El mayor riesgo de ciberseguridad no está donde creemos

Miles de pymes digitalizadas pero desprotegidas son el verdadero punto ciego de la ciberseguridad en España

En España seguimos hablando de ciberseguridad como si el problema estuviera, principalmente, en las grandes empresas. Es una comodidad mental porque nos permite imaginar que el riesgo está en otro sitio, en el IBEX, en los sectores más regulados, en las empresas que ya tienen CISO, presupuesto y proveedores especializados. Pero la foto completa va más allá, ya que el verdadero punto ciego está en miles de empresas medianas y pequeñas que ya operan conectadas, dependen de terceros, usan servicios digitales para mantener su actividad y, aun así, siguen tratando la ciberseguridad como una compra puntual o como una conversación exclusiva de IT. En un país con 1,51 millones de empresas activas con uno o más trabajadores, seguir mirando el problema solo desde la gran empresa es, sencillamente, un error.

La paradoja es evidente. España avanza en digitalización: el 74,2 % de las pymes ya alcanza un nivel básico de intensidad digital, 6,7 puntos porcentuales más que en 2023. Al mismo tiempo, el uso empresarial del cloud se sitúa en el 27,3 % y la implantación de inteligencia artificial en el 11,3 %. Es decir, cada vez más procesos dependen de sistemas conectados, datos, plataformas y proveedores externos. Pero digitalizar no equivale a operar con seguridad. De hecho, cuanto más se ensancha la dependencia digital, más estrecho se vuelve el margen de equivocación.

Por eso conviene abandonar una idea que sigue muy instalada en el mercado y que concibe la ciberseguridad como una capa tecnológica. Y no lo es. O, al menos, ya no basta con que lo sea. La tecnología es necesaria, pero no resuelve por sí sola un problema que en la práctica es organizativo y operativo. La seguridad de una empresa depende de cómo se definan responsabilidades, cómo gestiona identidades y accesos, cómo controla a terceros, cómo prioriza activos críticos y cómo prepara la recuperación cuando ocurre un incidente. INCIBE lo formula con bastante claridad al señalar que la seguridad al 100% no existe y que las empresas deben estar preparadas para reaccionar con rapidez y recuperar su actividad normal en un plazo que no comprometa el negocio. Esa es la conversación de fondo, no la de la herramienta, sino la de la continuidad.

Aquí aparece otro error. Creemos que los sectores más expuestos son, por definición, los más vulnerables. Pero no siempre es así. Los ámbitos más regulados y atacados suelen ser también los que más han avanzado, por lo que el riesgo puede estar en la zona intermedia. Compañías industriales, logísticas, de servicios o de la cadena de suministro que no se perciben a sí mismas como objetivo prioritario, pero que ya operan en entornos totalmente conectados.

La ciberseguridad ha dejado de ser un tema de IT desde el momento en el que se para la producción, se interrumpe el servicio, se bloquea una planta, se degrada la relación con clientes o se introduce un riesgo reputacional que afecta al negocio. Las directivas NIS2 y DORA empujan precisamente en esa dirección. Ya no hablan solo de proteger sistemas, sino de gestionar riesgos, resiliencia operativa, impacto económico, cadena de suministro y notificación de incidentes graves. La señal es clara: la ciberseguridad debe subir a la dirección y bajar a la operación.

Los datos de incidentes refuerzan esa urgencia. INCIBE gestionó 122.223 incidentes de ciberseguridad en 2025, un 26% más que en 2024, y detectó 237.028 sistemas vulnerables relevantes. Entre los incidentes más recurrentes figuraron el malware, el fraude online y el phishing. No estamos ante una amenaza hipotética, sino ante una presión sostenida que afecta a empresas reales. Además, se produce en un contexto en el que la inteligencia artificial amplía la superficie de exposición y acelera los ataques. Por tanto, la brecha entre empresas no estará solo en la tecnología. Estará en la operación, entre empresas que integren la ciberseguridad en su forma de operar y empresas que sigan tratándola como una compra.

En España no estamos desestimando el riesgo únicamente por falta de tecnología, estamos expuestos porque una parte decisiva del tejido empresarial sigue abordando la ciberseguridad demasiado tarde y desde el lugar equivocado. Mientras siga proyectándose como gasto, como complejidad añadida o como responsabilidad ajena, el riesgo seguirá creciendo en silencio, por lo que hace falta cambiar el enfoque. No debemos seguir repitiendo que "la ciberseguridad es importante", debemos ser capaces de ver que el problema no está donde solemos mirar y que la verdadera ventaja competitiva de las empresas estará en ser capaces de seguir operando cuando el entorno falle.

Fuente: El mayor riesgo de ciberseguridad no está donde creemos