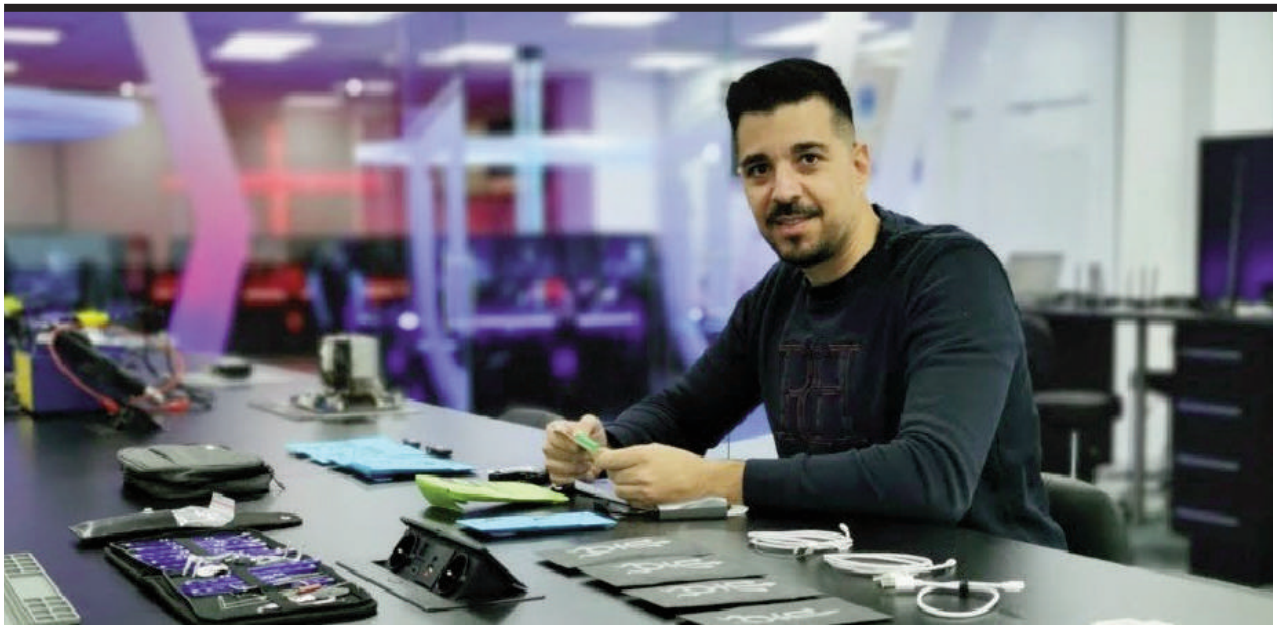

"En ciberseguridad, las empresas deben comenzar por analizar y definir de forma concisa las políticas de la organización"

¿Qué importancia tiene el desarrollo del talento en las empresas?
El desarrollo del talento en la Ciberseguridad es extremadamente importante en las empresas, especialmente en la actualidad donde hay grandes dificultades para encontrar a profesionales de este ámbito.
Por ello, desde UNIVERSAE, hemos lanzado recientemente varias titulaciones, el Máster propio en Gestión Estratégica de la Ciberseguridad, cuyo principal objetivo es formar a los mejores decisores al más alto nivel para que lleguen a liderar departamentos en materia de Ciberseguridad.
Junto al Curso de especialización en entornos de las tecnologías de la información, un Máster de Formación Profesional oficial, reconocido por el Ministerio de educación español, orientado a formar a todos aquellos iniciados en la informática que quieran iniciar su andadura en la Ciberseguridad.

Alrededor del 70% de las grandes organizaciones ha identificado que no puede encontrar candidatos con las habilidades requeridas. ¿Qué enfoque deben tomar las empresas?
Considero que las empresas pueden tomar varios enfoques. En primer lugar, capacitación interna. Las empresas pueden invertir en la capacitación de su personal existente para desarrollar habilidades en Ciberseguridad.
En segundo lugar, colaboración con centros de formación en la búsqueda de talentos, promoviendo entre los estudiantes la importancia de la Ciberseguridad y fomentando la formación en este ámbito. Además, las empresas pueden ofrecer prácticas y colaborar en proyectos. En este sentido UNIVERSAE cuenta con Campus23, un lugar de encuentro en el que empresas y profesionales buscan contribuir, a través de la experiencia, al impulso de la empleabilidad del alumno.
Por último, es importante que las empresas inviertan en investigación y desarrollo de tecnologías y soluciones innovadoras en Ciberseguridad, lo que puede

aportar un conocimiento especializado y diferencial frente a su competencia.

Una de cada cinco empresas han sufrido un ciberataque. De estos, el 15.9% no dispone de un plan de recuperación. ¿Qué medidas deben adoptar las empresas para prevenir estos ataques?

La primera medida, sin duda alguna, es la formación y concienciación en Ciberseguridad para todos los empleados de la organización, desde el escalón más bajo al más alto. El objetivo es poder identificar el primer vector de entrada por el que se propagan otra serie de ataques como, por ejemplo, el phishing.

Le deben de seguir otra serie de medidas como por ejemplo establecer una correcta gestión de accesos a los sistemas, con autenticación de doble factor, la segmentación de redes, gestión de privilegios y securización de los entornos de trabajo.

¿Cómo tener éxito con la estrategia de Ciberseguridad? ¿Tienen las empresas una estrategia adecuada?

Para tener éxito con una estrategia de Ciberseguridad, las empresas deben comenzar por analizar y definir de forma concisa las políticas de seguridad de la propia empresa y sus trabajadores, y que a su vez este alineado con los objetivos de negocio. Considero que el problema radica en la falta de concienciación en Ciberseguridad por parte del tejido empresarial español, ya que las pequeñas o medianas empresas tienden a creer que no son tan importantes como para recibir un ciberataque.

Si una pyme sufre un ciberataque al no haber realizado las acciones necesarias que prevean una respuesta eficaz y gestión de incidentes, puede ocasionarles desde el cese temporal del negocio hasta el cese total de su actividad laboral.

¿Qué se busca con la formación que ofrecéis en UNIVERSAE? ¿En qué áreas incidís?

Desde UNIVERSAE buscamos impulsar la coordinación, asesoramiento y prestación de actividades académicas en materia de Ciberseguridad con el objetivo de formar al mejor talento de España.

Pretendemos revolucionar el mundo educativo a través de nuestra metodología learning by doing, que se basa en el aprendizaje a través de la práctica en escenarios reales con los que favorecer y potenciar las aptitudes y habilidades de nuestros alumnos. Siempre contando con un equipo docente de primer nivel, instruidos de primera mano en las tácticas, técnicas y procedimientos que emplean los cibercriminales. Con nuestra oferta, el alumno una vez haya terminado sus estudios, tendrá capacidades más que suficientes que le permitan actuar con rapidez y solvencia cuando tenga que enfrentarse a un entorno hostil en el ejercicio de su profesión.

¿Qué medidas de Ciberseguridad implementáis en UNIVERSAE?

Andrés Soriano, CISO de UNIVERSAE

Desde UNIVERSAE trabajamos constantemente para la detección de cualquier tipo de amenaza. Todo ello acompañado de medidas de protección perimetrales, sistemas de detección de intrusos, auditorías constantes, etc. Y por supuesto, siempre al tanto de las tácticas, técnicas y procedimientos empleados por los ciberdelincuentes.

¿Qué ofrecen los profesionales que trabajan en el máster?

Los profesores en UNIVERSAE son primeras espadas del panorama de la Ciberseguridad nacional, internacional y mundial. Muchos de ellos prestan servicios en importantes empresas del sector tecnológico (Rootedcon, Microsoft, Halborn, Innotec, Naturgy, Ferrovial ...) e incluso algunos de ellos forman parte del comité de expertos que colabora al más alto nivel de seguridad, con las Fuerzas y Cuerpos de Seguridad del Estado, el Departamento de Seguridad Nacional o el Consejo de Seguridad de la Unión Europea.

Todas estas habilidades y experiencias hacen que el alumnado se forme y aprendan de la mano de los mejores profesionales que tenemos en España, y de esta forma adquieran todo tipo de habilidades con la que poder hacer frente a cualquier ciberincindente.

Referencias tecnológicas en la transposición de la Directiva Whistleblowing

La entrada en vigor de la reciente normativa de protección de los informantes, y que transpone, en España, la Directiva 2019/1937 de 23 de octubre, también conocida como Directiva Whistleblowing, ha supuesto, de un lado, la consolidación de obligaciones legales de configuración y garantías de protección que, en muchos casos, ya venían aplicándose en la implementación y funcionamiento de los canales de denuncias, ahora denominados "sistemas internos de información".

Sería especialmente extenso desgranar, aquí, el cúmulo de excesos regulatorios, contradicciones e incoherencias que, en mi humilde opinión, contiene esta norma y que, en buena parte, derivan de una falta de rumbo o abstracción que ya se advertían en la propia Directiva. No obstante, ello no puede suponer negar la necesidad y, especialmente, la utilidad preventiva y de autoconocimiento corporativo de estos sistemas internos en los esfuerzos corporativos de Compliance, así como el beneficio, como puesta en valor e impulso, que la Ley aporta para la mejora del funcionamiento de éstos (que serán obligatorios, en España, para las entidades de más de doscientos cincuenta empleados, a partir del 13 de junio de 2023, así como para las entidades a partir de cincuenta empleados, a partir del 1 de diciembre de 2023).