aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

Rapporto 2021 CSWI AIPSI

Il lavoro femminile nella sicurezza digitale in Italia

A cura di

Andrea Bozzetti
Marco Bozzetti
Laura Rivella

Ringraziamenti

Si ringraziano tutte le donne che hanno risposto al questionario e tutti i Soci di AIPSI, a partire dai Consiglieri, che hanno aiutato nella preparazione del Questionario CSWI di questa edizione, all'individuazione delle donne potenzialmente interessate a rispondere, ed alla realizzazione del presente rapporto finale.
Si ringrazione anche i Media Partner di AIPSI che hanno contribuito a promuovere la compilazione del questionario on line, e che promuoveranno la diffusione e la lettura di questa rapporto attraverso i loro diversi canali di comunicazione.

Dichiarazione di non responsabilità

I grafici ed i testi del presente rapporto sono stati elaborati e redatti con la massima accuratezza e correttezza possibile, partendo dalle risposte al questionario online totalmente anonimo e che pertanto non possono essere verificate. La loro affidabilità, dato il numero delle risposte, è significativa come tendenza, ma non sono in alcun modo di responsabilità da parte degli autori, Marco R. A. Bozzetti e Laura Rivella, di AIPSI.
Tutte le informazioni pubblicate NON costituiscono in alcun modo un servizio di consulenza, né di offerta ai lettori del rapporto. Gli autori, Andrea Bozzetti, Marco R. A. Bozzetti, Laura Rivella, oltre ad AIPSI, NON sono e NON potranno essere responsabili di qualsivoglia perdita o danno in cui si possa incorrere in seguito all'affidamento sul contenuto delle analisi e delle indicazioni del presente rapporto.

Pubblicato Novembre 2021.
Tutti i marchi depositati e i marchi di fabbrica citati nel presente documento sono dei rispettivi titolari.

AIPSI c/o Malabo srl Via Savona, 26 20144 Milano aipsi@aipsi.org tel 02 39443632

SOMMARIO AIPSI CSWI 2021

1. SINTESI DIREZIONALE

Il presente Rapporto AIPSI CSWI 2021 presenta e commenta i risultati dell'indagine di AIPSI[1], Italian Chapter di ISSA[2], attuata nel 2021 nell'ambito del Gruppo di Lavoro CSWI[3] di AIPSI, aperto anche a professioniste non Socie, che si occupa dello situazione in Italia delle donne che, in qualsiasi ruolo, settore e modalità, operano o trattano di sicurezza digitale nell'ambito della loro attività lavorativa.

L'indagine CSWI 2021 è stata condotta in maniera anonima tra le sole donne che volontariamente, saputo dell'iniziativa, hanno voluto parteciparvi compilando il questionario online costituito da 20 domande con risposte predefinite tra le quali scegliere. Il questionario è rimasto attivo online sotto il dominio aipsi.org dal mese di marzo a ottobre 2021: ad esso hanno risposto 468 professioniste che a vario titolo si occupano per lavoro di sicurezza digitale: operano in aziende private e pubbliche sia lato domanda cybersecurity che lato offerta, nella formazione in ambito universitario e non, e come libere professioniste, 9,2% (freelance con partita IVA). Il 13,8% è una imprenditrice, tipicamente di aziende dell'offerta di sicurezza digitale, ed l'8% opera in società di consulenza.

Il bacino delle rispondenti emerso dall'indagine è costituito in prevalenza da laureate (78%) che sono appassionate e soddisfatte dal loro lavoro, anche se esso pone problemi in termini soprattutto di tempo da dedicarvi, di aspetti organizzativi, di competenze, e di retribuzione. Il divario di genere esiste, ma sia questo sia i vari problemi di questo lavoro specialistico, interdisciplinare, in continua evoluzione sia tecnica che normativa-legislativa, sembrano essere ben gestiti limitando quanto possibile gli impatti, soprattutto sulla vita personale e famigliare.

Le rispondenti all'indagine sono prevalentemente adulte e senior: il 78,2% ha più di 35 anni, e solo il 21,8% ha tra i 18 ed i 34 anni. Questa seniority si riflette su molte delle risposte fornite, e caratterizza un bacino di rispondenti mature, preparate, ben consapevoli di che cosa significa lavorare in un campo così complesso, interdisciplinare, in continua evoluzione e di forte competizione. Per meglio analizzare l'impatto dell'età su vari temi considerati, si sono effettuate correlazioni tra le risposte a quel tema con la fascia di età e in taluni casi la laurea o non. L'essere donna nel campo della cybersecurity risulta favorevole solo per il 2,6% delle rispondenti, ma per il 57,1% risulta totalmente indifferente, mentre per il 22,1% è decisamente sfavorevole. Dalle risposte si percepisce chiaramente che il divario di genere, pur essendoci, è meno sentito, forse è inferiore e/o meglio gestito, rispetto ad altri settori anche dello stesso mondo digitale ed informatico, come riscontrato dall'indagine europea WID, Women In Digital, del 2021, che per la parte italiana è commentata nel Cap. 5.

Per più della metà delle rispondenti lavorare in questo campo piace per il suo alto tasso di innovazione, per il continuo contatto con le tecnologie digitali, oltre che per la sua interdisciplinarietà. Il dover affrontare problemi di complessità, tipici nella maggior parte di interventi nella sicurezza digitale, è considerato un aspetto positivo e di interesse per quasi 1/3 delle rispondenti. Invece gli aspetti ed i ritorni economici a livello personale non sono considerati motivanti e di primario interesse (tra l'1,15% ed il 7,5% a seconda delle diverse domande poste).

[1] AIPSI, Associazione Italiana Professionisti Capitolo italiano della mondiale ISSA, https://www.aipsi.org/

[2] ISSA, Information Systems Security Association, https://www.issa.org/

[3] Il Gruppo di Lavoro CSWI, Cyber Security Women Italy, è un Special Interest Group di AIPSI costituito da sole donne che si occupano professionalmente di sicurezza digitale

Quali le necessità e le prospettive di evoluzione/crescita nel prossimo futuro? Quasi la metà delle rispondenti ritiene di dover migliorare e approfondire le proprie conoscenze tecniche (49,4%), per il 28,57% quelle legali, per il 22,08% quelle organizzative e manageriali.
In termini di prospettive, il 43,4% intende continuare nella propria attività nella sicurezza digitale, accrescendo le sue competenze e specializzandosi ulteriormente, mentre un 27,6% intende passare, a breve o a medio termine, ad altre attività e ad altri ruoli. Quasi un ¼ delle rispondenti non ha al momento idee chiare su che cosa vorrebbe fare nel prossimo futuro.

2. EXECUTIVE SUMMARY

This Report presents and comments on the results of the survey CSWI 2021, carried out in 2021 by AIPSI, the Italian Chapter of ISSA.

The CSWI 2021 survey was conducted anonymously among the only women who voluntarily wanted to participate by filling out the online questionnaire consisting of 20 questions with predefined answers to choose from. The questionnaire remained active online under the aipsi.org domain from March to October 2021: 468 professionals responded to it who in various capacities deal with digital security work: they operate in private and public companies both on the cybersecurity demand side and on the offered, in university and non-university training, and as freelancers, (9.2%). 13.8% are entrepreneurs, typically of companies offering cybersecurity, and 8% work in consulting firms.

The emerged pool of respondents is mainly made up of graduates (78%) who are passionate and satisfied with their work, even if it poses problems in terms of time to dedicate to it, organizational aspects, skills, and salary. The gender gap exists, but the high specialized and interdisciplinary work in cybersecurity, always in evolution, seems to be well managed by the majority of the respondents, also by limiting the negative impacts as much as possible, especially on personal and family life.

The respondents are mainly adults and seniors: 78.2% are over 35 years old, and only 21.8% are between 18 and 34 years old. This seniority is reflected in many of the answers provided, and characterizes a pool of mature, prepared respondents, well aware of what it means to work in such a complex, interdisciplinary, constantly evolving and highly competitive field. To better analyze the impact of age on various topics considered, correlations were made between the responses to that topic with the age range and in some cases with the instruction level, with degree or not. Being a woman in the field of cybersecurity is favorable only for 2.6% of respondents, but for 57.1% it is totally indifferent, while for 22.1% it is decidedly unfavorable. From the responses it is clear that the gender gap in the cybersecurity field, is less felt, perhaps it is lower and / or better managed, compared to other sectors even in the same digital world, as found by the European survey WID, Women In Digital , of 2021, which for the Italian part is commented on in Chapter 5.

More than half of the respondents liked working in this field for its high and continuous innovation rate, for the continuous contact with digital technologies and for its interdisciplinary nature. The same complexity of a cybersecurity intervention, of any kind, is considered a positive and interesting aspect for 1/3 of the respondents. Instead, the economic returns on a personal level is not considered motivating and of primary interest (between 1.15% and 7.5% depending on the different questions asked).

What are the needs and prospects for evolution / growth in the near future? Almost half of the respondents believe they need to improve and deepen their technical knowledge (49.4%), for 28.57% the legal ones, for 22.08% the organizational and managerial ones.

For the near future, 43.4% intend to continue in their activity in cybersecurity, increasing their skills and further specializing, while 27.6% intend to move, in the short or medium term, to other activities and other roles. Almost a quarter of the respondents currently do not have clear ideas about what they would like to do in the near future.

3. L'INIZIATIVA CSWI DI AIPSI

CSWI, Cyber Security Women Italy, è uno "Special Interest Group[4]" (SIG) attivato da AIPSI nel secondo semestre 2018 che intende raggruppare tutte le donne attive professionalmente, in qualsiasi ruolo e a qualsiasi livello, nella sicurezza digitale, ed anche se non sono Socie AIPSI, con i seguenti principali obiettivi:

- La costituzione di una comunità femminile delle professioniste che si occupano, anche solo a tempo parziale o di tanto in tanto, di sicurezza digitale: quindi non solo esperte "tecniche" lato domanda ed offerta ICT[5], ma anche chi si occupa di sicurezza digitale a livello legale, di marketing, di psicologia/psichiatria, etc. Una comunità, da porre in relazione anche con altre, ed in primis con i Soci/e di AIPSI ed ISSA, e capace di far sentire la propria voce nel complesso mondo dell'ICT italiano sui temi più caldi e significativi riguardanti in senso lato la sicurezza digitale che coinvolgono ed impattano le donne.
- La realizzazione da parte AIPSI, anche in collaborazione con altre associazioni ed enti, di iniziative specificatamente orientate alle donne, per aiutarle nella loro crescita professionale. Questo è l'obiettivo primario di AIPSI verso tutti i propri Soci, indipendentemente dal loro sesso. I vari servizi che AIPSI ed ISSA già forniscono, soprattutto di tipo tecnico, sono validi per ogni tipo di genere. In questa ottica, la prima iniziativa intrapresa è l'indagine on line sul lavoro femminile riservata alle donne che si occupano, a qualsiasi livello e mansione, di sicurezza digitale, e che ha portato alla stesura di questo primo rapporto.

Il presente Rapporto AIPSI CSWI 2021 rappresenta la conclusione della seconda indagine tenuta nel 2021. La prima indagine tenuta nel corso del 2019, ha portato alla pubblicazione del primo Rapporto AIPSI CSWI 2020, scaricabile dopo il login da: https://www.aipsi.org/aree-tematiche/cswi-cyber-security-women-s-italy/676-rapporto-2020-indagine-aipsi-cswi-sul-lavoro-femminile-nella-cybersecurity-in-italia.html.
AIPSI ha creato nel proprio sito web una sezione dedicata al SIG SWI, cui far riferimento per le nuove iniziative e come archivio per quelle passate: https://www.aipsi.org/aree-tematiche/cswi-cyber-security-women-s-italy.html

[4] Un SIG è un Gruppo di Lavoro attivato per trattare uno specifico tema di particolare interesse per AIPSI e i suoi Soci.

[5] ICT, Information and Communication Technology

4. L'INDAGINE 2021 CSWI ED IL RELATIVO RAPPORTO FINALE

L'indagine CSWI 2021 , come la precedente, si è basata su un questionario on line attivato tramite il sistema open source LimeSurvey, nell'ambito del dominio aipsi.org. Il questionario CSWI 2021 ha recepito i suggerimenti emersi dalla prima edizione: ha mantenuto una struttura analoga, ma ha cambiato alcune domande ed alcune risposte.
Il questionario 2021 è stato reso accessibile da Internet il 10/3/2021, ed è stato chiuso a fine ottobre 2021, quindi in un arco temporale di meno di 8 mesi solari.
L'impostazione data all'indagine CSWI poggia su due punti principali:

- Le rispondenti devono essere e rimanere anonime
- Le rispondenti devono essere solo donne.

4.1 RISPOSTE ANONIME

Il questionario CSWI 2021 è totalmente anonimo: non viene richiesta alcuna informazione personale e/o identificativa del compilatore e della sua azienda/ente, non viene rilevato e tanto meno registrato il suo indirizzo IP, sulla banca dati delle risposte non viene nemmeno specificata la data di compilazione. Tutti i dati forniti vengono usati solo a fini di analisi complessiva e comunque il livello di dettaglio sulle caratteristiche tecniche dei sistemi ICT non consente in alcun modo di poter risalire alla azienda/ente rispondente. Per garantire un ulteriore livello di protezione ed evitare l'inoltro di più questionari compilati dalla stessa persona, il questionario, una volta completato e salvato, non può più essere modificato, e dallo stesso posto di lavoro non è più possibile compilare una seconda volta il questionario.
Gli autori ed AIPSI garantiscono inoltre la totale riservatezza sulle risposte raccolte, utilizzate solo per sintesi statistiche della presente indagine, per la produzione del presente Rapporto e per l'eventuale presentazione dei risultati in eventi.

4.2 RISPONDENTI SOLO DONNE

Dovendo garantire l'anonimato, la necessità contemporanea che le rispondenti fossero solo e veramente donne ha richiesto di non pubblicare l'indirizzo del questionario online, ma di inviarlo via e-mail:

- alle donne già presenti nelle mailing di AIPSI, quali socie, utenti donne registrate al sito web di AIPSI e alla mailing list della newsletter AIPSI, e a quelle conosciute personalmente dagli autori;
- alle donne che hanno inviato una email a CSWI@aipsi.org o a segreteria@aipsi.org per richiedere l'indirizzo web del questionario, dopo aver visto la campagna promozionale dell'iniziativa. In questo modo si è cercato di "chiudere" l'indagine alle sole donne o conosciute direttamente da AIPSI o alle donne che hanno richiesto di avere l'indirizzo web del questionario. Per queste ultime AIPSI ha verificato via Internet, ad esempio tramite LinkedIn e Facebook, che fossero veramente chi dichiaravano di essere, prima di inviare loro il link al questionario online.

4.3 ASPETTI METODOLOGICI DELL'INDAGINE AIPSI CSWI

Come già evidenziato, CSWI è un'indagine via web, anonima, cui possono rispondere tutte le donne interessate a contribuirvi con la loro realtà: esse vi partecipano su base volontaria, senza alcun controllo preventivo da parte del sistema sul web. Il bacino di rispondenti all'indagine non è pertanto predefinito e bilanciato statisticamente. L'indagine CSWI non ha pertanto valore strettamente statistico per fotografare/stimare l'intera situazione in Italia, ma dato il numero di rispondenti fornisce comunque una

interessante e reale indicazione sul lavoro femminile nella sicurezza digitale in Italia così come percepito dalle professioniste che a vario titolo vi operano. Ogni edizione dell'indagine CSWI crea uno specifico bacino di rispondenti: anche le risposte ad identiche domande tra edizioni diverse non possono essere considerate e confrontate da un punto di vista strettamente statistico, ma possono essere utili per evidenziare trend e caratterizzare meglio determinati contesti.
Per contattare il maggior numero possibile di rispondenti donne, AIPSI ha effettuato nel corso del 2021 delle campagne di invito a compilare il questionario CSWI sia sul proprio sito web e sui social net usati, prevalentemente LinkedIn, sia tramite le proprie newsletter. Ulteriori inviti alla compilazione del questionario da parte di donne sono stati inoltre effettuati nell'ambito di eventi sull'ICT e sulla sicurezza digitale tenuti da o nei quali era coinvolta AIPSI. Nel corso del 2021 si stima di aver raggiunto con tali campagne ben più di 1000 donne che si occupano do potrebbero occuparsi di sicurezza digitale; e significativa dovrebbe essere stato il "passa parola" tra professioniste.
Completata la fase di inviti a compilare il questionario, e chiuso lo stesso, gli autori hanno elaborato ed analizzato i dati raccolti tramite fogli elettronici, e sulla base di tali elaborazioni è stato redatto questo Rapporto AIPSI CSW 2021, pubblicato sul sito di AIPSI e che può essere scaricato gratuitamente da tutti gli interessati che effettuano il login: devono quindi registrarsi al sito stesso, fornendo ben pochi dati personali o aziendali, e con precise politiche di privacy e di gestione dei cooki non solo rese pubbliche, ma effettivamente seguite.

4.3.1 Elaborazione dei dati raccolti

L'elaborazione dai dati raccolti elimina per prima cosa quelli palesemente errati o che non hanno senso.
Il calcolo statistico per la creazione dei grafici differisce a seconda del tipo di risposte: singole, multiple, e se sono sotto domande , con relative risposte, di dettaglio rispetto ad una precedente risposta. Per le risposte multiple, il denominatore nel calcolo della percentuale è dato dal numero di rispondenti complessivo per quella domanda o insieme di domande, non per la sommatoria delle risposte avute: la somma finale delle percentuali di ogni singola risposta può essere pertanto superiore o inferiore al 100%.
Per le risposte singole ad una data domanda, il denominatore nel calcolo della percentuale è dato dalla somma delle rispondenti: la somma finale delle percentuali di ogni singola risposta è e deve essere sempre 100%.
In alcuni casi le domande fanno riferimento ad una specifica risposta di una domanda precedente. Per queste "sotto domande" il valore al denominatore per il calcolo della percentuale è dato dal numero delle rispondenti che hanno selezionato la specifica risposta cui fa poi riferimento la sotto domanda.
La correlazione tra i dati forniti da domande diverse dal questionario è effettuata tramite pivot del foglio elettronico contenente tutte i record delle risposte, e da questi fogli pivot vengono rielaborati i dati estratti ed eventualmente creati i relativi grafici.

5. LA DIVERSITÀ DI GENERE NEL DIGITALE IN ITALIA RISPETTO ALL'UNIONE EUROPEA

Il tema della "diversità di genere" è molto trattato in generale, a livello italiano e mondiale, con varie indagini, e talune considerano il mondo del lavoro e l'utilizzo di Internet e dei servizi digitali per analizzare il divario digitale di genere.

La cybersecurity fa parte del più generale mondo dell'informatica e dei sistemi digitale: data la sua forte interdisciplinarietà, essa coinvolge, o può coinvolgere, professioni e mestieri diversi, che fino a ieri poco avevano a che fare con l'ICT: si considerino gli psicologi per individuare le motivazioni di possibili attaccanti, gli analisti dei rischi, i gestori della documentazione, gli avvocati per cause legate agli attacchi e per la gestione della privacy, e così via. Questa trasversalità rende difficili indagini sulle persone che si occupano di sicurezza digitale, e poche e poco attendibili o strettamente limitate per tipo di specifica attività le indagini cui poter far riferimento.

Per meglio inquadrare la situazione al femminile nell'ambito professionale del digitale, e quindi della cybersecurity, si è considerata l'indagine europea "Women in Digital" (WID), correlata all'indagine per l'indice DESI, Digital Economy and Society Index, si veda https://digital-strategy.ec.europa.eu/en/news/women-digital-scoreboard-2021 e https://digital-strategy.ec.europa.eu/en/policies/desi

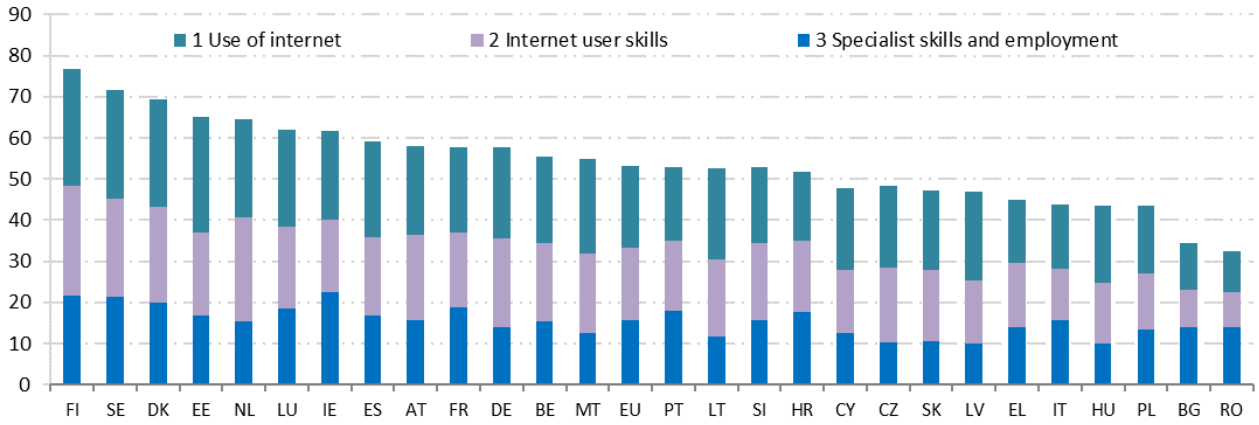


Fig. 5-1 (Fonte WID 2021)

La fig. 5-1 confronta in generale la situazione delle donne nei vari paesi dell'UE per il digitale secondo tre criteri/indici: l'uso di Internet, le competenze/conoscenze per usarlo, il numero di specialiste nell'ICT attive. La posizione dell'Italia (IT) è complessivamente al quint'ultimo posto, rispetto al quart'ultimo del 2020: un piccolo miglioramento ma sempre agli ultimi posti della classifica europea, analogamente a quanto avviene con l'indice DESI. L'indice percentualmente meno peggio, tra i tre criteri, è quello delle specialiste che lavorano nell'ICT.

La fig. 5-2 confronta il numero di specialisti nell'ICT (che include, almeno in parte, quelli operanti nella sicurezza digitale) per genere in Italia e, in media, nell'UE. Si evidenzia chiaramente il divario di genere sia in Italia sia in UE, ma anche le percentuali maschili sono basse, sia in Italia sia in UE, tenendo conto che i "dati" sono "il petrolio" del modo digitale e che l'ICT e la relativa trasformazione digitale stanno completamente trasformando il modo di lavorare e di vivere. Un gap di competenze ben noto, ma che di fatto non migliora e

rimane molto grave, se non vi si pone rimedio, in termini di competitività mondiale e di conseguente crescita, o decrescita, economica.

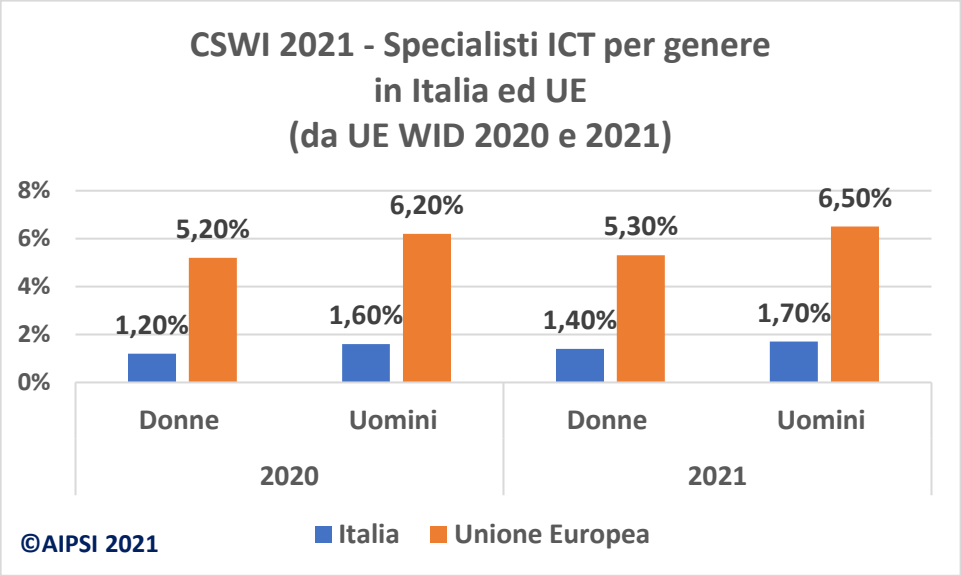


Fig. 5-2 (Fonte WID 2020 e 2021)

La fig. 5-3 mostra, per il 2020 ed il 2021, il divario retributivo di genere **non corretto** nel mondo digitale sia in Italia che in UE. Confrontando la permanenza percentuale di questo divario si evidenzia che per l'Italia è diminuito di 3 punti percentuali, mentre per l'UE, come media tra i vari Paesi, è aumentato di un punto.

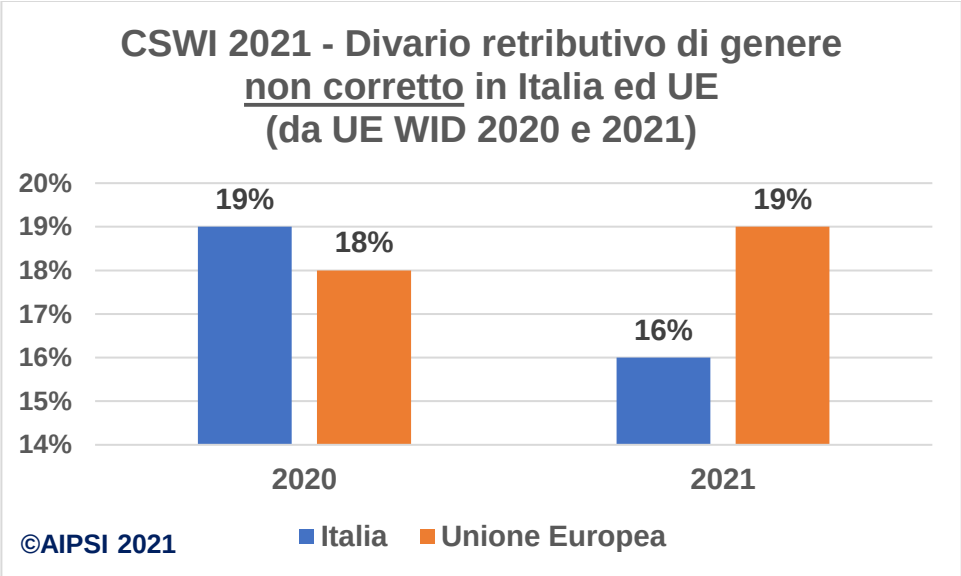


Fig. 5-3 (Fonte WID 2020 e 2021)

Questo dato conferma quanto emerso dalla presente indagine CSWI 2021 sul divario retributivo di genere nell'ambito della sicurezza digitale, si veda fig. 7-1.
Il divario esiste in ambito sia europeo sia italiano, ma almeno il bacino delle rispondenti di CSWI 2021 evidenzia una percezione meno critica del divario di genere, soprattutto per le professioniste che hanno già maturato qualche anno di esperienza, rispetto all'intero settore ICT o ad altri..

6. IL CAMPIONE EMERSO DELLE RISPONDENTI

Grazie alla lunga campagna promozionale per la compilazione del questionario, 468 professioniste hanno acceduto al questionario, rispetto alle 247 della prima edizione, che aveva avuto una ancor più lunga fase promozionale. Un netto miglioramento, ma ancora con molte rispondenti che hanno solo iniziato o risposto alle sole prime dimande, ma non completato l'intero questionario: un problema emerso anche nella prima edizione e che affligge la maggior parte delle indagine online ed anonime.
Tra le cause sicuramente un inziale problema tecnico della piattaforma Limesurvey tra versione inglese ed italiana del questionario, pur essendo solo in lingua italiana. Molto probabile poi la relativa lunghezza del questionario: essendo di sole 20 domande, e con le risil questionario non è stato poi ripreso poste preimpostate tra cui scegliere, richiedeva circa 15 minuti per la sua totale compilazione. Probabilmente troppo tempo da dedicare per alcune rispondenti. Un'altra causa può essere stata l'interruzione della compilazione del questionario online per sopraggiunte urgenze, ed esso non è stato poi ripreso e completato.
Il numero di rispondenti raggiunto è comunque significativo, e significative le risposte ottenute dall'indagine e nel seguito descritte e commentate.
Il primo dato importante, anche per meglio interpretare le successive risposte, è la **fascia di età** delle rispondenti, mostrata in fig. 6-1. Il maggior numero di rispondenti, 36,1% è nella fascia 45-54 anni, e complessivamente le over 45 si attestano al 61,3%.
La grande maggioranza delle rispondenti è quindi costituita da professioniste senior e very senior, con una fascia di giovani rispondenti, tra i 18 ed i 34 anni, che è del 21,8%, rispetto 34% della precedente edizione.

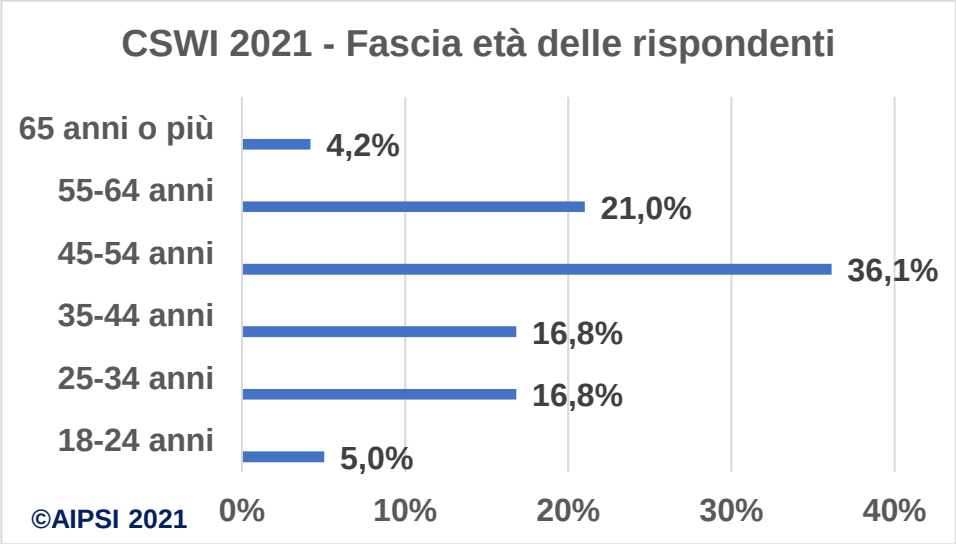


Fig. 6-1

Il livello di istruzione delle rispondenti è alto, come indicato nella fig. 6-2 . Più di 2/3 delle rispondenti hanno conseguito la laurea, e di queste solo il 9,3% ha una laurea triennale. Le non laureate sono il 28% delle rispondenti.
La fig. 6-3 mostra il tipo di laurea: la grande maggioranza, 67,1% ha conseguito una laurea di tipo Scientifico/Tecnico. Con Altro sono indicate lauree di tipo economico e di comunicazione.

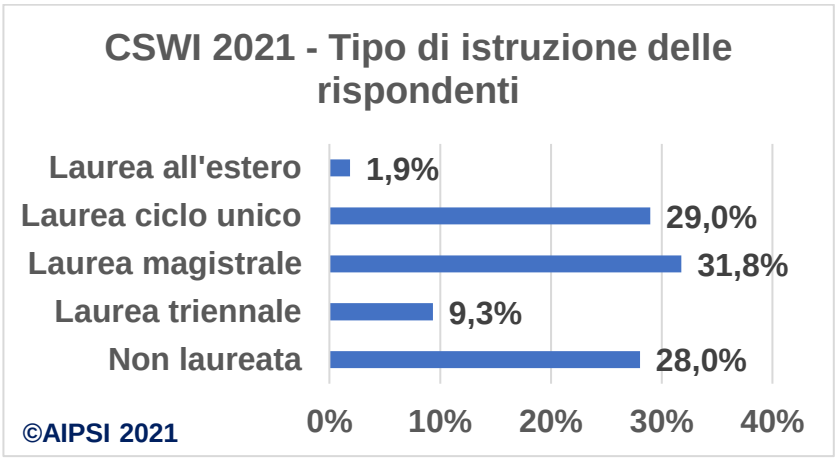


Fig. 6-2

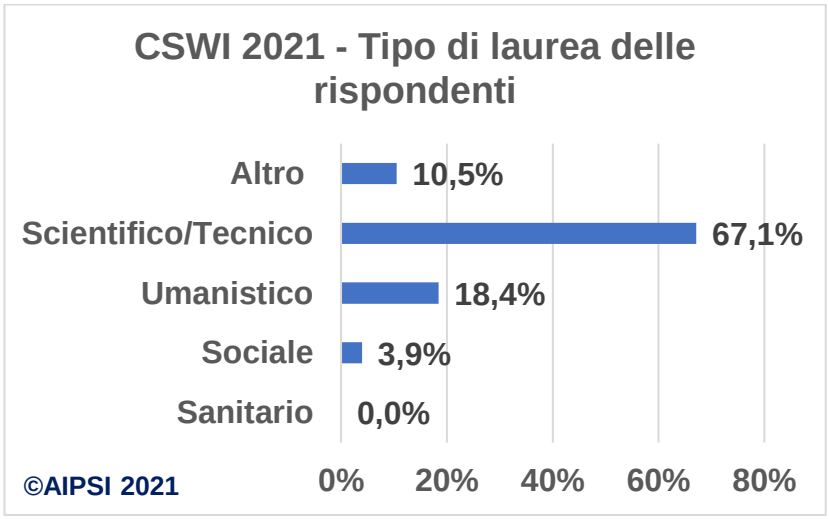


Fig. 6-3

Relativamente poche, il 22,7%, hanno acquisito specifiche certificazioni tecniche e/o manageriali inerenti la sicurezza digitale e la sua gestione, come indicato nella fig. 6-4.

Fig. 6-4

Come si evince dall'elenco della tabella in fig. 6-5, le certificazioni acquisite sono quelle più note e diffuse. Le ragioni più probabili includono la "seniority" anche professionale delle rispondenti, che acquisirono le certificazioni più significative ai loro tempi e che non sono interessate ad acquisirne di nuove, ed il numero relativamente limitato di rispondenti che svolgono determinati ruoli, come ad esempio quello di DPO, e che necessita quindi di alcune certificazioni più recenti. Nella voce "Altre" sono incluse certificazioni ECDL, sulla gestione della qualità e sulla gestione dei progetti, quali PMI e Prime.

La certificazione più diffusa tra le rispondenti è quella ITIL, tipica e molto nota in Italia per la gestione operativa dei sistemi informativi, e quindi anche della loro sicurezza. Al secondo posto come diffusione tra le rispondenti quella di Lead Auditor/ISO 27001, specifica per la sicurezza digitale, con il 6,8%, cui seguono tutte le altre con percentuali inferiori al 5%. Non deve stupire la percentuale assai bassa, 2,6% per le certificazioni DPO[6]: pur essendo assai diffuso il ruolo di DPO in Italia a seguito dell'introduzione del regolamento europeo GRDP sulla privacy, nessuna professionista con questo ruolo ha compilato il questionario, come evidenziato nella fig. 7-1; inoltre le certificazioni DPO non sono ancora diffuse tra i professionisti, donne e uomini, che rivestono tale ruolo, anche perché non ancora richieste come obbligatorie dalla maggior parte delle aziende/enti. La certificazione più europea e concettualmente più significativa per ogni ruolo e competenza ICT, l'eCF, ha ancora una diffusione molto limitata in Italia, soprattutto per le figure di Security Specialist e di Security Manager: ed anche se è l'unica ad essere riconosciuta, e promossa, da tutti i paese UE e per questo ha di fatto un valore "legale" europeo (per approfondimenti si veda https://www.aicanet.it/e-cfplus e https://www.aipsi.org/aree-tematiche/crescita-e-percorsi-professionali.html).

[6] Esistono diverse certificazioni per il ruolo di DPO, Digital Privacy Office, introdotto dal Regolamento Generale sulla Protezione dei Dati, n. 2016/679. Nel questionario la risposta indicata era volutamente generica con l'indicazione del solo acronimo DPO.

CSWI 20201- Certificazioni delle rispondenti (risposte multiple)	%
ITIL	8,4%
Lead Auditor (ISO 27001)	6,8%
Eucip	4,2%
CISA	2,6%
DPO	2,6%
COBIT	2,6%
eCF - UNI EN 16234-1:2016 Security Manager	1,6%
eCF - UNI EN 16234-1:2016 Security Specialist	1,1%
CISM	1,1%
CISSP	0,5%
SSCP	0,5%
CISP	0,5%
OPSA	0,5%
CCSK	0,5%
Altre certificazioni	6,3%

Fig. 6-5

La fig. 6-6 mostra che il 22,7% delle rispondenti ha acquisito o sta acquisendo un dottorato o master inerente la sicurezza digitale.

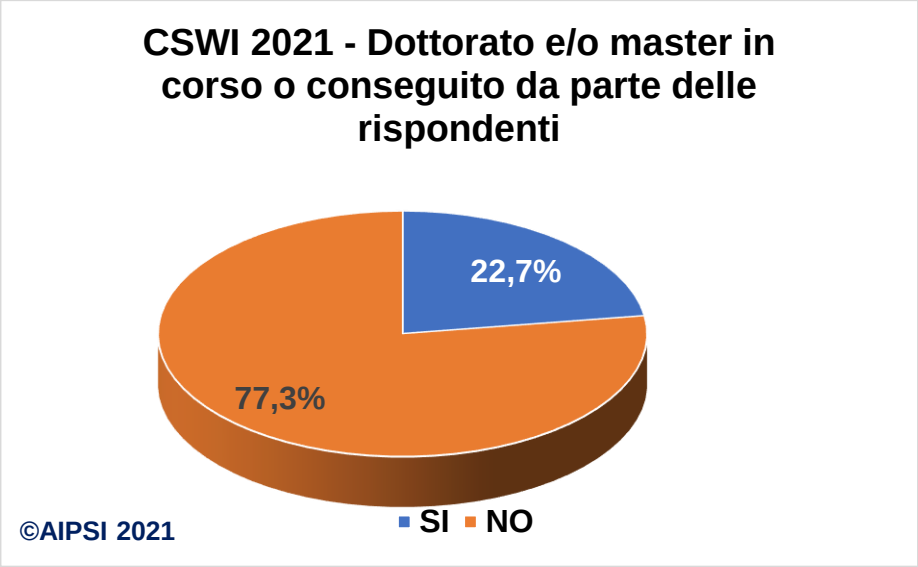


Fig. 6-6

7. ESSERE DONNA NEL MONDO DELLA SICUREZZA DIGITALE IN ITALIA: IL VISSUTO DELLE RISPONDENTI

Il presente capitolo analizza il tipo di lavoro ed il ruolo svolto nel campo della sicurezza digitale dalle rispondenti, e considera le difficoltà e i fattori positivi evidenziati nell'ambito della loro attività passate e presente nella sicurezza digitale. Sono i temi chiave per valutare l'effettivo divario di genere in questo settore, dove nella maggior parte dei casi una professionista deve dividere il suo tempo tra il lavoro, e quindi la possibilità di carriera, e la vita personale e domestica: la cura della famiglia, in particolare di figli giovani, a carico prevalente della donna, può incidere sul suo lavoro e sulla sua carriera.

La fig. 7-1 illustra il ruolo di lavoro svolto dalle rispondenti quando si occupano di cybersecurity. La maggior parte se ne occupa lato offerta, poche quelle se ne occupano lato domanda, e ancor meno quelle per la Pubblica Amministrazione. delle evidenzia quasi la metà delle rispondenti lavora presso una società fornitrice di soluzioni IT o di cybersecurity (il 48,1%), mentre "appena" il 17,3% opera presso società della domanda ICT, ossia di aziende utenti di informatica e di sicurezza digitale. Un significativo % delle rispondenti sono imprenditrici o operano ai vertici di aziende, e come decisori di vertice si occupano anche della sicurezza dei loro sistemi informativi, o le loro società sono del mondo ICT e vendono soluzioni di cybersecurity. Un 17,2% opera nella consulenza nella sicurezza digitale, e di queste il 9% sono freelance. Nessuna rispondente ricopre ruoli di CTO, CIO e CISO: in effetti nel mercato italiano ben poche donne rivestono, al momento, questi ruoli. AIPSI ha invitato alcune di queste poche, che conosce, a rispondere, ma purtroppo non si sono ricevute risposte da loro, dato il risultato. Si tenga conto che l'indagine è anonima, e AIPSI non sa chi compila il questionario e chi no, nell'ambito delle potenziali rispondenti contattate e alle quali è stato inviato il link al questionario online.
Le più giovani, come confermato anche nella fig. 7-2, sono ancora studentesse, alcune stanno facendo degli stage lavorativi in aziende, ed altre sono agli inizi della loro carriera nel campo della cybersecurity. Nella voce "Altro", che ha un considerevole 26,4%, confluiscono un 6,2% di ricercatrici nel campo della sicurezza digitale (si ipotizza in ambito universitario), un 3,7% di insegnanti nelle scuole superiori, tipicamente istituti tecnici, un 2,5% di docenti universitarie. La percentuale rimanente include soprattutto professioniste che rivestono ruoli nella vendita e nel marketing di aziende dell'offerta di cybersecurity.

La fig. 7-2 infatti dettaglia i diversi ruoli ricoperti dalle rispondenti in funzione della loro età, e conferma quanto già evidenziato al riguardo: la maggior parte delle rispondenti ha una età medio alta, come indicato nella fig. 6-1, con un 92,8% delle rispondenti con più di 35 anni. Nella fig. 7-2 la barra gialla evidenzia i ruoli ricoperti dalla fascia 45-54, che ricoprono con le percentuali maggiori i ruoli di dipendenti, imprenditrici, consulenti.

La fig. 7-3 mostra da quali ambienti lavorativi e di interesse provenivano le rispondenti, prima di occuparsi di sicurezza digitale. Poco meno della metà, come è prevedibile, proviene dall'informatica. Il 17% delle rispondenti proviene dal settore del marketing e delle vendite: tale percentuale è ragionevole e non inconsueta, dato che un certo numero di rispondenti opera nell'area marketing e vendite di aziende del settore cybersecurity, incluse nella voce "Altro" della fig. 7-1.
Le indicazioni di "Altro" della fig. 7-3 includono provenienze dal mondo legale, da quello della privacy e da quello economico.

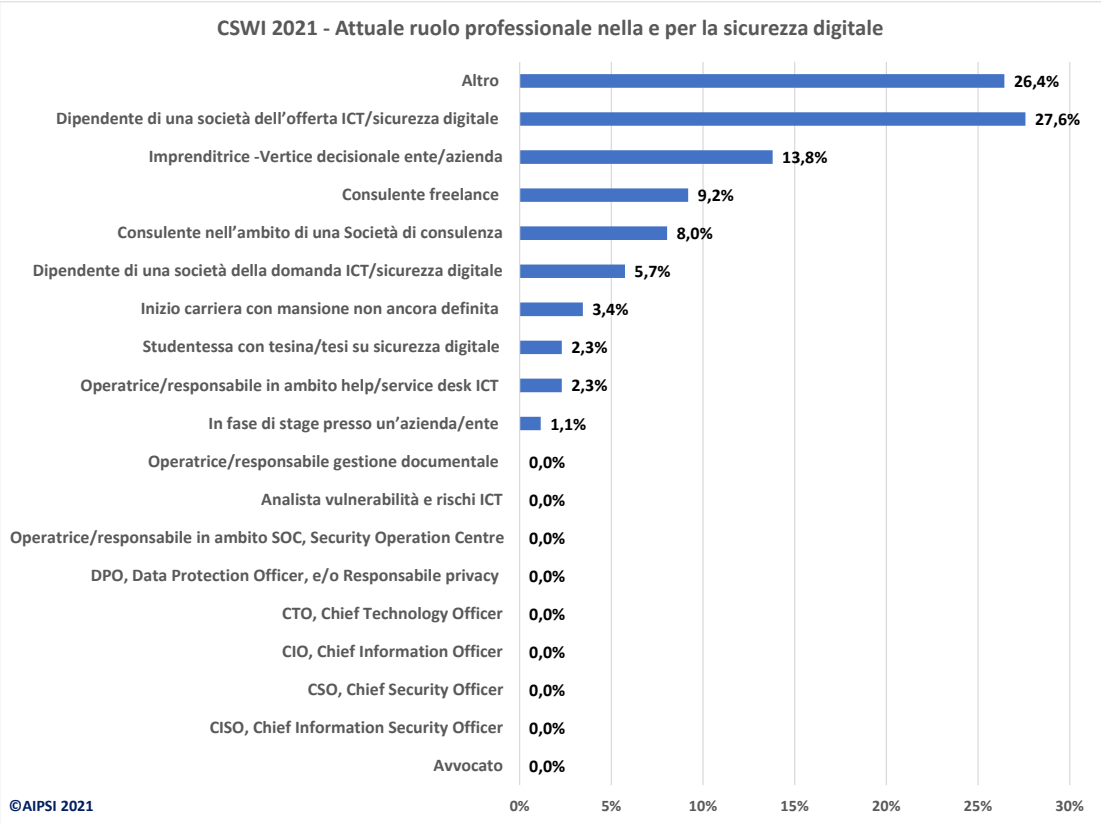

CSWI 2021 - Attuale ruolo professionale nella e per la sicurezza digitale
Altro 26,4%
Dipendente di una società dell'offerta ICT/sicurezza digitale 27,6%
Imprenditrice -Vertice decisionale ente/azienda 13,8%
Consulente freelance 9,2%
Consulente nell'ambito di una Società di consulenza 8,0%
Dipendente di una società della domanda ICT/sicurezza digitale 5,7%
Inizio carriera con mansione non ancora definita 3,4%
Studentessa con tesina/tesi su sicurezza digitale 2,3%
Operatrice/responsabile in ambito help/service desk ICT 2,3%
In fase di stage presso un'azienda/ente 1,1%
Operatrice/responsabile gestione documentale 0,0%
Analista vulnerabilità e rischi ICT 0,0%
Operatrice/responsabile in ambito SOC, Security Operation Centre 0,0%
DPO, Data Protection Officer, e/o Responsabile privacy 0,0%
CTO, Chief Technology Officer 0,0%
CIO, Chief Information Officer 0,0%
CSO, Chief Security Officer 0,0%
CISO, Chief Information Security Officer 0,0%
Avvocato 0,0%
©AIPSI 2021
0% 5% 10% 15% 20% 25% 30%

Fig. 7-1

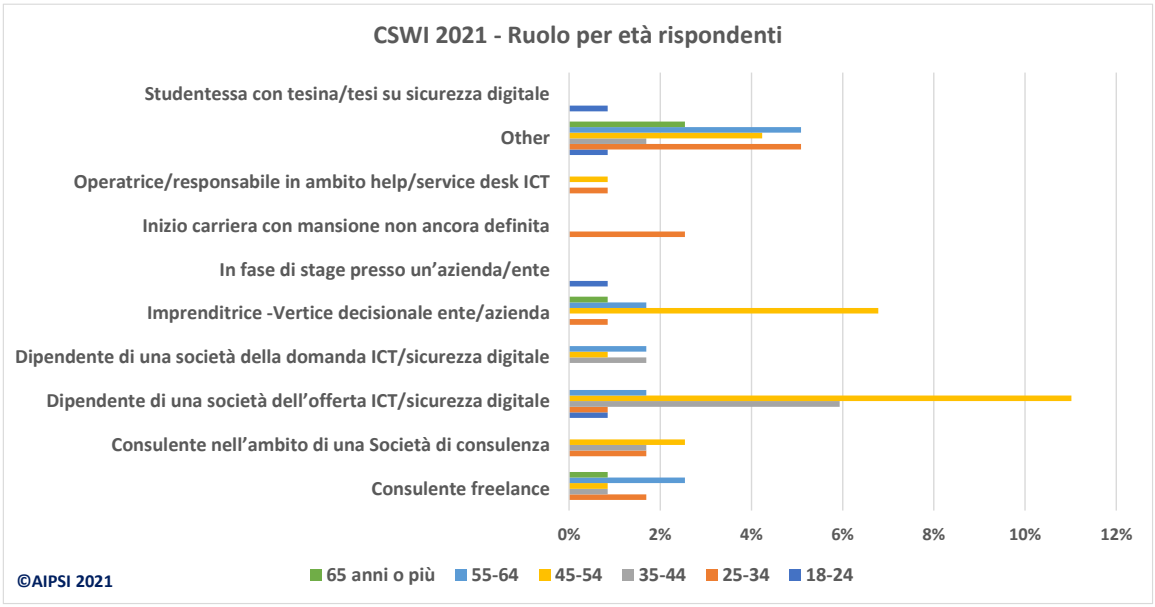

CSWI 2021 - Ruolo per età rispondenti
Studentessa con tesina/tesi su sicurezza digitale
Other
Operatrice/responsabile in ambito help/service desk ICT
Inizio carriera con mansione non ancora definita
In fase di stage presso un'azienda/ente
Imprenditrice -Vertice decisionale ente/azienda
Dipendente di una società della domanda ICT/sicurezza digitale
Dipendente di una società dell'offerta ICT/sicurezza digitale
Consulente nell'ambito di una Società di consulenza
Consulente freelance
0% 2% 4% 6% 8% 10% 12%
©AIPSI 2021
65 anni o più
55-64
45-54
35-44
25-34
18-24

Fig. 7-2

Fig. 7-3

Le attuali modalità operative delle rispondenti nel campo della sicurezza digitale sono sintetizzate nella fig. 7-4. Indipendentemente dal ruolo e dal tipo di lavoro, la metà esatta lavora a tempo pieno. Il 27,5% opera in maniera continua, ma solo a tempo parziale: la sicurezza digitale è un di cui tra le attività che svolge. Il termine "saltuariamente" ed "occasionalmente", spesso usati come sinonimi, hanno in questa indagine un preciso significato che è bene chiarire per evitare giustificati fraintendimenti. "Saltuariamente" sta ad indicare un lavoro che viene svolto ogni tanto, con una tempificazione varabile ma che è definita, ad esempio a livello contrattuale: la professionista lavora anche, non solo, nella sicurezza digitale, ma questa sua attività è periodica, ad esempio una volta alla settimana, al mese, etc. "Occasionalmente" significa che un lavoro inerente la sicurezza digitale potrebbe occorrere, ed ogni tanto avviene, ma è occasionale, non già previsto e schedulato/schedulabile: questa attività è svolta quando richiesta, ma le richieste non sono continue o periodiche.

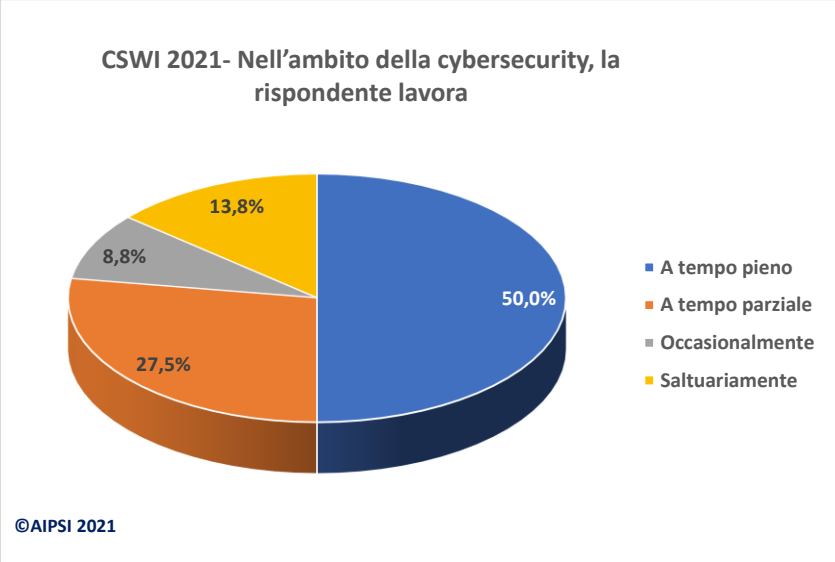


Fig. 7-4

Un aspetto assai importante nell'attività lavorativa è il poter ben conciliare le esigenze di tempo per l'attività professionale con quelle per la propria persona e per la propria famiglia. Questa conciliazione è

particolarmente critica per una donna, in qualsiasi tipo e ruolo lavorativo, e soprattutto per ruoli ad alta professionalità e/o dirigenziali. Conciliazione necessaria anche per le attività di sicurezza digitale, tema in rapida e continua evoluzione, e per il quale solo il 50% può operarvi a tempio pieno. L'altra metà delle professioniste deve condividere, e ben bilanciare, le attività di cybersecurity con altre attività lavorative.

La fig. 7-5 mostra che "solo" il 23,5% delle rispondenti, ha al momento problemi nel bilanciare e conciliare attività lavorativa e attività personale e per la famiglia.

Fig. 7-5

Considerando che questo problema è uno dei principali fattori del divario di genere, gli autori si aspettavano una percentuale maggiore. Le motivazioni per queste difficoltà non erano richieste in dettaglio nel questionario, ma era consentito di inserire libere indicazioni sulle difficoltà nel conciliare vita personale/domestica e vita lavorativa. Tale indicazioni sono sintetizzate nei seguenti punti:

- mancanza di un team di lavoro supportivo e collaborativo
- la disponibilità di tempo per seguire la famiglia, in particolare i figli e le loro attività scolastiche
- la difficoltà, in taluni casi l'impossibilità, di svolgere almeno alcune attività di cybersecurity da remoto (smart working)
- la frequente necessità di operare in trasferta, con tempi di lavoro che si dilatano restringendo fortemente quelli necessari per la famiglia ed i figli
- nel campo della cybersecurity c'è così tanto da fare e da studiare che le classiche 8 ore lavorative si devono per forza superare, spesso di molto
- sia lato domanda sia lato offerta cybersecurity, talvolta mancano gli adeguati moderni sistemi di automazione del controllo, monitoraggio e reportistica, con conseguente sovraccarico di lavoro manuale e spesso poco efficace
    - Continue richieste extra e disordinate da clienti e colleghi che ostacolano una pianificazione efficiente ed efficace con la conseguenza di gestire le attività in emergenza.
    - Ricoprire contemporaneamente il ruolo di coordinatore e quello operativo con la richiesta (implicita) di gestire entrambi come se fossero full time.

Data l'importanza delle risposte nell'ottica del "gap di genere", si è approfondita la loro analisi correlando le risposte avute in merito, correlandole con l'età delle rispondenti. La fig. 7-6 riporta tale correlazione ed

emerge, ed è un dato positivo, che le rispondenti "giovani", nella fascia 18-34 anni, per lo più non hanno problemi nel conciliare. E' abbastanza ovvio che questo avvenga anche per le professioniste oltre i 55 anni. Qualche problema al momento esiste, pur con le piccole percentuali complessive, nella fascia 35-54 anni.

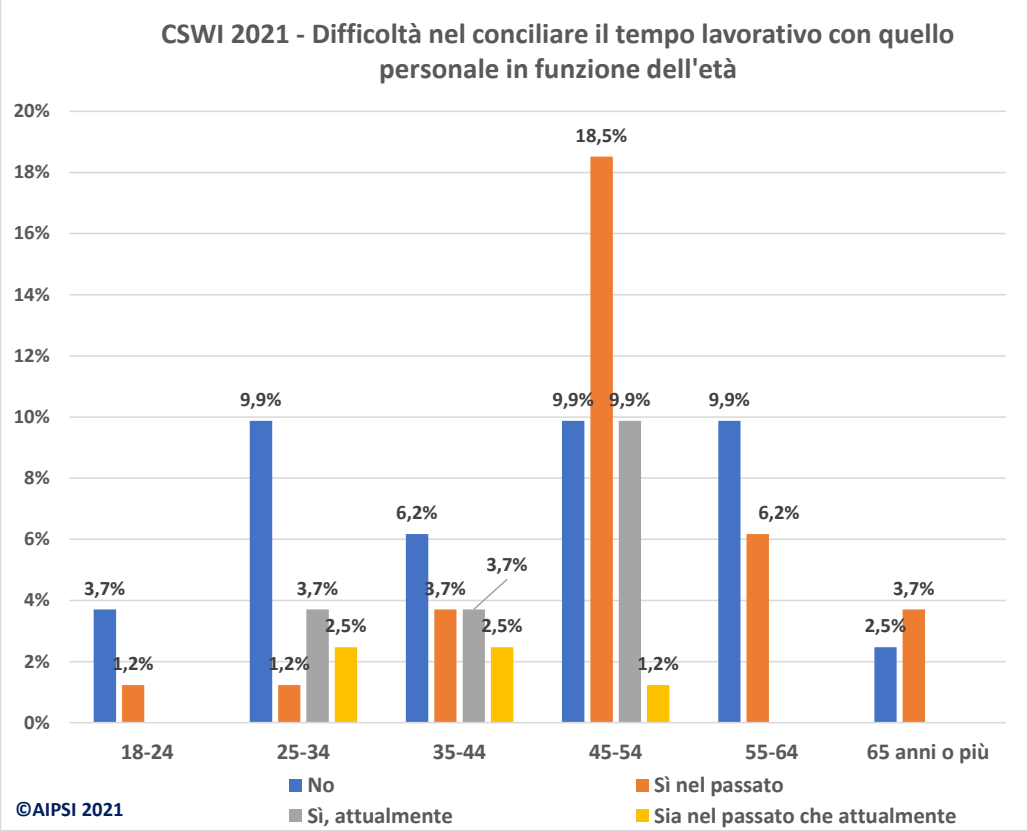


Fig. 7-6

Un fattore chiave del divario di genere, almeno nel contesto dell'indagine CSW 2021, è se essere donna, nell'ambito della cybersecurity, è ritenuto dalle rispondenti un fattore negativo oppure no. La fig. 7-7 mostra le risposte. Solo il 2,6% ritiene l'essere donna un aspetto favorevole per lavorare in questo campo. La maggioranza delle rispondenti, il 57,1%, ritiene che l'essere donna sia del tutto indifferente. Il 22,1% lo giudica un elemento sfavorevole, ed una percentuale di poco inferiore, dichiara di non essere in grado di valutarlo, sulla base della propria esperienza sul campo. Queste indicazioni, pur non avendo una valenza statistica da un campione rappresentativo della realtà femminile nel campo della sicurezza digitale in Italia, mostrano che la situazione nel nostro paese, in termini di gender gap, è abbastanza positiva, anche facendo riferimento alla più generale situazione dell'intero settore ICT nazionale dall'indagine WID europea, riportata nel Cap. 5.

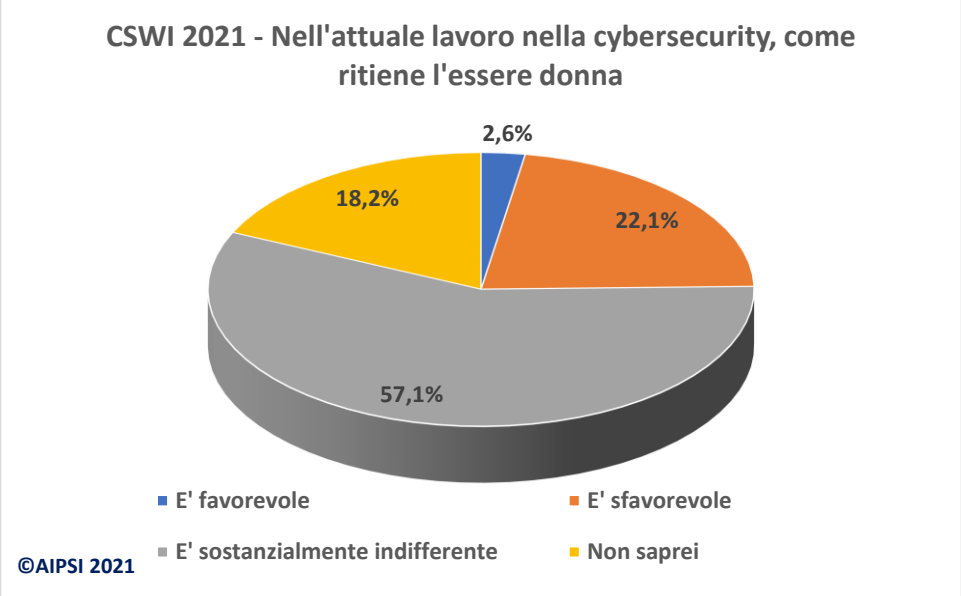


Fig. 7-7

Data l'importanza del fattore "donna", si è approfondita l'analisi correlando le risposte avute con la fascia di età: il risultato è nella fig. 7-8. La barra blu, che indica l'indifferenza, è in percentuale il primo in tutte le fasce d'età, a parte quella dei 35-44 anni, dove la percentuale più alta spetta a "mi sfavorisce". Tali indicazioni fanno riferimento al bacino di rispondenti liberamente emerso dall'indagine, e non ha nessuna pretesa di rappresentare statisticamente il mondo di chi si occupa di sicurezza digitale. Molte considerazioni possono derivare dalla fig. 7-8, e gli autori non intendono entrare in dettagli che sarebbero tutte delle ipotesi di fatto non verificabili. Ma come trend generale risulta logico che la fascia 35-44 sia quella che percentualmente più "soffre" nell'essere donna: è la fascia in cui la maggior parte delle donne è sposata, ha figli che vuole accudire, è ad un livello di maturità e di responsabilità professionale per le quale si attenderebbe dei riconoscimenti, di carriera o economici. Molto positivo, per gli autori, che nelle due fasce delle più giovani, dai 18 ai 34 anni, ci siano solo o una valutazione di indifferenza, o, ragionevolmente, un "non saprei".

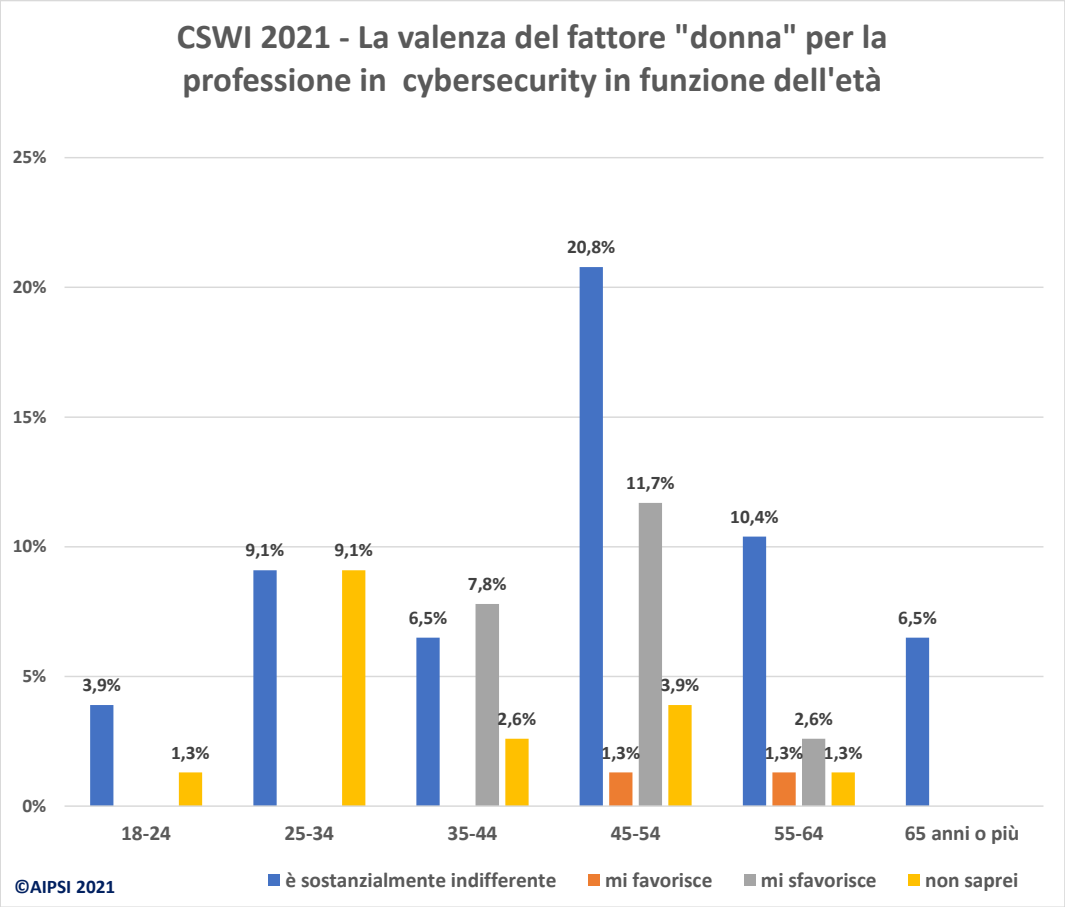


Fig. 7-8

Il terzo elemento basilare nel divario di genere è la **retribuzione**, e questo vale anche nel campo della sicurezza digitale, pur con la sua molteplicità e interdisciplinarietà. Infatti, come indicato nella fig. 7-9, il 34,2% delle rispondenti ritiene di essere remunerata meno dei colleghi uomini, a parità di fattori quali ruolo, responsabilità, anzianità lavorativa, competenze, etc., mentre solo il 3,9% reputa di essere pagata di più. Un quarto delle rispondenti ritiene di essere pagata sostanzialmente allo stesso modo degli uomini. Che la percentuale maggiore delle rispondenti, il 36,8 %, dichiari di non sapere se sia pagata più o meno rispetto a colleghi, è ragionevole. E' sempre difficile conoscere le retribuzioni, è un dato da sempre riservato; ed ancor più difficile è confrontare livelli retributivi a parità di ruolo, competenze ed età. Nel campo della sicurezza digitale, così articolato, trasversale e interdisciplinare, ove operano professioniste con competenze, ruoli e modalità così diversi, la difficoltà è ulteriormente aumentata data la conseguente forte variabilità retributiva. Il tipo di intervento in questo campo è sovente a progetto, con il coinvolgimento "a consumo" dei professionisti, tecnici o non, coinvolti.

L'indicazione delle rispondenti a CSWI 2021 comunque conferma che le donne tendono ad essere pagate meno degli uomini: una situazione comune a tutti i settori, ed anche a quello dell'informatica, così come inquadrato nel cap. 5. Di interessante riferimento generale per l'Italia i recenti dati ISTAT[7] sul gap salariale tra i due sessi nelle retribuzioni nelle aziende private: dall'ultima indagine ISTAT

[7] ISTAT, Istituto Nazionale di Statistica

(https://www.istat.it/it/archivio/194951) emerge, in generale e per ogni ambito lavorativo, che il differenziale retributivo delle donne rispetto agli uomini è negativo e pari al meno 12,2%. Lo svantaggio femminile aumenta al crescere delle retribuzioni orarie sia a livello territoriale che settoriale. All'aumentare del livello di istruzione cresce la retribuzione oraria per uomini e donne, ma cresce anche lo svantaggio retributivo per le donne. Per le posizioni con la laurea e oltre, la retribuzione oraria delle donne è di 16,1 euro contro 23,2 euro degli uomini; il differenziale è quindi pari a -30,6%.

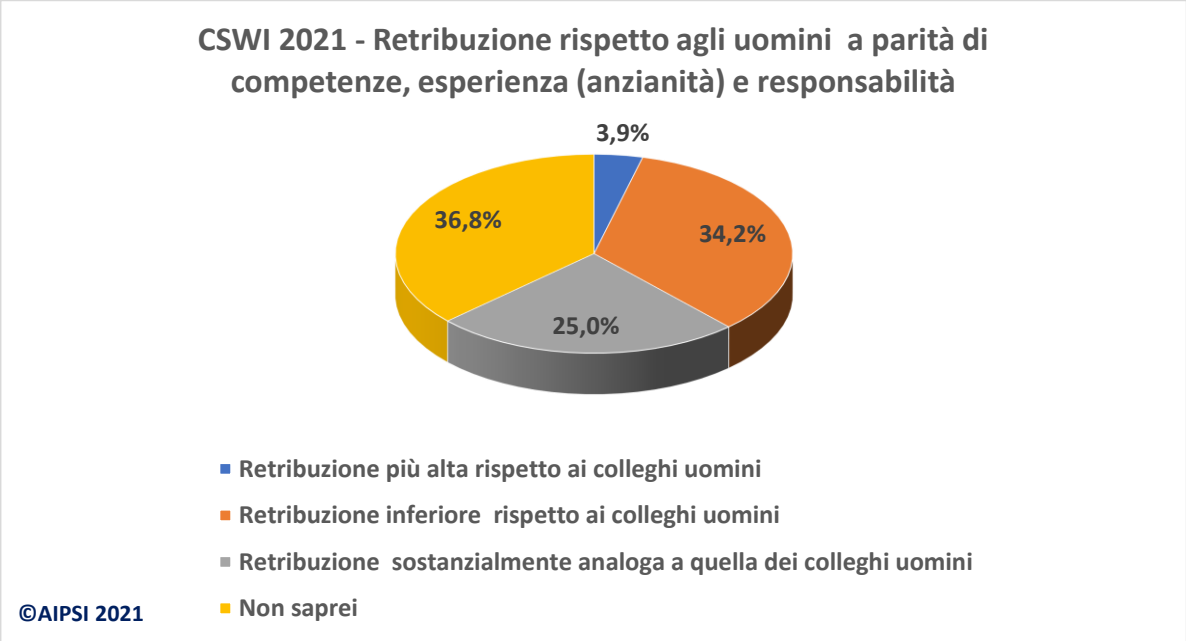
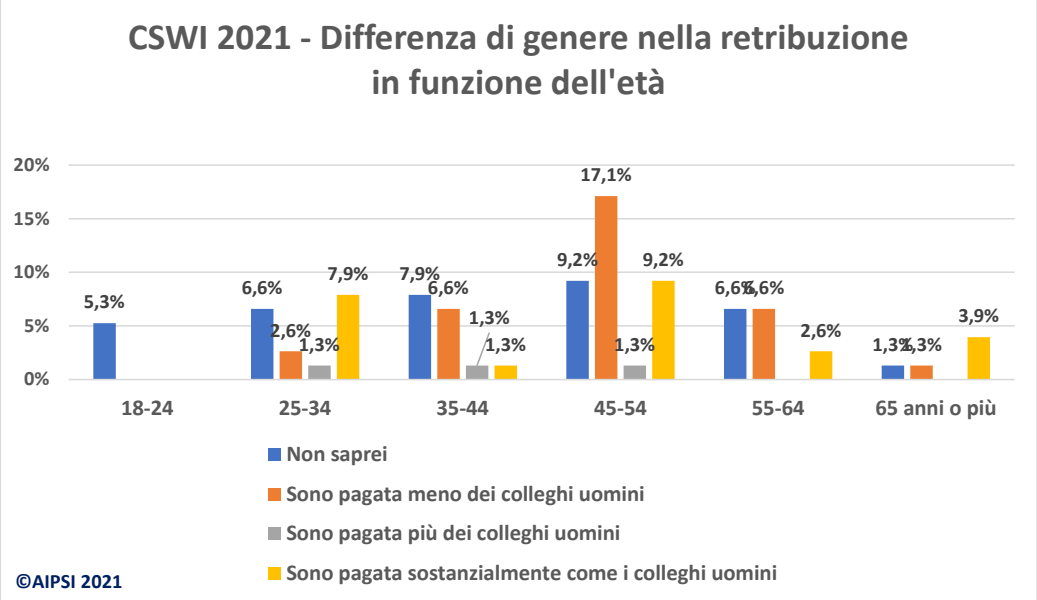


Fig. 7-9

Data l'importanza del tema, si è approfondita l'analisi correlando la retribuzione all'età, fig. 7-10, e al possedere, o no, la laurea, fig. 7.11. Entrambi gli approfondimenti confermano le indicazioni di massima sopra riportate. Interessante evidenziare come le percentuali delle professioniste che ritengono di essere pagate di più rispetto agli uomini si concentrano nelle fasce d'età tra 25 e 54 anni.



.

Fig. 7-10

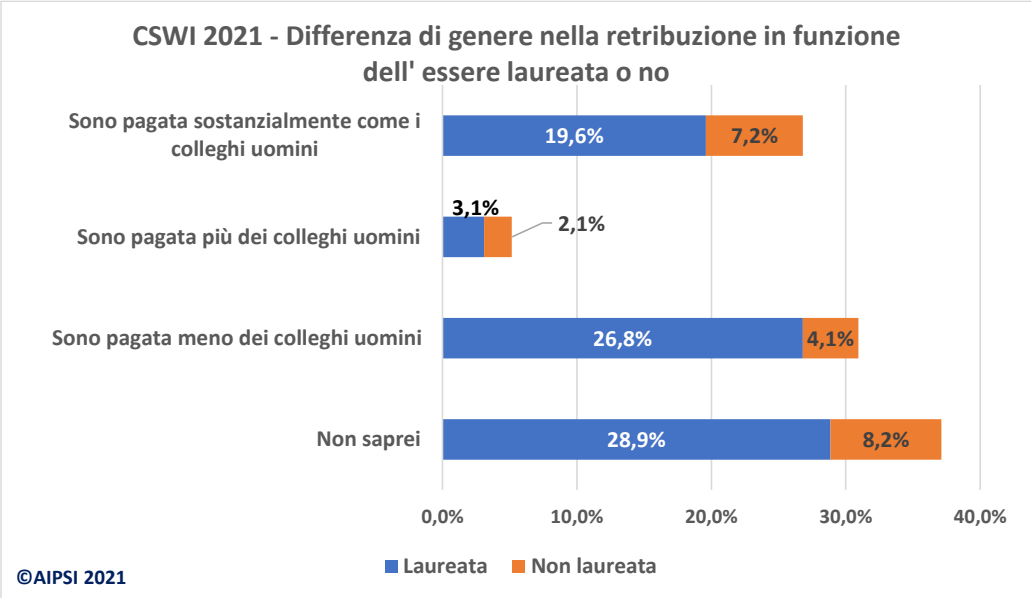


Fig. 7-11

7.1 ASPETTI POSITIVI E NEGATIVI NELLA PROPRIA ATTIVITÀ NELLA SICUREZZA DIGITALE

Al di là del conciliare il lavoro con la vita personale, analizzati con riferimento alle fig. 7-5 e 7-6, e agli aspetti economici della retribuzione analizzati con riferimento alle fig. 7-9, 7-10 e 7-11, la qualità del lavoro nel

campo della sicurezza digitale dipende da ulteriori elementi, che l'indagine CSWI 2021 ha cercato di fotografare.
In primo luogo si è chiesto quali sono gli elementi della cybersecurity che maggiormente "appassionano" e rendono interessante lavorare in questo campo. La fig. Fig. 7.1-1 mostra i risultati emersi.

Fig. 7.1-1

Il dato più significativo è che l'aspetto economico è all'ultimo posto: quasi tutte le rispondenti operano nella sicurezza digitale per l'interesse in questo campo, in continua evoluzione, innovativo, fortemente tecnologico e multidisciplinare: questi tre fattori si pongono percentualmente ai primi tre posti.
In "Altro" le rispondenti hanno indicato che in Italia sta crescendo significativamente il mercato della sicurezza digitale, anche a seguito della pandemia Covid-19 che di che colpo ha imposto un largo uso dei servizi in Internet ed il lavoro online da remoto (smart working).
La fig. Fig. 7.1-2 mostra quali sono gli aspetti positivi nell'attività che si svolge in ambito sicurezza digitale, e che di fatto riprendono quasi in toto i motivi per i quali questo campo "appassiona".

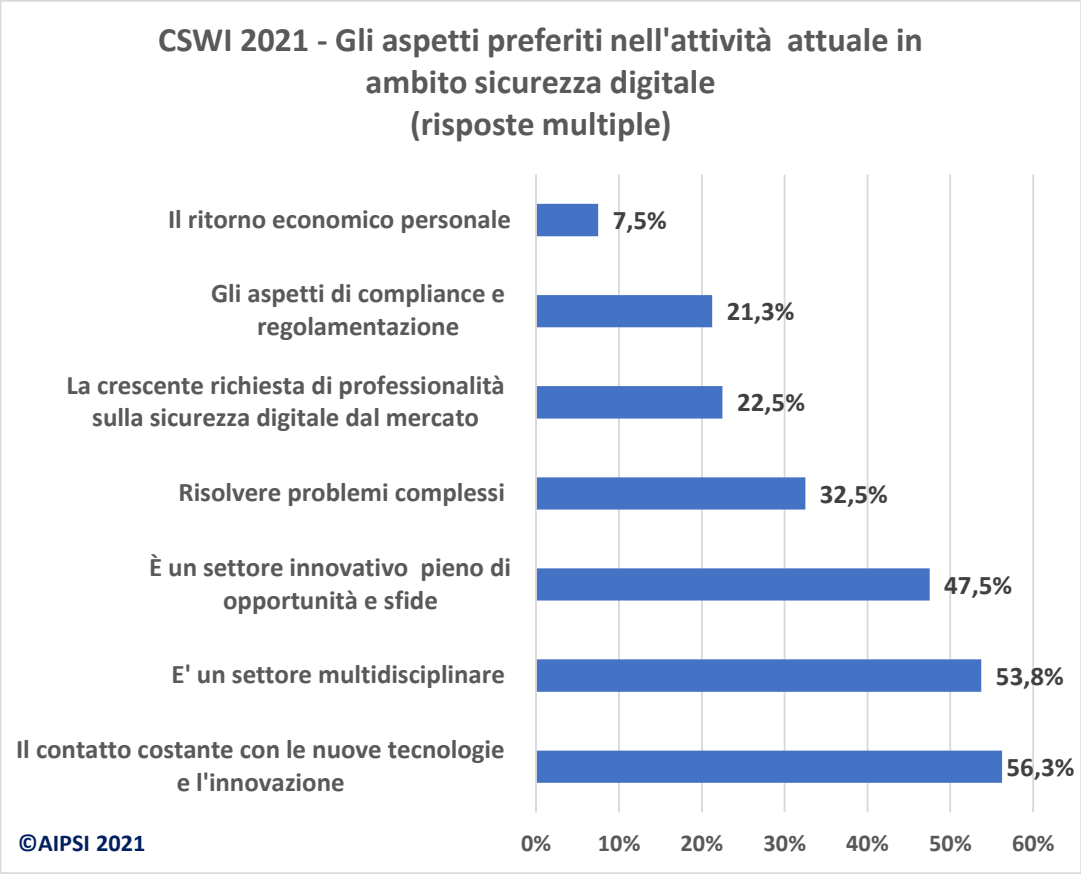


Fig. 7.1-2

Gli aspetti ritenuti positivi da più della metà delle rispondenti sono il contatto costante con le nuove tecnologie e la multidisciplinarità. Il progresso tecnologico e le innovazioni che ne possono derivare sono gli elementi preponderanti anche nel campo della cybersecurity. L'importanza della multidisciplinarietà evidenzia il prevalere dei così detti "soft skill", ossia di capacità di tipo personale, relazionale, comportamentale, comunicativo e di metodo, che differiscono dalle competenze e capacità tecniche legate a specifiche mansioni o ruoli. Il concetto di soft skill è generico e non univocamente definito. Rientrano in queste capacità, non facilmente misurabili e verificabili, ma essenziali, ad esempio il saper operare in gruppo, saper utilizzare il linguaggio più opportuno in funzione degli interlocutori, il saper organizzare il proprio lavoro e quello dei propri collaboratori, il capire quando entrare in dettagli e quando essere sintetici, il saper valutare i vari interlocutori, e così via.

Considerare un aspetto positivo il tema della compliance e della regolamentazione conferma l'importanza e l'interesse per la multidisciplinarietà, e si accorda anche percentualmente con quanto rilevato in merito alle certificazioni possedute dalle rispondenti (si veda fig. 6-4).

Alcune differenze tra l'aspetto interesse e aspetto positivo nella pratica lavorativa sono da segnalare:

- "risolvere problemi complessi", non solo di tipo tecnico, aumenta dal 23,8% di interesse al 32,5% nella pratica.
- l'aspetto della multidisciplinarietà aumenta di più di 6 punti percentuali. Nello svolgimento di

Gli aspetti negativi nel lavoro in ambito sicurezza digitale sono dovuti alle difficoltà che si hanno nello svolgerlo, e quanto indicato dalle rispondenti è mostrato nella fig. 7.1-3.

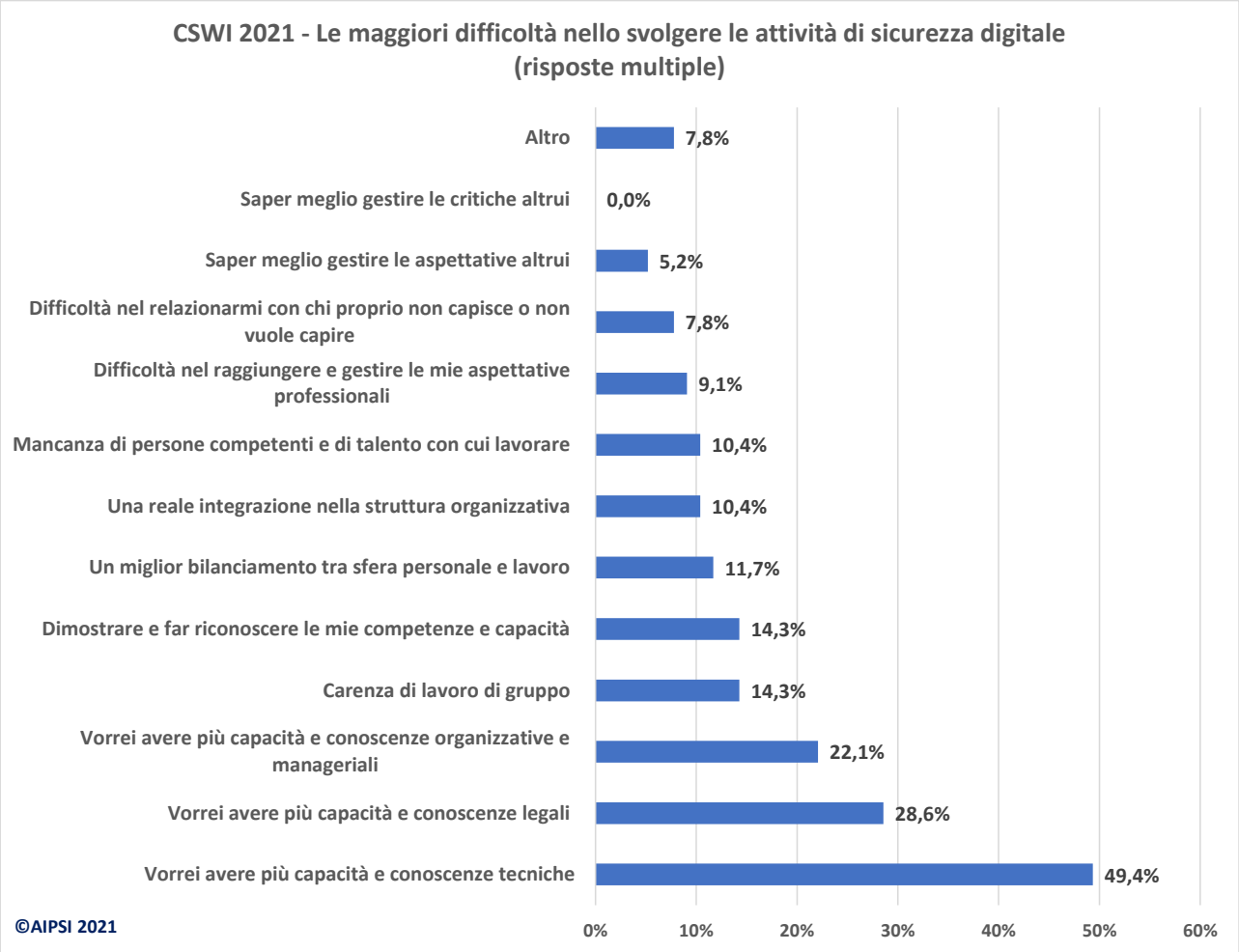


Fig. 7.1-3

Al primo posto si posiziona la necessità di avere maggiori competenze e conoscenza tecniche: una difficoltà personale, non del contesto, che evidenzia come quasi il 50% delle rispondenti senta fortemente il bisogno di perfezionarsi in primis sul lato tecnico, basilare per la sicurezza digitale in qualsiasi ruolo ed attività.
Al secondo posto, ma con una percentuale molto inferiore, la necessità di maggiori competenze nel campo legale e normativo, che fortemente ormai indirizza la sicurezza digitale: basta pensare al GDPR per la privacy.
Seguono poi vari temi tutti riguardanti aspetti organizzativi di competenze all'interno della struttura nella quale le rispondenti operano: in particolare mancanza di lavoro di gruppo e mancanza di colleghi ed interlocutori con le adeguate competenze per poter interoperare efficacemente. Quest'ultimo è un serio e grave problema sul quale da tempo AIPSI pone in guardia la domanda del settore: non solo mancano in assoluto degli specialisti sulla sicurezza digitale, ma questo vuoto è spesso impropriamente occupato da millantatori ed improvvisatori, che si spacciano per esperti, e causano seri guai ai clienti (la domanda) che sovente non hanno le minime competenze in materia per capire che quel tipo di offerta di fatto li sta truffando.

8. NEL PROSSIMO FUTURO

L'indagine CSWI ha voluto indagare sul prossimo futuro professionale delle rispondenti in termini di probabile loro futura evoluzione.
La prima domanda riguarda l'eventuale percorso di crescita previsto e percorribile, tipicamente delle strutture organizzative di maggiori dimensioni sia lato offerta sia lato domanda.
La fig. 8-1 mostra la sintesi delle risposte ricevute: la percentuale più alta è un "non so", molto ragionevole considerando che nella maggior parte di aziende ed enti pubblici ben difficilmente sono previsti percorsi di carriera per ruoli e competenze di nicchia quali quelli relativi alla cybersecurity. Una visione di maggior dettaglio, e quindi più chiara, e data dalla fig. 8-2 che pone in correlazione l'esistenza di percorsi di carriera per la cybersecurity rispetto al tipo di azienda/ente. Dalla figure emerge chiaramente che nelle aziende dell'offerta è prevalente, in percentuale, l'esistenza di percorsi di carriera predefiniti e pianificati (si veda la barra arancione). Nelle aziende dell'offerta prevale invece la mancanza di tali percorsi, così come nella voce "Altro" che include prevalentemente le Pubbliche Amministrazioni, Centrali e Locali, escluse le Università, i Centri di Ricerca e le scuole secondarie, che hanno specifiche voci.

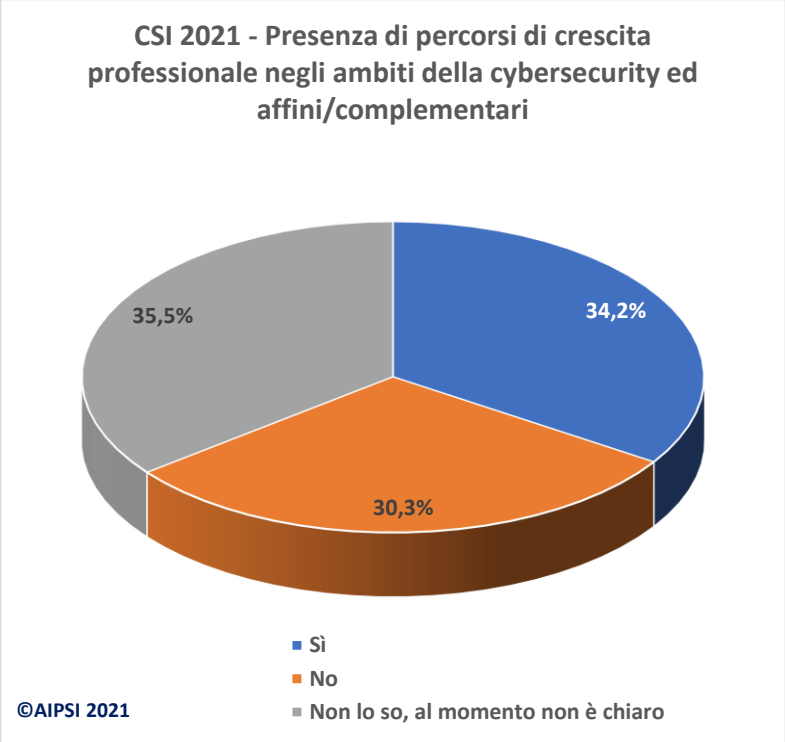


Fig. 8-1

La fig. 8-3 sintetizza le previsioni e le attese nel prossimo futuro delle rispondenti e costituisce il cuore di questo intero capitolo. La domanda nel questionario era a risposta singola, la rispondente doveva scegliere solo una delle risposte pre-definite.
La maggior parte delle rispondenti intende continuare e crescere, specializzandosi nel campo del sicurezza digitale.

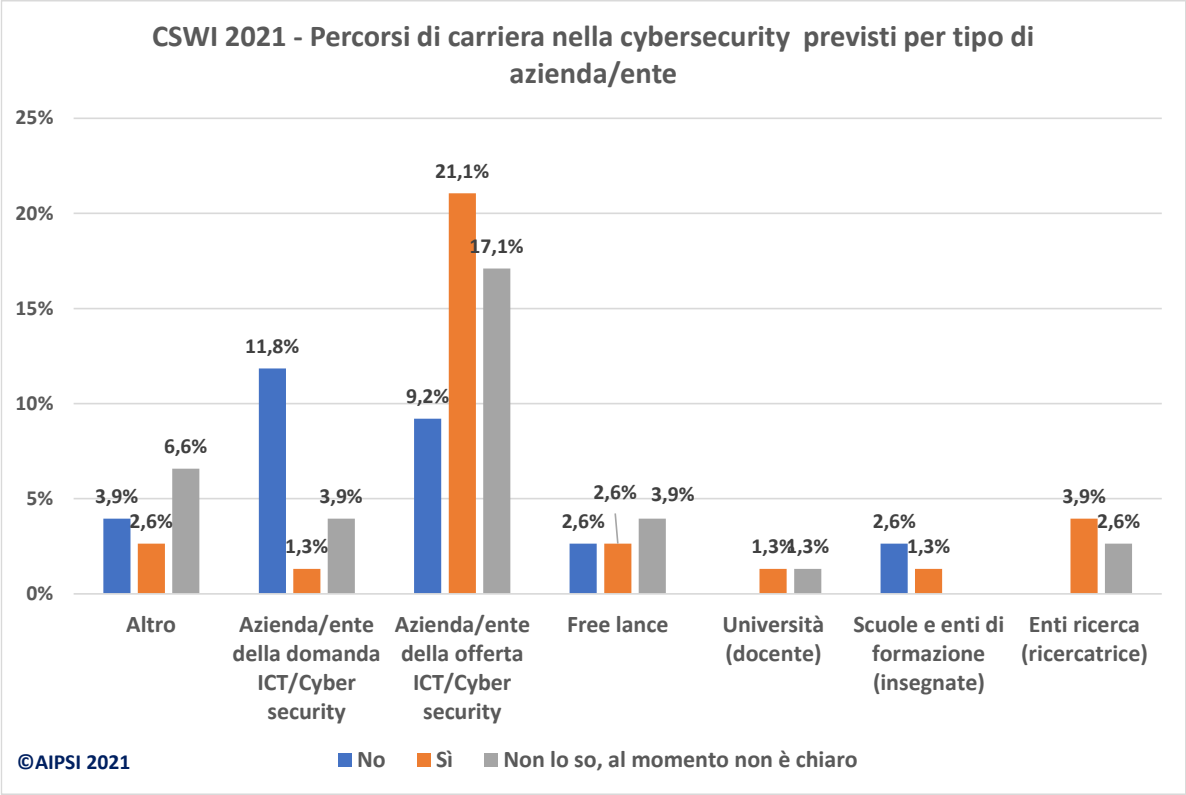


Fig. 8-2

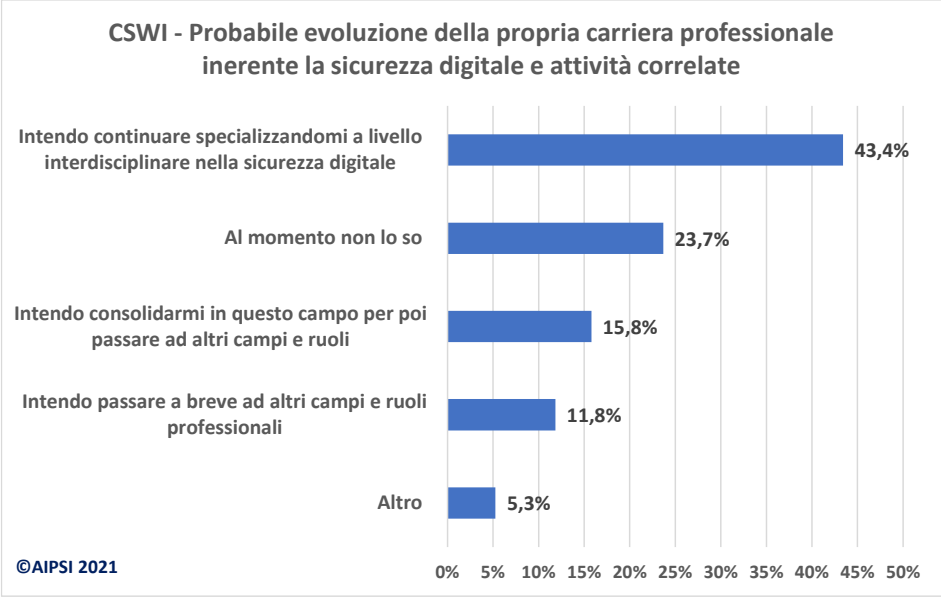


Fig. 8 -3

Per meglio analizzare queste scelte/previsioni per il futuro, esse sono state correlate con il tipo di azienda/ente presso cui la rispondente opera, ed il risultato è mostrato nella fig. 8-4.

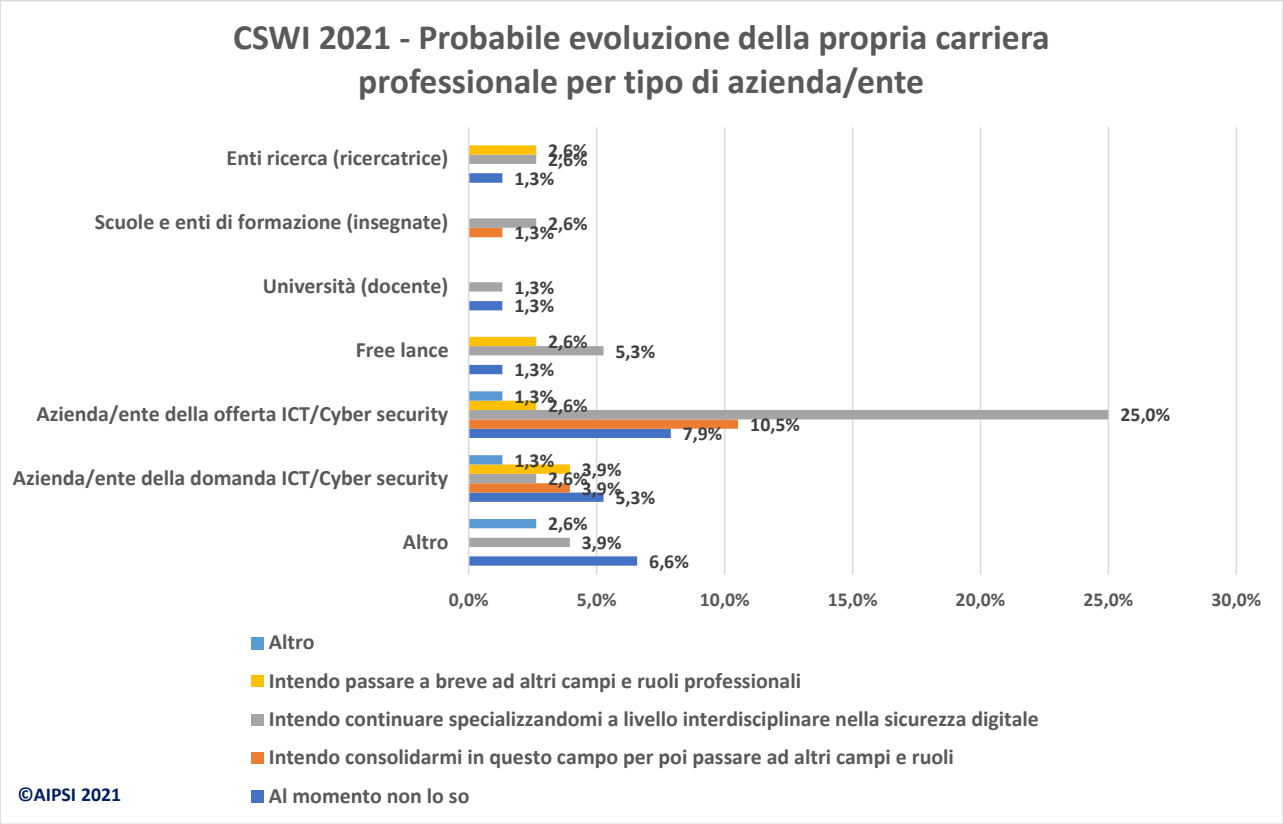


Fig. 8 -4

L'intenzione di specializzarsi, che è percentualmente la primaria, nella fig. 8-4 è evidenziata con la barra grigia: essa è nettamente prevalente lato offerta, per le free lance e per le insegnanti/docenti.
L'intenzione invece crescere e passare ad altri campi e ruoli, abbandonando quindi l'ambito della sicurezza digitale, è considerando da più di un quarto delle rispondenti (27,6%): l'8,11% lo vorrebbe a breve, il 15,8% dopo essersi ulteriormente consolidata nella posizione, quindi più a medio termine. Quest'ultima intenzione è per personale che opera in aziende della domanda e dell'offerta. L'uscita a breve è indicata, oltre che per le aziende della domanda e dell'offerta, anche dalle freelance, probabilmente stanche della continua battaglia che questo campo richiede (con una difficile adeguata remunerazione di questo sforzo) e dalle ricercatrici.

Il termine "Altro" fa riferimento a imprenditrici e responsabili (Amministratrice delegata, Direttrice Genarle, etc.) che sono già al vertice della possibile carriera almeno per l'ambito sicurezza digitale. Qualcuna intende cambiare il target del suo business, ed intraprendere diverse strade, data la crescente competitività e quasi saturazione dell'offerta nel mercato italiano della sicurezza digitale.
Tali tendenze ed aspettative sono confermate dalle indicazioni inserite liberamente in questa parte del questionario. Gli obiettivi ed i desiderata si riassumono in una crescita nella stessa azienda/ente, in posizioni di maggior responsabilità e potere (anche andando a sostituire il proprio attuale capo), o in una diversa azienda/ente, che però consentano un corretto bilanciamento dei tempi lavoro-casa e che investano nelle proprie risorse umane. I termini "più competenti" e "manager" ricorrono spesso nelle risposte libere fornite, così come "crescita", "acquisizione di competenze" e "responsabile", denotando una forte tensione al cogliere le opportunità di un settore in crescita come la sicurezza digitale, e una sicura determinazione nel mettere a frutto le proprie capacità al meglio.

9. ALLEGATI

ANDREA BOZZETTI

Andrea opera dal 2017 in **Malabo srl** a tempo parziale come Assistente del CEO nell'area contabilità e marketing, come web manager e SEO del sito www.malaboadvisoring.it, ed è coinvolto in alcuni progetti e iniziative quali l'indagine OAD, Osservatorio Attacchi Digitali in Italia, e l'indagine AIPSI CSWI sul lavoro femminile nella sicurezza digitale in Italia.

In parallelo all'attività con Malabo, dal 2021 opera con **Multivendor Service Srl,** per **c**oordinare e monitorare le attività di supply chain IT per conto del Comune di Milano, garantendo un elevato livello di efficienza e un approccio integrato nella fornitura dei servizi digitali richiesti dai clienti finali.

Precedenti impegni lavorativi includono:

- 2018-2020: attività a tempo parziale presso **Cooperativa FEMA-Milano** in qualità di "Head Steward" per coordinare e gestire un gruppo di 10 persone operanti come steward in vari importanti eventi in Milano.
- 2018-2019: attività a tempo parziale presso **Istituto Piepoli,** istituto indipendente di ricerche di mercato per:
    - sondaggi per aziende private di vendita al dettaglio, con analisi delle informazioni raccolte per comprendere il livello di soddisfazione degli intervistati rispetto all'oggetto del sondaggio
    - indagine di mercato per Ferrero per identificare il prezzo ottimale per il lancio di alcuni nuovi prodotti.

Andrea ha acquisito ad aprile 2020 la **Laurea Magistrale** in Relazioni Europee Internazionali alla **Università Cattolica del Sacro Cuore di Milano**, con una tesi su "*Evolution of Domestic Jurisdiction Notion on the basis of Security Council Procedure"*, dopo la **Laurea Triennale**, ottenuta a marzo 2018, in Scienze politiche economiche e sociali presso **l'Università Statale degli Studi di Milano** con una tesi su *"Circulation of Semipresidential Government's Form in Serbia and Montenegro"*. Presso questa Università ha guidato un gruppo di 5 studenti in un progetto di "Sustainable Development Economics" intitolato "Keasong Industrial Complex: A Free Economic Zone between South Korea and North Korea".

MARCO R. A. BOZZETTI

Marco Rodolfo Alessandro Bozzetti, ingegnere elettronico laureato al Politecnico di Milano, è fondatore e amministratore di Malabo S.r.l (www.malaboadvisoring.it), società di consulenza direzionale sull'ICT (Information and Communication Technology) creata nel 2001. Attraverso Malabo, Marco ha condotto e conduce interventi consulenziali presso Aziende ed Enti lato sia offerta sia domanda ICT. Marco ha operato con responsabilità crescenti presso primarie imprese di produzione, quali Olivetti ed Italtel, e di consulenza, quali Arthur Andersen Management Consultant e GEA/GEALAB, oltre ad essere stato il primo responsabile dei sistemi informativi dell'intero Gruppo ENI a livello mondiale (1995-2000). In tale posizione ha realizzato la terziarizzazione delle infrastrutture ICT dell'intero Gruppo (più di 22 Data Center) e della rete di comunicazione italiana in fibra ottica: a quella data una delle più grandi terziarizzazioni in Italia e in Europa. Agli inizi della sua carriera, in ambito Olivetti e del CREI del Politecnico di Milano, è stato uno dei primi ricercatori a livello mondiale ad occuparsi di internetworking, a partire dalla sua tesi di laurea.
A livello consulenziale innumerevoli gli interventi tecnici-organizzativi sui sistemi informatici di medie e grandi Aziende private, oltre che di alcuni Enti pubblici. aventi il principale obiettivo di allineare l'ICT al business, di innovarlo e di generare valore effettivamente misurabile.
I principali campi di intervento includono la governance ICT, la sicurezza digitale, l'analisi e gestione dei rischi ICT e dei loro impatti (BIA), il disegno di architetture ICT, la razionalizzazione e la gestione del sistema informatico, la definizione ed il supporto di strategie ICT, l'assessment delle tecnologie, delle competenze e dei ruoli ICT, l'analisi del valore per l'ICT, l'innovazione tramite l'ICT, la riorganizzazione di strutture e processi, il supporto per la compliance alle varie normative, in particolare alla privacy e al suo recente regolamento europeo GDPR (General Data Protection Regulation).
Dal 2009 Marco, in collaborazione con Malabo, AIPSI, Polizia Postale ed altri Enti ed associazioni, ha ideato e realizza OAD, Osservatorio Attacchi Digitali in Italia: è un'indagine via web, totalmente anonima e rivolta a tutti i settori merceologici, Pubbliche Amministrazioni incluse, che produce annualmente uno o più Rapporti sul fenomeno degli attacchi digitali intenzionali in Italia.

Marco è stato Presidente e Vicepresidente di FidaInform, di SicurForum in FTI e del ClubTI di Milano, oltre che componente del Consiglio del Terziario Innovativo di Assolombarda.
È attualmente Presidente di AIPSI, Associazione Italiana Professionisti Sicurezza Informatica e Capitolo Italiana della mondiale ISSA, e nel Consiglio Direttivo di FIDAInform, socio fondatore e componente del Comitato Scientifico dell'FTI, socio e revisore dei conti del ClubTI di Milano.
È certificato ITIL v3 ed EUCIP Professional Certificate "Security Adviser". È Commissario d'Esame in AICA per le certificazioni eCFPlus (EN 16234-UNI 11506).
Ha pubblicato articoli e libri sull'evoluzione tecnologica, la sicurezza digitale, gli scenari e gli impatti dell'ICT.

LAURA RIVELLA

Laureata in Scienze Internazionali e Istituzioni Europee presso il dipartimento di Scienze Politiche dell'Università Statale di Milano si è successivamente trasferita nel Regno Unito per affrontare il primo Master in Security Studies presso l'Aberystwyth University.

Dopo aver iniziato una carriera come Intelligence Analyst presso un'azienda di consulenza, ha deciso di intraprendere un ulteriore Master in Cybersecurity presso la University of Essex.

Nel suo attuale ruolo di Intelligence Analyst si occupa principalmente di gestire tutti il network di informazioni e intelligence interno all'azienda, di Compliance, OSINT (Open Source Intelligence) e Data Science.

L'Università dell'Essex ha chiesto la sua collaborazione per un progetto di ricerca e pubblicazione volto ad indagare il Risk Management della Sicurezza in Cloud, in particolar modo la sua evoluzione negli ultimi cinque anni.

Ha coordinato come Cosigliere AIPSI l'edizione 2021 del rapporto CSWI sul lavoro femminile in Italia nel campo della sicurezza informatica.

E' socia di AIPSI-ISSA, IEEE e BCS.

AIPSI

AIPSI, **Associazione Italiana Professionisti Sicurezza Informatica,** è la libera associazione no-profit, che raduna a livello individuale chi è interessato professionalmente alla sicurezza informatica, in qualsiasi ruolo e modalità, sia dipendenti sia autonomi, sia lato domanda sia lato offerta. Le Aziende/Enti non possono associarsi, ma possono sponsorizzare sue specifiche iniziative. AIPSI è il capitolo italiano di **ISSA, Information System Security Association**, la più grande organizzazione analoga a livello mondiale, che conta complessivamente oltre 13.000 soci. Il Socio AIPSI è contemporaneamente anche Socio ISSA.
Gli obiettivi principali di AIPSI sono:

- aiutare i propri Soci nella **loro crescita professionale e delle loro competenze**,
- **diffondere la cultura della sicurezza digitale** non ai soli propri Soci ma anche a tutto il pubblico**.**

Entrambi questi obiettivi sono ottenuti tramite la realizzazione ed erogazione di eventi, servizi ed opportunità, a livello nazionale ed internazionale, di elevata qualità. Il sito web di AIPSI (https://www.aipsi.org) e quello di ISSA (https://www.issa.org/) sono i due principali strumenti di interfaccia e di comunicazione coi Soci e con il pubblico anche istituzionale. Data la distribuzione di tutti i Soci, ma anche degli interessati alla cybersecurity, sull'intero territorio nazionale, da tempo ormai la quasi totalità degli eventi è online, sovente in collaborazione con altre associazioni, enti pubblici e di ricerca, aziende. AIPSI è inoltre socia di FidaInform, la Federazione italiana di varie associazioni a livello regionale come i ClubTI (https://fidainform.it/)

AIPSI ha realizzato, e sta realizzando, specifiche iniziative a livello italiano, che si affiancano a quelle erogate a livello internazionale da ISSA, e che includono l'autorevole rivista mensile **ISSA Journal**, webinar, facilitazioni per corsi e certificazioni, le opportunità di essere in una rete internazionale di professionisti, la possibilità di partecipare agli Special Interest Group, SIG, gruppi di lavoro specialistici su temi specifici: alla data sono attivi i SIG "Women in Security" e "Cyber Resilience".
Le iniziative AIPSI sono suddivise in due gruppi: quelle riservate ai soli Soci e quelle aperte a tutti gli interessati, Soci e non.
Come visibile in dettaglio sul sito web, le **iniziative AIPSI aperte a tutti** includono i **webinar** di approfondimento e discussione di temi inerenti la cybersecurity dal punto di vista tecnico, organizzativo e normativo/legislativo, la Newsletter mensile, l'iniziativa **AIPSI Giovani** per coinvolgere i giovani interessati alla cybersecurity (https://www.aipsi.org/aree-tematiche/aipsi-giovani.html), e **due indagini**:

- **OAD**, **Osservatorio Attacchi Digitali in Italia**, per il quale è stato realizzato un sito ad hoc, https://www.oadweb.it/, quale punto di riferimento e repository di tutti i rapporti annualmente pubblicati e di tutta la documentazione, ultimamente anche i videostreaming, degli eventi tenuti per presentare e discutere i dati emersi dalle indagini.
- **CSWI, Cyber Security Women's Italy**, sul lavoro femminile nella cybersecurity in Italia.

Le **iniziative AIPSI riservate ai soli Soci** includono

- Il **supporto**, anche con specifiche **mentorship** tra soci, alla **crescita professionale individuale** secondo l'impostazione ISSA **CSCL, Cyber Security Carrier Lifecycle**, contestualizzata alla realtà italiana/europea (per approfondimenti: https://www.aipsi.org/aree-tematiche/crescita-e-percorsi-professionali.html);
- Il supporto ed un significativo sconto per la **certificazione eCF (**UNI EN 16234-1:2016) per le figure di Security Manager e Security Specialist tramite AICA, accreditata Accredia;
- La possibilità di **partecipare**, per conto di AIPSI-ISSA, ad eventi e a tavoli istituzionali e **pubblicare articoli**, anche in collaborazione di altri Soci, su varie riviste, incluso il prestigioso ISSA Journal;
- I **Gruppi di Lavoro specialistici SIG** per l'approfondimento di tematiche di prevalente interesse dei Soci. Alla data sono attivi i seguenti SIG, ciascuno coordinato da un Consigliere AIPSI esperto del tema:
    - **L'uso dell'Intelligenza Artificiale in ambito sicurezza digitale** per strumenti di sicurezza, di gestione, di analisi vulnerabilità e rischi, etc.;
    - **Nuove logiche ed architetture per la sicurezza digitale,** che includono ad esempio Zero Trust, SASE, SOAR, etc.;

- **Crescita e percorsi professionali per la sicurezza digitale**, con riferimento a CSCL, certificazioni individuali, corsi, mentosrhip tra Soci. In questo ambito iniziano ad essere importanti anche in Italia le **onorificenze ISSA** per i meriti acquisiti professionalmente e nella vita dell'associazione, meriti che devono essere tutti documentati e valutati da apposite commissioni AIPSI ed ISSA.

Le caratteristche principali che differenziano AIPSI-ISSA da altre associazioni nazionali sulla sicurezza digitale includono:

- l'etica professionale dei suoi Soci (devono tutti firmare il codice etico ISSA, ed attenersi ad esso), in particolare di quelli che rivestono cariche nell'organizzazione: AIPSI (come ISSA) è no profit, con Soci solo persone fisiche e tutti operano su base strettamente di "volontariato": nessuno difende, o può difendere, interessi economici e fornitori, anche se questi sponsorizzano specifiche iniziative di AIPSI;
- la conseguente reale indipendenza di AIPSI da qualsiasi fornitore ed ente anche pubblico e regolatore. Grazie all'esperienza e alla disponibilità professionale dei suoi Soci più attivi, e all'interazione/collaborazione con altri Capitoli ISSA ed esperti, AIPSI è in grado di valutare e di confrontare soluzioni e proposte, anche normative e di legge, e di fornire costruttivi suggerimenti, come nel caso di pubblicazione di propri "White Paper" su temi "caldi" e dibattuti;
- la qualità dei propri interventi e delle proprie iniziative, effettiva e riconosciuta dal pubblico di interessati che ci segue. Qualità che deriva dalla capacità, esperienza, disponibilità ed etica dei Soci coinvolti e dalla capacità di collaborare con esperti dei fornitori, delle università e centri di ricerca , anche a livello internazionale. AIPSI, con le diverse iniziative sopra elencate, intende effettuare un effettivo trasferimento di conoscenza sulla multidisciplinare sicurezza digitale, e non solo ai propri Soci, fotografando e presentando il più aggiornato lo stato dell'arte della tecnologia e della normativa, ed illustrare e discutere innovazioni e trend tecnici e di mercato. Nessun intervento dei fornitori può essere solo commerciale: l'intervento è controllato a priori nei contenuti, che devono essere corretti e chiari, e, se possibile, con illustrazione di reali casi d'uso da parte di clienti.
- la focalizzazione sui temi più caldi e di maggior interesse per i Soci, grazie a periodici incontri ed indagini. Considerate anche le limitate risorse a disposizione ed i limiti intrinseci del "volontariato" perché sia di qualità, AIPSI preferisce effettuare un numero limitato di iniziative, ma di qualità;
- l'internazionalità che consente di avere contatti e di coinvolgere esperti dei vari Capitoli nazionali: come capitolo italiano, AIPSI ed i suoi Soci hanno quindi, o possono avere, visibilità ed interazioni-collaborazioni a livello mondiale. AIPSI rende quindi possibile ai suoi Soci di interagire e collaborare con esperti di cybersecurity di vari paesi: un potenziale di grande crescita non solo professionale ma anche di business.

aipsi

ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA