiva de Continuidad de Negocio es necesario revisar el proceso y cómo interactúa en el Comité de Crisis con el área de Seguridad de la Información/Ciberseguridad, según sea el caso, para la adaptación de la Estrategia y Planes de Continuidad antes de que ocurra el evento, y para la toma de decisiones y la activación necesaria, una vez el incidente existe o tiene el potencial de convertirse en una crisis.

En conclusión, la Ciber Resiliencia es la capacidad de recuperarse ante eventos de ciberataque, impidiendo o minimizando sus efectos desde la Seguridad de la Información y también estableciendo un Estrategia de Recuperación de Tecnología (DRP) adecuada integrada a la Continuidad de Negocio y la Gestión de Crisis.

Referencias

DRII (2019). CRLE 2000 Cyber Resilience for the Business Continuity Professional. Course Instituto Nacional de Ciberseguridad de España (INCIBE). (3 de marzo de 2021).
¿Qué es la ciber resiliencia y cómo influye en la seguridad? [Mensaje en un blog].
https://agenciab12.com/noticia/que-es-ciberresiliencia-como-influye-seguridad

Foro Económico Mundial - WEF (2020). The Global Risks Report 2020. (N.15). Recuperado de
https://es.weforum.org/reports/the-global-risks-report-2020

Organizational Resilience Framework BSI. (2021). Three essential elements of Organizational Resilience.
https://www.bsigroup.com/en-GB/our-services/Organizational-Resilience/Three-essential-elements-of-Organizational-Resilience/ y https://www.bsigroup.com/ en-GB/our-services/Organizational-Resilience/bsi-organizational-resilience-framework/

ICOR (2021). Organizational Resilience Framework. Traducción y adaptación al español iteam.
https://www.build-resilience.org/organizational-resilience-framework.php

The Resilience Institute (2021). Resilience Spiral. https://resiliencei.com/resources/resilience-spiral/

SGSI Blog de ISOTools Excellence (2019). ¿Qué es la ciber resiliencia? [Mensaje en un blog]. https://www.pmg-ssi.com/2019/10/que-es-la-ciber-resiliencia/

The Global State of Digital 2020 (2020). https://www.hootsuite.com/pages/digital-2020

The One Brief Aon. (2019) La Resiliencia Cibernética: ¿Qué hacer en caso de un posible ataque? https://theonebrief.com/latam/post/la-resiliencia-cibernetica-que-hacer-en-caso-de-un-posible-ataque/

Torres, J. C. & Ramírez, N. (2019). Resiliencia ¿Organizacional? LinkedIn. iteam Ltda. https://www.linkedin.com/pulse/resiliencia-organizacional-norman-ramirez/

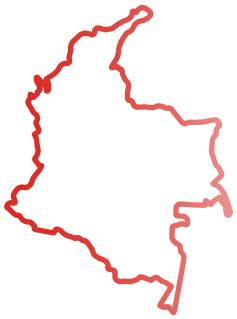
Norman A. Ramírez S. MBCP, CRMP, CCRP e Instructor (DRII), MBCI (BCI) & Auditor Líder ISO22301 (ICOR). *Posee amplia experiencia como emprendedor en su rol de Gerente General de iteam y como especialista Consultor Senior de Resiliencia Organizacional, Continuidad de Negocio y Riesgos Empresariales. Graduado de la Universidad de los Andes (Bogotá, Colombia), Ingeniero Industrial (1998) y Especialista en Sistemas de Información en la Organización - ESIO (2002).*

Reporte FortiGuard Labs

Primer Trimestre 2021

Más de 7 mil millones

de intentos de ciberataques en América Latina y el Caribe



Colombia

1,000 millones

de intentos de ciberataques

Crecen las amenazas de malware vía redes sociales

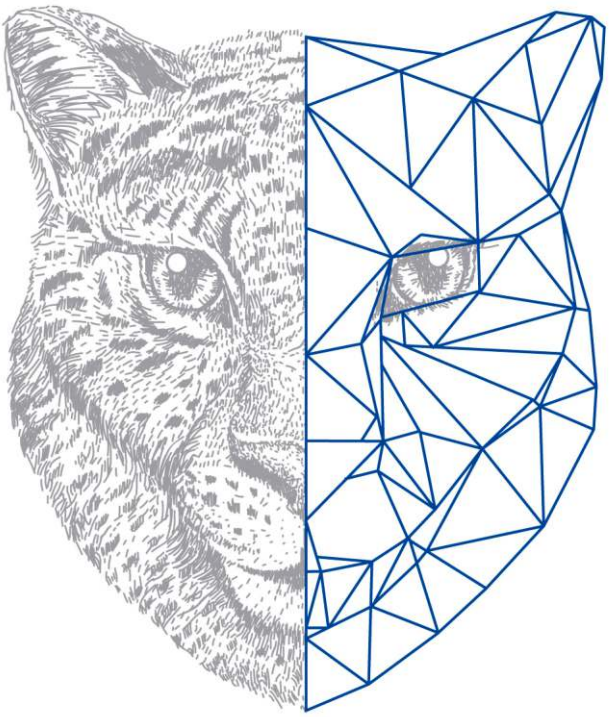
Malware basado en la web:

incremento en la **utilización de redes sociales** para difundir publicidad y sitios web engañosos.
Los **usuarios comprometidos** comparten mensajes con contenido malicioso a sus **contactos desde sus perfiles de redes sociales,** sin tener conocimiento de ello.

No sea parte de la estadística, hablemos para apoyarlo en su estrategia de ciberseguridad: **jbernate@fortinet.com**

www.fortinet.com/lat

NEOSECURE
SABEMOS DE SEGURIDAD



Más de **20 años** de trayectoria nos respaldan como especialistas en Soluciones de Ciberseguridad y Servicios Gestionados de Latinoamérica .

Seguridad Corporativa | SGS | Identidad Digital | Seguridad OT | Consultoría

10, 11 y 12 DE AGOSTO

POCWEEK2021

Haz parte de uno de los eventos más importantes y novedosos de la industria IT y OT

Contáctanos: marketingcolombia@neosecure.com

Visítanos en www.neosecure.com - Presencia Regional