KASPERSKY lab

LAS LAGUNAS DE CONOCIMIENTO EN CIBERSEGURIDAD: UNA BOMBA DE RELOJERÍA A PUNTO DE ESTALLAR

FUTUREPROOFING CYBERSECURITY

INVESTING IN TODAY'S TALENT TO SECURE TOMORROW

Declaraciones de Eugene Kaspersky

"Vivimos en una época en la que las empresas y las organizaciones del sector público se enfrentan a amenazas de seguridad cada vez más sofisticadas. Tanto las empresas como los servicios básicos de infraestructuras y finanzas necesitan contar con empleados con las habilidades necesarias para luchar contra los ciberdelincuentes si no quieren perder la batalla.

En un entorno en el que las empresas buscan combatir la creciente amenaza de la ciberdelincuencia y evitar la irrupción masiva en la vida pública y privada, los jóvenes talentos podrían acabar con la falta de habilidades y competencias existentes en materia de ciberseguridad.

La preocupación por la falta de este tipo habilidades unido a la necesidad de solucionar el problema, han llevado a Kaspersky Lab a encargar un estudio para conocer su alcance. Queríamos saber qué les parece a los jóvenes la ciberseguridad como carrera profesional y las posibles consecuencias para las empresas y la sociedad si la brecha de conocimiento sigue aumentando.

Los resultados de este informe son sorprendentes: los jóvenes tienen grandes capacidades informáticas, sienten curiosidad por los ciberataques y demuestran interés por encontrar formas de poner en práctica sus habilidades.

Sin embargo, el estudio también indica que el sector de la ciberseguridad no está atrayendo la atención de esta generación ni proporciona a los jóvenes una vía clara para encontrar trabajo, perfeccionar sus habilidades y servir a la sociedad. En su lugar, muchos sienten la tentación de usar sus habilidades en el "lado oscuro" participando en el desarrollo de ciberamenazas, en lugar de prevenirlas.

Debido a la frecuencia y la notoriedad de los ciberataques desarrollados por adolescentes, se deben poner en marcha más acciones para atraer a los jóvenes hacia carreras profesionales en el ámbito de ciberseguridad y para que usen sus habilidades para hacer el bien. Debemos canalizar los intereses de la nueva generación de forma adecuada, antes de que sea demasiado tarde y la brecha sea todavía mayor."

KASPERSKY lab

FUTUREPROOFING CYBERSECURITY

CONCLUSIONES CLAVE

Uno de cada cuatro (27 %) ha considerado la posibilidad de seguir una carrera en seguridad. El 47 % piensa que sería una buena forma de emplear su talento.Sin embargo, otros admiten que se sienten más inclinados a participar en actividades dudosas; a utilizar sus habilidades para divertirse (17 %); a realizar actividades opacas (16 %); o a obtener beneficios económicos (11 %).

27%

El 23 % de los jóvenes de 18 años conoce a alguien que lleva a cabo ciberactividades que podrían ser ilegales (por ejemplo, hackear)

23%

Más de la mitad (57 %) de los menores de 25 años considera que ser hacker es una habilidad "impresionante".

57%

Un 73 % de las empresas afirma que les resulta difícil encontrar suficientes profesionales de seguridad TI

73%

El 87 % de las empresas cree que es importante que los jóvenes se unan a la lucha contra el cibercrimen.

87%

Introducción

Las organizaciones se están dando cuenta de que no se trata de **si** se producirá un ciberataque, sino de **cuándo**. Esto se traduce en un mayor interés de los directivos por las medidas que se adoptan para proteger su organización y, como resultado, en un creciente apoyo a la ciberseguridad. El reto es que el equipo humano dedicado a la ciberseguridad no crece a la misma velocidad.

Antes de que finalice la década está previsto que la demanda global de expertos en ciberseguridad supere en un tercio a la oferta. La encuesta sobre empleo mundial de Frost and Sullivan anticipa una carencia de 1,5 millones de profesionales de seguridad para 2020. Por ello, se debe priorizar con rapidez para poder resolver esta carencia en el área de la ciberseguridad antes de que sea demasiado tarde.

¿Está haciendo el sector lo suficiente para animar a los jóvenes a seguir carreras profesionales en el ámbito de la ciberseguridad?¿Deben esforzarse las empresas por canalizar los intereses y el talento de los jóvenes en este ámbito? ¿O tal vez deben las institucioneseducativas preparar mejor a los jóvenes con habilidades más avanzadasen ciberseguridad?

Se prevé que la demanda mundial de expertos en ciberseguridad supere la oferta antes de que acabe esta década.

Para averiguarlo, Kaspersky Lab ha realizado un estudio entre 12.000 consumidores y profesionales TI en Estados Unidos y Europa (Reino Unido, Alemania, Irlanda, Francia, Italia, España y Países Bajos). Queríamos averiguar cómo atender esta demanda del mercado en cuanto a personal cualificado dedicado a la ciberseguridad y quién debe ser el responsable de hacerlo.

Según los resultados, si queremos animar a los jóvenes a que accedan a carreras profesionales en el ámbito de la ciberseguridad y así reducir la falta de profesionales que se detecta actualmente debe existir un esfuerzo combinado del sector y del sistema educativo. Esta generación está más cerca de la tecnología que las anteriores y el peligro es que, si no se canaliza de forma adecuada, todo este talento podría sentirse tentado de usar sus habilidades para fines delictivos. Los jóvenes deben conocer mejor las oportunidades profesionales que ofrece la ciberseguridad y se les debe animar a desarrollar sus habilidades para el bien de la sociedad. Combinando la formación y el aprendizaje en el trabajo, debemos atraer a los jóvenes antes de que la brecha crezca más.

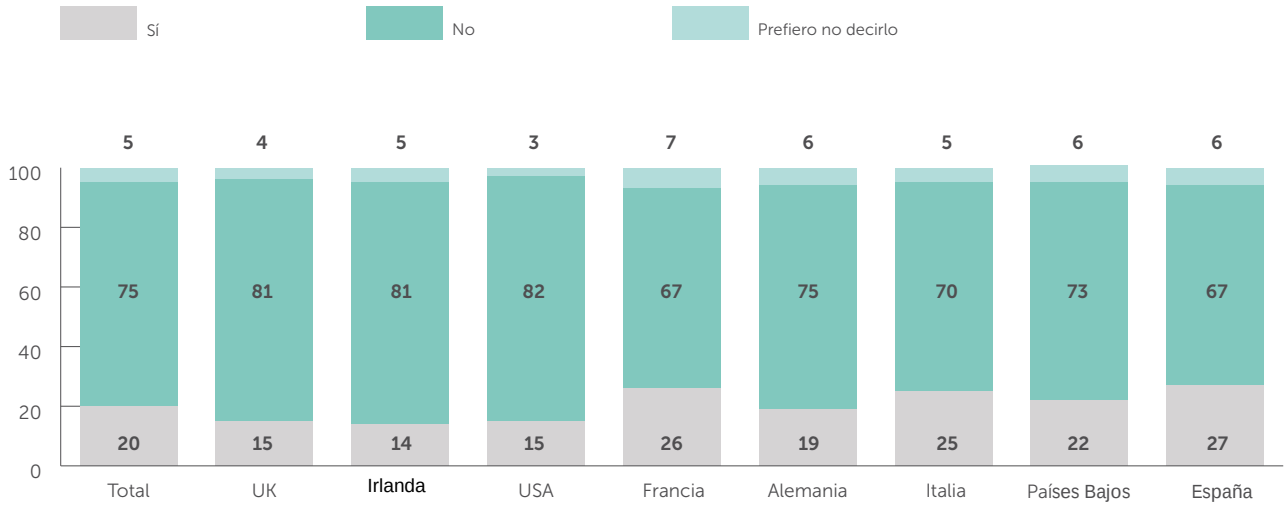
Conclusiones de la investigación

Los jóvenes se sienten atraídos por la ciberdelincuencia en lugar de evitarla

Los jóvenes de hoy día están muy cualificados, pero también son fáciles de impresionar. Como nativos digitales, estos jóvenes están completamente inmersos en el mundo digital; pero también se han acostumbrado a convivir con el impacto de los ciberataques a gran escala.

Hemos observado que el 23 % de los jóvenes de 18 años conoce a alguien cuyas actividades podrían ser ilegales (por ejemplo, hackear). Estas actividades son más frecuentes entre la gente joven en la universidad (24 %) y entre aquellos que acaban de finalizar sus estudios superiores y están trabajando (23 %). Por la otro lado, en el caso de los estudiantes que dejan la escuela y no tienen empleo el porcentaje se reduce y sólo el 15 % conoce a alguien que realiza ciberactividades que podrían ser ilegales.

¿Conoces a alguien que esté llevando a cabo actividades cibernéticas que podrían ser ilegales (por ejemplo, hacking)?



En muy pocas ocasiones su preocupación supera a su curiosidad. Algo menos de la mitad (47 %) de los menores de 25 años se sienten impresionados cuando oyen hablar de una empresa que ha sido atacada y a una tercera parte (33 %) les interesa saber cómo se realizó el ataque. También observamos que la preocupación aumenta con la edad. El 40 % de los jóvenes de 21 a 25 años afirma que les preocupa el alcance de los daños y la respuesta de la empresa, frente a sólo el 36 % de los jóvenes de 16 años.

Lo alarmante es que más de la mitad (57 %) de los menores de 25 años considera que ser hacker es una habilidad "impresionante". Un número importante de jóvenes usaría sus habilidades para divertirse (17 %), realizar actividades opacas (16 %) u obtener beneficios económicos (11 %).

Muchos jóvenes son expertos en eliminar su rastro: un tercio de los menores de 25 años (31 %) sabe ocultar su dirección IP. Y si tenemos en cuenta que sólo el 50 % se uniría a la lucha contra la ciberdelincuencia, se hace evidente la falta de implicación a la hora de usar sus habilidades para combatir los delitos.

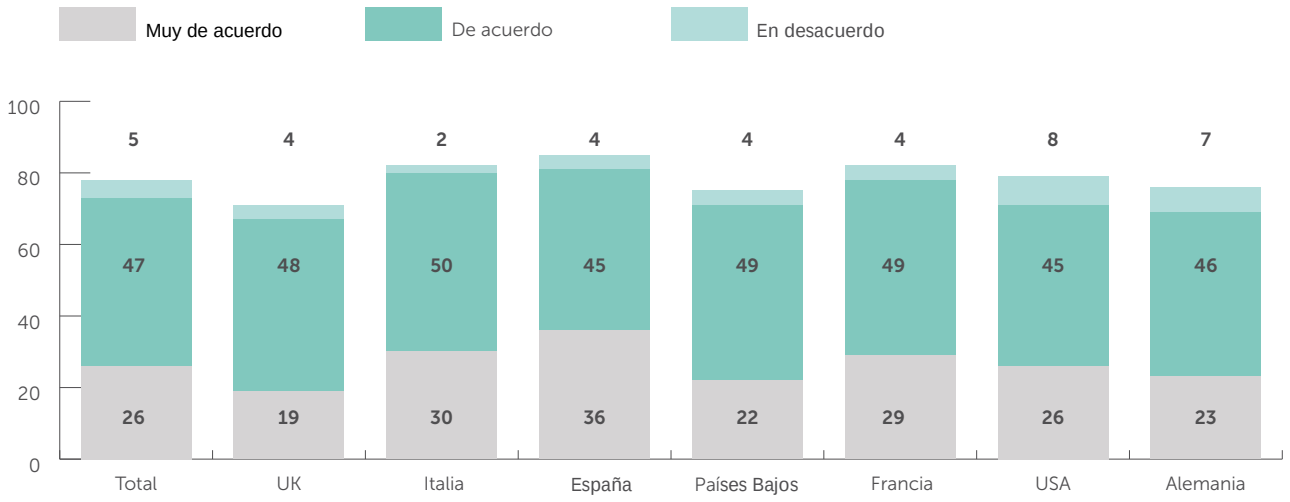
Las empresas necesitan jóvenes que les ayuden a luchar contra la ciberdelincuencia

Dada la creciente escasez de personal con habilidades cibernéticas, los jóvenes aficionados a las TI tienen la llave para ocupar nuevos puestos de trabajo en ciberseguridad. Este grupo tiene los conocimientos y las ganas de aprender, pero las empresas no canalizan sus intereses ni su talento hacia este ámbito.

Un gran número de profesionales del sector (93 %) reconoce que la profesión debe evolucionar con el panorama actual y futuro, y el 87 % cree que es importante que los jóvenes se unan a la lucha contra el cibercrimen.

El problema es que muchas empresas no tienen ningún puesto de ciberseguridad de primer empleo; la mayoría realizan promociones internas (72 %), con formación interna en función de las necesidades, y contratan externamente (53 %) a expertos de seguridad.

¿En qué medida está de acuerdo con la afirmación: "Es difícil encontrar profesionales enfocados en seguridad TI?



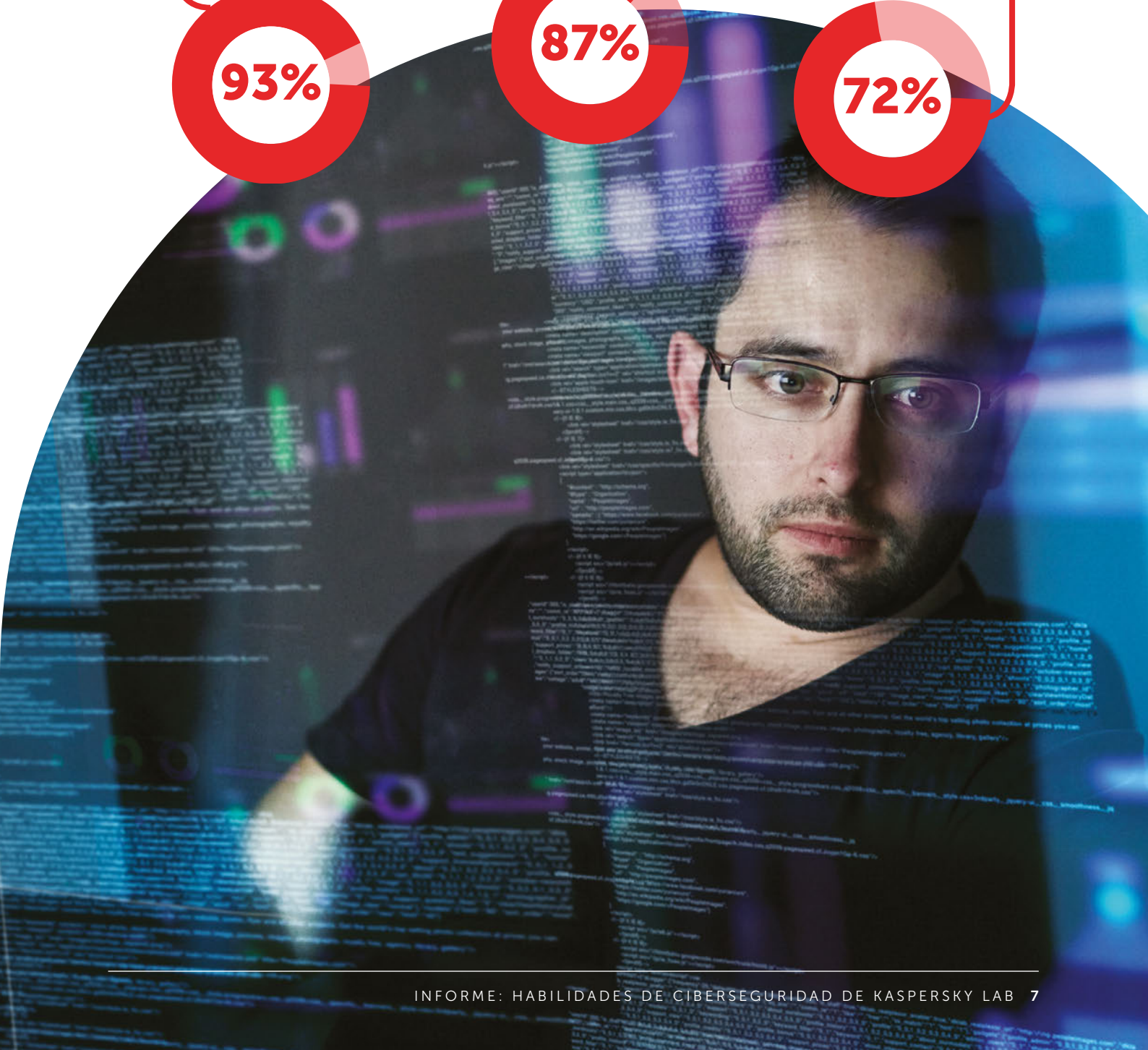
Es importante reconocer que, tal y como sucede con cualquier disciplina en el campo TI, las habilidades de seguridad se desarrollan con el tiempo. Cada uno tiene su puesto en función de sus habilidades, aprende en el trabajo y recibe la formación adecuada. Pero si tenemos en cuenta que casi tres cuartas partes (73 %) de las empresas considera que es difícil contratar profesionales de TI con las competencias adecuadas, ¿ha llegado el momento de rediseñar las vías tradicionales de acceso a la profesión de la ciberseguridad?

PRINCIPALES CONCLUSIONES

Un gran número de profesionales del sector (93%) reconoce que la profesión tiene que evolucionar al mismo ritmo que el entorno tecnológico actual y futuro.

El 87% cree que es importante que los jóvenes se unan a la lucha contra el cibercrimen.

Muchos empleados no tienen conocimientos sobre ciberseguridad; muchos son promocionados internamente (72%), con formación interna según las necesidades.

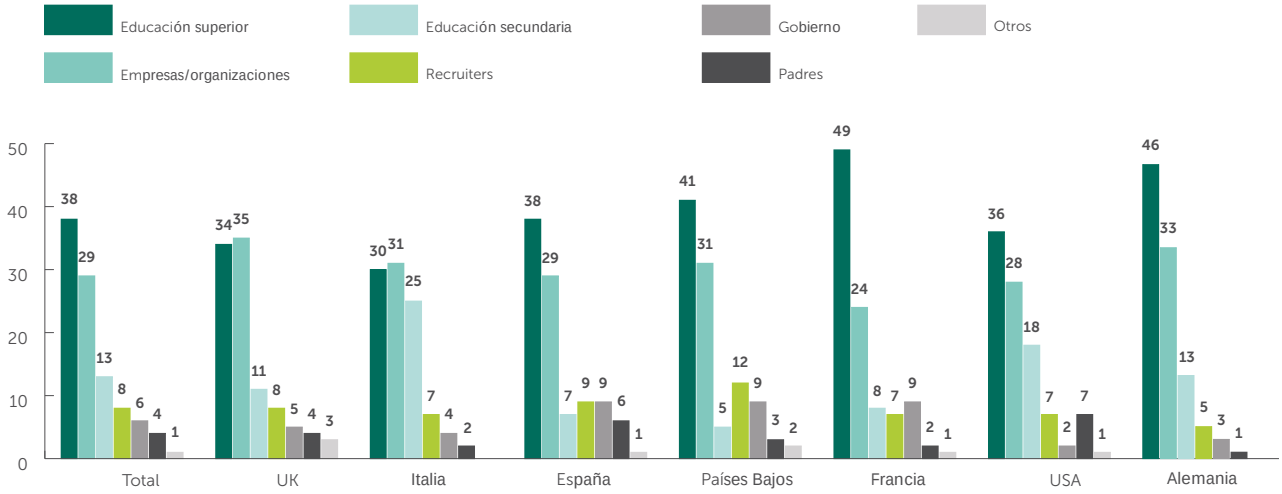


¿La responsabilidad es de las empresas o de los educadores?

La cuestión de quién es el responsable de atraer a la siguiente generación de talentos y el alcance del reto son de vital importancia. Necesitamos un plan que se base en el interés antes de que las mentes brillantes y curiosas den la espalda a la seguridad y usen sus habilidades para fines delictivos.

Según el sector TI, el sistema educativo desempeña un papel fundamental para animar a los jóvenes a acceder a la profesión y dotarles del nivel de habilidades y competencias necesarias. Según nuestro estudio, casi dos tercios de profesionales TI (62 %) consideran que son principalmente los centros educativos los que deben encargarse de preparar a las futuras generaciones de profesionales. El sector también tiene una función clara y primordial para garantizar su propio futuro, según el 27 % de los profesionales que atribuyen laresponsabilidad principal a la empresa.

Quién debe asumir la responsabilidad de fomentar el talento joven en la profesión?



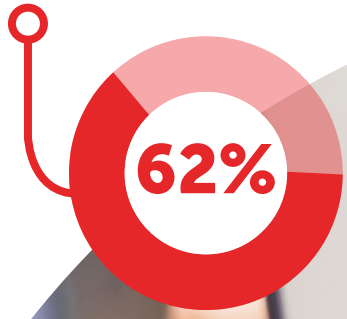
Curiosamente, en el estudio se detectaron diferencias importantes entre países en lo que se refiere a definir si la responsabilidad es del sistema educativo o de la empresa. En el Reino Unido se considera que las empresas tienen más responsabilidad: más de un tercio (35 %) de los encuestados afirma que las empresas deben contribuir más para ayudar a los jóvenes a incorporarse a los puestos de ciberseguridad. Por el contrario, en Italia (25 %) y Estados Unidos (18 %) se hace más hincapié en la educación secundaria, en comparación con la media, del 13 %.

En lo que respecta a garantizar que los jóvenes cuenten con las habilidades adecuadas, en general se hace más hincapié en una formación superior (49 %) y en las empresas y las organizaciones (27%). Pero, una vez más, observamos diferencias en función del país; por ejemplo, en los Países Bajos se espera más de las empresas (40 %).

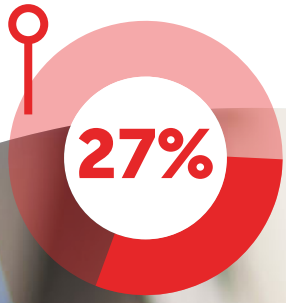
Evidentemente, existen diferencias debido a los diversos sistemas de educación y las prioridades del gobierno, pero, en realidad, se necesita un enfoque conjunto que una a las empresas y a los centros educativos para desarrollar e inculcar estas competencias a una generación ávida de tecnología.

PRINCIPALES CONCLUSIONES

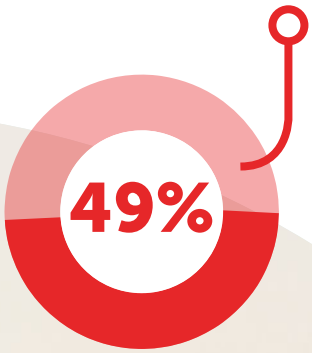
Según nuestra investigación, casi dos tercios de los profesionales TI (62%) consideraron que los centros de enseñanza son los principales responsables de la preparación de las futuras generaciones de profesionales.



La industria también tiene un papel claro a la hora de garantizar su propio futuro, con un 27% de los encuestados que cree que son las empresas las que deben asumir esta responsabilidad.



A la hora de garantizar que los jóvenes tengan las competencias adecuadas, en general, se debe poner mayor énfasis en la educación superior (49%).



Garantizar el futuro del sector de la seguridad

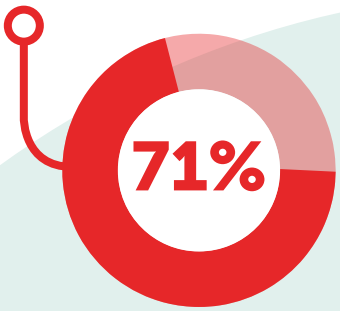
Se debe hacer más para desarrollar y atraer a los jóvenes talentos al sector porque la creciente laguna de conocimiento en el ámbito de la ciberseguridad es una bomba de relojería a punto de estallar.

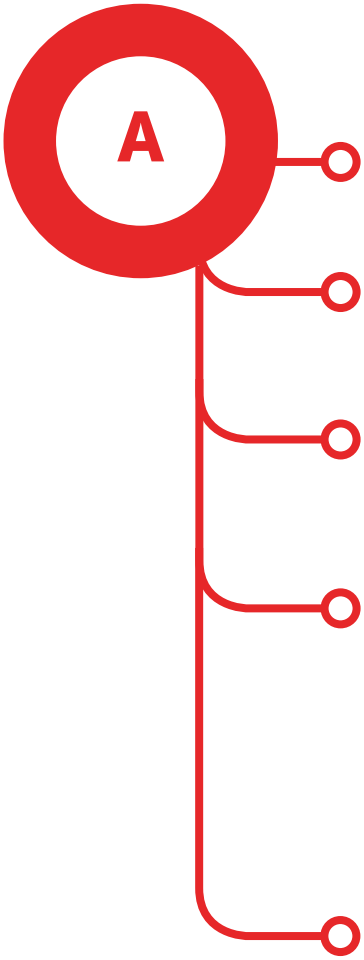
Debemos conseguir que a estos jóvenes cualificados les resulte más fácil y atractivo incorporarse al sector. Prácticamente tres cuartas partes de los jóvenes (71 %) no conocen las oportunidades de educación superior o prácticas en seguridad TI.

Aunque las empresas argumentan que los nuevos jóvenes no tienen habilidades prácticas sobre ciberseguridad ni la experiencia necesaria, muy pocas ofrecen puestos de primer empleo o en prácticas que puedan contribuir a conducir ese talento. De hecho, solo el 45 % tiene puestos o programas para recién licenciados.

Tres de cada diez (30 %) admiten que no disponen de los recursos internos para desarrollar licenciados en una función de ciberseguridad. Lo que es más preocupante es que solo uno de cada cinco (21 %) considera que un equipo de ciberseguridad tendría la responsabilidad exclusiva de la seguridad TI en el plazo de cinco años, y la mitad (50 %) cree que un equipo de TI más amplio debería ocuparse de la ciberdelincuencia.

Casi tres cuartas partes de los jóvenes (71%) no son conscientes de las oportunidades que ofrecen los postgrados en seguridad TI o las prácticas.





¿Cuál es la respuesta?

Según Kaspersky Lab, este informe es el inicio de un largo viaje para reducir la brecha de conocimientos cibernéticos. Resolver un problema de este calibre requiere los esfuerzos coordinados del sector, el sistema educativo y el gobierno.

Consideramos que las empresas deben llevar a cabo más acciones para animar a los jóvenes a seguir carreras profesionales en al ámbito de la ciberseguridad. Incluso entre los profesionales de seguridad TI, el 27 % admite que las organizaciones deben esforzarse más en ofrecer formación y programas para titulados superiores.

Las iniciativas impulsadas por el sector pueden contribuir a promocionar las carreras profesionales. Los concursos internacionales dirigidos a universitarios y jóvenes profesionales, por ejemplo, animan a los nuevos talentos a usar sus habilidades para afrontar varios retos de ciberseguridad, lo que les permite mostrar lo valiosos que serían para el sector y la sociedad en general.

Nuestro sector, si colabora estrechamente con las universidades, puede ser fundamental para desarrollar el talento y garantizar que los aprendizajes teóricos y prácticos responden a las expectativas y las necesidades futuras. Mediante diversas iniciativas, como asesoramiento sobre materiales de estudio, conferencias, presentación de tecnologías y colaboración en la investigación, el sector puede contribuir a animar, atraer y, lo que es más importante, informar y formar a la siguiente generación de ciberdefensores. Con la oferta de contratación, prácticas y puestos para licenciados, se sentarían unas bases sólidas en la relación entre el sector y el sistema educativo, lo que evitará que se desaprovechen habilidades valiosascuando más las necesitamos.

Las conclusiones de este informe ponen de manifiesto la magnitud de los desafíos a los que se enfrenta la industria, además de señalar varias áreas en las que se pueden hacer progresos. Debemos adoptar esta medidas para desactivar la bomba de relojería de la ciberseguridad antes de que estalle.

1 Datos de la encuesta: Kaspersky Lab encargó a Arlington Research encuestar a un total de 2.120 profesionales TI y a 11.531 jóvenes (de entre 16 y 25 años) en el Reino Unido, Italia, Irlanda, España, Países Bajos, Francia, Alemania y EE.UU. Ambos grupos de investigación se completaron en julio de 2016.

KASPERSKY LAB

Kaspersky Lab, 1st Floor
2 Kingdom Street
London, W2 6BD, UK

www.kaspersky.co.uk

KASPERSKY lab

FUTUREPROOFING CYBERSECURITY

INVESTING IN TODAY'S TALENT TO SECURE TOMORROW