

«Las empresas saben tus preferencias, te conocen mejor que tu amigo más íntimo»

Antonio Bueno Antón Experto extremeño en ciberseguridad

Estudió ingeniería en la UEx, luego en Sevilla y se especializó en Manchester; ahora promueve su propia sociedad sobre seguridad en la nube

LUCIO POVES

LOS SANTOS DE MAIMONA. Antonio Bueno Antón trabaja en la nube, pero no es meteorólogo ni nada que se le parezca. Estudió Ingeniería Industrial en la Universidad de Extremadura para luego pasarse a Ingeniería Informática en la Loyola de Sevilla. Tiene 28 años, es de Badajoz, donde hizo sus estudios en las Josefinas, y se ha especializado en lo que se llama arquitecto de ciberseguridad en la nube. En una palabra, ‘cancerbero’ de los sistemas que se guardan en la tan traída y llevada nube informática para que no sean atacados por elementos externos.

Ha trabajado para NTT Data o en Indra –donde llegó a ser consultor junior y sénior– siempre ligado a temas de ciberseguridad, pero también en otras ramas de la informática.

En 2024 se marchó a Manchester para cursar un máster de computación en la nube y seguridad en la red.

–¿Que quería hacer en Manchester?

–Pues yo me voy concretamente porque quiero especializar mi carrera en ‘cloud computing’, ya que está muy extendido sobre todo con el auge de la inteligencia artificial. Buscando másteres por toda Europa, compruebo que en Inglaterra existe la posibilidad de especializarme muy concretamente en la ciberseguridad en la nube.

–¿Y en eso está trabajando ahora?

–Como arquitecto de seguridad me encargo de garantizar que los despliegues de las empresas en la nube están a prueba de vulnerabilidades. Por ejemplo: en una aplicación de comunicación de mensajería por móvil, he de decidir qué tipo de encriptación tienen esos datos, para que cuando los envíes no puedan ser leídos o utilizados por ciberdelincuentes. La encriptación es una forma de codificar los datos para que solo las partes autorizadas puedan entender la información. –¿Es seguro almacenar en la nube?

–Lo que los usuarios almacena-



Antonio Bueno, especialista extremeño en ciberseguridad. L. P.

mos a día de hoy en la nube es una milésima parte del volumen de datos que realmente circulan por ella. La mayoría de estos datos provienen de empresas o instituciones como puedan ser bancos, gobiernos, hospitales, universidades... Todas estas instituciones almacenan estos datos en proveedores de la nube, como pueden ser Google, Microsoft o Amazon... En este punto, nuestro trabajo se centra en escoger la mejor opción en seguridad, precio y disponibilidad para que la aplicación, y los datos de estas empresas, circulen de manera segura desde sus oficinas hasta la nube.

–¿Se podría paralizar una ciudad mediante un ataque a la seguridad de una de estas empresas?

–La respuesta corta es sí. Empresas como Endesa, Ayesa o Iberdrola, por ejemplo, almacenan datos críticos en estas nubes; por eso cuentan con los mejores especialistas en ciberseguridad y arquitectura en la nube para anteponerse a estas problemáticas. Es mi trabajo.

–Hay mucha gente que se lo pregunta, ¿alguien nos escucha a través de elementos tan sencillos como el móvil o una nevera casera?

–Sí, somos observados y escuchados día a día; cada vez más dispositivos cuentan con cámaras, micrófonos, sensores y, desde hace muy poco, inteligencia artificial (IA). Esto es lo que conocemos como dispositivos IoT, que pueden ser tu lavadora, las

cámaras de un parking, los robots aspiradora que limpian tu casa, el sistema de control de las vías férreas... Todos estos dispositivos se comunican a través de la nube y su información y control quedan expuestos a posibles vulnerabilidades. Imaginemos que un terrorista tuviera en su mano la posibilidad de controlar una estación de ferrocarril. Sería un caos. Con el auge de la Inteligencia Artificial cada vez estamos más expuestos. Los gobiernos y los ciudadanos en general invierten cada vez más en llenar nuestras calles y casas con estos dispositivos. Por tanto nuestra profesión toma cada vez más un papel más importante.

–¿Por qué tanto interés en conocer nuestra privacidad?

–Más allá de los ciberdelincuentes, las empresas están interesadas en conocer nuestras preferencias u orientaciones para poder vender más productos. Por ejemplo, tu teléfono tiene activado el GPS todos los días y, junto con los gastos bancarios de tu tarjeta, saben qué días vas al supermercado y qué sueles com-

prar, si tienes hijos o no; por eso no es de extrañar que te aparezcan anuncios de zapatos después de haber visitado una zapatería. Al final, estas empresas te conocen mejor que tu amigo más íntimo. Elaboran perfiles que te describen a la perfección. –¿En qué estás trabajando actualmente?

–Actualmente estoy trabajando en un proyecto que combina la Inteligencia Artificial del ahora con la ciberseguridad del futuro. Estamos negociando con Emiratos Árabes Unidos para vender una IA capaz de utilizar la potencia de los ordenadores cuánticos. Son ordenadores que utilizan las propiedades de la física cuántica para obtener una potencia de cálculo inmensamente mayor. En España contamos con el mayor ordenador cuántico de Europa, en San Sebastián, y con otros dos más en Barcelona y Galicia. Estos ordenadores no están pensados para que los utilices en tu casa, sino para entidades como la NADSa, gobiernos, laboratorios de investigación... Para solventar problemas matemáticos imposibles de resolver a día de hoy.

El día Q

–¿Estos superordenadores cuánticos, pueden suponer un peligro para la ciberseguridad?

–La mayor amenaza a las que nos enfrentamos en los próximos años es el alcance de lo que conocemos como el Día Q. Es el día en el que los ordenadores cuánticos sean capaces de romper la encriptación que usamos a día de hoy para todos los dispositivos que utilizamos con mucha frecuencia –cámaras, móviles, smartwatches, robots– e incluso cuestiones muchas más críticas, como el control de la electricidad de una ciudad, o el lanzamiento de un cohete. Todos los países quedarían absolutamente desnudos. Precisamente por eso estamos trabajando en adelantarnos a este problema, con soluciones que implementan la encriptación postcuántica.

–¿Ante este problema, que dibuja para su futuro?

–Gracias a que he podido rodearme de expertos en la materia, este 2026 planeo constituir una sociedad que venda soluciones a empresas desde unos cientos seguros para la próxima era. Basándome en encriptación avanzada planeo desarrollar productos que solventen los problemas del almacenamiento, seguridad e integridad de nuestros datos, resolviendo los problemas de hoy con la seguridad del futuro.

INTIMIDAD

«Sí, somos observados y escuchados día a día, cada vez más dispositivos cuentan con cámaras, micrófonos y ahora la IA»

SEGURIDAD

«La mayor amenaza a la que nos enfrentamos en los próximos años es el alcance de lo que se conoce como el Día Q»