No. 155 Abril - Junio 2020 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. 2020

Seguridad y ciberseguridad

¿Qué hemos aprendido en esta década?

¿Cuáles son los retos a 2030?

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

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

NUEVOS CONVENIOS PARA ASOCIADOS

Alfaomega CLOUD

IDEM TECHNOLOGIES

emi
Una empresa del Grupo Falck

emermédica
Porque tu salud nos mueve.

sura

Semana

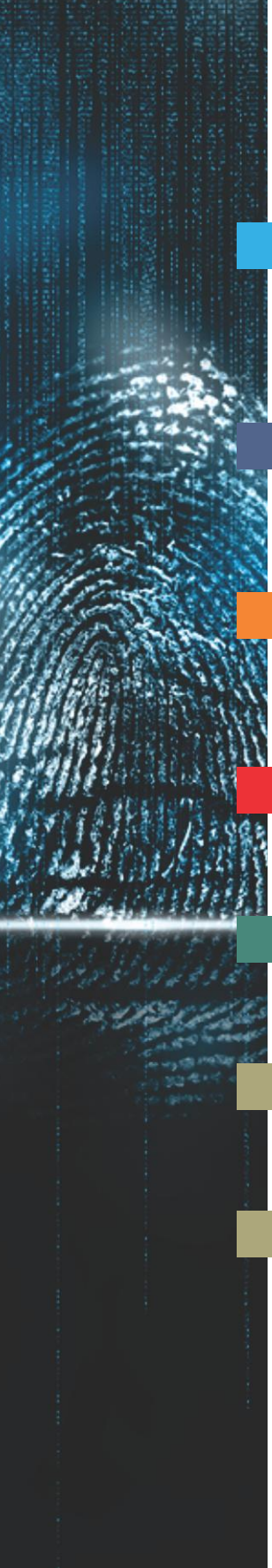
EL TIEMPO

open english

PREVER

Unión de Contadores Asociados

para mas información: 3015530540 o al correo acis@acis.org.co



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 2020
Calle 93 No.13 - 32 Of. 102
Teléfonos 616 1407 - 616 1409
A.A. 94334
Bogotá D.C.
www.acis.org.co

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

No te olvides pasar por nuestra Bolsa de Empleo

https://acis.org.co/bolsadeempleo/

Revive nuestras conferencias en nuestro Canal de Youtube

aciscolombia

Para ingresar a nuestra charla semanal:
https://meet.google.com/nyw-vwxr-muu

Llamado a Conferecista Semanal

Es la oportunidad de dar a conocer tus conocimientos. Participa como conferencista en nuestros miércoles de conferencia

Escribenos: Acis@acis.org.co
Inscribete: https://n9.cl/v87b

Seguridad de la información y ciberseguridad empresarial

DOI: 10.29236/sistemas.n155a1

De las buenas prácticas al desarrollo de capacidades. Los nuevos escenarios que propone la convergencia tecnológica y de disciplinas científicas abren oportunidades y retos inéditos, así como amenazas emergentes.

Jeimy J. Cano M.

Revisando las reflexiones en el número 115 de la Revista "SISTEMAS", publicado en 2010 sobre el futuro de la seguridad de la información, se afirmaba que: "*las enseñanzas de la inseguridad de los últimos 10 años podríamos resumirlas en una exigente necesidad de interconexión permanente, acceso a la información ágil e instantánea y sobremanera, interacción constante y sin restricciones*" (Cano, 2010).

Esta afirmación muestra que, durante la primera década del nuevo milenio, la conectividad creó un escenario digital de interacción permanente, en el que se configuró un

“halo” de confianza en la tecnología de información y comunicaciones para un aumento en el flujo de datos que privilegió la eficiencia de las operaciones en las empresas. En este sentido, y muchas veces sin notarlo, se fueron configurando fallas y vulnerabilidades, perfeccionando las estrategias de los adversarios con ataques novedosos.

Lo que ocurrió durante la segunda década del milenio coincide con los análisis planteados en el número 115 de nuestra revista. La convergencia de la seguridad de la información con la seguridad física y electrónica, la tercerización de las áreas de tecnología de información y la desobediencia de los usuarios se convirtieron en la base de los retos para los profesionales de la seguridad de la información los cuales, cruzados con las cambiantes exigencias del negocio y la dinámica de los mercados, configuraron un caldo de cultivo sazonado para la propagación de la inseguridad en cada uno sus actores (Cano, 2010).

La perspectiva para los próximos diez años (2020-2030) sugiere un escenario diferente y con experiencias aumentadas para los clientes de las empresas. Los ecosistemas digitales, la realidad aumentada, las cadenas de bloques, la computación en el borde y el advenimiento de los sistemas ciberfísicos, desplegados en las diferentes industrias y sectores productivos, serán el nuevo contexto para que los adversarios tomen posiciones estratégicas y desarrollen nuevas propuestas agresivas que tensionen los renovados modelos de seguridad y control de las compañías (Cano, 2020).

En este contexto, la sensación de que “pensábamos que conocíamos los riesgos”, da lugar a una nueva lectura de la realidad, en un ambiente cibernéticamente aumentado, con situaciones inéditas para las organizaciones y cuyo tratamiento no responde ni a las buenas prácticas ni a los estándares vigentes, sino al desarrollo de capacidades para defender y anticipar escenarios asimétricos.

Es por esto que la revista “SISTEMAS”, de la Asociación Colombiana de Ingenieros de Sistemas −ACIS−, ha decidido revisar, explorar y analizar en prospectiva la dinámica de la seguridad/ciberseguridad en los próximos diez años. Con ese objetivo, fueron convocados profesionales de distintas disciplinas, quienes desde su área de experiencia proponen reflexiones para seguirle la pista al desarrollo de la protección de los conocidos activos de información y los nuevos activos digitales, desde las lecciones aprendidas, los negocios y retos actuales, así como las tendencias futuras que desde hoy se avizoran en el horizonte.

El ingeniero Armando Carvajal Rodríguez, columnista invitado, establece desde su práctica de consultoría un marco base para reflexio-

nar sobre la seguridad de la información y la evolución de la inseguridad, como un reto clave en la gestión de riesgos y como fundamento para advertir iniciativas de ataque y responder a los hechos que podrían desestabilizar empresas y naciones. En esa dirección presenta el artículo “Reflexiones sobre la seguridad de la información en la economía 5.0”.

El entrevistado en este número de la revista es José Eduardo Campos, especialista en ciberseguridad, con más de 25 años de experiencia, consultor y director de proyectos innovadores de desarrollo empresarial en los Estados Unidos, con enfoque en mercados emergentes en América Latina, Sudeste Asiático e India.

Por su parte, el ingeniero Andrés Almanza Junco presenta el análisis de los resultados de la versión número veinte 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 oportunidad, se observan dos décadas de la evolución de las prácticas de seguridad y control en las empresas y en el país.

El foro contempla la validación y prospectiva de la seguridad y control, en la opinión de los mismos participantes en el foro del año 2010. Los ingenieros Juan Camilo Reyes, Javier Díaz, Evans, Andrés Almanza Junco y el abogado Rafael Gamboa Bernate revisaron sus planteamientos de esa época, en el marco de los últimos 10 años, para documentar su visión a 2030 para los negocios. Ellos advierten sobre la necesidad de reinventar las prácticas de seguridad de la información, además de avanzar en una perspectiva interdisciplinaria, orientada a que los profesionales y ejecutivos de seguridad y control puedan enfrentar un escenario cada vez más disruptivo, inestable e hiperconectado, con una mayor exigencia de anticipación, más que de prevención.

Así mismo, nuestros lectores dispondrán de dos artículos sobre el uso de la movilidad como estrategia de formación en seguridad de la información y las lecciones aprendidas en seguridad y control durante los últimos diez años. Un primer documento de autoría del ingeniero Julio Poveda Gómez, se ocupa de analizar las vías para articular las estrategias de “aprendizaje móvil”, a través de una aplicación para enseñar conceptos de seguridad informática.

El segundo artículo, escrito por este servidor, aborda las lecciones aprendidas en la última década en seguridad de la información, así como los retos emergentes para la seguridad/ciberseguridad. Allí se es-

tablecen cinco temáticas relevantes (*la computación la nube, la computación móvil, la convergencia tecnológica, las redes sociales y la asimetría de los ciberconflictos*), que sustentan las bases para asumir los retos en el marco de las empresas digitales y tecnológicamente modificadas.

La totalidad de este contenido muestra un panorama actual y prospectivo de las prácticas y desafíos de la seguridad/ciberseguridad, como una excusa académica y práctica para superar las certezas propias de los estándares y prácticas existentes. Los diferentes temas invitan a todos los profesionales en las diferentes áreas, a explorar las nuevas realidades de la protección de los activos de información y de los nuevos activos digitales, sin perjuicio de la transformación de los retos e inestabilidades políticas, económicas, sociales, tecnológicas, legales y ecológicas vigentes y futuras.

Referencias

Cano, J. (2010) Seguridad de la información: ¿qué hemos aprendido y para dónde vamos? *Revista SISTEMAS.* Asociación Colombiana de Ingenieros de Sistemas (ACIS). 115. 4-1.

Cano, J. (2020) Retos de seguridad/ciberseguridad en el 2030. Reflexión sobre un ejercicio prospectivo incompleto. *Revista SISTEMAS*. Asociación Colombiana de Ingenieros de Sistemas (ACIS). No. 154. 68-79. Doi: 10.29236/sistemas.n154a7.

***Jeimy J. Cano M., Ph.D, CFE, CICA**. Profesor distinguido de la Facultad de Derecho. Universidad de los Andes. Ingeniero y magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Especialista en Derecho Disciplinario de la Universidad Externado de Colombia. Ph.D en Business Administration en Newport University, CA. USA. y Ph.D en Educación, 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. Es director de la revista Sistemas de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*

Reflexiones sobre la seguridad de la información

DOI: 10.29236/sistemas.n155a2

Retos y expectativas en la economía 5.0. Despliegue de los asistentes digitales (robots en software)

Resumen
La quinta revolución industrial nos vuelve a invitar a que los robots en software nos asistan y que sean ellos los que hagan las tareas repetitivas para que los seres humanos tengamos tiempo de ser innovadores, resolvamos problemas impredecibles, comprendamos las emociones de nuestra humanidad y que, mediante el pensamiento crítico podamos complementarnos con los demás.

Palabras claves
Economía Lineal, Economía Circular, Transformación Digital, Ciberseguridad.

Introducción

En algunas ocasiones, al terminar la jornada y revisar retrospectivamente lo realizado, sentimos que hacemos diariamente tareas repetitivas. Tenemos la sensación de que somos autómatas; nos sentimos como si fuéramos robots, pues todos los días reproducimos actividades como leer correos, diligenciar hojas electrónicas, volcar hojas electrónicas en los sistemas de información de la organización para la que trabajamos y un sinnúmero de reportes, entre otras.

En el caso específico del oficial de seguridad o CISO, que ejecuta actividades propias como hacer análisis de vulnerabilidades, penetrar fallas, hacer análisis de riesgos de ciberseguridad y seguridad de la información, ayudar a ejecutar controles para gestionar la seguridad de la información, se tiene la impresión de un parecido con los robots. Aún con la pasión con que las ejecutamos, nos percatamos de que estas son tareas repetitivas, especializadas, propias de un autómata.

Ahora, frente a un evento no predecible como la pandemia COVID-19, nos invade la sensación de estar encasillados, sin esperanzas y llenos de incertidumbre por el creciente número de muertos debido al virus. Afortunadamente, estamos reunidos en familia y, estando en nuestros hogares debido al aislamiento obligatorio decretado por el Gobierno Nacional, nos colman sentimientos de gratitud con Dios que antes no teníamos con tanta frecuencia. Son sentimientos fuertes que expresan agradecimiento con lo que nos rodea, con lo que nos provee la naturaleza, en especial con nuestras familias, con nuestras parejas y hasta con nuestras empresas, pues nuevamente constatamos que nada está establecido perpetuamente; que todo cambia y debemos adaptarnos al cambio.

El autor de este documento considera que el Covid-19 es un evento aleatorio de tipo catastrófico por los efectos de los impactos económicos y sociales causados, que pudo haber sido prevenido, la capacidad de enfrentar eventos aleatorios es único de los seres humanos, pero estamos sumergidos en las actividades repetitivas del quehacer diario, por lo tanto la transformación hacia una economía circular es inevitable, y la seguridad de la información y la ciberseguridad no pueden escapar a la atracción tan fuerte como la generada por la economía 5.0, esta nos brinda la capacidad de resolver problemas no predecibles mediante la creación de nuevas ideas, en cambio de continuar haciendo tareas repetitivas que no generan valor.

Economía circular

Vivimos y nos desenvolvemos en una economía lineal donde pare-

ciera que la razón de existir es la adquisición de propiedades y productos de forma repetitiva, en un ciclo de no terminar. Independiente de la clase social en la que estemos enmarcados, todos queremos obtener cada vez más productos, sin importar a dónde se dirijan los residuos del proceso desde su diseño hasta su creación, por lo tanto, no existe una conciencia colectiva del efecto a largo plazo de no reciclar. Esto se evidencia cuando desechamos artículos al haber finalizado su ciclo de vida o, peor aún, cuando queremos renovarlos porque anhelamos tener en nuestras manos la última tecnología disponible en el mercado, así objetivamente no la necesitemos.

En la economía lineal pueden observarse las siguientes fases desde la entrada de las materias primas que intervienen en el proceso, hasta la obtención del producto final: extracción, refinamiento, fabricación, ensamblaje, generación de desechos o residuos y entrega del producto final. Es muy importante anotar que las materias primas están encasilladas en una obsolescencia programada; por ejemplo, un firewall de perímetro para BD y/o aplicaciones Web, un control DLP, como algunos otros productos de ciberseguridad, después de tres o cuatro años, serán obsoletos por la obsolescencia programada y los residuos no reutilizados; en consecuencia, fue impactada negativamente la naturaleza. Por ello en la actualidad, somos el reflejo de la cuarta revoluciónn industrial; una sociedad de consumo desmedido e irresponsable con la naturaleza, y estos recursos naturales disminuidos son los que le dejaremos a las futuras generaciones, nuestros hijos.

En esta cuarta revolución industrial o Economía 4.0, el ser humano ha creado tecnologías innovadoras y disruptivas que nos han permitido iniciar la transformación digital de sociedades y gobiernos. Algunas de estas tecnologías son la computación en la nube, la analítica de grandes volúmenes de datos o Big Data, la Inteligencia Artificial, la impresión 3D, IoT y los lenguajes de programación RPA (por sus siglas en inglés, automatización de procesos mediante robots), entre otros (Deloitte, 2020).

Sin embargo, no todo es negativo en la cuarta revolución industrial; actualmente, los novedosos “trabajadores digitales” o “asistentes digitales” están siendo aprovechados por las diferentes industrias para reducir costos, disminuir la probabilidad de errores en los procesos, mejorar la actitud y aumentar la moral de los empleados humanos.

RPA + Inteligencia Artificial + Analítica de patrones, le permite hoy al ser humano enfocarse en las tareas más humanas, es un inicio incipiente de la colaboración entre humanos y robots de software. En el presente año, emergerán tecnologías robóticas con apoyo de otras

Figura 1: Tecnología disruptiva RPA (Elaboración propia)

de inteligencia artificial, que le sugerirán al humano, de forma automática, cuáles actividades repetitivas se pueden automatizar.

El punto más alto de la cuarta revolución industrial es la transformación digital de las empresas, que aún se está dando y durará unos años más, antes de que la explotemos en la incipiente quinta revolucion industrial. Por ejemplo, en Colombia la banca y las telecomunicaciones hacen uso intensivo de la robótica por software en sus operaciones y ciberseguridad, pero el sector salud, defensa y justicia, por nombrar algunos, estan distantes de iniciar la transformacion digital, la mejor evidencia es como estamos afrontando la pandemia Covid-19 a nivel judicial, segun lo informado por los medios de comunicacion locales.

En la naciente quinta revolución industrial, la base será la economía circular, cuyo objetivo no será la adquisición de productos, sino la adquisición de servicios.

Entonces veremos muchos productos de ciberseguridad y seguridad de la información en forma de servicios; por ejemplo, protección contra amenazas IoT, protección contra amenazas de la inteligencia artificial en automóviles autónomos, protección, gestión y analítica de riesgos emergentes, entre otros.

Por lo tanto, la cantidad de innovación requerida será un factor crítico para evitar la destrucción de los ecosistemas en los que vivimos a causa de la extracción desmedida de materias primas o insumos para fabricar los productos que se venderán como servicios. Esta quinta revolución industrial propone el complemento del hombre con la máquina; será común encontrarnos en nuestros trabajos con los llamados "ciberhumanos": parte humano, parte máquina. Es decir, humanos hibridos que tendran piernas y hasta brazos ciberneticos.

Hoy en la cuarta revolucion industrial encontramos en el sector financiero, en especial en las organizaciones bancarias como, por ejemplo, Bancolombia, unos 12.000 robots en software que asisten a los trabajdores bancarios (Attended Bot) y unos 3.000 robots en software que ya no requieren de intervencion humana (Unattended Bot) (Otálvaro, 2019).

La cuarta revolución industrial construyó las tecnologías disruptivas que serán utilizadas y explotadas masivamente en la naciente quinta revolución industrial; en esta, podrán observarse las siguientes fases: producción, consumo y reciclaje.

Se define la economía circular como "Repensar, Reutilizar, Reparar,

Figura 2: Trabajador o asistente digital (Elaboración propia)

Figura 3: Iniciando la Transformación Digital (Elaboración propia)

Restaurar, Re-manufacturar, Reducir, Re-proponer, Reciclar y Recuperar" (Minambiente, 2018).

Los principios de la economía circular, son: diseñar para minimizar el desperdicio, mantener productos y materiales en uso, regenerar los sistemas naturales; esto nos trae las siguientes ventajas: mejorar el capital y proteger el medio (Naturaleza), hacer mejor gestión de los ciclos técnicos y biológicos, minimizar el impacto de los residuos en la naturaleza (AMV, 2018).

El autor de este articulo considera que la transformación digital que comenzó en la cuarta revolución industrial debe iniciar como un cambio de cultura y, sobre todo, en un cambio de actitud mental. Un buen inicio es hacer una alineación de nuestra organización con la propuesta de la economía circular, para lo cual debemos crear, en nuestras organizaciones, un proceso o área, o Centro de Excelencia (CoE) donde se puedan repensar nuestros productos y servicios como servicios digitales puros. Creo que no hemos terminado la cuarta y ya estamos en la quinta revolución industrial.

Las tecnologías disruptivas son herramientas muy poderosas, pero no deben ser la piedra angular, pues el hecho de invertir en herramientas no garantiza el éxito de la transformación digital; primero deben revisarse las estrategias para alinear la

inversión. Un libro interesante de David Rogers, titulado *The Digital Transformation Playbook: Rethink Your Business for the Digital Age,* propone que debemos reevaluar nuestro actual negocio, revisando las estrategias sobre cinco aspectos importantes del negocio: "Los Clientes, La Competencia, Los Datos, La Innovación y el Valor" (Rogers, 2016).

La quinta revolución industrial nos vuelve a invitar a que los robots en software nos asistan y que sean ellos los que hagan las tareas repetitivas para que los seres humanos tengamos tiempo de ser innovadores, para que nos dediquemos a resolver problemas impredecibles, para que comprendamos las emociones de nuestra humanidad y para que, mediante el pensamiento crítico, podamos complementarnos con los demás para visualizar una sociedad más humanitaria, más incluyente, más equilibrada, más segura para con la información y la vida, y sobre todo más compasiva con los demás.

Seguridad informática hace 10 años

En los últimos 10 años hemos visto la aplicación de la economía lineal en la seguridad de la información. Como, por ejemplo, hemos visto evolucionar la seguridad informática hacia la ciberseguridad, y hoy encontramos que las organizaciones, en general, entienden que existe un concepto más alto llamado "seguridad de la información", que contiene a la ciberseguridad; es decir, contempla la seguridad informática cuando interactúa mediante Internet para intercambiar información.

Además, hemos estado monitoreando y poniendo controles sobre la información en uso, información en reposo e información en movimiento. En controles, hemos visto pasar el firewall de perímetro hacia el firewall personal, ahora moviéndose el firewall con el usuario debido a los dispositivos móviles, IoT y servicios en la nube.

El antivirus basado en firmas estáticas (hash) evolucionó hacia el antimalware basado en heurística y ahora en analítica y comportamiento anómalo de patrones. Las redes sociales ahora son canales de comunicación críticos para entender los comportamientos de consumo y las necesidades de los clientes, pero suponen riesgos de seguridad en la información.

Adicional a estos cambios, el factor humano se ha transformado en un componente de los nuevos mapas de riesgos en línea usados en ciberseguridad para determinar un estado temporal de la ciberseguridad. La protección de fuga de información o DLP (*Data Leak Prevention*) basada en el apagado y encendido de puertos evolucionó hacia el DLP basado en analítica y tendencia de patrones sobre el comportamiento del usuario. Hemos visto pasar la gestión de los

riesgos conocidos hacia los riesgos emergentes y ahora es evidente la gestión integrada de los riesgos a nivel corporativo.

En los últimos 10 años, también hemos visto que finalmente los países establecieron leyes para la protección de los datos personales por parte de las organizaciones. En Colombia, por ejemplo, existe la Ley 1581 de 2012 y para proteger los datos reservados de las organizaciones se expidieron los Decretos 1377 de 2013, Decreto 886 de 2014 y el Decreto 1759 de 2016.

El cumplimiento de normas como la ISO 27001, ISO 31000, ISO 22301 e ISO 27032, para citar algunas, se han convertido en un estándar a seguir por la mayoría de las organizaciones, por lo menos para gestionar los riesgos conocidos. La norma ISO 27001:2013 propone dos controles importantes para proteger la información: Clasificación de la información en el control A.8.2.1 y el Etiquetado de la Información en el control A.8.2.2. También propone clasificar la información en por lo menos cuatro categorías: información pública, información privada o de uso interno, información secreta" e información personal.

La medición de comportamientos observables en seguridad de la información mediante indicadores y métricas como las denominadas PKI (indicadores de riegos de rendimiento) y KRI (indicadores de riesgos de seguridad), entre otros, son el lenguaje comúnmente utilizado en los procesos de cumplimiento, riesgos, ciberseguridad y seguridad de la información.

Asistentes digitales: breve prospectiva para 2030

Veremos innovación al entrelazar diferentes áreas del conocimiento para evitar ataques dirigidos que buscan denegación de servicios críticos a la sociedad debido a la aparición de nuevas enfermedades sin vacunas que atacarán a poblaciones específicas a nivel mundial, es muy probable que aparezcan los servicios de hacking biológico, es decir hacking a nivel genético.

Ataques a tecnologías fuertemente implementadas en servicios como el RPA, la Inteligencia Artificial y el Blockchain, entre otros, debido a la naturaleza inherente de la vulnerabilidad en esos servicios, así como a la ausencia de análisis de riesgos emergentes de ciberseguridad y seguridad de la información.

Los atacantes utilizarán Robótica, Analítica e Inteligencia Artificial para predecir comportamientos y preparar los ataques e intrusiones a los servicios de la quinta revolución industrial.

Entonces, debemos estar a la vanguardia y adelantarnos al cambio, diseñando procesos altamente robotizables y resilientes; estaremos un paso adelante y preparados para asumir el reto que plantea una economía circular, de servicios co-

mo producto final, de respuesta ágil como factor común, y de escalabilidad y agilidad de los productos y procesos para atender rápidamente las nuevas y cambiantes necesidades del mercado.

Conclusiones

1. Las situaciones imprevistas como el COVID-19 nos retan y nos presionan a innovar, a experimentar cruzando elementos de diferentes áreas del conocimiento. Estos eventos inciertos nos presionan a crear en medio de la desesperanza, pues al estar en medio de las dos revoluciones industriales más notables de la historia de la humanidad, es una clara invitación a transformarnos digitalmente, siendo el momento de reinventarnos en todo nivel.

2. Debemos hacer que los robots de software nos asistan y que sean ellos los que hagan las tareas repetitivas para que nosotros seamos innovadores, para que nos dediquemos a resolver problemas impredecibles, para que comprendamos las emociones de nuestra humanidad y que, mediante el pensamiento crítico, podamos complementarnos con los otros y visualizar una sociedad más humanitaria, más incluyente, más equilibrada, más segura y, sobre todo, más compasiva con los demás.

3. Hasta la cuarta revolución industrial, la raza humana muestra señales de una enfermedad mental similar a la esquizofrenia: muestra de ello es el consumo y producción desenfrenados; queremos crecer y producir sin tener la mínima responsabilidad sobre el impacto de nuestros residuos en la naturaleza.

4. En la quinta revolución industrial, tendremos en nuestras oficinas los ciberhumanos, compañeros de trabajo humanos con partes cibernéticas

5. Las empresas multinacionales tendrán un proceso o área de economía circular para repensar los actuales productos y servicios como servicios puros que la sociedad pagará por su utilización o consumo.

6. Los productos de seguridad de la información y ciberseguridad también se venderán como servicios puros.

7. La Inteligencia Artificial se aplicará a los diferentes ámbitos de la vida real y, en particular, a la seguridad de la información, pero también será vulnerada.

Referencias

Jorge Otálvaro, VP Bancolombia. (12 de julio 2019) *Automation Anywhere*. Recuperado el 22 de mayo de 2020 https://www.youtube.com/watch?v=DI4MtfW8Z8U.

Ministerio de Ambiente y Desarrollo Sostenible - Minambiente. (2108, Noviembre) *Colombia le apuesta a las 9R en*

economía circular. Recuperado el 23 de mayo de 2020 de https://www.minambiente.gov.co/index.php/noticias/4225-colombia-le-apuesta-a-las-9r-en-economia-circular.

Ateneo Mercantil de Valencia - AMV. (18 de junio 2018) *Economía Circular - Ciclo Cuarta Revolución Industrial*. Recuperado el 24 de mayo de 2020 de https://www.youtube.com/watch?v=VxeYSUTtF6g.

Rogers, D. (2016). *The Digital Transformation PlayBook, Rethink your business for the digital age*, Columbia Business School.

Deloitte (2020). *Tendencias de tecnología 2020*. Deloitte Insights. De: https://www2.deloitte.com/content/dam/Deloitte/co/Documents/technology/(7)%20Horizonte%20siguiente.pdf

***Armando E. Carvajal R**.: Es Ingeniero de Sistemas de la Universidad INCCA de Colombia, cuenta con una especialización en "Construcción de Software para redes" de la Universidad de los Andes y una maestría en "Seguridad informática" de la Universidad Oberta de Cataluña (España). Se desempeña como Arquitecto de soluciones en la empresa Globaltek, organización especializada en Seguridad de la Información y Robótica de procesos. Ha sido conferencista en las jornadas internacionales de Seguridad Informática ACIS Colombia desde 2007; tiene experiencia dictando especializaciones en seguridad informática. Autor del libro "Fundamentos en la Inseguridad de la Información, Tomo I: Un enfoque basado en la práctica", Editorial Académica Española.*

Reflexiones de un experto en plena pandemia

DOI: 10.29236/sistemas.n155a3

No existe un análisis del riesgo para determinar las soluciones básicas que requieren los usuarios y que el Estado debería proporcionarles, advierte José Eduardo Campos.

Sara Gallardo M.

Especialista en ciberseguridad con más de 25 años de experiencia, los primeros en Brasil de donde es oriundo, consultor y director de proyectos innovadores de desarrollo empresarial en los Estados Unidos, con enfoque en mercados emergentes en América Latina, Sudeste Asiático e India, José Eduardo Campos atendió las inquietudes que apuntan a la evolución y futuro del sector.

A su recorrido profesional como investigador le aporta certificaciones profesionales que contemplan seguridad, privacidad y auditoría de sistemas (CISSP, CISA, CISM, CPP, CIPT). En la actualidad es director de educación en el capítulo de ISACA *Puget Sound* y profesor adjunto de ciberseguridad, en Central Washington University.

Autor de varios libros y conferencista, declara ser amante activo de las medias maratones, fiel lector de libros sobre ficción científica, seguidor de Agatha Christie y atrapado en el realismo mágico de Gabriel

García Márquez en “Cien años de soledad”.

Desde su residencia en Seattle atendió la entrevista.

Revista Sistemas: *Diez años atrás los dispositivos móviles, la computación en la nube y la regulación, ya eran considerados como asuntos clave en el marco de seguridad y ciberseguridad. Hoy ¿es posible afirmar que se han abordado de una forma responsable, considerando la nueva sociedad, la madurez de los usuarios, los desarrollos tecnológicos y su aplicación? ¿Cuál es su análisis de la evolución al respecto?*

José Eduardo Campos: Hemos mejorado en la privacidad básica suministrada por los proveedores de la nube, porque las pequeñas y medianas compañías (pymes), no tienen ni los recursos ni el conocimiento para acceder a la información y tampoco los usuarios comunes, mientras los criminales sí aumentan su actividad delictiva todos los días. En tal sentido, no existe un análisis del riesgo para determinar las soluciones básicas que requieren y que el Estado debería proporcionarles.

RS: *¿Cuál es el papel que deberían desempeñar los proveedores de tecnología, relacionado con el análisis de riesgo y las soluciones básicas que el Estado debería suministrar, según usted lo manifiesta?*

JEC: Apenas en el año 2000 los proveedores de tecnología empezaron a invertir para suministrar

orientación a quienes no tenían el conocimiento. Pero, en ese entonces el contexto era otro, las personas no accedían a la tecnología como lo estamos viendo hoy en el encierro obligado producto del coronavirus. Por esa razón, lo que se pueda decir al respecto está muy lejos de ese momento, la situación es muy distinta. Las comunicaciones hoy son en línea a través de diferentes aplicaciones y los usuarios se sienten a gusto. En esa medida, los riesgos son muchos, deben existir las garantías para una conexión segura y el Estado debe proteger a los usuarios que se han multiplicado.

RS: *Pues si el Estado antes no lo hizo, hoy mucho menos podrá actuar en esa dirección, considerando las prioridades que le impone la pandemia.*

JEC: Colombia siempre estuvo adelantada con relación a otros países de Latinoamérica y las escuelas de computación son muy buenas. Estuve varias veces en el país y conocí a muchos profesionales de seguridad y vi cómo trabajaban de la mano con el Gobierno sobre privacidad y seguridad para diferentes tipos de usuarios, desde grandes corporaciones, hasta la persona natural. Es muy necesaria la cooperación entre Gobierno y sociedad civil, en la medida en que la tecnología siempre va mucho más adelante en sus desarrollos que las políticas públicas. Entre los desarrollos y la salida de una ley hay tres o cuatro años. De tal manera que la empresa privada debe trabajar de la mano con el Estado para entender lo que viene.

Por ejemplo, el tema que hoy tiene mucha fuerza y es centro de debate entre proveedores y usuarios es la inteligencia artificial. Tiene un montón de beneficios, pero también entra en juego la ética y, por supuesto, la regulación. De manera que la sociedad civil debe estar informada sobre el futuro inmediato de los avances tecnológicos.

Además, debe existir un equilibrio entre los desarrollos tecnológicos y quienes van a hacer uso de ellos, para disponer de información y alertas tempranas. El punto de discusión que se presenta hoy en la academia o en las asociaciones de profesionales de la seguridad es cómo prepararnos ante la avalancha de la tecnología en esta cuarta revolución industrial, para poder atender a toda clase de usuarios, desarrollando en ellos competencias que les permitan estar preparados para asumir los adelantos que vienen en camino. Algunos estudios indican que, si bien existen el pensamiento crítico, el análisis del riesgo y otras habilidades, en el inmediato futuro se tratará de capacidades humanas enfocadas en la diferencia entre la máquina y el ser humano.

En otras palabras, se requiere educación y como ésta toma su tiempo, es inminente empezar ya a diseñar mecanismos de inversión con tales

objetivos. Muchas veces la emoción elimina la posibilidad de pensar en la gente.

RS: *Sobre la educación y las políticas públicas las decisiones al respecto están en manos de los Gobiernos de turno, algunos cuestionados con pruebas en varios países, por el uso que le dan a la tecnología para influenciar a los ciudadanos y ganar adeptos, hecho que lesiona la confianza de la sociedad civil. ¿Usted qué piensa?*

JEC: Siempre creo que los cambios sociales ocurren desde la sociedad al Gobierno, en todos los países, aunque menos en los que la dirigencia es fuerte, como Rusia, China y otros. Y las acciones al respecto fluctúan entre la rapidez y la lentitud. De ahí que sea tan importante la injerencia de las asociaciones de profesionales, a través del trabajo mancomunado con los gobiernos, especialmente de los grupos dedicados a la investigación tecnológica, para fijar las políticas públicas alrededor de una educación continuada a largo plazo. El país que puede ilustrar este aspecto puede ser Francia, con sus acuerdos participativos en tales decisiones.

RS: *¿Qué opina sobre la seguridad y la ciberseguridad como un servicio?*

JEC: Con la computación en la nube ya se ve la oferta de antivirus básicos, pero también el uso de la inteligencia artificial para detección y prevención de ataques, como lo hacen Google, Apple, Microsoft, entre otras corporaciones, con acceso a tanta información sobre código malicioso para fijar patrones de prevención. Los usuarios, llámense pymes, grandes corporaciones o los gobiernos, ven solamente la foto, mientras los proveedores de servicios ven la película completa.

Y, a medida que la inteligencia artificial sea más accequible y económica será una herramienta muy importante. De la misma manera, el machine learning es el futuro para diseñar rutas; dependiendo de las decisiones surgen las acciones hacia lo más crítico.

RS: *La responsabilidad de los desarrolladores de la tecnología y, por supuesto, de los profesionales en seguridad y ciberseguridad, se triplica, cuando los ciudadanos están de por medio y suceden hechos como los descritos en el documental "Nada es privado", sobre el uso de los datos con fines políticos. ¿La ética ha inspirado su ejercicio profesional?*

JEC: Esos riesgos ocurren en todos los países con el poder de procesamiento en la nube y la rápida comunicación, situaciones para las que los usuarios no están preparados. Y en esta pandemia con los nuevos usuarios estamos sumando riesgos. En políticas públicas relacionadas con la privacidad, muchos gobiernos están pensando en adaptar las mismas estrategias de China, Singapur, Corea del Sur, que contemplan el uso de disposi-

tivos móviles por parte de los ciudadanos para hacer el *tracing*, que es seguir a los ciudadanos a través de sus móviles para identificar los que fueron infectados y si siguen la cuarentena ordenada por el Gobierno.

Ahí se presenta un balance entre los beneficios y la privacidad de los ciudadanos, de ahí que sea posible disponer de la información de las personas relacionada con lo que hacen, sus gustos y demás.

RS: *Claro, no somos invisibles, no gozamos del derecho que nos asiste a la invisibilidad.*
JEC: Exactamente, de manera que es necesario hacer un balance y ahí surge el análisis de riesgos sobre lo que se quiere. Muchas personas tienen la opción de no usar una tecnología pensando precisamente en su derecho a la privacidad. En la regulación europea GDPR (General Data Protection Regulation o Regulación General de Protección de Datos), la privacidad es clave, porque los ciudadanos no quieren que los invadan. En los Estados Unidos, la sociedad está un poco más estructurada para cuestionar al Gobierno al respecto.

RS: *En ese último aspecto difiero de su apreciación, toda vez que en muchas oportunidades la tecnología ha sido utilizada con objetivos específicos para mostrar una realidad que no es y los ciudadanos incultos la asumen como verdad.*
JEC: Me devuelvo al punto inicial, depende de la formación del ciudadano, del pensamiento crítico. Si no es consciente de los riesgos que enfrenta al compartir su información sin control, todo puede pasar.

En este país, bancos muy importantes con una buena infraestructura de seguridad han sido atacados y su reputación ha sido alterada, porque alguien dejó una puerta abierta en la nube. De ahí la importancia de generar conciencia sobre una forma segura de comunicación y una disciplina en el manejo de la información personal.

RS: *Contemplando el antes y el después producto de la pandemia que afrontamos, la investigación en la academia, en los desarrolladores de tecnología y en los gremios de profesionales dedicados a la seguridad y la ciberseguridad cambiará de rumbo. ¿Cuál es su visión?*
JEC: Soy optimista. De aquí en adelante la investigación académica se acelerará. Desde mi experiencia como parte del *board* de una escuela de posgrado en la Universidad de Washington, vemos que las organizaciones están conscientes de la crisis y todo el mundo puede parar. Hay hambre de conocimiento, de manera que será muy importante la investigación y, por supuesto, de inversión. Muy especialmente en temas como la privacidad. Los profesionales de esta rama de la tecnología podemos influenciar a las organizaciones, los Gobiernos y demás sobre los riesgos a los que están enfrentados y sobre cómo aprovechar desarrollos

como la inteligencia artificial, el *blockchain*, entre otros.

***RS:** Y, sobre la ética que debe cobijar esos desarrollos, ¿qué opina?*
JEC: La ética jugará un papel preponderante. En Francia se acaba de anunciar un esfuerzo en esa dirección a través de la inteligencia artificial. Ocupará las primeras filas en los debates para proteger la información y los derechos de los ciudadanos, en el marco del uso seguro de la tecnología. Esta crisis disparará tales temas.

***RS:** ¿Cuáles serán los principios que regirán en términos de seguridad y ciberseguridad?*
JEC: Entender que, si no lideramos el uso de la tecnología y no logramos el enganche con los usuarios, alguien más va a tomar nuestros puestos en la organización. Será imposible manejar los volúmenes de información si no tenemos aplicaciones que cubran todo. Debemos cambiar comportamientos, ser más humildes y estar atentos a los desarrollos tecnológicos que vendrán en los próximos cinco años.

***RS:** ¿En qué no se pueden equivocar los responsables de la función de seguridad/ciberseguridad para ser exitosa en los próximos 10 años?*
JEC: Con relación a los usuarios, no podemos olvidarnos que la ciberseguridad es para empoderar e influenciar las decisiones en las organizaciones y las entidades de cualquier naturaleza. Tenemos que despertar credibilidad en los directivos de las compañías sobre la importancia de nuestro trabajo y el alcance que tiene en el negocio.

***RS:** Desde su perspectiva, ¿cuál será la transformación más significativa en seguridad y ciberseguridad que producirá esta pandemia?*
La habilidad de estar preparados, la capacidad y la competencia de escuchar a los clientes y responder rápido. Zoom es el mejor ejemplo, las fallas de seguridad que tuvo la aplicación, fueron solucionadas, la compañía reconoció los problemas, trabajó sobre ellos y suministró una rápida respuesta para no afectar su imagen ni alejar a los usuarios.

***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.; es editora de esta revista.*

XX Encuesta Nacional de Seguridad Informática

DOI: 10.29236/sistemas.n155a4

Lecciones aprendidas y prospectiva de futuro

Resumen
La encuesta de seguridad informática, capítulo Colombia, soportada por la Asociación Colombiana de Ingeniero de Sistemas (ACIS) y realizada a través de Internet, entre los meses de febrero y abril de 2020, contó con la participación de 214 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, HackLabGirls LATAM, y WOMCY, entidades y comunidades que colaboraron en la distribución y 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 al respecto 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.

Particularmente hay que resaltar que se presentó una investigación con un análisis longitudinal de los primeros 18 años de la encuesta, en un evento internacional denominado, "Estudio de la evolución de la Seguridad de la Información en Colombia: 2000 – 2018" (Cano & Almanza, 2020), donde se presenta un análisis de la historia de la seguridad y ciberseguridad en Colombia, que hace una lectura documentada del pasado, y que, sumado a este documento, permite realizar un poco de prospectiva de cómo podría llegar a ser 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 43 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 permiten a las organizaciones definir una postura clara en materia de protección.

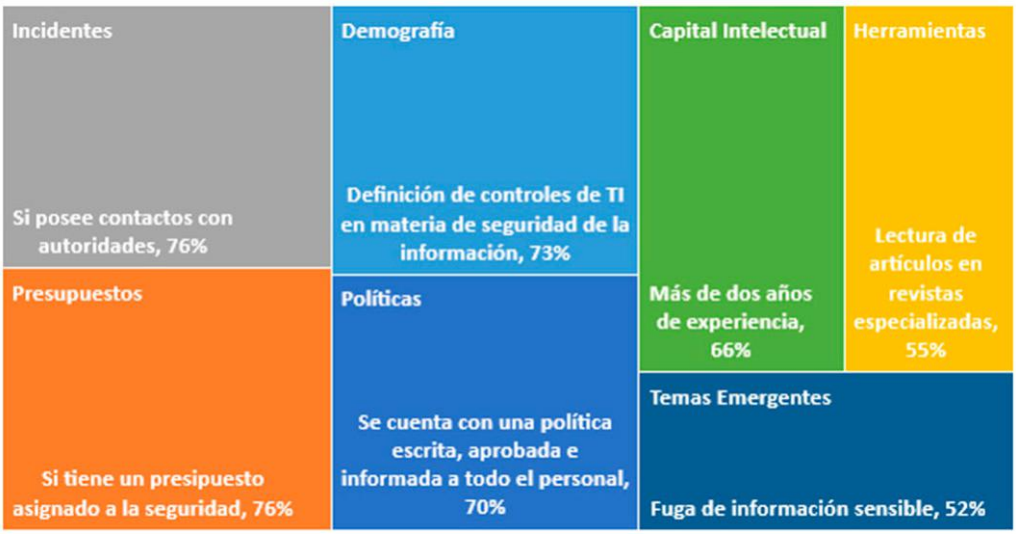
Políticas de seguridad: Busca conocer el estado de las políticas de seguridad, la práctica de la gestión de riesgos y su integración en el contexto organizacional.

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.

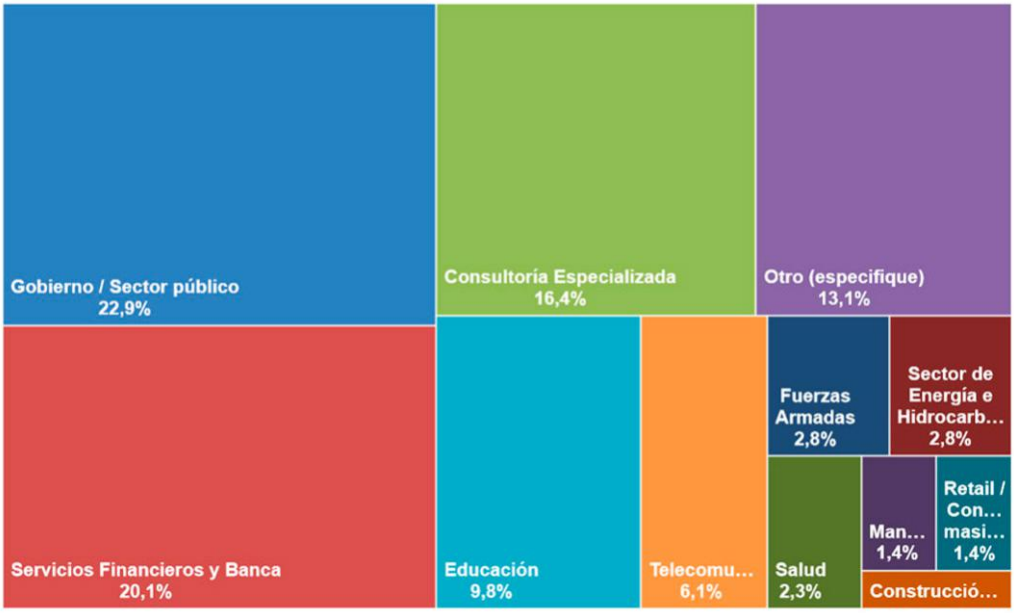
Temas emergentes: En esta sección se analizan varios aspectos, entre ellos: la percepción del futuro en materia de ciberseguridad; la vinculación de los directivos de la organización en la ciberseguridad empresarial, además de la responsabilidad y el papel del líder de seguridad en el desarrollo de la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

Hallazgos principales

De la información recogida en este estudio se muestran en la siguiente gráfica los aspectos clasificados como importantes por todos los encuestados y reunidos en un grupo denominado top de Hallazgos de las dimensiones de la encuesta.



Gráfica 1: Top de Hallazgos



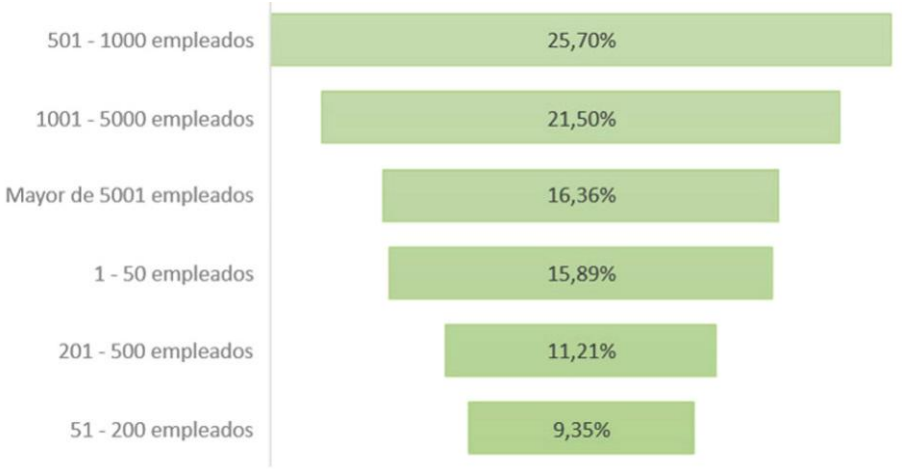
Gráfica 2: Sectores participantes

En la gráfica 1 se encuentran los datos más relevantes de la encuesta. El 74% de los encuestados reconoce no usar una estrategia de e-discovery o descubrimiento electrónico para soportar los litigios o reclamaciones legales, un 70% cuenta con un presupuesto para la seguridad de la información en las empresas de la realidad de Colombia. Un 70% indica que la tarea fundamental del responsable de seguridad en Colombia es definir los controles de TI en materia de seguridad de la información. El 70% de los encuestados respondió que en sus empresas se hacen los ejercicios de evaluaciones de riesgos en donde se incluye a la seguridad de la información. Las áreas de seguridad en Colombia están conformadas entre 1 y 5 personas como lo resalta el 64% de los participantes. Las amenazas persistentes avanzadas son la preocupación más importante según el 50% de los encuestados en Colombia. Por último, el 44% manifiesta que la forma como se mantienen actualizados de las fallas de seguridad en Colombia es a través de la lectura de revistas especializadas en materia de seguridad.

Demografía

Sectores participantes

La gráfica 2 refleja la participación de 13 sectores de la economía colombiana. Los tres segmentos con mayor participación de la encuesta para este año fueron Gobierno, Sector Financiero y la Consultoría Especializada.

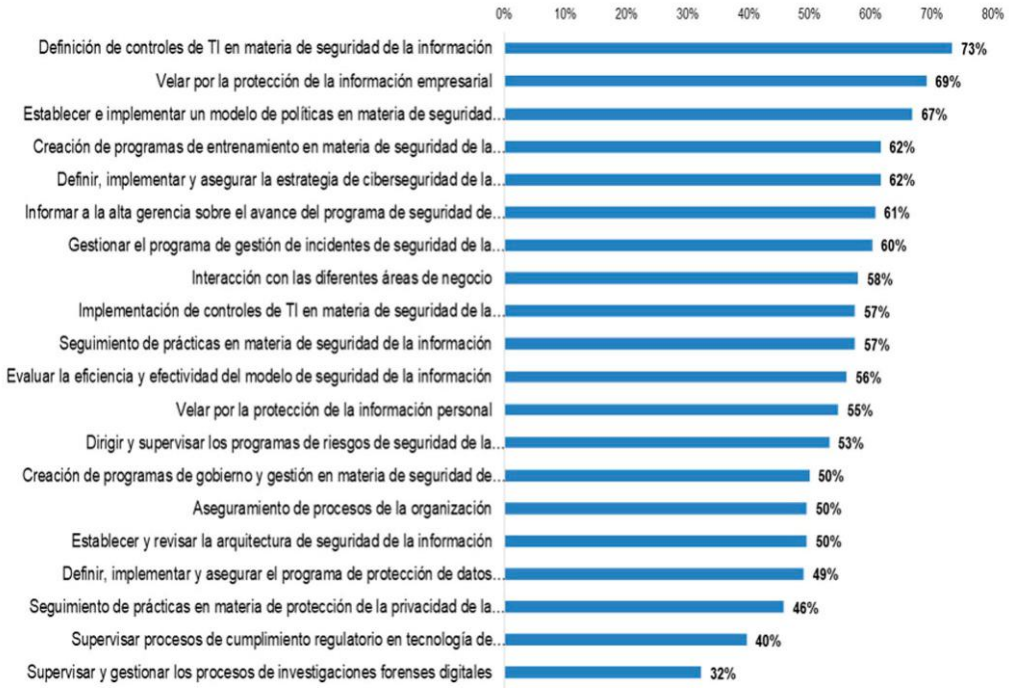


Gráfica 3: Tamaño de las empresas participantes.

La Grafica 3 muestra el tamaño de las empresas en Colombia, de acuerdo con el número de empleados. El 25% de las empresas están entre los 501 a 1000 empleados, el segundo lugar son las empresas pequeñas (21,50%) que cuentan con 1001 a 5000 empleados.

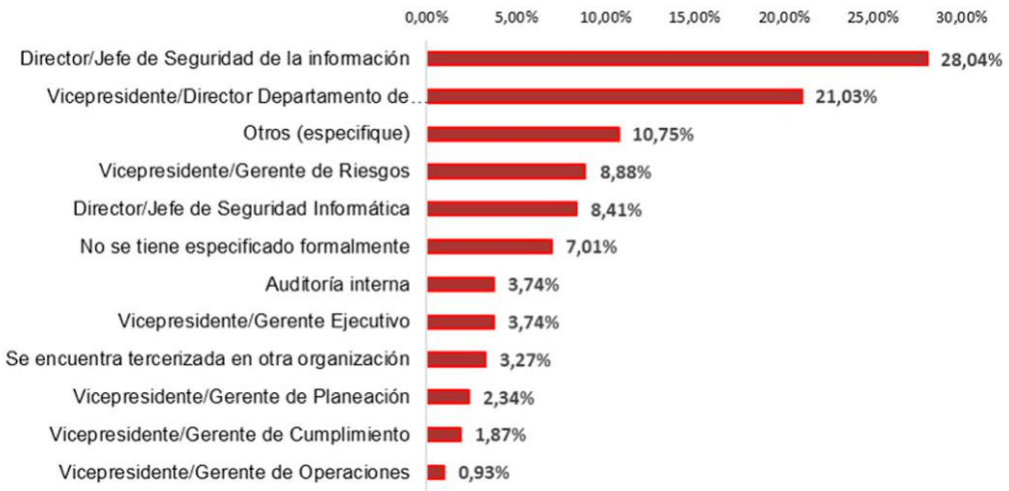
La gráfica 4 muestra los cargos de los encuestados, entre los que se cuentan. Profesionales de las áreas de TI, Oficiales de Seguridad, Auditores Internos, Directores de Seguridad de la Información. Así mismo, figuran otras clasificaciones para los profesionales de seguridad digital en el país, tales como analistas y profesionales de planta de seguridad, docentes de cátedra y planta de las áreas de seguridad como los más relevantes.

Gráfica 4: Cargos de los encuestados



Gráfica 5: Funciones del responsable de seguridad

En la gráfica 5 se observan las tareas realizadas por los profesionales de seguridad dentro de las organizaciones. El porcentaje más alto está representado por la definición de controles de TI en materia de seguridad de la información, velar por la protección de la información em-



Gráfica 6: Dependencia del área de seguridad

presarial y establecer e implementar un modelo de políticas en materia de seguridad de la información como las principales.

La gráfica 6 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 del Director/Jefe de Seguridad Informática y como tercer lugar la Vicepresidencia/Director Departamento de Tecnologías de la Información.

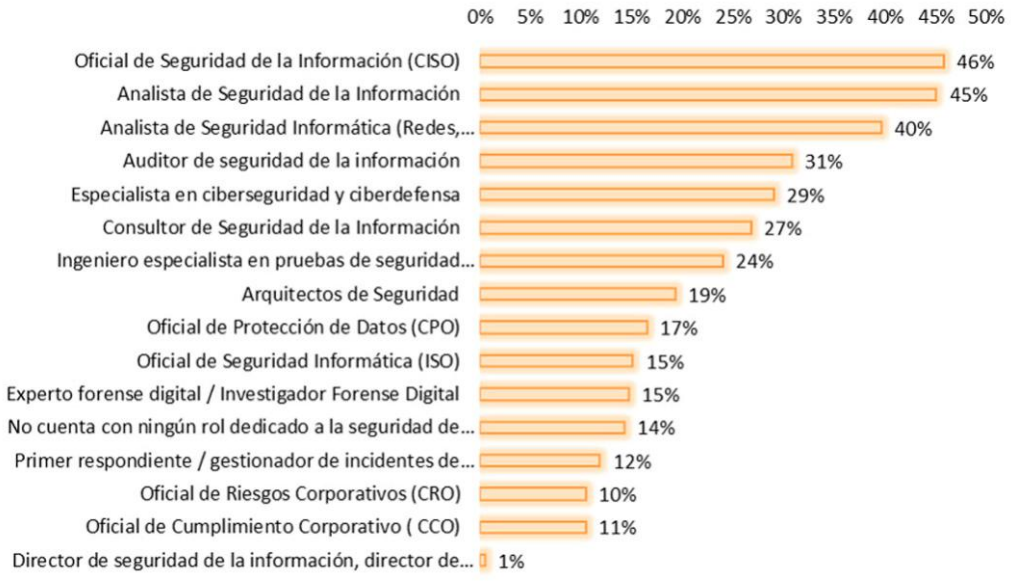
En la gráfica 7 se observan los roles dentro de una organización, en materia de seguridad digital. En Colombia figuran los analistas de seguridad (información e informática); le sigue el cargo denominado CISO, al que se suman los ingenieros de pruebas, entre los principales roles.

Consideraciones de los datos

Según El *Data Breach Report* (2020) de la Firma Verizon, manifiesta que el tamaño de las empresas sí importa. En su metodología define que las empresas de menos de 1000 empleados son consideradas (SMB) (*Small, Medium Business*) y por encima de 1000 empleados son consideradas grandes empresas.

En ambos casos el informe indica que es muy probable que las pequeñas empresas no estén generando los esfuerzos suficientes para identificar a sus adversarios.

Al contrastar con los resultados de este año, encontramos que en Co-



Gráfica 7: Roles de Seguridad

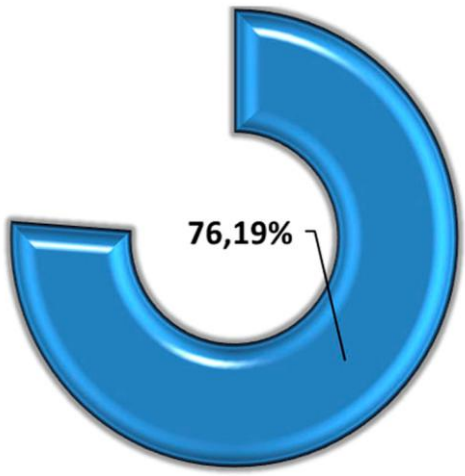
lombia hay una distribución de empresas interesante: participan empresas grandes de más de 1000 empleados con un 38% y 62% son de menos de mil. Por tanto se puede advertir que existe una alta probabilidad de que las empresas colombianas puedan ser víctimas de un ataque informático.

De acuerdo con CISCO (CISCOc, 2019), una de las funciones primarias de los responsables de seguridad de las empresas está relacionada en primer lugar con la atención a los riesgos, colocar límites a los temas de presupuestos, colaboración con las áreas de la organización, educar y crear cultura, saber cómo se presentan los beneficios de las inversiones en seguridad y ser estratégico en la venta de la implementación de soluciones técnicas de seguridad.

En otro informe Kaspersky (2019), se resalta que la identificación de riesgos y amenazas son tareas claves de los profesionales de seguridad. En otro reporte (Marlin Hack, 2020), se afirma que solo el 50% del tiempo del profesional de seguridad se dedica a su función principal que es la de proteger y defender el negocio, así mismo, el 40% manifiesta que su función principal es la de buscar soluciones tecnológicas de protección. Al revisar la tendencia nacional para 2020 ésta dista completamente. La función principal está relacionada con la implementación de soluciones de TI.

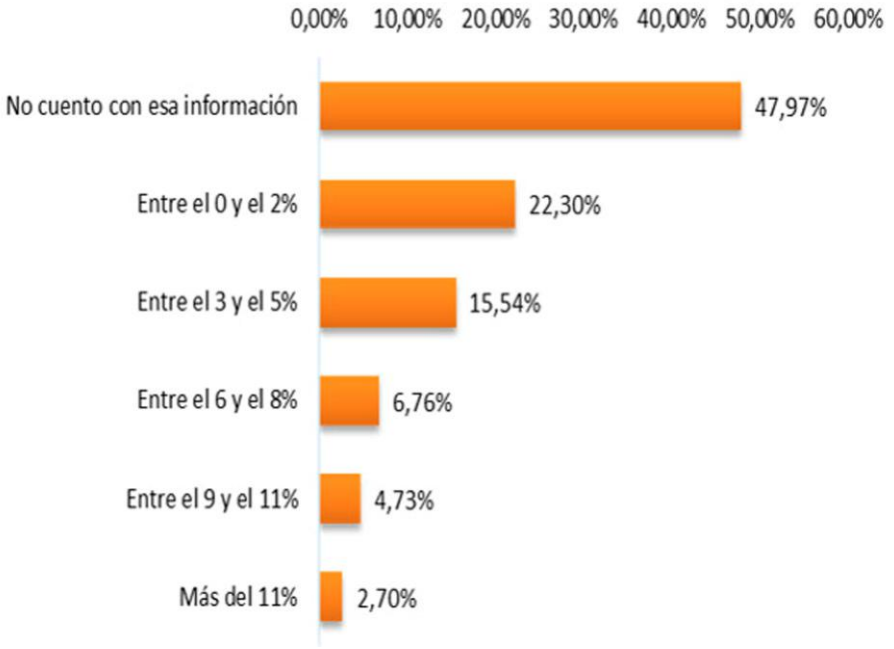
Presupuestos

La realidad colombiana es muy interesante, en materia de presupuestos en el mundo de la seguridad digital. El 76% de los participantes manifiesta que sí tiene presupuesto asignado a la seguridad digital de sus organizaciones, lo cual se refleja en la gráfica 8.

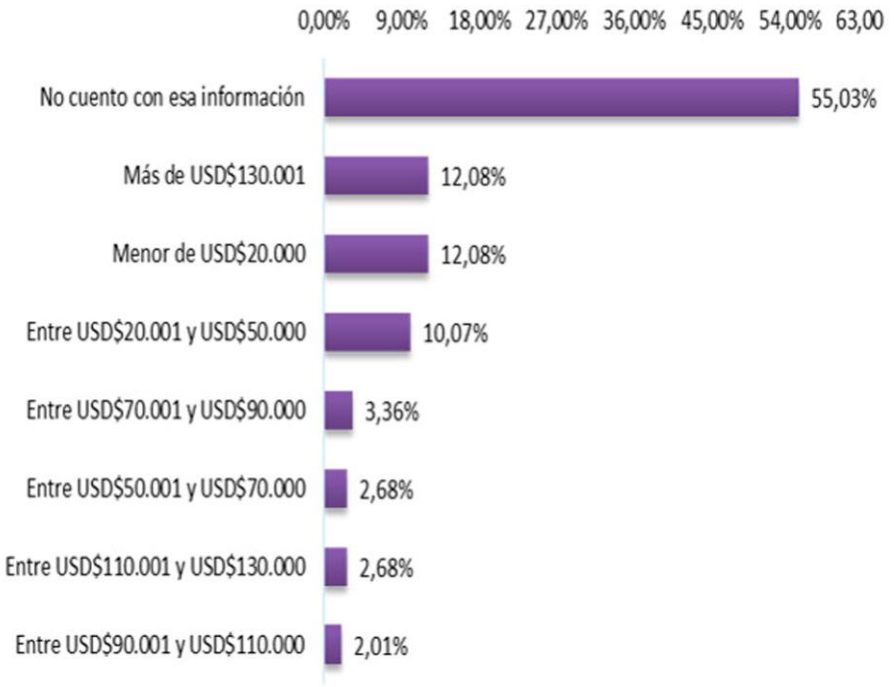


Gráfica 8: Presupuesto de Seguridad

La gráfica 9 muestra el monto del presupuesto en relación con el presupuesto global; cerca del 47% de los encuestados lo conoce, mientras que el 54% dice no conocer o no tener la información. La gráfica 10 refleja la distribución de los presupuestos en dólares. Para este año cerca del 45% tiene un monto asignado para la seguridad, el 55% restante manifiesta no conocer dicha información. Esto se puede explicar, toda vez que los cargos de mayor participación están com-



Gráfica 9: Porcentaje del presupuesto Global



Gráfica 10: Presupuesto de Seguridad

Gráfica 11: Inversión de Seguridad

puestos por auditores y los profesionales de las áreas de tecnologías que pueden no conocer los detalles internos de las áreas de seguridad. La otra razón para que se dé esta realidad es que muchos de los roles de las organizaciones están asociados con los analistas de seguridad, quienes suelen no conocer estos detalles. La gráfica 11 muestra cómo se están realizando las inversiones en materia de seguridad, siendo la inversión en tecnologías de seguridad la de mayor interés. Las otras temáticas que se resaltan son la contratación de servicios de consultoría, la renovación del licenciamiento de algunas tecnologías en materia de seguridad digital, la capacitación del área de seguridad, monitoreo y gestión con terceros. La gráfica 12 representa la distribución de los sectores principales y sus franjas de inversión, por los rubros estudiados donde se hacen las inversiones. En ella se pueden ver las tendencias de cada uno de los sectores, ejemplo el sector de fuerzas armadas que sus inversiones están por encima de los US$130.000 en la renovación de licencias y/o hardware, como su valor más representativo, en las otras consideraciones mueven sus presupuestos sobre la misma franja de los US$130.000.

Consideraciones de los datos

Los reportes internacionales ratifican la tendencia de Colombia de ver aumentos pequeños en los presupuestos de seguridad en las organizaciones, de todos los tama-

ños y sectores. Sin embargo, al revisar el informe Ponemon-IBM (2020) y de ISACA (2020), muestran que los presupuestos año a año se incrementan, confirmando la tendencia de Colombia.

En el informe de Ponemon-IBM (2020) solo el 33% considera que se tienen los presupuestos adecuados en materia de ciberseguridad para garantizar la ciberresiliencia, se pasó en promedio de $US3,4 millones a $US3,6 millones. Si bien influyen las realidades económicas y digitales en donde se realizan los estudios lo que sí vale resaltar son las tendencias de tener unos pre-

	Adquisición e implementación de tecnología de seguridad informática	Capacitación/Actualización del personal de seguridad de la información	Contratación de servicios de asesoría/consultoría	Renovación de licenciamiento y mantenimiento de hardware y software	Servicios de monitoreo y gestión de seguridad con terceros
Consultoría Especializada					
Entre USD$20.001 y USD$50.000	2,13%	5,41%	0,00%	4,88%	0,00%
Entre USD$90.001 y USD$110.000	0,00%	0,00%	2,70%	0,00%	3,23%
Menor de USD$20.000	6,38%	13,51%	8,11%	4,88%	6,45%
Educación					
Entre USD$20.001 y USD$50.000	2,13%	0,00%	0,00%	2,44%	0,00%
Entre USD$50.001 y USD$70.000	2,13%	0,00%	2,70%	2,44%	0,00%
Menor de USD$20.000	2,13%	2,70%	0,00%	2,44%	0,00%
Fuerzas Armadas					
Más de USD$130.001	4,26%	2,70%	0,00%	4,88%	0,00%
Gobierno / Sector público					
Entre USD$110.001 y USD$130.000	4,26%	2,70%	2,70%	4,88%	9,68%
Entre USD$20.001 y USD$50.000	6,38%	2,70%	8,11%	4,88%	3,23%
Entre USD$50.001 y USD$70.000	6,38%	2,70%	5,41%	7,32%	0,00%
Entre USD$70.001 y USD$90.000	2,13%	2,70%	2,70%	0,00%	3,23%
Entre USD$90.001 y USD$110.000	2,13%	2,70%	2,70%	2,44%	3,23%
Más de USD$130.001	6,38%	2,70%	5,41%	4,88%	6,45%
Menor de USD$20.000	2,13%	2,70%	0,00%	2,44%	3,23%
Otro (especifique)					
Entre USD$20.001 y USD$50.000	0,00%	8,11%	5,41%	2,44%	3,23%
Entre USD$70.001 y USD$90.000	0,00%	0,00%	2,70%	0,00%	0,00%
Más de USD$130.001	6,38%	8,11%	8,11%	9,76%	6,45%
Menor de USD$20.000	2,13%	8,11%	2,70%	4,88%	3,23%
Sector de Energía e Hidrocarburos					
Más de USD$130.001	8,51%	5,41%	5,41%	4,88%	9,68%
Servicios Financieros y Banca					
Entre USD$20.001 y USD$50.000	4,26%	5,41%	5,41%	2,44%	6,45%
Entre USD$70.001 y USD$90.000	4,26%	2,70%	2,70%	4,88%	6,45%
Entre USD$90.001 y USD$110.000	2,13%	2,70%	2,70%	2,44%	3,23%
Más de USD$130.001	10,64%	8,11%	8,11%	7,32%	9,68%
Menor de USD$20.000	10,64%	2,70%	10,81%	9,76%	12,90%
Telecomunicaciones					
Entre USD$110.001 y USD$130.000	0,00%	2,70%	2,70%	0,00%	0,00%
Entre USD$20.001 y USD$50.000	2,13%	2,70%	2,70%	2,44%	0,00%

Gráfica 12: Montos en dólares de las inversiones de seguridad. Sectores vs. inversiones

supuestos más dotados para el mundo de la ciberseguridad. En el caso Colombia lo que sí se puede ver es que la franja mayor a los $US130.000 dólares también tiene un porcentaje importante y con tendencia a seguir creciendo en los próximos años.

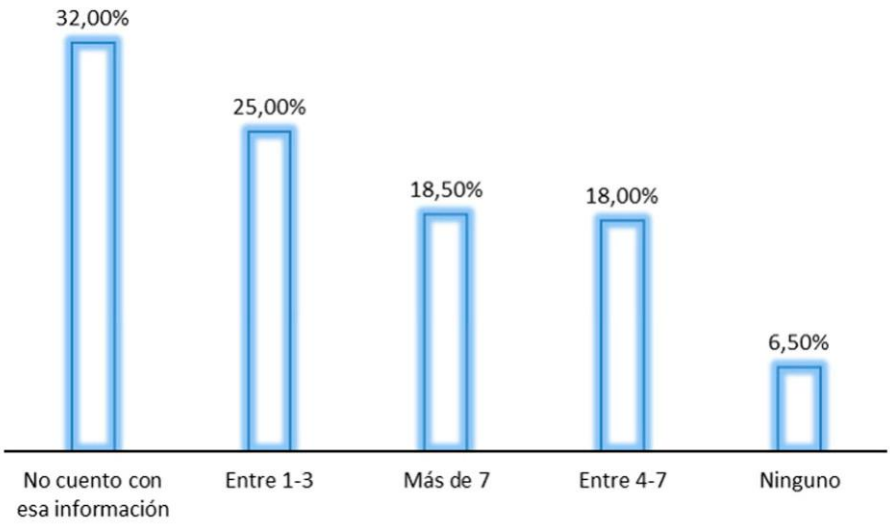
Incidentes

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.

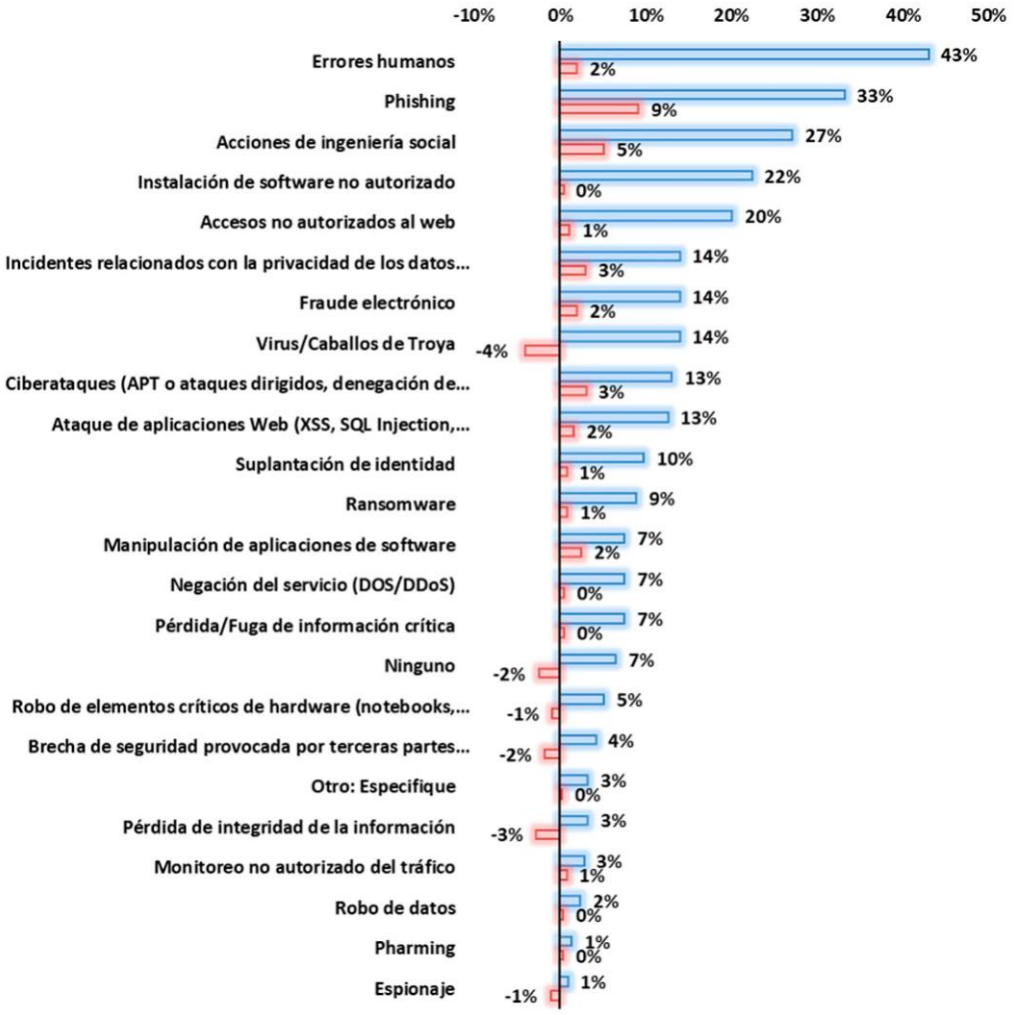
La gráfica 13 muestra la cantidad de incidentes que se presentan en Colombia, según los participantes. El 68% de ellos manifiesta haber tenido, por lo menos, un incidente de seguridad o ciberseguridad en sus organizaciones. El 32% de los participantes no tiene información al respecto, el 6,5% de los participantes resaltan que no tuvieron un incidente de seguridad.

La gráfica 14 relaciona los tipos de incidentes que se presentaron en las organizaciones, así como su variación con relación al año anterior. Tenemos en este sentido, errores humanos, phishing y ataques generales de ingeniería social como los principales de este año, y comparado con el año inmediatamente anterior es el phishing el que más varía con un 9%. Llama la atención que para 2020 decrece en un 2% aquellos que dicen no haber recibido ningún ataque durante el año.

La grafica 15 que es un valor nuevo medido este año, se evalúa cuanto en promedio le puede estar costando un incidente de seguridad a las



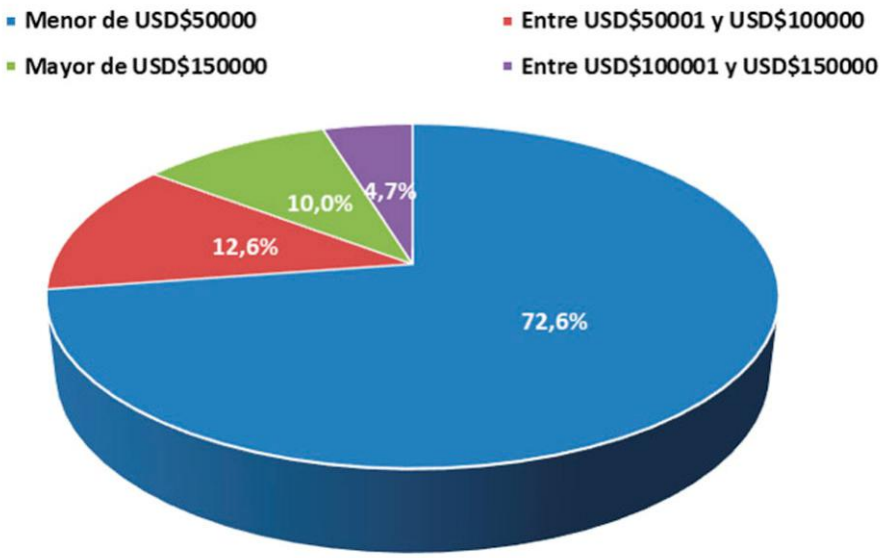
Gráfica 13: Cantidad de Incidentes. Incidentes



Gráfica 14: Tipos de Incidentes de Seguridad

empresas. Los datos muestran que cerca del 73% manifiestan que sus incidentes cuestan menos de $US 50.000, cerca del 13% entre $US 50.000 y $US 100.000, el 10% manifiesta que le cuesta más de $US 150.000 y el resto manifiesta que está en la franja de los $US 100.001 hasta los $US 150.000 dólares.

La gráfica 16, muestra ante quien se reportan los incidentes de seguridad. Los datos reflejan que, ante un incidente y su identificación, el 52% de los participantes lo notifican a los directivos de la organización, 37% a los equipos de atención de incidentes CSIRT (*Computer Security Incident Response Team*), 27% a las autoridades de orden



Gráfica 15: Costos de los Incidentes

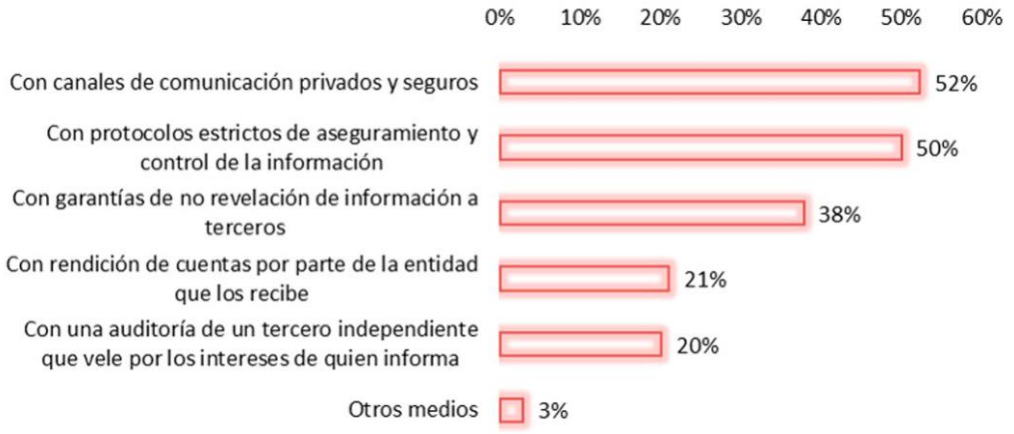
Gráfica 16: A quien se reportan los incidentes

Gráfica 17: Razones para no denunciar los incidentes

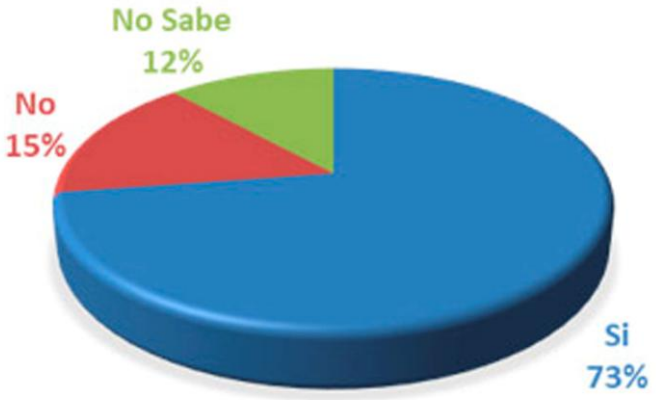
nacional como los datos más relevantes.

La gráfica 17, muestra las razones por las que no se denuncian los incidentes. En esta fundamentalmente la imagen 34%, la reputación 28%, y la responsabilidad legal 24% son las razones que aducen los encuestados de por qué no se denuncian los incidentes. La gráfica 18 muestra la forma los mecanismos que se podrían utilizar para compartir información o denunciar información. En primer lugar, está usar canales privados y cifrados como el mecanismo más idóneo 52% y protocolos de aseguramiento de la información bien definidos (50%), sería la forma en como estos intercambios de información se realizarían.

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



Gráfica 18: Mecanismos para denunciar/compartir

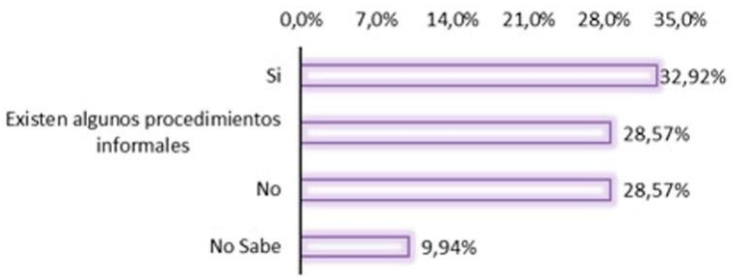


Gráfica 19: Consciencia de la Evidencia Digital

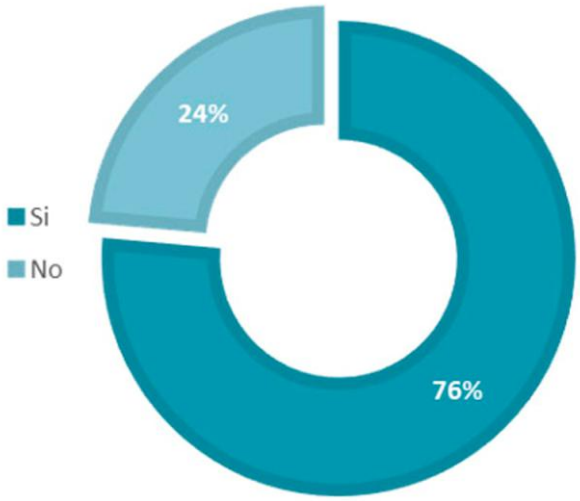
adecuado mejoramiento. La gráfica 19, resalta la importancia y consciencia en relación con el adecuado manejo de la evidencia digital. El 73% resalta que es consciente de ello. Sin embargo, la gráfica 20 muestra que solo el 33% posee un procedimiento para hacer la gestión de la evidencia digital y el 29% manifiesta informalidad en la práctica de los procedimientos adecuados. La gráfica 21 resalta que el 76% mantiene algún tipo de contacto con autoridades del orden local o regional.

Consideraciones de los datos

Los reportes internacionales como Ponemon-IBM (2020) y EY (2020), resalta que al menos el 57% de las organizaciones estudiadas han tenido un incidente de seguridad, que desemboca en una disrupción de la organización y/o algún proceso de TI, así mismo resalta que al menos 55% ha sufrido de brechas de seguridad donde se han comprometido al menos 1000 registros de datos, donde existe información sensible de clientes y confidencial.



Gráfica 20: Procedimiento de Gestión de Evidencia Digital



Gráfica 21: Contactos con autoridades locales/regionales

Accenture (2020), manifiesta que la respuesta de incidentes como proceso de la organización que 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 manifiesta 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.

No obstante, en el mismo estudio consideran que se deben hacer más esfuerzos para aquellos que todavía tienen dudas, como son los casos en nuestro país. En Colombia aún no se piensa del todo en ello y por tanto se evidencia que no se está cerca de esta práctica. El costo de los incidentes es otro de los factores claves, el estudio de Accenture (2020) muestra en sus datos que el promedio de costos totales de un ciberataque es de $US380.000 dólares por incidente.

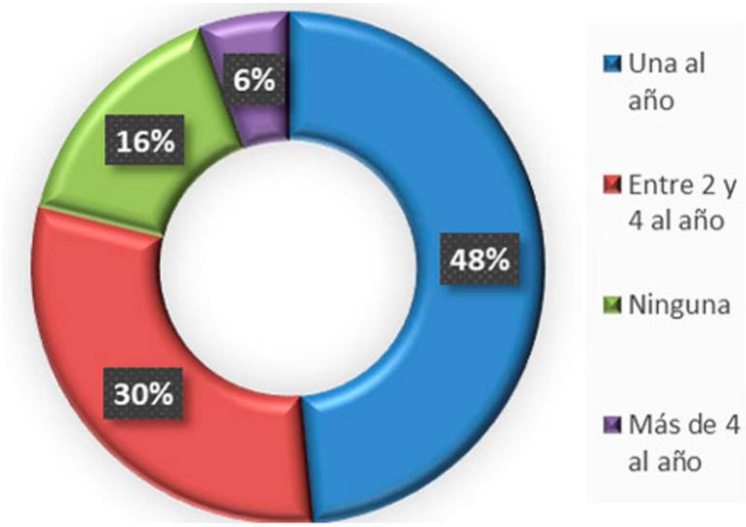
En Colombia y por primera vez este estudio analiza los costos estimados de un incidente de seguridad, cuyos resultados no confirman las lecturas internacionales. La mayoría de los encuestados (73%) relaciona que los costos de los incidentes están por debajo de los $US 50.000 dólares, y solo el 27% considera los costos por encima de ese valor. En este punto, pueden considerarse dos lecturas, una que no es están considerando todos los costos implicados a la hora de analizar un incidente siguiendo una metodología concreta, y otra, que

el plan de gestión de incidentes no es evaluado regularmente como lo sugiere el estudio de CISCO (2020), el cual manifiesta que en las empresas medianas y pequeñas está práctica no es desarrollada.

La práctica de la gestión de incidentes que en Colombia según los datos recabados se identifica como una práctica no desarrollada, resultado que ratifica los hallazgos del informe de EY (2018) que describe que las inversiones en seguridad están orientadas a fortalecer la gestión de incidentes toda vez que se considera una práctica que tiene muy poca madurez en las organizaciones cerca del 10% de los participantes hace esta consideración. El informe de Deloitte (2019), resalta que los mayores impactos de un incidente se expresan en términos perdidas de utilidades (21%), pérdida de confianza (21%), pérdida de reputación (16%), multas y sanciones (14%). Estos datos ratifican las preocupaciones de los responsables de seguridad en Colombia al no denunciar los incidentes, comoquiera que la pérdida de la reputación, de confianza, las sanciones y/o multas son las razones que se aducen para no hacerlos.

Herramientas

La gráfica 22 muestra el uso de las evaluaciones de seguridad como una de las prácticas más usadas. Un 84% de los participantes manifiesta hacer uso de esta práctica como instrumento clave para validar el estado de la seguridad digital de la organización. El 48% de los participantes usa esta práctica una vez al mes; el 30% entre dos y 4 veces al año; el 6% manifiesta usa más de 4 veces al año y el 16% dice no usarla.



Gráfica 22: Evaluaciones de Seguridad

Etiquetas de fila	Una al año	Entre 2 y 4 al año	Ninguna	Más de 4 al año
Gobierno / Sector público	20,50%	3,73%	1,86%	0,62%
Servicios Financieros y Banca	8,07%	9,94%	2,48%	2,48%
Consultoría Especializada	6,83%	6,21%	4,35%	0,00%
Otro (especifique)	5,59%	2,48%	0,62%	1,24%
Educación	4,35%	3,73%	0,62%	0,00%
Telecomunicaciones	0,62%	1,24%	3,11%	0,62%
Fuerzas Armadas	0,00%	1,24%	0,00%	0,62%
Sector de Energía e Hidrocarburos	1,24%	0,62%	0,00%	0,00%
Salud	0,62%	0,62%	0,62%	0,00%
Construcción / Ingeniería	0,62%	0,00%	0,62%	0,00%
Manufactura	0,00%	0,00%	1,24%	0,00%
Retail / Consumo masivo	0,00%	0,62%	0,00%	0,00%

Gráfica 23: Evaluaciones de Seguridad por Sectores.

La gráfica 23 indica como los sectores de están usando las evaluaciones de seguridad. El sector Gobierno, con un 21% usa al menos una prueba de seguridad al año, el sector Financiero cerca del 10% lo hace entre 2 y 4 veces al año, y la consultoría especializada con un 7% lo hace también una vez al año.

La gráfica 24, muestra cuáles son los mecanismos de seguridad comúnmente usados en las organizaciones. VPNs 52%, soluciones Antimalware 44% y WAF (*Web Application Firewalls*) 42% son los de mayor uso, sin embargo, comparado con el año inmediatamente anterior, las herramientas anti DDOS (16%), los WAF (16%), los firewall de nueva generación (14%), los SIEM (14%) (*Security Information Event Management*), los servicios de SOC (13%) y las VPNs (12%) son los que mayor crecimiento respecto del año anterior.

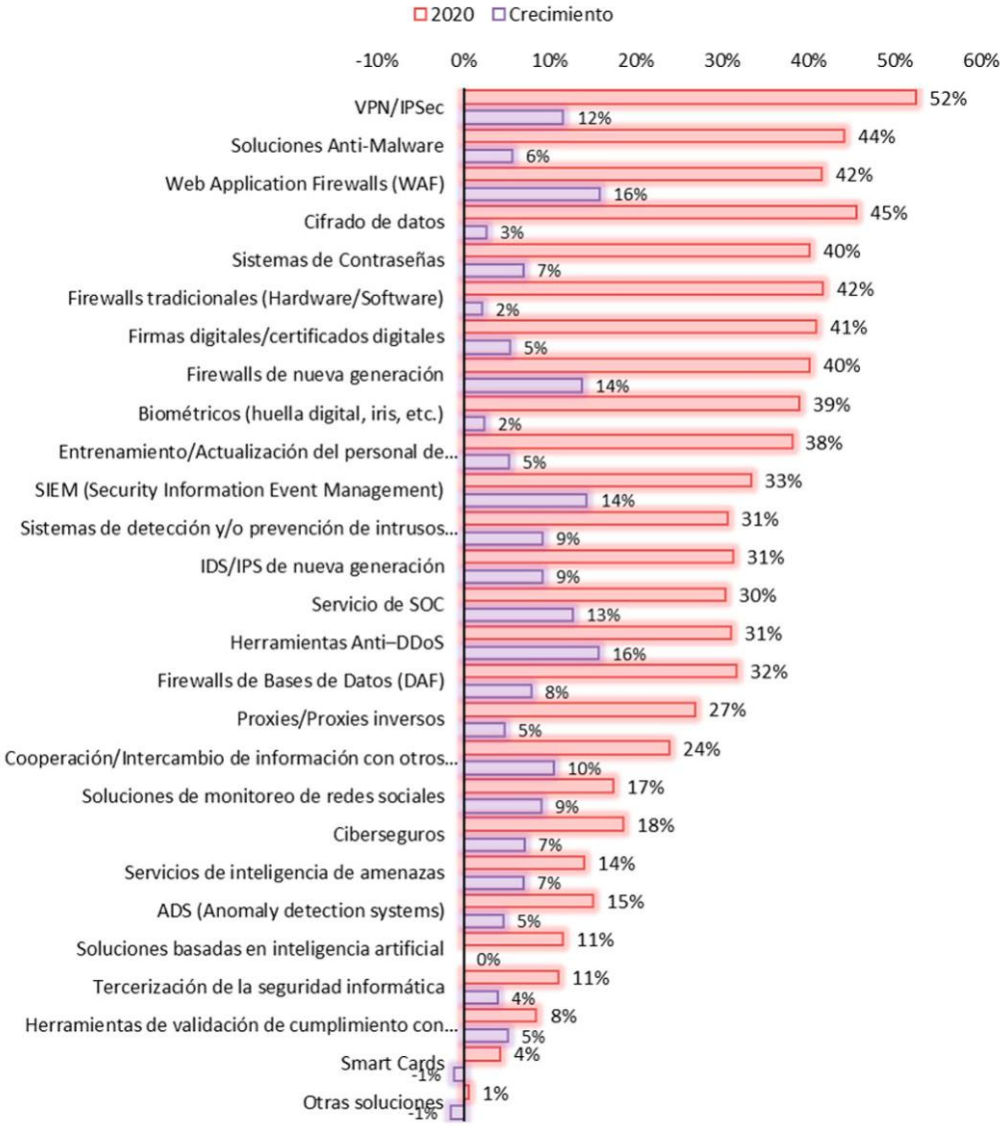
La gráfica 25 resalta las herramientas que más se usan para notificarse de las fallas de seguridad los profesionales. El 55% usa la lectura de sitios especializados como la práctica más común.

Consideraciones de los datos

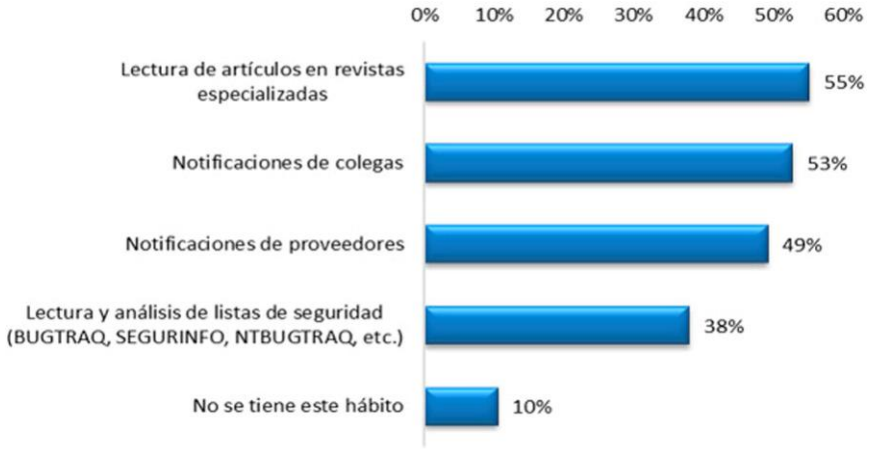
La tendencia en Colombia se mantiene al compararse con los años anteriores. Así mismo lo ratifican los datos internacionales, el informe de CISCO (2020) que sostiene que el 86% de las empresas pequeñas y medianas valoran la efectividad de sus programas de seguridad, comparado con el 90% de las empresas de gran tamaño. En el mismo informe sostiene que las empresas mejoran sus infraestructuras de seguridad, aun así, no son suficientes para atender los desafíos de protección y continuidad de la operación como les gustaría.

En el estudio de Ponemon-IBM (2020), se resalta que las empresas están tendiendo a usar herramientas de automatización para la seguridad, tales como herramientas de

inteligencia artificial y máquinas de aprendizaje, movimiento que también se ve como tendencia de Colombia. Así las cosas, en Colombia los datos muestran una evolución significativa de esta práctica y basado en ello se puede visualizar que despunta una tendencia en este 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 (2020), quien señala que las investigaciones de seguridad son las formas más utilizadas para descubrir brechas de seguridad.



Gráfica 24: Mecanismos de Seguridad usados



Gráfica 25: Mecanismos de notificación

Políticas

La gráfica 26 refleja el estado de las políticas de seguridad en las organizaciones colombianas; el 69,6% de los encuestados manifiestan que tienen formalizada sus políticas de seguridad, el 21,7% actualmente en desarrollo y solo el 8,7% dicen no tener políticas de seguridad de la información.

La gráfica 27, muestra lo que manifiestan los participantes al indagar por los obstáculos por los cuales no hay una postura adecuada de seguridad en sus empresas. La ausencia de una cultura, la falta de apoyo directivo y la falta de colaboración entre área son las tres razones principales que se mantiene como obstáculos de la seguridad.

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

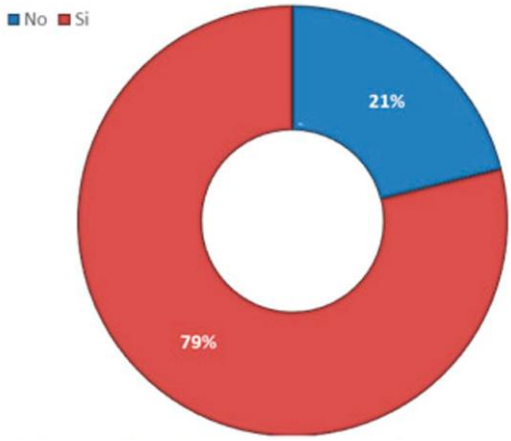
Gráfica: 26 Estado de las Políticas

Gráfica 27: Obstáculos de la Seguridad

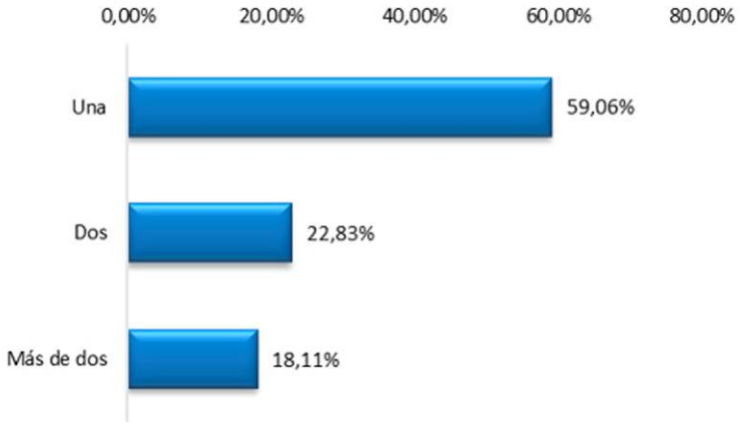
riesgos de seguridad digital y la incluyen en sus ejercicios globales de gestión de riesgos. En la gráfica 29, cerca del 60% realiza el ejercicio de evaluación de riesgos una vez al año, el 22,8% dos al año y el 18% más de dos al año.

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 no tener un proceso formal de gestión de riesgos (44%).

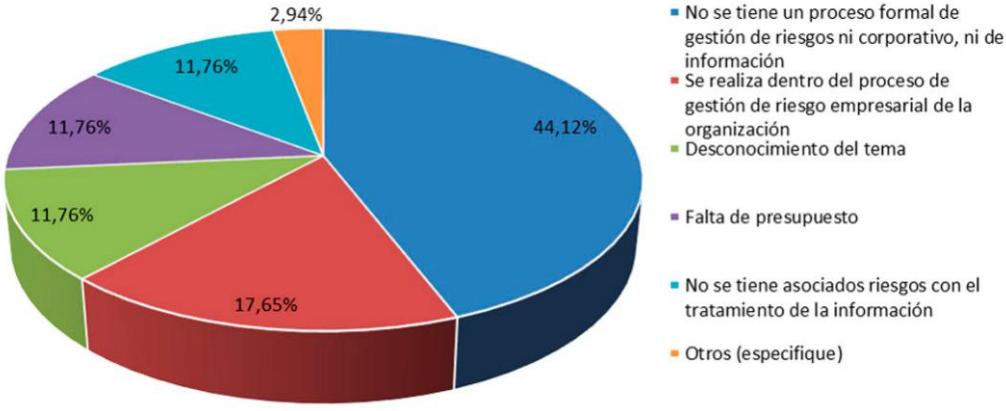
La Gráfica 31 muestra el tipo de metodologías usadas al realizar los ejercicios de gestión de riesgos de seguridad; la ISO 31000, con un 34%, es la metodología más usada. La Gráfica 32, muestra que los incidentes de seguridad son asociados a algún tipo de riesgos. El 51% de los incidentes de seguridad se aso-



Gráfica 28: Gestión de Riesgos de Seguridad

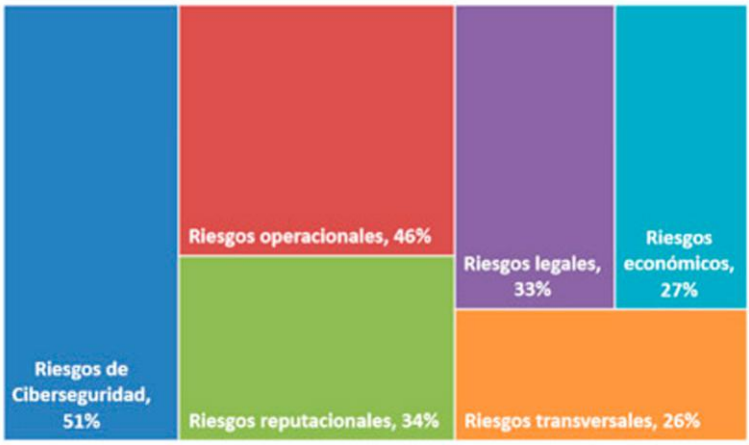


Gráfica 29: Cantidad de Gestión de Riesgos en Seguridad



Gráfica 30: Razones para no realizar la gestión de riesgos

Gráfica 31: Tipos de Metodología



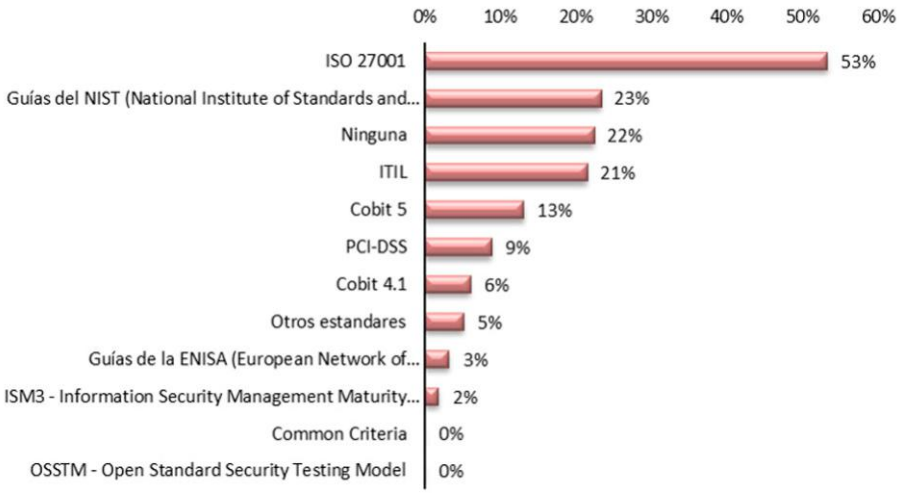
Gráfica 32: Tipos de Riesgos

cian a los riesgos de ciberseguridad; el 46% lo asocian a riesgos de operación, el 34% los relacionan con riesgos reputacionales.

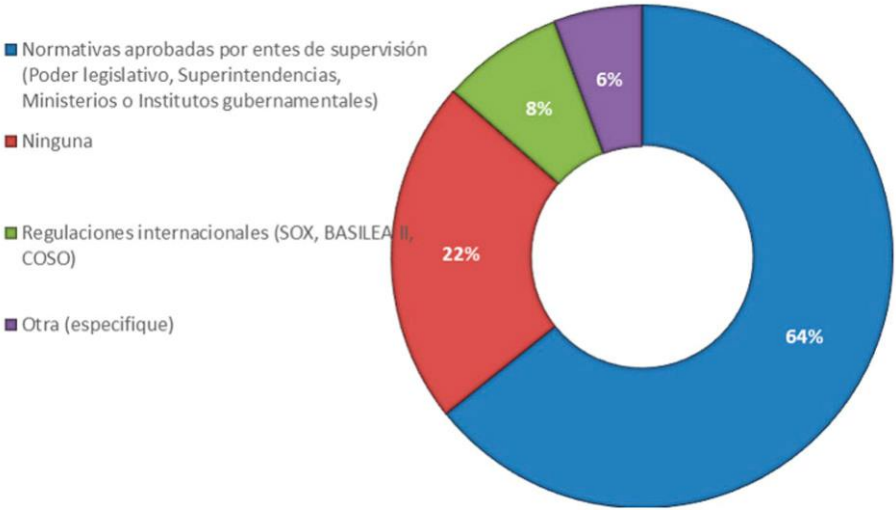
La gráfica 33 ilustra el uso de los distintos marcos de trabajo (*frameworks*) usados en las organizaciones colombianas: ISO/IEC 27001, NIST, Ninguna, ITIL y Cobit 5 son los más usados. La gráfica 34 refleja las regulaciones que las organizaciones deben asegurar. En el caso colombiano, el 64% de los participantes manifiesta que sí existen regulaciones que las organizaciones debe cumplir.

Consideraciones de los datos

Los riesgos de seguridad de la información y ciberseguridad en defi-



Gráfica 33: Marcos de trabajo usados

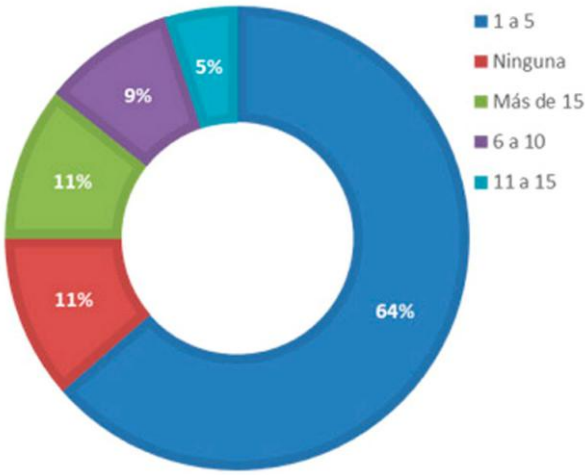


Gráfica 34: Regulaciones o normativas

nitiva son una realidad como lo es ratificado en el informe del Foro Económico Mundial (WEF, 2020), el cual manifiesta que la prioridad de estos tipos de ataques es alta en las organizaciones del mundo. Esto ratifica la tendencia de los resultados de Colombia que ven en la práctica de gestión de riesgos una herramienta vital para la construcción de capacidades frente a la atención de los ciberataques, por su parte el estudio de Pricewaterhouse Coopers (PwCb, 2020) resalta que una mayor digitalización en el contexto actual, habilita a la función de gestión de riesgos corporativos a tener relevancia, a responder y pronosticar mejor, y comprometer a las partes interesadas para actuar en un ecosistema digital, como el actual.

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 (CISCOb, 2020) que manifiesta que aquellas compañías que se adhieren a sus prácticas y políticas de seguridad tienen costos menores por brechas relacionadas con los datos en comparación con quienes no se adhieren, lo cual puede apoyar el comportamiento de Colombia en este sentido.

La tendencia internacional se orienta a que, cada vez más, existirán regulaciones más globales. La regulación GDPR (*General Data*



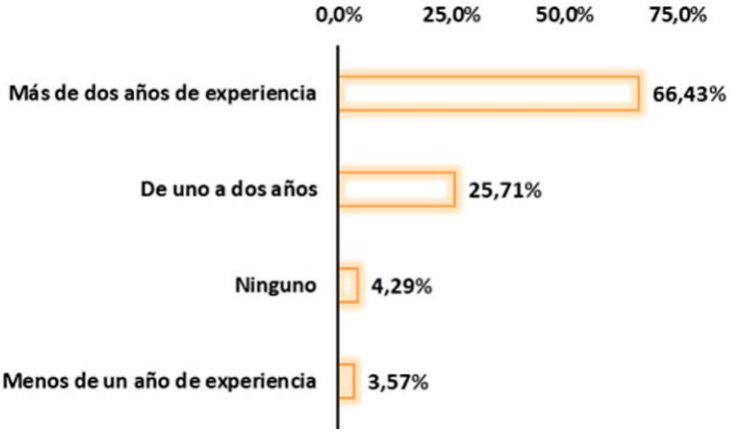
Gráfica 35: Recursos dedicados a la Seguridad

Protection Regulation) nace como una necesidad de la Comunidad Europea (EU), de gran impacto a nivel global.

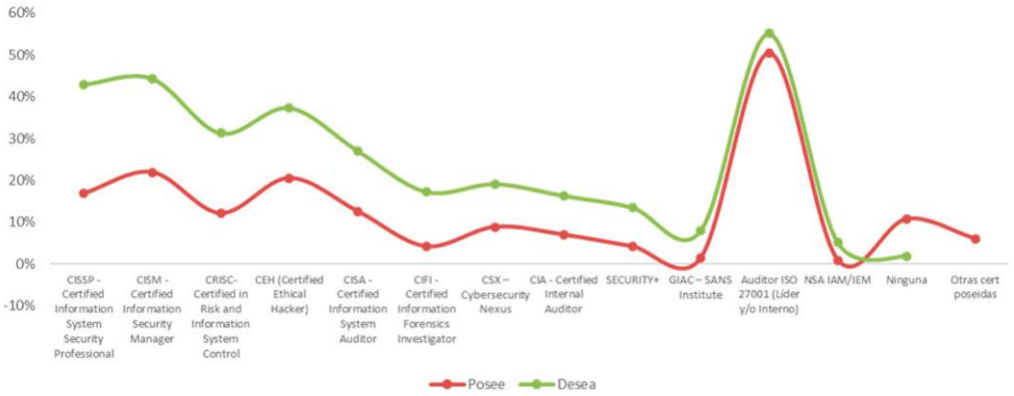
Capital intelectual

La gráfica 35 relaciona los recursos que son dedicados a la seguridad en las empresas, cerca del 89%, manifiesta tener recursos dedicados a la seguridad, la predominancia es de 1 a 5 con un 64%. La gráfica 36 resalta que el tiempo de experiencia promedio para que los profesionales de seguridad sean contratados en Colombia es superior a dos (2) años (66%).

La gráfica 37, representa la comparación de las certificaciones que los profesionales de seguridad poseen en la actualidad y que desean alcanzar en el tiempo. CISSP, CISM,



Gráfica 36: Experiencia del profesional



Gráfica 37: Certificaciones alcanzadas vs deseadas

CRISC y CEH, son las certificaciones que mayor variación tienen entre lo que se tiene actualmente y lo deseado en el futuro.

La gráfica 38, indaga sobre la forma en que la educación ha participado en la formación de los profesionales de seguridad. El 31% manifiesta y reconoce que se están ofreciendo programas académicos de grados y posgrado en temas de seguridad, el 29% que los niveles de investigación son escasos en Colombia.

Consideraciones de los datos

La experiencia del profesional de seguridad de las organizaciones en Colombia es clave, así como su formación. Las tendencias internacionales igual ratifican los resultados

Gráfica 38: Papel de la educación

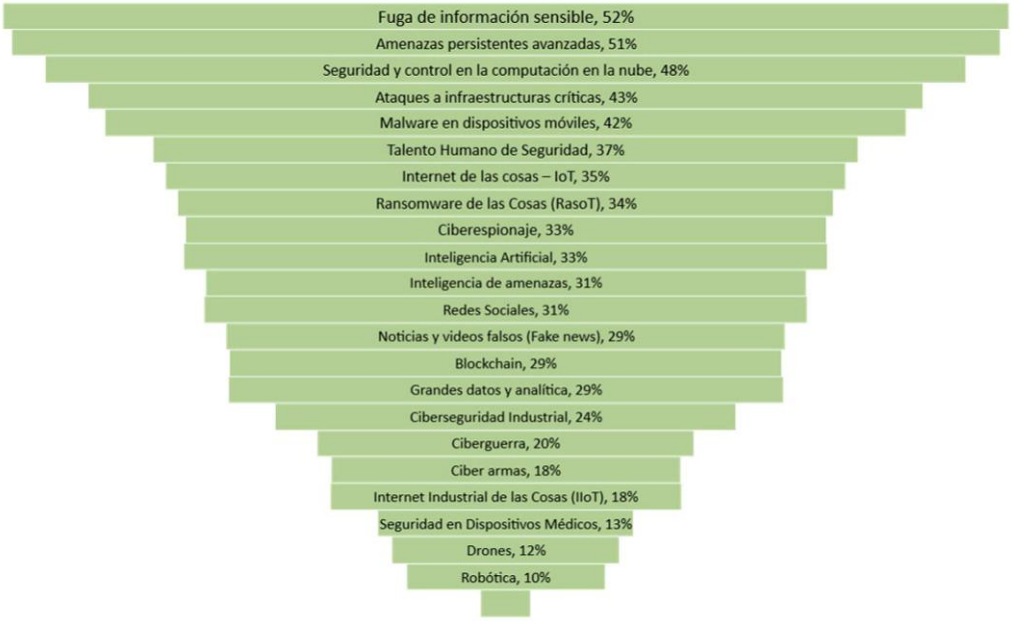
de Colombia. En su informe ISACA (2020), resalta que es clave la experiencia de los profesionales de seguridad. De igual forma, el reporte de MarlinHawk (2020), muestra que el promedio de los profesionales estudiados del mundo de la seguridad tiene 4 años en una posición en esta área. Desde el mismo 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 (2020) muestra en sus datos que solo el 47% considera algo importante un grado universitario para los profesionales de seguridad y le dan más importancia a la experiencia (73%). El informe también resalta que ni los grados universitarios, ni los cursos complementarios de formación, dan una garantía que demuestre conocimientos avanzados, o habilidades suficientes.

En relación con las certificaciones, CISSP, CISM, CRISK y CEH, muestran ser las certificaciones, que tienen más 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. Por otra parte, el estudio de ISC^2 (2019) ratifica que son los profesionales de seguridad quienes en su mayoría pagan por las certificaciones que obtienen.

Con relación a la educación y su importancia en la vida del profesional de la seguridad, los datos muestran en Colombia, que se reconocen los esfuerzos que hacen los programas por formar a los profesionales de seguridad. Datos que se pueden ver refrendados en el documento de ISC^2 (2019), donde se manifiesta que cerca del 87% de la población analizada tienen algún tipo de estudio formal y estudio avanzado académico con relación al mundo de la seguridad, reforzando así la tendencia de Colombia a tener programas formales de educación superior en ciberseguridad.

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 (2019). 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 como 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.



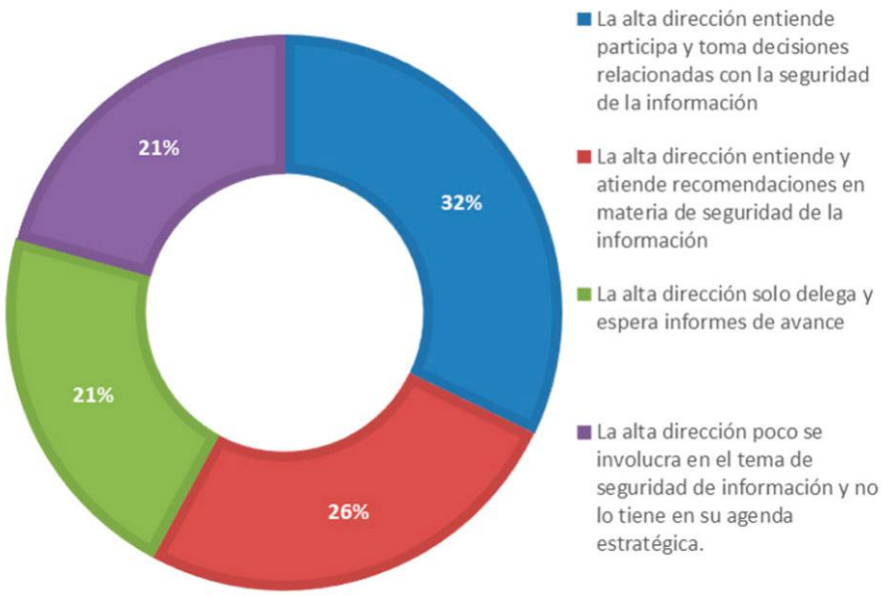
Gráfica 39: Temas emergentes

Temas emergentes

La gráfica 39 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.

La gráfica 40, relaciona la forma en como las juntas directivas, o comités ejecutivos se relacionan con la seguridad. El 51% están atendiendo y participando activamente, mientras que el 42% restante delega o poco se involucra en los temas de seguridad en Colombia.

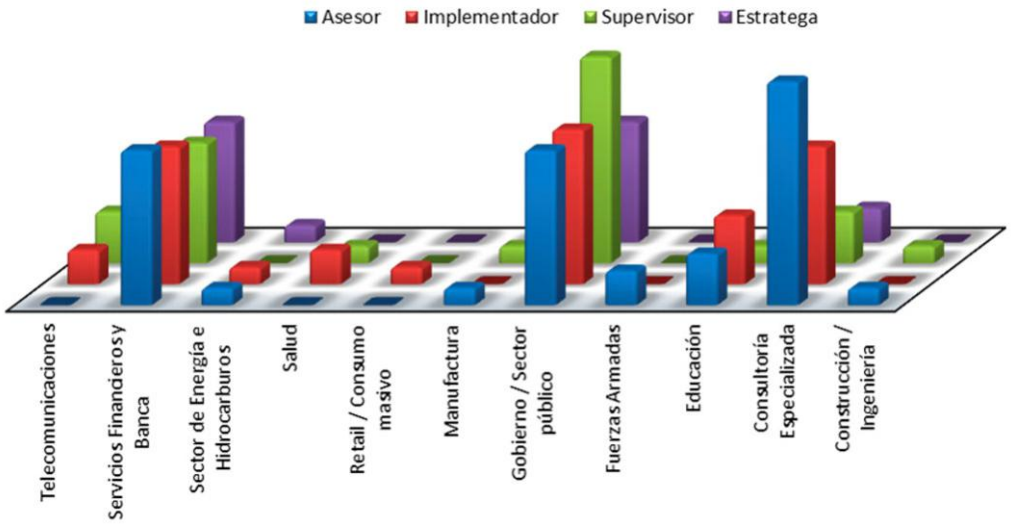
Las gráficas 41, 42 y 43 reflejan la forma como el CISO se ve, se desenvuelve y cómo puede evolucionar en el contexto de las organizaciones nacionales. La gráfica 40 muestra la forma como es visto el profesional de seguridad, en los diferentes sectores de la industria. En este año el 31% resalta que en Colombia es visto como un Asesor, luego como Implementador, Supervisor y en último lugar como Estratega. Interesante ver como en cada industria tienen una vista de su posición. Mientras el sector Financiero y la consultoría especializada esa es la vista que predomina (Asesor), con mucho más fuerza en el sector de consultoría, en el sector de Gobierno, lo ven con fuerza como un Supervisor, esto es, una persona que vela por la eficacia y eficiencia del programa de seguridad, su visión del control es la que rige



Gráfica 40: Involucramiento de los Directivos

como principio, vela por los riesgos, y el cumplimiento.

La gráfica 41 muestra la forma como el líder de seguridad entrega información a los grupos de interés, el 51% manifiesta que entrega información con relación a los riesgos en seguridad y ciberseguridad, el 43% manifiesta que entrega in-



Gráfica 41: Cómo ven al CISO

Gráfica 42: Entrega de información del profesional de seguridad

formación relacionada con los aspectos técnicos, el 40% indica que entrega información relacionada con la gestión, y así mismo, con las brechas de seguridad, y el 14% no entrega información a ningún grupo de interés.

La Gráfica 43 muestra las oportunidades de crecimiento y mejora en las que los profesionales de seguridad pueden trabajar, como parte del cierre de brechas existentes. En primer lugar, las capacidades de gestión son el primer espacio que reconocen como oportunidad para mejorar (52%), las capacidades de liderazgo en segundo lugar (46%), las capacidades técnicas y de experiencia en tercer lugar (44%), las

Gráfica 43: Camino de crecimiento de un profesional de seguridad

capacidades de pronóstico con un 36%, la formación académica y técnica un 33% como los aspectos de mejoras y oportunidades.

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 (2020), soportan las consideraciones locales, en el sentido de observar a las amenazas avanzadas y los desafíos de la nube como factores claves a tener en cuenta. 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. Por su parte ESET (2019), considera a la inteligencia artificial y las máquinas de aprendizaje un componente clave en su informe de tendencias, que también tiene cabida en los datos de la encuesta de Colombia.

En cuanto a los profesionales de seguridad se ratifica que las habilidades gerenciales, el liderazgo y la comunicación son piezas fundamentales de los nuevos líderes de seguridad, así lo manifiesta se ratifica en el reporte Fortinet (2019). 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. ISACA (2020) por su parte, resalta que las brechas más amplias que deben cerrar los profesionales son las “habilidades blandas”, con un 32%, seguido de sus habilidades técnicas con un 30%, que coincide con la realidad en Colombia. 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 (2020) donde resalta que el 50% de los CEO de su estudio global están preocupados por los temas relacionados con las ciberamenazas y el 33% de éstos lo ubica en top 5 de preocupaciones en la ejecución de la estrategia de seguridad. 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 éstos riesgos.

Reflexiones finales

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 una invitación para desarrollar nuevos, continuos y creativos esfuerzos en procura de proteger y crear valor como la confianza, confiabilidad y resiliencia en un mercado cada vez más competitivo y exigente.

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.

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.

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 indica 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. 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.

2. La posición del profesional de seguridad continúa su proceso de afianzamiento dentro de las organizaciones. Hoy vemos que el responsable de seguridad ha evolucionado un poco más en su formación técnica, aunque aún debe ser fortalecida como lo ratifican los datos. No obstante, ha ido creando capacidades en otras dimensiones que se convierten en claves para el desem-

peño de su función. 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.

3. 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. La educación definitivamente juega un papel vital, y de igual manera junto con los entes de certificación se deben trabajar de manera conjunta para ir cerrando las brechas que no solo en Colombia, sino en el mundo se tienen con respecto a los talentos de seguridad que se requieren en los ambientes organizacionales.

4. La realidad digital hace que todos a todos los sectores e industrias lleven su mirada al tema de ciberseguridad. Sectores como el sector 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.

5. Los riesgos como instrumento catalizador de un programa de seguridad se convierten en Colombia en una buena herramienta, para desarrollar el programa de ciberseguridad. Los Líderes de seguridad digital están considerando este instrumento como una valiosa oportunidad para elevar su interlocución con los niveles directivos y ejecutivos, y juntos poder tomar caminos acordes a la realidad digital de la empresa.

6. La confianza digital, se convierte 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.

7. 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 lla-

mado tanto a 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.

8. 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 permeen 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.

9. Las nuevas tecnologías como Cloud, IoT, IA, *machine learning* entre 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.

10. 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.

11. 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. El 2020 está marcado por la construcción de nuevos normales, basado en los eventos globales que vive el mundo, y por tanto no la ciberseguridad, no será la excepción. En este ejercicio, será necesario repensar lo ya conocido y concebido como verdades definidas para reescribir nuevas prácticas, y así, apoyar a las empresas para caminar por la constante de la incertidumbre, que define las pautas de los movimientos del ecosistema digital en el que se desenvuelven las organizaciones hoy.

Referencias

(ISC)2, (2019). (ISC)2 Cybersecurity Workforce Study, 2019. Recuperado de: https://cybersecurity.isaca.org/state-of-cybersecurity

Booz Allen Hamilton (2020). 2020 Cybersecurity Threat Trends Outlook. Recuperado de: https://content.fireeye.com/m-trends/rpt-m-trends-2020

CISCO (2020). Big Security in a Small Business World. Recuperado de: https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-smb-cybersecurity-series-may-2020.pdf

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. Recuperado de: https://www.researchgate.net/publication/339629757_Estudio_de_la_evolucion_de_la_Seguridad_de_la_Informacion_en_Colombia_2000_-_2018

CISCOb (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

CISCOc (2019). Anticipating the Unknowns. Recuperado de: http://ebooks.cisco.com/story/anticipating-unknowns

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

ENISA (2020). Cybersecurity Skills Development In The EU. Recuperado de: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union/at_download/fullReport

ESET (2019). Cybersecurity Trends 2020- Thechnology is getting smarter – Are We? . Recuperado de: https://www.welivesecurity.com/wp-content/uploads/2019/12/ESET_Cybersecurity_Trends_2020.pdf

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

Fireeye (2020). M-Trends 2020. Recuperado de: https://content.fireeye.com/m-trends/rpt-m-trends-2020

Fortinet (2019). The Ciso Ascends From Technologist To Strategic Business Enabler. Recuperado de:

https://hub.fortinet.com/hiring-guides/the-ciso-ascends-from-technologist-to-strategic-business-enabler

ISACA (2020). Global Update on Workforce Efforts and Resources. Recuperado de: https://cybersecurity.isaca.org/state-of-cybersecurity

Kaspersky (2019). What It Takes to Be a CISO: Success and Leadership in Corporate IT Security. Recuperado de: 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/wp-content/uploads/2020/02/Nominet_The-CISO-Stress-Report_2020_V10.pdf

Ponemon-IBM (2019). The Cyber Resilient Organization. Recuperado de: https://newsroom.ibm.com/2019-04-11-IBM-Study-More-Than-Half-of-Organizations-with-Cybersecurity-Incident-Response-Plans-Fail-to-Test-Them

PwC (2020). 23nd Annual Global CEO Survey. Recuperado de: https://www.pwc.com/gx/en/ceo-survey/2020/reports/pwc-23rd-global-ceo-survey.pdf

PwCb (2020). Being a Smarter risk taker through digital transformation. Recuperado de: https://www.pwc.com/us/en/services/risk-assurance/library/assets/pwc-2019-risk-study.pdf

Verizon (2020). Data Breach Investigation Report. Recuperado de: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

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

***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 Ingenieria de Sistemas | especialista en seguridad en redes y master 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.*

***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–.*

Diez años más tarde

DOI: 10.29236/sistemas.n155a5

Retos y amenazas a la seguridad y ciberseguridad en 2030.

Sara Gallardo M.

Despierta 2020 y la humanidad se enfrenta a un enemigo oculto que amenaza la vida, las relaciones interpersonales y la economía mundial, sin reparo alguno. Y mientras la pandemia ocasionada por el COVID- 19 aumenta y los científicos no cesan en su afán por crear o encontrar una vacuna contra el coronavirus, los expertos en seguridad y ciberseguridad están en alerta máxima.

Una situación imprevisible y no registrada en el marco del análisis de riesgos que tiene a los habitantes de este planeta sometidos al confinamiento obligatorio, decretado por los mandatarios de turno y haciendo uso de las tecnologías de información y las comunicaciones para mantenerse a flote, como nunca lo habían hecho.

Es así como en un abrir y cerrar de ojos la virtualidad se convirtió en única protagonista para mantener en ese escenario al mundo, en términos sociales, económicos y geopolíticos. A través de esos hilos invi-

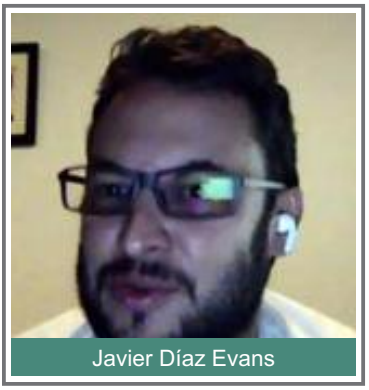
sibles funcionan los negocios de las empresas grandes, medianas y pequeñas y el resto de espacios que cobijan al ser humano.

Ante semejante realidad, la incertidumbre brilla y el gran reto se cifra en manejar las amenazas y aprovechar las oportunidades para sobrevivir en medio de la crisis. La pandemia mostró sus efectos de inmediato. Basta observar el traslado de la fuerza laboral a la movilidad y el teletrabajo o trabajo remoto, que en un trimestre pasó del 16.5% al 77.7%.

De ahí la inimaginable trascendencia del encuentro programado para esta edición, con el propósito de analizar la década comprendida entre 2010 y 2020, en términos de seguridad y ciberseguridad. Reunión a la que fueron convocados los mismos profesionales que diez años atrás analizaban el entorno y hacían sus pronósticos: Javier Díaz Evans, director global de Ingresos de A3Sec; Juan Camilo Reyes Fierro, Security Services Business Leader, Spanish South America (SSA), en IBM, Rafael H. Gamboa Bernate, abogado socio de Data & TIC Consultores y Andrés Ricardo Almanza J., miembro del Comité Editorial.

"En esta oportunidad queremos abordar la problemática de la seguridad y la ciberseguridad, cómo se


Andrés R. Almanza J.


Javier Díaz Evans


Juan Camilo Reyes F.


Rafael H. Gamboa B.

percibe en Colombia, hacia dónde vamos, qué va a pasar, cómo nos imaginamos el futuro y cuáles van a ser los desafíos, entre otras inquietudes, en un ejercicio comparativo con los mismos invitados diez años atrás en la edición 115", manifestó Jeimy J. Cano M., director de la revista para abrir el debate.

Andrés R. Almanza J.
Miembro Comité Editorial
En el ejercicio programado para hoy contemplamos dos momentos. El primero de ellos, está orientado a comparar sus respuestas entre 20-10 y 2020. En esa dirección, ¿cómo creen que les fue en esa medida de pronósticos?

Javier Díaz Evans
Director Global de Ingresos de A3Sec
El panorama ha cambiado en forma sustancial, muchos de los temas compartidos en ese momento, hoy, diez años después, son rescatables. Entre ellos están la disponibilidad y los cambios producidos por la nube. Fueron resueltos algunos problemas y nos encontramos resolviendo algunos nuevos.

Jeimy J. Cano M.
Diez años atrás, Javier Díaz Evans manifestaba: "En los próximos 10 años, la continuidad del negocio será un tema resuelto, mientras las organizaciones transfieran este riesgo a las empresas que soporten los servicios de computación en la nube".

Javier Díaz Evans
Eso es una realidad, no veo bancos con miedo de ir a la nube; por el contrario, hay muchas empresas que están obteniendo múltiples beneficios de esta tecnología, trabajando en esta pandemia de forma

muy fluida. Realmente creo que se trata de un tema resuelto. Sobre la privacidad, un asunto que también tocamos bastante en 2010, seguimos igual. No sé si en ese momento lo definí como una problemática futura, pero en este momento sí lo es.

Jeimy J. Cano M.
¿Qué tendremos que hacer para que no se afecte la privacidad de la información? Parece ser que esos dos temas siguen vigentes como problemática.

Juan Camilo Reyes F.
Security Services Business Leader, Spanish South America (SSA)
IBM

La disponibilidad no ha cambiado. En general, nos fue bien con las predicciones. Discutíamos en ese momento si el *compliance* y los asuntos relacionados eran un problema, hoy lo son; no varió la problemática del CISO, por el contrario, creció y en ese momento no considerábamos muchos vectores que hoy se tienen en cuenta para las industrias. Pero, un aspecto que no contemplábamos con tanta influencia era la nube que hoy demanda tanta atención, en términos de seguridad. En ese momento creíamos en un perímetro que hoy no existe, la información está en todas partes. Eso nos lleva a cambiar una serie de paradigmas. En ese momento fue una lectura acertada; considerábamos que el CISO en las organizaciones tendría un futuro con un poco más de relevancia, hecho que viene ocurriendo y que a las juntas directivas empieza a inquietar. Fue un muy buen ejercicio y acertamos en múltiples cosas.

Jeimy J. Cano M.
Diez años atrás Juan Camilo Reyes decía: "…lo más importante de la seguridad de la información está en el análisis de esos riesgos que van desde el perímetro hasta el dato, y que requieren un conocimiento más profundo de los procesos de negocio previo a la parte tecnológica".

Juan Camilo Reyes F.
Consideremos cómo estamos hoy. PCI no fue adoptada como base de algún estándar en Colombia, pero la obligatoriedad en la legislación peruana está soportada en PCI; el hecho de que en Colombia no se haya adoptado, no quiere decir que

en la región no lo fuera. HIPPA, en términos de datos personales, pone de manifiesto que el sector salud es el más crítico y puede generar algún tipo de discriminación. No adoptamos HIPPA, pero sí, una ley de protección de datos que contempla algunas de sus prioridades. En términos de datos, a nivel global hay una legislación en todos los puntos para mantener la privacidad. Las organizaciones hoy pelean con GDPR, un estándar de privacidad que acepta la comunidad europea, pero que en organizaciones como la que yo represento, nos obliga a poner cláusulas en todos los contratos para evitar contratiempos.

Rafael H. Gamboa B.
Abogado
Socio de Data & TIC Consultores
El asunto de la nube hoy no se discute, su importancia, su realidad, su necesidad. Hace 10 años muchos abogados oscilaban entre afirmar que no se podía hacer nada o simplemente que en la nube todo se podía hacer. Hoy hay más consenso en que sí se puede. A pesar de esta realidad, el año pasado un colega manifestaba que el Gobierno: (i) No podía tener nube, por asuntos de territorialidad, (ii) Que deberíamos ir a Linux y (iii) Montar un datacenter aquí en Colombia. Lo cierto es que hoy, diez años después, todos estamos arriba (en la nube), no tiene sentido pensar que el Gobierno opte por un datacenter propio y los ejemplos de China o Brasil donde "obligaron" a grandes proveedores a establecer datacenters en el territorio, no es aplicable, toda vez que esas economías son mucho más grandes. Sobre la privacidad, actualmente sucede una situación similar a la que ocurría hace 10 años, en la que, en virtud de los ataques del 11 de septiembre de 2001, mucha gente renunció a su privacidad para que el Estado le diera seguridad, la disyuntiva era seguridad vs. privacidad. Hoy, poco menos de 10 años después, la discusión sobre privacidad es la misma. Hace 10 años, la amenaza era un ataque terrorista, hoy es una pandemia. Una de las grandes diferencias es que las personas naturales eran quienes solicitaban protección al Estado, hoy son los Estados los que la requieren en aras de la salud pública, para establecer sistemas de seguimiento. Y, en términos de control jurídico, las normas han evolucionado muchísimo. Europa y Colombia tienen un híbrido en lo relacionado con el tratamiento de los datos y culturalmente somos mucho más norteamericanos, pero frente a las normas, más europeos. La privacidad cada vez cobra mayor fuerza y dinamismo. Hoy en día los gobiernos no tienen otra alternativa que colaborar y empezar a compartir información, en la medida en que ya no se trata de una amenaza como la de diez años atrás, sino de un asunto de salud pública.

Jeimy J. Cano M.
Diez años atrás Rafael Gamboa manifestaba: "En cuanto a los pro-

blemas resueltos e inexistentes en el año 2020, considero que la validez de la información electrónica, como manifestación inequívoca de voluntad y de identificación. La responsabilidad en el correcto actuar profesional".

Rafael Gamboa B.
El volumen de la información y la velocidad del procesamiento son algo increíble, basta mencionar el Conpes en Big Data 3920 de 2018, relacionado con este tema. Sobre la validez y el manejo de la información electrónica ya está muy avanzado, debido a que ya hay muchas herramientas, aún dentro del proceso judicial. Hoy hay más herramientas para probar veracidad e identidad que hace 10 años.

Andrés R. Almanza J.
Hice la comparación con los datos de la encuesta, con base en este resumen. Y, me llama la atención que ustedes citen las mismas tensiones de diez años atrás. En aspectos como la nube, la movilidad, la densidad digital, entre otros es evidente. Hoy la seguridad y la privacidad no son temas separados. Los técnicos vemos la conexión de estos dos mundos. Me queda la inquietud sobre la posición del CISO, en términos del terreno ganado, en el caso particular de Colombia.

En los 10 años los presupuestos en Colombia se basan en renovación y licenciamiento y la inversión se cifra en adquirir tecnología, Lo que preocupa es la seguridad en la nube, a pesar de que los profesionales de la seguridad no lo tienen claro. Las tendencias renovación y licenciamiento de *software* se convirtieron en una realidad. Con relación al mundo móvil, ustedes están más conectados con la realidad global que con la situación colombiana; aquí se invierte el dinero en los *commodities* estándar existentes, toda vez que los presupuestos no dan para resolver los problemas de la nube.

El riesgo no será una excepción, sino lo normal. La información sí se reconoce como un activo; sobre los datos reconocen carencias en términos de protección de los mismos. Sobre la privacidad ustedes fueron unos visionarios al catalogarla como una realidad latente. No obstante, en la encuesta las diferentes cifras de los datos y los promedios muestran que en la práctica la privacidad no es una de las tareas fundamentales de los profesionales responsables de la seguridad. Atienden los eventos, pero no son una prioridad, no son los incidentes más atendidos en las organizaciones durante estos 10 años. Están como en el puesto 12 o 13 frente a los promedios.

Así que la privacidad es un tema que no está claramente digerido dentro de las organizaciones. En la práctica lo hemos visto, los técnicos descargamos la responsabilidad de los asuntos de la privacidad en el área jurídica. Con relación a las otras tres dimensiones, en el ca-

so de Colombia la regla es 27000. Por el lado del cumplimiento, nosotros estamos sujetos en lo nacional e internacional de manera muy fuerte. Y, los profesionales en Colombia carecen de habilidades gerenciales claves para lograr que los asuntos de seguridad lleguen a otro nivel dentro de las organizaciones. Esto se debe a que los temas que proponen giran en su zona de confort y están relacionados con vulnerabilidades, amenazas, pero no han enriquecido su lenguaje para entrar en comunicación con la alta dirección de las compañías. Y, por último, las funciones desempeñadas por un profesional de la seguridad (CISO) apuntan a proteger la información de la compañía, exigir controles, seguir las prácticas y las políticas. En otras palabras, en estos diez años no se ve un CISO con otro perfil. En algunos aspectos ustedes están muy cerca de lo obtenido en la encuesta.

Jeimy J. Cano M.

El día a día del CISO en 2030: ¿Cuáles cree usted que serán los problemas resueltos e inexistentes en el 2030? ¿Cuáles cree usted que serán los nuevos retos y problemas a los que tendrá que enfrentarse en el 2030?

Juan Camilo Reyes F.

En mi opinión, tristemente debo señalar que ninguno. Desde 2014 alrededor de mi experiencia personal tuve la oportunidad de realizar una mirada más regional en Suramérica y he encontrado que la definición de los básicos, sigue mal hecha; todavía se encuentran organizaciones en que la simple segmentación de redes está mal, no hay sistemas de clasificación de información, tampoco de seguridad, la información está dispersa en múltiples sistemas, y estos son síntomas generalizados que no son más que la ausencia de una estrategia clara para proteger la información. Las organizaciones se dedicaron a adquirir tecnología sin saber para qué ni en qué la iban a utilizar. Así lo muestra la presentación realizada de los datos en torno a la inversión en seguridad. Si no veo la caja, el papel que me dice la licencia, no siento que la organización esté creciendo y tenga un verdadero activo, así que se deja de lado la planeación para establecer las bases adecuadas en la protección de la información. Sobre cuáles problemas están resueltos y son inexistentes me oriento más a que continuamos atacando los problemas conocidos en 2010, que siguen sin resolver y así continuarán en 10 años más. Todavía existen compañías en las que la ciberseguridad seguirá siendo vista como un costo, y si no se transforman muy probablemente desaparecerán en el corto plazo, toda vez que la transformación digital es inminente para subsistir. La transformación digital no es otra cosa que ayudarnos a crecer los ingresos, facilitar la operación a través de tecnología y ésta será susceptible de ataque a través de la violación de los protocolos de seguridad. Así que, lastimosamente,

mejoraremos en algunos temas, pero continuaremos con las dificultades en los aspectos básicos no resueltos. Avanzaremos en todos aquellos aspectos que representen un riesgo monetario tangible; por ejemplo, mantener de mejor manera una red resiliente, preocupación del responsable de seguridad, frente al poco interés en el dato. Se avanzará en los asuntos que frenen la transformación digital de la organización como se la habían imaginado. Si no nos ocupamos de proporcionar más 'dientes' a la ley de protección de datos personales, se tratará de un tema ocupando los puestos 12, 14 o 15 en el escalafón de las preocupaciones.

Javier Díaz Evans

Me referiré en el siguiente orden: negocio, tecnología y rol del CISO. En cuanto al negocio va aparecer la crisis de la confianza de las organizaciones muy relacionado con el uso de los datos y directamente con la privacidad. Vamos a ver problemas en las empresas que no son transparentes en la recolección y uso de datos personales, reto que debe ser controlado y gestionado por el responsable de seguridad de información o privacidad. Sobre la visibilidad, sacar provecho de los datos, será algo resuelto. La seguridad estará completamente soportada en Big Data y en su explotación para la generación de inteligencia que nos ayude a detectar y responder de forma efectiva a los incidentes y brechas. Aparecerá un nuevo reto llamado la hiperautomatización; en otras palabras, que todas las tareas repetitivas y la capacidad de interconectar la infraestructura de seguridad y tecnológica ayude a responder ante los riesgos e incidentes a la velocidad que requerimos para reducir el tiempo de exposición ante los ataques. Las arquitecturas de seguridad multicapas, que hemos transformado en la actualidad a arquitecturas sin perímetro, se orientarán a la protección de servicios efímeros y equipos personales potentes. Los modelos de seguridad soportados en gestión de riesgo van a desaparecer, debemos transformar la ciberseguridad a la velocidad de la tecnología.

Por otra parte, nos vamos a enfrentar al humano aumentado, es decir, a utilizar la tecnología para aumentar capacidades físicas y/o cognitivas del hombre. El reto será enfren-

tar a los atacantes que están sentados frente a un computador, desarrollando mucho más sus habilidades para obtener un beneficio. Por último, en el frente tecnológico se encontrará el reto de la inteligencia artificial, debemos asegurar que se emplee para beneficio de todos y no de unos pocos.

Frente al aspecto humano solo quiero plantear mi percepción del rol del CISO. Hace una década llegó a reportar directamente al CEO. Creo que estamos viviendo el declive y pronostico que en 2030 puede que no tenga relevancia a nivel directivo, como le puede pasar al responsable de tecnología.

Rafael Gamboa B.

Uno de los temas que más ha avanzado tiene que ver con la relevancia de la seguridad que, hasta hace poco no era clara dentro de la organización; pero, lo cierto es que un actuar diligente, no puede desconocer su importancia con el negocio. La nube en el 2030 tendrá que ver con la centralización de la información para facilitar su administración por parte del responsable y de los titulares. Otro tema que esperaría estuviera resuelto es el de los reportes de incidentes, toda vez que en la actualidad nadie quiere reportarlos, pero en un futuro mediato y a largo plazo, el reporte no buscará sancionar a las organizaciones, sino estará enfocado en el fortalecimiento del área, al poder conocer todos los ataques o fallas de que han sido objeto. El Gobierno, los reguladores y las organizaciones deberán tener conciencia en torno a que el reporte es necesario para la región, en cada sector. Por ejemplo, un reporte de incidentes en el sector financiero se hace, no para denunciar a un banco, sino para fortalecer a dicho sector. Se espera que para 2030 la regulación sea clara, en torno a la inteligencia artificial. Sobre el declive del CISO, no creo que se dé, más aún en la medida en que las herramientas tecnológicas se masifican y los riesgos aumentan. Si a esto le sumamos el contexto del teletrabajo o trabajo remoto, la seguridad y la ciberseguridad cobran mayor relevancia.

Juan Camilo Reyes F.

Al reporte de incidentes que plantea Rafael Gamboa, se suma el aspecto cultural. En Colombia se buscan culpables más que oportuni-

dades de mejora. De ahí que esa cultura que hay detrás incida para no realizar dicho reporte. Se trata entonces de un cambio inmenso dentro de las organizaciones colombianas. Las multas son irrelevantes, siempre y cuando no sean altas, lo mismo que sucede sobre la protección de datos. Creo que para 2030 estos asuntos todavía no serán cubiertos y ese es el gran reto. Estoy de acuerdo en que la imagen reputacional es un tema de peso, pero en esa combinación, como no hay posibilidades de que el Estado castigue esa omisión, pues las organizaciones hacen poco, de ahí que no creo resuelto el reporte de incidentes para 2030. Tenemos que fortalecer la ley de protección de datos, ese es el gran reto. Y sobre el CISO no estoy de acuerdo en que va a desaparecer, toda vez que se están dando cuenta de que el gran negocio se va a dar en la plazoleta digital y es necesario moverse hacia allá, en donde cuesta menos producir dinero y se capta mucha más gente. En ese espectro, el CISO será crítico y entiendo que su rol tiene que mutar. Parte de la desfiguración que tenemos sobre la imagen del CISO es que esté más enfocado en la parte técnica, pero cuando se tiene un profesional que apalanca el negocio, el entorno tiene que cambiar. Y eso se va a dar porque el negocio dependerá de la tecnología y quien la proteja habrá de ocupar un lugar relevante en las organizaciones. No creo en su desaparición; por el contrario, tomará mucha fuerza.

Jeimy J. Cano M.

¿Cuáles cree usted que serán los nuevos temas de investigación en seguridad y ciberseguridad que surgirán en esta década y se desarrollarán a partir del 2030?

Javier Díaz Evans

La inteligencia artificial ocupa un gran espacio en las investigaciones de ciberseguridad, no sólo en resolución de problemas del día a día, sino en cómo hacer uso de la misma para apoyar en la mejora continua, quiero decir, usar la inteligencia artificial para mejorar la inteligencia artificial. El tiempo de permanencia (Dwell Time) nos está doliendo y no tenemos la capacidad de aplicar las metodologías de gestión de riesgo en el entorno actual y futuro, en el que nuevas técnicas, tácticas y procedimientos aparecen y son aplicados por los atacantes.

Jeimy J. Cano M.

Diez años atrás, Javier Díaz Evans anotaba: "…Frente a las actividades indebidas o malos usos de los usuarios, la seguridad no puede ir en contra del acceso o la facilidad de uso de la tecnología; debemos controlarlos y pensar en la efectividad y el logro de nuestros objetivos básicos de seguridad: confidencialidad, integridad, disponibilidad y privacidad".

Javier Díaz Evans

La seguridad se soporta en los mismos fundamentos, sólo hacemos uso de nuevas tecnologías para

mejorar la efectividad de nuestros modelos. Ese tipo de premisas no han cambiado mucho.

Juan Camilo Reyes F.

Hay que dividirlo en dos líneas. La primera se refiere al CISO frente a los nuevos retos en general, como líder de un equipo con la responsabilidad de atender los eventos de carácter técnico sobre la información. El segundo asunto sobre cómo reformar el rol del CISO para que se convierta en un habilitador de los negocios, será otra de las grandes misiones que tendrá. Desde el punto de vista técnico, se nos vienen importantes retos en seguridad. Coincido sobre el humano mejorado, que yo defino más como inteligencia artificial buena, versus la mala. Al disponer las herramientas de inteligencia artificial ¿qué tanta capacidad tenemos para controlar e impedir que el hacker haga uso de ella? Me parece que el uso del *blockchain* será muy importante hacia 2030. Es entender cómo a través de tener múltiples puntos en los cuales la información me impide hacer cambios o se ejecuten ataques a la integridad y se utilizará como parte de la seguridad. Este uso será de vital importancia. Un tercer aspecto clave para 2030 será la criptografía post computación cuántica, toda vez que las capacidades de cómputo dentro de cinco o seis años serán infinitamente mayores, gracias a ella. Así que la criptografía actual no servirá. El atacante tendrá nuevas herramientas para hackear la criptografía actual, y es necesario trabajar ya sobre estos aspectos. Un ejemplo sencillo de la necesidad son los carros. Actualmente, la vida útil de un carro en nuestra región supera los 10 años. Si hoy en día se tienen carros que vienen con sistemas conectados a internet, los algoritmos de cifrado que usen serán vulnerables en 10 años. La criptografía deberá ser cambiada desde ya, para poder atender las capacidades de cómputo a futuro. Y, por último, sobre el aseguramiento del IOT, nos falta mucho conocimiento en este ambiente; le estamos dando direcciones IP y conectividad a todo, pero los fabricantes todavía no tienen los procesos y protocolos adecuados para fabricarlos con seguridad. Sobre el segundo reto, el CISO de 2030 tendrá que hablar el lenguaje misional de la organización. Hoy en día continúa haciendo sustentaciones técnicas a problemas relacionados con la misión y eso tiene que cambiar. Proteger la información tiene que dejar de ser un problema técnico para convertirse en un asunto de negocio. Estos diez años nos servirán para que el CISO retome su papel relevante de poder hablar el lenguaje del negocio.

Jeimy J. Cano M.

Diez años atrás, Juan Camilo Reyes aseguraba: "…Los usuarios no van a preguntarnos qué tipo de algoritmo o herramienta estamos utilizando para lograrlo. Todo se verá reducido a acuerdos de niveles de servicio".

Juan Camilo Reyes F.
La migración ha sido muy lenta y ese es uno de los problemas que tenemos en Colombia; todavía cuando la gente pide algo, se refiere a una máquina y aún existe el romanticismo del CISO por la tecnología, hecho que no le ha permitido evolucionar. Se siente sólido con el conocimiento técnico, pero no le sirve para hablar con el CEO y pedir lo que requiere.

Rafael Gamboa B.
El primer elemento es el trilingüismo que debe existir en la organización; el negocio, la tecnología y las leyes, deben ser consideradas como un todo, trabajarlos de manera independiente no tiene sentido.

Es necesario establecer el marco de acción misional o de negocio para que la tecnología sirva de soporte y que el área jurídica permita la ejecución misional y comercial mitigando los riesgos. La ley jamás va a estar al día con los desarrollos tecnológicos. No tiene sentido tener *hardware* en el sótano del edificio, si existen proveedores de infraestructura con equipos robustos y escalabilidad a la medida de mis necesidades temporales. La dificultad que ofrecen estos proveedores de nube, es que, por lo general, se trata de sociedades extranjeras sin presencia jurídica en Colombia, por lo que no son objeto de legislación colombiana. En cuanto a la regulación de nube en Colombia, sólo hasta 2019 con la Circular 5 de la Superfinanciera surge como la primera regulación nube, que no dice nada exótico, pero vía reglamentaria, exige que sus vigilados o supervisados que usen nube, deben garantizar que, en caso de tomas de control, la Superfinanciera pueda acceder a la información.

Jeimy J. Cano M.

La sociedad en el 2030:
¿Qué dispositivos y controles cree usted que serán de uso masivo y general para el 2030?
Previendo un aumento exponencial de la densidad digital, un incremento de flujos de datos personales, el cruce de datos entre entidades a nivel internacional y la aparición de nuevas estrategias de seguridad y control, ¿cómo visualiza usted la sociedad del 2030?

Juan Camilo Reyes F.

Veo mucho más masivo el monitoreo de la información de marca y personal en la *deep* y *dark web*, tanto para las corporaciones como para los perfiles de ejecutivos. Las organizaciones saben que en el mundo oscuro se está hablando de ellas; hay sentimientos hacia ellas. Se quiere monitorearlas con el propósito de saber qué está pasando en ese tráfico oscuro y esto les va a servir para disponer de una información de riesgo más nutrida. Vamos a ver un cambio en el análisis de riesgos en las empresas, aunque sigamos en un modelo muy cualitativo alrededor de si el riesgo es o no alto, entre otras consideraciones. Y lo que va a pasar es que cada vez recibiremos más presión para mostrar este tema en números. Así que el análisis de riesgos sufrirá profundos cambios en los próximos años, alrededor de metodologías cuantitativas. Se nos va a acabar el discurso de "esto va a tener un alto riesgo" solamente en estos términos, porque va a requerir una discusión monetaria detrás para justificarlo. También veremos la aparición de servicios de ciberseguridad para el hogar muy fuertes. Habrá organizaciones ayudando a proteger el televisor, el servicio de gas, la nevera y otros electrodomésticos. Incluso me imagino que parte de las revisiones técnico mecánicas contemplarán niveles de parches con el carro; será un problema importante de seguridad. Veo la masificación de los seguros frente a los ataques, no sólo a nivel corporativo, sino en las personas, quienes querrán contratar un servicio para proteger su funcionamiento en el ciberespacio. Todo esto se traduce en una mayor conciencia sobre los peligros de la conectividad lo que va a generar innovación y nuevos servicios para los ciudadanos. Esa es mi visión para el 2030 sobre estos asuntos.

Javier Díaz Evans

Estoy seguro que las personas estarán llenas de dispositivos, hiperconectadas, muchos sensores, dispositivos para capturar todo acerca de nosotros; las empresas deben generar multiexperiencias a través de lo que nos dan esas herramientas. La sociedad tendrá la posibilidad de separar la información relevante con valor, de la información basura, dejaremos de ser buenos buscando lo que no necesitamos a ser buenos seleccionando conocimiento válido. Durante esta década vimos ese problema en la sociedad y algunos lograron, mediante el consumo de información sesgada,

orientar las decisiones de un país. En la parte de negocio vuelvo al tema de la crisis de la confianza; para mí la privacidad debe ser asimilada como un derecho, no como una característica o principio de seguridad. Tener en cuenta la ética en los negocios para no abusar en ese tipo de temas. En 2030 la crisis en la confianza se verá latente, poniendo fin mediante el control social de empresas que no son transparentes en el uso de la información de sus clientes. Por otra parte, también creo que existirá un crecimiento exponencial de los dispositivos autónomos, como robots, para ejecutar muchas tareas actuales; un ejemplo es la logística o domicilios con drones. Esto que estamos viviendo en la actualidad puede afectar la globalización, haciendo que los países cierren mucho las posibilidades de comercio internacional.

Rafael Gamboa B.
Para responder lo primero es preguntarnos ¿quiénes van o vamos a estar en 10 años? Es probable que los mayores de 40, no seremos el sector más activo, serán los jóvenes que han nacido exponiendo su vida en redes sociales. Si a esto le sumamos la presente situación de salud pública, pues podemos vislumbrar un relacionamiento virtual mucho mayor, y me refiero a la exhibición a través de las redes sociales, que más allá de ser una moda es algo normal para las personas en ese momento. ¿Qué puede pasar o que actitud adoptar? Continuar de la misma manera exponiéndose u optar por la desaparición de la vida virtual. Eventualmente esto puede pasar. Sobre los controles de uso masivo serán la aplicación de sistemas biométricos, tales como la huella, el iris u otras alternativas las que reemplacen las claves, temas de memoria o dispositivos, todo encaminado a una conducta de distanciamiento social y de seguridad, al igual que de comodidad. Sobre la eventual pérdida de privacidad y ante la existencia de muchísima información de las personas, las empresas para cargos críticos optarán por un perfil ideal, perfecto y bueno. Esto creará muchos cambios y a los candidatos se les exigirá una absoluta renuncia a su privacidad, con miras a proteger la organización. Todos estaremos marcados. Es necesario prepararnos para ese momento, porque ineludiblemente llegará.

Jeimy J. Cano M.
Una noticia reciente apunta a que para ingresar a los países a mediano plazo tendremos que portar certificados de inmunidad frente a una enfermedad. Esto comienza a hacer carrera.

Andrés R. Almanza J.
Lo que menciona Rafael ya lo puso en práctica el gobierno chino para el control de la pandemia. En el 2030 la situación será más exponencial. Lo de China está causando un efecto dominó, y se está viendo en España para localizar a sus ciudadanos infectados. Vamos a em-

pezar a dejar de ver la privacidad de una forma rígida a una forma más sensible. Este será un gran planteamiento a futuro. Y en tal sentido, me gustaría dejar aquí la pregunta: veo a un *Chief digital officer* asumiendo muchas funciones y más evolucionado. ¿Buscará crear experiencias confiables para que el CISO pueda conversar con la Junta Directiva?

Juan Camilo Reyes F.
Para complementar lo planteado en términos de privacidad por Rafael Gamboa, cobran fuerza las brechas de seguridad. Es decir, se deja a libertad del atacante cómo utilizar esos datos y frente a eso nos toca cambiar el proceso de autenticación y verificación, toda vez que ya no se tiene la confianza de los datos. Vamos a tener mayores datos de autenticación.

Jeimy J. Cano M.
¿Cuál será el principio de seguridad que estará más amenazado en 2030: confidencialidad, integridad, disponibilidad? ¿Será necesario repensar nuevos principios de seguridad y control como los propuestos por Donn Parker en 1998, en su libro "Fighting Computer Crime. A New Framework for Protecting Information"?

Donn B. Parker, matemático e investigador del *Stanford Research Institute International*, publica por primera vez su propuesta de refundar los fundamentos de seguridad de la información en 1991 en la 14 Conferencia Nacional de Seguridad Informática realizada en Baltimore, USA, con un artículo titulado: "RESTATING THE FOUNDATION OF INFORMATION SECURITY" en el que plantea la necesidad de contar con seis (6) atributos básicos en seguridad de la información, en lugar de los tres (3) conocidos a la fecha como son confidencialidad, integridad y disponibilidad.

Lo que la literatura ha denominado el Hexágono de Parker, establece seis componentes de la seguridad de la información como se menciona a continuación:

- *Disponibilidad*: usabilidad de la información para un propósito.
- *Utilidad*: pertinencia de la información para un propósito.
- *Integridad*: la completitud, totalidad y legibilidad de la información y la calidad no cambian con respecto a un estado anterior.
- *Autenticidad*: validez, conformidad y autenticidad de la información
- *Confidencialidad*: acceso y divulgación limitada del conocimiento.
- *Posesión*: la custodia, el control y la capacidad de utilizar la información

En publicación reciente contextualiza aún más su propuesta indicando que estos seis (6) elementos permitirán seleccionar con diligencia medidas de salvaguardia y prácticas concretas de seguridad y control para:

- evitar la negligencia,
- motivar una sociedad ordenada y protegida,
- asegurar el cumplimiento de las leyes, regulaciones y auditorías,
- desarrollar una conducta ética, y
- habilitar el comercio y la competencia de forma exitosa.

Javier Díaz Evans

Muchas veces los CISOS se alejan de los fundamentos de los modelos de seguridad. Es muy importante entender que los datos con una estructura crean información y ésta el conocimiento y éste con alguna acción genera las ventajas competitivas de las organizaciones. La seguridad busca proteger esos datos, frente a diferentes riesgos que puedan afectar propiedades claras como la confidencialidad, integridad y disponibilidad. Aquí aparece una primera problemática y es la propiedad de los datos. El propietario es quien tiene la capacidad de transmitirnos las necesidades de protección, justificados en el valor de los mismos. Para los datos personales, sin un responsable claro dentro de las organizaciones, lo resolvemos con regulación, con el fin de limitar los usos y las necesidades de protección de los mismos.

La preocupación no es que las empresas tengan la información de las personas, el verdadero problema se soporta en cómo la utilizan y qué beneficios obtienen de usos nos autorizados. Por otra parte, tenemos la necesidad de soportar decisiones en términos de seguridad. Para ello encontramos la metodología de riesgos, que nos ayuda a dar sustento a nuestras decisiones, y a proporcionarnos una guía sobre qué acciones debemos priorizar en nuestros planes. De la metodología de riesgos rescato los mapas de riesgo, en lo que tratábamos de definir todos los posibles eventos que podían afectarnos, pero como nos puede demostrar el COVID-19, debemos prepararnos para lo desconocido, que es lo que realmente nos puede impactar. Esos riesgos nos impactan si tenemos una vulnerabilidad o, en otros términos, tener una brecha o incidentes si no tenemos controles o si la efectividad de éstos no es la adecuada.

Para concluir la idea, la realidad que estamos viviendo nos muestra que los modelos de seguridad, como los conocemos, deben transformarse para lograr enfrentar lo desconocido, ser ágiles para adaptarse a los nuevos riesgos y ligeros para ser eficientes y capaces de mejorar continuamente.

Juan Camilo Reyes F.

Yo no había leído el modelo, cuando lo leí en la preparación para esta reunión me pregunté por qué un modelo de 1988 que parece ser muy fuerte y otro de 2010 tampoco se está usando y llegué a la conclusión que un modelo debe basarse en la simplicidad. Si es así, es replicable. No podemos irnos a un modelo que tenga muchas aristas, tenemos que simplificarnos, el modelo se mantiene porque es enten-

dible. Porque cuando las cosas se hacen más complicadas y lo afectan, esto hace que no tenga éxito. En consecuencia, sí creo que debemos replantearnos porque tenemos una responsabilidad frente a lo que manejamos. Ese modelo debe tratar de mantenerse lo más simple posible. Y ahí veo la falla de Don Parker, un modelo robusto, muy bueno, pero no es simple. Ahí es donde debemos buscar la forma para remodelarlo.

Rafael Gamboa B.
Para 2030, el principio de seguridad más amenazado será el de la privacidad, a la cual renunciaremos los titulares, a cambio de satisfacer las necesidades. Uno de los grandes cambios en materia de "propiedad" de los datos personales en Colombia y en el mundo, es que ya se definió que ésta no es de la empresa, sino de la persona misma, que libre y voluntariamente los entrega a una compañía para que hagan tratamientos; cuando hablamos de privacidad nos referimos al sujeto y si hablamos de la confidencialidad, nos referimos a las acciones del individuo. En otras palabras, vamos a un escenario en el que las empresas van a tener pleno conocimiento de los datos de las personas, quienes los entregaron a cambio de la satisfacción de un interés, pero conservan la facultad de revocar dicha autorización en el momento que lo deseen. Esto genera confianza por parte de la persona a la empresa que administra y trata sus datos.

Jeimy J. Cano M.
Lo que quiere decir que pasaremos del control de acceso al control del uso.

Rafael Gamboa B.
Sí. O en el momento en que la persona se sienta empoderada habrá un libre tráfico de la información en el marco de un buen tratamiento. En virtud de la autorización que la persona proporcione para ese manejo.

Jeimy J. Cano M.
Existen teorías en ese sentido que incorporan un nuevo elemento adicional a la confidencialidad, integridad y disponibilidad, a propósito del internet de las cosas y los sistemas ciberfísicos emergentes, que es el concepto de "Safety". En donde lo que ocurre en el mundo lógico, termina afectando el mundo físico.

Javier Díaz Evans
Hace 10 años cuando asumí el rol de CISO, traté de unificar en mi rol los temas de riesgo operativo, riesgos tecnológicos y seguridad física (*safety*). Fue una experiencia muy interesante; pero, pensando en que se pueden gestionar con modelos de riesgos, encontré que son prácticas diferentes y rápidamente fue necesario desarrollar otras habilidades para poder presentar soluciones a las problemáticas del mundo físico en la junta directiva. En la actualidad veo que esa visión de hace 10 años para integrar frentes de trabajo se ha perdido y encontramos cada vez más profundi-

zación en las funciones, separando los expertos de seguridad tecnológica de los expertos en gobierno y seguridad de la información. Creo que eso diluye mucho las responsabilidades del CISO.

Juan Camilo Reyes F.

En la triada es necesario buscar nuevos elementos para agregar a los que ya tenemos. Y por eso quería dejar seguridad por fuera. La tríada está enfocada en la información. Y en el ámbito de las redes nos debe preocupar que la ciberseguridad sea vista como un potencial en el que la vida puede estar en riesgo. Esto se sale mucho de las características de la información a las que se refiere la tríada y merece un capítulo aparte. La ciberseguridad ya no será sobre una característica de la información, sino sobre la labor del CISO. Estoy de acuerdo en que su misión está robustecida por todo lo que se plantea en el modelo de Parker, porque la función de dicho profesional va más allá de la confidencialidad, integridad, y disponibilidad. A esto se agrega el cuidado del ciberespacio y de la organización en ese entorno. Y, en esa evolución, la tríada tiene que existir enfocada al manejo de la información, pero no como el único objetivo del rol del CISO, quien ahora tiene una arista sobre cómo proteger la imagen de la organización en el ciberespacio y otro tipo de asuntos diferentes. El nuevo modelo debería orientarse al rol del CISO y no a las características de la información únicamente.

Rafael Gamboa B.

Me quiero referir a la importancia del CISO y a la existencia del abogado y los controles de seguridad. ¿Es posible vivir sin ellos? Sí. Cuando miramos la evolución de la tecnología, realmente un CISO no se necesita para que la empresa genere dinero, se trata de una función meramente preventiva. Igual sucede con el abogado. Pero ante un incidente o un tema jurídico o de seguridad, la primera pregunta estará enfocada sobre la implementación de medidas, la existencia del CISO, la del abogado y si la respuesta es negativa, la valoración será que se actuó de manera negligente. Por cuenta de la cuarentena, muchas empresas que tenían proyectos de transformación digital, tuvieron que acelerar los procesos para poder sobrevivir comercialmente.

Jeimy J. Cano M.

Hoy nos convoca un entorno interdisciplinar, donde las fronteras se rompen y tensionan lo que entendíamos hasta la fecha. En el modelo de Donn Parker es lo que se ve, vamos hacia una interdisciplinariedad. Y en esa dirección veremos un nuevo profesional enfocado en la ciberbioseguridad que relaciona la bioseguridad, la ciberseguridad y la seguridad ciberfísica. Por ejemplo, la impresión 3D de un hueso, lo implantes cocleares, escenarios convergentes que terminan afectando el mundo físico. El cambio apunta a considerar ya no lo disciplinar, sino lo interdisciplinar. Un ecosistema

en el que vamos a estar interactuando.

Reflexiones finales

Juan Camilo Reyes F.

Hay una mudanza del rol del CISO que parte del hecho de la interdisciplinariedad. Hay que pensar en los riesgos que estamos en posibilidad de mitigar con base en nuestro conocimiento y cómo lo usamos para proteger el negocio. Esto hace que no podamos quedarnos únicamente en lo técnico, se requiere una formación social, de comunicación y de negocio para entender la magnitud del rol y que éste siga teniendo la trascendencia en 2030, y debemos estar preparados. Va a exigir empezar a formarse en muchas otras disciplinas. Se tratará de una carrera maravillosa, muy completa.

Javier Díaz Evans

El foco de la función de ciberseguridad está en atacar dos frentes de trabajo. El primero, la gestión de riesgos, nuestras capacidades con esta metodología en seguridad se reducen para enfrentar lo desconocido. Nunca nos imaginamos que todos estuviéramos trabajando desde la casa durante más de un mes, como lo estamos haciendo, impacto que lo han sentido las empresas. Son muy pocas las compañías que en medio de esta pandemia están operando al 100%, aquellas lograron aplicar controles que apoyaran este evento, lo más seguro es que no lo hayan pensado y menos gestionado este riesgo. Hay que pensar en cómo transformar los modelos de toma de decisión y evolucionar de forma continua los controles para que realmente sean efectivos. Un ejemplo del tema de controles poco eficientes, es el control de sensibilización en seguridad. Muchas organizaciones dedican muchos recursos y tiempo en transmitir a los colaboradores conocimientos de seguridad para que, mediante ese conocimiento, los usuarios cambien hábitos que pueden generar brechas o debilidades en nuestro modelo. La realidad es que es muy poco eficiente, debemos identificar comportamientos anómalos de los usuarios y corregir de forma inmediata para cambiar esos malos hábitos. Por último, el mensaje más importante que les dejo, es que nuestra misión no debe ser únicamente proteger los datos; debemos asumir nuestra responsabilidad en apoyar a las empresas para aplicar la ética en los negocios, ser responsables y transparentes para minimizar la crisis de confianza en las instituciones. Debemos ir más allá del concepto de resiliencia, tener la capacidad de aprender constantemente de los errores y fallas, una capacidad que debe explotar al máximo el CISO para no perder jerarquía y seguir apoyando en esta transformación tecnológica que vivirán las industrias de todo tipo.

Rafael Gamboa B.

El riesgo más grande de una organización es el empleado. Capaci-

tarlos es primordial, pero a pesar de hacerlo, muchas veces no es suficiente. Soy un convencido de que el control técnico es clave. El reto más grande del 2030 arrancó en el 2020, sobre cómo cambiamos la modalidad de interactuar; nos probó que sí podemos trabajar de una forma diferente. La tecnología seguirá evolucionando, será más rápida. El riesgo se ha ampliado mucho más y el reto es cómo vamos a actuar frente al nuevo entorno.

Andrés J. Almanza J.

Veo el futuro lleno de muchas oportunidades con un ambiente cada vez más complejo. Un líder de seguridad digital más comprometido en construir confianza digital que recoja los principios de valor y responsabilidad. Vamos a tener un mundo con mucha más capacidad, existirán más roles para que la interdisciplinariedad esté más presente en la dinámica organizacional. Se tratará de prestar servicios digitales de extremo a extremo y la información será de ellas. Es necesario considerar cómo la función crea valor, no hay opción de devolverse, porque la demanda ya llegó. Una empresa sin la presencia del área jurídica no podrá subsistir.

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.; es editora de esta revista.*

Seguridad y ciberseguridad 2009-2019

DOI: 10.29236/sistemas.n155a6

Lecciones aprendidas y retos pendientes.

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

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

Introducción

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

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

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

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

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

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

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

Computación en la nube

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

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

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

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

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

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

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

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

Computación móvil

Los móviles como una tendencia

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

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

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

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

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

Lecciones aprendidas

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

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

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

Convergencia tecnológica

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

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

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

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

que las conexiones y flujos configuran en los objetos.

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

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

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

Redes sociales

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

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

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

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

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

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

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

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

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

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

Asimetría de los ciberconflictos

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

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

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

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

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

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

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

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

Lecciones aprendidas

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

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

Retos pendientes

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Reflexiones finales

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

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

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

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

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

En consecuencia, las lecciones aprendidas de ésta última década

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

Referencias

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Mobile learning

DOI: 10.29236/sistemas.n155a7

Para acercar a los usuarios regulares a la seguridad informática.

Resumen
La tecnología se ha convertido en una herramienta fundamental en nuestras actividades diarias. Por ejemplo, usamos teléfonos inteligentes para comunicarnos con nuestros familiares y amigos, realizar actividades laborales, operaciones financieras y entretenernos con aplicaciones y redes sociales. Sin embargo, debido a su poco conocimiento en el tema, los usuarios regulares no son conscientes de los riesgos asociados al usarla, por lo que están expuestos a tomar decisiones equivocadas que los podrían convertir en víctimas de cibercriminales. Adicionalmente, la coyuntura global de salubridad que ha generado el virus COVID-19 ha incrementado el uso de dispositivos electrónicos, aplicaciones e Internet, que agudizan la exposición de los usuarios regulares a riesgos cibernéticos.

Palabras clave
Mobile Learning, Seguridad Informática, Tecnologías de la Información y Comunicación, Usuarios Regulares

Introducción

Tener conocimientos sobre seguridad informática es fundamental en un mundo en el que dependemos de la tecnología para gran parte de nuestras actividades. Los desarrollos tecnológicos han traído progreso para la sociedad, pero, a su vez, retos para la protección de la privacidad de las personas. Durante 2019, en Colombia se reportó un aumento en el número de accesos a Internet, (6 de cada 10 colombianos tienen acceso a Internet móvil (Portafolio, 2020). Por otro lado, en ese mismo año, se registraron 28.827 casos de ciberataques y los incidentes que más se reportaron fueron Phishing (42%), suplantación de identidad (28%), envío de *malware* (14%) y fraudes en medios de pago en línea (16%) (TicTac, 2019). Estas cifras son contundentes y plantean serios interrogantes sobre el conocimiento de los usuarios en seguridad informática.

Más aún, el virus COVID-19 ha forzado a muchas personas a quedarse en sus casas, aumentando el uso de dispositivos electrónicos e Internet para trabajar, informarse, entretenerse, adquirir bienes y acceder a atención médica, entre otras posibilidades. De ahí la exposición de los usuarios regulares a software malicioso detrás de noticias falsas y estafas cibernéticas. En la tabla 1 se evidencia que servi-

Tabla 1

Estadísticas de crecimiento en uso de aplicaciones populares durante las medidas de cuarentena por COVID-19 en el mundo.

Aplicación	Estadísticas que evidencian crecimiento en uso
Facebook	50% de incremento en mensajes en Instagram y Facebook en varios países y un incremento de más de 1000% en llamadas grupales en Italia
Microsoft Teams	Incremento del 775% en usuarios mensuales en Italia y 44 millones de usuarios en todo el mundo en un día
Slack	Entre el 1 de febrero y el 18 de marzo, tuvieron 7000 nuevos clientes, y en marzo 25 tuvieron 12.5 millones de usuarios conectados al mismo tiempo
WhatsApp	40% de incremento en uso
Zoom	En marzo alcanzaron un pico de 200 millones de participantes en reuniones diarias
HouseParty	Tasa de descarga 323x más alta que su promedio en febrero 2020

Elaboración propia con estadísticas tomadas de (The New York Times, 2020), (Forbes, 2020), (TechCrunch, 2020), (ZDNet, 2020) y (Zoom Blog, 2020).

Figura 1. *Interés a lo largo del tiempo de Microsoft Teams, Zoom, Skype y Meet. Gráfico creado con Google Trends el 3 de abril de 2020 a las 3:01 PM.*

cios como Microsoft Teams, Slack, WhatsApp y Zoom, por ejemplo, han reportado incrementos significativos en su porcentaje de uso durante las cuarentenas impuestas por varios gobiernos en todo el mundo.

Nota: cabe resaltar que las cifras por aplicación pueden ser más altas en países en una etapa más avanzada de la cuarentena. Por ejemplo, en España, WhatsApp ha tenido un crecimiento del 51% (Tech Lapse, 2020).

El creciente aumento del interés en tecnologías que facilitan el teletrabajo y la comunicación con familiares también se ve reflejado en las tendencias de búsqueda de Google (Figura 1).

Los parámetros seleccionados fueron: **búsqueda web** en **Colombia entre el 3 de febrero y el 3 de abril de 2020** de **todas las categorías** con **términos de búsqueda** *Microsoft Teams*, *Zoom*, *Skype* y *Meet*.

Se observa en las herramientas analizadas (Microsoft Teams, Zoom, Skype y Meet), hay un incremento significativo del interés a partir del 15 de marzo (Figura 2), día en que el gobierno canceló las clases presenciales de instituciones de educación pública en el país (El Tiempo, 2020). Ese mismo día, Colombia reportó 11 nuevos casos de contagio de COVID-19 y una cifra total de 45 (Semana, 2020). Dos días después, se anunciaría el simulacro de aislamiento en Bogotá (W Radio, 2020) y tres días

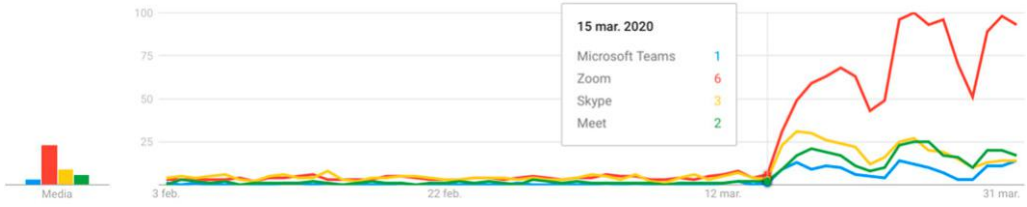


Figura 2. *Interés de Microsoft Teams, Zoom, Skype y Meet el 15 de marzo. Gráfico creado con Google Trends el 3 de abril de 2020 a las 3:01 PM.*

Figura 3. *Interés de Microsoft Teams, Zoom, Skype, Meet y WhatsApp el 15 de marzo.*

más tarde, se declararía la cuarentena total en Colombia.

Si se añade el término de búsqueda *WhatsApp* (línea morada), se observa que este también presentó un aumento en interés a partir del 15 de marzo (Figura 3).

Dada la situación del incremento en el interés y uso de varias aplicaciones tecnológicas, es pertinente analizar la cantidad de herramientas de enseñanza sobre seguridad informática que apoyen a los usuarios regulares. Con búsquedas en Google y en las tiendas de aplicaciones Google Play Store y Apple App Store, se identificó que hay muchas fuentes gratuitas de aprendizaje sobre seguridad informática en inglés; sin embargo, en español son pocas, específicamente dirigidas a usuarios regulares, limitando su acceso a esta información. Si bien los teléfonos inteligentes y las aplicaciones móviles son populares en Colombia y el mundo, la siguiente tabla demuestra que hay muy pocas apps gratuitas en español dirigidas a usuarios regulares para enseñarles conceptos básicos de seguridad informática (Tabla 2).

Nota: cabe resaltar que Google Play Store es la tienda más grande de aplicaciones para dispositivos con sistema operativo Android, el más usado en dispositivos móviles en Colombia y el mundo (Deloitte, 2019) y (Statcounter, 2020).

Por lo anterior, los usuarios regulares necesitan más herramientas educativas gratuitas y en español que les ayuden a entender los riesgos asociados al uso de la tecnología. Esto les permitirá ampliar sus conocimientos para que puedan tomar decisiones más seguras al navegar en Internet y usar redes sociales entre otras actividades con dispositivos tecnológicos (Welivesecurity by eset, 2018). Actualmente, existe la oportunidad de utilizar los dispositivos móviles, cada vez más accesibles para la mayoría de la sociedad, como herramienta para promover el aprendizaje de conceptos de seguridad informática a usuarios regulares. A este concepto de enseñanza también se le conoce como *mobile learning*.

Desarrollo

El *mobile learning* es una forma de enseñanza que busca, mediante el

Tabla 2
Estadísticas del Google Play Store

Aspecto	Cifra
Número total de apps	2'861,885
Apps educativas	254,638
Apps educativas gratuitas	238,665
Apps educativas gratuitas sobre seguridad informática	~600
Apps educativas gratuitas sobre seguridad informática en español	~250
Apps educativas gratuitas sobre seguridad informática en español dirigidas a usuarios regulares	~10

Elaboración propia con estadísticas tomadas de (AppBrain, 2020), estadísticas obtenidas con un scraper para Google Play Store (Facundoolano, 2020) y con búsquedas manuales en el portal web de Google Play Store. Los datos fueron obtenidos el 3 de abril de 2020 a las 3:26 PM.

uso de teléfonos móviles y tabletas, apoyar el proceso de aprendizaje de las personas (Universidad Politécnica de Madrid, 2013). Este esquema educativo está compuesto por tres elementos: un dispositivo móvil, conectividad a Internet y aplicaciones móviles educativas. Este tipo de aprendizaje está teniendo auge principalmente por las siguientes características o ventajas respecto a las formas tradicionales de aprendizaje (Tabla 3).

Un ejemplo de una iniciativa de *mobile learning* es TICSeguro, una aplicación móvil educativa para dispositivos móviles Android, diseñada e implementada con el objetivo de enseñar conceptos de seguridad informática. Ésta se caracteriza por ser gratuita, estar disponible en español, enseñarles a los usuarios regulares a proteger su información en línea de una manera sencilla y didáctica y tener varias lecciones en temas como Phishing

Tabla 3
Características básicas del mobile learning

Característica	Descripción
Ubicuo	Acceso desde cualquier lugar y momento
Portable	Los dispositivos móviles proveen movilidad del aprendizaje con el usuario
Activo	El estudiante tiene un rol más activo en el aprendizaje
Accesible	Su costo es más bajo en comparación con otras herramientas
Sensores multifunción	Los dispositivos móviles tienen sensores que pueden enriquecer el proceso de aprendizaje

Elaboración propia basada en la información presentada en (Universidad Politécnica de Madrid, 2013).

y redes sociales. Adicionalmente, TICSeguro le permite al usuario ver su progreso por cada lección. Esta es la vista principal de TICSeguro (Figura 4).

Existen otras herramientas basadas en *mobile learning* que buscan ayudar a las personas a aprender conceptos básicos para proteger su información en el uso de tecnología. La siguiente tabla compara TICSeguro con otras aplicaciones de *mobile learning* enfocadas en la enseñanza de la seguridad informática (Tabla 4).

Conclusiones

La modalidad de aprendizaje *mobile learning* representa una oportunidad para enseñar y afianzar conceptos de seguridad informática a los usuarios regulares por varios motivos. Uno de ellos es que cada vez los dispositivos móviles son más accesibles para las personas (sus precios se han reducido considerablemente en los últimos años). Así mismo, estos dispositivos presentan mejoras continuas en sus capacidades de hardware (memoria, capacidad de procesamiento y sensores) y software, que enriquecen los ambientes virtuales de aprendizaje con videos de alta calidad, animaciones, uso de la realidad virtual e inteligencia artificial para mejorar la experiencia del usuario. La portabilidad de los dispositivos móviles también es un aspecto a favor del *mobile learning*, porque las personas pueden acceder al conocimiento y aprender desde cualquier ubicación, incluso

Figura 4. *Vista principal de TICSeguro. Imagen propia.*

Tabla 4
Comparación de herramientas de mobile learning sobre seguridad informática

	TICSeguro	Aprende seguridad en la red	Cybrary	Curso de Introducción a la Seguridad Informática	Hackend
Origen	Colombia	España	Estados Unidos	Colombia	España
Autor	Educational Apps Dev	Junta de Andalucía	Cybrary, Inc	Platzi	INCIBE
Idioma	Español	Español	Inglés	Español	Espanol
¿A quién se dirige?	Usuarios regulares	Niños	Usuarios que quieren realizar una carrera en TI y seguridad informática	Usuarios regulares	Niños
¿Qué ofrece?	Lecciones para aprender conceptos básicos de seguridad informática. Cada lección tiene un vídeo, enlaces a recursos externos y un cuestionario	3 juegos para aprender sobre el uso seguro de las Tecnologías de la Información y Comunicación	Cursos sobre ciberseguridad, pruebas de penetración, Ethical Hacking, cloud computing y certificación CRISC entre otros	Un curso a manera de vídeos con varios módulos y laboratorios	Juego de aventura en el que el usuario juega misiones en las que aprende buenas prácticas de ciberseguridad en una empresa
Disponible para dispositivos con sistema operativo	Android	iOS	Android y iOS	Android y iOS (mediante la app de Platzi)	Android y iOS
Costo	Gratis	Gratis	Algunos cursos son gratis y otros pagos	Pago	Gratis
Ventajas	Mejora la experiencia del usuario utilizando un sensor del celular (el usuario agita su celular para validar su respuesta en los cuestionarios), incluye vídeos, cuestionarios y permite que el usuario monitoree su progreso	Se basa en juegos tradicionales como encuentra las parejas, trivias y toma decisiones	Disponible para Android y iOS, provee certificados de cursos completados y ofrece cursos en temas más avanzados	Provee un certificado por tomar el curso y tiene laboratorios	Gratis y basada en juegos
Desventajas	Disponible únicamente para Android	Disponible únicamente para iOS y enfocada en usuarios menores a 12 años	Disponible en inglés y enfocada en cursos avanzados	Se paga por su uso	Enfocada en brechas de ciberseguridad en las empresas y en niños mayores de 4 años
Link	https://play.google.com/store/apps/details?id=com.educationalappsdev.ticseguro&hl=es	https://apps.apple.com/ar/app/aprende-seguridad-en-la-red/id1080918415	https://www.cybrary.it/mobile-app/	https://platzi.com/cursos/seguridad-informatica/	https://www.incibe.es/protege-tu-empresa/hackend

Elaboración propia con datos tomados de (Educational Apps Dev, 2020), (Andalucía es digital, 2015), (Cybrary, 2020), (Platzi, 2020) e (INCIBE, s.f.).

sin tener acceso a Internet (hay aplicaciones que funcionan en modo *offline*).

Iniciativas como TICSeguro buscan aprovechar los beneficios del *mobile learning* para motivar a los usuarios a aprender y reforzar sus conocimientos sobre seguridad informática u otros temas. En el caso de TICSeguro, se utiliza un sensor de los celulares llamado acelerómetro para que el usuario verifique las respuestas de los cuestionarios agitando su celular, proveyendo una experiencia más amigable. En situaciones como la generada por el virus COVID-19 afectan las formas de aprendizaje tradicionales y han generado la necesidad de innovar y experimentar nuevas formas de transmitir conocimiento para interactuar con otras personas mediante los dispositivos móviles.

Por último, a las personas se les debe sensibilizar sobre la necesidad de auto capacitarse en temas de seguridad informática, toda vez que, a medida en que usan más tecnologías, están expuestos a más riesgos informáticos. El *mobile learning* es una alternativa más que existe para poder fortalecer el co-

nocimiento acerca de seguridad informática de los usuarios regulares. Otras iniciativas pueden ser lideradas desde las universidades, con el apoyo de entidades nacionales y regionales para divulgar campañas de sensibilización. Así mismo, aprovechando los avances de las Tecnologías de la Información y Comunicación tales como la realidad virtual y la inteligencia artificial, se pueden desarrollar más herramientas o recursos que mejoren la capacitación y sensibilización en temas de seguridad informática.

Referencias

"Aprende seguridad en la red", la nueva app para enseñar a los menores el uso seguro de las tecnologías (2015). *Andalucía es digital*. Recuperado de https://www.blog.andaluciaesdigital.es/app-aprende-seguridad-en-la-red/

Android and Google Play statistics (2020). *AppBrain*. Recuperado de: https://www.appbrain.com/stats

Build your IT and cybersecurity career from anywhere (2020). *Cybrary*. Recuperado de: https://www.cybrary.it/mobile-app/

Consumo móvil en Colombia. Los cambios importantes generalmente no ocurren de la noche a la mañana (2019). *Deloitte*. Recuperado de: https://www2.deloitte.com/co/es/pages/technology-media-and-telecommunications/articles/consumo-movil-en-colombia-2019.html

TICSeguro (2020). *Google Play Store*. Recuperado de: https://play.google.com/store/apps/details?id=com.educationalappsdev.ticseguro&hl=es_419

Se suspenden clases presenciales en todos los colegios del país (2020). *El Tiempo*. Recuperado de: https://www.eltiempo.com/politica/coronavirus-en-colombia-se-suspenden-clases-presenciales-en-colegios-publicos-y-privados-473100

google-play-scraper (2020). *GitHub*. Recuperado de: https://github.com/facundoolano/google-play-scraper

Microsoft Teams Has Seen A 775% Rise In Users In Italy Because Of COVID-19 (2020). *Forbes*. Recuperado de: https://www.forbes.com/sites/martingiles/2020/03/30/microsoft-cloud-service-775-percent-rise-covid-19/#4349adcd6862

Hackend, se acabó el juego (s.f.). *INCIBE*. Recuperado de: https://www.incibe.es/protege-tu-empresa/hackend

Curso de Introducción a la Seguridad Informática (2020). *Platzi*. Recuperado de https://platzi.com/cursos/seguridad-informatica/

Seis de cada 10 colombianos tienen acceso a internet móvil (2020). *Portafolio*. Recuperado de: https://www.portafolio.co/economia/seis-de-cada-10-colombianos-tienen-acceso-a-internet-movil-537543

Sube a 45 el número de casos de coronavirus en Colombia (2020). *Semana*. Recuperado de: https://www.semana.com/nacion/articulo/coronavirus-en-colombia-sube-a-45-el-numero-de-casos-de-coronavirus-el-pais/656988

Mobile Operating System Market Share Worldwide (2020). *Statcounter*. Recuperado de: https://gs.statcounter.com/os-market-share/mobile/worldwide

Report: WhatsApp has seen a 40% increase in usage due to COVID-19 pandemic (2020). T*echCrunch*. Recuperado de: https://techcrunch.com/2020/03/26/report-whatsapp-has-seen-a-40-increase-in-usage-due-to-covid-19-pandemic/

Slack adds 7K customers in 7 weeks amid remote-work boom, besting its preceding 2 results (2020). *TechCrunch*. Recuperado de: https://techcrunch.com/2020/03/19/slack-adds-7k-customers-in-7-weeks-amid-remote-work-boom-besting-its-preceding-2-quarters-results/

Under quarantine, media is actually social (2020). *TechCrunch*. Recuperado de: https://techcrunch.com/2020/03/21/showing-up-not-showing-off/

COVID-19: WhatsApp dominates growth of social platforms during quarantine (2020). *Tech Lapse*. Recuperado de: https://techlapse.com/global/covid-19-whatsapp-dominates-growth-of-social-platforms-during-quarantine/

Facebook is 'Just Trying to Keep the Lights On' as Traffic Soars in Pandemic (2020). *The New York Times*. Recuperado de: https://www.nytimes.com/2020/03/24/technology/virus-facebook-usage-traffic.html

Microsoft tweaks Xbox and Teams services during surge in cloud demand (2020). *The Verge*. Recuperado de: https://www.theverge.com/2020/3/29/21198673/microsoft-cloud-demand-xbox-gamerpics-disable-coronavirus-pandemic

Tendencias Cibercrimen Colombia (2019). *CCIT*. Recuperado de: http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-20 19-2020/

Guía para la implantación del Mobile Learning (2013). *Universidad Politécnica de Madrid*. Recuperado de: http://serviciosgate.upm.es/docs/asesoramiento/guia_implementacion_movil.pdf

Recursos en español para aprender sobre seguridad informática (2018). *Welivesecurity by eset*. Recuperado de: https://www.welivesecurity.com/la-es/2018/07/03/recursos-espanol-aprender-seguridad-informatica/

Claudia López anuncia simulacro de aislamiento en Bogotá (2020). *W Radio*. Recuperado de: https://www.wradio.com.co/noticias/bogota/claudia-lopez-anuncia-simulacro-de-aislamiento-en-bogota/20200317/nota/4023619.aspx

Slack hits user milestone amid remote work boom (2020). *ZDNet*. Recuperado de: https://www.zdnet.com/article/slack-hits-user-milestone-amid-remote-work-boom/

A Message to Our Users (2020). *Zoom Blog*. Recuperado de: https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

Julio Andrés Poveda G. *Ingeniero de Sistemas y Computación de la Universidad de los Andes. Asistente graduado y estudiante de la maestría en seguridad de la información en la misma universidad. Sus áreas de interés están enfocadas en la seguridad usable y privacidad. Realizó una pasantía de investigación en la Universidad de Cornell, en donde trabajó y participó en trabajos de investigación relacionados con el abuso de las tecnologías de la información y la privacidad, en el contexto de la violencia de pareja (Intimate Partner Violence).*

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

Semana Virtual
Jornada de Gerencia Proyectos de T.I.

6 al 10 de Julio
Conéctate
11AM Y 5PM

Pre Jornada	Jornada
PDU=liderazgo	PDU Liderazgo PDU Estrategia PDU Técnico

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

XX Jornada Internacional Virtual Seguridad Informática

Seguridad de la Información 20 años después, lecciones aprendidas y prospectiva de futuro

Conferencias y Taller

Agosto 26 y 27