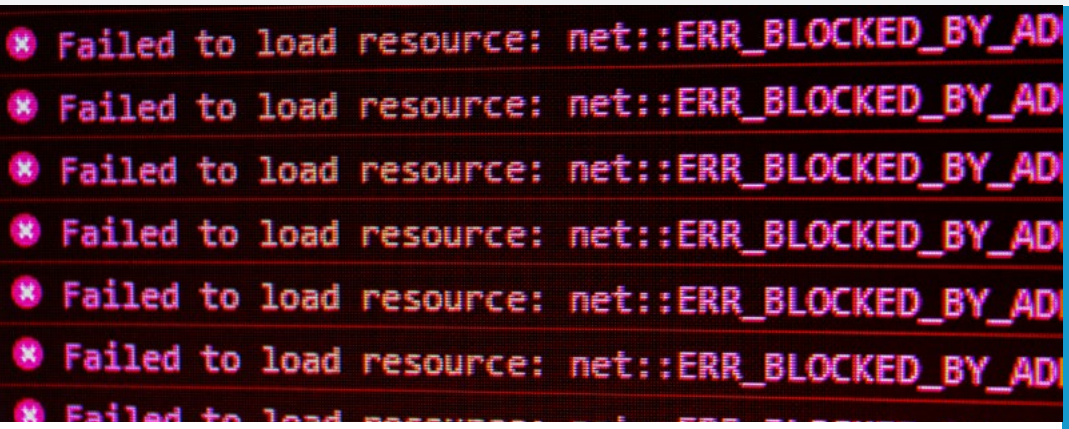
INSURZINE
WEEKLY
VENERDÌ 18 SETTEMBRE 2026 | N.184



L'errore che nell'AI agentica non lascia segni

L'observability copre il sistema. Non copre la persona che ne riceve l'output — ed è lì che il rischio si sposta.

di Edoardo Sorrentino

Il tavolo raccontato da Fiorella Cipolletta nella seconda puntata di Insurance in the Mirror (InsurZine, 22 maggio 2026) ha messo a fuoco un salto reale: dal chiedersi "il sistema funziona?" al chiedersi "l'agente sta ragionando come intendevo che ragionasse?"
È il passaggio dal piano infrastrutturale a quello semantico, e le piattaforme di monitoraggio lo rincorrono con ragione. Ma c'è un passaggio successivo che quel confronto lascia aperto, e su cui si gioca ben più del singolo sinistro: la qualità del giudizio professionale, ovunque un output dell'AI diventi la base di una decisione.

IL PASSAGGIO CHE L'OBSERVABILITY NON COPRE

Un sistema può comportarsi esattamente come progettato, passaggio per passaggio, e il singolo output davanti a chi lo riceve essere comunque quello sbagliato.

La ragione è aritmetica, non speculativa. Il vulnus è nella concatenazione: anche una precisione del 99,9% per passaggio, composta su un centinaio di passaggi in sequenza, si aggrega a circa il 90%. Un processo su dieci non è accurato. E quell'esito non ha un aspetto diverso da uno corretto: è un output che si legge perfettamente, non uno che si segnala da sé.
METR, l'istituto indipendente che misura le capacità dei modelli di frontiera, ha testato agenti AI su compiti di lunghezza crescente: la curva del successo decade esattamente così, perché basta fallire un sotto-compito per far fallire l'intero processo.

continua a pag. 2

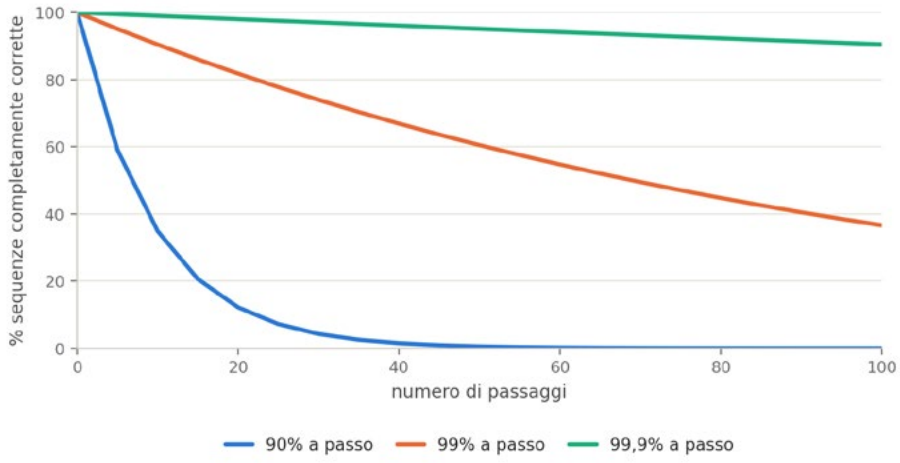
IN PRIMO PIANO

WeSec, a Milano il primo Salone della Sicurezza promosso da ABI

di Redazione

Il 22 e 23 settembre Milano ospiterà la prima edizione di **WeSec – Il Salone della Sicurezza**, il nuovo appuntamento promosso dall'**ABI** e dedicato alle trasformazioni che stanno ridefinendo la sicurezza del settore bancario e finanziario. Al centro delle due giornate ci saranno geopolitica, intelligenza artificiale, infrastrutture critiche e nuove vulnerabilità.
L'iniziativa è promossa da ABI e organizzata da ABI-Servizi in collaborazione con **CERTFin, ABI Lab, OSSIF e FEduF**, con **Deloitte** nel ruolo di *Knowledge Partner*. L'obiettivo è favorire un confronto tra istituzioni, autorità nazionali ed europee, banche, Forze dell'ordine, industria, ricerca e imprese tecnologiche, adottando una lettura integrata dei rischi che caratterizzano uno scenario internazionale segnato da instabilità, accelerazione tecnologica e tensioni geopolitiche.
"WeSec nasce dalla consapevolezza che sicurezza e in-

continua a pag. 2



Sequenze completate correttamente al crescere del numero di passaggi, per tre livelli di accuratezza per passo.

Nei sistemi reali il 99,9% per passo è oggi irrealistico; a un più verosimile 90% bastano 5 passaggi perché il successo scenda al 60%, per poi crollare praticamente a zero sui processi lunghi.
E c'è chi lo ha misurato sulle pratiche vere: τ-bench non chiede a un agente se sa risolvere un caso, ma se sa risolvere lo stesso caso otto volte di fila, con otto clienti diversi. Un agente che ne chiude correttamente il 61% al primo tentativo ne gestisce otto consecutive solo nel 25% dei casi.
Gli agenti reali in parte si autocorreggono, e la curva empirica è meno ripida di quella teorica. La direzione però non cambia - ed è la direzione che serve a chi deve dimensionare i controlli.

PERCHÉ NESSUNO SE NE ACCORGE

L'errore composto non lascia segni. Un dato assurdo si nota. Un output fluente, coerente, formalmente corretto - e disallineato dalla realtà in un punto specifico - molto più difficilmente. I controlli abituali verificano la coerenza interna, non la corrispondenza con i fatti esterni.
C'è poi una ragione più diretta: l'osservabilità del sistema finisce esattamente dove l'output arriva a chi deve decidere se agire. Quello che succede dopo non lo misura nessuna piattaforma.

DALLA VERIFICA AL SOGNO LUCIDO

La deriva non riguarda solo i sistemi sotto governance. Riguarda l'uso quotidiano e individuale che un professionista fa dell'AI per formarsi un'opinione - dove nessun controllo formale interviene, perché non è un processo aziendale: è una conversazione.
La fiducia si costruisce dove lo strumento risponde bene a compiti con una risposta corretta, e da lì si trasferisce - senza che nessuno lo decida - a un terreno dove quella verifica non esiste più: un giudizio, una strategia.

> *È lì che l'AI inizia a fare sogni lucidi: addestrata per essere persuasiva e coerente, dove la verità non è oggettiva smette di calcolare e costruisce logiche brillanti, plausibili, difficilmente contestabili.*

L'ATROFIA INVISIBILE

C'è un effetto più insidioso della singola decisione sbagliata. Più si affida il proprio pensiero all'AI, più si diventa supervisori passivi delle proprie conclusioni - e la supervisione passiva non è neutrale: nel tempo, atrofizza il giudizio.
Non è un timore astratto. Su *Lancet*, nel 2025: endoscopisti con oltre 2.000 esami alle spalle hanno perso il 20% di capacità diagnostica quando operavano senza AI, dopo pochi mesi di uso abituale. Nessuno se n'era accorto.
Se non si costruisce più una valutazione, ma si convalida solo un'opinione già formata, la capacità di cogliere l'eccezione degrada: non un esperto che si avvale dell'AI, ma un timbro umano su una logica che non si controlla più.

novazione sono oggi sempre più interdipendenti e costituiscono una leva strategica per lo sviluppo economico e sociale", ha dichiarato **Marco Elio Rottigni**, Direttore Generale dell'ABI.
Secondo Rottigni, affrontare rischi sempre più complessi richiede "un modello di sicurezza partecipata e integrata basato sulla collaborazione tra soggetti pubblici e privati, sulla condivisione delle informazioni e sulla diffusione della cultura digitale".
Un'attenzione che trova riscontro anche negli investimenti sostenuti dal settore. Nel 2026 le risorse destinate dalle banche alla sicurezza confermano un trend in costante crescita e si attestano su un miliardo di euro, mentre tra il 2020 e il 2025 sono stati investiti complessivamente circa 5 miliardi di euro nella sicurezza fisica e *cyber*.
Il programma di WeSec affronterà il contrasto alle minacce informatiche, la resilienza delle infrastrutture critiche, la sovranità tecnologica e finanziaria, l'evoluzione dell'intelligenza artificiale e la protezione dei dati. Spazio anche alla cooperazione internazionale, alla sicurezza fisica e alla diffusione di una cultura della prevenzione capace di coinvolgere istituzioni, imprese e cittadini.

Edoardo Sorrentino

COSA SI PUÒ MISURARE, SENZA NUOVI STRUMENTI

Bastano tre domande, poste al processo e non al singolo che lo esegue.
Che percentuale delle decisioni prodotte dall'agente riceve una verifica indipendente - non un controllo di conformità, una verifica sostanziale? Il numero che conta non è quante decisioni produce l'agente, ma il rapporto fra quel numero e la capacità di verificarle. Se il primo cresce e la seconda resta ferma, il rapporto peggiora - anche se ogni controllo, preso da solo, resta accurato.
La verifica è progettata dentro il processo, o dipende dalla buona volontà di chi dovrebbe farla? Un flusso che genera valore eliminando il controllo caso per caso non lo recupera per intenzione individuale. O il campionamento è architettura, o non accade.
Chi, in questa catena, ha davvero l'autorità di fermare una scelta che non torna - e cosa gli costerebbe farlo? Se la risposta è "nessuno" o "il prossimo rinnovo", l'accuratezza di ciò che passa per quella catena non dipende dalla competenza di chi ci lavora. Dipende da ciò che nessuno aveva titolo per interrompere.

IL TEST CHE SOSTITUISCE LA DOMANDA SBAGLIATA

Non serve sapere se una valutazione l'ha prodotta un sistema o una persona: è una distinzione sempre meno decidibile, e non è la domanda che conta. Quella utile vale per qualunque pratica passi su una scrivania:

> *Cosa qui potrebbe essere dimostrato sbagliato, e da chi?*

Se la risposta è "niente" - nessuna fonte, nessun dato, nessuna previsione fatta prima del risultato - quello che si ha in mano può essere corretto, ma non è conoscenza: è un'ipotesi ben scritta, e un settore che stima il rischio non può trattare le due cose come equivalenti.
Non verifichiamo solo per correggere gli errori dell'AI. Verifichiamo per mantenere viva la capacità di accorgerci che un errore esiste. Delegare la produzione del lavoro senza continuare a misurarsi con i dati reali significa delegare anche il giudizio - e per un'assicurazione è l'asset più costoso da perdere.

Promosso da

ABI Associazione Bancaria Italiana

WeSec
IL SALONE DELLA SICUREZZA

IL NUOVO APPUNTAMENTO SU SICUREZZA, GEOPOLITICA, AI E INFRASTRUTTURE

MILANO ALLIANZ MiCo NORTH WING
22 - 23 SETTEMBRE 2026
salonewesec.com

Iscriviti subito, la partecipazione è gratuita

Organizzato da
ABISERVIZI ABI EVENTI

Media Partner
BANCAFORTE innovation key

In collaborazione con
ABI Lab · CERTFin · FEduF · OSSIF

#wesec

Con il patrocinio di
Commissione europea

Con la partecipazione di
BANCA D'ITALIA EUROSISTEMA

Partner Istituzionale
pappa

Knowledge Partner
Deloitte.

Main Partner
Altirium · aruba.it · BANCOMAT · expriVia · INTESA SANPAOLO · nexi · VISA

Partner
AATech · A&F · ALFAGROUP · Almaviva Group · ADC · Augusto Vacca & Partners · BANCARIA · BANCO BPM · BETTINI · caleidos · cdp · CATO NETWORK · CBI · CeSI Centro Studi Internazionali · CHECK POINT · Class CNBC · cleafy · Clusit · CODACONS · Complaion · CONFCONSUMATORI APS 50° ANNIVERSARIO · CRIF · CUBE AI · CY4GATE · DECRIPTO · DEEPSEARCH · Deutsche Bank · dinova · EAGLE PROJECTS · Economy Group · eng · EUROBORSA · everbridge · experian · FASTWEB + vodafone · feedzai · Fintech District · FINOMNIA · Gruppo Cassa Centrale · Identità Digitale Milano · INDAGO · IMH · INSURZINE · Ipsos Doxa · ITALIA informa · Kai · KPMG · Luiss Business School · LUTECH · mancaretti · MCM GROUP · Menz Veritas · mib · MFM Milano Finanza · Movimento Consumatori · netskope · OneTrust · PAZZESCO · PingIdentity · BLUDIS · PMI.it · REEVO · SANS · GIAC · securindex.com · Security Mind · Informazione per la Sicurezza · S2E · sky · tas · UNC Consumatori · U.Di.Con. · Università Campus Bio-Medico di Roma · Wall Street Italia · WW2GLOBAL · WOMEN for Security · XTN

Il rischio climatico non ha una geografia del merito

Cosa succederebbe se iniziassimo a trattare il rischio climatico fisico come un'esternalità condivisa, da distribuire e ridurre, invece che come un costo locale da assorbire dopo che è già accaduto?

di Roberto Carnicelli, CEO di Eoliann

Il 26 agosto un ghiacciaio è crollato vicino al Langtang Lirung, in Himalaya. Ha innescato piene improvvise lungo 72 chilometri del fiume Trishuli: **almeno 1000 morti, quasi 4.500 dispersi**, villaggi interi spazzati via, corpi trascinati per 240 chilometri fino in territorio indiano. Il crollo ha generato una scossa di magnitudo 5.2, registrata dai sismometri di mezzo mondo.

Non lo racconto per cronaca: le cifre, purtroppo, sono già arrivate ovunque. Lo racconto perché quel collasso pone una domanda che raramente ci facciamo con la dovuta onestà: **chi paga il conto di un rischio già generato, e chi invece lo ha causato?**

Il Nepal emette una frazione minima delle emissioni globali di gas serra. Eppure sta pagando, con i propri ghiacciai e con le proprie vite, un riscaldamento a cui ha contribuito pochissimo. Non è la prima volta che il clima si comporta così, e non sarà l'ultima: **il rischio climatico non ha una geografia del merito**. Non premia chi ha emesso meno, né risparmia chi vive più in alto o più lontano. Non distingue tra chi ha causato il problema e chi ne paga le conseguenze. Chi vive di pastorizia in Asia centrale, la popolazione del Nepal, chi è stato evacuato per gli incendi in Europa quest'estate non hanno nulla in comune, se

Roberto Carnicelli

non il fatto di pagare tutti un conto che non hanno aperto loro.
E non serve guardare così lontano per trovarne conferma. Secondo Copernicus, giugno e luglio 2026 sono stati i mesi più caldi mai registrati in Europa occidentale: circa 70mila ettari bruciati in Italia (il 133% in più rispetto alla media degli ultimi vent'anni) e oltre 435mila in tutta Europa. Il meccanismo è lo stesso, cambia solo la latitudine.
C'è un concetto, preso in prestito dall'economia ambientale, che aiuta a leggere questi eventi con più lucidità: quello di **esternalità negativa**. È il costo generato da un'attività economica che ricade non su chi la genera, ma su altri, spesso lontani, spesso senza voce in capitolo. È lo stesso principio alla base delle emissioni di CO2, ma qui lo applichiamo non solo alle cause del cambiamento climatico, bensì al rischio fisico che quel cambiamento ha già messo in moto.
Oggi il rischio climatico fisico viene quasi sempre prezzato localmente, in modo disomogeneo, e quasi sempre a evento già avvenuto. Una compagnia assicurativa si ritira da un'area a rischio alluvione. Un comune ricostruisce dopo un incendio. Sono tutte risposte legittime, ma tutte tardive, e tutte locali, come se il conto potesse essere chiuso lì dove si presenta, senza risalire a monte.
Ma cosa succederebbe se iniziassimo a trattare il rischio climatico fisico come un'esternalità condivisa, da distribuire e ridurre, invece che come un costo locale da assorbire dopo che è già accaduto?
Non ho una risposta definitiva a questa domanda e purtroppo credo che nessuno ce l'abbia ancora, del tutto. Ma è, mi sembra, la domanda giusta da porsi in apertura di questa nuova stagione di eventi estremi. Una contabilità onesta del rischio climatico comincia dal riconoscere una cosa semplice: non esiste più un rischio climatico che riguardi solo qualcun altro.
È anche da questa convinzione che nasce il lavoro quotidiano che faccio con Eoliann, la climate tech italiana che guido: provare a rendere misurabile, in anticipo e non a evento già avvenuto, il rischio climatico fisico delle infrastrutture, perché prevedere è il primo passo per redistribuire, e redistribuire è il primo passo per non lasciare che il conto lo paghi sempre chi non lo ha aperto.

INSURZINE .TV

MiaFintech, l'open insurance e AI accelerano l'evoluzione delle compagnie

Bruno Natoli ci racconta come piattaforme componibili, open insurance ed embedded insurance possano aiutare le compagnie a integrare sistemi legacy, partner e nuovi servizi digitali, senza perdere di vista compliance e sicurezza.

GUARDA LA PUNTATA

INSURZINE.TV

Adyen, il pagamento del premio al centro della relazione tra compagnie e assicurati

Gabriele Bellezze, Country Manager Italia di Adyen spiega come semplicità, autonomia nella scelta del metodo di pagamento e rapidità nei rimborsi possano migliorare la customer experience e rafforzare la fidelizzazione tra compagnia e assicurato.

GUARDA LA PUNTATA

INSURZINE WEEKLY

Direttore responsabile: Andrea Turco *andrea.turco@insurzine.com*
Editore e Redazione: Oltre La Media Group srl – Via Pescantina 8 – 20162 Milano
T: 388 8265893
E-mail: *info@insurzine.com*
Per inserzioni commerciali: *giovanni.sorgente@insurzine.com / daniele.vanz@insurzine.com*
Testata giornalistica registrata presso il Tribunale di Milano - Numero 111 del 9 Aprile 2018