

PRIMO PIANO

Itas, ecco gli obiettivi al 2020

Rafforzamento patrimoniale, una raccolta premi superiore a 1,7 miliardi di euro e un miglioramento del Solvency ratio. Sono gli obiettivi in cima alla lista del nuovo piano industriale 2018-2020 di Itas, approvato ieri dal cda. Nello specifico, il gruppo trentino punta a una crescita virtuosa in tutti i comparti, con un risultato netto che dovrà passare dai 5 milioni di euro stimati per l'esercizio 2017 ai 18 milioni a fine piano. Nei rami danni, l'obiettivo è centrare una crescita del 4,2% annuo, per passare dai 780 milioni di fine 2017 a circa 900 milioni nel 2020. Una crescita che, spiega Itas in una nota, "sarà in parte frutto dell'acquisizione", avvenuta nel 2016, "delle oltre 30 agenzie Rsa", supportata anche "dall'ottimo lavoro svolto dalla rete agenziale già esistente", e in cui il ramo auto dovrà mantenere una crescita omogenea e in linea con gli standard di riferimento. Nei rami vita si punta a centrare a fine piano due obiettivi principali: raggiungere un Solvency ratio del 142% e raddoppiare il volume dei premi dai 330 milioni di fine 2017 a 775 milioni nel 2020. Secondo il dg di Itas, Raffaele Agrusti, "gli obiettivi del piano sono tesi al rafforzamento patrimoniale della società". Per leggere la news completa, [clicca qui](#).

Beniamino Musto

RISK MANAGEMENT

Per il cyber, consapevolezza e approccio integrato

Il sistema assicurativo da solo non può coprire il rischio informatico. È necessario affrontare il tema in una logica di abbinamento del servizio con la polizza. Partendo da una corretta analisi, con l'individuazione di strategie di mitigazione del rischio. Ma, soprattutto, serve un salto culturale. Se ne è parlato ieri al convegno nazionale di Aiba

Nel solo 2017 l'umanità ha generato una quantità di dati pari a quella prodotta dall'inizio della storia. Una nuova era fatta di otto miliardi di oggetti connessi alla rete che si stima diventeranno 20 miliardi entro il 2020. Eppure, nonostante il mondo interconnesso sia più vulnerabile, secondo una ricerca del Politecnico di Milano, solo il 15% delle aziende italiane è protetto sul rischio cyber e il 30% sta valutando quali azioni intraprendere. Con queste evidenze si è aperto, ieri a Roma, il convegno nazionale di **Aiba**, intitolato *Security code. I nuovi scenari per la gestione e il finanziamento del cyber risk nella industria 4.0, alla luce del Regolamento Gdpr*. Un'occasione di riflessione in cui intermediari, compagnie, esperti di sicurezza e imprese si sono confrontati sul tema, alla luce della direttiva europea in vigore dal prossimo 25 maggio. "Il rischio cyber – ha osservato il presidente di Aiba, **Luca Franzì De Luca** – è entrato in tutte le aziende, ma queste stentano ad affrontarlo, mantenendo un atteggiamento scaramantico". L'obiettivo dei broker, in questo senso, è duplice: da un lato creare consapevolezza per aiutare le imprese a compiere il necessario salto culturale, dall'altro sensibilizzare il comparto sulla creazione di un'offerta che colga le specificità di ogni singola azienda e colmi la "voragine di protezione" attualmente presente sul mercato.



Un momento del convegno.

UNA MINACCIA DA CAVALCARE

Serve, dunque, consapevolezza e i dati lo confermano: negli Stati Uniti, un'azienda su tre è tutelata sul rischio cyber, mentre in Italia la media è di 1,5 ogni 10 imprese, per un totale di 30 milioni di euro di coperture. "Siamo ancora all'età della pietra, tanto più che, nel 2021, gli investimenti stimati in intelligenza artificiale ammonteranno a 47 miliardi di dollari", ha commentato **Maria Bianca Farina**, presidente dell'**Ania**. (Continua a pag. 2)



INSURANCE CONNECT su FACEBOOK

Seguici sulla pagina cliccando qui



(Continua da pag. 1)

“Quindi è necessario – ha aggiunto – agire velocemente per colmare quel gap fra il bisogno di protezione di aziende e cittadini e ciò che è stato messo in atto dalle compagnie”. La questione, ha osservato Farina, è che “l’attuale percezione del problema non è tale da far muovere l’offerta”, penalizzata anche dalla difficoltà di apprezzare il rischio in mancanza di una storicità. Qui si apre “un’opportunità immensa per i broker”, laddove il cyber richiede “quell’altissima capacità consulenziale tipica degli intermediari in generale, e dei broker in particolare”. Però, ha ammonito, “bisogna lavorare insieme”. Dal canto suo, l’Ania si sta muovendo su più fronti: sia con l’acquisizione dei dati inerenti il cyber crime, su cui il Gdpr (Regolamento generale sulla protezione dei dati) verrà in aiuto obbligando le imprese alla pubblicazione degli attacchi subiti, sia con la diffusione di figure per la sicurezza dei dati nelle aziende. Su questo, ha sottolineato la presidente dell’Ania, “c’è consapevolezza, ma manca una reale mobilitazione. E siamo noi assicuratori a essere deputati a mobilitarci, in quanto gli unici ad avere competenze, strumenti e cultura per valutare il rischio”. Dal canto loro, ha avvertito, i broker devono “cavalcare il cyber che resta il rischio del domani. Anzi, dell’oggi”.



LA POLIZZA NON È L'UNICA SOLUZIONE

Il convegno è proseguito con una tavola rotonda in cui i partecipanti hanno affrontato il tema dal punto di vista normativo, regolamentare, di mercato e di gestione del rischio.

Il nodo più importante resta l’offerta, che oggi è costituita da coperture che si potrebbero definire più di *data protection* che di rischio informatico a tutto tondo. “Il cyber è un rischio incalcolabile”, ha avvertito Franz De Luca, esortando i broker e le compagnie a unirsi in un tavolo di lavoro che affronti il problema in modo diverso, precisando che “la polizza non può essere la panacea di tutti i mali”. È necessario, ha spiegato, partire dall’analisi delle potenziali minacce, per giungere a strategie di mitigazione in funzione dei processi aziendali, analizzando le coperture in una logica correlata al rischio specifico dell’azienda. In questo, il Gdpr rappresenta l’opportunità per affrontare il cyber da un punto di vista integrato e monitorato nel tempo, vista la dinamicità di questo rischio. “Non esiste un’unica soluzione – ha ammesso il presidente di Aiba – perché ogni soluzione deve essere specificamente adatta a seconda delle esigenze del singolo cliente, a partire dalla definizione del perimetro dei rischi da trasferire”.

ABBINARE SERVIZIO E ASSICURAZIONE

La necessità di un approccio integrato è stata sostenuta anche da **Alessandro De Felice**, presidente di **Anra**, secondo cui “la risposta assicurativa deve essere variegata e in funzione dell’impresa. L’importante – ha osservato – non è piazzare una polizza, ma trasformare la vendita in un’attività di consulenza di valore in una logica di integrazione del servizio con la componente assicurativa: questa è la grande opportunità che hanno i broker per proporre soluzioni che finora il mercato assicurativo non è stato in grado di avanzare”.

UN CAMBIO CULTURALE

L’altra occasione da cogliere, si diceva, è il Gdpr, che aiuterà anche a capire in che modo gli altri rischi vengono presidiati, gestiti, mitigati e conosciuti. Sulla normativa è intervenuto **Stefano Mele**, avvocato presso **Carnelutti Studio Legale Associato**. “Regna un vuoto assoluto di attenzione da parte delle Pmi – ha evidenziato Mele – e anche qui serve un salto culturale che sposti il focus dal concetto di privacy a quello di protezione dei dati personali”. Secondo il legale, è solo cambiando questo punto di vista che sarà possibile giustificare lo sforzo che le aziende devono compiere, da qui al 25 maggio, per adeguarsi.

Il Gdpr, ha sottolineato **Francesco Teodono**, security unit leader di **Ibm Italia**, ha aiutato le aziende “ad aprire gli occhi sul tema”, ma, ha avvertito, mancano le risorse lavorative per affrontare la materia: “non basta dotarsi di software e tool. Servono figure che li sappiano gestire”. In questo senso, la normativa sarà di aiuto: la cyber security resta “un’attività artigianale” basata sull’esperienza umana e l’essere compliant agevola quel cambio culturale in cui l’apporto umano resta protagonista.

CHIAREZZA E TRASPARENZA

Parlando di compliance, il regolatore evidenzia i principali requirement dell’offerta cyber. Le soluzioni assicurative, ha sottolineato **Pietro Franchini** del servizio studi e gestione dati dell’**Ivass**, “non possono coprire tutto: è necessario valutare il rischio residuo, fare in modo che sia assicurabile e costruirsi un buon pricing”. Ma le polizze devono anche fare chiarezza. Devono essere trasparenti relativamente alle garanzie incluse ed escluse, e devono essere corredate da servizi accessori di gestione del rischio e della crisi. Il punto, secondo Franchini, è “se tutto questo il mercato assicurativo sia già in grado di farlo”.

All’offerta si affianca il problema della domanda: “il cliente – ha concluso Franz De Luca – non è ancora pronto a investire in polizze cyber, e i broker sono impegnati nel promuovere un salto culturale sia come operatori qualificati del mercato, sia nei rapporti con il regolatore, per far sì che questa opportunità non vada sprecata”.

MERCATO

Linee guida in vigore dal prossimo anno

L'Ivass fissa i termini per l'applicazione del nuovo modello: dal 1° gennaio 2019 per i nuovi prodotti, mentre per quelli già in commercio la revisione si protrarrà nel corso del prossimo anno



Dalle parole (che si spera possano essere più semplici e chiare) ai fatti. Le nuove linee guida per la stesura dei contratti assicurativi non resteranno lettera morta, come uno di quei buoni propositi finiti nel cassetto e lì rimasti in attesa di un'applicazione prossima ventura: il nuovo modello entrerà in vigore a partire dal prossimo anno. Lo ha stabilito l'Ivass, fissando in una lettera al mercato i termini per l'applicazione delle novità. Il nuovo modello sarà operativo dal 1° gennaio 2019 per i prodotti di nuova commercializzazione, mentre per quelli già presenti sul mercato il processo di revisione potrà protrarsi per tutto il corso del prossimo anno.

L'annuncio è arrivato all'indomani della pubblicazione del documento *Contratti semplici e chiari*, redatto dall'Ania in collaborazione con le principali rappresentanze di agenti, broker e consumatori.

L'iter della revisione

Obiettivo annunciato delle nuove linee guida, com'è noto, è quello di migliorare la comprensibilità dei documenti posti di fronte al consumatore che si appresta ad acquistare una polizza. È in quest'ottica che vanno letti gli inviti a evitare inutili sovrapposizioni e ridondanze, usare un linguaggio più asciutto e lineare, garantire la corrispondenza fra rubriche e contenuto del contratto. Una necessità che l'istituto presieduto da **Salvatore Rossi** aveva sollevato già nell'ottobre del 2016, rilevando, come si legge nella lettera, "come un frequente motivo di insoddisfazione della clientela derivi dal fatto che le clausole contrattuali non sono sempre chiare e univoche. L'Ivass aveva pertanto sollecitato il settore "a confrontarsi con i consumatori e con gli intermediari di assicurazione per individuare eventuali punti di convergenza per la semplificazione dei contratti e proporre possibili soluzioni".

Un traguardo che le varie associazioni riunite in un tavolo tecnico, a detta dell'Ivass, sembrano aver raggiunto in pieno,

"eliminando ad esempio la vecchia distinzione tra condizioni generali e condizioni speciali di polizza, foriera di molte incomprensioni". Le nuove linee guida, prosegue la lettera, renderanno "più fluida la lettura e la comprensione del contratto consentendo all'assicurato un esercizio più agevole dei diritti che gli derivano".

Qualche raccomandazione in più

L'auspicio dell'Ivass è che ora "le società di assicurazione aderiscano alle predette linee guida e diano quanto prima progressiva attuazione alle stesse, procedendo alla redazione e revisione dei contratti" nei tempi stabiliti.

In aggiunta a quanto già inserito nelle linee guida, l'Autorità ha inoltre raccomandato che i contratti rivisti "rechino in copertina l'indicazione che gli stessi sono stati redatti secondo le linee guida del tavolo tecnico". L'istituto ha poi invitato le compagnie a segnalare, utilizzando la casella di posta elettronica semplificazione.contratti@ivass.it, "quali prodotti sono stati rivisti secondo tali linee guida, anche al fine di consentire all'istituto di darne informativa sul proprio sito". Il canale per la segnalazione sarà avviato a partire dall'inizio del prossimo anno e, successivamente, ogni tre mesi fino al completamento processo di revisione: la segnalazione potrà essere effettuata anche in caso di "revisioni che fossero attuate prima del 1° gennaio 2019".

La lettera si chiude infine con una raccomandazione, la stessa avanzata dall'Ania al momento di pubblicare delle nuove linee guida: l'Ivass ha infatti sottolineato "l'importanza di indicare, nei prodotti di assicurazione contro i danni diversi dall'Rc auto, un termine entro cui le imprese si impegnano a corrispondere l'indennizzo all'assicurato". Un punto su cui, evidentemente, è mancato il consenso di tutti i convenuti al tavolo tecnico.

Giacomo Corvi



Insurance Review

Strategie e innovazione
per il settore assicurativo

La rivista che rende l'informazione specialistica
dinamica e immediata.
Uno strumento di aggiornamento e approfondimento
dedicato ai professionisti del settore.

Abbonati su www.insurancereview.it
Abbonamento annuale € 80,00 (10 numeri)

oppure scarica l'app **Insurance Review**



SMART WORK
LAVORO PO

ATTUALITÀ **50 SCENARI**

*zza contro
Brexit*

Ed è subito Ins

Puoi sottoscrivere l'abbonamento annuale nelle seguenti modalità:

- Compilando il form on line all'indirizzo www.insurancetrade.it/abbonamenti
- Inviando un'email a abbonamenti@insuranceconnect.it

Modalità di pagamento:

- On line con Carta di Credito all'indirizzo www.insurancetrade.it/abbonamenti
- Bonifico bancario Antonveneta IBAN IT 94 U 01030 12301 0000 0158 0865

Insurance Daily

Direttore responsabile: Maria Rosa Alaggio alaggio@insuranceconnect.it

Editore e Redazione: Insurance Connect Srl – Via Montepulciano 21 – 20124 Milano

T: 02.36768000 E-mail: redazione@insuranceconnect.it

Per inserzioni pubblicitarie contattare info@insuranceconnect.it

Supplemento al 16 Marzo di www.insurancetrade.it – Reg. presso Tribunale di Milano, n. 46, 27/01/2012 – ISSN 2385-2577