



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

El 69% de las empresas cree que no será capaz de responder a las amenazas de ciberseguridad sin la inteligencia artificial

En 2020, dos de cada tres planea implantar IA para reforzar sus sistemas de defensa

Madrid, 11 de julio de 2019 – Las empresas están aumentando el ritmo de inversión en sistemas de IA como defensa frente a la siguiente generación de ciberataques, concluye un nuevo estudio del [Instituto de Investigación de Capgemini](#). Dos tercios (69%) de las compañías reconocen que no podrán responder a las amenazas críticas sin IA. Con un número en aumento de dispositivos para usuarios finales, redes e interfaces de usuario como resultado de los avances en la nube, el Internet de las Cosas (IoT), la 5G y las tecnologías de interfaz conversacional, las organizaciones se enfrentan a la urgente necesidad de ampliar y mejorar continuamente su sistema de ciberseguridad.

Para el estudio, bajo el título [Reinventing Cybersecurity with Artificial Intelligence: the new frontier in digital security](#), se entrevistó a 850 ejecutivos de alta dirección de las áreas TIC de seguridad y operaciones de empresas de siete sectores y en diez países, incluido España. También se realizaron entrevistas en profundidad con expertos del sector, startups de ciberseguridad y representantes del mundo académico.

Estas son sus principales conclusiones:

La ciberseguridad basada en IA es hoy imprescindible: Más de la mitad (56%) de los directivos afirma que sus analistas de ciberseguridad se ven desbordados por el inmenso volumen de unidades de información que deben vigilar para detectar y prevenir intrusiones. Además, el tipo de ciberataques que requieren una intervención inmediata o que no pueden ser solucionados con rapidez suficiente por los ciberanalistas ha crecido considerablemente, en particular:

- Ciberataques que afectan a las aplicaciones sujetas a exigencias temporales (el 42% contesta que han aumentado las incidencias. De media, el tipo de estas incidencias ha crecido un 16%).
- Ataques automatizados, a velocidades que sólo una máquina puede alcanzar, que mutan a un ritmo que no puede ser neutralizado mediante sistemas de respuesta tradicionales (el 43% declara un aumento de ataques con esta velocidad. A su vez, estas ofensivas han crecido un 15% de media).

Ante estas nuevas amenazas, una clara mayoría de empresas (69%) cree que no va a tener capacidad para responder a los ciberataques sin el uso de la IA, y el 61% afirma que necesita IA para identificar las amenazas críticas. Uno de cada cinco directivos ha experimentado una brecha de ciberseguridad en 2018, de las que el 20% costó a su organización más de 50 millones de USD.



Los directivos aceleran la inversión en IA por razones de ciberseguridad: Una clara mayoría de directivos acepta que la IA es fundamental para el futuro de la ciberseguridad:

- El 64% contesta que reduce el coste de la detección de brechas de seguridad y de la respuesta a estas brechas, que cae un 12% de media.
- El 74% indica que permite disminuir el tiempo de respuesta: una reducción del 12% del tiempo necesario para detectar amenazas, reparar las brechas e implementar parches.
- El 69% afirma también que la IA mejora la precisión en la tarea de detección de brechas y el 60% asegura que aumenta la eficiencia de los analistas de ciberseguridad, reduciendo el tiempo que invierten en el análisis de falsos positivos y aumentando la productividad.

En consecuencia, cerca de la mitad (48%) contesta que los presupuestos para la IA en ciberseguridad se incrementarán en 2020 en casi un tercio (29%). En términos de despliegue, el 73% está realizando ensayos de casos de uso para IA en ciberseguridad. Solo una de cada cinco empresas utilizaba IA en el área de ciberseguridad antes de 2019, pero se espera una expansión meteórica de su adopción: cerca de dos de cada tres (63%) organizaciones planea desplegar IA en 2020 para dar reforzar sus sistemas de defensa.

"La IA ofrece enormes oportunidades en materia de ciberseguridad", afirma Oliver Scherer, CISO de Grupo MediaMarktSaturn Retail, líder europeo en distribución minorista de electrónica de consumo. "Esto se debe a que permite pasar de la detección, la reacción y la subsanación manuales a un sistema automático de reparación, algo que las organizaciones querrían conseguir en los próximos tres o cinco años".

Sin embargo, existen importantes barreras para la implantación de la IA a escala general: El reto más importante para la implantación de la IA en el campo de la ciberseguridad es la dificultad para transformar los casos de uso de pruebas de concepto en un despliegue completo en todos los niveles de la organización. El 69% de los encuestados admite que está teniendo dificultades en esta área.

Geert van der Linden, responsable del área de Ciberseguridad del Grupo Capgemini explica: *"Las organizaciones se enfrentan a un volumen sin parangón de ciberamenazas de gran complejidad y se han dado cuenta de la importancia de la IA como primera línea de defensa. Los analistas en materia de seguridad están desbordados y casi una cuarta parte de ellos declara que no es capaz de analizar con éxito todos los incidentes identificados, por lo que es fundamental que las organizaciones incrementen su inversión y se centren en los beneficios que la IA puede aportar a sus empresas mejorando sustancialmente su ciberseguridad".*

Por otro lado, la mitad de las organizaciones consultadas señala también el problema de la integración con sus infraestructuras, sistemas de datos y contexto de aplicaciones actuales. Si bien la mayoría de los directivos contesta que sabe lo que quiere conseguir con la ciberseguridad basada en la IA, solo la mitad (54%) ha identificado las series de datos que se requieren para hacer operativos los algoritmos de IA.

Por su parte, Anne-Laure Thieullent, responsable de AI & Analytics de Capgemini concluye: *"Las organizaciones deben dirigir primero sus esfuerzos a resolver los problemas subyacentes de implementación que impiden que la IA alcance todo su potencial de ciberseguridad. Esto significa crear una hoja de ruta para la eliminación de las barreras principales y centrarse en los casos de uso que más*



fácilmente puedan aplicarse en toda la organización y que ofrezcan los mejores resultados. Las empresas deben seguir estos pasos si quieren estar preparadas para hacer frente al ritmo de cambio constante de las amenazas cibernéticas. De ese modo, ahorrarán dinero y reducirán la probabilidad de una violación devastadora de la seguridad de sus datos”.

El informe puede descargarse [aquí](#).

Field Code Changed

Metodología de la investigación

Para realizar el informe se consultó a 850 altos directivos de empresas de siete sectores (productos de consumo, retail, banca, seguros, automoción, *utilities* y telecomunicaciones) con sedes en Alemania, Australia, España, Estados Unidos, Francia, Italia, Países Bajos, Reino Unido, Suecia e India. Una quinta parte de los ejecutivos eran directores de tecnologías de la información (CIO) y uno de cada diez, directores de seguridad de la información (CISO) en sus respectivas empresas. El Instituto de Investigación de Capgemini también realizó entrevistas en profundidad a representantes destacados del mundo empresarial y académico sobre la situación actual y el impacto de la IA en el campo de la ciberseguridad.

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 2018, registró unos ingresos mundiales de 13.200 millones de euros.

Más información en www.capgemini.com/es-es/

People matter, results count

Acerca del Instituto de Investigación de Capgemini

El Instituto de Investigación 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. Recientemente ha sido reconocido como líder por la calidad de sus informes por analistas independientes.

Más información en www.capgemini.com/es-es/instituto-de-investigacion-de-capgemini/