Expansión &EMPLEO

PAÍS: España
PÁGINAS: 8
TARIFA: 23310 €
ÁREA: 1018 CM² - 90%

FRECUENCIA: Semanal
O.J.D.: 20661
E.G.M.: 131000
SECCIÓN: SUPLEMENTO

30 Mayo, 2020

Gorodenkoff

Las formaciones relacionadas con la ciberseguridad ponen el acento en el conocimiento de técnicas como el 'pentesting' o programación para potenciar perfiles híbridos.

EL DESAFÍO DIGITAL

La ciberseguridad se consolida como un valor más en los negocios

La protección informática ha cobrado un nuevo cariz con la pandemia. Las altas direcciones se han visto obligadas, ahora más que nunca, a adquirir una visión de 360 grados sobre sus efectos jurídicos y financieros. **Por Ángel G. Perianes**

Hoy en día existe un agujero gigantesco dentro de los equipos de gestión de las empresas, porque muy pocos entienden la realidad de la ciberseguridad. Todas tienen su jefe informático, y es como si hablara en chino para el resto". Son palabras de Robert Maxwell, director de los dobles grados de Ciberseguridad con *Business Analytics* y con Derecho en la Universidad Francisco de Vitoria. Tal como cuenta, estas titulaciones de la institución privada madrileña responden a la necesidad, creciente en los últimos años, de preparar generaciones híbridas, con un alto conocimiento sobre la protección tecnológica, la privacidad de datos y sus impactos e implicaciones en los ámbitos empresarial y financiero.

El ritmo vertiginoso de la transformación digital de las organizaciones –acentuada con la pandemia del coronavirus–, ha hecho de la ciberseguridad una habilidad transversal. Por eso, según Maxwell, cada vez son más las universidades y escuelas de negocios que apuestan por ofrecer formación a jóvenes procedentes del mundo financiero y jurídico. En su caso, los estudios que dirige son los primeros en Europa que vinculan estas áreas en grados universitarios.

En este tipo de formación, adquirir ese rol bilingüe entre dos realidades distintas no pasa por acceder a ellas con perfiles eminentemente técnicos ni con conocimientos matemáticos de nivel ingeniero. Más bien, se les pide un carácter inquisitivo. "Estos programas están planteados para que ellos tengan iniciativa a la hora de buscar y abordar documentaciones en holandés o cirílico, idiomas que no tienen por qué saber. Aquí lo más importante es que tengan inquietud para enfrentarse a ello", asevera.

> Aunque el objetivo no es crear técnicos, se busca que sepan interpretar estrategias y repercusiones

Desde un enfoque práctico, los estudiantes recorren ámbitos específicos de la ciberseguridad para poder interpretar su incidencia en empresas o en un bufete. Esto incluye lenguajes de programación como Python, técnicas de *pentesting* (tests de penetración para encontrar debilidades de un sistema informático), *hacking* ético, fundamentos de criptografía, análisis forense, gestión de bases de datos relacionales, arquitectura de sistemas, derecho digital o *big data*.

Tal como manifiesta Maxwell, las claves que han permitido que este tipo de estudios sean funcionales son, por un lado, encontrar aliados en universidades punteras en esta materia, como la de Tel Aviv. Y por otro, involucrar a las empresas en el diseño del programa. "No se trata de dar con gente que vende un producto, sino de tocar consultoras, despachos o compañías grandes, como Indra o Telefónica". En función de sus necesidades, programas como estos van incorporando materias para que los jóvenes tomen contacto con el entorno profesional, a través de conocimientos demandados por esas mismas empresas.

> El reglamento de la protección de datos es uno de los vértices que más destacan las escuelas de negocios

De igual modo, en las escuelas de negocios se hace hincapié en que sus estudiantes aprendan a desenvolverse y a conocer el impacto que tiene el Reglamento General de Protección de Datos (RGPD) en el aspecto económico. El profesor del Instituto de la Economía Digital de Esic, Óscar Lage, afirma que, "quienes aspiran a ser directivos tienen que tener claro qué pueden o no hacer, porque antes había modelos de negocio que se basaban en explotar los datos sin pedir consentimiento. Ahora, todo está sujeto al RGPD, y esos perfiles deben sensibilizarse con ello".

La realidad es que, poco a poco, las compañías luchan con más vehemencia para conseguir que los departamentos de ciberseguridad tengan mayor peso y no cuelgue de un departamento financiero. Ése es el motivo por el cual, según Lage, estos perfiles "tienen que tener un lenguaje común sobre análisis de riesgo y de cómo proteger a la empresa. Para que puedan tener esas conversaciones de concienciación".

> Las compañías y los gabinetes cada vez participan más en la elaboración de este tipo de programas

Esta necesidad surge tanto en las grandes compañías como en las que empiezan desde abajo. Así, tal como comenta Lage, es fácil encontrar una *start up* que se crea en un garaje, y que necesita recurrir a la figura de un *compliance* que garanice que cumple correctamente la regulación, para que monitorice y reporte posibles riesgos de organizaciones con las que pretendan hacer tratos comerciales. La idea es evitar sanciones por incumplimientos legales o regulatorios, y sufrir pérdidas financieras o de reputación.

La entrada en vigor del Reglamento Europeo de Protección de Datos en 2017 introdujo perfiles nuevos, como el de delegado de protección de datos (DPO), es decir, perfiles jurídicos que de forma progresiva van cobrando peso en estudios de este tipo. Tal como manifiesta Raúl Prieto, responsable del área de Gobierno de Seguridad de la Información de Sothis, los programas formativos están haciendo hincapié en dotar a los profesionales de capacidades de colaboración con otros perfiles profesionales. "Por ejemplo, el DPO debe ser capaz de trabajar junto al director de seguridad de información (CISO) para abordar las brechas de seguridad tanto desde una vertiente técnica como desde otra jurídica", aclara.

En opinión de Javier Zamora, profesor de sistemas de información en IESE, esto responde al problema generalizado de que la alta dirección ha tratado la ciberseguridad como un tema meramente tecnológico. Por eso, uno de los aspectos que destacan los títulos de transformación digital para altos directivos de esta escuela de negocios son las simulaciones de ataques hacia una institución financiera. "Así vemos el tipo de respuesta o coordinación para que conozcan las limitaciones de la tecnología y tengan una visión de 360 grados con la que, sin ser expertos técnicos, adquieran criterios para comprobar casos de negocio", expresa. Porque, según subraya, "cualquier servicio o producto, tarde o temprano, va a estar conectado y los datos que genera son el principal activo. Por eso hay que enseñar a verlo no sólo desde un punto de vista técnico, sino también de negocio".

Formar a los que ya trabajan

"El gran mercado es el de dentro de la empresa. En la dirección hacia la que vamos, la idea es crear formaciones para la gente que ya está trabajando". Así explica Robert Maxwell, director de los dobles grados de Ciberseguridad con *Business Analytics* y con Derecho en la Universidad Francisco de Vitoria, la necesidad actual de generar formaciones de corta duración para trabajadores. Si bien la oferta formativa empieza a ser cada vez más extensa –sobre todo, en posgrados–, la realidad, según Maxwell, es que existe una falta de estudios con los que actualizar conocimientos en un mundo tan cambiante, sin tener que abordar un programa de uno o dos años. "Si tu empresa está en plena transformación digital, si no sabes qué tienes que hacer, tu transformación te va a poner en riesgo dentro de ella", asevera. Por eso, este experto asegura que, en su caso, intentan paliar ese déficit con jornadas de protección de datos personales abiertas. Fundamentalmente, porque este tipo de público es el que "está en las trincheras y sabe cómo funciona esta realidad", argumenta Maxwell.