Prensa Capgemini
Paqui López /Ángeles García Molero
Tel: +34 916577000
Sofía García/Ramón Corpas
Tel: + 34 915312388

Responsables del mundo empresarial advierten de la necesidad urgente de reforzar la oferta profesional en competencias de ciberseguridad ante el aumento de la brecha digital

Un nuevo estudio revela que la demanda de competencias en materia de ciberseguridad en las empresas está creciendo más rápido que la oferta interna y que hacen falta ideas innovadoras para reducir la diferencia, tanto en la búsqueda como en la retención de talento digital

Madrid, 26 de febrero de 2018 – Un informe del Instituto de Transformación Digital de Capgemini pone de relieve el aumento de la brecha en materia de competencias de ciberseguridad y la necesidad urgente de implantar nuevas estrategias de búsqueda y retención de personal con esas habilidades para que las organizaciones limiten los ciberriesgos y generen ventajas competitivas. El informe, *Cybersecurity Talent: The Big Gap in Cyber Protection*, muestra que, de todas las competencias digitales necesarias para las organizaciones con aspiraciones al liderazgo digital, las relativas a la ciberseguridad son las que presentan una mayor brecha entre la demanda y la oferta.

Para el estudio se encuestó a más de 1.200 directivos de alta dirección y empleados, y se analizó el sentimiento en redes sociales de más de 8.000 empleados de ciberseguridad. El 68% de las empresas declaró tener una necesidad alta de competencias de ciberseguridad, frente al 61% que necesitaba competencias de innovación y el 64%, competencias analíticas. La demanda de estas competencias se comparó a continuación con la disponibilidad de profesionales especializados ya en plantilla. El resultado fue una diferencia de 25 puntos porcentuales en competencias de ciberseguridad (con una disponibilidad del 43% de personas con conocimientos especializados ya presentes en la organización), frente a una diferencia de 13 puntos porcentuales en competencias analíticas (51% ya presente) y de 21 puntos porcentuales en competencias de innovación (40% ya presente).

"La deficiencia de competencias en materia de ciberseguridad tiene un efecto muy real en las organizaciones", afirma Mike Turner, director de Operaciones de la práctica de Ciberseguridad de Capgemini a nivel mundial. *"Invertir meses y no semanas en encontrar candidatos adecuados no solo resulta ineficiente, sino que, además, deja a las organizaciones peligrosamente expuestas a los casos cada vez más extendidos de ciberataques. Los responsables de las empresas deben replantearse con urgencia la manera de buscar y retener talento en este campo, especialmente si desean maximizar los beneficios de la inversión en transformación digital".*

Según las previsiones, la demanda de personas con conocimientos en ciberseguridad es ya una realidad que, además, aumentará en el futuro: un 68% de los encuestados señala que existe una alta demanda de estos perfiles hoy en día, y el porcentaje aumenta hasta el 72% ante la cuestión de si está necesidad continuará en 2020. En un contexto de crecientes casos de ciberataques y en un momento en el que las organizaciones tienen necesidad no solo de protegerse sino también de conseguir la máxima ventaja competitiva de su digitalización, el informe recomienda el establecimiento de una serie de prioridades tácticas a los responsables del mundo empresarial.

Prioridad 1 – integrar seguridad
La primera prioridad para las empresas es determinar el grado de integración eficaz de la seguridad en la organización. ¿Qué cultura de ciberseguridad hay, más allá del equipo con responsabilidad directa en la protección de datos? ¿Cuánto conocimiento tienen sobre seguridad los desarrolladores de aplicaciones y gestores de redes?

"Es importante mejorar el área de ciberseguridad en el conjunto de la organización, dotando a la empresa de principios y procesos que sean seguros en todos los niveles de la organización", explica Mike Turner. *"Establecer correctamente los fundamentos en el desarrollo de aplicaciones; desarrollar un código seguro; mejorar la capacidad de los ingenieros de redes y los arquitectos cloud de garantizar la seguridad de la nube. Esta es una buena manera de cerrar la brecha de competencias, porque enseña a la organización a ser segura desde su diseño".*

Prioridad 2 – maximizar el conjunto de competencias ya existente
"Otra prioridad es sacar a la luz las competencias de seguridad que ya existen, pero que no se han reconocido todavía. La mitad de todos los empleados invierte sus propios recursos en desarrollar competencias digitales[1], lo que demuestra sus ganas de mejorar. Las organizaciones a las que les cuesta conseguir talento exterior pueden encontrar trabajadores cuyas competencias pueden adaptarse con la formación adecuada. Las funciones con competencias complementarias y transferibles son, entre otras, las de operaciones en la red, administración de bases de datos y desarrollo de aplicaciones".

Asimismo, las empresas deben pensar en la necesidad de integrar la seguridad en todos los servicios y aplicaciones y contratar a comunicadores de empresa que complementen los conocimientos técnicos de su equipo. Analistas de negocio y personal de marketing podrían ser transferidos a puestos encargados de ciberseguridad para la adopción de buenas prácticas en toda la compañía.

Prioridad 3 – salir del camino preestablecido
Una tercera prioridad es que las organizaciones vayan más allá de las estrategias habituales de reclutamiento y entiendan las competencias básicas en materia de ciberseguridad. Buscar cualidades y capacidades ya presentes en perfiles de trabajo completamente diferentes y entrevistar a candidatos a los que normalmente la empresa no prestaría atención. Las personas que desempeñan funciones matemáticas, por ejemplo, tienen a menudo una capacidad alta de reconocimiento de patrones. *"Cambiar el punto de vista ayuda a ver las competencias que son transferibles",* añade Mike Turner.

Prioridad 4 – reforzar la retención de capital humano
La última recomendación del informe se refiere a la retención del talento. En un mercado laboral tan competitivo, las organizaciones deben esforzarse también por conservar a los empleados que ya tienen para no empeorar la falta de competencias.

El informe revela que los empleados con conocimientos de ciberseguridad valoran las organizaciones que ofrecen condiciones flexibles de trabajo, fomentan el aprendizaje y dan prioridad a un desarrollo profesional claro y accesible. Según las respuestas dadas por los profesionales de ciberseguridad en las redes sociales, uno de los cinco peores aspectos de su puesto es la difícil conciliación entre la vida personal y la profesional, lo que se convierte en una de las principales razones para abandonar una empresa. Una gran mayoría (81%) de los empleados del área de ciberseguridad estuvieron de acuerdo con la siguiente afirmación: *"Prefiero*

[1] Informe publicado por Capgemini con la colaboración de LinkedIn: "The Digital Talent Gap—Are Companies Doing Enough?"

trabajar en organizaciones en las que puedo tener una oportunidad clara de desarrollo profesional", frente al 62% del conjunto de los empleados de diferentes departamentos encuestados. El número es incluso mayor (84%) para los empleados de ciberseguridad de las generaciones Y y Z[2], que resaltaron la falta de progresión profesional como motivo principal de preocupación. Resolver estas otras cuestiones es también un requisito fundamental para crear una oferta viable y sostenible en el campo de la ciberseguridad.

Metodología del estudio

El Instituto de Transformación Digital de Capgemini encuestó a 1.200 directivos y empleados de empresas con una facturación de más de 500 millones de dólares en 2016 y una plantilla de más de 1.000 empleados. La encuesta se realizó entre junio y julio de 2017 e incluyó nueve países: España, Francia, Alemania, India, Italia, Países Bajos, Suecia, Reino Unido y Estados Unidos; y siete sectores: automoción, banca, productos de consumo, seguros, retail, telecomunicaciones y suministros básicos.

Capgemini también realizó entrevistas en profundidad a responsables de recursos humanos de empresas internacionales, asociaciones de ciberseguridad y el mundo académico para conocer las mejores prácticas para la reducción de la brecha de competencias de ciberseguridad. Por último, se analizó el sentimiento en redes sociales de 8.400 actuales y antiguos empleados de 53 empresas de ciberseguridad con una plantilla de al menos 100 personas. Las empresas seleccionadas operan principalmente en el ámbito de la ciberseguridad, en especial en las áreas de seguridad de datos, seguridad de la nube, seguridad de las comunicaciones móviles, seguridad de las empresas, seguridad del correo electrónico y seguridad de aplicaciones.

El informe puede descargarse aquí

Acerca de Capgemini

Un líder global en servicios de consultoría, servicios de tecnología y transformación digital, Capgemini está a la vanguardia de la innovación para abordar la diversidad de oportunidades que tienen sus empresas clientes en el dinámico entorno de las plataformas, la nube y lo digital. Respaldada por una sólida trayectoria de 50 años y una dilatada experiencia multisectorial, Capgemini ayuda a las compañías a alcanzar sus objetivos de negocio mediante una amplia gama de servicios que cubre desde la estrategia, hasta las operaciones. Capgemini actúa bajo la firme convicción de que el valor de negocio de la tecnología se genera y desarrolla a través de las personas. Capgemini es una compañía multicultural de 200.000 profesionales, presente en más de 40 países y, en 2017, registró unos ingresos mundiales de 12.800 millones de euros.

Más información en https://www.capgemini.com/es-es/ *People matter, results count*

Acerca del Instituto de Transformación Digital **de Capgemini**

El Instituto de Transformación Digital es el think tank interno de Capgemini para el estudio del ámbito digital. El instituto publica investigaciones sobre el impacto de las tecnologías digitales en grandes negocios tradicionales. El equipo se apoya en la red mundial de expertos de Capgemini y trabaja codo con codo con socios académicos y tecnológicos. El instituto cuenta con centros de investigación especializados en Estados Unidos, Reino Unido y la India.

[2] Las generaciones Y y Z están compuestas por aquellos entre 18 y 36 años.