

No existe una sólida educación en seguridad

Sara Gallardo M.

Eso dijo, entre muchas otras verdades, Iván Arce, experto en la materia.

A Iván Arce su juventud le ha alcanzado para todo. Ha sabido alimentar la pasión por las tecnologías de información, con el deseo permanente de conocimiento a través de un diario aprendizaje.

Sus primeros pasos, después de lucir la toga y el virrete en su grado como ingeniero de sistemas enriquecido con varias especializaciones, los dedicó a la práctica de la consultoría independiente y al desarrollo de software.

Con esa experiencia en la columna del haber en su estado de cuentas personal, fue nombrado vicepresidente de Investigación y Desarrollo, en una

empresa dedicada a la integración de telefonía y sistemas.

En esa posición le dio rienda suelta a crecer como persona y a aprender sobre la marcha, mientras observaba el entorno y se nutría de la vida empresarial y sus alcances.

El paso siguiente no podía ser otro que lanzarse a la aventura como cofundador y CTO de la firma Core Security Technologies. Organización en la que imprime su huella y estilo propios en la dirección técnica, en los procesos de ingeniería, investigación y desarrollo.

Su amplio recorrido profesional, lo ha hecho merecedor del reco-

nocimiento internacional, en todo lo relacionado con seguridad informática. Por eso su agenda está comprometida para participar en diferentes acontecimientos de la industria, en los que siempre es invitado de honor.

Y, por supuesto, no podía dejar de lado esa acumulada experiencia sin trasladarla a diferentes auditorios, para dictar charlas especializadas en diferentes países.

Además, un grupo fiel de lectores está atento a los artículos que Iván escribe como colaborador para un amplio número de publicaciones y editor asociado de la revista IEEE Security & Privacy.

Razones más que suficientes para que la revista Sistemas decidiera entrevistarlo.

¿Desde su perspectiva cómo es el panorama de la seguridad informática en Latinoamérica?

Vista en el marco de los usuarios de tecnología y de organizaciones de los sectores público y privado, ONGs, instituciones educativas y empresas, entre otros, la seguridad informática es un tema de poca relevancia. Si



Iván Arce

bien, la conciencia de la problemática de seguridad informática como un asunto que es necesario resolver ha crecido sustancialmente en los últimos años, el nivel de atención e inversión económica y de todo tipo-, además de los resultados obtenidos hasta el momento, son bastante pobres.

La rápida adopción de nuevas tecnologías como una forma de acortar la brecha tecnológica y de competitividad con regiones de mayor desarrollo, no está acompañada de un esfuerzo similar de cara al uso de dichas tecnologías, la seguridad y la privacidad de personas y organizaciones no escapan de ese panorama. Más allá de eso, tam-

poco es irrelevante mencionar que, históricamente, Latinoamérica no representa más de un cinco u ocho por ciento del mercado mundial de seguridad informática.

¿Dicha descripción aplica también en Colombia? ¿En qué específicamente?

No tengo conocimiento específico sobre el estado de las cosas en

Colombia. Sí podría generalizar y decir que la problemática de seguridad informática es similar -salvo algunos detalles- en toda Latinoamérica. En general, diría que Brasil, México, Chile, Argentina y Colombia son los países con mayor grado de desarrollo, pero cada uno de ellos tiene características propias y detalles que los distinguen.

Con base en su experiencia, ¿cuáles son las vulnerabilidades más frecuentes relacionadas con la seguridad informática?

Sin duda, los mayores problemas de seguridad informática se encuentran en las estaciones de trabajo o computadoras personales. En ellas se aloja un inmenso número de programas con serias falencias de seguridad -vulnera-

bilidades de todo tipo- y están al comando de usuarios sin una conciencia o experiencia clara sobre el tema. La gran mayoría de los problemas que nos afectan a diario tiene que ver directa o indirectamente, con aspectos de seguridad o privacidad en computadoras personales.

¿Cuáles son las más difíciles de controlar?

Clasificaría las más difíciles de controlar en dos categorías que no son

mutuamente excluyentes. Aquellas vulnerabilidades que afectan a muchas personas, quienes requieren que los usuarios finales se involucren en su resolución y esta es de un alto costo. Por ejemplo, vulnerabilidades en estaciones de trabajo, dispositivos móviles, equipos de consumo masivo, entre otros.

Aquellas vulnerabilidades que derivan de prácticas y procesos inseguros en su esencia, pero bien establecidos en la industria del software y el hardware, muy costosos de alterar, como el software de base y las aplicaciones cuyo ciclo de desarrollo carece de una estrategia de seguridad madura y embebida en el proceso de ingeniería.

¿Usted considera que existe un marco de educación adecuado sobre seguridad en Latinoamérica?

No. Creo que seguridad y privacidad son temas de inmensa relevancia para nuestros sistemas educativos y deben ser abordados en forma seria, empezando en las etapas medias del proceso educativo -educación media, terciaria y carrera de grado-, si no antes. El mundo actual es casi completamente dependiente de la tecnología y esta introduce una nueva problemática de privacidad y seguri-



dad en la vida de las personas. Abordar el tema y desarrollar un entendimiento temprano de esta problemática y su relación con el resto de las actividades de las personas es, en mi opinión, la única vía para posibilitar un crecimiento sostenido y sustentable, con una visión propia a largo plazo del uso de la tecnología que contemple también las características propias y únicas de nuestra región.

Si existe ese marco, ¿en qué se basa el énfasis?

El énfasis está en las etapas más tardías del proceso educativo- maestrías, posgrados, especializaciones-, y está casi exclusivamente centrado en los aspectos tecnológicos; y, en menor medida, en negocios de la problemática de seguridad informática. A los temas de privacidad, que generalmente parecerían de menor índole tecnológico, se les da menor relevancia en el marco actual, hecho que me parece una tremenda equivocación en las prioridades.

En la formación actual de los ingenieros de sistemas ¿cómo se aborda el tema?

Con maestrías, doctorados, especializaciones o a lo sumo mate-

rias en las carreras de grado, pero rara vez con un enfoque más holístico que se introduzca en la naturaleza misma de la disciplina de estudio. Creo que este tipo de formación lleva a la concepción y adopción de soluciones de carácter táctico, en detrimento de una visión estratégica de seguridad y privacidad integrada en todos los niveles de trabajo de los profesionales de ingeniería/sistemas. También se le imprime un marcado tinte tecnológico a la problemática de seguridad y, en mi opinión, seguridad y privacidad son asuntos para los que no existe una solución tecnológica 'correcta' o 'pura', sino alguna que requiere un análisis más amplio que contemple factores sociales, políticos y económicos.

Los profesionales de sistemas o de ingeniería que se capacitan en nuestra región -y en todo el mundo-, no reciben ni buscan una formación profesional sobre seguridad en esos términos y es natural que sea así en esa etapa del proceso educativo.

¿Cómo se manejan las certificaciones, cuál es su alcance y aplicabilidad real en las empresas?

"La rápida adopción de nuevas tecnologías como una forma de acortar la brecha tecnológica y de competitividad con regiones de mayor desarrollo, no está acompañada de un esfuerzo similar de cara al uso de dichas tecnologías, la seguridad y la privacidad de personas y organizaciones no escapan de ese panorama"...

Difícilmente, una certificación de seguridad es un indicativo de la capacidad, experiencia o conocimiento real de un individuo en la materia. A lo sumo, es un indicativo de la existencia de algún tipo de formación básica

en el tema, siguiendo la pauta del programa particular que puede ser malo, mediocre o medianamente bueno. Un experto en seguridad informática no se forma como resultado de la acumulación de cursos y certificaciones, sino de la acumulación y la aplicación de una disciplina de trabajo y de estudio adquirida en otro contexto - escuela, universidad, trabajo, casa, etc.-, combinada con las capacidades creativas, de innovación, perseverancia y adaptación, propias de cada individuo. No obstante, eso no impide que las certificaciones se adopten y se usen como un indicador de capacidad profesional y principalmente como un mecanismo del mercado laboral y de capacitación profesional, para establecer jerarquías, niveles salariales, planes de capacitación y justificar diversos tipos de decisiones y proyectos.

¿Son conscientes las empresas de la gravedad del tema, de su vulnerabilidad?

En general, diría que las empresas más conscientes de sus problemas en ese entorno son aquellas que pueden ver una relación directa entre su seguridad y sus negocios. Los bancos,

instituciones financieras, militares y las empresas cuyos negocios están fuertemente basados en el uso de tecnología, tienen una conciencia más desarrollada sobre estos asuntos. Son también las que tienen el mayor interés en solucionar los problemas, en ignorarlos o desconocerlos por completo, toda vez que la naturaleza de sus negocios no admite que el tema se aborde con medias tintas.

¿Cuentan con una infraestructura preventiva y correctiva al respecto?

Si, en su gran mayoría. El problema es que se adopta infraestructura defensiva -prevención- sin considerar la tecnología ofensiva como una opción válida y necesaria para completar el proceso de seguridad y convertirlo en efectivo. Es como jugar al fútbol con 10 defensores, sin árbitro, con un reglamento propio y suponer que el otro equipo lo va a respetar. En el momento en que el contrario hace un gol, el partido está irremediablemente perdido, si no se cambia el esquema de juego, el reglamento o el oponente. Creo que la razón por la cual muchos ataques siguen siendo efectivos y vigentes, a pesar de los grandes y cos-

tosos esfuerzos de prevención y corrección, es que prevalece una concepción puramente defensiva de la seguridad.

En los países latinoamericanos ¿cuáles sectores son los más frágiles y vulnerables? ¿Conoce casos que pueda citar?

Organismos públicos y de gobierno, los sectores de comunicaciones, energía, educación y salud. En general, aquellos que carecen de recursos financieros para invertir en seguridad, que adoptan tecnologías nuevas sin haber alcanzado un grado de madurez en su uso o la combinación de ambos aspectos.

Todo ello es agravado por el hecho de que las soluciones de seguridad existentes no están diseñadas ni orientadas para cubrir las necesidades de los sectores con esas características, y porque en nuestra región las prioridades de inversión son, entendiblemente, otras y muy distintas a las de los grandes mercados de la seguridad informática -Estados Unidos, Europa, Asia/Pacífico-.

¿Cómo define la seguridad en bancos, frente a los servicios y los usuarios?

Los bancos por necesidad tienen

iniciativas de seguridad más maduras que la mayoría de las organizaciones de otros sectores. Dichas iniciativas son, generalmente, de alta o mediana efectividad contra los ataques y atacantes poco sofisticados y se convierten en menos efectivas, a medida que el perfil del posible atacante se vuelve más sofisticado o dispone de mayores recursos. El balance justo de inversión en seguridad para una institución financiera es un problema de manejo de riesgo y dichas instituciones tienen experiencia y práctica en ese campo. Sin embargo, existen dos cuestiones que influyen negativamente en la seguridad de los bancos.

Por una parte, la tendencia a abordar el problema como una simple cuestión de manejo de riesgo 'financiero', desconociendo cualquier variable que no sea claramente utilizable en los modelos de riesgo en uso o de moda.

Y, de otro lado, la tendencia a sobredimensionar los logros y minimizar las falencias de seguridad, actitud que influye negativamente en la percepción interna y externa del estado real de las cosas, disminuye la transparencia y daña las relaciones de con-

fianza entre los distintos grupos de interés -usuarios, proveedores, accionistas, entidades reguladoras, auditores externos, administradores, auditores y diversos grupos internos-, que necesitan de una relación armoniosa, si se pretende lograr un buen nivel de seguridad que no sea efímero o volátil.

¿Un usuario colombiano puede sentirse seguro utilizando los servicios electrónicos para sus transacciones?

No he tenido más que una esporádica interacción con servicios electrónicos de Colombia. No desconozco el interés y la dedicación al tema de varios individuos y organizaciones colombianas -por ejemplo ACIS-, pero carezco de experiencia y conoci-

miento práctico sobre los pormenores particulares de ese país.

Personalmente, no me siento seguro utilizando servicios electrónicos para transacciones, sin importar el país de origen, destino o transporte de las comunicaciones, pero eso no impide que los use. De la misma manera que no me siento seguro al cruzar una calle o al salir a caminar por el parque. No obstante, lo hago. Creo que la seguridad pasa más por identificar las actitudes, valores e indicadores concretos que a uno le inspiran confianza. En mi caso, son bastante simples; se trata de transparencia, humildad y una fuerte experiencia y sustento tecnológico basado en excelencia técnica y fundamentación científica.

Sara Gallardo M. Periodista, comunicadora, Universidad Jorge Tadeo Lozano. Ha sido directora de las revistas *Uno y Cero*, *Gestión Gerencial* y *Acuc Noticias*. Editora de *Aló Computadores*. Redactora en las revistas *Cambio 16*, *Cambio* y *Clase Empresarial*. Fue corresponsal de la revista *Infochannel* (México). Autora del libro *"Lo que cuesta el abuso del poder"*. Es corresponsal en Colombia del Diario *"La Prensa"* de Panamá y revista *IN de Lanchile*; editora de esta revista.