

EVENTO FINALE DI PRESENTAZIONE
DEI RISULTATI DEL MICROPROGETTO

{WE|CO|RE}

WomEn COoperating for cybeRsEcurity

Giovedì **22 Gennaio** 2026
Ore **16:00 - 18:00**

Castello di Lucento
Via Pianezza n. 123 - 10151 - Torino

Interverranno:

Ore 16:00
Dott. Luca Sanlorenzo
Direttore Generale di API Torino

Saluti Istituzionali di API

Ore 16:15

Assessore alla Legalità e Sicurezza della Città Metropolitana di Torino **Marco Porcedda**

Saluti Istituzionali

Ore 16:45

Dott.ssa Maria Luigia Ghiggia
CEO AMIS S.R.L. e Presidente di API Donna

Saluti Istituzionali API ; Risultati raggiunti con il Programma **WE.CO.RE. 2025** e prospettive future

Ore 17:20
Dott.ssa Gabriella Mattio
Referente Corsi e Aziende di Alliance Française Torino

17:50
Conclusioni e Chiusura

Saluti Istituzionali e ruolo strategico di Alliance Française nei rapporti bilaterali Italia Francia

Introduce, Modera e Conclude:
Dott.ssa Annalisa Cacciopoli
Project Manager e Communication Strategist nell'ambito del Microprogetto WE.CO.RE. WomEn COoperating for cybeRsEcurity

Interreg
France – Italia ALCOTRA

Partner

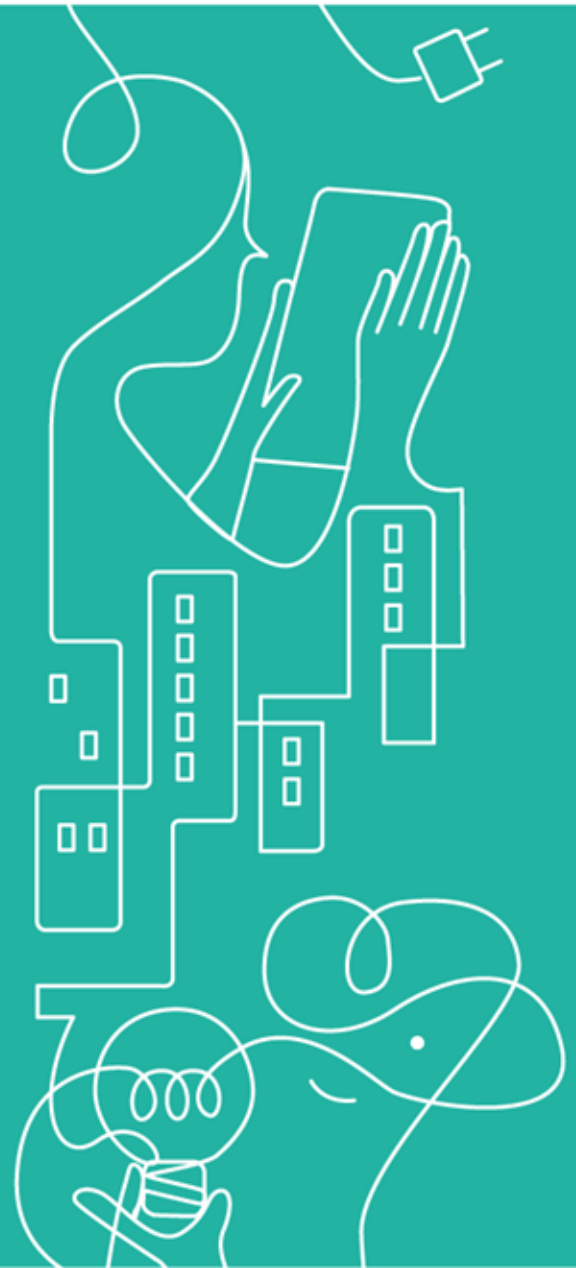
Introduzione

Dott.ssa Annalisa Caccioppoli

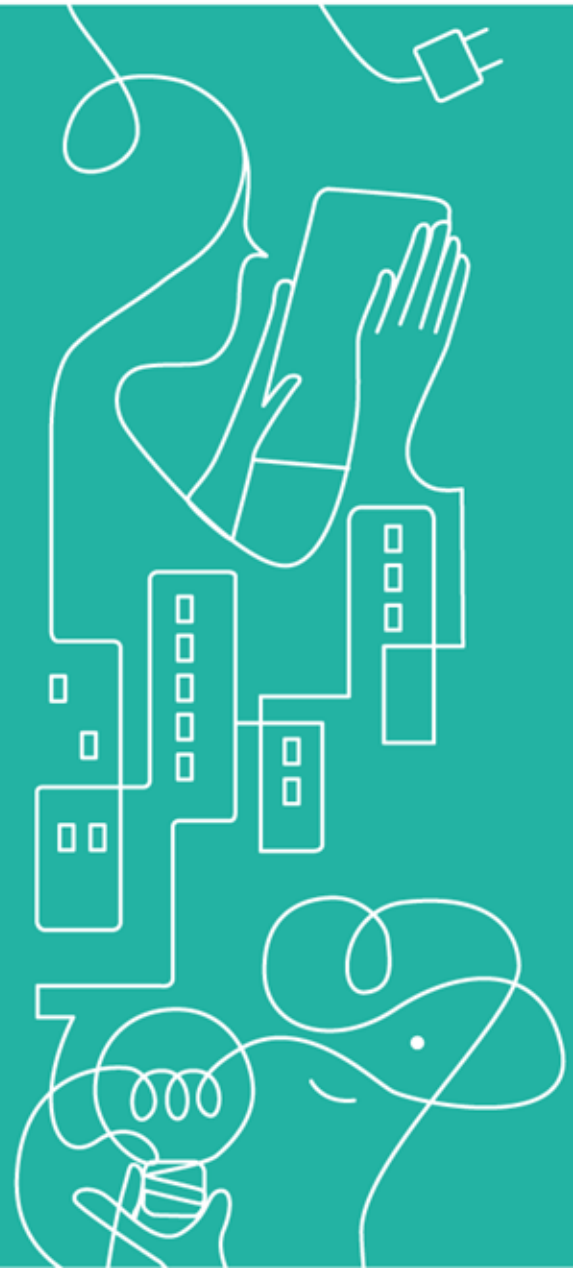
Project Manager - Communication Strategist

Microprogetto WE.CO.RE.

WomEn Cooperating for cybeRsEcurity



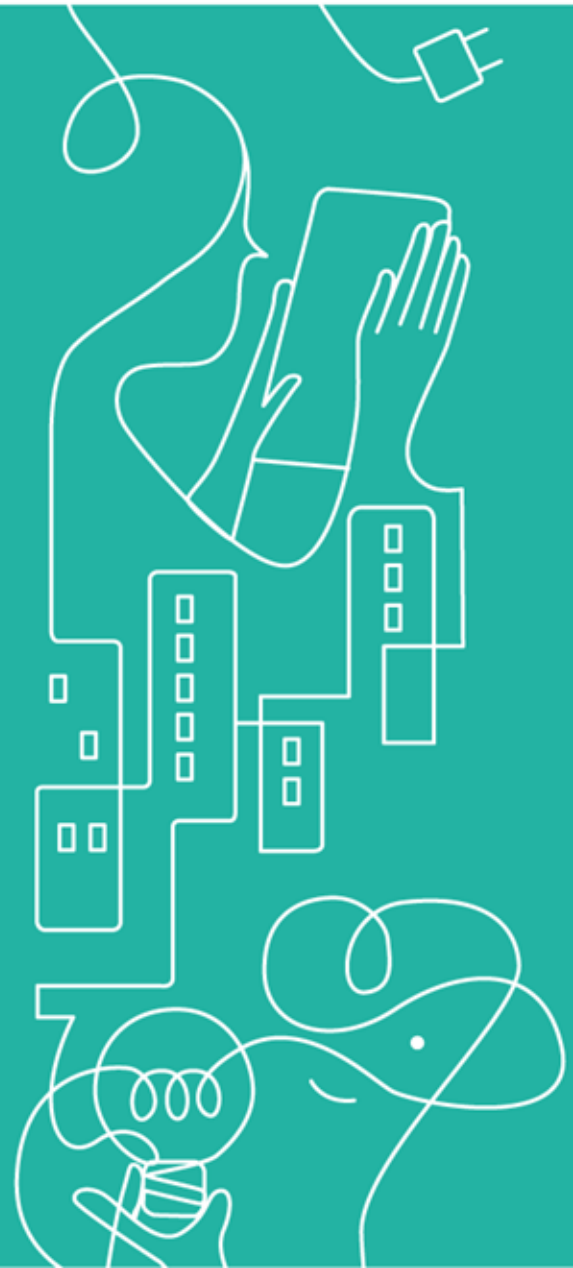
1. ROADMAP DEL MICROPROGETTO WE.CO.RE.;
2. ECOSISTEMA STRUTTURATO DI COOPERAZIONE TRANSFRONTALIERA PER LA SICUREZZA DELLE INFRASTRUTTURE DI RETE;
3. FORMAZIONE E CONSULENZA (CYBERSECURITY TRANSITION PLAN) GRATUITE



Saluti Istituzionali di API Torino

Dott. Luca Sanlorenzo

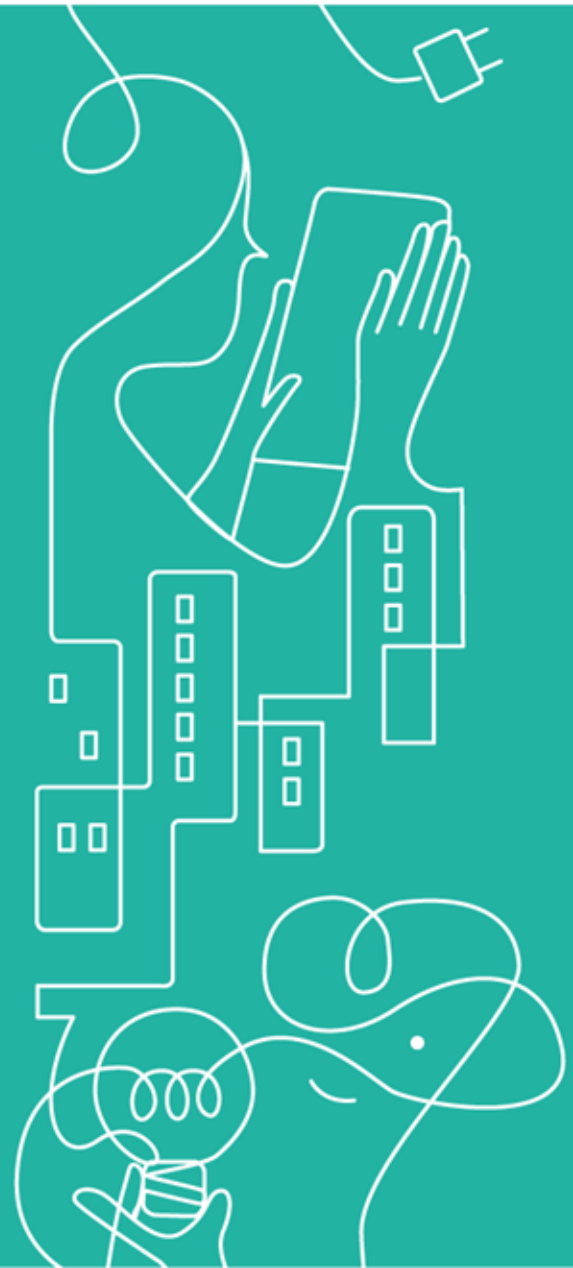
Direttore Generale di API Torino



Saluti Istituzionali della Città Metropolitana di Torino

Dott. Marco Porcedda

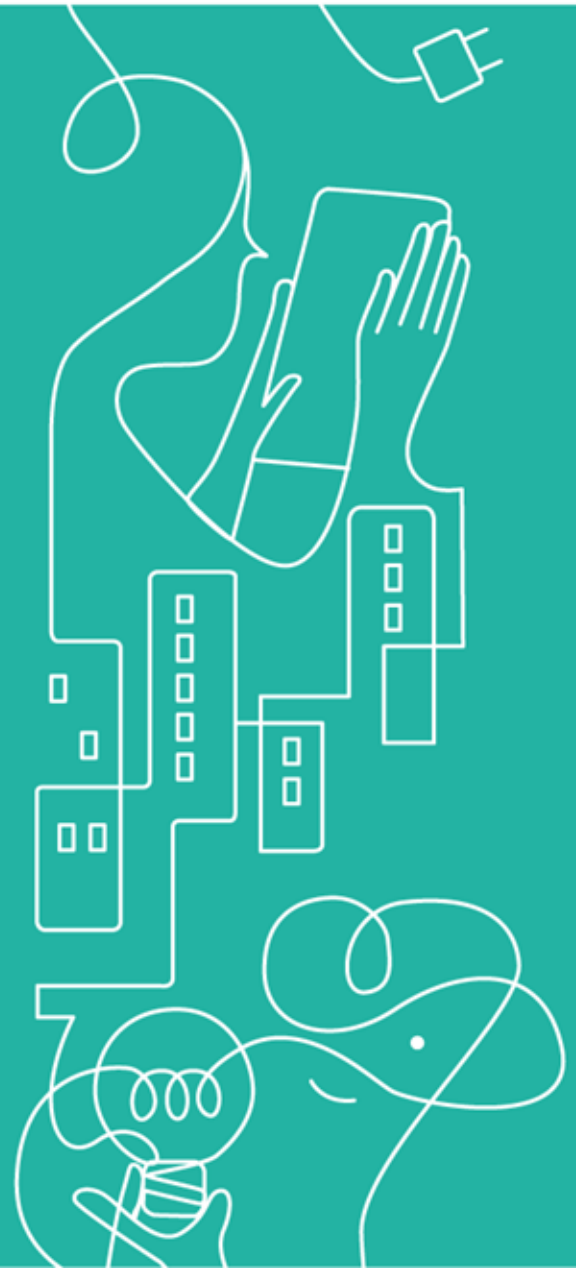
Assessore alla Legalità e Sicurezza



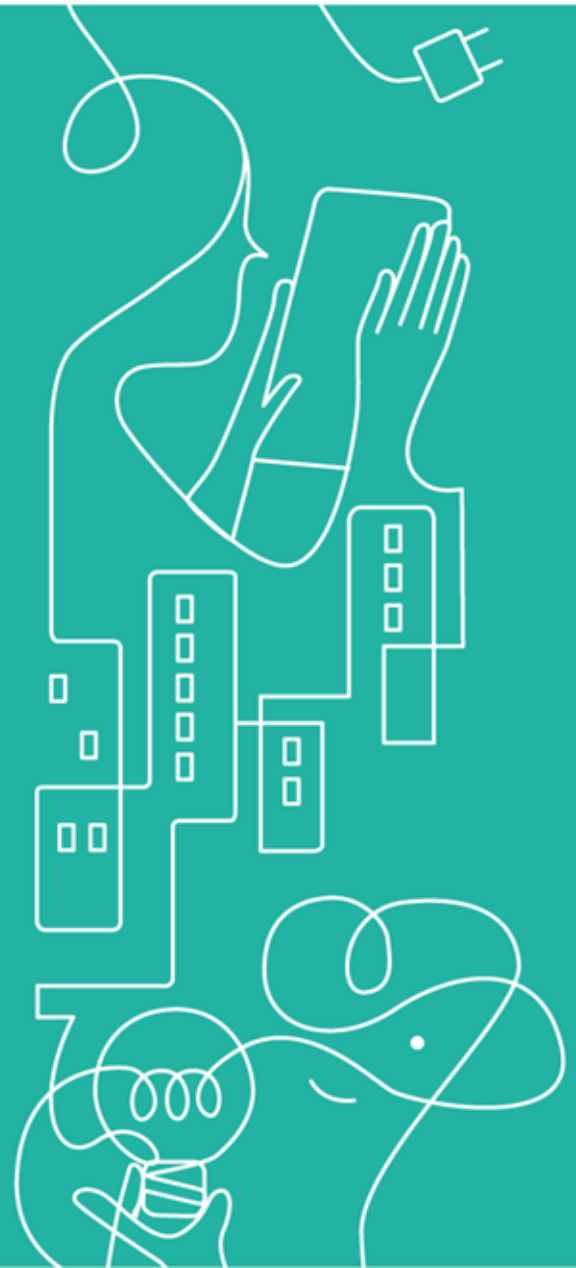
Saluti Istituzionali di API DONNA

Dott.ssa Maria Luigia Ghiggia

CEO A.M.I.S. SRL e Presidente APID



Risultati raggiunti con il Programma WE.CO.RE. 2025 e prospettive future



Introduzione & Saluti

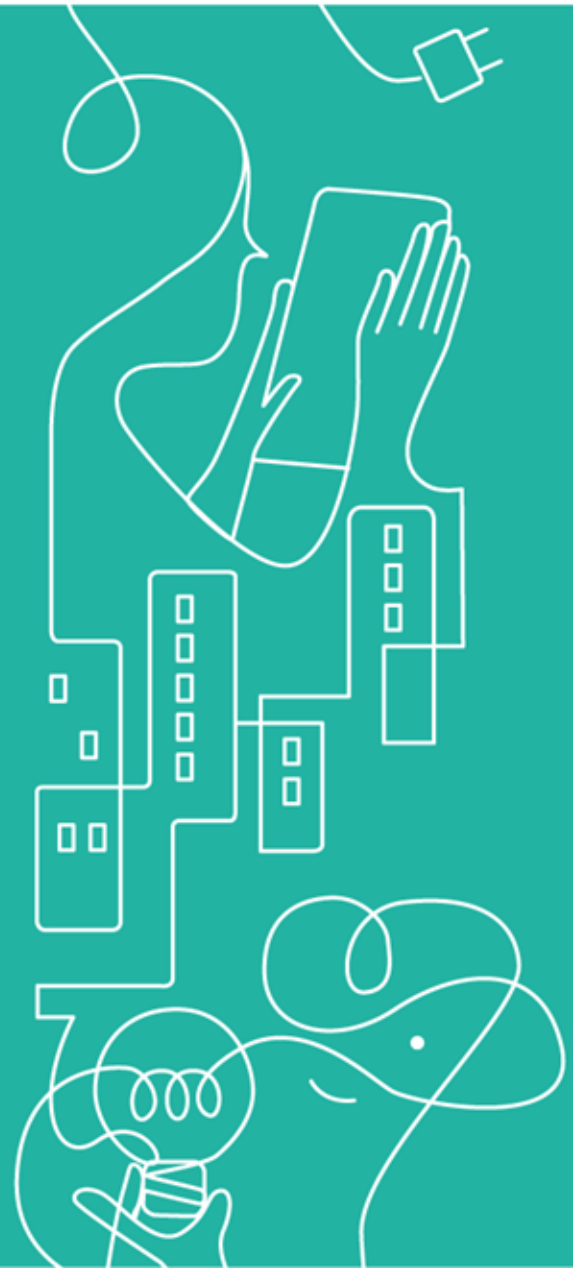
Il Microprogetto WomEn COoperating for cybeRsEcurity ha consentito a 16 aziende italo – francesi fondate e guidate da donne di poter usufruire di un Programma di formazione e consulenza manageriale adattabile alla realtà ed alle esigenze delle aziende beneficiarie.

La priorità del Programma è RIDINAMIZZARE L'ECONOMIA NELLA ZONA ALCOTRA di cui fanno parte i territori di Torino e Nizza

Intervento Dott.ssa Ghiggia – Presidente
API Donna, CEO A.M.I.S. SRL

Risultati raggiunti con il Programma WE.CO.RE. 2025 e prospettive future

Tale priorità fa riferimento all'obiettivo strategico "Un'Europa più competitiva e intelligente" e si concentra sullo sviluppo delle competenze del tessuto imprenditoriale per facilitare la transizione industriale e l'accesso ai servizi e prodotti locali grazie agli strumenti digitali. Essa è in sinergia con il partenariato europeo per le PMI innovative, che incoraggiano la leadership economica dell'industria europea attraverso lo sviluppo di nuovi strumenti, servizi e competenze. E' in tale ottica che, sin dalla fase iniziale di pianificazione dell'idea progettuale, tale azione pilota è stata concepita come percorso di cooperazione transfrontaliera di medio - lungo periodo, per consentire agli ecosistemi imprenditoriali di governare le sfide della trasformazione digitale con strumenti pratici ed efficaci di sicurezza digitale ed IA, ed aumentare allo stesso tempo l'innovazione e la competitività. E' molto importante puntare su finanziamenti europei che consentano di creare un ecosistema di competenze ed opportunità professionali che vadano in tale direzione. APID è in una fase importante di disseminazione dei risultati raggiunti da Capofila di tale progetto di cooperazione territoriale ed i risultati raggiunti rappresentano un nuovo inizio per uno scale up del Programma WE.CO.RE.

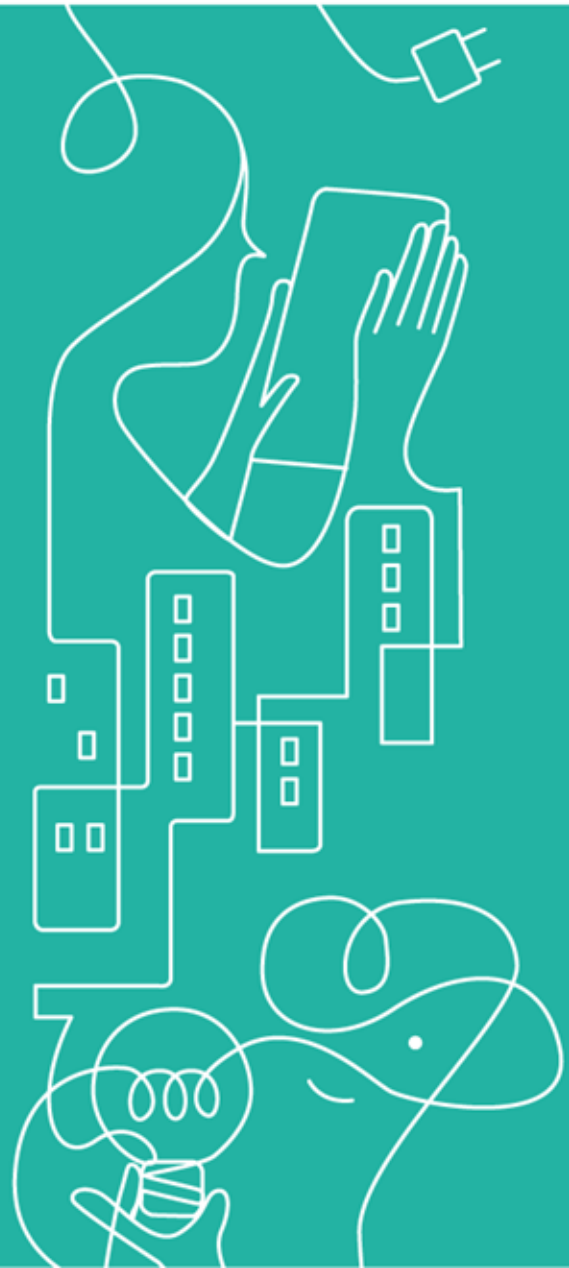


Intervento Dott.ssa Ghiggia – Presidente
API Donna, CEO A.M.I.S. SRL

Risultati raggiunti con il Programma WE.CO.RE. 2025 e prospettive future

Fase Attuale

Diagnostica post formazione per la verifica delle conoscenze acquisite dalle aziende beneficiarie



Fase Attuale

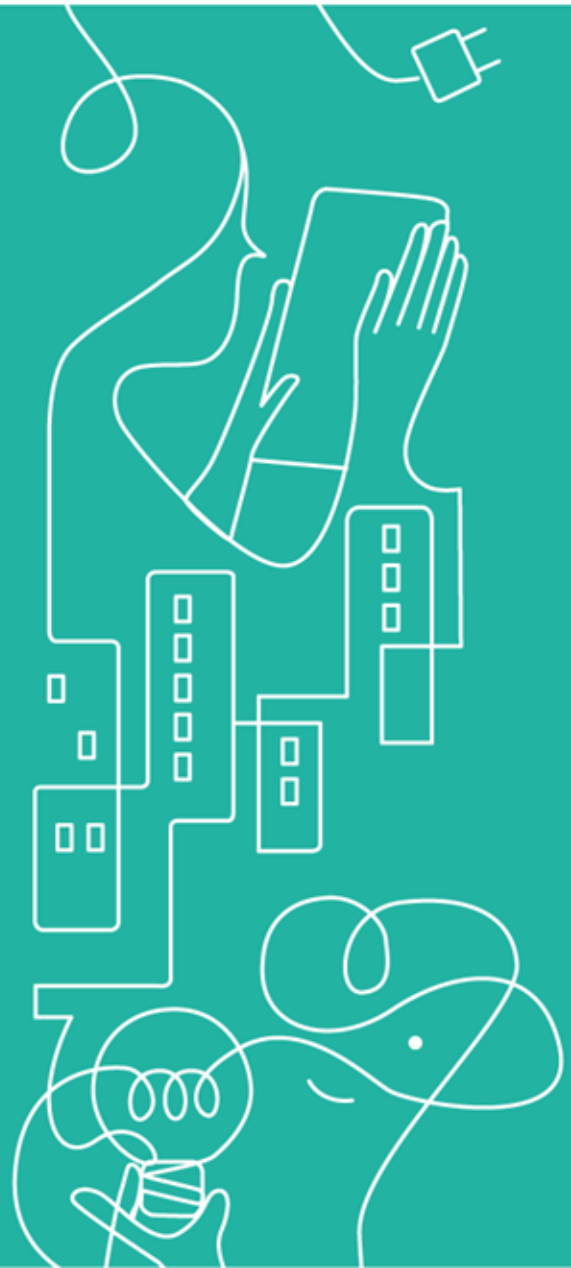
Diagnostica post formazione per la verifica delle conoscenze acquisite dalle aziende beneficiarie

9 risposte su 16

Le risposte consentono al TEAM WE.CO.RE. di presentare una roadmap personalizzata e misure specifiche per la sicurezza del sistema informativo.

Sezioni del questionario:

1. Informazioni generali: dettagli di base sulla tua azienda e sulle tue attività;
2. Maturità in materia di sicurezza informatica: valutazione delle pratiche e della consapevolezza della tua azienda in materia di sicurezza informatica;
3. Maturità e strumenti digitali: valutazione degli strumenti e delle tecnologie digitali utilizzati all'interno della tua azienda;
4. Maturità imprenditoriale: comprensione del tuo approccio individuale alla digitalizzazione e alla sicurezza informatica.

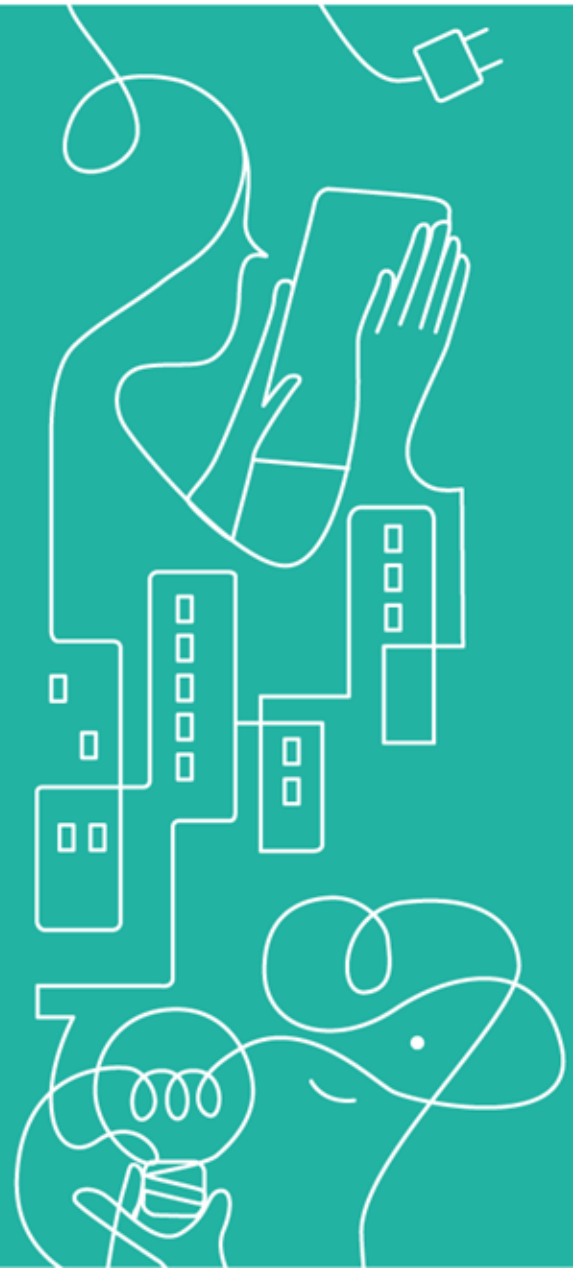


Intervento Dott.ssa Ghiggia – Presidente
API Donna, CEO A.M.I.S. SRL

Fase Attuale

Diagnostica post formazione per la verifica delle conoscenze acquisite dalle aziende beneficiarie

Settore Industriale	N. Aziende	Numero di Dipendenti	N. Aziende
Manifatturiero (Manufacturing)	4	4 - 10 dipendenti	6
Finanza / Settore Bancario	1	1 - 3 dipendenti	1
Tecnologia / IT	1	11 - 50 dipendenti	1
Settore Architettura	1	51 - 250 dipendenti	1
Produzione bottoni (settore tessile) e distribuzione	1	Totale Risposte	9
Commercio al dettaglio / E-commerce	1	-	-
Totale Risposte	9	-	-



Intervento Dott.ssa Ghiggia – Presidente
API Donna, CEO A.M.I.S. SRL

Fase Attuale

Diagnostica post formazione per la verifica delle conoscenze acquisite dalle aziende beneficiarie

Numero di Postazioni IT	Dati Sensibili Gestiti	Attacchi Subiti	Identificazione Attività Prioritarie
4 - 10	Segreti industriali	No	Idea generale delle attività/dati
1 - 3	Dati riservati dei clienti	No	Idea generale delle attività/dati
4 - 10	Segreti industriali, Brevetti, Dati commerciali, Dati clienti	No	Elenco preciso e aggiornato
4 - 10	Nessuno dei sopra indicati	No	Idea generale delle attività/dati
4 - 10	R&S, Brevetti, Dati commerciali, Dati clienti	No	Idea generale delle attività/dati

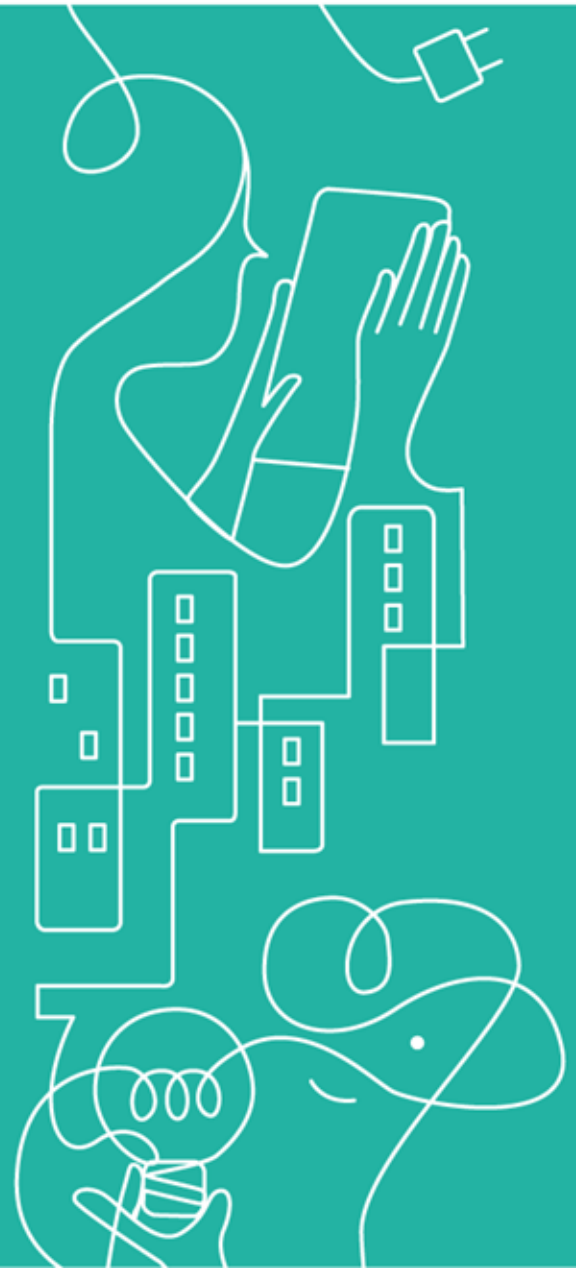


Intervento Dott.ssa Ghiggia – Presidente
API Donna, CEO A.M.I.S. SRL

Fase Attuale

Diagnostica post formazione per la verifica delle conoscenze acquisite dalle aziende beneficiarie

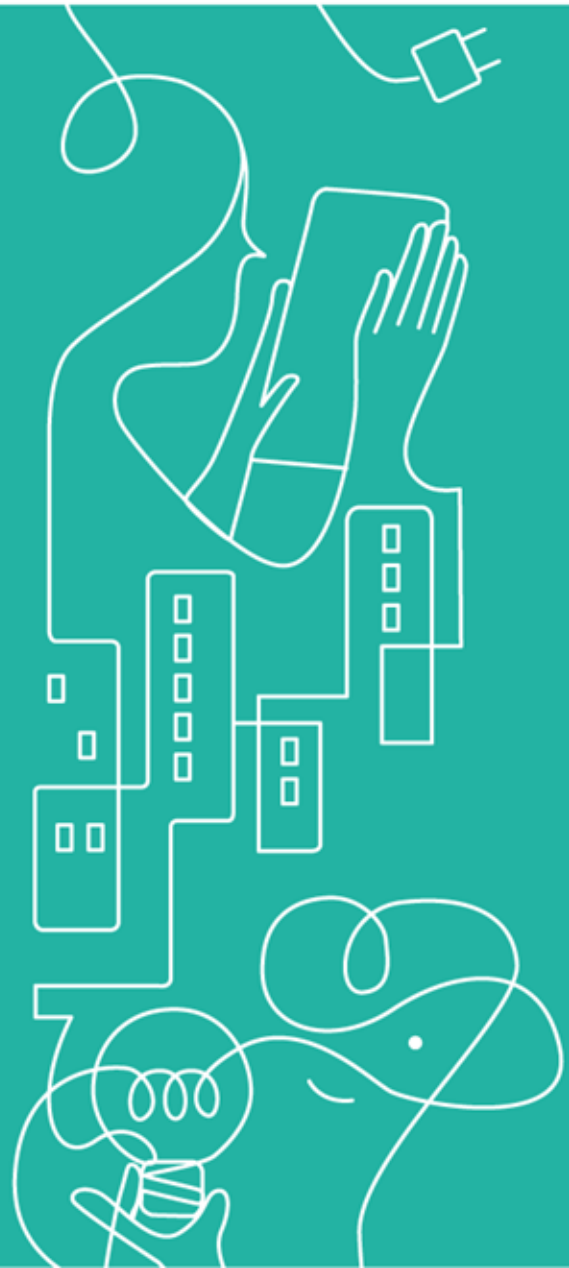
51 - 250	Brevetti, Dati commerciali, Furto dati interni, Dati clienti	Sì (Compromissione account/postazione)	Elenco preciso e aggiornato
11 - 50	Nessuno dei sopra indicati	No	Idea generale delle attività/dati
4 - 10	R&S, Dati clienti	Sì (Compromissione account, fornitore/partner)	Idea generale delle attività/dati
1 - 3	Dati riservati dei clienti	No	Idea generale delle attività/dati



Fase Attuale
Diagnostica post formazione per la verifica delle conoscenze acquisite dalle aziende beneficiarie

Punti Chiave Emersi dall'analisi precedente:

1. **Infrastruttura:** La maggior parte delle aziende utilizza tra le 4 e le 10 postazioni di lavoro IT.
2. **Sicurezza Informatica:** * La maggioranza dichiara di non aver mai subito attacchi informatici. Tuttavia, si registrano due casi di compromissione: uno relativo a una grande infrastruttura (51-250 postazioni) e uno in una piccola realtà (4-10 postazioni), quest'ultimo avvenuto anche tramite un partner o fornitore.
3. **Gestione dei Dati:** I "Dati riservati dei clienti" sono la tipologia di informazione sensibile più comune tra le aziende intervistate.
4. Consapevolezza **del Rischio:** La maggior parte delle aziende ha solo un'idea generale delle attività e dei dati da proteggere prioritariamente; solo due aziende dichiarano di possedere un elenco preciso e aggiornato.

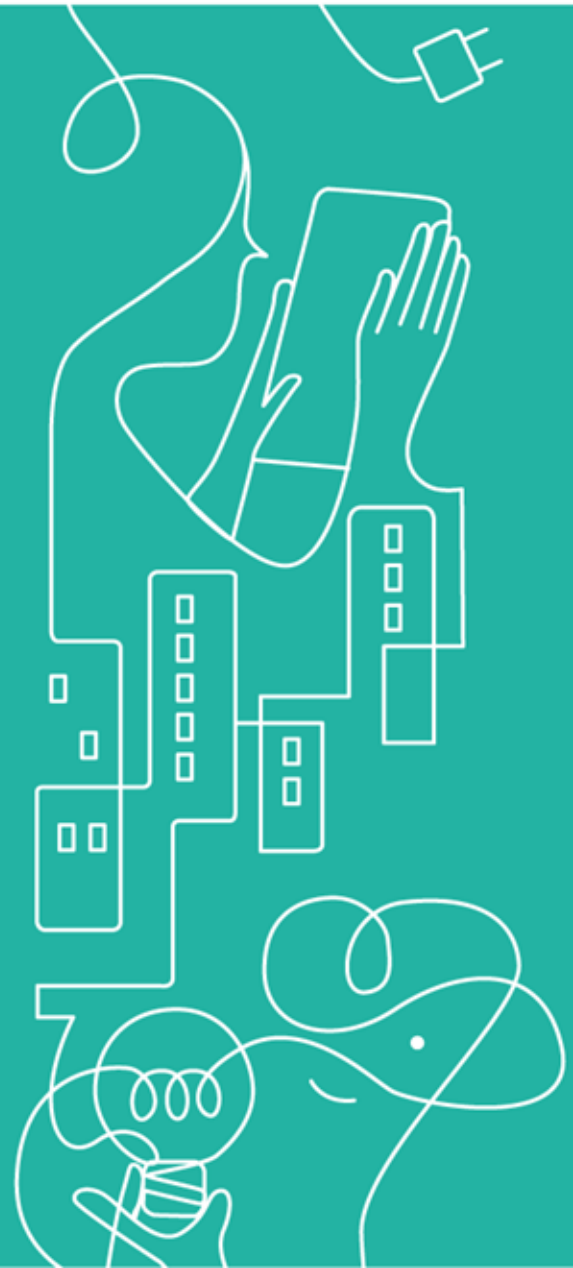


Intervento Dott.ssa Ghiggia – Presidente
API Donna, CEO A.M.I.S. SRL

Fase Attuale

Diagnostica post formazione per la verifica delle conoscenze acquisite dalle aziende beneficiarie

Misura di Sicurezza	Implementata (Sì)	Parziale / No	
Piano IT Dettagliato	1	8	
MFA per Accesso Remoto	4	5	
Requisiti Cyber nei Contratti	4	5	
Restrizione Privilegi Admin	3	6	



Fase Attuale

Diagnostica post formazione per la verifica delle conoscenze acquisite dalle aziende beneficiarie

Analisi dettagliata dei dati relativi alle policy di sicurezza informatica e alla gestione dei sistemi per le 9 aziende intervistate:

1. Pianificazione e Documentazione IT

La maggior parte delle aziende opera con una documentazione limitata, il che rappresenta un rischio per la continuità operativa:

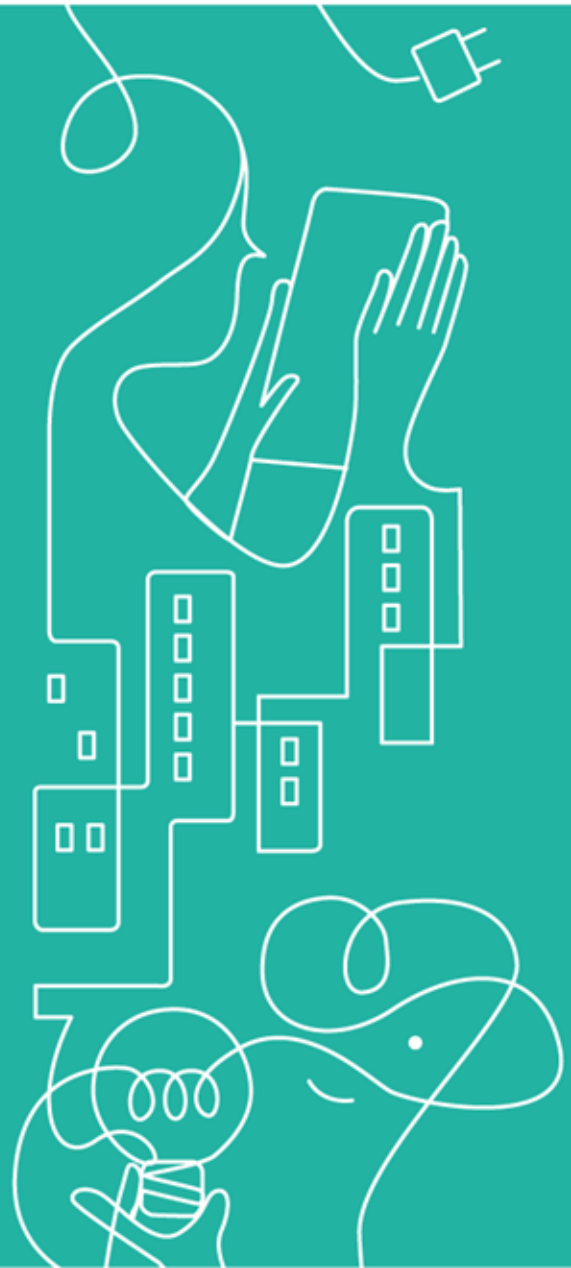
2. Piano dei sistemi informativi: 7 aziende su 9 possiedono solo un "macro piano" non dettagliato o parziale. Solo 1 azienda dispone di un diagramma dettagliato e aggiornato con l'elenco delle interconnessioni esterne.

3. Dati Personali: Solo 4 aziende hanno elencato tutti i dati personali trattati, mentre le restanti non lo sanno o non hanno effettuato la mappatura.

4. Requisiti nei Contratti: Solo 4 aziende formalizzano requisiti di cybersecurity nei contratti con i fornitori IT.

5. Gestione degli Accessi e Password

Le pratiche di gestione delle credenziali mostrano vulnerabilità significative, specialmente per quanto riguarda



Fase Attuale

Diagnostica post formazione per la verifica delle conoscenze acquisite dalle aziende beneficiarie

I privilegi elevati:

1. Amministratori di sistema: In 5 aziende su 9, gli utenti comuni hanno privilegi di amministratore sulle proprie workstation, o la rimozione di tali privilegi è ancora in corso.

2. Password: La maggior parte delle aziende (7 su 9) applica requisiti di complessità per le password.

3. Account Amministrativi: Solo 4 aziende effettuano una revisione sistematica e annuale degli account amministrativi per disattivare quelli inattivi.

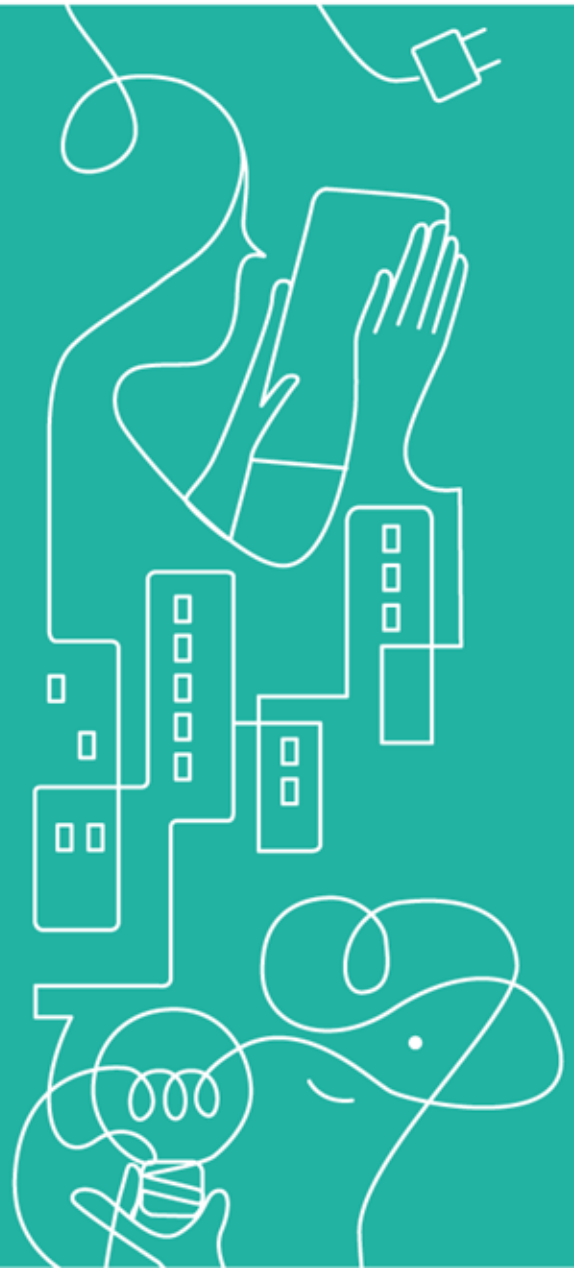
4. Protezione del Lavoro Remoto e Aggiornamenti

La sicurezza degli accessi esterni e la manutenzione dei software sono gestite in modo eterogeneo:

5. Multi-Factor Authentication (MFA): Solo 4 aziende proteggono le connessioni remote con l'autenticazione a più fattori. Per 3 aziende questo parametro "non è applicabile" o non è implementato.

Aggiornamenti Software: 5 aziende dichiarano di distribuire gli aggiornamenti sistematicamente, ma ammettono l'esistenza di eccezioni non ancora gestite. Le restanti 4 aziende applicano misure aggiuntive per garantire la protezione di server e utenti. **Sintesi delle Criticità Riscontrate**

Il quadro generale delinea una **fragilità organizzativa**: la maggior parte delle aziende intervistate non ha il pieno controllo sui privilegi degli utenti (rischio di installazione software malevoli) e non protegge adeguatamente gli accessi da remoto. La mancanza di piani dettagliati rende queste realtà meno resilienti in caso di incidente informatico grave.

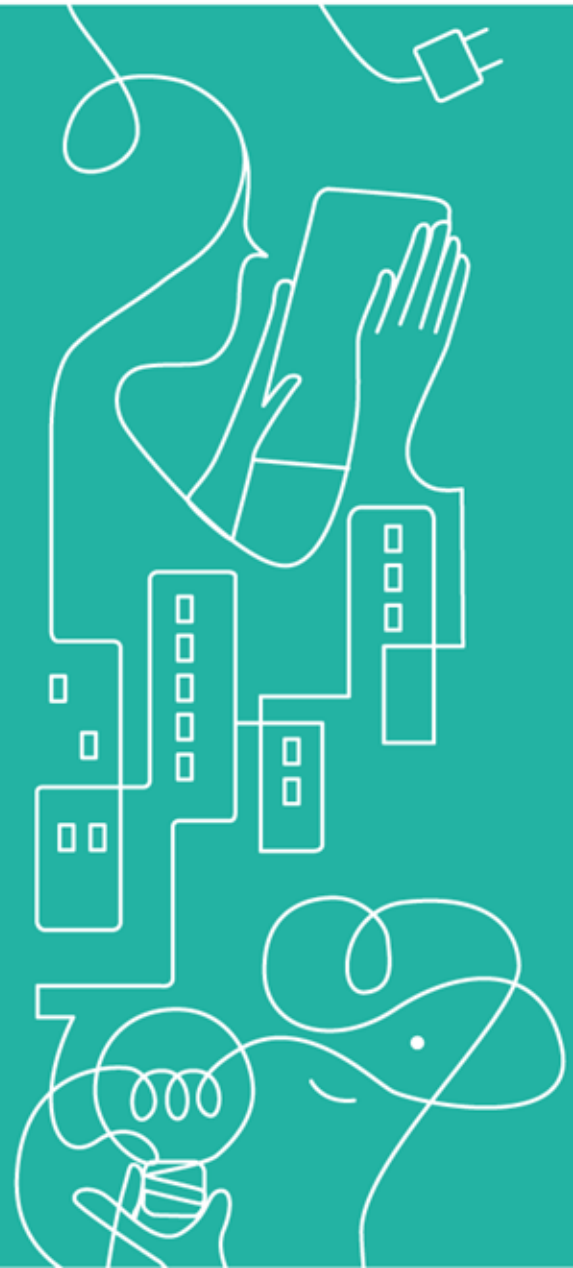


Intervento Dott.ssa Ghiggia – Presidente
API Donna, CEO A.M.I.S. SRL

Fase Attuale

Diagnostica post formazione per la verifica delle conoscenze acquisite dalle aziende beneficiarie

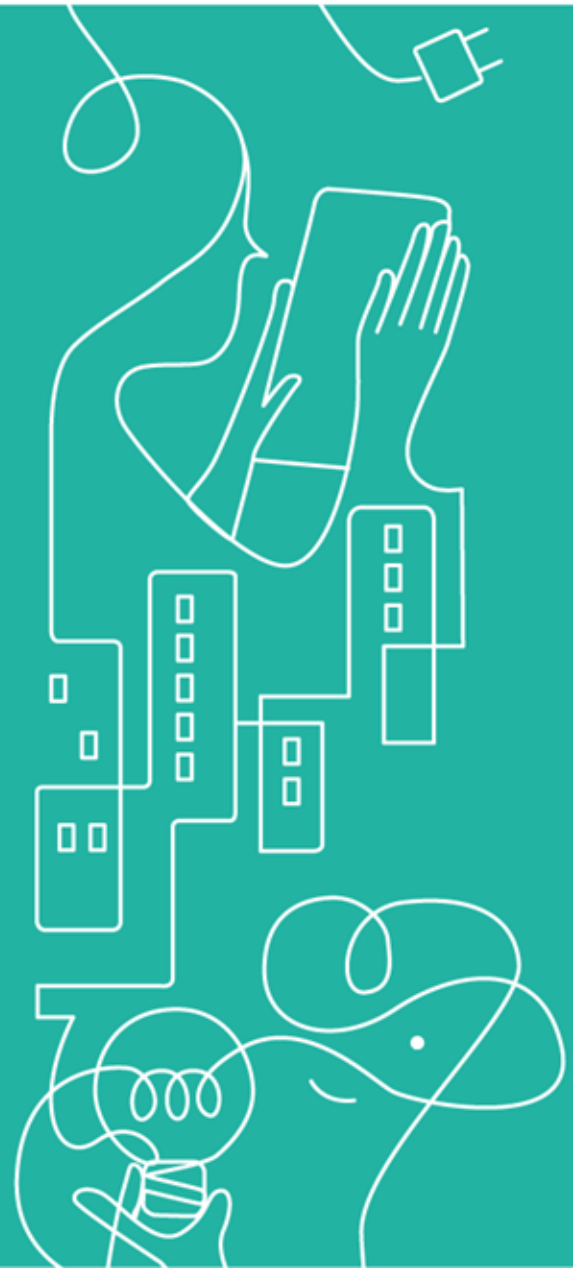
Al questionario diagnostico segue il colloquio ONE TO ONE per la definizione del Piano di miglioramento della strategia di sicurezza aziendale.



Saluti Istituzionali e Presentazione di Alliance Française

Dott.ssa Gabriella Mattio

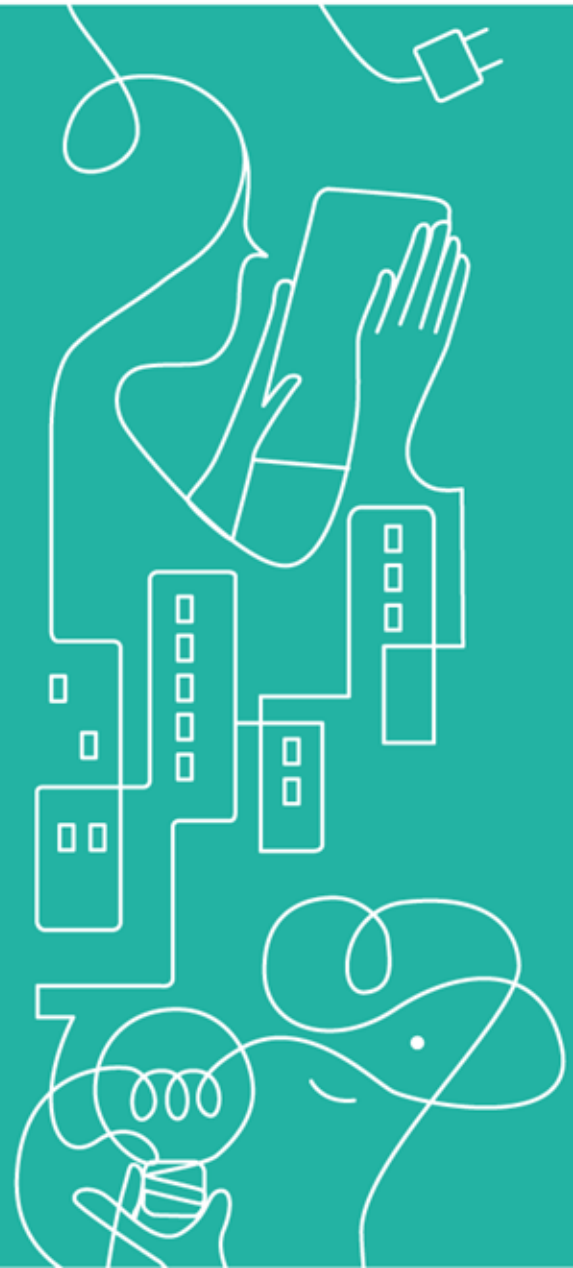
Referente Corsi e Aziende



Chiusura e Saluti
Dott.ssa Annalisa Caccioppoli
Project Manager & Communication Strategist

Chiusura e Saluti
Invito a seguirci su

https://www.we-core.net/



GRAZIE PER L'ATTENZIONE

