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-

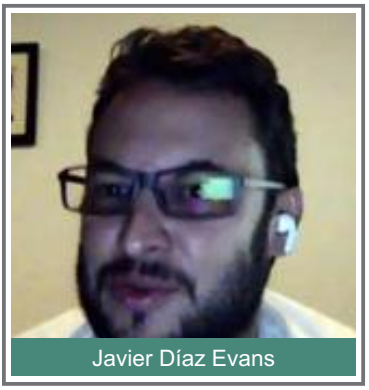
sibles funcionan los negocios de las empresas grandes, medianas y pequeñas y el resto de espacios que cobijan al ser humano.

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.*