RASSEGNA STAMPA

“La sfida della cibersicurezza per un’Italia sempre più digitale. Politiche, competenze, regole”

Febbraio 2024

INDICE

Testate cartacee

Il Sole 24 Ore – Cybersecurity, le Pmi sono indietro ma cresce l'offerta negli atenei 4

Italia Oggi - Sicurezza dei dati, troppi oneri 5

L'Arena - «Cybersecurity, più consapevolezza formazione e meno burocrazia» 7

Testate online

CorCom - Cybersecurity, allarme I-Com: "Troppi adempimenti, competitività a rischio" 8

Italia Oggi - Sicurezza dei dati, troppi adempimenti per le imprese 13

MSN - Troppe regole sulla cybersicurezza impattano male sulla competitività delle imprese 16

Agenzia per la Cybersicurezza Nazionale - Frattasi: La crescita della sicurezza digitale del Paese è centrale 18

Adriaeco – Cybersicurezza, Asstel: Filiera TLC strategica 20

Rome International - "La sfida della cibersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole" 22

Agenzie di stampa

AGI - Troppe regole sulla cybersicurezza impattano male sulla competitività delle imprese 24

AGI - Cybersicurezza: studio, per imprese problema aumento adempimenti 26

AGI - Cybersicurezza: studio, per imprese serve formazione personale 27

AGI - Cybersicurezza: studio, offerta formativa raddoppiata in 1 anno 28

AGI - Cybersicurezza: Frattasi, se pmi non investono spariranno 29

AGI - Cybersicurezza: Frattasi, presto norma obbligo notifica minacce 30

9colonne - Camera, convegno su cibersicurezza 31

9colonne – Cybersicurezza, I-Com: per 74% imprese adempimenti normativa impattano su competitività 32

9colonne - Cybersicurezza, Asstel: investimento straordinario competenze digitali 35

Askanews - Cybersecurity: aumento adempimenti impatta su competitività. Ricerca I-Com: "Investire su competenze e formazione" 36

ANSA - Cybersicurezza: report I-Com, imprese temono per competitività. 'Troppi adempimenti'. Ma cresce l'offerta formativa 39

Dire – Cybersicurezza. I-Com: aumentano adempimenti normativi, a rischio competitività aziende 40

LaPresse - Cybersicurezza: Asstel, serve politica industriale 43

Italpress – Cybersicurezza: I-Com "Aumentano adempimenti a rischio competitività" 44

Il Sole 24 ORE

diffusione:54720
tiratura:87266

Cybersecurity, le Pmi sono indietro ma cresce l'offerta negli atenei

Studio I-Com

Da due terzi delle imprese solo il 5% del budget It investito in cibersicurezza

Andrea Biondi

Investimenti in cybersecurity in crescita, ma ancora troppo contenuti e soprattutto con differenze evidenti fra grandi imprese, che stanno spingendo sull'acceleratore e Pmi, in cui la necessità di investire per migliorare gli standard di sicurezza cibernetica fa fatica a far breccia.

È una delle indicazioni che emerge dal rapporto annuale dell'Osservatorio I-Com sulla Cibersicurezza che sarà presentato nel corso del convegno pubblico dal titolo "La sfida della cibersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole", in programma in mattinata a Roma presso la Sala Matteotti della Camera dei Deputati.

Il punto di partenza, ovviamente, sono le dimensioni in crescita del fenomeno su scala globale, non solo in Italia. I numeri su questo versante sono estremamente chiari. Come evidenziato dai dati Clusit, nel solo primo semestre del 2023 si è raggiunta una quota di 1.382 attacchi cyber: ben 637 in più rispetto al primo semestre del 2018. E fra 2018 e 2022 quegli attacchi sono saliti del 60 per cento. Gli attacchi con severity "critica" – e quindi con ingenti perdite economiche e di dati – sono passati dal 32% nel 2021, al 36% nel 2022 e al 40% di inizio 2023.

Numeri che impongono una riflessione seria, dunque, ma che finiscono per scontrarsi con un impegno da parte delle aziende che appare tutt'altro che in linea. Quasi i due terzi delle imprese rispondenti alla survey condotta da I-Com a fine 2023 hanno dichiarato di assegnare meno del 5% del budget IT alla cybersecurity. E non sorprende che figurino solo grandi e medie imprese fra chi dedica tra il 5 e il 15% delle risorse. Inoltre il 51% dice di non aver deciso se incrementare le risorse e il 12% ha già chiarito che non lo farà.

Una ventata di ottimismo arriva invece lato formazione. Ad aumentare infatti è la "dote" accademica. Secondo le ultime rilevazioni, effettuate a gennaio 2024, c'è un interesse decisamente crescente per queste tematiche da parte del mondo accademico che presenta 520 tra corsi e insegnamenti relativi alla cibersicurezza rispetto ai 234 individuati a inizio 2023.

> **A gennaio attivi 520 tra corsi e insegnamenti rispetto ai 234 che erano stati individuati a inizio 2023**

Nel dettaglio, l'analisi di I-Com ha individuato 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. Pertanto, il totale delle lauree specifiche (triennali e magistrali) sul tema della cibersicurezza ammonta a 41: ben 15 in più rispetto a quelle rilevate a gennaio 2023

© RIPRODUZIONE RISERVATA

La proprietà intellettuale è riconducibile alla fonte specificata in testa alla pagina. Il ritaglio stampa è da intendersi per uso privato

ItaliaOggi Sette

diffusione:88589
tiratura:133263

PNRR Istruzioni per l'uso

a pag. 6

I dati dello studio di I-Com evidenziano l'impatto degli adempimenti sulla competitività

Sicurezza dei dati, troppi oneri

La moltiplicazione di prescrizioni ostacola la compliance

Pagina a cura
DI ANTONIO LONGO

Per il 74% delle imprese italiane il crescente numero di adempimenti previsti dalle normative in materia di cybersicurezza impatta negativamente sulla competitività aziendale. In particolare, ad ostacolare il processo di compliance, ossia l'adeguamento al dettato legislativo, sono la mancanza di competenze idonee (51,2%), l'incertezza interpretativa della normativa (44%) e la moltiplicazione di prescrizioni che impongono adempimenti diversi (41%). Secondo l'81% delle aziende per migliorare l'ecosistema della cybersecurity si dovrebbe puntare sulla consapevolezza e sulla formazione del personale in maniera diversificata per ruolo e competenze.

Si tratta dello scenario delineato dal rapporto "La sfida della cybersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole", realizzato dall'Istituto per la Competitività (I-Com), che fornisce una panoramica sullo stato dell'arte della cybersicurezza in Italia e in Europa in merito a approcci normativi, grado di sicurezza, attacchi subiti da aziende e istituzioni pubbliche, sistemi di certificazione, consapevolezza di aziende e cittadini.

"Cruciale insistere sul rafforzamento della cultura di base in cybersicurezza e investire su iniziative idonee a formare i cittadini, affinché acquisiscano al meglio queste capacità", osserva Stefano da Empoli, presidente I-Com. "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".

Dai dati Clusit, citati nel focus, si evince come negli ultimi anni il numero di cyberattacchi annuali a livello globale sia cresciuto di oltre il 60%, passando da 1.554 del 2018 a 2.489 del 2022. Inoltre, anche i valori del primo semestre del 2023 appaiono preoccupanti, in quanto si è raggiunta la quota di 1.382 attacchi, ben 637 in più rispetto al primo semestre del 2018. Negli ultimi tre anni, peraltro, prevalgono gli attacchi che hanno prodotto effetti dannosi importanti per le vittime, comprese ingenti perdite economiche e di dati. In Italia, nel primo semestre del 2023, sono stati registrati 132 attacchi di particolare gravità, ossia una media di 22 al mese, circa dieci volte più elevata rispetto a quella rilevata nel 2018.

A rischio la competitività aziendale. In base agli esiti dell'indagine sull'impatto degli adempimenti prescritti dalle normative sulla cybersicurezza sulla competitività aziendale, per il 39% delle grandi imprese la principale criticità è legata agli investimenti tecnico-organizzativi necessari alla compliance, il 54% delle aziende di medie dimensioni si concentra sulla numerosità degli oneri burocratici e amministrativi richiesti, il 29% delle piccole imprese si preoccupa prioritariamente dell'impatto sui rapporti con la filiera. Per quanto riguarda, invece, i fattori che rendono difficoltosa la compliance rispetto alle norme, prevale la mancanza di competenze idonee, sia internamente sia sul mercato del lavoro, a seguire l'incertezza interpretativa della normativa e la moltiplicazione, spesso disorganica, di prescrizioni che impongono adempimenti diversi ma che sono tese al raggiungimento del medesimo obiettivo. Sul fronte dell'eventuale incremento delle risorse destinate alla cybersecurity, il 51,2% dei rispondenti sta ancora valutando tale eventualità, il 36,1% delle imprese ha già deciso di aumentare gli investimenti mentre il restante 12,6% non stanzierà ulteriori risorse. Peraltro, oltre che puntare sulla consapevolezza e sulla formazione del personale, le aziende ritengono che vadano riservati più aiuti finanziari alle imprese e rafforzata la collaborazione pubblico-privata.

In merito all'adozione di una o più certificazioni volontarie di cybersicurezza, la maggior parte delle imprese delle tre classi dimensionali non ha conseguito alcun tipo di certificazione. Considerando solo le grandi imprese rispondenti, il 36% delle stesse ha già adottato una o più certificazioni di cybersecurity, mentre un ulteriore 8% sta lavorando per ottenere la prima entro un anno. Tra le medie imprese i risultati sono ben diversi, solo l'11% ha acquisito almeno una certificazione, mentre il 14% intende ottenere la prima certificazione entro un anno.

Quanto alle piccole imprese, solo una di quelle che ha risposto all'indagine ha già adottato una certificazione e un'altra punta a perseguire la prima entro un anno. Tra gli ostacoli percepiti dalle imprese per l'ottenimento di una certificazione volontaria, il principale (38%) risiede nei costi elevati che non sono considerati come proporzionati ai benefici che ne possono conseguire. A seguire, quasi il 27% sostiene che i tempi per l'esecuzione della valutazione e il rilascio della certificazione sono troppo lunghi. Tra coloro che hanno dichiarato di avere adottato almeno una certificazione, i principali effetti direttamente riconducibili ad essa sono il miglioramento dell'immagine e della reputazione dell'impresa nei confronti degli stakeholders (45%), una maggiore consapevolezza dei dipendenti e dei collaboratori esterni (39,7%) e più possibilità di partecipare a bandi di gara pubblici o privati (29,5%).

Il panorama legislativo. Vista la crescente importanza del tema si assiste al proliferare di interventi normativi, tanto a livello europeo quanto a livello nazionale. L'Ue sta delineando un ecosistema normativo della sicurezza informatica piuttosto articolato. Il regolamento n. 881/2019 (Cybersecurity Act) ha fissato gli obiettivi, i compiti e gli aspetti organizzativi relativi all'Enisa (Agenzia dell'Unione europea per la cybersicurezza) e ha delineato un quadro per l'introduzione di sistemi europei di certificazione della cybersecurity. Nel 2020 la Commissione europea ha lanciato il "Cybersecurity package", costituito in primis dalla "Strategia dell'Ue in materia di cibersicurezza per il decennio digitale", a cui ha fatto seguito la direttiva n. 2557/2022 sulla resilienza dei soggetti critici (direttiva Cer – Resilience of critical entities). Il 27 dicembre 2022, invece, è stata approvata la direttiva 2022/2555 (Nis2) che ha prescritto l'adozione di misure tecniche, organizzative e operative adeguate e proporzionate in materia di cybersicurezza. La direttiva, inoltre, ha declinato obblighi di segnalazione in caso di incidenti significativi, ha previsto misure di vigilanza e individuato misure per garantire la sicurezza della filiera. Ad integrazione, nello scorso mese di settembre la Commissione europea ha pubblicato i primi orientamenti sull'applicazione di alcune norme fondamentali della direttiva Nis2. Il termine di recepimento per gli Stati membri delle direttive Cer e Nis2 è fissato al prossimo 17 ottobre.

Anche in Italia si è definito un nuovo ecosistema normativo in materia di sicurezza informatica. Il decreto legge n. 105/2019, convertito con la legge n. 133/2019, ha istituito il Perimetro di sicurezza nazionale cibernetica (Psnc) al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi

La proprietà intellettuale è riconducibile alla fonte specificata in testa alla pagina. Il ritaglio stampa è da intendersi per uso privato

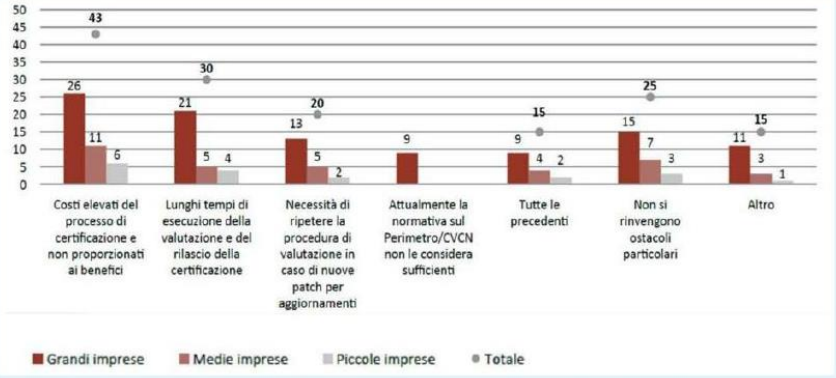
ItaliaOggi Sette

diffusione:88589
tiratura:133263

informatici delle amministrazioni pubbliche, degli enti e degli operatori. Nel 2021 è stata, poi, istituita, in attuazione delle previsioni del Pnrr, l'Agenzia per la cybersicurezza nazionale (Acn), mentre proprio nei giorni scorsi ha avuto il via libera definitivo da parte del parlamento Legge di delegazione europea 2022-2023 che si occupa, in particolare, dei principi e dei criteri per l'esercizio della delega per il recepimento della direttiva Nis2.

© Riproduzione riservata

Gli ostacoli verso la certificazione



Fonte: "La sfida della cybersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole", I-Com

La proprietà intellettuale è riconducibile alla fonte specificata in testa alla pagina. Il ritaglio stampa è da intendersi per uso privato

L'Arena
il giornale di Verona dal 1866

diffusione:25597
tiratura:34017

INDAGINE

«Cybesecurity, più consapevolezza formazione e meno burocrazia»

Per il 74% delle imprese il crescente numero di adempimenti previsti dalle normative in materia di cybersicurezza 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.

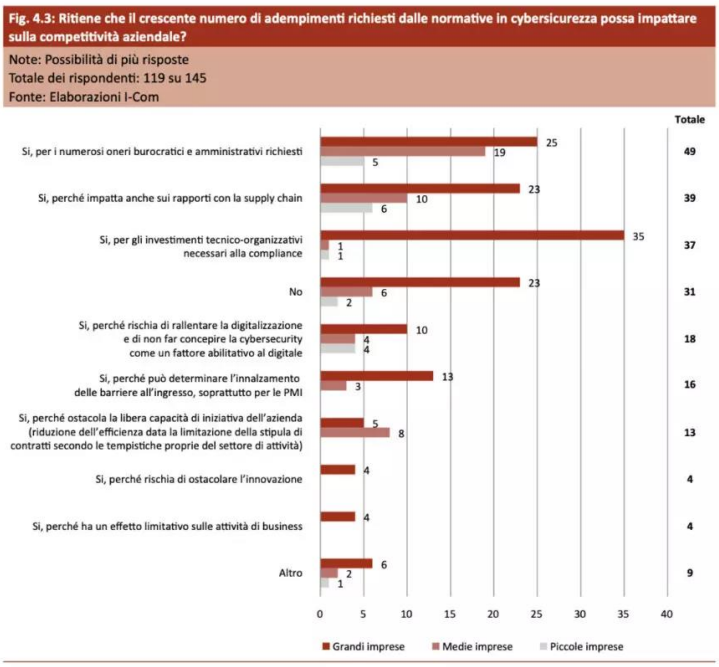
A testimoniarlo è una survey dell'Istituto per la Competitività (I-Com) dalla quale risulta che ad ostacolare il processo di conformità sono la mancanza di competenze idonee (sia interne che sul mercato del lavoro), seguito dall'incertezza interpretativa delle norme e dalla moltiplicazione di prescrizioni 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 di quest'anno I-Com ha osservato un netto miglioramento dell'offerta formativa in cybersicurezza 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 cybersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole», realizzato dall'Istituto per la Competitività. Tra le evidenze spicca la quota degli esponenti delle imprese convinti che il crescente numero di adempimenti richiesti dalle normative in cybersicurezza 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.

ANALISI E FOCUS
Attacchi informatici
Le buone prassi
da seguire in azienda
Security

La proprietà intellettuale è riconducibile alla fonte specificata in testa alla pagina. Il ritaglio stampa è da intendersi per uso privato

CorCom – *15 febbraio 2024* - https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-allarme-i-com-troppi-adempimenti-competitivita-a-rischio/ - **Cybersecurity, allarme I-Com: "Troppi adempimenti, competitività a rischio"**

Tre aziende su quattro sono preoccupate per la mole crescente di adeguamenti normativi. Ancora forte il gap di competenze, anche se l'offerta di formazione è in aumento su tutto il territorio nazionale. Asstel sottolinea il ruolo della filiera tlc. Frattasi (Acn): "La sicurezza è un tema nazionale. Le Pmi investano o spariranno"



Di Patrizia Licata

Tanti **adempimenti** previsti dalle norme sulla **cybersicurezza** possono danneggiare la competitività aziendale: lo afferma il 74% delle imprese in Italia in un sondaggio condotto dall'Istituto per la competitività, I-Com, all'interno del **Rapporto "La sfida della cibersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole" (SCARICA QUI IL REPORT COMPLETO).**

Questo impatto negativo si lega principalmente agli **oneri** burocratici e amministrativi richiesti, ma anche agli **investimenti tecnico-organizzativi** necessari alla compliance. Il processo di conformità è ostacolato innanzitutto dalla mancanza di **competenze**, nonché dall'incertezza interpretativa delle norme e dalla moltiplicazione di prescrizioni che impongono adempimenti diversi.

Secondo il presidente di I-Com, **Stefano da Empoli**, è "**Cruciale insistere sul rafforzamento della cultura di base in cybersicurezza e investire su iniziative** idonee a formare i cittadini, affinché acquisiscano al meglio queste capacità. 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 – ha proseguito da Empoli. – Appare dunque utile che queste forme di **collaborazione pubblico-privato** possano essere rafforzate e messe maggiormente a sistema".

Per il direttore generale dell'Agenzia per la cybersicurezza nazionale (**Acn**), prefetto **Bruno Frattasi,** intervenuto al convegno di presentazione dello studio I-Com, "**La cybersicurezza è un tema nazionale, non legato alla singola impresa. È un tema generale di competitività del Paese** che non può essere trascurato. **Il ritorno che una Pmi può avere** nel breve termine, investendo in cybersicurezza, è poco, ma **nel medio-lungo è tanto**. Bisogna fare capire alle Pmi che, se non raggiungeranno presto la maturità sulla sicurezza, probabilmente saranno votate a una sparizione dal mercato".

Cybersecurity, troppi adempimenti minacciano la competitività

Lo studio del think tank guidato dall'economista Stefano da Empoli fornisce una panoramica sullo stato dell'arte della cybersicurezza in Italia e in Europa sotto molteplici punti di vista, dagli approcci normativi al grado di sicurezza e agli attacchi subiti da aziende e istituzioni pubbliche, dai sistemi di certificazione all'awareness di imprese e cittadini.

Tra agosto e ottobre 2023 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 i risultati spicca la quota degli esponenti delle imprese convinti che il crescente numero di adempimenti richiesti dalle normative in cybersicurezza possa impattare sulla competitività aziendale. 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; infine, il 29% delle piccole imprese si preoccupa prioritariamente dell'effetto sui rapporti con la supply chain.

La mancanza di competenze e awareness

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%).**

Le aziende citano anche la mancante (o insufficiente) consapevolezza dei livelli apicali per quanto riguarda l'ambito cybersecurity, nonché l'aspetto rigido e prescrittivo di alcune normative di settore, il che comporterebbe una gestione più costosa e meno efficace nel medio-lungo periodo.

Va notato che quasi due terzi delle imprese rispondenti assegnano meno del 5% del budget It alla cybersecurity. A dedicare tra il 5 e il 15% del budget alla sicurezza sono per lo più le grandi imprese (27), seguite dalle medie (4). Inoltre, vi è un minimo ricorso al ruolo del Customer security manager, presente solo nel 16,8% delle aziende partecipanti, per lo più grandi imprese (16), seguite dalle medie (3) e una sola piccola.

Il nodo delle certificazioni volontarie

In merito all'adozione di una o più certificazioni volontarie di cybersicurezza, 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, chenon 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.

L'offerta formativa in Italia è raddoppiata

Per migliorare l'ecosistema cybersecurity in Italia l'**81%** delle aziende pensa che si dovrebbe puntare sulla **consapevolezza** e sulla **formazione** del personale in maniera diversificata per ruolo e competenze. Inoltre, 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.**

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.

Il ruolo delle università e degli Its

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 cybersicurezza in Italia ha raggiunto quota 111 corsi di studio interamente dedicati.

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 cybersicurezza (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 cybersicurezza sono il 17,6% rispetto al numero complessivo di quelli attivi e l'offerta formativa erogata ha visto l'avvio di un numero considerevole di corsi in sicurezza informatica.

Frattasi: "Acn sta investendo 22 milioni di euro"

Il direttore generale di Acn, Frattasi, ha chiarito che **gli investimenti in cybersicurezza sono irrinunciabili: "Vanno fatti, nel pubblico nel privato",** ha detto. **"Come sostenerli? L'Acn lo sta facendo, con 22 milioni** che nascono da una misura Ue a cui possiamo accedere. **Con Confindustria e Generali stiamo facendo un piano di sensibilizzazione delle Pmi** per fare comprendere all'uditorio che possono attingere a queste risorse, che sono cospicue ma molto distribuite sono modeste. **Possiamo però incrementarle.** A capo del centro europeo di competenze abbiamo un italiano, è un successo del nostro paese, frutto del lavoro di squadra tra Governo, Farnesina, Acn. Una scelta strategica perché è lì che c'è l'allocazione delle risorse ed è una buona notizia su cui lavorare. C'è un tema del rapporto tra autorità investigativa, giudiziaria e resilienza – ha proseguito Frattasi – Ora il ransomware è la principale minaccia alla nostra economia. Non è solo la minaccia usata dagli hacker che seguono delle ideologie ma anche dalla criminalità organizzata, in misura maggiore di quanto immaginiamo. Se crediamo in una maggiore esigenza punitiva rispetto a questo – ha concluso il prefetto – diamo una maggiore resilienza al paese".

Asstel: "La sfida delle competenze al centro dell'attenzione della filiera tlc"

"Le tlc, attraverso i propri asset, hanno sempre sostenuto i processi di innovazione del Paese. Il settore tlc è strategico a livello globale come abilitatore della trasformazione digitale. In questo contesto, **le competenze nella cybersecurity giocano un ruolo cruciale**. Servono professionisti altamente qualificati in grado di di accompagnare l'innovazione. La collaborazione tra pubblico e privato si misura in questo campo: insieme, possiamo creare alleanze per valorizzare le nuove competenze, per definire profili digitali e percorsi formativi in linea con l'evoluzione del mercato del lavoro", ha affermato **Marco Rendina**, responsabile Lavoro e relazioni industriali di **Asstel,** nel corso

dell'evento "La sfida della cybersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole".

"**Per questo la sfida delle competenze e la trasformazione del lavoro sono attualmente al centro dell'attenzione di tutta la filiera tlc**. Le imprese attribuiscono grande importanza alla formazione permanente: nel 2022, quasi la totalità dei lavoratori è stata coinvolta in attività di upskilling e reskilling e ogni persona ha seguito circa sei giornate di formazione, in aumento rispetto alle quattro o cinque giornate previste alla fine del 2021 per gli anni successivi. **Asstel pone particolare attenzione al tema dell'orientamento, lavorando con il mondo della scuola** con l'obiettivo di stimolare la curiosità dei giovani studenti verso gli abiti di studio Stem".

Rendina ha concluso: "La riforma degli Its è una prima grande risposta del Paese all'evoluzione del sistema formativo determinata dal Pnrr per sviluppare le competenze necessarie al mercato del lavoro delle studentesse e degli studenti. La filiera delle tlc ritiene questo passaggio fondamentale per costruire quelle figure professionali, oggi mancanti, in grado di accelerare la trasformazione digitale dell'Italia".

Italia Oggi – *26 febbraio 2023* - https://www.italiaoggi.it/news/sicurezza-dei-dati-troppi-adempimenti-per-le-imprese-202402231953262113 - **Sicurezza dei dati, troppi adempimenti per la imprese**

La moltiplicazione di prescrizioni ostacola la compliance. I dati dello studio di I-Com evidenziano l'impatto degli obblighi sulla competitività. Anche a causa dell'incertezza normativa e della mancanza di competenze

Di Antonio Longo

Per il 74% delle imprese italiane il crescente numero di adempimenti previsti dalle normative in materia di cybersicurezza impatta negativamente sulla competitività aziendale. In particolare, ad ostacolare il processo di compliance, ossia l'adeguamento al dettato legislativo, sono la mancanza di competenze idonee (51,2%), l'incertezza interpretativa della normativa (44%) e la moltiplicazione di prescrizioni che impongono adempimenti diversi (41%). Secondo l'81% delle aziende per migliorare l'ecosistema della cybersecurity si dovrebbe puntare sulla consapevolezza e sulla formazione del personale in maniera diversificata per ruolo e competenze.

Si tratta dello scenario delineato dal rapporto “La sfida della cybersicurezza per un’Italia sempre più digitale. Politiche, competenze, regole”, realizzato dall’Istituto per la Competitività (I-Com), che fornisce una panoramica sullo stato dell’arte della cybersicurezza in Italia e in Europa in merito a approcci normativi, grado di sicurezza, attacchi subiti da aziende e istituzioni pubbliche, sistemi di certificazione, consapevolezza di aziende e cittadini.

"Cruciale insistere sul rafforzamento della cultura di base in cybersicurezza e investire su iniziative idonee a formare i cittadini, affinché acquisiscano al meglio queste capacità", osserva Stefano da Empoli, presidente I-Com. “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”.

Dai dati Clusit, citati nel focus, si evince come negli ultimi anni il numero di cyberattacchi annuali a livello globale sia cresciuto di oltre il 60%, passando da 1.554 del 2018 a 2.489 del 2022. Inoltre, anche i valori del primo semestre del 2023 appaiono preoccupanti, in quanto si è raggiunta la quota di 1.382 attacchi, ben 637 in più rispetto al primo semestre del 2018. Negli ultimi tre anni, peraltro, prevalgono gli attacchi che hanno prodotto effetti dannosi importanti per le vittime, comprese ingenti perdite economiche e di dati. In Italia, nel primo semestre del 2023, sono stati registrati 132 attacchi di particolare gravità, ossia una media di 22 al mese, circa dieci volte più elevata rispetto a quella rilevata nel 2018.

A rischio la competitività aziendale

In base agli esiti dell’indagine sull’impatto degli adempimenti prescritti dalle normative sulla cybersicurezza sulla competitività aziendale, per il 39% delle grandi imprese la principale criticità è legata agli investimenti tecnico-organizzativi necessari alla compliance, il 54% delle aziende di medie dimensioni si concentra sulla numerosità degli oneri burocratici e amministrativi richiesti, il 29% delle piccole imprese si preoccupa prioritariamente dell’impatto sui rapporti con la filiera. Per quanto riguarda, invece, i fattori che rendono difficoltosa la compliance rispetto alle norme, prevale la mancanza di competenze idonee, sia internamente sia sul mercato del lavoro, a seguire l’incertezza interpretativa della normativa e la moltiplicazione, spesso disorganica, di prescrizioni che impongono adempimenti diversi ma che sono tese al raggiungimento del medesimo obiettivo. Sul fronte dell’eventuale incremento delle risorse destinate alla cybersecurity, il 51,2% dei rispondenti sta ancora valutando tale eventualità, il 36,1% delle imprese ha già deciso di aumentare gli investimenti mentre il restante 12,6% non stanzierà ulteriori risorse. Peraltro, oltre che puntare sulla consapevolezza e sulla formazione del personale, le aziende ritengono che vadano riservati più aiuti finanziari alle imprese e rafforzata la collaborazione pubblico-privata.

In merito all’adozione di una o più certificazioni volontarie di cybersicurezza, la maggior parte delle imprese delle tre classi dimensionali non ha conseguito alcun tipo di certificazione. Considerando solo le grandi imprese rispondenti, il 36% delle stesse ha già adottato una o più certificazioni di cybersecurity, mentre un ulteriore 8% sta lavorando per ottenere la prima entro un anno. Tra le medie imprese i risultati sono ben diversi, solo l’11% ha acquisito almeno una certificazione, mentre il 14% intende ottenere la prima certificazione entro un anno.

Quanto alle piccole imprese, solo una di quelle che ha risposto all'indagine ha già adottato una certificazione e un'altra punta a perseguire la prima entro un anno. Tra gli ostacoli percepiti dalle imprese per l'ottenimento di una certificazione volontaria, il principale (38%) risiede nei costi elevati che non sono considerati come proporzionati ai benefici che ne possono conseguire. A seguire, quasi il 27% sostiene che i tempi per l'esecuzione della valutazione e il rilascio della certificazione sono troppo lunghi. Tra coloro che hanno dichiarato di avere adottato almeno una certificazione, i principali effetti direttamente riconducibili ad essa sono il miglioramento dell'immagine e della reputazione dell'impresa nei confronti degli stakeholders (45%), una maggiore consapevolezza dei dipendenti e dei collaboratori esterni (39,7%) e più possibilità di partecipare a bandi di gara pubblici o privati (29,5%).

Il panorama legislativo

Vista la crescente importanza del tema si assiste al proliferare di interventi normativi, tanto a livello europeo quanto a livello nazionale. L'Ue sta delineando un ecosistema normativo della sicurezza informatica piuttosto articolato. Il regolamento n. 881/2019 (Cybersecurity Act) ha fissato gli obiettivi, i compiti e gli aspetti organizzativi relativi all'Enisa (Agenzia dell'Unione europea per la cybersicurezza) e ha delineato un quadro per l'introduzione di sistemi europei di certificazione della cybersecurity. Nel 2020 la Commissione europea ha lanciato il "Cybersecurity package", costituito in primis dalla "Strategia dell'Ue in materia di cibersicurezza per il decennio digitale", a cui ha fatto seguito la direttiva n. 2557/2022 sulla resilienza dei soggetti critici (direttiva Cer – Resilience of critical entities). Il 27 dicembre 2022, invece, è stata approvata la direttiva 2022/2555 (Nis2) che ha prescritto l'adozione di misure tecniche, organizzative e operative adeguate e proporzionate in materia di cybersicurezza. La direttiva, inoltre, ha declinato obblighi di segnalazione in caso di incidenti significativi, ha previsto misure di vigilanza e individuato misure per garantire la sicurezza della filiera. Ad integrazione, nello scorso mese di settembre la Commissione europea ha pubblicato i primi orientamenti sull'applicazione di alcune norme fondamentali della direttiva Nis2. Il termine di recepimento per gli Stati membri delle direttive Cer e Nis2 è fissato al prossimo 17 ottobre.

Il sistema normativo italiano

Anche in Italia si è definito un nuovo ecosistema normativo in materia di sicurezza informatica. Il decreto legge n. 105/2019, convertito con la legge n. 133/2019, ha istituito il Perimetro di sicurezza nazionale cibernetica (Psnc) al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori. Nel 2021 è stata, poi, istituita, in attuazione delle previsioni del Pnrr, l'Agenzia per la cybersicurezza nazionale (Acn), mentre proprio nei giorni scorsi ha avuto il via libera definitivo da parte del parlamento Legge di delegazione europea 2022-2023 che si occupa, in particolare, dei principi e dei criteri per l'esercizio della delega per il recepimento della direttiva Nis2.

MSN – *15 febbraio 2024* - https://www.msn.com/it-it/money/storie-principali/troppe-regole-sulla-cybersicurezza-impattano-male-sulla-competitivit%C3%A0-delle-imprese/ar-BB1ijKCw?ocid=finance-verthp-feeds - **Troppe regole sulla cybersicurezza impattano male sulla competitività delle imprese**

AGI - Per il 74% delle imprese il crescente numero di adempimenti previsti dalle normative in materia di cybersicurezza può impattare negativamente sulla competitività aziendale. È quanto emerge dal rapporto "La sfida della cibersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole" dell'Istituto per la Competitività (I-Com) che ha condotto un'indagine con l'obiettivo di verificare la rispondenza applicativa del quadro regolatorio europeo e nazionale in materia di cybersecurity.

Per il 39% delle grandi imprese, in particolare, 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.

Il report evidenzia, inoltre, che 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.

In merito all'adozione di una o più certificazioni volontarie di cibersicurezza, la maggior parte delle imprese prese in esame 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. Tra le medie imprese, invece, 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 (esempio EUCC) possono incentivare le imprese a certificarsi.

ACN – *16 febbraio 2024* - https://www.acn.gov.it/notizie/contenuti/frattasi-la-crescita-della-sicurezza-digitale-del-paese-e-centrale

Frattasi: La crescita della sicurezza digitale del Paese è centrale

Il Direttore Generale ACN alla Camera dei deputati ad un Convegno dell'Istituto per la Competitività

"Asl, Pubbliche amministrazioni, società di trasporto pubblico: un universo della pubblica amministrazione che si è presentato in maniera non adeguata rispetto all'incombenza della minaccia informatica. Dobbiamo portare a emersione questa minaccia con l'obbligo della notifica". Così, questa mattina, il Direttore Generale dell'Agenzia per la Cybersicurezza nazionale, prefetto Bruno Frattasi, al convegno promosso dall'Istituto per la Competitività (I-Com) presso la Sala Matteotti

della Camera, dal titolo: "La sfida della cybersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole".

"La norma dell'obbligo di notifica - ha precisato Frattasi - non ha nessuna intenzione di mettere sul banco degli imputati le pubbliche amministrazioni. Sappiamo che il processo di digitalizzazione è andato avanti lentamente e ha avuto criticità. L'approccio è collaborativo, cioé tu devi farmi conoscere la minaccia a cui sei esposto, devi mettermi nelle condizioni di poterti dare il mio supporto".

Il tema della sicurezza informatica, da un punto di vista concettuale, rientra nel più ampio contesto della sicurezza in generale. "Conoscere la minaccia", ha precisato i Direttore, "significa contrastarla meglio. Anche l'AI potrà aiutarci ad avere una migliore conoscenza della minaccia informatica e, quindi, a poterla contrastare più adeguatamente. Un disegno di legge in arrivo alle Camere riguarda la Cybersicurezza con norme che affrontano il tema dal punto di vista della risposta penale, cioé la risposta punitiva, e norme che affrontano il tema dal punto di vista della resilienza, la crescita della resilienza del Paese".

Particolare attenzione alle PMI. "La crescita della sicurezza digitale del paese è centrale. Il ritorno che una PMI può avere nel breve, investendo in cybersicurezza, è poco, ma nel medio-lungo, è tanto. È un tema nazionale, non legato alla singola impresa" ha aggiunto Frattasi. "Investimenti vanno fatti, nel pubblico e nel privato. Come sostenerli? L'ACN lo sta facendo, con 22 milioni che nascono da una misura Ue a cui possiamo accedere. Con Confindustria e Generali stiamo facendo un piano di sensibilizzazione delle PMI per fare comprendere all'uditorio che possono attingere a queste risorse e che possiamo anche incrementarle. A capo del Centro europeo di competenze, l'ente strategico che gestisce i progetti e le risorse destinate allo sviluppo digitale, abbiamo ora un italiano; è un successo del nostro paese, frutto del lavoro di squadra tra Governo, Farnesina, ACN.

Altro tema cruciale è la formazione di competenze. "Da parte di ACN - ha affermato Frattasi - c'è un impegno serio. Oggi stiamo finanziando borse di studio e dottorati sui temi cyber. È un modo di dare il nostro contributo".

Adriaeco – *18 febbraio 2024* - https://www.adriaeco.eu/2024/02/18/cybersicurezza-asstel-filiera-tlc-strategica/ - **Cybersicurezza, Asstel: Filiera TLC strategica**

Necessaria una politica industriale dedicata ed un investimento straordinario nelle competenze digitali

«Le TLC, attraverso i propri asset, hanno sempre sostenuto i processi di innovazione del Paese. Il Settore TLC è strategico a livello globale come abilitatore della trasformazione digitale attraverso la connettività, la progettazione e lo sviluppo di nuovi servizi digitali che rispondono alle esigenze di persone, imprese e Pubblica Amministrazione. Queste sfide richiedono di investire sulla qualità dei servizi, sull'innovazione di processo e di prodotto, nonché sulla crescita e sull'aggiornamento delle competenze professionali delle persone impiegate nelle imprese della Filiera e sulla capacità di attrarre talenti. In questo contesto, le competenze nella cybersecurity giocano un ruolo cruciale. Servono professionisti altamente qualificati in grado di di accompagnare l'innovazione. La collaborazione tra pubblico e privato si misura in questo campo: insieme, possiamo creare alleanze per valorizzare le nuove competenze, per definire profili digitali e percorsi formativi in linea con l'evoluzione del mercato del lavoro».

Così Marco Rendina, Responsabile Lavoro e Relazioni Industriali Asstel, nel corso dell'evento "La sfida della cybersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole".

«Per questo la sfida delle competenze e la trasformazione del lavoro, sono attualmente al centro dell'attenzione di tutta la Filiera TLC. Le imprese attribuiscono grande importanza alla formazione permanente: nel 2022, quasi la totalità dei lavoratori è stata coinvolta in attività di upskilling e reskilling e ogni persona ha seguito circa sei giornate di formazione, in aumento rispetto alle quattro o cinque giornate previste alla fine del 2021 per gli anni successivi. Asstel pone particolare attenzione al tema dell'orientamento, lavorando con il mondo della scuola con l'obiettivo di stimolare la curiosità dei giovani studenti verso gli abiti di studio STEM. Il monitoraggio I-Com delle attività di formazione ha evidenziato come vi siano 520 corsi di formazione universitaria, 41 lauree specifiche e 70 corsi specializzati post-laurea sulla cybersicurezza: un dato che può e deve essere implementato.L'ampliamento dell'offerta formativa deve coinvolgere primariamente gli Istituti Tecnici Superiori: si tratta dell'anello di congiunzione tra il mondo della scuola e del lavoro. La riforma degli ITS è una prima grande risposta del Paese all'evoluzione del sistema formativo determinata dal PNRR per sviluppare le competenze necessarie al mercato del lavoro delle studentesse e degli studenti. La Filiera delle TLC – conclude Marco Rendina – ritiene questo passaggio fondamentale per costruire quelle figure professionali, oggi mancanti, in grado di accelerare la trasformazione digitale dell'Italia».

Rome International - https://www.romeinternational.it/eventi/la-sfida-della-cibersicurezza-per-unitalia-sempre-piu-digitale-politiche-competenze-regole/ - **“La sfida della cibersicurezza per un’Italia sempre più digitale. Politiche, competenze, regole”**

L’Istituto per la Competitività (I-Com) organizza l’annuale convegno pubblico dell’Osservatorio I-Com sulla Cybersecurity dal titolo “***La sfida della cybersecurity per un’Italia sempre più digitale. Politiche, competenze, regole***” in programma giovedì 15 febbraio a Roma presso la **Sala Matteotti, Camera dei Deputati**, con inizio **alle ore 9,50 e termine alle ore 13,00**.

L’evento verterà sull’analisi dello stato dell’arte della cybersecurity in Italia e in Europa da molteplici punti di vista, tra cui in particolare gli approcci normativi a livello italiano ed europeo, il grado di sicurezza e gli attacchi subiti da aziende e istituzioni pubbliche , sistemi di certificazione, sensibilizzazione delle imprese e dei cittadini.

Parteciperanno:
Bruno Frattasi, *Direttore Generale Agenzia per la Cybersicurezza Nazionale;*

Laura Raimondo, *Direttore generale Asstel*;

Alessandro Giglio Vigna, *Presidente Commissione Politiche dell'Unione europea Camera dei Deputati*;

Selene Giupponi, *Segretario Generale e Fondatrice Women4Cyber Italia*;

Alessandro Manfredini, *Presidente AIPSA*;

Ranieri Razzante, *Professore di Tecniche e regole della cybersecurity Università Suor Orsola Benincasa*

In occasione dell'iniziativa verrà presentato il *rapporto annuale prodotto da* ***I-Com*** sul tema.

AGI – *15 febbraio 2024* - https://www.agi.it/cronaca/news/2024-02-15/regole-cybersecurity-competitivita-imprese-25307539/ - **Troppe regole sulla cybersicurezza impattano male sulla competitività delle imprese**

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

Per il 74% delle imprese il crescente numero di adempimenti previsti dalle normative in materia di cybersicurezza può impattare negativamente sulla competitività aziendale. È quanto emerge dal rapporto "La sfida della cibersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole" dell'Istituto per la Competitività (I-Com) che ha condotto un'indagine con l'obiettivo di verificare la rispondenza applicativa del quadro regolatorio europeo e nazionale in materia di cybersecurity.

Per il 39% delle grandi imprese, in particolare, 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.

Il report evidenzia, inoltre, che 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.

In merito all'adozione di una o più certificazioni volontarie di cibersicurezza, la maggior parte delle imprese prese in esame 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. Tra le medie imprese, invece, 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 (esempio EUCC) possono incentivare le imprese a certificarsi.

Cybersicurezza: studio, per imprese problema aumento adempimenti

(AGI) - Roma, 15 feb. - Per il 74% delle imprese il crescente numero di adempimenti previsti dalle normative in materia di cybersicurezza può impattare negativamente sulla competitività aziendale. E' quanto emerge dal rapporto "La sfida della cibersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole" dell'Istituto per la Competitività (I-Com) che ha condotto un'indagine con l'obiettivo di verificare la rispondenza applicativa del quadro regolatorio europeo e nazionale in materia di cybersecurity. Per il 39% delle grandi imprese, in particolare, 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. Il report evidenzia, inoltre, che 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%).

Cybersicurezza: studio, per imprese serve formazione personale

(AGI) - Roma, 15 feb. - 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. È quanto emerge dal rapporto "La sfida della cibersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole" dell'Istituto per la competitività (I-Com). Per oltre il 55% del campione analizzato sarebbe opportuno superare la logica dei test obbligatori dinanzi al CVCN (il Centro di Valutazione e Certificazione Nazionale dell'Agenzia per la Cybersicurezza Nazionale) 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".

Cybersicurezza: studio, offerta formativa raddoppiata in 1 anno

(AGI) - Roma, 15 feb. - L'attività di formazione sulla cibersicurezza nel nostro Paese vede, a gennaio 2024, 520 tra corsi e insegnamenti rispetto ai 234 individuati a inizio 2023. Lo evidenzio il report dal titolo "La sfida della cibersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole" dell'Istituto per la Competitività (I-Com). 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, lo studio di I-Com rileva 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.

Cybersicurezza: Frattasi, se pmi non investono spariranno

(AGI) - Roma, 15 feb. - "Bisognerebbe far capire agli operatori della nostra struttura portante dell'economia italiana, ovvero le pmi, che, se non raggiungeranno un grado di maturità della sicurezza digitale, anche in breve tempo, probabilmente avranno un destino piuttosto infelice. Cioè, saranno votate alla sparizione dal mercato". Lo ha detto il direttore dell'Agenzia per la Cybersicurezza nazionale, Bruno Frattasi, intervenuto al convegno sul report "La sfida della cybersicurezza per un'Italia sempre più digitale" dell'Istituto per la Competitività I-Com. "Questo è un tema nazionale - ha aggiunto ancora il prefetto Frattasi - è un tema generale di competitività del Paese in un contesto, quello del mercato digitale nazionale e dell'unione europea, che non può essere trascurato. Quindi gli investimenti vanno fatti sia nel pubblico, che nel privato".

Cybersicurezza: Frattasi, presto norma obbligo notifica minacce

(AGI) - Roma, 15 feb. - "Un disegno di legge in arrivo alle Camere riguarda la Cybersicurezza con norme che affrontano il tema dal punto di vista della risposta penale, cioè la risposta punitiva, e norme che affrontano il tema dal punto di vista della resilienza, la crescita della resilienza del Paese". Lo ha detto il direttore dell'Agenzia per la Cybersicurezza nazionale, Bruno Frattasi, intervenuto al convegno sul report "La sfida della cybersicurezza per un'Italia sempre più digitale" dell'Istituto per la Competitività I-Com. "Il 'ransomware' è la principale minaccia che pende sulla nostra economia – ha aggiunto il prefetto Frattasi - e che pende sul nostro capo probabilmente in misura ancora maggiore di quanto noi oggi siamo in grado di misurarla. Quindi è ovvio che se diamo una maggiore risposta punitiva al crimine informatico diamo anche una risposta alla capacità di resilienza del nostro Paese". "Il disegno di legge - ci sono norme che di fatto anticipano rispetto alla data di ottobre il tema NIS 2 per la pubblica amministrazione - ha spiegato Frattasi - da un anno che sono direttore generale dell'Agenzia ed ho visto che la maggior parte degli incidenti informatici di cui mi sono dovuto occupare hanno riguardato le Asl, le pubbliche amministrazioni, comuni di media e grande entità, società di trasporto pubblico. Un universo della pubblica amministrazione che si è presentato in maniera non adeguata rispetto all'incombenza della minaccia informatica. Abbiamo un problema di far emergere questa minaccia attraverso l'obbligo della notifica. Conoscere la minaccia significa poterla contrastare meglio e magari anticiparla. L'IA potrà aiutarci ad avere una migliore conoscenza della minaccia informatica e quindi a poterla anche contrastare più adeguatamente". "La norma dell'obbligo di notifica - ha proseguito Frattasi - non ha nessuna intenzione di mettere sul banco degli imputati le pubbliche amministrazioni. Sappiamo che il processo di digitalizzazione è andato avanti lentamente ed ha avuto criticità. L'approccio è collaborativo, cioè tu devi farmi conoscere la minaccia a cui sei esposto, devi mettermi nelle condizioni di poterti dare il mio supporto".

Camera, convegno su cibersicurezza

(9Colonne) Roma, 15 feb - Si tiene oggi, dalle 9,50 alle 13, presso la Sala Matteotti della Camera, il convegno "La sfida della cibersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole" promosso dall'Istituto per la Competitività (I-Com). L'evento -verterà sull'analisi dello 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. In occasione dell'evento - al quale partecipa il direttore generale Agenzia per la Cybersicurezza Nazionale Bruno Frattasi - verrà presentato il rapporto annuale realizzato da I-Com sul tema.

Cybersicurezza, I-Com: per 74% imprese adempimenti normativa impattano su competitività

(9Colonne) Roma, 15 feb - Per il 74% delle imprese il crescente numero di adempimenti previsti dalle normative in materia di cybersicurezza 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 cybersicurezza 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 cybersicurezza 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 cybersicurezza 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 cybersicurezza, 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 cybersicurezza 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 cybersicurezza 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 cybersicurezza 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 cybersicurezza (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 cybersicurezza 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.

Cybersicurezza, Asstel: investimento straordinario competenze digitali

(9Colonne) Roma, 15 feb - "Per questo la sfida delle competenze e la trasformazione del lavoro, sono attualmente al centro dell'attenzione di tutta la Filiera TLC. Le imprese attribuiscono grande importanza alla formazione permanente: nel 2022, quasi la totalità dei lavoratori è stata coinvolta in attività di upskilling e reskilling e ogni persona ha seguito circa sei giornate di formazione, in aumento rispetto alle quattro o cinque giornate previste alla fine del 2021 per gli anni successivi. Asstel pone particolare attenzione al tema dell'orientamento, lavorando con il mondo della scuola con l'obiettivo di stimolare la curiosità dei giovani studenti verso gli abiti di studio STEM. Il monitoraggio I-Com delle attività di formazione ha evidenziato come vi siano 520 corsi di formazione universitaria, 41 lauree specifiche e 70 corsi specializzati post-laurea sulla cybersicurezza: un dato che può e deve essere implementato. L'ampliamento dell'offerta formativa deve coinvolgere primariamente gli Istituti Tecnici Superiori: si tratta dell'anello di congiunzione tra il mondo della scuola e del lavoro. La riforma degli ITS è una prima grande risposta del Paese all'evoluzione del sistema formativo determinata dal PNRR per sviluppare le competenze necessarie al mercato del lavoro delle studentesse e degli studenti. La Filiera delle TLC - conclude Marco Rendina - ritiene questo passaggio fondamentale per costruire quelle figure professionali, oggi mancanti, in grado di accelerare la trasformazione digitale dell'Italia".

Cybersecurity: aumento adempimenti impatta su competitività. Ricerca I-Com: "Investire su competenze e formazione"

Milano, 15 feb. (askanews) - 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.

Dal Rapporto "La sfida della cibersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole", il 74% degli imprenditori è convinto che il crescente numero di adempimenti richiesti dalle normative in cibersicurezza possa impattare sulla competitività aziendale. 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%).

Quanto 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 - commenta 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 emesse 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.

Cybersicurezza: report I-Com, imprese temono per competitività. 'Troppi adempimenti'. Ma cresce l'offerta formativa

(ANSA) - ROMA, 15 FEB - Sulla cybersicurezza aumentano gli adempimenti alla normativa e questo può mettere a rischio la competitività delle aziende: per questo è necessario investire su competenze e formazione. È quanto è emerso dal Rapporto dell'Istituto per la Competitività (I-Com) presentato questa mattina nella Sala Matteotti della Camera dei Deputati. Il report 'La sfida della cybersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole' è stato realizzato tra agosto e ottobre 2023 dal think tank guidato dall'economista Stefano da Empoli. Alla presentazione del documento anche il direttore generale dell'Agenzia per la Cybersicurezza Nazionale Bruno Frattasi.

Dalla relazione è emerso che per il 74 per cento delle imprese il crescente numero di adempimenti previsti dalle normative in materia di cybersicurezza può impattare negativamente sulla competitività aziendale: a ostacolare il processo di compliance sono la mancanza di competenze idonee (51,2 per cento) seguita dall'incertezza interpretativa della normativa (44 per cento) e dalla moltiplicazione delle prescrizioni che impongono adempimenti diversi (41 per cento). Più di 4 aziende su 5 (l'81 per cento) ritengono dunque che per migliorare l'ecosistema cybersecurity si dovrebbe puntare sulla consapevolezza e sulla formazione del personale in maniera diversificata per ruolo e competenze. In ogni caso a gennaio 2024 I-Com ha osservato un netto miglioramento dell'offerta formativa in cybersicurezza nel nostro Paese, con 520 tra corsi e insegnamenti, oltre il doppio rispetto ai 234 registrati a inizio 2023, in particolare nel Lazio (101 tra corsi e singoli insegnamenti), poi in Campania (53) e in Lombardia (47).

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

Cybersicurezza. I-Com: aumentano adempimenti normativi, a rischio competitività aziende

(DIRE) Roma, 15 feb. - 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.

Cybersicurezza: Asstel, serve politica industriale

«Per questo la sfida delle competenze e la trasformazione del lavoro, sono attualmente al centro dell'attenzione di tutta la Filiera TLC. Le imprese attribuiscono grande importanza alla formazione permanente: nel 2022, quasi la totalità dei lavoratori è stata coinvolta in attività di upskilling e reskilling e ogni persona ha seguito circa sei giornate di formazione, in aumento rispetto alle quattro o cinque giornate previste alla fine del 2021 per gli anni successivi. Asstel pone particolare attenzione al tema dell'orientamento, lavorando con il mondo della scuola con l'obiettivo di stimolare la curiosità dei giovani studenti verso gli abiti di studio STEM. Il monitoraggio I-Com delle attività di formazione ha evidenziato come vi siano 520 corsi di formazione universitaria, 41 lauree specifiche e 70 corsi specializzati post-laurea sulla cybersicurezza: un dato che può e deve essere implementato". "L'ampliamento dell'offerta formativa deve coinvolgere primariamente gli Istituti Tecnici Superiori: si tratta dell'anello di congiunzione tra il mondo della scuola e del lavoro. La riforma degli ITS è una prima grande risposta del Paese all'evoluzione del sistema formativo determinata dal PNRR per sviluppare le competenze necessarie al mercato del lavoro delle studentesse e degli studenti. La Filiera delle TLC - conclude Marco Rendina - ritiene questo passaggio fondamentale per costruire quelle figure professionali, oggi mancanti, in grado di accelerare la trasformazione digitale dell'Italia».

Cybersicurezza: I-Com "Aumentano adempimenti a rischio competitività"

ROMA (ITALPRESS) - 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. Dell 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 cost 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.