Cibersicurezza, I-Com: “Aumentano gli adempimenti alla normativa, a rischio la competitività delle aziende. Necessario investire su competenze e formazione. Nel 2024 più che raddoppiati corsi e insegnamenti universitari in materia”

- **Presentato oggi alla Camera il Rapporto dell’Istituto per la Competitività (I-Com) nell’ambito dell’Osservatorio sulla Cibersicurezza.**
- **Per il 74% delle imprese il crescente numero di adempimenti previsti dalle normative in materia di cybersicurezza può impattare negativamente sulla competitività aziendale.**
- **Ad ostacolare il processo di compliance sono la mancanza di competenze idonee (51,2%), seguita dall'incertezza interpretativa della normativa (44%) e dalla moltiplicazione di prescrizioni che impongono adempimenti diversi (41%).**
- **L’81% delle aziende ritiene che per migliorare l’ecosistema cybersecurity si dovrebbe puntare sulla consapevolezza e sulla formazione del personale in maniera diversificata per ruolo e competenze.**
- **A gennaio 2024 c’è stato un netto miglioramento dell’offerta formativa in cibersicurezza nel nostro Paese, con 520 tra corsi e insegnamenti, oltre il doppio rispetto ai 234 registrati a inizio 2023. La distribuzione regionale della complessiva offerta formativa si concentra nel Lazio (101 tra corsi e singoli insegnamenti), in Campania (53) e in Lombardia (47)**.

Roma, 15 febbraio 2024 – Per il 74% delle imprese **il crescente numero di adempimenti previsti dalle normative in materia di cibersicurezza può impattare sulla competitività aziendale** principalmente a causa degli oneri burocratici e amministrativi richiesti, nonché per gli investimenti tecnico-organizzativi necessari alla compliance, con possibili ripercussioni anche sui rapporti con i fornitori. **A testimoniarlo è una survey dell’Istituto per la Competitività (I-Com)** dalla quale risulta che **ad ostacolare il processo di conformità sono la mancanza di competenze idonee (sia interne che sul mercato del lavoro), seguito dall’incertezza interpretativa delle norme e dalla moltiplicazione di prescrizioni che impongono adempimenti diversi.** Per migliorare l’ecosistema cybersecurity in Italia, secondo l’81% delle aziende si dovrebbe puntare sulla consapevolezza e sulla formazione del personale in maniera diversificata per ruolo e competenze. Proprio sul tema **a gennaio 2024** I-Com ha osservato **un netto miglioramento dell’offerta formativa in cibersicurezza nel nostro Paese, contando 520 tra corsi e insegnamenti, oltre il doppio rispetto ai 234 individuati a inizio 2023**.

Sono questi alcuni degli elementi che emergono dal Rapporto *"La sfida della cibersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole"*, realizzato dall'Istituto per la Competitività (I-Com) e presentato in occasione del convegno pubblico annuale che si è tenuto oggi presso la Sala Matteotti della Camera dei Deputati, nell'ambito delle attività relative all'Osservatorio I-Com sulla Cibersicurezza e al quale hanno partecipato numerosi tra esperti della materia, rappresentanti delle associazioni e delle istituzioni. Lo studio del think tank guidato dall'economista **Stefano da Empoli** fornisce una panoramica sullo stato dell'arte della cibersicurezza in Italia e in Europa sotto molteplici punti di vista, tra i quali figurano in particolare gli approcci normativi a livello italiano ed europeo, il grado di sicurezza e gli attacchi subiti da aziende e istituzioni pubbliche, i sistemi di certificazione, la consapevolezza di aziende e cittadini.

Tra agosto e ottobre 2023 **l'Istituto per la Competitività (I-Com) ha condotto un'indagine con l'obiettivo di verificare la rispondenza applicativa del quadro regolatorio europeo e nazionale in materia di cybersecurity**, con particolare riferimento al Perimetro di Sicurezza Nazionale Cibernetica (PSNC), coinvolgendo aziende appartenenti a vari settori e avvalendosi anche del sostegno di alcune delle principali associazioni di categoria.

Tra le evidenze spicca la quota degli esponenti delle imprese convinti che **il crescente numero di adempimenti richiesti dalle normative in cibersicurezza possa impattare sulla competitività aziendale, tesi condivisa dal 74% dei rispondenti**. In particolare, **per il 39% delle grandi imprese la principale criticità è legata agli investimenti tecnico-organizzativi necessari alla compliance**, mentre **il 54% delle aziende di medie dimensioni** si concentra prettamente sulla **numerosità degli oneri burocratici e amministrativi richieste** e, infine, **il 29% delle piccole imprese** si preoccupa prioritariamente **dell'effetto sui rapporti con la supply chain**.

Tra i fattori che rendono più difficoltosa la compliance rispetto alle norme in materia di cybersecurity si segnalano la mancanza di competenze idonee sia internamente, sia sul mercato del lavoro (51,2% delle risposte in totale), seguita dall'incertezza interpretativa della normativa (44%) e dalla moltiplicazione – a volte disorganica – di prescrizioni che impongono adempimenti diversi, ma che sono tese al raggiungimento del medesimo obiettivo (41%).

In merito all'adozione di una o più **certificazioni volontarie di cibersicurezza**, **la maggior parte delle imprese non ne ha conseguito alcun tipo**. **Considerando le grandi imprese, il 36% ha già adottato una o più certificazioni, mentre un ulteriore 8% sta lavorando per ottenere la prima entro un anno**. Di converso, tra le medie imprese è l'11% ad aver acquisito almeno una certificazione, mentre il 14% intende ottenere la prima entro un anno. Delle piccole imprese, solo 1 ha già adottato una certificazione e un'altra punta a perseguire la prima entro un anno. Per il 38% il primo **ostacolo**

all'ottenimento di una certificazione volontaria di cybersecurity risiede nei **costi elevati del processo di certificazione**, che **non sono percepiti come proporzionati ai benefici** che ne possono conseguire, mentre quasi il 27% sostiene che **i tempi per l'esecuzione della valutazione e il rilascio della certificazione sono troppo lunghi**. **Appare incoraggiante, invece, che il 70% delle aziende sia d'accordo in merito al fatto che standard comunitari (es. EUCC) possono incentivare le imprese a certificarsi**.

Per migliorare l'ecosistema della cibersicurezza in Italia, secondo **l'81% delle imprese si dovrebbe puntare sulla consapevolezza e sulla formazione del personale in maniera diversificata per ruolo e competenze.** Per oltre il **55% del campione sarebbe opportuno superare la logica dei test obbligatori dinanzi al CVCN in favore dell'accreditamento dei fornitori di fiducia**, mentre un **44% opta per un approccio semplificato con tempistiche controllate** secondo una valutazione dei rischi basata su criteri standard.

"Cruciale insistere sul rafforzamento della cultura di base in cibersicurezza e investire su iniziative idonee a formare i cittadini, affinché acquisiscano al meglio queste capacità", ha commentato il presidente I-Com **Stefano da Empoli**. *"Molte delle iniziative già attive in questo campo nascono e si sviluppano anche grazie al settore privato, spesso in collaborazione e/o col patrocinio di enti pubblici. Appare dunque utile che queste forme di collaborazione pubblico-privato possano essere rafforzate e messe maggiormente a sistema"*.

Per comprendere come si sta evolvendo l'offerta formativa italiana in ambito cybersecurity, a partire dal 2022 **I-Com ha intrapreso un'attività di monitoraggio delle attività di formazione sulla cibersicurezza nel nostro Paese.** Secondo le ultime rilevazioni, effettuate a gennaio 2024, c'è un interesse crescente per queste tematiche da parte del mondo accademico, che a **gennaio 2024** presentava **520 tra corsi e insegnamenti relativi alla cybersecurity rispetto ai 234 individuati a inizio 2023**.

Nel dettaglio, l'analisi ha registrato 259 insegnamenti singoli all'interno di corsi di laurea magistrale, 105 insegnamenti singoli in lauree triennali, 44 progetti di ricerca in dottorati, 34 lauree magistrali, a fronte di 22 corsi all'interno di dottorati di ricerca, 26 master, 23 corsi singoli all'interno di master di I e II livello e 7 lauree triennali interamente dedicate alla cybersecurity. Il **totale delle lauree specifiche (triennali e magistrali) ammonta a 41, ben 15 in più** rispetto a quelle rilevate a gennaio 2023. La formazione post-laurea si affianca a quella universitaria con differenze in termini quantitativi piuttosto importanti: tra progetti di ricerca in dottorati e master di primo e secondo livello sono stati conteggiati ben 70 corsi. Nel complesso, **la formazione specializzata in materia di cibersicurezza in Italia ha raggiunto quota 111 corsi di studio interamente dedicati**.

Per quanto riguarda la **distribuzione regionale dell'offerta formativa**, questa appare **piuttosto disomogenea con una forte concentrazione nel Lazio (101 tra corsi e singoli insegnamenti), in Campania (53) e in Lombardia (47)**. In relazione alle lauree triennali, magistrali, master e progetti di ricerca in dottorati, il Lazio si conferma la regione più interessata con 26 percorsi complessivi, catalizzando buona parte dell'offerta sia in termini di lauree dedicate (8 tra magistrali e triennali), sia per quanto concerne la specializzazione post-laurea (10 master e 8 progetti di ricerca in dottorato). **L'alto numero di master specifici sui temi della cibersicurezza (26) sembra suggerire un'elevata domanda di approfondimento post-laurea su questi temi.**

Nell'ambito della formazione superiore, un ruolo di rilievo è rivestito anche dagli ITS che hanno lo scopo di formare personale tecnico in aree strategiche per lo sviluppo del tessuto economico del Paese. Come si evince dal monitoraggio INDIRE e da un'analisi svolta da I-Com, **gli ITS che si occupano di cibersicurezza sono il 17,6% rispetto al numero complessivo di quelli attivi**, l'offerta formativa erogata ha visto l'avvio di un numero considerevole di corsi in sicurezza informatica specifici e di singoli insegnamenti sul tema all'interno di corsi attinenti a materie differenti.

Per ulteriori informazioni contattare:

Roberto Gagliardini
Segretario generale e Direttore comunicazione I-Com
T. +39 335 81 76 245
gagliardini@i-com.it

Luca Chiapponi
Public Affairs e Comunicazione I-Com
T. +39 327 45 56 217
chiapponi@i-com.it