# Estado de ciberseguridad en España 2023

La ciberseguridad es un tema de creciente importancia para las empresas, gobiernos y organizaciones de todo el mundo. El aumento de la digitalización y la conectividad, junto con la sofisticación de las técnicas de ciberataque, han hecho que la seguridad de la información sea una prioridad para todos los actores.

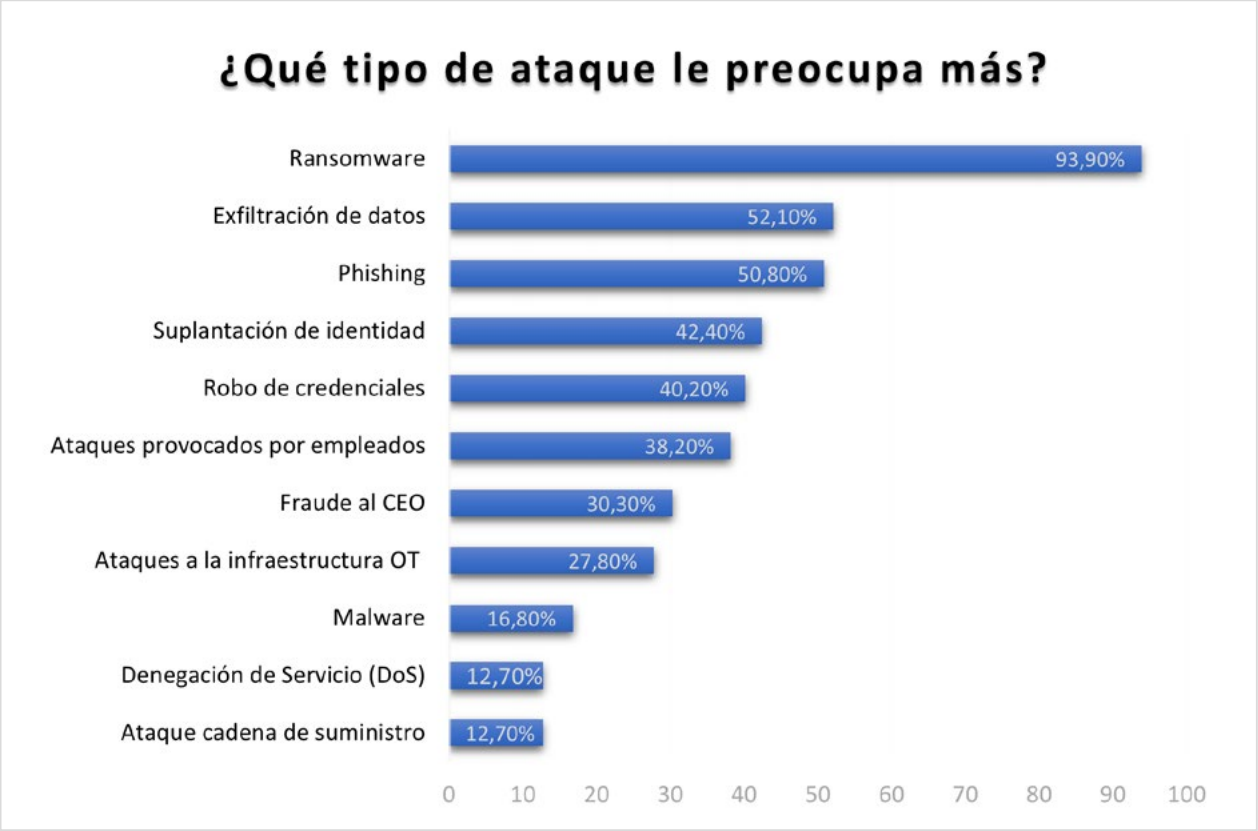
La ciberseguridad tiene un impacto directo en las empresas, ya que puede afectar a su funcionamiento, reputación y rentabilidad. Los ciberataques pueden provocar la pérdida de datos, el robo de información confidencial, el chantaje o el bloqueo de sistemas.

> “El estado de la ciberseguridad en España es una preocupación creciente”

La sofisticación de las técnicas de ciberataque, la escasez de talento cualificado o la falta de concienciación son algunos de los retos a los que se enfrentan los responsables de ciberseguridad. Para hacer frente a los mismos las empresas están invirtiendo en una serie de tecnologías de protección, entre las que se incluyen: Seguridad de la nube, de los endpoints, de la red o de los datos.

Con el objetivo de conocer la realidad de la empresa, Ciberseguridad TIC, en colaboración con Secure&IT, ha realizado una encuesta entre profesionales españoles para conocer qué tipo de amenaza preocupa más a las empresas, qué tipo de tecnologías tiene implantadas en su empresa, cómo impacta la situación geopolítica o cuales son los proyectos que tienen previsto abordar en el corto plazo.

# ¿Qué tipo de ataque le preocupa más?




**Las empresas deben estar preparadas para hacer frente a una amplia gama de ciberamenazas. Pero unas preocupan más que otras. Desde el malware en general al ransomware en particular pasando por el tradicional phishing o la suplantación de identidad, preguntamos qué es lo que más preocupa a los responsables de ciberseguridad.**

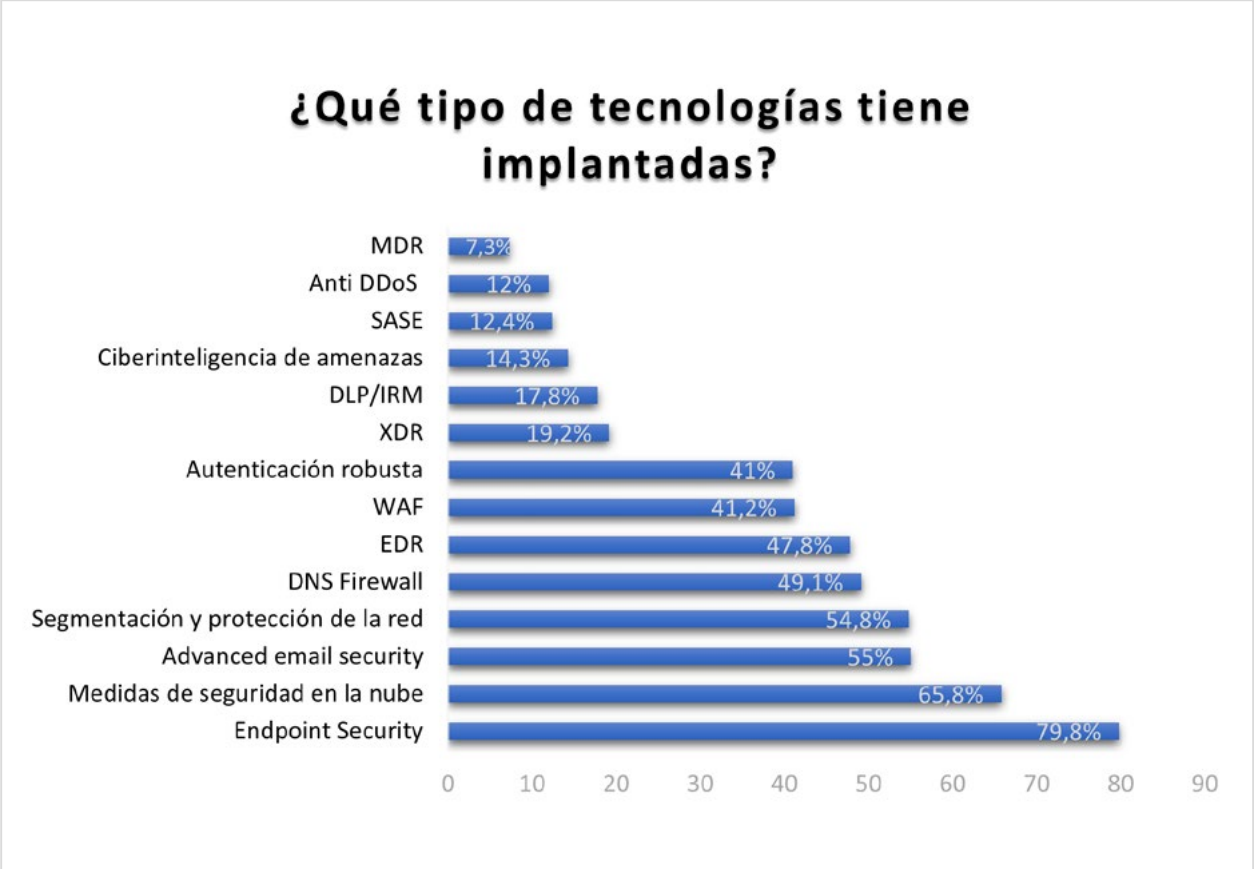
**El ransomware sigue siendo una de las ciberamenazas más graves que enfrentan las empresas. De hecho, es la que más preocupa al 93,9 % de los encuestados, seguido de la exfiltración de datos (52,1 %), el phishing (50,8 %) y la suplantación de identidad (42,4 %).**

# ¿Qué tipo de tecnologías tiene implantadas?

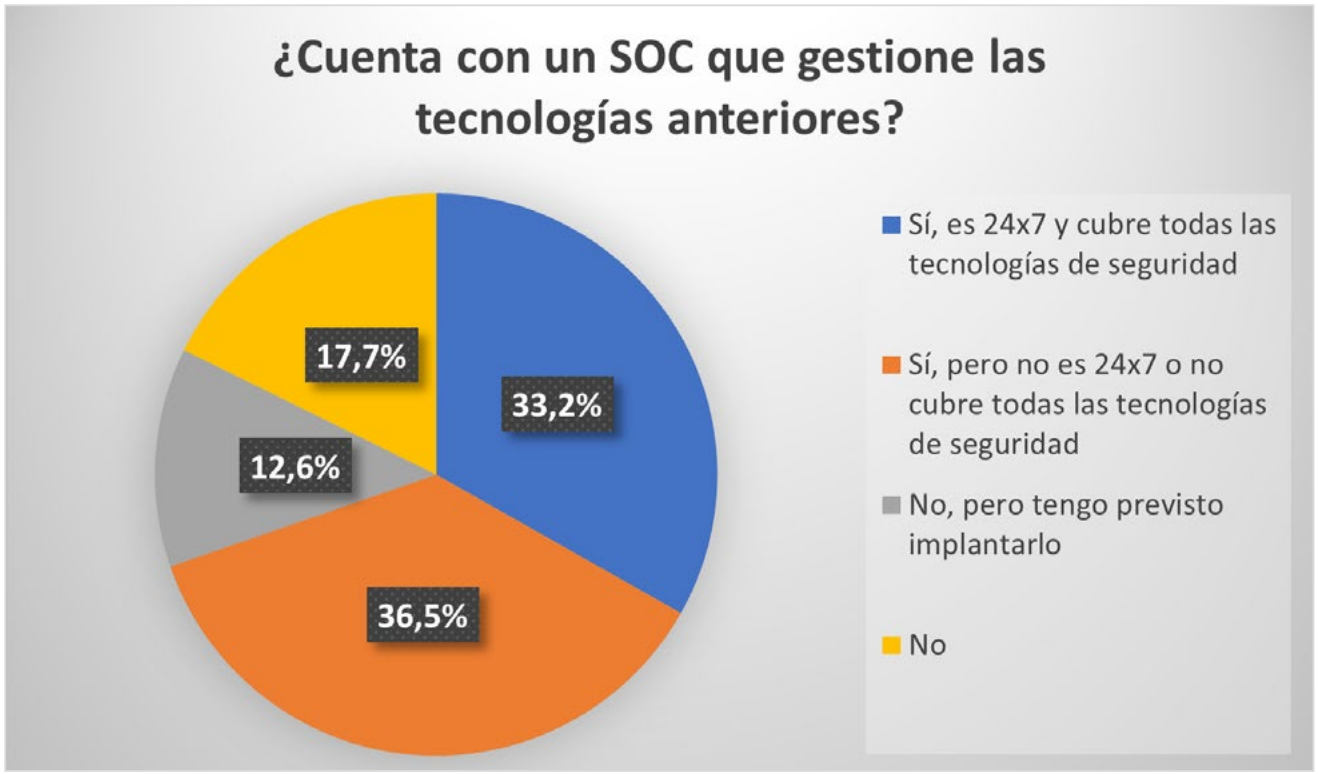
**En este estudio se plantearon una serie de tecnologías de seguridad básicas que toda empresa debería, en mayor o menor medida, tener implementadas. Los datos recogidos no sorprenden. Firewalls, antivirus, o seguridad en la nube son las tecnologías más implementadas por las compañías españolas. Claro que también son las más tradicionales.**

**La seguridad del endpoint (79,8 %) es la más adoptada, seguida de medidas específicas de seguridad en la nube (65,8 %).**

**Por otra parte, años después de contar las bondades de SASE (Secure Access Service Edge) esta tecnología ha sido adoptado por el 12,4 % de las empresas, lo que significa que aún le queda mucho recorrido.**



# Centro de operaciones de seguridad o SOC




**Los beneficios de tener un SOC son numerosos, tanto para las empresas como para sus clientes. Son capaces de monitorizar, vigilar, registrar, gestionar y actuar de manera inmediata ante cualquier evento que afecte a la seguridad de la información de las organizaciones.**

**Entre sus tareas: vigilancia y monitorización 24x7x365; operación, gestión y soporte de sistemas de seguridad TI; gestión de políticas de seguridad y cumplimiento normativo; respuesta rápida ante incidentes de seguridad.**

**La mayoría de las empresas cuentan con un centro de seguridad, aunque son más (36,5 %) las que tienen acceso a un SOC que no es 24x7, ni cubre todas las tecnologías.**

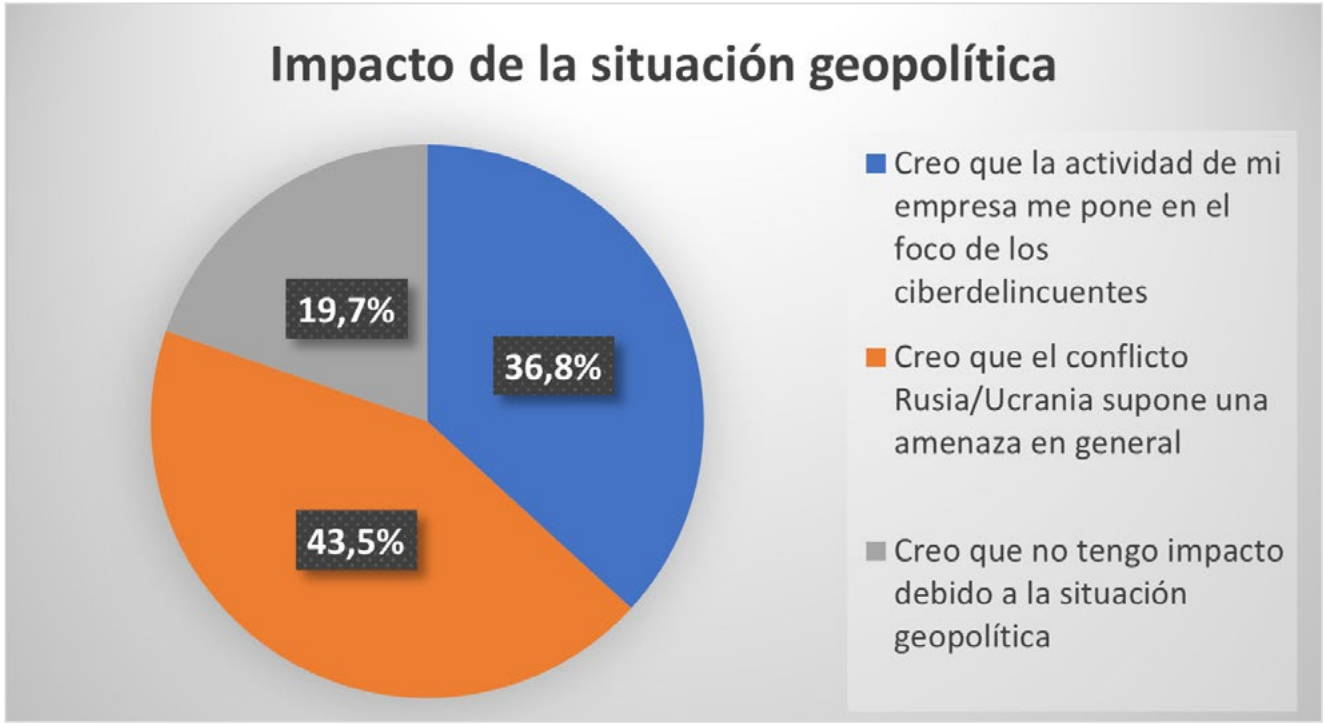
**Las empresas que no tienen un SOC pueden optar por externalizar sus servicios de ciberseguridad a un proveedor de servicios de seguridad (MSSP). Los MSSP ofrecen una amplia gama de servicios de ciberseguridad, como monitoreo de la red, detección de amenazas y respuesta a incidentes.**

# Gobierno de la ciberseguridad

**El Gobierno de la ciberseguridad es el conjunto de principios, políticas, procesos y procedimientos que regulan la gestión de la ciberseguridad en una organización. Su objetivo es garantizar que la organización proteja sus activos de información de las ciberamenazas y es parte esencial de la gestión de la ciberseguridad en cualquier organización.**

**Preguntados por las acciones que tienen implantadas en las empresas, destaca la amplia adopción de herramientas de concienciación, tanto para la alta dirección (51 %) como de manera más genérica (81,3 %). Asimismo, destaca la gestión de la privacidad y el Derecho TIC (81,3 %) y la adopción de políticas formales de seguridad (60,7 %).**

# Situación geopolítica



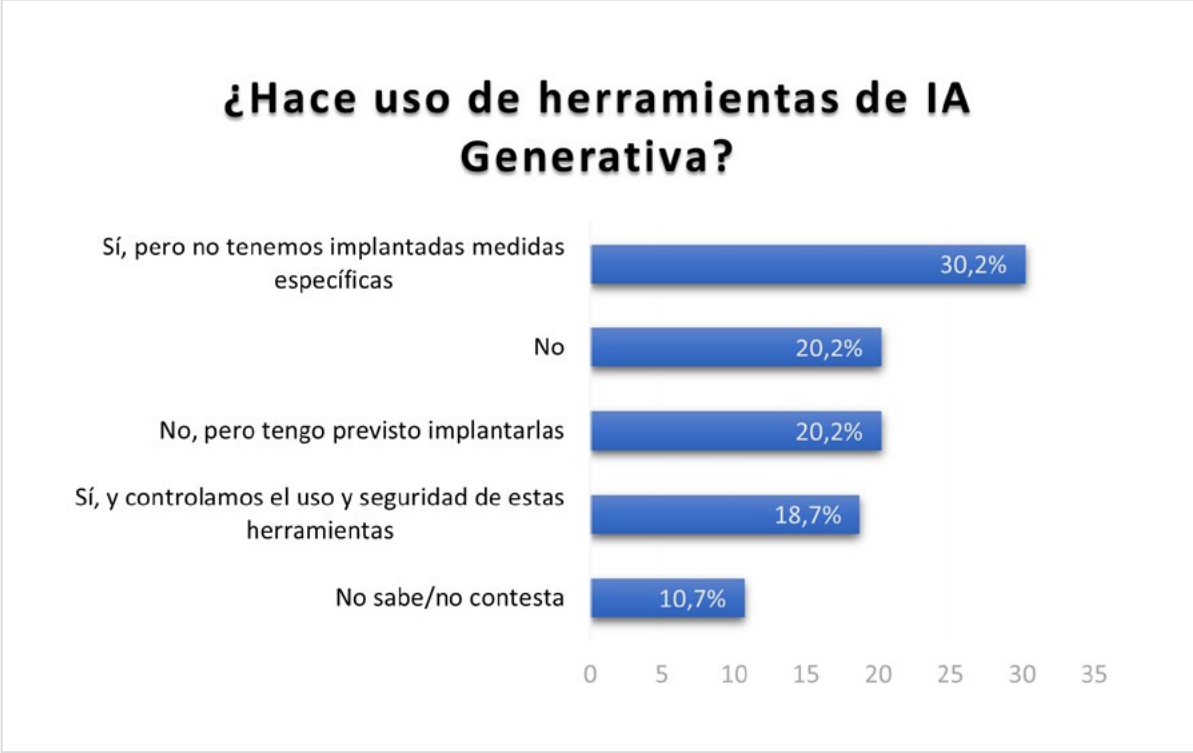

**La situación geopolítica tiene un impacto significativo en la ciberseguridad de las empresas porque pueden aumentar el riesgo de ciberataques, su sofisticación alcance. De hecho, los ciberataques dirigidos a Ucrania han tenido un impacto en las empresas de otros países, ya que han afectado a la infraestructura crítica y a las cadenas de suministro.**

**Para el 43,5 % de los encuestados, el conflicto Rusia/Ucrania supone una amenaza general. Y un 36,8 % considera que la actividad de su empresa les pone en el foco de los ciberdelincuentes.**

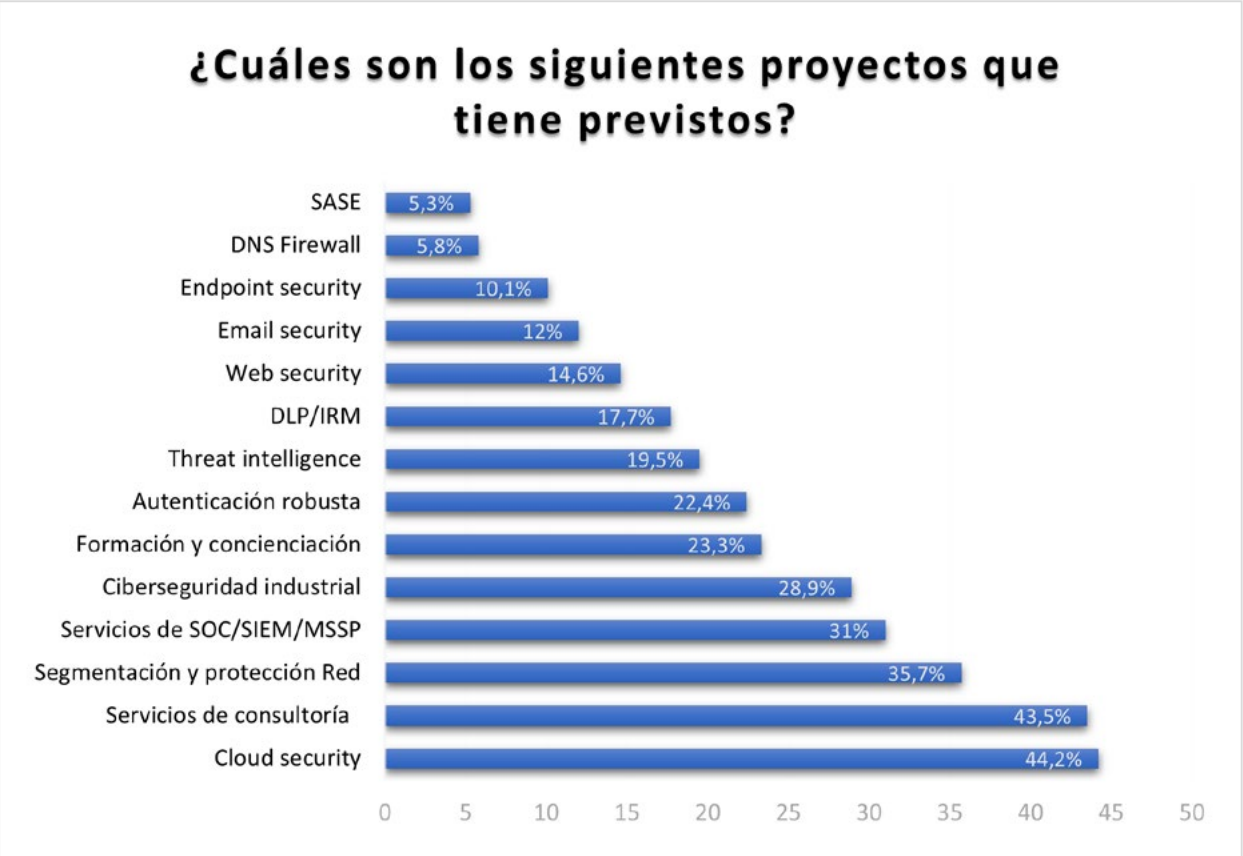
# Uso de la IA Generativa

**Es evidente que el uso de IA generativa, como ChatGPT o Bart, ha explotado este año. La IA generativa es una rama de la Inteligencia Artificial que se centra en la creación de contenido, y que tiene el potencial de automatizar tareas, crear nuevos productos y servicios y mejorar la experiencia del cliente.**

**Más del 10 % de los encuestados no han respondido a esta pregunta. Del total, un 18,7% aseguran controlar el uso y la seguridad de estas herramientas, mientras que un 30,2 % dicen utilizarlas sin tener implantadas medidas específicas, un hecho que está generando enormes riesgos dentro de las empresas.**



# Inversiones a futuro

**Las empresas deben estar preparadas para hacer frente a las ciberamenazas adoptando las tecnologías de seguridad adecuadas. A punto de acabar este 2023, preguntamos a los directivos españoles cuáles son sus planes, qué proyectos tienen pensado afrontar en un futuro cercano.**

**La seguridad en la nube se ha convertido en el foco de inversión para el próximo año para el 44,2 por ciento de los encuestados, seguida de los servicios de consultoría de cumplimiento y procesos de seguridad (43,5 %). Además, el 35,7 % de las empresas invertirán en segmentación y protección de la red.**