La escasez de talento en el mundo de la ciberseguridad

Jennifer Sesmero - Global Head of Talent and Training in Cybersecurity BBVA
7 July 2023

Actualmente, el talento en ciberseguridad está cobrando una mayor importancia en las empresas, provocado principalmente por el aumento de amenazas cibernéticas y la necesidad de protección de datos y otros activos digitales. La falta de recursos y la escasez de profesionales de ciberseguridad cualificados para abordar estos desafíos, unido a los diferentes fenómenos psicosociales que se han dado en los últimos años, hacen que las empresas nos reinventemos y busquemos nuevas fórmulas para mitigar el impacto de la escasez de talento en ciberseguridad a nivel global.

Atendiendo al contexto actual de incertidumbre y crisis económico social, se ha acelerado una profunda reflexión de los modelos de trabajo por parte de los individuos. Esta reflexión se ha materializado en el suceso denominado "la gran renuncia" que se dió en USA, debido principalmente a las consecuencias del shock emocional que supuso la pandemia. Más de 47,8 millones de trabajadores de Estados Unidos en 2021, dejaron su empleo de forma voluntaria, según el Departamento de Trabajo. El efecto de este movimiento ha provocado que el 50% de los empresarios no puedan cubrir vacantes de empleo. Por otra parte, se ha visibilizado que muchos de estos perfiles que renunciaron a su puesto fue para obtener otro y con ello, mejorar sus condiciones laborales.

Esta situación ha evolucionado a otro fenómeno no menos preocupante, el denominado *"quiet quitting*", donde el propio empleado ciñe sus tareas a aquellas estrictamente descritas en su función y establece límites claros para mejorar el equilibrio entre el trabajo y la vida personal. Con esta práctica se podría llegar a suponer que el talento se autolimita y más en un mundo tan innovador y cambiante como es el de la ciberseguridad.

La transformación digital agrava este problema según el reciente informe de ISC2, el déficit mundial de talento en ciberseguridad aumenta un 26% en el último año hasta los 3,4 millones. Se necesitan en todo el mundo 8,1 millones de expertos en ciberseguridad, de los cuales actualmente estamos trabajando 4,7 millones de profesionales.

Y sin dejar de lado la gran ola de despidos en las grandes tecnológicas, que suman ya más de 150.000 bajas. Las diferentes causas y estrategias de reorganización de plantilla no permiten sacar conclusiones sobre una posible recesión en el mercado de perfiles tecnológicos, en concreto de

ciberseguridad. Las empresas tecnológicas, animadas por unos ingresos récord, emprendieron una carrera desenfrenada de contratación durante la pandemia. Los salarios alcanzaron niveles muy altos al mismo tiempo que la competencia se disputaban a los mejores. Por este motivo, la media de un empleado en un mismo puesto, no superaba los 2 años. Y, a medida que la vuelta a la normalidad se hacía más efectiva, llegaron los despidos.

Si analizamos esto último se evidencia que las compañías implicadas han integrado diversas razones para justificar esta decisión, que en su mayoría se reducen a la necesidad de minimizar costes a medida que el crecimiento económico se ralentiza a nivel global. Pero en lo que nos compete a nosotros, en cuanto a perfiles de ciberseguridad, para abordar este gran reto de talento, las organizaciones deberán plantear de forma diferente una estrategia completa en materia de gestión de talento '*end to end*'.

Esta estrategia de gestión de talento '*end to end*' está basada en unos principios de diseño que todas las compañías deberían integrar en su ADN acompañado de una serie de planes y programas. El objetivo es poder garantizar que en los próximos años dispongamos del mejor equipo y talento suficiente para hacer frente a las amenazas crecientes y poder mantener así los altos estándares de seguridad en las compañías.

En nuestro caso, nos apoyamos en una serie de principios de diseño, entre ellos, destacan:

1. Acceder al mejor talento a nivel mundial. Como he comentado en puntos anteriores, la escasez de talento en el mundo de la ciberseguridad está muy presente actualmente. Con este principio de diseño y basándonos en nuestros planes de formación y desarrollo, no sólo queremos disponer de talento en ciberseguridad, sino tener el mejor talento, en definitiva, conformar el mejor equipo.

2. Posicionarse como marca empleadora de referencia en materia de ciberseguridad y mantenerse en el tiempo.

Este principio va muy en línea con el anterior. Tenemos que potenciar aún más que nuestra organización sea una marca empleadora y atrayente en el mercado en este ámbito. Para eso tenemos una ardua labor de transparentar todo el trabajo que llevamos haciendo durante años en los equipos más técnicos de ciberseguridad y cómo lo hacemos en el campo de la ciberseguridad, con el objetivo de que la entidad sea uno de los mejores lugares para trabajar del sector.

3. Cuidar el talento interno, una prioridad.

Cuando nos referimos a talento interno, hablamos de cualquier empleado que trabaje dentro de la organización, que no se encuentre dentro del equipo de ciberseguridad, pero que se haya planteado realizar un "*reskilling*" o, lo que es lo mismo, cambiar de profesión.

Hay que apostar por capacitar y desarrollar nuestro talento interno y para eso debemos accionar diferentes palancas. Primeramente, formación puntera.

Para ello, contamos con el mejor certificador a nivel mundial en ciberseguridad, SANS (sans.org). Y, además, potenciamos la flexibilidad entre nuestros equipos, apoyándonos en un modelo híbrido de teletrabajo y ofrecemos un amplio catálogo de más de 80 cursos de formación especializada en ciberseguridad, desarrollados por expertos en el campo dentro de la organización.

Como conclusión, la gestión de este talento ha de hacerse de forma global y homogénea. Cuando nos referimos al talento especializado en ciberseguridad, estamos hablando de individuos con la capacidad de aprender rápidamente. La industria de la seguridad informática es altamente dinámica, por lo que los profesionales deben mantenerse actualizados de manera constante.

Por lo tanto, tenemos que contratar a personas con experiencia en ciberseguridad, formar nuevos profesionales a través de programas de capacitación, tanto internos como externos, y desarrollar soluciones tecnológicas avanzadas para prevenir y detectar amenazas.