Opinión

La trampa de pagar cualquier precio por la calidad

Ferran Carreras

En los mercados financieros hay consensos que terminan convirtiéndose en dogmas. Uno de los más extendidos en los últimos años es la idea de que las llamadas empresas de calidad son, por definición, activos seguros. Compañías con balances saneados, altos retornos sobre el capital, márgenes elevados y flujos de caja predecibles han pasado a ocupar el centro de muchas carteras como si representaran una especie de refugio dentro de la renta variable. Y, sin embargo, ahí empieza el error. La calidad no elimina el riesgo; en muchos casos, simplemente lo disfraza.

El atractivo del llamado *quality investing* es comprensible. Frente al inversor que compra negocios baratos de calidad dudosa o al que paga múltiplos muy exigentes por crecimiento futuro, la calidad parece ofrecer una síntesis tranquilizadora: empresas excelentes, bien gestionadas y capaces de componer beneficios durante años. El problema surge cuando el mercado transforma una buena filosofía de inversión en una fe ciega. Entonces deja de analizar los riesgos reales del negocio y empieza a confundir estabilidad histórica con inmunidad futura.

El primer ángulo muerto es la fragilidad estructural. Muchas de las empresas admiradas por su eficiencia han llevado la optimización tan lejos que han eliminado cualquier colchón de seguridad. Cadenas de suministro ultratensadas, dependencia excesiva de un solo proveedor o geografía, inventarios mínimos y estructuras de costes rígidas pueden elevar el retorno sobre el capital en tiempos normales, pero también amplifican el daño cuando llega una disrupción. La crisis de semiconductores demostró que un balance impecable no sirve de mucho si la producción se detiene. La calidad financiera puede convivir con una gran vulnerabilidad operativa.

El segundo riesgo es más silencioso: la fragilidad estratégica. El mercado suele asumir que una ventaja competitiva consolidada es un activo permanente, cuando en realidad ocurre lo contrario. Cuanto mayor es la rentabilidad de un negocio, mayor es el incentivo para que nuevos competidores lo ataquen. La historia empresarial está llena de líderes que confundieron dominio con invulnerabilidad. El problema no es solo la amenaza externa. También lo es la complacencia interna: directivos que protegen los márgenes actuales a costa de la innovación futura o que, por necesidad de "hacer algo", terminan destruyendo valor mediante adquisiciones absurdas, diversificaciones mal planteadas o inversiones guiadas más por el ego que por la lógica del capital.

¿Es el ROIC una jaula?

Existe además una paradoja poco discutida. Cuanto más premia el mercado la calidad, mayor es la presión sobre los gestores para no deteriorar las métricas que la sostienen. El ROIC, que debería ser una señal de excelencia, puede convertirse en una jaula. Si toda la organización vive obsesionada con preservar márgenes y rentabilidades de corto plazo, la empresa puede dejar de invertir en proyectos que hoy parecen menos rentables, pero que son esenciales para defender su posición dentro de cinco años. La calidad, llevada al extremo, corre el riesgo de comerse su propia capacidad de adaptación.

Pero el mayor peligro para el inversor suele aparecer en otro sitio: el precio. Una gran empresa puede ser una mala inversión si se compra demasiado cara. Es quizá la lección más incómoda para el mercado actual. Cuando una compañía excelente cotiza con múltiplos extremos, el accionista ya no compra solo calidad; compra también una expectativa casi perfecta. En ese punto la asimetría juega en su contra. Si el negocio cumple, la rentabilidad puede ser simplemente razonable. Si decepciona un poco, el castigo bursátil puede ser severo, no por deterioro del negocio, sino por compresión del múltiplo.

Eso explica por qué algunas compañías impecables desde el punto de vista operativo han generado retornos decepcionantes en Bolsa. No porque fueran peores de lo que parecía, sino porque el mercado exigía de ellas algo casi imposible: crecimiento prolongado, márgenes intactos y ausencia total de contratiempos. En otras palabras, las había convertido en activos diseñados para decepcionar.

La conclusión no es que haya que desconfiar de las empresas de calidad. Sería absurdo. La conclusión correcta es otra: no basta con admirar un buen negocio, hay que auditar su fragilidad. Conviene preguntarse si su eficiencia es robusta o simplemente frágil, si su ventaja competitiva se ensancha o se erosiona y, sobre todo, si el precio ya descuenta un futuro demasiado perfecto. Porque en los mercados el riesgo rara vez está donde todos lo ven. A menudo se esconde precisamente en aquello que el consenso considera intocable.

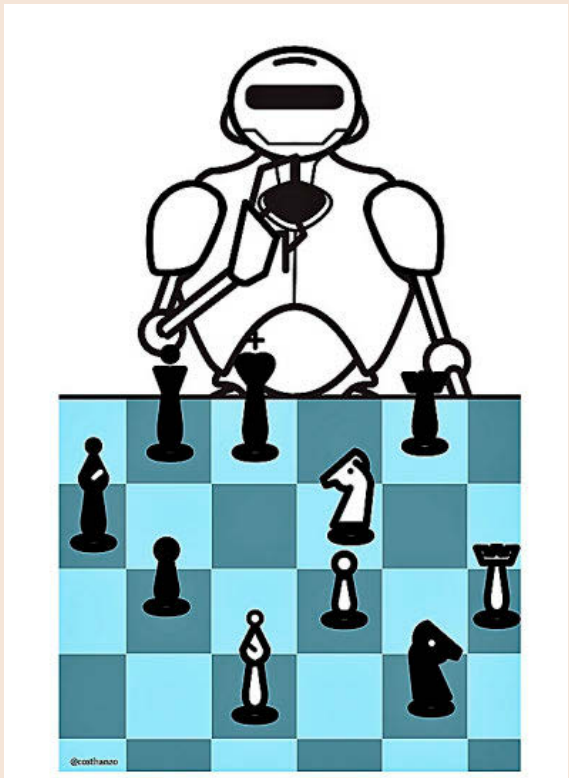
Analista de Gesinter

Cuando el atacante es una IA: el plan que ya no puede esperar

Sandra Sieber

El pasado 7 de julio llegó al despacho de los consejeros delegados de los 110 mayores bancos de la zona euro una carta poco habitual. La firmaba Claudia Buch, máxima supervisora del Banco Central Europeo, y no contenía una recomendación ni una guía de buenas prácticas, sino una orden con fecha límite: antes del 31 de octubre, cada entidad debe presentar un plan de acción contra ciberataques potenciados por inteligencia artificial, con medidas concretas, responsables designados, recursos asignados y plazos de ejecución. Ese mismo día, la Junta Europea de Riesgo Sistémico emitía una alerta formal sobre los modelos de IA de frontera, después de haber elevado en apenas tres meses su valoración del riesgo cibernético de "elevado" a "severo".

Conviene subrayar el detalle que muchos titulares pasaron por alto: la carta no fue dirigida a los directores de tecnología, sino a los consejeros delegados. El supervisor no está pidiendo un ajuste técnico. Está diciendo que esto es un asunto de gobierno corporativo, de los que se despachan en el consejo y no en el sótano de sistemas.



El BCE ha puesto fecha, 31 de octubre, a algo que hasta ahora era un debate de expertos: defenderse de ciberataques ejecutados por inteligencia artificial

¿Qué ha cambiado para justificar tanta urgencia? Hasta hace poco, la IA era para el atacante una herramienta auxiliar: correos de *phishing* mejor redactados, algo más de automatización. Los modelos más avanzados han cruzado otro umbral. Según la alerta europea, ya son capaces de descubrir vulnerabilidades, generar código de ataque funcional y ejecutar ofensivas completas de forma autónoma, a una velocidad y escala sin precedentes. La propia carta del BCE lo describe como "un cambio de largo plazo en el panorama de amenazas y no un fenómeno temporal". Y encierra una asimetría incómoda: a largo plazo, estas mismas capacidades reforzarán las defensas; a corto y medio plazo, la ventaja es del atacante. Quien encuentra el fallo en horas juega contra organizaciones que tardan meses en parchearlo.

Habrá quien piense que esto es, ante todo, un problema de bancos: infraestructura crítica, dinero de por medio, regulación a raudales. Es una objeción razonable. Pero no cambia la conclusión, sino que la refuerza. Los bancos son, precisamente, las organizaciones que más invierten en ciberseguridad de toda nuestra economía, y aun así el supervisor considera que no están preparadas para lo que viene. Si ellos necesitan un plan urgente, ¿qué decir del resto de empresas, que se enfrentan exactamente al mismo panorama de amenazas con menos medios, menos práctica y ningún supervisor que les ponga fecha?

La anatomía de un buen plan

Lo más valioso de la carta del BCE es que convierte una amenaza difusa en una plantilla de trabajo que cualquier comité de dirección puede copiar. A corto plazo pide tres cosas: acelerar la gestión de vulnerabilidades y el parcheo a escala, porque los ciclos trimestrales de actualización son una invitación al desastre cuando el adversario opera en horas; reforzar la detección y la monitorización apoyándose en IA defensiva, porque ningún equipo humano puede vigilar a la velocidad del ataque; y estrechar el control sobre los proveedores tecnológicos, ese eslabón de la cadena por el que hoy entran buena parte de los incidentes. A medio plazo, medidas estructurales: defensa en profundidad, higiene cibernética y modernización de las infraestructuras heredadas que todavía sostienen la operativa de demasiadas organizaciones.

Traducirlo a la propia empresa significa, primero, saber qué se tiene: inventario de activos digitales y mapa de exposición. Significa actualizar el factor humano, porque el *phishing* hiperpersonalizado y los *deepfakes* de voz y de vídeo han dejado obsoleta la formación tradicional: hoy hacen falta protocolos de verificación reforzados para órdenes de pago y decisiones sensibles, partiendo de que la voz al otro lado del teléfono puede no ser quien dice ser. Y significa, sobre todo, gobernanza: un responsable con nombre, presupuesto propio y métricas que el consejo de dirección revise con la misma seriedad que las financieras.

Hay, además, otra cara del riesgo que sería un error esconder: la IA que la propia empresa utiliza. Empezando por la que utiliza sin saberlo, porque en casi todas las organizaciones los empleados ya usan herramientas de IA sin permiso ni control, y no se puede proteger lo que ni siquiera se ve. Y siguiendo por la que sí está autorizada: fugas de datos a través de herramientas generativas, modelos mal gobernados, decisiones automatizadas sin supervisión humana. El Reglamento Europeo de IA ya impone obligaciones crecientes a todos los sectores, y DORA lo hace en el financiero. Protegerse de la IA ajena y gobernar la propia no son dos planes distintos: son las dos mitades del mismo.

Y esto no puede esperar a después del verano. Hay que ponerlo en la agenda del próximo comité de dirección, y la buena noticia es que empezar no exige grandes consultoras ni presupuestos: exige responder a tres preguntas: ¿Dónde somos vulnerables, incluida la IA que ya usa la organización con y sin permiso? ¿De qué proveedores dependemos y qué pasaría mañana si uno de ellos cae? ¿Y cuánto tardaríamos en volver a operar, partiendo de que el atacante puede llevar meses dentro sin hacer ruido cuando por fin lo descubramos?

Estas tres respuestas son el primer eslabón del plan de protección digital que debería tener cualquier empresa: de la primera sale el inventario de exposición, de la segunda el mapa de dependencias y de la tercera la medida real de nuestra resiliencia. Todo lo demás –medidas, responsables, recursos, plazos– se construye sobre ellas.

Los bancos entregarán sus deberes el 31 de octubre porque no les queda otra. Las demás empresas no recibirán ninguna carta. Pero la amenaza no distingue entre quienes tienen supervisor y quienes no. Actuar ahora –sin que nadie nos obligue– no es un gesto de prudencia: es la diferencia entre implantar un buen gobierno de la IA o descubrir, un día cualquiera, que ya es tarde.

Profesora en IESE