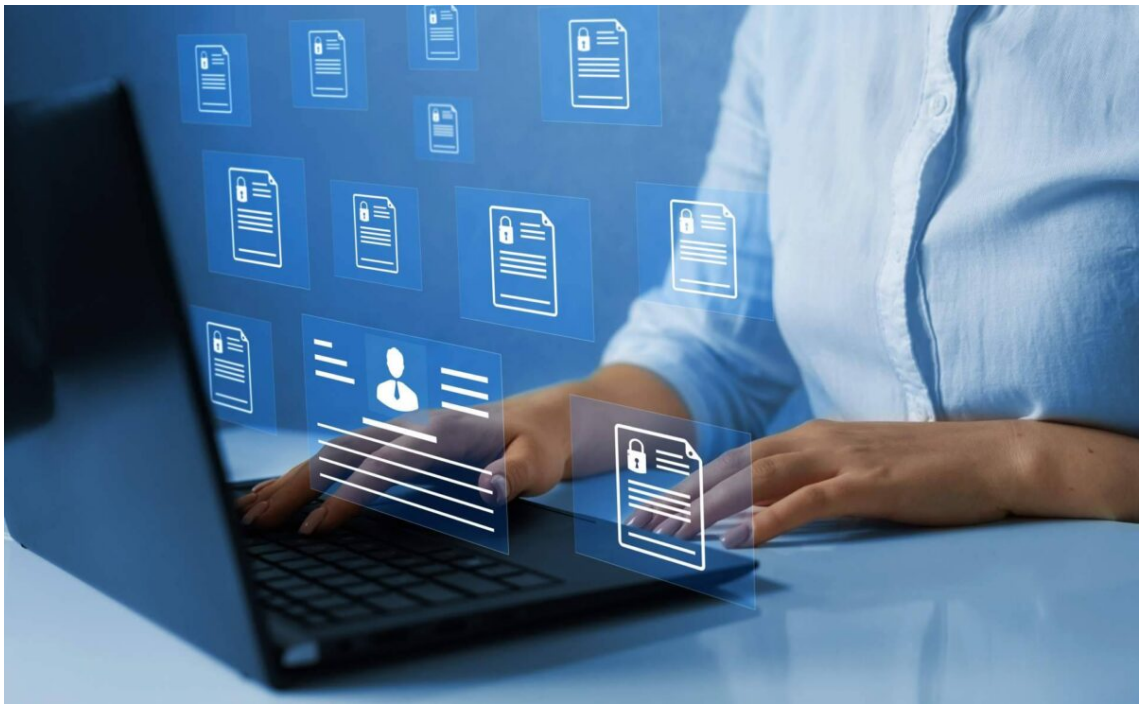
GIRONA NOTICIES.COM + Periodisme

Shadow AI: the risk employees bring into the office

Actualidad Empresarial | 25/11/2026 | 20:02



An employee pastes a contract into a chatbot to get a summary. Another uploads a spreadsheet containing customer data so AI can create a chart. No one has authorized it, no one is monitoring it and, without anyone realizing it, that information has just left the company.

This is known as shadow AI, and it is already a widespread phenomenon. According to a study by consulting firm Cegid involving more than 2,000 European professionals, more than eight in ten employees (82%) use artificial intelligence tools without their employer's permission. Spain stands out: four in ten workers (40%) admit to using them regularly, the highest percentage among the countries studied. And only 44% have received specific training.

The worrying figure

Verizon's latest Data Breach Investigations Report (DBIR 2026) ranks shadow AI among the most common non-malicious internal actions. Two in three users access AI services using personal accounts on work devices. What gets uploaded most often? Source code and technical documentation—in other words, the knowledge that makes a company valuable.

Banning AI does not work. Employees use it because it saves them time, and if one door is closed, they will look for another way in. The key is to see what is happening and set sensible rules.

See, decide and protect

This is where cloud security solutions such as Netskope, a leader in the SASE/SSE model, come

in. They show which AI applications each team uses, distinguish between corporate and personal accounts, and block only what is dangerous: for example, allowing an assistant to be used while preventing customer data or confidential documents from being pasted into it. All without slowing down everyday work.

Technology, however, is only one part of the solution. A clear AI usage policy, employee training and someone to review alerts every day are also needed. That is why demand is growing for IT security companies that handle the entire cycle: assessment, deployment and monitoring.

Before deploying anything, it makes sense to start with business cybersecurity audits, which show what data is being exposed and where. From there, protection is tailored to the reality of each business, not the other way around.

It is not just a concern for large companies

Small and medium-sized businesses are the most exposed: they have fewer resources for monitoring and often do not even know which tools their teams use. Among the cybersecurity companies with experience in this field is GRUPO LINKA, a Netskope partner in Spain, which combines the technology with a managed security service so the company does not have to handle it alone.

AI is here to stay in the office. The question is whether it comes in through the front door, under control, or through the back.

Autor:
AgenciaNinja

https://gironanoticies.com/en/shadow-ai-the-risk-employees-bring-into-the-office/