DIARIO DE NAVARRA

Fecha: 17/12/2023 Audiencia: 123.494 Sección: AUTONOMIA
Vpe: 7.621 € Tirada: 42.022 Frecuencia: DIARIO
Vpe pág: 8.550 € Difusión: 35.284
Vpe portada: 9.435 € Ocupación: 89,13%

"Ni la mejor de las tecnologías puede protegernos de nuestros descuidos"

Juan Ramón Aramendía Muneta Coordinador del Centro de Ciberseguridad de Navarra

Este ingeniero de Telecomunicaciones con amplia experiencia en seguridad informática asume el liderazgo del Centro de Ciberseguridad de Navarra con el objetivo de lograr que empresas y particulares reduzcan el riesgo de ciberataques

CARLOS LIPÚZCOA Pamplona

El coordinador del recientemente creado Centro de Ciberseguridad de Navarra, Juan Ramón Aramendía Muneta (Pamplona, 13 de octubre de 1976), acumula un extenso currículo profesional relacionado con la seguridad informática, sector para el que ha trabajado durante los últimos dieciséis años en las empresas S21Sec, Look Wise y Auriga. Previamente, estuvo contratado otros siete años por la multinacional norteamericana Lucent Technologies, primero en Bélgica y después en Madrid. Tras un breve periodo dedicado a la enseñanza y la divulgación, ahora se ha puesto a los mandos del ente público que aspira a convertirse en la ventanilla única para todo tipo de necesidades de ciberseguridad, tanto para las empresas como los particulares y las Administraciones Públicas.

Tras toda una trayectoria en la empresa privada, ¿qué tal su llegada al sector público?

Llevo muy poco, solo dos semanas, pero claro que es diferente. Primero me estoy poniendo un poco en situación y asimilando la atribuciones de los distintos departamentos y las sociedades públicas. La verdad es que estoy cómodo. Nasertic es una empresa muy seria y llena de buenos profesionales que hacen un montón de cosas y que tocan tecnologías diversas y punteras.

¿No será usted un hacker?

(Se ríe). No, para nada.

Pero tendrá conocimientos, ¿no?

Tengo conocimientos pero no me dedico a ello. Lo mío ha sido liderar equipos de desarrollo de tecnologías de ciberseguridad. Ahora, cuando doy las clases, sí que hacemos algunas cositas un poco relacionadas con el hacking. Es cierto que muchas veces, cuando hablas de ciberseguridad, la gente tiene el estereotipo del hacker y parece que este campo solo esté relacionado con ellos.

¿Qué tipo de perfiles profesionales trabajan en este sector?

Un estudio de un organismo europeo de ciberseguridad ha identificado hasta 32 perfiles diferentes en esta industria. No obstante, en los orígenes del sector es verdad que casi todos eran hackers. La empresa con la que me introduje en este mundillo, S21sec, se fundó en 2000 a partir de un concurso de hackers al que fueron para captar talento. En aquellos tiempos no había ningún tipo de formación reglada y eran personas autodidactas que se dedicaban al hacking por pura vocación. Posteriormente, el sector empezó a despuntar y entró en una fase más madura y estructurada. Por ejemplo, las empresas de ciberseguridad tienen grandes departamentos jurídicos en los que trabajan muchos abogados, ya que es muy importante el cumplimiento de la normativa, que es muy abundante y abarca lo local, regional, nacional, europeo e internacional.

¿Será bueno tanto legalismo?

La ciberseguridad es un asunto muy serio que puede poner en peligro la propia viabilidad de las empresas. Muchas solo invierten en protegerse una vez han sufrido un ataque o cuando han visto que otra empresa vecina lo ha padecido. Gracias al marco normativo, las compañías se ven obligadas a invertir en prevención. Ahí es donde entra el sector de la ciberseguridad, guiándolas en un entorno en el que no sabrían ni por dónde empezar. Hay que elaborar un plan director que recoja el punto de partida en el que está la empresa y los pequeños pasos que hay que ir dando para reducir la exposición al riesgo informático. Para garantizar la eficacia de las medidas adoptadas, es necesario también hacer un seguimiento periódico que ponga a prueba la seguridad informática con auditorías, lo que se denomina el hacking ético.

¿Hay que meterse en la cabeza de los ciberdelincuentes para combatirlos?

El primer paso para mejorar la ciberseguridad en cualquier organización es conocer tu propia infraestructura. La tecnología está hecha por humanos y siempre va a tener vulnerabilidades. Lo importante es identificar las partes críticas de tu infraestructura que contienen aquella información más sensible y comprender sus vulnerabilidades. Luego hay que ponerse en la piel del ciberdelincuente, que intenta utilizar esos agujeros para cometer sus fechorías. Es un juego del gato y el ratón que va evolucionando constantemente y que obliga a adaptar continuamente las medidas de seguridad para que sean eficaces.

¿No hay forma de reducir el riesgo a cero?

El riesgo cero no existe en ningún ámbito de la vida. Tampoco en la seguridad informática. La tecnología es algo que, a día de hoy, se ha extendido para abarcarlo casi todo y que ha adquirido un grado de complejidad elevadísimo. No hay que olvidar que está hecha por humanos, por lo que contiene muchos pequeños fallos. Estas diminutas erratas se acaban heredando porque el desarrollo tecnológico es incremental, es decir, tú te basas en algo que hizo otro anteriormente para dar el siguiente paso. Por tanto, es absurdo obcecarse con lograr la invulnerabilidad informática y centrarse en modular la protección de forma que la seguridad sea tanto más elevada como la importancia de la información a salvaguardar.

Dado que las personas son las que diseñan, instalan y usan la tecnología, ¿son acaso el mayor agujero de seguridad?

El coordinador del Centro de Ciberseguridad de Navarra posa en la sala de servidores del Gobierno

A mi me gusta verlo de esta manera. Por ejemplo, los bancos ahora intentan que no vayas a la oficina y lo hagas todo online, ya sea con una aplicación web o para el móvil. A la gente mayor le están diciendo en las sucursales que se instalen estas apps y, con limitaciones, han aprendido a usarlas. Sin embargo, ¿quiénes les han informado de los riesgos que tiene el uso de esa tecnología? Es decir, nos están poniendo en nuestras manos tecnología avanzada que está muy bien, porque nos facilita la vida, pero que exige acompañarla de una formación que nadie facilita. Son herramientas para las que la gente no está preparada. Y hablo de la gente mayor, pero también hay que incluir a los niños y jóvenes, incluso a sus padres, que tampoco saben muchas veces evitar comportamientos de riesgo.

¿Son inseguras las aplicaciones?

Las aplicaciones están muy bien hechas y son fáciles de usar, pero hay que saber manejarlas y conocer sus riesgos. La mayoría de los ataques informáticos, diría que un 80%, serían fácilmente evitables siguiendo unas sencillas pautas de seguridad. Si alguien nos pide por la calle nuestra tarjeta de crédito para apuntar el número, el nombre y el código de seguridad no se lo daríamos, pero somos capaces de meter esos datos sin pestañear en una página web cualquiera atraídos por una ganga. Por mucha seguridad que tenga el banco, nadie puede protegerte de tus errores. Cuando éramos peque-

ENTREVISTA DE *domingo*

DIARIO DE NAVARRA

Fecha: 17/12/2023 Audiencia: 123.494 Sección: AUTONOMIA
Vpe: 7.788 € Tirada: 42.022 Frecuencia: DIARIO
Vpe pág: 8.550 € Difusión: 35.284
Vpe portada: 9.435 € Ocupación: 91,09%

DNI

Juan Ramón Aramendía Muneta nació en Pamplona el 13 de octubre de 1976. Es el pequeño de los dos hijos que tuvo el matrimonio formado por **María Jesús Muneta Salinas** y **Félix Aramendía Oroquieta**. Sus padres eran propietarios de un taller de reparación de vehículos, conocido como **Argileku**, en la confluencia de la calle Olite y la avenida de Baja Navarra, así como dos tiendas de venta de repuestos. El nuevo coordinador del Centro de Ciberseguridad de Navarra estudió en **Jesuitas** hasta su ingreso en la **Universidad Pública de Navarra**, donde se graduó como **ingeniero de Telecomunicaciones**. Fue de los primeros alumnos que se benefició del programa Erasmus y estuvo un año, el cuarto curso, en el **Politécnico de Turín**. Está casado con **Raquel Ruiz de Gaona Lana**, ingeniera industrial, con la que ha tenido dos hijos: **Ainara** (10 años) y **Jon** (8 años). Trabajó tres años y medio en Bélgica para la multinacional norteamericana **Lucent Technologies**, que posteriormente le trasladó a Madrid, donde residió otros tres años y medio. Regresó a Pamplona en 2007 contratado por **S21sec**, una empresa pionera en España en ciberseguridad. Allí se hizo cargo del desarrollo de tecnología de seguridad informática. También se responsabilizó del área para la **protección de cajeros automáticos**. Esta línea de negocio fue adquirida por la multinacional italiana **Auriga**, para la que trabajó desde 2020. En los últimos tiempos se centró en la docencia en el curso de especialización en ciberseguridad en el **centro de FP de Donapea**. En mayo de este año presentó su currículo para liderar el nuevo Centro de Ciberseguridad de Navarra, cargo para en el que se incorporó hace pocas semanas.

de Navarra. JOSÉ CARLOS CORDOVILLA

"Tenemos talento y hay que aflorarlo"

C.L. Pamplona

¿Qué papel va a jugar el Centro de Ciberseguridad en la jungla del ciberespacio?
Nuestra vocación es promover la ciberseguridad tanto entre los ciudadanos de a pie como entre las empresas. Para llegar a la gente hay que poner en marcha campañas de sensibilización dirigidas a colectivos específicos como, por ejemplo, mayores, niños o padres. Tenemos que hacer esa labor de difusión para intentar paliar en buena medida la inseguridad informática, que en su mayoría consiste en estafas burdas. También nos interesa generar talento del que pueda nutrirse la industria en ciberseguridad en Navarra y que permita su crecimiento.

¿Hay escasez de profesionales en seguridad informática?
Cada vez más. He podido constatar que los cursos de especialización en la Formación Profesional están funcionando, pero no con la tasa de éxito que podríamos esperar para un sector en pleno crecimiento. La ciberseguridad ya está en boca de todos, no como antes, cuando éramos cuatro chalados. Ahora tienes una comida familiar y sale el tema. Pero esta inquietud luego no se refleja en la demanda de este tipo de cursos. Hay un máster en la UPNA que creo que se va a cancelar. Preguntando e indagando, he llegado a la conclusión de que estamos llegando demasiado tarde.

EN FRASES

"Nuestra vocación es promover la ciberseguridad tanto entre los ciudadanos de a pie como entre las empresas"

"Navarra lidera el proyecto Ciberreg que está formado junto con otras siete comunidades y tiene un presupuesto de 28 millones de euros"

¿A qué se refiere?
La demanda laboral de profesionales del ámbito tecnológico es altísima y las empresas se los rifan. Los graduados no tienen necesidad de hacer una especialización porque los contratan nada más acabar. Tenemos que llegar un poquito antes e intentar primero que les pique el gusanillo. La ciberseguridad es muy vocacional. En Navarra hay mucho talento y desde el Centro de Ciberseguridad queremos hacerlo aflorar. Sin profesionales, no podemos desarrollar una industria con un potencial enorme en empleo y rentabilidad.

¿Ese talento tiene que venir de las ingenierías o también sirven los titulados de FP?
De hecho tenemos dos líneas para estudiantes de FP, una en Donapea y otra en el Mariana Sanz. Se trata de especializaciones pensadas para después del grado superior. En Donapea está especializado en OT, es decir, tecnologías de la operación que se usan en procesos productivos como Volkswagen o Gamesa. Es donde yo doy clase, aunque también contamos con expertos que vienen de Volkswagen o del Gobierno de Navarra. La de Mariana Sanz se corresponde a las Tecnologías de la Información clásicas como la infraestructura típica de ordenadores y servidores de cualquier empresa. Esa diferenciación desde el punto de vista de seguridad es necesaria porque cambia el enfoque o la aproximación a la securización de diferentes tipos de infraestructuras.

¿Con qué medios va a contar el Centro de Ciberseguridad para su labor?
El nacimiento del Centro de Ciberseguridad de Navarra está ligado a los fondos europeos Next Generation. Al hilo de los PERTE, se puso en marcha el programa nacional Retech con diferentes líneas de innovación tecnológica, que tenía a su vez un apartado de ciberseguridad. El departamento de Universidad, Innovación y Transformación Digital del Gobierno de Navarra presentó el proyecto Ciberreg. Está liderado por la Comunidad foral pero integra a otras siete Comunidades Autónomas. En total, son unos 28 millones de euros, de los que 3,5 millones han sido presupuestados para Navarra a lo largo de los próximos tres años. Hay también una parte para un centro de respuesta ante incidentes. Tenemos que montar toda esa infraestructura que permita darles respuesta, para lo que contaremos con recursos propios, pero principalmente haremos uso de empresas del sector.

¿Y cuando se acaben esos 3,5 millones habrá continuidad?
Esta es una apuesta de futuro, no es flor de un día. Vamos a aprovechar los fondos Next Generation para lograr un primer impulso, pero el Centro de Ciberseguridad de Navarra continuará después su camino porque es necesario.

¿De cuánto personal van a disponer?
Vamos a tener a tres personas y luego ,a partir de ahí, vamos a trabajar con licitaciones. Todo el servicio que vayamos a canalizar a través del Centro de Ciberseguridad de Navarra será con licitaciones de terceras empresas. Por otro lado, vamos a promocionar un catálogo de producto y servicios de ciberseguridad en Navarra, es decir, el quién es quién.

ños nos decían que no habláramos con extraños, pero ahora los chavales entablan conversaciones con cualquier desconocido en el chat de un juego o a través de una app.

En los foros de ciberseguridad suelen decir que la contraseña más usada sigue siendo 123456. ¿Algún consejo para corregirlo?
Hay que tener nombres de usuario y contraseñas diferentes y complejas en cada uno de los servicios que usemos. Eso es un problema para memorizarlas todas, pero hay aplicaciones que se llaman gestores de contraseñas que lo hacen muy sencillo. Yo las uso. Son capaces de generar claves aleatorias que le ponen las cosas difíciles a los cacos.

¿Cuál usa usted?
Tengo instalada Keepass. También es esencial activar la identificación en dos pasos, es decir, aquella que no solo exige meter usuario y contraseña, sino que también te envía un mensaje al móvil o al correo electrónico para confirmar tu identidad.

¿Hay que tener instalado un antivirus?
Windows cuenta con un sistema de protección llamado Defender que es bastante bueno a día de hoy. Si mantenemos actualizadas nuestras aplicaciones y las del sistema operativo, podría ser suficiente. No obstante, yo recomendaría contar también con un antivirus comercial.

¿Es alguno mejor que otro?
Son todos muy parecidos y ofrecen buenos niveles de protección. En mi casa, tengo instalado el McAfee.