Reflexiones de un experto en plena pandemia

DOI: 10.29236/sistemas.n155a3

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

Sara Gallardo M.

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

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

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

García Márquez en “Cien años de soledad”.

Desde su residencia en Seattle atendió la entrevista.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

***RS:** Y, sobre la ética que debe cobijar esos desarrollos, ¿qué opina?*

JEC: La ética jugará un papel preponderante. En Francia se acaba de anunciar un esfuerzo en esa dirección a través de la inteligencia artificial. Ocupará las primeras filas en los debates para proteger la información y los derechos de los ciudadanos, en el marco del uso seguro de la tecnología. Esta crisis disparará tales temas.

***RS:** ¿Cuáles serán los principios que regirán en términos de seguridad y ciberseguridad?*

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

***RS:** ¿En qué no se pueden equivocar los responsables de la función de seguridad/ciberseguridad para ser exitosa en los próximos 10 años?*

JEC: Con relación a los usuarios, no podemos olvidarnos que la ciberseguridad es para empoderar e influenciar las decisiones en las organizaciones y las entidades de cualquier naturaleza. Tenemos que despertar credibilidad en los directivos de las compañías sobre la importancia de nuestro trabajo y el alcance que tiene en el negocio.

***RS:** Desde su perspectiva, ¿cuál será la transformación más significativa en seguridad y ciberseguridad que producirá esta pandemia?*

La habilidad de estar preparados, la capacidad y la competencia de escuchar a los clientes y responder rápido. Zoom es el mejor ejemplo, las fallas de seguridad que tuvo la aplicación, fueron solucionadas, la compañía reconoció los problemas, trabajó sobre ellos y suministró una rápida respuesta para no afectar su imagen ni alejar a los usuarios.

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