La ciberseguridad multigeneracional

DOI: 10.29236/sistemas.n175a5

Jeimy J. Cano y Andrés Almanza moderadores de la reunión dieron la bienvenida a los participantes y procedieron a iniciar el debate.

"Este número 175 está dedicado a los asuntos de seguridad de la información, de la ciberseguridad, además, tiene que ver con los veinticinco (25) años de la Jornada Internacional de Seguridad Informática y todo lo que eso representa alrededor de la dinámica de ACIS, para el sector y el gremio", manifestaron los moderadores.

Luego, cedieron la palabra a los invitados para su respectiva presentación y entrar de lleno al debate.

Gonzalo Romero
Soy ingeniero de sistemas y computación, especialista en telemática de la Universidad de Los Andes y agradezco mucho la invitación para participar en este panel; en la actualidad, me desempeño como director de seguridad de la información en una organización multinacional americana que opera el dominio de Internet de Colombia.

Tengo alrededor de 20 años de experiencia en temas de seguridad de

la información y más de 35 en temas de infraestructura tecnológica (IT).

John César Arango
Soy ingeniero de sistemas, especialista en ciberseguridad, con dos especializaciones en redes y telecomunicaciones y otra en finanzas.

Tengo una empresa de ciberseguridad que se dedica a la seguridad ofensiva y soy docente, director de la especialización en ciberseguridad de la Universidad Católica de Mendizábal, además de docencia del módulo de ética, el *hacking* que normalmente dictan varias universidades, no solamente de Colombia, sino también de otros países.

Luego de las presentaciones de los invitados, se dio paso a la formulación de las preguntas por parte de los moderadores del encuentro, Jeimy J. Cano y Andrés Almanza.

¿Cómo han visto la evolución de la seguridad de la información a la ciberseguridad empresarial?

Gonzalo Romero
Antiguamente, nos enfocábamos en proteger los datos de la organización, había un interés, una concentración total en proteger los datos. Y eso se ha convertido ahora en una partecita dentro de una visión holística integral que prioriza en dos grandes puntos que son primero, la resiliencia operacional y segundo, la continuidad del negocio.

Me parece que eso es lo que ha sucedido. Nos estábamos enfocando en algo muy acotado y pasamos a algo mucho más global, mucho más organizacional, más integral en términos de protección. Antiguamente protegíamos el dato, hoy protegemos la organización, el negocio. ¿A partir de qué? A partir de temas de resiliencia y continuidad. Antes hablábamos de controles perimetrales, de dispositivos de seguridad, de firewalls o cortafuegos, accesos restringidos. Ahora estamos hablando de modelos mucho más dinámicos, más adaptativos.

La protección requiere de una gestión de riesgos eficiente, una respuesta proactiva y claramente la automatización que brinda la inteligencia artificial para poder anticipar y neutralizar las amenazas antes de que impacten las operaciones del negocio.

John César Arango
De verdad ha habido un cambio. Antes se pensaba en algo muy básico, es decir, tenemos que instalar Fire Wall, antivirus y manejar parches, eso era lo que uno hablaba anteriormente, hoy nos preparamos ante un ataque. Eso ha cambiado. O sea, qué debemos hacer si pasan los ataques o cuándo pasarán. Mantenemos esa zozobra.

No sabemos cuándo nos va a tocar. Si bien es cierto que la resiliencia exige algo más allá de la técnica, para la conciencia colectiva necesitamos integrar todas esas gene-

raciones en el mismo lenguaje de la seguridad.

Jeimy J. Cano M.
¿Hoy, cuáles elementos de la ciberseguridad son completamente diferentes a los que se conocían antes en seguridad de la información?

John César Arango

Para mí lo nuevo es que se trata de un apoyo bastante bueno. En el caso de una empresa en la que hice un análisis de tráfico para descubrir un problema, la inteligencia artificial me indicó exactamente cuáles eran los filtros a utilizar. Eso me pareció ´descrestante´ y me ahorró mucho tiempo.

Pero también y pensándolo como docente, he visto ya trabajos en los que la productividad de las personas a veces decae debido a que mantienen el uso de la inteligencia artificial de una forma inapropiada.

Gonzalo Romero

Estoy completamente de acuerdo; la inteligencia artificial (IA) es una herramienta con la que no contábamos antes, algo tan útil para identificar anomalías, para predecir ataques, para responder en tiempo real a las situaciones. Me parece que es una ventaja, un beneficio grandísimo que tenemos como gestores de seguridad en las organizaciones. Me parece que nos apoya y nos ayuda.

John César Arango
Ahora la seguridad se volvió un juego y le apostamos al juego, pero ahora ya no lo es, y dejó de serlo para convertirse en algo mucho más complejo, están acabando con la infraestructura, la reputación y la imagen de nuestro negocio.

Andrés Almanza
Gonzalo mencionó algo que vale la pena reflexionar: en el pasado nos

distraíamos con las cajas, hoy no. Por ejemplo, ahora al poner todo el CM, el XDR, ahora está de moda el NDR, el EDR, el DDR y el PPPR, por mencionar algunos. Entonces, ¿no estaremos heredando esos problemas del pasado a hoy? Lo que pasa es que ahora es software y ahora es desarrollo. ¿Hay otro cambio? Ahora hay cajas de hardware, cajas negras. Y hay sorpresas. Ahora es software con inteligencia artificial que yo puedo acomodar a como yo diga, a como yo indique, a como yo quiera predecir y evolucionar y progresar.

Jeimy J. Cano M.

¿Habría que actualizar las prácticas de seguridad de la información frente a los retos que tienen la empresa en el contexto digital? ¿Cómo se debería hacer ese cambio?

John César Arango

Estamos viviendo un cambio empresarial bastante importante. Entre las leyes está, por ejemplo, la Ley de Protección de Datos Personales la 1581. Varias cosas han exigido que muchas empresas se monten en dos voces de las leyes y eso nos permite de alguna manera que vayan en esa transformación.

Ahora veo que la gente se va volviendo más consciente de la seguridad, de la ciberseguridad; cada día necesitan más proveedores y varias empresas para eso. La gente no entiende que la nube es una responsabilidad compartida y muchas veces insegura.

Sería bueno que las empresas se vincularan a esos grupos de respuesta de incidentes, además de tener un servicio con unos terceros expertos en auditoría, para revisar ese tipo de cosas. Obviamente estamos hablando ya de empresas media pymes y grandes.

Gonzalo Romero

Absolutamente. En el contexto digital actual, caracterizado por la alta capacidad de integración, el uso creciente de inteligencia artificial y la sofisticación de las amenazas, es indispensable revisar y actualizar continuamente las prácticas de seguridad de la información. Ya no basta con defender perímetros; hoy el enfoque debe ser dinámico, basado en riesgos, y profundamente integrado con la estrategia del negocio.

El cambio debe comenzar por transformar la cultura organizacional: la seguridad no puede seguir viéndose como un área aislada o como una carga operativa, sino como un habilitador de confianza, continuidad y evolución digital. Esto exige adoptar marcos de referencia modernos como CSF y AI RMF de NIST, Zero Trust, fortalecer la gobernanza de datos, automatizar procesos críticos y, sobre todo, empoderar a las personas.

La verdadera resiliencia operacional y de negocio no se construye solo con tecnología, sino con conciencia, corresponsabilidad y liderazgo compartido.

Jeimy J. Cano M.

El algoritmo ¿está haciendo lo que tiene que hacer? ¿El algoritmo tiene la matemática correcta que tiene que utilizar? ¿El algoritmo está dando resultados consistentes? ¿El algoritmo está bien diseñado, bien hecho?

Gonzalo Romero

John César resume una serie de detalles clave a tener en cuenta y estoy totalmente de acuerdo con ellos; desde mi perspectiva, debemos orientar las prácticas de seguridad hacia la continuidad del negocio, revisando exhaustivamente el alcance y las métricas del plan de contingencia, conformado en ultimas por el plan de continuidad de negocios, el análisis de impacto de negocio, el plan de recuperación ante desastres y la gestión de incidentes dentro de nuestras organizaciones; de esta manera, estaremos avanzando en el despliegue de nuestra resiliencia operacional, tanto humana como corporativa.

Traigo a colación la situación que describió el propio Sr. Bryan Krebs con el ataque de denegación de servicios que sufrió su muy reconocido blog "KREBS ON SECURITY" a mediados de mayo; con un pico de 6.3 Tbps, ha sido uno de los ataques más grandes jamás registrados. Según él, a pesar del ataque, el sitio web estuvo activo en todo momento y no presentó interrupción alguna. Esto es lo que yo denomino *Resiliencia Operacional*.

En palabras coloquiales, me pueden estar intentando incluso destruir, pero yo estoy en línea, activo. Yo estoy ofreciendo mis servicios como si nada estuviese sucediendo tras bambalinas; a eso es a lo que debemos apuntarle, más allá del análisis previo y posterior al incidente, que sucedió con las "cajas", etcétera.

Creo que por aquí va el asunto: debemos capacitar a los CISO para que diseñen, desplieguen y gestionen cada vez mejores y más robustos planes de contingencia; ahora bien, una cosa muy bonita es tener el documento del plan. Pero ¿cuándo y cuántas veces al año se ejecuta el plan? acaso solo debe desplegarse cuando el auditor lo requiere? el objetivo radica única y exclusivamente en el cumplimiento? a partir de lo descrito por Krebs, el ejercicio del CISO con su equipo de trabajo, y apalancado en el área

de IT, incluye el estar muy atento a los resultados del análisis de tráfico de red de sus plataformas y servicios; en este caso particular, nota efectivamente que su mapa de calor está en rojo, pero sus servicios están plenamente activos y disponibles.

Una pregunta suelta: ¿ustedes saben cuál es el país que estadística e históricamente participa más en el FIRST, un evento anual muy reconocido que congrega a los CERT y CSIRT de todo el mundo? Japón.

Yo tuve el privilegio de participar como conferencista en el evento del 2014, celebrado a finales del mes de junio en Boston, Massachusetts, Estados Unidos. Este evento sucedió 3 años después del tsunami más devastador en la historia nipona.

Jamás olvidaré que cuando terminó la plenaria de apertura del evento, todos los japoneses tenían unos papelitos en sus manos y de repente se levantaron de sus puestos y nos entregaron a cada uno de los que asistíamos el papelito, que mostraba los recuadros de lo que parecía una corta “tira cómica”; todos casi nos ponemos a llorar. ¿Saben qué decía el papelito? Pues decía "¿Cómo protegerse de un tsunami?" Es uno de los ejemplos más claros y concisos de cooperación y solidaridad que haya visto; desde ese momento, me quedó muy claro quiénes son los japoneses: aprenden de sus situaciones y de sus errores, pero no se quedan ahí, comparten su propia realimentación como parte de su proceso de mejora continua.

Jeimy J. Cano M.
Nuestra pregunta número cuatro: ¿Cómo debería transformarse la formación de los profesionales en seguridad cibernética y qué competencias nuevas se deben considerar? ¿Cómo actualizar las que tenemos a la fecha dentro los retos y escenarios que se viven en la actualidad?

John César Arango
Hace un año fui profesor de una especialización de desarrollo de software y lo primero que les pregunté en mi materia.

Y lo primero que les pregunté fue si sabían qué era AWS y ninguno conocía el término. Me pareció increíble eso. El enfoque obviamente tiene que ser interdisciplinario, hoy en día debemos tener en cuenta la inteligencia artificial, la ciencia de datos, el análisis forense digital, internet de las cosas, blockchain, computación en la nube, entre otras. Además de integrar esas competencias blandas tales como comunicación, liderazgo, pensamiento crítico, resolución de problemas.

Gonzalo Romero
Desde mi perspectiva, la formación en seguridad digital necesita cambiar de raíz: no se trata solo de aprender a gestionar herramientas

o reaccionar ante incidentes; eso es parte inherente de nuestro rol y responsabilidades, claro, pero ya no es suficiente. Hoy estamos en un entorno donde los riesgos son mucho más complejos, donde hay IA involucrada, donde los datos están en todas partes y las decisiones de seguridad tienen un impacto directo sobre el negocio, en la imagen, en la reputación e incluso en la confianza social.

Entonces, lo que necesitamos es una formación mucho más integral. Hay que formar profesionales que no solo dominen la parte técnica —que sigue siendo clave— sino que también conozcan de riesgos, de comunicación, de ética, de regulación, y que tengan la capacidad de adaptarse a entornos híbridos y altamente automatizados. Y algo que es clave: si o si, tenemos que dejar de ver al área jurídica como un obstáculo; el profesional de seguridad digital tiene que empezar a comprender los aspectos normativos y legales, y ver a los equipos legales como aliados estratégicos. No son un fantasma ni un rival: son parte del mismo equipo que ayuda a cuidar la organización desde otra dimensión.

Y para actualizar las competencias que ya tenemos, hay que dejar atrás esa lógica de acumular certificaciones por cumplir; definitivamente necesitamos entrenamiento realista, inmersivo, continuo, espacios donde se simulen crisis, donde se aprenda haciendo, donde el error también sea una fuente de aprendizaje. Porque al final, no estamos formando técnicos operativos: estamos formando guardianes de la confianza digital.

Considero que debe haber una política pública; pero ¿cuándo se va a construir? No lo sé.

Andrés Almanza
Que interesante punto que tienes Gonzalo para conectarlo con las ideas de John, que es tratar a la ciberseguridad como un reto de política pública; al hacerlo de esa manera será el momento en donde vamos a poder conectar diferentes visiones y articular de alguna manera lo que se requiere desde el punto de vista de gobernanza, del ejercicio de gobierno, lo que implica desarrollar una serie de prácticas que entre todos las deben construir.

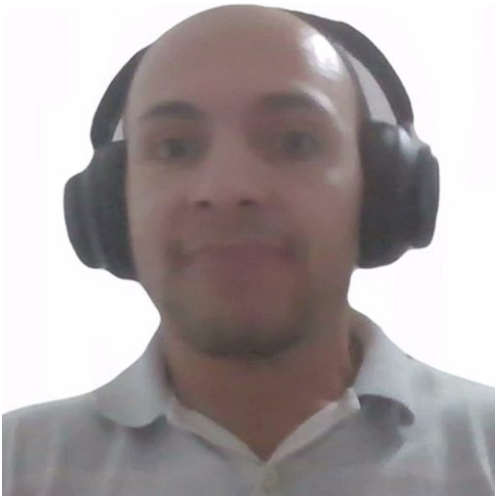
Jeimy J. Cano M.
Desde su perspectiva práctica, académica y empresarial ¿cómo viven esa experiencia y cómo van a gestionar ese tema de aquí en adelante?

John César Arango
Me parece una fortaleza que se puede complementar bastante. Es necesario trabajar en un ambiente multigeneracional. En Bolivia conocí a un muchacho, a un joven que su conocimiento lo construyó completo a través de internet. Hace una ingeniería inversa, sobre los cajeros descubre la vulnerabilidad, es un ´monstruo´, pero no le gusta ha-

blar de tecnología. Ahora no necesariamente el coach es el experto, ahora se trata de jóvenes que aportan a la organización en una manera importante. Se requiere motivarlos mucho.

Si sabemos concentrar el esfuerzo, vamos a encontrar muchas cosas buenas que nos van a ayudar en el camino hacia la resiliencia operacional, hacia la continuidad del negocio, hacia la protección de la marca hacia la protección de la reputación.

Andrés Almanza



Para complementar, dado que Gonzalo lo puso en el tintero esa práctica del mentoring y el mentoring reverso, que es útil en estos ambientes multigeneracionales que son cada vez más continuos y de hecho tú encuentras empresas que tienes las cinco generaciones que hoy existen marcadas en un ambiente organizacional.

Entonces, el mentoring Reverso ha venido tomando fuerza este ejercicio que busca conectar experiencias con innovación en el contexto de los seres humanos para que los mayores, pues aprendan de los jóvenes cómo es que ellos ven los problemas.

La experiencia en vez de ser una capa que rechaza el uno del otro, lo que hace que al quitarla y dejarse en la piel de los seres humanos hace dos personas se conecten. Una experiencia interesante fue acompañar un proceso en el que una persona con u se convirtió un alto nivel de experiencia, se convirtió en mentor de un joven, y en esa conexión fue muy satisfactorio ver los aprendizajes de ambas partes. Entonces se construyó un espacio muy humano.

En contextos multigeneracionales es clave que se gestionen desde la humanidad y menos desde el conocimiento, así es posible que haya aportes y crecimientos entre todas las visiones que se encuentran en estos espacios de intercambio de experiencias y aprendizajes.

El contexto digital actual, ha venido reescribiendo la forma en cómo el humano se desenvuelve, por tanto, suelo decir que los avances tecnológicos de esta era están empujando cada día más, a las personas a saber ser más y solo aquellos que logren eso, serán los que más capital, valor y potencial mostraran en el futuro.