Confianza digital: ¿Innovación confiable?

Este número de la revista está dedicado a todos los asuntos relacionados al concepto base de la confianza digital.

DOI: 10.29236/sistemas.n179a5

Los directivos de la revista Sistemas Jeimy J. Cano M. y Andrés Almanza J. dieron la bienvenida a los invitados Rafael Gamboa Serrano de Data y TIC y Víctor Vásquez Mejía, director de IT Advisory en KPMG Colombia y formularon el primer asunto a tratar.

¿Cuáles son los elementos básicos que dan forma al concepto sobre confianza digital?

Rafael Gamboa

La confianza digital es la posibilidad que tiene una empresa, una persona, un estado digital, para usar la tecnología con una expectativa razonable de seguridad, transparencia y responsabilidad.

Se trata de un sistema confiable, es decir, saber quién está interactuando con la persona. Ahí hablamos de identidad, de autenticación, de controles de acceso. Un segundo elemento es, una vez yo identifico a la persona con la que estoy interactuando, es qué estoy recogiendo o para qué lo estoy recogiendo. Entonces, ahí aparecen normas, datos personales, la 1581 de 2012, pues que obviamente establece principios de finalidad, li-

bertad, transparencia, todos estos temas. Un tercer punto que tenemos es, si el sistema es seguro, y ahí ya obviamente entran el código penal, ley 1273-2009. Un cuarto asunto es si la operación es verificable, y ahí entra un tema mucho más técnico, y se trata de todos los temas de logos, trazabilidad, auditoría, evidencia, para poder determinar que lo que se dijo fue lo que ocurrió con la persona que dijo ser, y siempre decimos eso, y es que toda la parte jurídica siempre es en caso de alguna reclamación, entonces en caso de una reclamación, una queda, llámese penal o del titular, es donde cobra muchísima relevancia estos logs, estas trazabilidades para poder generar certeza al juez, a la fiscalía o a la misma contraparte, es que usted sí lo dijo, usted sí se conectó. Un quinto punto es qué pasa si el sistema falla, y ahí es donde se dispara todo lo que nosotros veníamos haciendo, y es ver quién va a responder por esa confianza. Y digamos que quién va a responder es el que puso el sistema a disposición de las personas y cómo va a demostrar que no incurrió en el error, sino que la otra persona fue el que incurrió en el error eventualmente, y qué herramientas se suple para poder demostrarlo. Y algo muy importante que no quiero dejar pasar muy jurídicamente aceptado, pero no es menor, y es que siempre que yo pongo a disposición un sistema informático, los jueces han reconocido que yo no puedo trasladarle el riesgo por su mal uso a los usuarios, valga la redundancia. sino que si yo pongo a disposición al sistema, yo tengo que responder por ese sistema, inclusive, como digo yo, contra la propia inversibilidad de los clientes. Entonces veíamos por eso es que cuando había una, toda la época del phishing, que decía, oh, es culpa suya, oh, usted se fue a engañar, oh, es que el sistema falló por allá en la porra, dicen, no es problema mío, usted me responde por ese sistema. Y eso es algo bien importante, sobre todo a la hora de poner a disposición sistemas informáticos. En otras palabras, un sistema confiable no es solo el que no se cae. Un sistema confiable es el que puede explicar lo que hizo. bien o mal, pero poderlo soportar.

Víctor Vásquez

Desde una visión de aseguramiento, todas las organizaciones se montaron en la ola de la transformación digital. Desde esa perspectiva ¿qué están generado? Servicios digitales, herramientas y eso al final, ¿qué es? Implementación de cualquier tipo de tecnología. Hoy el gran reto es cómo aseguro que todo lo que yo saque a producción para prestar un servicio o mejorar algo en cualquier organización lo puedo hacer de forma que sea confiable que sea segura y que tenga una serie de elementos. En el tema de la ética y transparencia se enmarcan muchos de los elementos que mencionaban anteriormente

que son como una especie de dominios que hay que trabajar para que definitivamente cualquier servicio aplicación o herramienta o tecnología que se implemente en una organización pues cumpla con eso. Que sea confiable para los diferentes stakeholders que la puedan usar utilizar o necesiten algo de esta tecnología en las organizaciones.

Andrés Almanza

Entonces ¿se podría utilizar confianza como un reemplazo sustituto de confianza seguridad y al revés? porque ambas posturas me llevarán a decir en algún momento que un sistema confiable podría transmitir la idea de qué es seguro y un sistema seguro podría transmitir la idea de qué es confiable y eso podría crear algún tipo de tensión en las organizaciones y podría también ser trampa.

Jeimy J. Cano M

¿La confianza digital es un concepto interdisciplinario? ¿Hay que convocar especialistas de diferentes áreas para darle sentido y profundidad al concepto aplicado en una organización?

Víctor Vásquez

En mi opinión hay que interactuar con diferentes personas en las organizaciones. Esto no es solo de seguridad, no es solo de tecnología, no es solo de auditoría, sino que ahí tienen que intervenir varias funciones dentro de una organización, dentro de un marco organizado, para poder implementar cualquier tecnología. Inclusive ISACA propone que un comité específico de Digital Truth, donde intervengan diferentes áreas de la organización. Y definitivamente sí es interdisciplinario.

Rafael Gamboa

La confianza digital no la construye una sola disciplina, no lo podría jamás constituir una sola disciplina, ni únicamente los ingenieros, ni solo los administradores, sino es una conjunción de elementos para donde tenemos. Entonces, procurando no extenderme mucho, digamos, ahorita que andamos mucho con tema financiero, uno dice, oiga, ¿cómo es el sistema? O sea, cuando uno dice el sistema, ¿qué es? Es que el sistema por quien está constituido. ¿Quién se inventó la arquitectura? ¿Quién la diseñó? Un in-

geniero, clarísimo. Pero el abogado es el que tiene que revisar la legitimidad, digamos, del tema de los datos, del tema contractual, de los impactos que tiene ese sistema o el cumplimiento normativo. Así no haya norma, ¿no? que eso es algo bien importante, no sé, solo con el tema de la inteligencia artificial, no está regulado, y yo soy de los que digo que jamás va a estar regulado la inteligencia artificial, lo cual no quiere decir que no vamos a utilizar esa herramienta, porque la vamos a seguir utilizando, sin lugar a dudas, en Colombia y en todos los países hay regulación de inteligencia artificial, y que un abogado diría, no la puedes utilizar, eso no va a pasar, o sea, claramente lo vamos a seguir utilizando, entonces el rol del abogado un poco es Cómo ser ese puente, cómo ser ese, cómo si lo hacemos con algo muy importante y es lo que se conoce como la mitigación del riesgo. Pero ese es otro elemento que se lo adjudica otra persona al gobierno. Entonces tenemos el ingeniero, el abogado que revisa y el experto en seguridad informática identifica las amenazas.

Porque por cuenta del halo del UX, como nos dicen a las abajadas, es que usted no le puede preguntar tantas cosas porque afecta al UX.

Entonces uno es como, ¿usted quiere engañar a la persona? Porque más allá de llevarlo a un tema va a generar una... desconfianza en el sistema en el producto en el proveedor y eso es un tema muy delicado que debe estar alineado el experto de el diseñador de experiencia el quinto importantísimo es el gerente es el que define el apetito del riesgo el callo que tenga ¿sabe qué? no fuimos me importa un carajo voy a decir que esto hace y deshace.

Y usted ingeniero, hágame caso, abogado me lo paso por la galleta, el experto en seguridad informática no me importa porque yo lo que quiero es esto. Y ese es el que en últimas va a decir qué tanto voy a hacerlo o va a ser el gerente que dice no, yo tengo que cumplir y hasta que no haya una ley específica de la República de Colombia o de Venezuela o de Panamá donde diga cómo puedo utilizar los sesgos algorítmicos de la inteligencia artificial, no voy a hacer nada.

Pero está el negocio por otro lado. Y finalmente, la alta dirección que decide si la innovación está alineada con la promesa de valor de la empresa. Oiga, nosotros sí vamos a hacer esto. Nosotros estábamos en un banco las semanas, 15 días, que decía, si mi cliente tiene la posibilidad de tener una mejor oferta, que se vaya para otro lado, porque yo soy un banco enfocado en social y si yo no tengo la capacidad ni las herramientas técnicas, los dejo libres, y uno dice, chévere, y otros bancos dicen, no, yo voy a retener a este cliente de patas y manos, en-

tonces, claro, un error es creer que la confianza digital solo es un tema tecnológico, no lo es, es un sistema, hace parte de todo lo que se tiene, y básicamente lo que uno dice es, no sé, en un tema de scoring, que en este tema de scoring el ingeniero es el que dice qué modelo predice bien, el abogado es el que dice si los datos fueron escogidos legítimamente, el de negocio dice cómo pudo mejorar sin aumentar el riesgo y el de experiencia dice si entendió por qué fue rechazado o no y finalmente cómo puede mostrar que no hubo una discriminación en un tema tan complejo donde hay una norma y una tendencia que se llama la transparencia algorítmica donde la Corte Constitucional ha dicho, usted tiene que decirme por qué llegó a ese resultado. Y cuando miramos ese resultado de un scoring de crédito, es súper complejo porque hay un know-how, hay una... Y lo decíamos, obviamente, sin nombres, es porque a mí no me gustan darle crédito a los abogados. ¿Por qué? Porque yo sé que los abogados son mala paga. ¿Es legítimo? Sí. ¿Es legal? Sí. En mi negocio, yo soy un profesional y tengo que proteger de la mejor manera recursos que no son nuevos, que no son míos. Entonces, pues la confianza digital no es solamente código, no se vive solamente el código, sino cómo ese código afecta derechos, decepciones y expectativas humanas. Es como lo que uno tiene ahí en su concepto, entendiéndolo como un todo.

Jeimy J. Cano M.

Entonces el tema de la transparencia algorítmica hasta cierto punto es válida, pero cuando hace elaboraciones muchísimo más profundas y mucho más detalladas, pues posiblemente no vamos a entender ni vamos a poder seguirle el paso a cómo se ejecutan esas redes neuronales de aprendizaje profundo no sabemos exactamente cómo lo van a hacer. Hay momentos en que se nos pierde, se nos pierde completamente, desde el punto de vista técnico.

Andrés Almanza

En mi opinion surge otra pregunta que queda ahí en el aire y es qué sería de las cosas, qué tendríamos que pensar de cara a un futuro. O sea, porque apenas escuchándolos empiezo a decir, ok, sí, estamos en el presente, pero el futuro nuestro, yo estoy de acuerdo

con los dos. La transparencia algorítmica se va a perder, sobre todo Jeimy que lo menciona como muy explícitamente. se va a perder y se va a seguir degradando en la medida en que sigan creciendo nuestras redes neuronales, a punto en donde en algún momento tendremos que pensar si vamos a prescindir de la transparencia inclusive para poder seguir hablando de confianza o si no lo vamos a tener que pensar. De hecho, una de las cosas en la misma línea de Rafael es que si uno no le hace mantenimiento al algoritmo, el algoritmo se degrada.

De hecho, eso es una de las recomendaciones cuando uno tiene inteligencia artificial por lo menos generativa funcionando. Si uno no le hace mantenimiento al algoritmo, el algoritmo cada vez más va a responder menos bien, con mayor precisión con menos precisión cada vez más se va degradando el algoritmo; como diría Stephen Covey si no se afila la sierra pues no se corta bien el hacha aquí es igual entonces eso es un tema que la transparencia pone realmente un reto a la confianza digital muy importante. Porque uno quisiera que realmente la inteligencia artificial operara en un acuario, para que uno pudiera ver cómo los algoritmos están funcionando completamente hasta el final. Pero no. Llega un momento en que se nos pierden, por el solo el hecho de ejecución. O sea, inclusive los señores de OpenAI y los de Antropic dicen que llega un momento en que nosotros no sabemos por qué responde la inteligencia artificial así. No sabemos; entonces eso es un tema realmente espinoso espinoso cuando estamos hablando de confianza digital bueno,

Jeimy J. Cano M.

¿Existen marcos de trabajo concretos para desarrollar el concepto de confianza digital? ¿Conocen ustedes alguno que se aplique en Colombia?

Rafael Gamboa

Así como aquí regula todo, no, no hay, no hay una única ley de confianza digital, como se puede decir, lo que sí hay son normas que regulan las distintas etapas de esta confianza, camas, llamémosla así, entonces, pues la primera, datos personales, sin duda, todos son datos, ley 1581 del 2012, decreto 1074, que es cómo puedo manejar, cómo debo manejar los datos, que en últimas es un generador de confianza para los titulares. Una segunda capa sería, sin duda, el tema del data financiero, un tema reputacional, que ya nos brincamos a la 12.66 de 2008 para temas de obligaciones dinerarias. Una tercera capa, el tema de la seguridad de la información, Ley 1273-2009, cómo penalmente se está protegiendo todo ese tema, cómo se protege el tema del acceso abusivo, del daño informático, interceptaciones, violación de datos personales, porque es que acordémonos que esta ley sur-

ge más allá del convenio UDAPES, surge es porque Cuando empezaron este tipo de reclamaciones, la respuesta del juez dijo, y el fiscal dijo, este es un ciberdelito. Eso no está tipificado, eso no es un delito. Y por eso es que nos tocó correr a sacar eso. De hecho, yo siempre utilizo esta ley para demostrar cómo los hechos generaron la norma del derecho. Los hechos generaron el derecho, a diferencia de la ley 527, donde el hecho de tener una ley de comercio electrónico no generó automáticamente ley de comercio electrónico. La explosión. La explosión, exactamente. Siempre digo, nosotros tuvimos ley de comercio electrónico antes que Estados Unidos, y eso quiere decir que tenemos mejor comercio electrónico. La respuesta es no. Entonces aquí la 1273 surge por una necesidad de tipificar actuaciones de phishing, de hacking, de todos esos temas que se venían desarrollando pero no estaban tipificados. Una cuarta etapa es el tema de las evidencias y transacciones digitales. Claro, ahí sí nos remontamos a nuestra antiquísima ley 527 del 99, que fijó un marco interesante. Esta ley, yo siempre digo que ya tiene más papás que quién sabe quién. Lo cierto es que aquí fusilamos esta norma. Nos trajimos una serie de conceptos que siguen teniendo vigencia y que nos siguen estableciendo unos principios bien importantes sumado a decisiones jurisprudenciales donde dice, oiga, en últimas a mí lo que me tiene que generar es convencimiento al juez o a la persona que está haciendo. O sea, más allá de lo que de lo que. La prueba tecnológica es generar convencimiento a la contraparte o generar convencimiento al juez, al juzgador, al fiscal. Y finalmente una quinta capa, que por supuesto siempre hay que mencionarla, y son los CONPES. Son los CONPES el 3995 sobre confianza jurídica. Y seguridad digital o el decreto 767 de política de gobierno digital, que muy seguramente va a venir a cambiar, pero estos compes dicen por dónde nos vamos a mover. Fíjense que este Conpes trae una cantidad de cosas que se vienen desarrollando inclusive hace un mes nos terminaron sacando un decreto de Open Finance aunque el compes hablaba de Open Data terminaron aterrizando en Open Finance porque eventualmente lo que podían hacer entonces para responder en forma concreta. Si hay marcos aplicables en Colombia, lo que más falta muchas veces es poderlo integrar. Articulación es la palabra.

Jeimy J. Cano M.

Ok. Sí, interesante. Pues aquí hizo Rafael una enumeración de, digamos, de los recursos jurídicos que tenemos hoy en Colombia, ¿no? Sí, desde protección de datos personales, avias data, la ley 1273, todo el tema de la 527 y claramente los CONPES donde, digamos, se han articulado algunas de estas iniciativas a nivel nacional. Intere-

sante. Como arquitectura, ¿no? Como arquitectura legal alrededor del tema.

Víctor Vásquez

ISACA tiene o diseñó un marco específico que nos habla de confianza digital, que es el DTEV. Nace más o menos como en el 22, y lo que nos habla es de realmente un ecosistema digital confiable considerando como cuatro vertices, que son las personas, los procesos, la tecnología, la organización, y que logra integrar atributos claves para la confianza que los hemos mencionado ahí, pero mire que aquí los integra, ¿no? De una forma como organizada, habla de seguridad, privacidad, integridad, resiliencia, calidad, confiabilidad.

Entonces es un marco que busca no reemplazar lo que hay, sino integrar, ¿no? Cómo integrar lo mejor de NEEDS, cómo integrar COVID, cómo integrar, no sé, la 27.000, o esta regulación que se mencionaba a nivel local, porque a nivel local no hay nada explícito diseñado específicamente para eso, ¿no? Hay muchas, como mencionaba, normatividad que en conjunto nos puede ayudar.

Pero un marco como estos fue diseñado para eso, ¿no? Para integrar y tener una visión más holística de lo que es confianza digital en un ecosistema digital para generar confianza, ¿no?

Jeimy J. Cano M.

Entonces, yo creo que la palabra clave aquí es ecosistema, es decir, muchos actores que interactúan entre ellos para generar de alguna manera valor para aquellos que están dentro del ecosistema. Entonces, eso es como conectando un poco con la arquitectura que proponía Rafael, casi que eso tiene que articularse ¿no? o sea por ejemplo el modelo que presenta Isaac que es el DTEF que tiene todo este montón de elementos y componentes pues de alguna manera es una visión mucho más amplia y que de alguna forma cuando Rafael integra y pone toda la arquitectura legal detrás pues de alguna forma cobra muchísimo más dinámica ¿sí? porque está detrás no solamente el desarrollo de la iniciativa digital sino la responsabilidad por esa iniciativa digital que es lo que eleva el nivel de confianza final-

mente en algunas organizaciones le preguntan a uno siempre con el tema de inteligencia artificial y quien responde. Si eso falla, ¿quién responde? Que es un poco lo que precisamente comenta y articula Rafael en su respuesta.

Entonces miremos como los dos lados que hemos venido como revisando. No sé, Andrés. Ahí lo único que se me ocurre, porque creo que la palabra clave es ecosistema, y de pronto lo que yo agregaría es que en este momento ese ecosistema, para que sea mucho más confiable, articulando todas las cosas escuchadas es no existe un elemento que pese más que otro para poder desarrollar esa confianza es lo que me traigo con todas estas cosas entonces estos ecosistemas confiables son elásticos entre todos sus componentes y de todos va a depender que esa confianza aumente para producir más valor y con que uno solo de sus elementos, que sería la otra cosa, el lado negativo, si lo quisiéramos llamar, con que uno solo de sus elementos no tenga el soporte suficiente, va a generar efectos, cascada, que va a hacer que ese ecosistema en total, puede que una de sus aristas del ecosistema esté funcionando uno a la otra, si no está funcionando adecuadamente, genera esa diatriba de no hay confianza del ecosistema y por ende va a tener algún problema. La pregunta ahí podrá ser, ¿eso será suficiente para la sostenibilidad de una empresa en un entorno digital como el que tenemos y vamos a tener? El tiempo lo dirá. Muy interesante esto que hemos venido conversando. Bueno, seguimos con la siguiente pregunta. Ahora sí, centrado en el tema de inteligencia artificial y con incorporación de la inteligencia artificial en prácticamente todos los escenarios de las organizaciones y la sociedad. ¿Cómo juega la confianza digital en este nuevo escenario?

Víctor Vásquez

Pues hoy en día se vuelve más relevante hablar de confianza digital y con esos dos vértices, la ética y la transparencia, sobre todo cuando hablamos de inteligencia artificial que si no está, como decía Jamie, probada periódicamente, evaluada, alineada, pues puede generar muchos resultados no deseados, porque lo pienso para... para algo, pero si no le implemento como sus límites, su marco, el tema, hoy se está hablando mucho del gobierno, cómo gobernar la IA, o sea, cómo llegar a implementarla de forma más confiable en las organizaciones para ayudar a que se obtengan los objetivos que quiere la organización.

Entonces definitivamente se vuelve más relevante hablar de confianza y hablar específicamente con la idea de transparencia y de ética, ¿no? Cómo usamos éticamente las diferentes herramientas y que vemos que esto va evolucionando

muy rápido y hablamos de algo... Y ya en ocho días ya el panorama evoluciona muy, muy, muy rápido.

En eso encaja muy bien el marco de ISACA y prácticamente hace dos años ya se está desarrollando y mostrando como este marco podía ser utilizado para empezar de forma organizada a trabajar con este tipo de tecnologías emergentes que ya hoy en día se volvió más masiva ok, solo una pregunta adicional Víctor, ahí en el marco de ISACA de alguna manera se detalla los componentes por cada uno de ellos y de alguna manera como las métricas, pues, muestra unos dominios que hay que abordar, básicamente, y como ya hay varios papers de cómo utilizar este marco para las implementaciones de IA de forma confiable, pero al final es hacerlo con un gobierno, con una organización, con un método.

Jeimy J. Cano M.
La ventaja de este marco es eso, que da como unos lineamientos, unos dominios, unas áreas, unas funciones que hay que contemplar para implementar la IA o cualquier tecnología.

Rafael Gamboa
Claro, ustedes saben, y Jamie que me conoce tanto, y Ricardo, yo soy ingeniero wannabe, pero uno dice, claro, una información jurídica, pero ¿cómo funciona? Entonces, claro, uno dice, pues, es que antes la tecnología almacenaba y transmitía información, y me acuerdo muchos años en que decía, oiga, me va a quitar el trabajo la firma digital.

Y me decía, no, pues no, internet me lo va a hacer el trabajo. Ahora no solo almacena ni transmite, sino que recomienda, previse, clasifica y hasta decide. Entonces, claro, uno coge al ingeniero y los ingenieros dicen, oiga, ¿y ya? Ya no, pues ya, pues fácil, va a sacar dependiendo de los datos, del modelo, de los parámetros, del entrenamiento, de la inferencia y el monitoreo. O sea, Uno más uno es dos.

O sea, más o menos va a salir ahí porque son elementos muy, entre comillas, tangibles y claros, aunque no lo son. En cambio, usted le pasa la misma pregunta al abogado y le dice, es que la respuesta de la IA tiene que tener en cuenta si los datos eran legítimos, si eran ciertos, lo que se llama la contaminación de los datos, ¿quién revisa eso? Jurídicamente lo revisaron, nadie lo revisa. Oiga, ¿la finalidad fue informada a las personas para que lo utiliza? Si hay un modelo que eventualmente pueda discriminar, así sea legítima esa discriminación, si lo había, si estaba identificado y las empresas contrataron con esos parámetros y quedaron así en el contrato. Si el resultado es explicable, lo que pretende la Corte Suprema, la Corte Constitucional con la transparencia algorítmica, usted tiene que decirme por qué me rechazaron el crédito, si hay intervención

humana o no, o si todo fue automático, porque lo que dice la Corte Constitucional es donde haya un byte de decisión automática, usted tiene que decirme por qué lo explicó. ¿O cómo llegó a esa conclusión? ¿Y quién va a responder en caso de error? A mí no me vaya a decir que es que, que jueque, que jueque, que no. Usted es el que tiene que responder. Que jueque, que jueque, que usted es el que tiene que responderme. Y finalmente, ¿cómo vamos a auditar la decisión? La transparencia está muy en línea de la auditabilidad de las decisiones a las que llega.

Y hay unas decisiones vía revisión constitucional que está diciendo que cualquier entidad jurídica pública que maneje recursos públicos, público privado que maneje recursos públicos, tienen que tener la capacidad de poder explicar y auditar y ser auditables las decisiones, lo cual se vuelve súper difícil. Entonces, en Colombia hay alguna regulación puntual. No, no la hay. Digamos que todos los proyectos están en línea de lo que dice Europa. La Unión Europea, lo que es el reglamento europeo de la IA. Y uno dice, ¿por qué? Porque allá son Dios y allá saben todo. Y uno dice, no, el efecto Bruselas es absoluto no, porque claro, en Latinoamérica consumimos mucha normatividad europea, digo yo, por el idioma, porque nos llega todo a través de España, pero lo cierto es que allá en Europa ya le levantaron la mano y ya hay una serie de proyectos conocidos como Omnibus Digital, donde para el tema de datos personales y para el tema de regulación de inteligencia artificial, dice, oiga, no me ponga ese... Un universo fantástico Disney, porque es que se vuelve imposible negociar.

Entonces, cuando uno mira el mercado, uno dice, ¿quiénes son los líderes? China y Estados Unidos. ¿Quiénes son los líderes en inteligencia artificial? China y Estados Unidos. ¿Quién es el que más regula? Europa, que ni siquiera es líder, que ni siquiera tiene la potencialidad de ser líder por temas presupuestales y por temas de desarrollo. Entonces, ahí es donde uno sí tiene que aterrizar desde el punto de vista latinoamericano, cómo es que vamos a manejar. Entonces, ¿cómo se maneja el tema de la confianza? Lo mencionábamos anteriormente con temas de protección de datos, avías data, seguridad digital... Los compes, etcétera, etcétera. Entonces ahí es donde uno dice el reto no es que el modelo responda. A mí no importa que el modelo funcione o no funcione, sino a mí como organización lo que más me importa es que pueda responder por el modelo, saber responder. ¿Por qué dijo uno o dos? ¿Por qué fue que lo dijo? Ese es, digamos, el gran reto y desafío y de ahí no nos van a sacar a los jueces y de ahí no nos van a sacar a los abogados. Yo a tener que explicar algo que eventualmente es inexpli-

cable, como decía ahorita Jamie, y es que yo ni siquiera sé por qué llegó, porque hay muchísimas concusiones de información y si a esa data original o real le sumamos todos los sistemas de alimentación de data sintética, pues va a ser imposible, no difícil, imposible.

Entonces, pero tenemos que tener claro que los jueces no se van a mover de ahí. Van a decir usted tiene que explicarme y el desafío es yo como organización, cómo voy a poder demostrar o convencer al juez o al supervisor regulador que sí sé lo que está haciendo mi sistema y por qué lo está haciendo.

Jeimy J. Cano M.
Aquí se hace evidente el tema de la confianza ese tema de que hay un tercero que tiene una identidad no humana que está ayudando a hacer cosas y que de alguna manera respondiendo a una programación respondiendo a unos datos propone elabora, diseña y como decía Rafael hasta decide Y ahí sí, claramente, cuando hablamos de decidir sobre un campo específico, pues claramente los efectos se tienen que colocar sobre la mesa con claridad, porque lo que está en juego es algún tercero o algún derecho que se vaya a vulnerar.

Andrés Almanza
Fundamental lo que yo creo que también rescato, porque me conectó mucho las palabras de Víctor. Y tomando tus palabras, Jeimy, el tema de gobernar, ¿se va a volver o se vuelve para fortalecer esa confianza? O sea, un instrumento que sí o sí no podemos, dado la IA, necesita hoy con tantas capacidades que puede desarrollar, inclusive decidir, necesitará, no digamos que un bozal freno, pero yo veo lo que menciona Víctor, como el instrumento que sí puede, sí o sí, han coincidido casi todos los expertos, es decir, la IA para que sea estructurada, eficiente, pueda tener unas implicaciones y no tenga tanto dolor como a veces lo vemos, necesita ser gobernada. como un instrumento fundamental que va a apalancar esa confianza dentro de todo el ecosistema entonces yo creería que habría que hacer un resalto de gobernar la IA va definitivamente a apalancar como esa confianza que va a tener que plasmarse en todo el ecosistema si de hecho hay una frase que dice recientemente dice el problema no es incorporar la inteligencia artificial sino como gobernarla y a que velocidad

Jeimy J. Cano M.
Y a qué velocidad, correcto. Y a qué velocidad. Y eso es realmente el gran reto que hay de aquí detrás, ¿no? O sea, y el marco que la debe cubrir precisamente para poder habilitar todas sus posibilidades que podemos tener de aquí en adelante. Entonces, es realmente interesante, digamos, las dos posturas, muy en assurance, muy en legal, pero tienen una línea de convergencia, ¿no?

Y vamos ya para ser juiciosos con el tiempo a la quinta y última pregunta. Dice, ¿qué recomendaciones darían a los ejecutivos de tecnología y gerentes de empresa para apropiarse, es una palabra bien importante, del concepto de confianza digital? ¿Cómo mostrar que es un concepto clave y relevante para la promesa de valor digital de la empresa.

Rafael Gamboa

Hay una serie de recomendaciones aunque suena pero sí temas a tener en cuenta lo mejor que obviamente lo digo desde el punto de vista de abogado con un algo de conocimiento técnico. Y en últimas, de los riesgos que tienen las organizaciones, porque insisto, un abogado sobre todo es el enfoque litigante y lo que hemos visto siempre en las organizaciones, los contratos, todo nuestro enfoque es cuál es el real riesgo. A mí donde me pongan en un contrato que es que si me incumple se va a ir a la cárcel la resta de la vida. Yo no me mato por eso porque es una cláusula claramente y absolutamente ilegal que en el escenario judicial pues nunca va a prosperar. Pero aquí sí es importante entender varios puntos. Uno, dejar de creer que la confianza digital es un asunto, está en el aspecto legal, es decir, que el contrato es lo único y que va a definir, o sea, que la confianza digital es un asunto de cierre, legal de cierre, es decir, que yo hago un contrato y que con eso ya fue suficiente sin fijarme en las otras condiciones del producto, cómo está construido, cómo está la tecnología, porque es que el papel aguanta todo y eso hay que tenerlo súper claro. Si a mí me ponen a escoger entre tecnología y papel, pues casi que prefiero es la tecnología que el papel yo como hago para evitar que cumplan las lo iba dudando lo iba dudando no no no yo soy super ayatol en eso digo si y con Jeimy hemos compartido muchos foros donde a uno le preguntan es que me están negando mi derecho a la información porque me tienen bloqueado internet yo digo bloqueelo es el mejor sistema para que le cumplan su política de internet o sea ¿Que eso es ilegal o es ilegal? No sé, es un tema donde yo, si yo no implemento herramientas tecnológicas y ocurre algo, lo primero que me van a decir es ¿por qué no implementó herramientas tecnológicas? Y me van a calificar de negligente por no haber utilizado esas herramientas tecnológicas. Y ese es un tema súper, súper sensible, pero real. No solo ver lo que dice la norma fría en un papel, sino ¿qué pasa si? Un segundo punto es documentar las disecciones técnicas. Eso es importantísimo, uno lo ve todos los días, es, oiga, ¿usted por qué decidió eso? ¿Quién lo decidió? ¿Para qué lo decidió? Nadie tiene ni idea y ese es un leak, esa es una falla que siempre las organizaciones tienen, es que no documentan todas las decisiones mediante logs, mediante evaluaciones de impacto de

privacidad, bitácoras de cambio, nada de eso, nunca queda documentado y ese es un tema que cuando ocurre se vuelve supremamente relevante. Tres, hacer privacidad, seguridad e inteligencia artificial desde el diseño. Trabaja desde el diseño, no, sino cuáles son los requerimientos funcionales, cómo vamos a minimizar el tema de los datos, el control de acceso, cómo vamos a manejar eso desde el momento cero, cómo lo vamos a implementar desde el momento mismo del diseño, como su mismo nombre lo dice. Un cuarto punto es traducir cumplimiento a controles técnicos si bien dijimos que no todo va a estar regulado hay normas y esas normas hay que cumplirlas gusten o no, hay normas entonces como decía un profesor de procesal en la universidad la ley tiene vacíos pero el derecho no, el derecho tiene que entrar a regular esa realidad de la inteligencia artificial tiene que entrar a regular esos vacíos o esas incertidumbres tecnológicas y ahí es donde entran elementos como debida diligencia, negligencia experiencia, profesionalidad que es algo que utilizamos doctor Jamie usted es un profesional usted tiene que saber así no se le ocurra usted es el profesional yo no sé y es usted el que tiene que saber entonces eso es algo bien importante y que toda esta semana hemos estado precisamente en ese tema diciéndole a unos profesionales que usted no me diga que no sabe porque usted entre los dos usted es el que sabe entonces es un tema bien importante de entender esa traducción de normas profesionalidad a cómo lo manejan lo manejan medir la confianza, entender cuál es el apetito del riesgo de la organización. Es importantísimo.

Aquí no trabajamos en escenarios dignos, sino cómo lo vamos a manejar. Y algo que suena casi que obvio, pero que nadie utiliza, y es creen un comité pequeño, tres personas, que hagan seguimiento y actualicen todos los temas. ¿Por qué? Porque es que las cosas se firman y nadie volvió a ver ese proyecto, nadie volvió a manejar esa herramienta, y lo que sí nos ha demostrado la experiencia es que cuando hay un seguimiento, no digo diario, semestral, quincenal, no, semestral es mucho, quincenal o mensual, sí podemos advertir los riesgos, porque están cambiando todo el tema y en inteligencia artificial, lo que era la locura, o sea, es que lo hablábamos en Open Finance, hace tres años nadie hablaba de Open Finance, perdón, nadie hablaba de inteligencia artificial, hoy por hoy nadie deja de hablar de inteligencia artificial.

Entonces, claramente los ingenieros son los que construyen los sistemas, pero son los abogados los que ayudamos a que estos sean sostenibles, defendibles y legítimos. Es la única manera en la que podemos procurar utilizar una herramienta que no va a estar regula-

da, pero que no podemos hacerle el quite. Uy, yo ahorita, Rafael, yo creo que esas se las voy a robar de esas tres palabras que acabo de decir, que son claves, sostenibles, defendibles y legítimos. La inteligencia artificial tiene que cumplir esos tres.

Y en ese sentido, los abogados tendrán que trabajar de manera interdisciplinaria, claramente ingenieros y todos, alrededor de esas tres palabras para darle carnecita. Es decir, qué significa defendible, qué significa sostenible y qué significa legítimo.

Hay muchas disciplinas conjugadas para darle... digamos marco a ese ejercicio final de de cómo se llama de esas recomendaciones casi que que es el las recomendaciones para el ejecutivo oiga ponga en su comité a trabajar alrededor de estas tres palabras y de la forma para que no para que nosotros podamos decir mire cuando hablamos que nuestra inteligencia artificial es sostenible, defendible, legítima hablamos de esto eso es como un marco casi que de debido cuidado guardada proporciones o no Rafael, tal cual.

Y no son tomas jurídicas y no son tecnológicas, son transversales. Las dos le aplican en distinta óptica, pero le aplica definitivamente en la necesidad técnica y en la necesidad jurídica. Interesante, muy interesante.

Víctor Vásquez

Darle como un nivel, llevarlo a nivel estratégico, ¿no? Pensando que eso habilita crecimiento, temas de reputación, sostenibilidad, entonces hay que involucrar eso en el plan estratégico, en el gobierno corporativo, en las agendas de las juntas directivas, del comité de auditoría, o sea, tiene que subir de nivel, ¿no? Y ser top down, ¿no? Desde arriba hacia abajo.

Lo otro es que hay que ponerlo también, porque nos ponemos muy técnicos, y a esos niveles se pierden, ¿no? Entonces hay que hablarle en términos de negocio, ingresos.

Si los clientes confían, pues van a pedir más o a cobrar. me va a ayudar pues en temas de negocio, ¿no? Me compran más y pueden que con esa confianza pues sigan con mi organización.

En temas de riesgo, pues sí, si tengo menos riesgos, pues tengo menos pérdidas, sanciones. En temas de cumplimiento, pues voy a tener menos multas. En temas de reputación, pues me va a mejorar la ventaja competitiva.

En innovación, pues voy a tener más confianza dentro de mi organización para implementar nuevas tecnologías como la IA. Lo otro tiene que ser un tema integral, porque a veces todos estos temas de tecnología se piensa como en TI,

cuando se piensa en aseguramiento, se piensa en auditoría, y se piensa como aisladamente, ¿no?

Entonces, esto es un tema integral, ¿no? Que contempla varios... varios dominios y que no puede ser no puede ser aislado solo la responsabilidad para TI y finalmente pues digo los marcos pues son para utilizarlos entonces hay que lo llamaría a los ejecutivos y hay una documentación muy sencilla, muy fácil para ejecutivos de lo que es este marco de Digital Truth, entonces también pues leerla y no inventarse la rueda, porque queremos inventarnos la rueda y ya varias personas a nivel global se sentaron, pensaron, hicieron los planteamientos, entonces hay que utilizar eso, ¿no? No inventarnos la rueda, sino tomar eso y mirar cómo lo adapto a mi organización con algo lógico, ¿no? Un método de cómo hacerlo más fácil sin inventarme algo nuevo, ¿no? Ya está definido, pues utilicémoslo, ¿no? Y leamos más el tema, ¿no?

Jeimy J. Cano M.
Entonces, mire, yo creo que aquí, y quiero retomar y cerrar con esta pregunta, porque es un concepto que lo introdujo Rafael, que era el tema del apetito de riesgo. Y ese apetito de riesgo creo que podría ser como el elemento base para poder llegar a la confianza digital.

Es decir, en la medida en que yo tengo claro cuál es mi apetito de riesgo, y tengo claro qué capacidades tengo para responder frente a ese apetito de riesgo, pues así voy a construir mejor mi confianza digital.

Rafael Gamboa
Nosotros lo hablamos formal e informalmente con los clientes, decimos, oiga, ¿cuál es su apetito del riesgo? ¿Cuál es su ADN de la organización? Que también es cierto, hay organizaciones, hay empresas que son muy jurídicas, y si nuestra ley no está, hay unas que son absolutamente comerciales, diría que la mayoría... Y hay otras que son muy tecnológicas y dicen, pues yo lo hago, pero lo cierto, y siempre hablamos en la oficina del trilingüismo, de entender de dónde saca la plata el negocio, cuál es el valor de la tecnología, entendida que la tecnología solo es útil si aumenta utilidad y reduce costos, y cuál es el marco jurídico, es decir, dónde nos vamos a mover. Y una consideración final que dicen, no, yo soy muy respetuoso de la ley, todos somos respetuosos de la ley, pero desde el punto de vista jurídico, legal, nadie debería tener ni nube ni redes sociales. ¿Por qué? Porque lo que se establece en los términos de uso de la nube o de las redes sociales, cuando estamos hablando de los grandes proveedores AWS, Azure, Huawei, lo que quiera, dice que cualquier disputa, legislación extranjera. Y es lo mismo que dicen las redes sociales. Entonces, desde el punto de vista

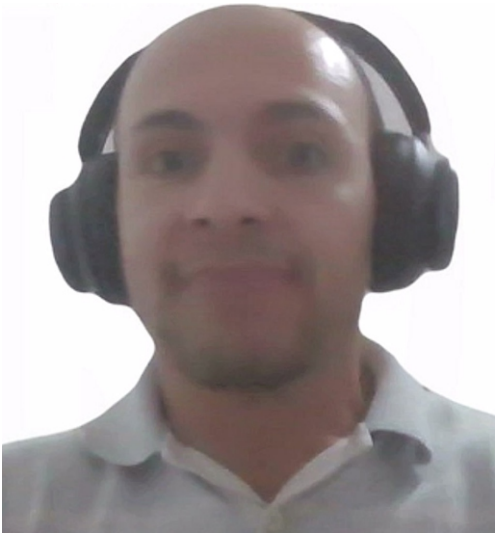
legal, exegético conservador, uno no debería tener ni nube ni redes sociales. ¿Quién no va a tener nube ni redes sociales? Nadie. El mismo Estado dice, ni loco yo voy a hacer eso, voy a dejar de utilizarlo porque es una necesidad. Entonces, ¿cuál es mi riesgo? Cuando hablamos de entidades públicas, decimos mi objeto misional, ese es mi riesgo, mi objeto misional se potencia con redes sociales y con nube y cuando hablamos de entidades privadas mi objeto misional es generar utilidades. Entonces yo no voy a tener todo on-premise, súper inseguro, cuando puedo tener muy buenas alternativas comerciales y lo que hago es mitigar el riesgo. Yo como compenso el apetito, lo compenso con la mitigación del riesgo, mitigación técnica, mitigación jurídica, información a los eventuales afectados y a las autoridades, y fue básicamente lo que hizo la superfinanciera que tuvo la oportunidad de trabajar hace varios años cuando expidió la circular de tercerización de servicios dijo señores llegaron a regular una situación que ya existía y era que todo el mundo ya estaba subido en la nube pero la superfinanciera dijo oiga vigilados supervisados usted quiere tercerizar servicios pero dentro de las muchas cosas que debe tener de seguridad claridad arquitectura es que en caso de toma de control

Víctor Vásquez
Yo como supervisor, usted va a firmar Banco X con un proveedor, va a firmar un otro, donde me permita a mi supervisor acceder a su datacenter, a su información, inclusive en su contra. Entonces hoy por hoy todos tienen que firmar cuando contratan con un proveedor de nube, tienen que firmar y negociar con el proveedor de nube que en caso de toma de control le deben dar acceso a la superfinanciera.

Y eso es simplemente la mitigación de un riesgo de tercerizar a una empresa que no tiene presencia ni está sometida a autoridad colombiana a ver yo cómo esta autoridad pudiera cumplir su objeto misional que es mantener seguridad y confianza en el sector asegurador.

Jeimy J. Cano M.
Muy interesante. Víctor. Yo creo que desde un planteamiento de riesgos es como ese acercamiento que decía yo a términos de negocio, ¿no? De cómo se mide el riesgo en cada organización y que los impactos positivos y negativos de confiar o no confiar en la tecnología se vuelve un tema que podrías llegar desde ese punto de vista a acercarlos al negocio y ser más conscientes de que hay que trabajar en estos temas desde el punto de vista estratégico, teniendo ese entendimiento de cuál es el riesgo que quiere cubrir la organización y sus temas de tolerancia y apetito para efectivamente implementar o no, o trabajar con con esta tendencia, este término de confianza digital.

Andrés Almanza



Sí, el apetito de riesgo, porque a mí me gustó mucho lo que decía Rafael del tema de el solo objeto social ya define el criterio del apetito, que fue como yo lo entendí. Entonces, eso me parece como una vista muy interesante. Porque también llamará a que las empresas entiendan cuál es el objeto social, por lo menos en las privadas, que es donde más está hacia el lado comercial, si ese puede ser el marcador definitivo. Porque al final lo que tú estás planteando es, si la empresa conoce su apetito y lo tiene claro, pues va a modelar mejor ese factor de confianza.

Entonces, si vamos más atrás, entonces es lo que está diciendo Rafael, Para acercarlo con lo de Víctor, acercarlo al nivel ejecutivo, se está conociendo bien la empresa, su objeto social en los términos más profundos posibles para que ese apetito de verdad sea con claridad y no sea simplemente como decir, bueno, sí, yo tengo un alto apetito al riesgo, pero tú no sabes qué es alto apetito al riesgo en el momento de la crisis. El apetito al riesgo yo lo dejo escrito en la ley de papel, pues sigue funcionando. Alto apetito al riesgo, pero eso no lo sabemos sin entender mejor el concepto del objeto social, que creo que es un interesante indicador que podría dar una pauta verdaderamente real de cuánto puede ser ese apetito real.

Jeimy J. Cano M.

Bueno, yo creo que vamos cerrando este ejercicio y quisiera que cada uno hiciera como su mensaje de cierre, de síntesis de lo que hemos conversado y con eso vamos cerrando nuestra sesión. Entonces no sé quién quiere empezar con su reflexión final sobre esto que hemos conversado.

Víctor Vásquez

Sí, creo que definitivamente toca buscar más espacios como estos y subirle el nivel para que generar más conciencia. Realmente se está hablando poco, ¿no? Sabemos que es importante, pero no está teniendo la relevancia que debería tener hablar más y en diferentes niveles de este tema de confianza digital y realmente sí es un tema relevante para los negocios, ¿no? Para generar negocios hay que tener confianza, ¿no? entonces creo

que eso es mi mensaje que hay que trabajar más en espacios como este o espacios académicos para generar más iniciativas y que esto coja mayor tracción y se utilicen los marcos que existen actualmente como el DT de Isaac

Rafael Gamboa

Siempre he pensado, he dicho que la confianza es el activo más importante de cualquier organización. O sea, la gente compra, hace o deja de hacer con determinada organización por la confianza que le tiene. La gran oportunidad de mejora o el gran riesgo que tiene cualquier entidad es la parte tecnológica. A mí el sistema me falla, pierdo confianza, se pierden clientes, entonces ya no se trata solamente con que la tecnología funcione, sino que adicionalmente pueda estar complementada, soportada por el tema de la por el tema jurídico, porque necesariamente vivimos en un entorno jurídico y debo cumplirlo.

Andrés Almanza

Coincido con las dos visiones. Me gusta lo de Víctor de buscar más espacios y yo ampliaría en que los espacios con múltiples actores. Creo que una de las conclusiones fundamentales de hoy es definitivamente ecosistemas, multidisciplinaridad. Son dos aspectos claves de cara a lo que hoy estamos viviendo con la acelerada realidad que vivimos. Gobernar un ambiente denso, con la IA de por medio, con lo que se viene con Quantum. Entonces la confianza definitivamente es algo esencial, no para la seguridad, sino para la sostenibilidad de un negocio. Yo creo que lo de Rafael y sus tres pilares hacen o le ponen un marco importante a la confianza. La confianza hay que hacerla sostenible y legible.

¿La otra cuál es? Sostenible, defendible y legítima. Entonces la confianza hay que hacerla legítima, defendible y sostenible. Y yo creo que ahí hay un interesante framework que tendremos que explorar, desarrollar a través de un marco cualquiera que este sea, hoy por hoy, pues el de Isaaca, que es uno de los que más se conoce, cualquiera que sea, pero tenemos ahí un punto clave que de cara al futuro de los negocios tendrá que ser tenido en cuenta en todos los escenarios. Y como lo dices tú, Jeimy, sobre todo en esos ambientes ejecutivos donde este tema debe ser más una conversación continua. ¿Cómo vamos a hacer sostenible la confianza de nuestros clientes?