INSURANCE Daily

N. 2843 LUNEDÌ 15 SETTEMBRE 2025

PRIMO PIANO

Frodi, un fondo da 204,5 mln

È stato fissato in 204,5 milioni di euro l'ammontare del Fondo per indennizzare i risparmiatori vittime di frodi finanziarie e che hanno sofferto un danno ingiusto non altrimenti risarcito o i risparmiatori danneggiati dal default dei titoli obbligazionari della Repubblica argentina costituito nel 2006 dal ministero dell'Economia. Lo prevedono le disposizioni attuative del fondo indennizzi per i risparmiatori vittime di frodi finanziarie contenuto nel decreto del presidente del Consiglio del 30 luglio 2025 pubblicato in Gazzetta Ufficiale.

Il Fondo, si legge, "è alimentato dall'importo dei conti correnti e dei rapporti bancari definiti come dormienti all'interno del sistema bancario, nonché del comparto assicurativo e finanziario, definiti con regolamento da adottare, ai sensi dell'articolo 17 della legge 23 agosto 1988, n. 400, su proposta del ministro dell'Economia e delle finanze". La gestione del fondo è affidata, mediante convenzione di durata triennale, alla Consap.

"Nel rispetto di quanto previsto dal decreto, pari a complessivi 204,5 milioni di euro, si provvede, nel rispetto degli equilibri di finanza pubblica, mediante uno o più versamenti all'entrata del bilancio dello Stato per la successiva riassegnazione al fondo nel limite di 1,5 milioni per l'anno 2025, 61,5 milioni nell'anno 2026 e 141,5 milioni per l'anno 2027", riporta la Gazzetta Ufficiale.

B.M.

GLOSSARIO

Deepfake

Si sono ormai affermati come un potente strumento per la diffusione della disinformazione, perché in grado di confondere il confine tra realtà e finzione. La creazione di contenuti falsi ma convincenti pone serie sfide alla società, perché la creazione di narrazioni avvincenti può plasmare l'opinione pubblica. Dai cosiddetti shallowfake ai casi più sofisticati di phishing che usano l'intelligenza artificiale, ecco quali sono le principali tipologie e i maggiori rischi connessi

Un *deepfake* è un contenuto multimediale, costituito da un'immagine, un video o un audio, creato o manipolato con l'ausilio di tecniche di intelligenza artificiale.

Lo scopo è quello di far sembrare autentica una cosa falsa: il termine deriva infatti dalla combinazione di *deep learning* (la tecnica utilizzata per creare questi contenuti) e *fake* (falso).

Questi contenuti possono essere usati per diffondere disinformazione, danneggiare la reputazione di qualcuno o commettere frodi, ma anche per puro intrattenimento. Sono utilizzati sostituendo il volto o la voce di una persona con quella di un'altra, facendo dire a qualcuno cose che non ha mai detto, creando video a sfondo pornografico oppure allo scopo di diffamare personaggi pubblici. La loro crescente sofisticazione rende sempre più difficile distinguerli dai contenuti autentici.

Esistono varie categorie di questi falsi, dai cosiddetti *shallowfake*, fino ai veri e propri deepfake, che usano l'intelligenza artificiale: qui di seguito ne forniremo alcuni esempi.

SHALLOWFAKE, IL FALSO CON MEZZI RUDIMENTALI

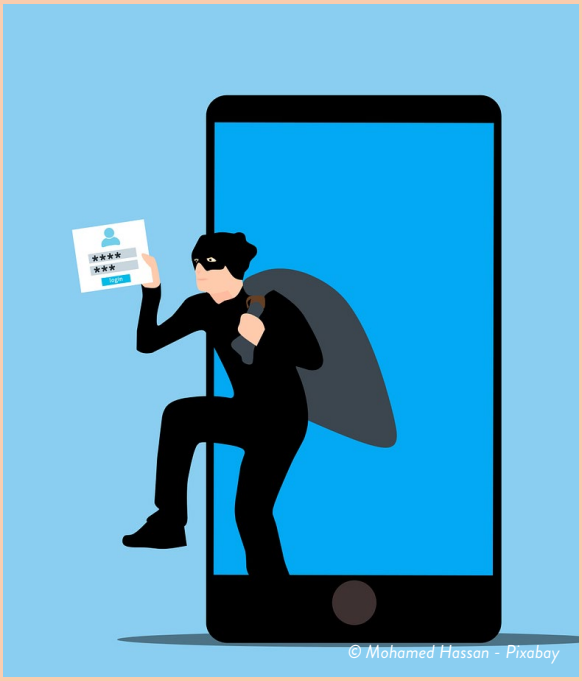
Partiamo dal shallowfake. *Shallow* vuol dire *poco profondo* e quindi si contrappone al termine deep (profondo). La tecnologia degli shallowfake è ormai piuttosto datata: prevede l'editing di contenuti multimediali tramite software piuttosto vecchi, come **Photoshop**. In realtà, non si tratta di veri e propri deepfake, perché non è previsto l'uso dell'intelligenza artificiale, ovvero di sistemi di deeplearning. Non sono per questo meno pericolosi, perché possono essere creati e distribuiti assai più facilmente e velocemente dei deepfake. È accaduto, ad esempio, che un passaporto canadese manipolato con questo sistema sia stato utilizzato ben 2.500 volte nel giro di un solo mese, prima che le autorità se ne accorgessero.

IL DEEPLEARNING PER CREARE VIDEO E AUDIO REALISTICI

I deepfake video sono supporti sintetici in cui l'immagine di una persona è alterata digitalmente o sostituita con quella di un altro soggetto, utilizzando tecniche di apprendimento automatico (deeplearning). Questa tecnologia può creare video estremamente realistici, che fanno sembrare che qualcuno dica o faccia qualcosa che in realtà non ha mai detto o fatto.

Meno ovvi e talvolta considerati meno efficaci dei deepfake visivi sono i deepfake audio o vocali, anche noti come file di clonazione vocale.

Questi deepfake sono creati addestrando modelli di intelligenza artificiale, attraverso l'uso di registrazioni esistenti della voce di una persona. Se addestrata, l'AI può generare nuovi audio che imitano perfettamente la voce originale e, una volta replicato un modello della voce di quella determinata persona, è possibile farle dire qualsiasi cosa.



IL PHISHING PORTATO A UN LIVELLO SUPERIORE

Il phishing tramite e-mail o messaggi di testo è una pratica ben nota, ma il deepfake phishing porta questo sistema a un livello superiore, includendo clonazione vocale e videochiamate. Un eventuale aggressore può quindi utilizzare un deepfake video su una piattaforma di teleconferenza, per indurre la vittima a condividere informazioni riservate (come le credenziali) o manipolarla, per convincerla a effettuare transazioni finanziarie non autorizzate. È sufficiente utilizzare filmati disponibili al pubblico.

Il deepfake phishing segue quindi gli stessi principi fondamentali degli attacchi di ingegneria sociale: confondere e manipolare le vittime, sfruttare la loro fiducia e aggirarne le misure di sicurezza. Sono sistemi molto efficaci, grazie alla credibilità che ispirano: si tratta di audio, video o immagini estremamente realistici, che riescono a facilitare l'accesso da parte degli aggressori, aumentando la probabilità che le vittime credano al messaggio falso a loro propinato.

Combinando la tecnologia deepfake con tecniche di ingegneria sociale, inoltre, gli aggressori possono creare messaggi altamente personalizzati, il che rende i tentativi di phishing più convincenti e più difficili da rilevare, anche perché il deepfake phishing sfrutta la fiducia intrinseca che le persone ripongono nelle informazioni visive e vocali che ricevono: quando vedi e senti una persona familiare, è più probabile che tu acconsenta alle sue richieste, condividendo informazioni anche molto sensibili.

Le misure di sicurezza tradizionali, infine, come i filtri email e i sistemi di riconoscimento vocale, possono avere difficoltà a rilevare i deepfake a causa del loro elevato livello di sofisticazione, anche perché il deepfake phishing sfrutta spesso tattiche psicologiche, per creare un senso di urgenza o di paura, inducendo le vittime ad agire rapidamente senza verificare a fondo l'autenticità della richiesta.

UNA CRISI A LIVELLO GLOBALE

Nell'agosto del 2024 la Commissione Europea ha pubblicato una lettera di informazione intitolata: *Deepfake: a global crisis*, nella quale affrontava il problema generato dalla diffusione di questi falsi. Secondo la comunicazione della Commissione, i deepfake si sono ormai affermati come un potente strumento per la diffusione di fenomeni di disinformazione, ponendo serie sfide alla società. Per il loro tramite è spesso confuso il confine tra realtà e finzione, creando contenuti falsi ma estremamente convincenti: i deepfake consentono la creazione di narrazioni avvincenti che plasmano l'opinione pubblica.

Questi contenuti si stanno anche diffondendo assai rapidamente, perché sono creati per catturare l'attenzione del pubblico. La loro rapida diffusione sui social media sta rendendo assai difficile controllare la divulgazione di informazioni non vere, giacché questi falsi sono specificamente progettati per sfruttare le vulnerabilità di individui e organizzazioni.

La crescente sofisticazione della tecnologia dei deepfake sta ponendo enormi sfide per la loro individuazione e confutazione. Nel campo della medicina e della finanza, ad esempio, vi sono serie preoccupazioni circa la creazione di documenti, quali cartelle cliniche false o alterate e furti di identità.

I deepfake rappresentano dunque un problema globale. Regolamentarne efficacemente l'uso e prevenire le violazioni della privacy richiederà pertanto una cooperazione a livello internazionale: questa tecnologia sta evolvendo molto rapidamente e sarà necessario uno sforzo comune per contrastarla.

IL VADEMECUM DEL GARANTE ITALIANO DELLA PRIVACY

Già nel dicembre del 2020, il Garante italiano della Privacy ha pubblicato un vademecum intitolato *Deepfake: Il falso che ti "ruba" la faccia (e la privacy)*, nel quale si metteva in guardia il pubblico sulla diffusione di app e software che rendevano possibile realizzare deepfake, anche molto ben elaborati e sofisticati, utilizzando un comune smartphone.

La diffusione di questi falsi è di conseguenza notevolmente aumentata, e con essa i rischi connessi, tra cui il furto d'identità e il cosiddetto deepnude, in cui persone ignare vengono rappresentate nude, in pose discinte e situazioni compromettenti, o addirittura in contesti pornografici.

Video *deepnude* sono utilizzati, a totale insaputa dei soggetti rappresentati, anche per alimentare la pratica del sexting (cioè lo scambio e diffusione di immagini di nudo, che può coinvolgere soggetti minori), la pornografia illegale e anche reati gravi come la pedopornografia o il revenge porn, cioè la condivisione online, a scopo di ricatto, denigrazione o vendetta (da parte di ex partner, amanti o spasimanti respinti) di foto e video a contenuto sessuale, spesso completamente falsi.

I deepfake possono anche riguardare politici o *opinion leader* allo scopo di influenzare l'opinione pubblica. Video deepfake possono ad esempio essere inviati agli elettori che simpatizzano per un determinato personaggio politico, rappresentandolo mentre compie azioni poco lecite o mentre si trova in situazioni sconvenienti, per screditarlo e influenzare le opinioni o il voto.

I deepfake possono così contribuire alla diffusione di fake news e alla disinformazione generale, privando le persone della cosiddetta *autodeterminazione informativa* (far sapere di sé ciò che si decide) e incidendo sulla loro libertà decisionale.

L'IMPIEGO NELLE FRODI ASSICURATIVE

Le stesse compagnie assicurative possono essere vittime di frodi intentate con l'aiuto dell'intelligenza artificiale. Ciò può avvenire da parte degli assicurati, che potrebbero presentare richieste di risarcimento false o esagerate, oppure da parte dei terzi danneggiati.


© Joseph Mucira - Pixabay

Nel Regno Unito, ad esempio, si è scoperto che delle telecamere a circuito chiuso, presentate a supporto di un presunto incidente, erano state manipolate per modificare data, ora e targa del veicolo che si presumeva avesse causato l'incidente.

Nel settore assicurativo sono sempre più comunemente adottati sistemi di automazione per la gestione di sinistri e l'utilizzo di supporti come le foto digitali è letteralmente raddoppiato dall'inizio della pandemia. È dunque possibile che vi siano foto alterate che gonfiano l'ammontare dei sinistri, o fuorvianti, perché nascondono informazioni. È poi possibile che vecchie foto siano utilizzate in nuovi sinistri o che immagini trovate su internet siano utilizzate in una richiesta di risarcimento.

In pratica, sembra che la velocità di adozione dei nuovi sistemi automatizzati non sia al passo con l'esigenza di rilevamento delle frodi. Sebbene esistano vari strumenti di rilevamento di shallowfake e deepfake, le compagnie assicurative non sembrano ancora disporre di personale con competenze tali da saper valutare i rischi corsi nella gestione di tali strumenti.

Cinzia Altomare

INSURANCE Daily

N. 2843 LUNEDÌ 15 SETTEMBRE 2025

RICERCHE

Cyber, rallenta la crescita delle coperture

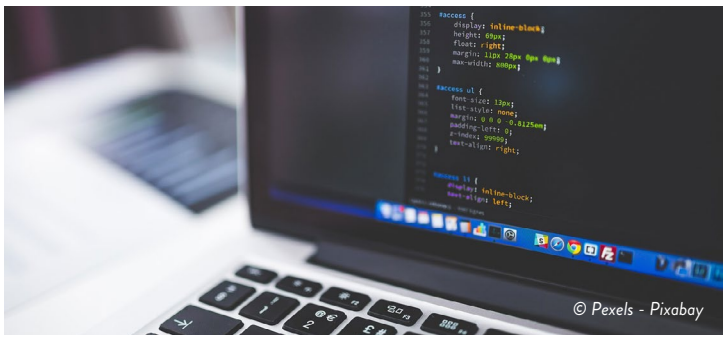
Gli analisti di Swiss Re evidenziano la disponibilità di un'ampia offerta assicurativa in questo ambito. Rimane rilevante il potenziale delle piccole e medie imprese, ancora sottoassicurate e quindi centrali per lo sviluppo futuro del mercato

Negli ultimi anni la crescita globale dell'assicurazione cyber è rallentata significativamente, nonostante un panorama di minacce informatiche in continua evoluzione. Più nello specifico, il tasso di crescita annuo composto (Cagr) dei premi cyber osservato tra il 2017 e il 2022 è rapidamente passato dalla doppia cifra (+31%) a una cifra singola tra il 2022 e il 2026 (+5%).

A certificarlo, lo scorso novembre, era stato il *Cyber reinsurance team* di **Swiss Re**, il quale di recente è tornato sull'argomento con un aggiornamento che mette in evidenza le condizioni attuali del mercato e si interroga sulle possibili vie per un'espansione futura.

Sebbene il settore cyber continui a essere una linea di business promettente, si legge nel nuovo report, si prevede che i premi totali per il 2025 raggiungeranno i 15,6 miliardi di dollari, ed è improbabile che si realizzino le ambiziose previsioni di crescita esponenziale di cui si era parlato negli ultimi anni.

Attualmente il Nord America continua a dominare il settore, detenendo il 66% della quota di premi (circa 10,28 miliardi di dollari). L'Europa resta la seconda regione per importanza, con il 21% dei premi, mentre l'area Asia-Pacifico è al terzo posto con una quota del 10%. In molte economie di queste regioni, gli analisti del riassicuratore svizzero definiscono il potenziale di crescita del mercato cyber come evidente e promettente. Le regioni America Latina e Medio Oriente e Africa, invece, al momento restano marginali in termini di premi.


© Pexels - Pixabay

Le ragioni della frenata

La crescita complessiva del mercato cyber può essere scomposta in due componenti principali: da un lato la crescita organica dell'esposizione (cioè nuovi clienti che acquistano polizze e clienti esistenti che acquistano coperture più ampie), dall'altro la crescita dei tassi (cioè premi più alti per gli stessi limiti). Secondo Swiss Re, l'aumento della concorrenza è una delle principali ragioni per cui il settore è ora al terzo anno consecutivo di riduzione dei tassi: l'offerta di assicurazione cyber continua a superare la domanda.

Il contesto sempre più competitivo ha comportato ulteriori concessioni su premi, limiti, coperture e controlli di sicurezza informatica. Tuttavia, il panorama delle minacce informatiche e delle perdite continua a evolversi rapidamente: le preoccupazioni riguardo a eventi di perdita sistemica e l'aumento delle controversie legali in materia di privacy richiedono cautela nei confronti di riduzioni annuali dei premi.

Il mercato cyber, si legge nel report, deve stabilizzarsi su un livello sostenibile di tassi per poter assorbire eventi estremi e garantire la sostenibilità a lungo termine di questa co-

pertura critica per le imprese. In parallelo, l'espansione verso nuovi segmenti di clientela aiuterà a compensare il rallentamento della crescita degli ultimi anni.

Le Pmi sono ancora sottoassicurate

Le piccole e medie imprese costituiscono il 90% di tutte le aziende a livello globale ma, rispetto ad altri segmenti, rimangono fortemente sottoassicurate in termini di copertura cyber. Per colmare il divario occorre prima di tutto riconoscere la complessità e diversità di questa clientela. Le Pmi non sono delle versioni ridotte di aziende di grandi dimensioni ma hanno caratteristiche, bisogni ed esposizioni cyber proprie e distinte.

Peraltro, anche tra queste realtà bisogna fare delle distinzioni: i dati dei mercati nordamericano ed europeo mostrano che il tasso di adozione dell'assicurazione cyber varia sensibilmente tra micro-imprese (con una penetrazione tra il 5-10%) e Pmi (tra il 10-20%). Anche le abitudini d'acquisto sono diverse, con le prime che tendono a sottoscrivere la copertura cyber come estensione di polizza, mentre le seconde preferiscono soluzioni stand-alone. Ciò che invece accomuna queste realtà è una conoscenza limitata della sicurezza informatica, budget assicurativi ristretti e un grande potenziale di crescita organica.

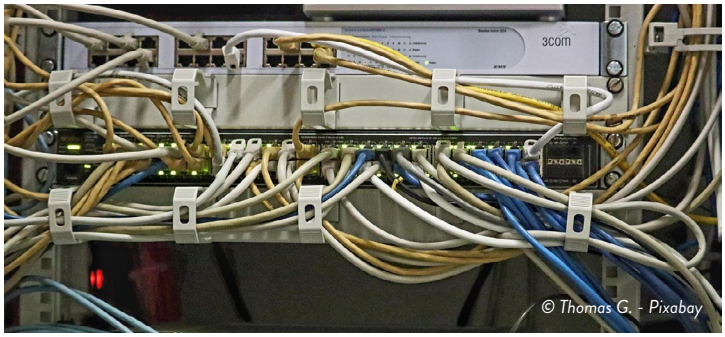
Oggi, a livello globale, le Pmi e le micro-imprese compongono insieme il 30% del mercato totale dei premi cyber (circa 4,7 miliardi di dollari). Rappresentano dunque un enorme gap di protezione e, con esso, una vasta opportunità di crescita per il mercato cyber, sia attirando nuovi clienti, sia facendo upgrade dei clienti esistenti da coperture accessorie a polizze stand-alone.

Cinque leve per crescere

Le ragioni alla base del divario di protezione cyber tra le Pmi sono molteplici e, quindi, sono diverse anche le azioni necessarie per colmarlo. Pur esistendo differenze regionali, un'analisi globale condotta dal riassicuratore ha identificato cinque leve fondamentali per la crescita della protezione cyber per queste aziende.

Prima di tutto, le Pmi spesso sottovalutano o fraintendono i rischi cyber. Molte credono di essere troppo piccole per essere un bersaglio e non sono consapevoli dei benefici dell'assicurazione cyber. Ciò che si può fare, quindi, sono campagne mirate di educazione sui rischi cyber (tenendo presente che i primi a dover essere formati sono agenti e broker tradizionali, che possono mancare di competenze in ambito cyber).

In secondo luogo, molti prodotti assicurativi cyber esistenti non sono adatti alle piccole e medie imprese, essendo state originariamente progettate per grandi aziende e semplicemente ridimensionate. Occorre allora progettare prodotti specifici per le Pmi in modo che siano semplici, accessibili e modulari, e che offrano coperture essenziali con estensioni opzionali. Il terzo scoglio individuato dagli analisti riguarda il budget assicurativo limitato di queste realtà. Spesso l'assicurazione cyber è considerata troppo costosa, anche perché non ne vengono compresi appieno i benefici. La soluzione è sviluppare prodotti adatti alle Pmi, focalizzandosi sulle coperture essenziali per evitare premi eccessivamente elevati.



© Thomas G. - Pixabay

Gli ultimi due ostacoli sono rappresentati da modelli di distribuzione tradizionali non adatti e valutazioni del rischio così complesse da scoraggiare l'adozione. Le soluzioni sono rispettivamente quella di utilizzare piattaforme digitali di distribuzione (o Api verso piattaforme terze) per semplificare il processo d'acquisto, e quella di adottare modelli di sottoscrizione scalabili e basati sulla tecnologia che utilizzano automazione e scoring del rischio per snellire il processo e ridurre i costi.

Nel complesso, il divario di protezione nelle Pmi rappresenta un'opportunità per il mercato cyber, che può così superare le preoccupazioni legate a un possibile rallentamento e puntare su nuove vie di crescita organica (e la riassicurazione sarà fondamentale per aiutare a gestire questo tipo di esposizione). Tuttavia, conclude il documento, è importante riconoscere che l'aumento del tasso di penetrazione tra queste imprese porterà inevitabilmente nuovi rischi.

Michele Starace

Per approfondire su www.insurancetrade.it:

- *Vulnerabilità "zero-day"*
- *Cyber risk, aumentano i furti di dati sul dark web*

INSURANCE DAILY
Direttore responsabile: Maria Rosa Alaggio alaggio@insuranceconnect.it
Editore e redazione: Insurance Connect Srl – Via Montepulciano, 21 – 20124 Milano
T: 02.36768000 email: redazione@insuranceconnect.it
Per inserzioni pubblicitarie contattare: info@insuranceconnect.it
Supplemento al 15 settembre di www.insurancetrade.it – Reg. presso Tribunale di Milano, n. 46, 27/01/2012 – ISSN 2385-2577

INSURANCE Daily

N. 2843 LUNEDÌ 15 SETTEMBRE 2025

INTERMEDIARI, COME REINVENTARE I MODELLI COMMERCIALI

2 OTTOBRE 2025 | 9:00 - 17:00

Hotel Meliá – Via Masaccio, 19 – Milano

PROGRAMMA MATTINA

Modera: Maria Rosa Alaggio, direttore di Insurance Trade e Insurance Review

09:00 – 09:30	**REGISTRAZIONE**
09:30 – 09:50	**IL PRESIDIO DEI RISULTATI ECONOMICI, UN PERCORSO DA CONDIVIDERE** *Presentazione dei risultati della survey condotta da Scs Consulting* *- Giorgio Lolli, manager di Scs Consulting*
09:50 – 10:30	**INIZIATIVE PER IL CONTROLLO DELLA REDDITIVITÀ** *- Paolo Beltrami, titolare dello Studio Beltrami* *- Laura Puppato, vice presidente di Agit* *- Enzo Sivori, presidente di Aua*
10:30 – 10:50	**OPPORTUNITÀ E RESPONSABILITÀ DI UNA RELAZIONE OMNICANALE CON IL CLIENTE** *- Lorenzo Sapigni, direttore generale per l'Italia di Cgpa Europe – Rappresentanza generale per l'Italia*
10:50 – 11:10	**PMI, PROTEZIONE PERSONALIZZATA GRAZIE ALL'AI**
11:10 – 11:30	**COFFEE BREAK**
11:30 – 12:45	**TAVOLA ROTONDA – CLIENTI E INTERMEDIARI, UN LEGAME PER LA PROTEZIONE DEL PAESE** *- Vincenzo Cirasola, presidente di Anapa Rete ImpresAgenzia* *- Claudio Demozzi, presidente di Sna** *- Robert Gauci, ceo del Gruppo Helvetia Italia* *- Umberto Guidoni, co-direttore generale di Ania* *- Roberto Novelli, capo dell'ufficio Segreteria di presidenza e del consiglio di Ivass* *- Flavio Sestilli, presidente di Aiba* *- Simone Tarchiani, chief commercial officer di Unipol* *- Luigi Viganotti, presidente di Acb*
12:45 – 13:00	**Q&A**

** Invitato a partecipare*

Main sponsor

CARGLASS®

CGPA europe

helvetia La tua Assicurazione svizzera

QBE

ROLAND

SCS CONSULTING make your future happen

VIASAT A TARGA TELEMATICS COMPANY

Official sponsor

ACB Associazione Categoria Brokers

INSURANCE Daily

N. 2843 LUNEDÌ 15 SETTEMBRE 2025

INTERMEDIARI, COME REINVENTARE I MODELLI COMMERCIALI

2 OTTOBRE 2025 | 9:00 - 17:00

PROGRAMMA POMERIGGIO

Modera: Maria Rosa Alaggio, direttore di Insurance Trade e Insurance Review

13:00 – 14:00 **LUNCH**

14:00 – 14:30 **COMPONENTE DI SERVIZIO, QUANDO LA QUALITÀ È PERCEPITA DAL CLIENTE**
- *Lamberto Ingrà, digital & service delivery director di Belron Italia*
- *Mariagrazia Musto, presidente di Asap*
- *Giuseppe Sutera, presidente del gruppo agenti Italiana Assicurazioni*
- *Gaetano Vicinanza, presidente del gruppo agenti Sara Assicurazioni*

14:30 – 15:30 **BROKER: STRUMENTI E SOLUZIONI PER L'UNIONE TRA DOMANDA E OFFERTA ASSICURATIVA**
- *Stefano Agnesi, partner e principal broker di Wide Group*
- *Davide Anselmo, general manager di Qbe Italia*
- *Pietro Pipitone, direttore generale di Roland Italia*
- *Nicola Raimondi, chief operating & business management officer di Pib Italy*

15:30 – 15:50 **NUOVE SOLUZIONI PER L'ASSISTENZA AL CLIENTE**
- *Vincenzo Ferrante, training & partnership, sales executive BL insurtech di Viasat*
- *Luigi Viganotti, presidente di Acb*

15:50 – 17:00 **TAVOLA ROTONDA – INTERMEDIARI, COME REINVENTARE I MODELLI COMMERCIALI**
- *Ennio Busetto, presidente dell'Aaa*
- *Mario Cipriano, presidente di Uea*
- *Michele Colio, head of distribution marketing e customers di Zurich Italia**
- *Pierguido Durini, presidente del gruppo agenti Helvetia*
- *Federico Serrao, presidente del gruppo agenti Generali Italia*
- *Domenico Siciliano, head of agency network di Unipol*
- *Enrico Ulivieri, presidente del gruppo agenti Zurich*

ISCRIVITI AL CONVEGNO

SCARICA IL PROGRAMMA

** Invitato a partecipare*

Main sponsor

CARGLASS

CGPA europe

helvetia La tua Assicurazione svizzera

QBE

ROLAND

SCS CONSULTING make your future happen

VIASAT A TARGA TELEMATICS COMPANY

Official sponsor

ACB Associazione Categoria Brokers

INSURANCE Daily

N. 2843 LUNEDÌ 15 SETTEMBRE 2025

La competitività nell'assicurazione auto si gioca su strategie in grado di attribuire valore e qualità ai dati sviluppando progettualità, basate anche sull'intelligenza artificiale, che coinvolgono le attività di underwriting e pricing, il marketing, la gestione dei sinistri.
L'obiettivo è trasformare le potenzialità dei dati in capacità di misurare il rischio, costruire modelli di business, personalizzare l'offerta, potenziare l'area sinistri e il contrasto alle frodi. Intorno ai dati si sviluppano politiche per il rigore tecnico, processi favoriti dalla digitalizzazione, così come una molteplicità di prodotti e servizi per una relazione evoluta con il cliente, sempre più integrati in un ecosistema della mobilità.

Programma

14:00 - 14:30 **Registrazione**

14:30 - 14:40 **Benvenuto ai partecipanti e apertura lavori**
Maria Rosa Alaggio, direttore di Insurance Review e di Insurance Trade
Corrado Sciolla, ceo di OCTO

14:40 - 14:50 **Keynote speech**
Matteo Carbone, fondatore e direttore dell'IoT Insurance Observatory

14:50 - 16:00 **Tavola rotonda – Dal prodotto auto ai servizi integrati per l'ecosistema della mobilità**
Giuseppe Benincasa, segretario generale di Aniasa
Marco Brachini, direttore marketing, brand and customer relationship di Sara Assicurazioni
Alberto Busetto, amministratore delegato di Generali Jeniot
Matteo Lazzarini, dirigente della Direzione Generale Ambiente e Clima - Struttura Aria, Regione Lombardia
Gianfilippo Lena, ad di Telepass Assicura
Giampiero Rosati, procurement director di Ayvens
Corrado Sciolla, ceo di OCTO
Modera: Maria Rosa Alaggio, direttore di Insurance Review e di Insurance Trade

16:00 - 17:10 **Tavola rotonda – Digitalizzazione, telematica e AI per lo sviluppo dell'assicurazione auto**
Mauro Massimo Bonacaro, products, marketing & distribution channels manager di ConTe.it
Marco Cuffia, direttore tecnico danni di Reale Mutua
Eugenio Lamberti, regional leader sales Italy di OCTO
Elena Repetto, chief operating officer e chief technology officer del Gruppo Helvetia Italia
Francesco Tomasoni, responsabile IT - Architetture di business e innovazione di Vittoria Assicurazioni
Maurizio Rainò, head of claims di Axa Italia
Modera: Maria Rosa Alaggio, direttore di Insurance Review e di Insurance Trade

17:10 - 17:20 **Conclusioni e ringraziamenti**

17:20 - 18:30 **Networking cocktail**

CLICC

SOLD OUT