it Digital MAGAZINE

Nº 4 · ABRIL 2023

Descarga esta revista y ábrela con Adobe Acrobat Reader para aprovechar sus opciones de interactividad

it User TECH & BUSINESS

NUEVOS ENFOQUES SOBRE LA EXPERIENCIA DEL CLIENTE

it Reseller TECH & CONSULTING

LAS NUEVAS TENDENCIAS TIC REDEFINEN LA CESTA DE LA COMPRA TECNOLÓGICA

it Digital Security

SEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS: ¿ESTAMOS PREPARADOS?

ENTREVISTA A SUSANA QUINTANILLA, DIRECTORA GENERAL DE SANITAS HOSPITALES

ENTREVISTA A ANDRÉS SORIANO, CISO DE UNIVERSAE

TENDENCIAS EN TORNO A CLOUD Y EL PAPEL DEL CANAL, A DEBATE

#ENTREVISTA

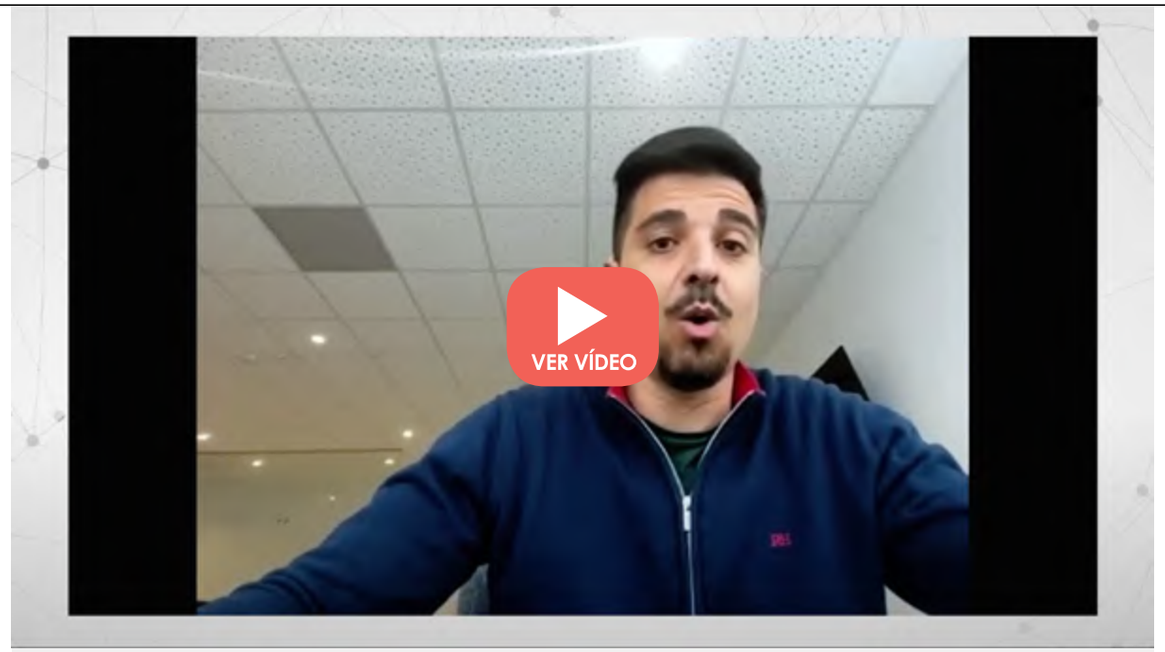
“El cibercrimen se ha convertido en una industria”

ANDRÉS SORIANO, CISO DE UNIVERSAE

DESIRÉE RODRÍGUEZ

En un sector como el de la ciberseguridad, en el que faltan perfiles desde hace años, es más vital si cabe que esos perfiles sean capaces de enfrentarse al mundo real lo más rápido posible. Por eso, en Universae han decidido hacer de la tecnología su valor diferencial y montar unas instalaciones específicas en las que sus estudiantes en ciberseguridad puedan enfrentarse a escenarios reales, practicar con tecnología real y reaccionar ante problemáticas reales. Para conocer mejor cómo se lleva a cabo esta formación y qué ofrece Universae, hemos hablado con Andrés Soriano, CISO de la compañía, quien ha compartido con nosotros su visión sobre la tecnología, desafíos y talento del futuro de la ciberseguridad.

ITDM >> Abril 2023



ENTREVISTA >> ANDRÉS SORIANO, CISO DE UNIVERSAE

¿Cómo surge Universae y cuál es su propuesta?
Universae surge de la mano de unos profesionales que tienen más de 15 años de experiencia en el sector educativo tienen un objetivo muy firme: cambiar las reglas de la formación profesional que hay en España y adaptarla al estado actual de la enseñanza. Nos encontramos ante una sociedad ampliamente digitalizada que requiere nuevas formas de docencia y apostamos firmemente por la docencia online pero no queremos es que esta docencia online se vea muy mermada o diferente a la docencia tradicional por lo tanto hacemos mucho hincapié en la metodología educativa y en los avances tecnológicos. Por todo ello incorporamos a nuestro modelo educativo una serie de tecnologías innovadoras o disruptivas como son la realidad virtual, la realidad aumentada, los entornos comunicativos... herramientas que nos permiten, desde la distancia, que el alumno pueda tener los recursos que tendría de forma presencial.

Más allá de la apuesta por aprovechar las capacidades únicas de la tecnología, ¿cuál es su valor diferencial?
En Universae nos definen diversos valores: el primero sería la oferta académica, pues toda se compone de formaciones profesionales de carácter oficial reguladas por el Ministerio de Educación y Formación Profesional. Universae ofrece 55 titulaciones de 13 áreas diferentes: desde la rama sanitaria a la rama de Protección Civil y emergencias, pasando por la informática y, como en mi caso, la rama de la ciberseguridad. Otro valor diferencial sería nuestro método educativo pues, como ya te comenté antes, no sólo nos basamos en un valor tecnológico sino que también tenemos un modelo educativo detrás: lo denominamos el modelo Universae 360, que es un ecosistema educativo inmersivo, integrado por todos estos entornos ramificados, simuladores de realidad virtual... que lo que hace es ofrecer una experiencia global al alumno al darle la capacidad de estudiar y de formarse con todos aquellos contenidos a los que tendría acceso en una enseñanza presencial o que son de difícil acceso para incrementar mucho más su empleabilidad y su potencial a la hora de tener, en un futuro, mejores prestaciones. Y, en tercer lugar, tenemos lo que denominamos el campus. El campus 23 surge con el objetivo de que Universae se convierta en un trampolín entre empresas y alumnos. En Universae tenemos muy claro que nuestro éxito radica en empleabilidad de nuestro alumnado y por eso desde el día 1 potenciamos que, tanto empresas como alumnos, se conozcan, desarrollen actividades, sepan qué es lo que pide una empresa de un perfil profesional como sería el del alumno y qué es lo que el alumno puede encontrarse el día de mañana si accede al mercado laboral en esa empresa. En definitiva, ponemos en contacto a empresa y alumnado desde el primer momento que inicia su andadura académica.

¿Cómo hacen frente a la gran falta de talento que existe actualmente en ciberseguridad?
Básicamente nosotros diferenciamos los sectores que necesitaban las empresas españolas y vimos que claramente en ciberseguridad hay varios diferenciados: está el sector del alumno que se quiere iniciar en la en la ciberseguridad, y nosotros lo atendemos con nuestro Máster de Especialización en Ciberseguridad en torno de las tecnologías de la información, cuyo objetivo es que cuando terminen este máster estén preparados para iniciar su andadura en ciberseguridad y formar parte de un equipo de ci-

berseguridad en cualquier empresa. Para ello entre sus asignaturas tienen: análisis forense informático, bastionado de redes, hacking ético, gestión de incidentes... es un grado formativo multidisciplinar que va a favorecer que el alumno esté perfectamente formado en su andadura a nivel de ciberseguridad. Luego ya tenemos otro escalón más avanzado como es el escalón de dirección: formar los futuros decisores, CISO, managers... que ocupan los cargos de responsabilidad en nuestras empresas y este ámbito lo cubrimos con el lanzamiento de nuestro Máster en Gestión Estratégica de la Ciberseguridad. Un máster que tenemos avalado por RootedCON, la mayor Comunidad de ciberseguridad de habla hispana, y con él aspiramos básicamente a formar a los mejores decisores de ciberseguridad de nuestro país. Además, podemos alardear de que tenemos al mejor abanico docente: Jorge Ulla, de Innotec; Jorge Bermúdez, fiscal de delitos tecnológicos; Román Ramírez; Javier Rodríguez... es decir, tenemos a primeras espadas en el ámbito de la ciberseguridad nacional e internacional.

Cuentan con una infraestructura única en la que se incluye equipamiento de vanguardia en lo que respecta al análisis forense de dispositivos electrónicos y de hacking...

Tenemos siete sedes diferenciadas a lo largo de todo el mundo, haciendo especial hincapié en Latinoamérica y en España. Estamos asentados principalmente en Murcia, Madrid y Barcelona.En Madrid inauguramos nuestro Madrid CybersecurityLab, un entorno de aproximadamente 500 m2 destinados exclusivamente a la ciberseguridad. Este entorno se compone de tres áreas bien diferenciadas: un laboratorio de análisis forense, en el que nuestros alumnos van a poder hacer todo tipo de prácticas de análisis; la sección de hacking, que es una zona muy diferenciada para hacer ejercicios en directo de Red Team y Blue Team, lógicamente monitorizados y en un entorno controlado totalmente en todo momento por el profesorado; y, por último, nuestro valor diferenciador es nuestro superordenador. Tenemos un ordenador de cracking que está compuesto por 12 tarjetas gráficas envidia 4090 que aporta una inmensa capacidad de cómputo y de descifrado.
De hecho, Universae no solo lo pone a disposición del alumnado, sino que también lo ponemos a disposición de aquellas empresas o entidades gubernamentales, como pueden ser Fuerzas y Cuerpos de Seguridad del Estado, Policía Nacional, Guardia Civil, Centro Nacional de inteligencia... que necesiten hacer uso de él en algún momento determinado en sus investigaciones.

¿Cuál es su mayor reto?

Mi función de CISO no es otra que velar por la seguridad de mi empresa, es decir, dotarla de todas aquellas herramientas y medidas de seguridad que permitan asegurar el desarrollo de nuestro negocio y protegernos de todas aquellas ciberamenazas externas o internas. Sin embargo, en Universae tenemos un plus añadido: somos una entidad educativa y, como

> “LAS HERRAMIENTAS PRINCIPALES PARA HACER FRENTE AL CIBERCRIMEN SON LA FORMACIÓN, INFORMACIÓN Y CONCIENCIACIÓN”
>
> **ANDRÉS SORIANO**, CISO de **Universae**

tal, debemos velar, además, por la seguridad y la disponibilidad de todos nuestros sistemas con respecto a nuestros alumnos, de tal manera que el riesgo al que podamos vernos afectados no afecte y seamos capaces de garantizar que todos nuestros servicios académicos estén disponibles en todo momento con nuestros alumnos y, asimismo, podamos garantizar la propia seguridad de nuestros alumnos. Es una tarea complicada, pero tener en nuestras filas a un cuerpo docente de tanto nivel me hace la tarea más fácil.

Desde hace años se habla de una falta de talento en el sector tecnológico y más si cabe en el de la ciberseguridad, ¿también sufren la falta de perfiles a la hora de proteger sus activos?
En ciberseguridad hay muchísima demanda y se espera muchísima más de cara a los próximos años. La retención del talento es difícil, sin embargo, desde Universae apostamos por que nuestro talento y los que formamos se queden en España. Todos nuestros temarios están basados en esas necesidades que las empresas nos están transmitiendo y el mercado laboral requiere pero a su vez es difícil retener ese talento, porque en una carrera profesional todos aspiramos a mejorar y eso supone mucha rotación de plantilla.

En ciberseguridad es normal la alta rotación de personas. ¿Cuál es para usted la mayor dificultad y qué espera que veamos en los próximos meses?
Para mí la mayor dificultad es hacer frente a todo ese entramado de ciberdelincuencia que tenemos por ahí fuera ahora mismo. Nos encontramos en una sociedad altamente interconectada y digitalizada, no podemos funcionar sin esa tecnología y es cierto que las redes del cibercrimen organizado son conscientes de ello y, como siempre ha sucedido, antes estaban los delitos tradicionales y ahora los delitos actuales que llevan aparejada el uso de las nuevas tecnologías. El Ministerio de Interior publicaba en enero un informe el que informaba de que los delitos cibernéticos habían crecido respecto a los 2 años anteriores en un 89%. Para hacernos una idea de las cantidades, ya estamos hablando de que, entre los meses de enero y noviembre del año 2022, en España se denunciaron 267.000 delitos aproximadamente. Delitos que solo en el año 2022 aumentaron con relación al año anterior un 22%. Es decir, es algo que exponencialmente va en aumento y es difícil de parar. Cada vez salen nuevas técnicas, nuevas vulnerabilidades... Las nuevas organizaciones criminales tienen departamento de I+D. El cibercrimen se ha convertido en una industria, y, como tal, invierte recursos e invierten personal y hacen todo lo necesario para que su actividad delictiva llegue a puerto. Por lo tanto, es una situación, la de los próximos años, que es preocupante. Ejemplo de ello es lo que lo que sucedió en el Hospital Clínic de Barcelona, que supuestamente ha sido víctima de un ataque de ransomware y se encuentran en una situación comprometida, pues tienen que ver por qué se ha producido la infección. La principal vía de ataque suele ser el propio ser humano, que sigue siendo el eslabón más débil. Por eso hay que tener en cuenta que una de las herramientas principales para hacer frente a este problema son la formación, información y concienciación. Y esta formación tiene que ir desde el eslabón más bajo, el becario, hasta el escalón más alto, como puede ser el CEO, porque todos somos susceptibles y hacer clic en ese enlace o en ese software malicioso que quiere instalarse o que quiere tomar el control de nuestro equipo. Las empresas y administraciones tienen que ser conscientes del enemigo al que nos enfrentamos y de que la formación en sí es prioridad absoluta en todo tipo de organismos y de organizaciones. Luego ya vendrán las nuevas herramientas técnicas y las mejoras como puede ser el implemento de software de herramientas de detección de intrusos, de diferentes tipos de hardware como el firewall, etcétera, pero si tenemos todas esas herramientas sin concienciación del personal que tiene que tratarlas no va a servir de nada. ■

MÁS INFO +

» Universae

» Universae pone en marcha una incubadora tecnológica de formación en ciberseguridad

» Qué hacer para reducir las brechas de seguridad con origen en errores humanos

COMPARTIR EN REDES SOCIALES