Progetto PNRR M1C1 I 1.5 - Cybersecurity -
”Assessment e potenziamento della resilienza cyber di ARPAC”

Potenziamento della *Cybersecurity & Data Protection Awareness* dei dipendenti agenziali

Sommario

1 Introduzione alle attività di Cyber Awareness

Nel contesto attuale, caratterizzato da un rapido sviluppo tecnologico e da un aumento della frequenza e della gravità degli attacchi informatici, la sicurezza delle informazioni è diventata una priorità imprescindibile per le Organizzazioni ed investire nella formazione e nella sensibilizzazione del personale rappresenta una strategia fondamentale per affrontare efficacemente queste sfide.

Un team ben informato e sensibilizzato mediante lo sviluppo di programmi di formazione trasversali a tutta la popolazione Aziendale può mitigare significativamente il rischio e l'impatto di incidenti di sicurezza, contribuendo così al rafforzamento dei sistemi e delle informazioni sia Aziendali che in relazione all'identità digitale di ogni singola persona coinvolta.

Lo sviluppo di programmi di formazione che coinvolgano tutti i livelli Aziendali assicura che ogni Dipendente comprenda il proprio ruolo cruciale nella protezione delle informazioni. Solo attraverso una consapevolezza diffusa delle minacce informatiche e delle misure di prevenzione sarà infatti possibile garantire una solida difesa contro gli attacchi informatici, un ambiente di lavoro sicuro ed il rispetto delle normative di settore.

In particolare, le attività formative e di sensibilizzazione sono divenute centrali all'interno delle Organizzazioni anche in relazione alle novità normative nazionali ed europee che, di fatto, prevedono obblighi e standard di formazione in materia di cybersicurezza.

La Direttiva (UE) 2022/2555, il D. Lgs. 138/2024 e la Determinazione dell'Agenzia per la Cybersicurezza Nazionale (ACN) 164179 del 14 aprile 2025, solo per citarne alcune, impongono agli Organi Direttivi delle Organizzazioni l'obbligo di implementare programmi formativi con contenuti afferenti all'ambito della sicurezza informatica, delle informazioni e della cybersicurezza.

Di fatto è necessario, quindi, promuovere l'offerta periodica di formazione, coerentemente con le mansioni lavorative svolte, per migliorare e favorire l'acquisizione di conoscenze e competenze.

Allo stesso modo, anche gli standard e le best practice di settore, non da ultimo lo standard ISO/IEC 27001:2022 (Sistema di Gestione per la Sicurezza delle Informazioni), enfatizza l'importanza del miglioramento continuo secondo il ciclo Plan-Do-Check-Act (cd. PDCA).

Tali attività sono state inquadrate nel più ampio progetto previsto nell'ambito dell' "Avviso Pubblico di ACN per la presentazione di proposte di interventi di potenziamento della resilienza cyber dei grandi Comuni, dei Comuni capoluogo di Regione, delle Città Metropolitane, delle Agenzie regionali sanitarie e delle Aziende ed enti di supporto al Servizio Sanitario Nazionale, delle Autorità di sistema portuale, delle Autorità del Bacino del Distretto idrografico e delle Agenzie regionali per la protezione dell'ambiente a valere sul Piano Nazionale di Ripresa e Resilienza, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" – Codice d'investimento M1C1I1.5".

Di fatto l'Agenzia con nota prot. n. 23488 del 12.04.2024 ha presentato domanda di partecipazione all'Avviso pubblico ACN n. 8/2024; ACN con prot. n. 30550 del 23.09.2024 ha approvato l'aggiornamento degli elenchi predisposti dalla Commissione di valutazione definendo la graduatoria definitiva con ammissione e finanziamento del progetto di ARPA Campania.

In questo documento, verranno delineati gli obiettivi e le modalità di sviluppo ed attuazione del Programma di Cybersecurity Awareness, delineando i risultati ottenuti, con l'intento di analizzare i benefici in tema di consapevolezza sulla sicurezza informatica.

L'attività è stata svolta con il supporto tecnico specialistico del Fornitore Esterno – EY Advisory S.p.A. nell'ambito dell'AQ CONSIP ID 2296, Lotto 2 "Servizi di Compliance e Controllo".

2 Sviluppo del programma formativo per i target coinvolti

L'efficacia di un programma di formazione su temi di sicurezza delle informazioni è strettamente legata ad un'attenta individuazione dei differenti cluster delle risorse destinatarie delle attività di formazione e sensibilizzazione al fine di adattare i contenuti formativi alle specifiche esigenze dei soggetti e alle vulnerabilità all'interno di un'organizzazione.

La suddivisione è stata quindi individuata come segue:

- ✓ *Personale Dirigente;*
- ✓ *Personale dei Dipartimenti Provinciali, comprensivo anche della U.O.C. Siti Contaminati e Bonifiche;*
- ✓ *Personale del Comparto della Struttura Centrale ARPAC.*

Una volta individuati i target dei soggetti interessati sono state avviate le attività per lo sviluppo e l'implementazione del programma formativo, diviso in tre fasi principali ed eseguito con l'obiettivo di garantire dei contenuti efficaci e coinvolgenti per i Dipendenti:

- **Fase 1 -** Identificazione del fabbisogno formativo;
- **Fase 2 -** Pianificazione e raccolta delle esigenze formative;
- **Fase 3 -** Programmazione ed Erogazione delle attività formative.

Nel corso di queste tre fasi è stato essenziale il supporto continuo e proattivo della Direzione Generale, ossia dei Referenti interni della Unità Operativa Sistemi Informativi e Informatici (UO SINF) che hanno svolto un ruolo centrale per la buona riuscita del progetto formativo, permettendo l'implementazione di un programma dettagliato sulla base delle esperienze concrete dei Dipendenti agenziali, sollecitandone la partecipazione.

Il supporto del Management è comprovato essere di fondamentale importanza per fornire la visione strategica dell'attività a tutti i Dipendenti, e di fatto le attività sono state precedute da note protocollate interne, a firma del Direttore Generale, volte a preavvisare la popolazione agenziale delle attività, promuovendole anche come monte ore per il piano formativo obbligatorio di ARPAC.

2.1 Identificazione del fabbisogno formativo

La prima fase del programma ha avuto ad oggetto la pianificazione e la raccolta delle esigenze formative del personale.

In questa fase è stata condotta, congiuntamente ai referenti succitati, un'analisi approfondita del contesto dell'Agenzia e dei seguenti elementi:

- le competenze attuali dei Dipendenti;
- le lacune esistenti;
- i ruoli e le responsabilità specifiche;
- la tipologia di informazioni che ciascun'area gestisce durante la propria routine lavorativa.

Pertanto, a valle della valutazione suddetta sono state definite delle attività formative suddivise in

- n. 2 distinte edizioni per il personale Dirigente, ciascuna edizione composta da n. 3 sessioni
- n. 13 sessioni formative per il personale di Comparto dei Dipartimenti, comprensivo anche della U.O.C. Siti Contaminati e Bonifiche e per il personale del Comparto incardinato nelle UO della Struttura Centrale.

Le attività sono state così strutturate al fine di consentire a tutta la popolazione agenziale di potervi prendere parte.

Il materiale formativo prodotto per la platea dei Dirigenti, nonché per la platea del Comparto dei Dipartimenti provinciali e UOC SICB e del Comparto della Struttura Centrale, è stato focalizzato su aspetti generali, in relazione alla sicurezza delle informazioni e cybersecurity e, successivamente, per ciascun target sono stati effettuati degli approfondimenti ad-hoc sulla base delle modalità succitate (ad es. è stata prevista una sezione sul ruolo della dirigenza in tema di sicurezza delle informazioni per il personale Dirigente).

Il materiale ed i contenuti proposti sono stati costruiti e validati con il supporto dei Referenti interni UO SINF.

Pertanto, in linea generale, il materiale formativo ha affrontato le seguenti tematiche:

- **L'importanza della Cybersecurity e scenario normativo vigente,** ove è stata fornita l'overview di base degli aspetti di cybersecurity, nonché i trend a livello internazionale ed italiano in relazione alle minacce ed agli attacchi informatici.
  Inoltre, è stato trattato lo scenario normativo vigente (in ambito Cybersecurity & Data Protection) che, allo stato attuale, è in forte evoluzione;
- **Il rischio Cyber e le minacce informatiche,** ove è stata fornita una panoramica delle principali minacce che il personale potrebbe trovarsi ad affrontare, come ad esempio phishing e ransomware, unitamente ad un focus su ARPAC come possibile obiettivo;
- **Pratiche di igiene Informatica,** ove sono state analizzate le attuali modalità di utilizzo dei social media e di gestione delle password, per identificare le aree di miglioramento necessarie per garantire la sicurezza delle informazioni e sono stati forniti consigli pratici da implementare quotidianamente;
- **Sicurezza dei Dispositivi,** ove sono state esaminate le pratiche attuali per la protezione dei dispositivi Aziendali ed identificate le potenziali vulnerabilità, e sono stati forniti strumenti di miglioramento;

- **Cultura della Sicurezza,** ove è stata enfatizzata l'importanza di una mentalità orientata alla sicurezza, incoraggiando il personale a segnalare comportamenti sospetti ed a seguire le best practices.

Nella fase di organizzazione della attività sono state anche previste delle attività di monitoraggio e gestione delle sessioni, con l'implementazione di strumenti che hanno permesso la verifica in termini di partecipazione ed il tracciamento dei numeri dei partecipanti.

Per ogni sessione di formazione è stato effettuato un test di valutazione interattivo per consentire ai partecipanti di valutare la propria comprensione degli argomenti e dei temi trattati nonché di stimolare dei dibattiti interattivi efficientando la trasmissione dei contenuti.

È stato inoltre previsto il rilascio di un attestato di partecipazione al termine delle sessioni unitamente ad un prontuario esplicativo relativo alle best practice di sicurezza in materia Cybersecurity e Data Protection.

2.2 Programmazione ed erogazione delle attività formative

A valle del completamento della raccolta delle esigenze formative, si è proceduto con la programmazione e l'erogazione delle attività formative.

Mediante il supporto dei Referenti citati è stato sviluppato un piano di erogazione delle sedute formative che tenesse in considerazione le specifiche esigenze dei Dipendenti.

Le attività formative sono state quindi suddivise in moduli ed erogate attraverso diverse modalità, secondo le esigenze definite, tra cui:

- **Workshop in aula**: sessioni interattive condotte da esperti 'in presenza', che offrono opportunità di discussione ed approfondimento su temi specifici della cybersecurity;
- **Sessioni di formazione da remoto**: sessioni di formazione virtuali ed interattive, condotte da esperti, che permettono di raggiungere tutti i Dipendenti, indipendentemente dalla loro posizione o orario di lavoro.

Questo approccio ibrido ha garantito una partecipazione ancora più massiva, poichè i Dipendenti, indipendentemente dalla loro posizione o orario di lavoro, hanno avuto la possibilità di non rinunciare alla formazione.

Alla data, è stata erogata l'edizione n. 1 - composta da n. 3 sessioni - per il personale Dirigente, due delle quali sono state effettuate tramite workshop in aula, a cui è stata aggiunta una terza sessione di recupero online.

Per i Dipartimenti di Benevento, Caserta e Napoli sono state erogate tutte le sessioni previste con workshop in aula; per i Dipartimenti di Salerno ed Avellino, nonché per il personale di Comparto della

Struttura Centrale e della UOC SICB sono state erogate tutte le sessioni previste, ma da remoto, comprensive anche di una sessione di recupero successiva per permettere, a chi fosse stato assente durante la propria sessione di riferimento,d di partecipare alla formazione.

Durante l'erogazione delle attività formative, per entrambe le modalità, sono stati inclusi casi studio pratici e test di valutazione interattivi, che hanno reso la formazione più efficace ed interattiva: questi elementi pratici hanno consentito ai partecipanti di applicare le conoscenze acquisite, migliorando la loro capacità di riconoscere ed affrontare minacce informatiche.

A completamento delle attività formative, e per applicare il principio del miglioramento continuo, nel progetto è stata prevista la distribuzione di una *newsletter* mensile inerente le *best practices* in materia di sicurezza informatica, relativa alle attività quotidiane svolte dal personale, inviata mensilmente a tutta la popolazione agenziale.

Il servizio consiste nella produzione e distribuzione di un'infografica, facilmente leggibile, finalizzata a garantire un costante aggiornamento delle conoscenze in tema di sicurezza delle informazioni ed efficientare l'assimilabilità dei contenuti trattati.

3 Key performance indicator dell'attività[1]

Le attività svolte sono state accolte con profondo senso di partecipazione da parte di tutti i Dipendenti coinvolti, i quali si sono dimostrati proattivi, fortemente partecipativi nonché stimolati al dibattito.

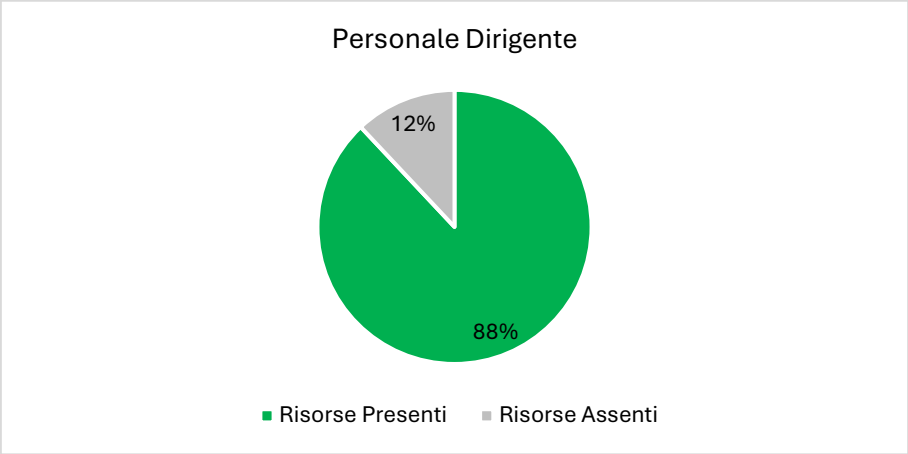
Per permettere un'approfondita valutazione del programma sulla base delle sedute finora erogate sono stati implementati strumenti di monitoraggio della partecipazione della popolazione agenziale alle sessioni di formazione, facendo un distinguo sulla base dei target di riferimento individuati.

3.1 Personale Dirigente

Per il personale Dirigente sono state effettuate 2 sessioni in data 14 marzo 2025, tenutesi presso la sala riunioni della struttura centrale di ARPAC, mentre una terza sessione, di recupero, è stata effettuata online per permettere la partecipazione dei Dipendenti assenti nelle precedenti sessioni.

Di seguito le percentuali della partecipazione totale, alle sessioni, per il personale Dirigente:

[1] Si evidenzia che la UO Sistemi Informativi e Informatici non è presente nelle numeriche/ statistiche che saranno descritte di seguito, in quanto impegnata prossimamente in un'attività formativa ad-hoc.



Il numero di risorse totali coinvolte nella formazione è stato di 50 Dirigenti, ed è stata registrata una partecipazione totale (per tutte le sessioni suddette) dell'88% dei Dipendenti coinvolti, con una percentuale di assenti del 12%: la flessibilità delle modalità di erogazione, con la possibilità di partecipazione online ad una sessione di recupero, ha quindi garantito una copertura molto vasta della popolazione dirigenziale.

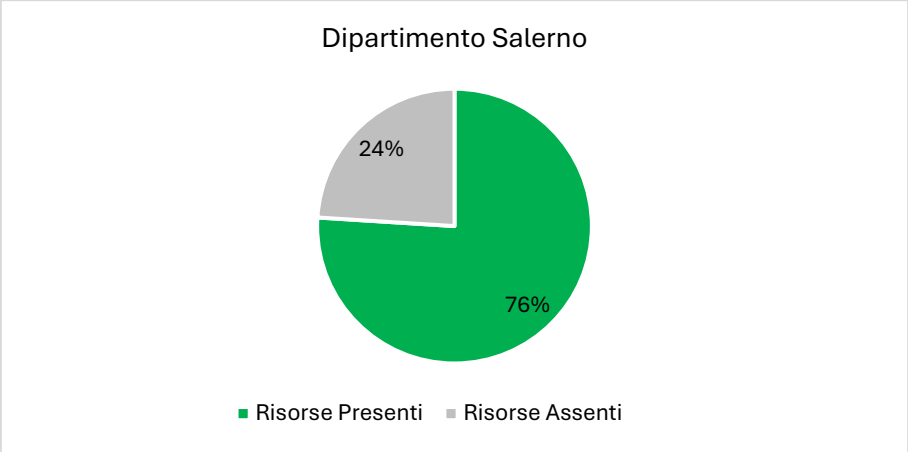
3.2 Personale di Comparto dei Dipartimenti Provinciali, comprensivo anche della UOC Siti Contaminati e Bonifiche, e personale di Comparto della Struttura Centrale

Per il personale di Comparto dei Dipartimenti Provinciali, comprensivo anche della UOC Siti Contaminati e Bonifiche, e per il personale di Comparto della Struttura centrale, sono state convocate 567 risorse.

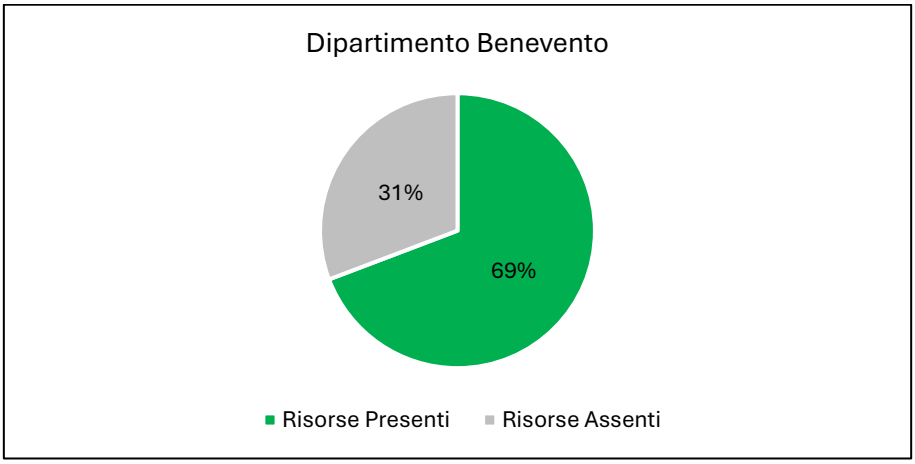
Le sessioni sono state tenute in presenza, presso i Dipartimenti ove è stato possibile per la disponibilità di una sala riunioni, e/o online, a seconda quindi delle specifiche esigenze dei Dipendenti.

Per ogni sessione è stata tracciata, sulla base del numero di risorse convocate, la partecipazione o l'assenza delle risorse: di seguito le percentuali di partecipazione, distinte per sessione:

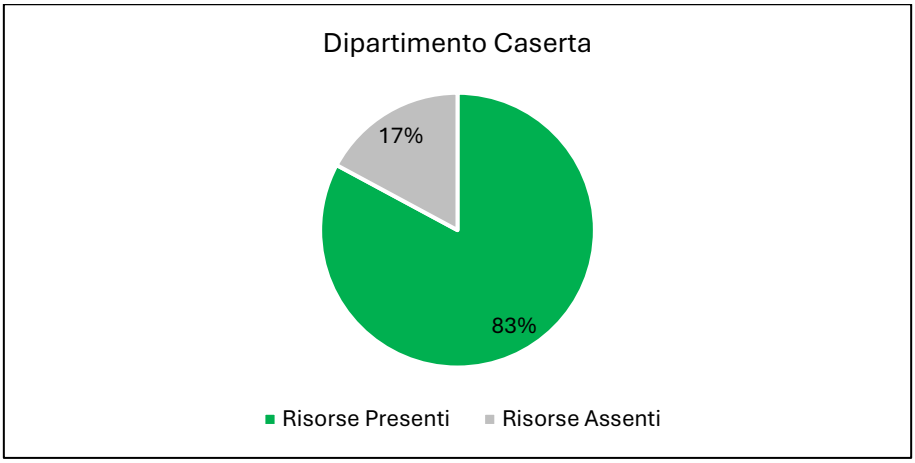
- **Dipartimento Salerno – sessione online:**



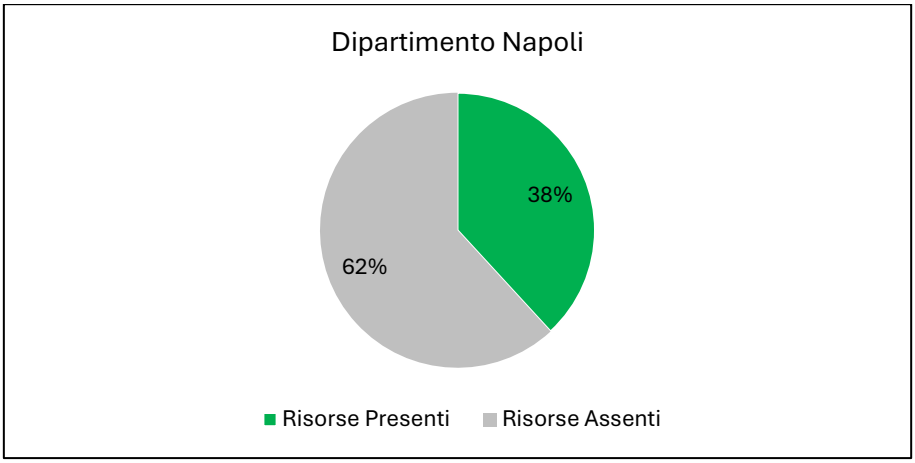
- **Dipartimento Benevento – sessione in presenza:**



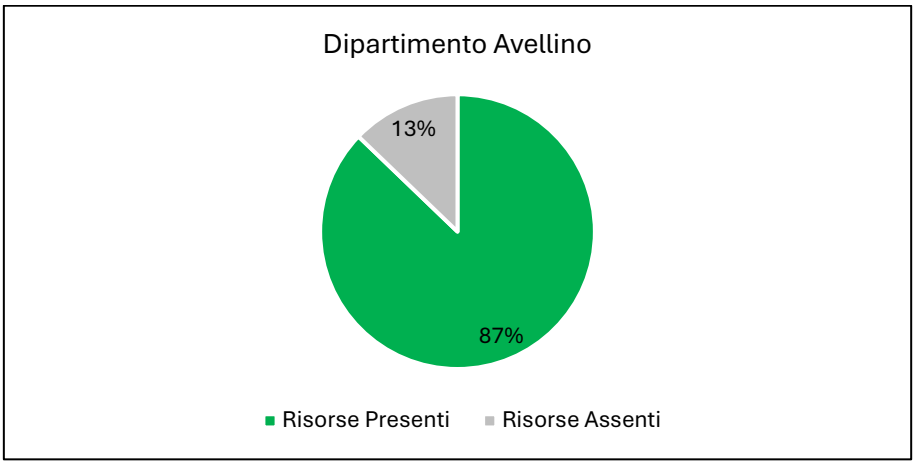
- **Dipartimento Caserta – sessione in presenza:**



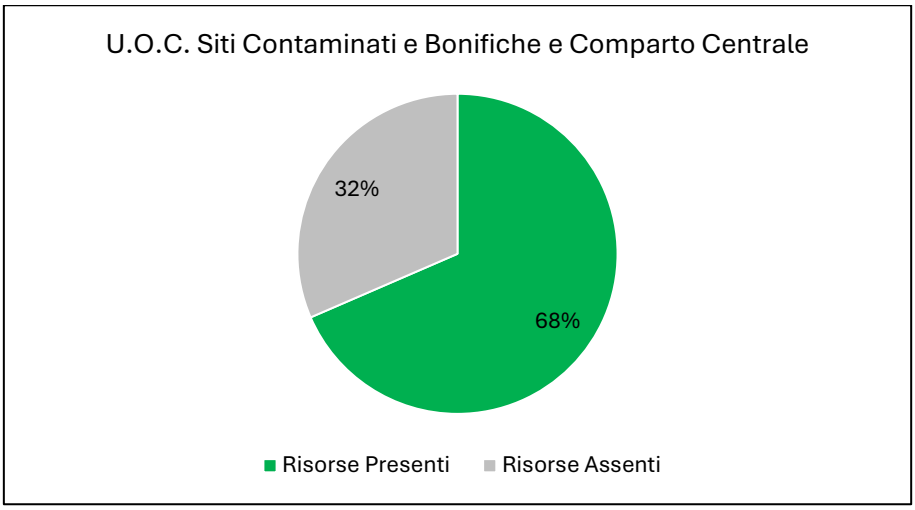
- **Dipartimento Napoli – sessione in presenza:**



- **Dipartimento Avellino – sessione online:**

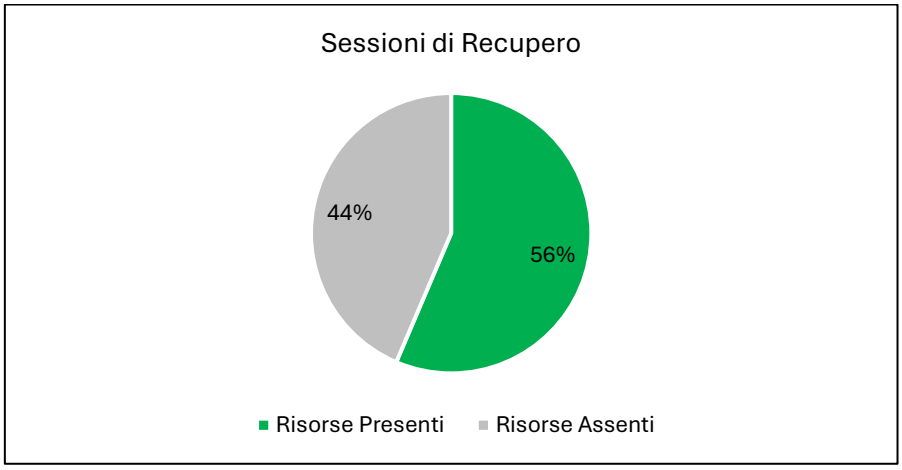


- **U.O.C. Siti Contaminati e Bonifiche e Comparto Centrale – sessione online:**



La partecipazione generale alle sessioni di riferimento è stata di 372 presenti e 195 assenti.

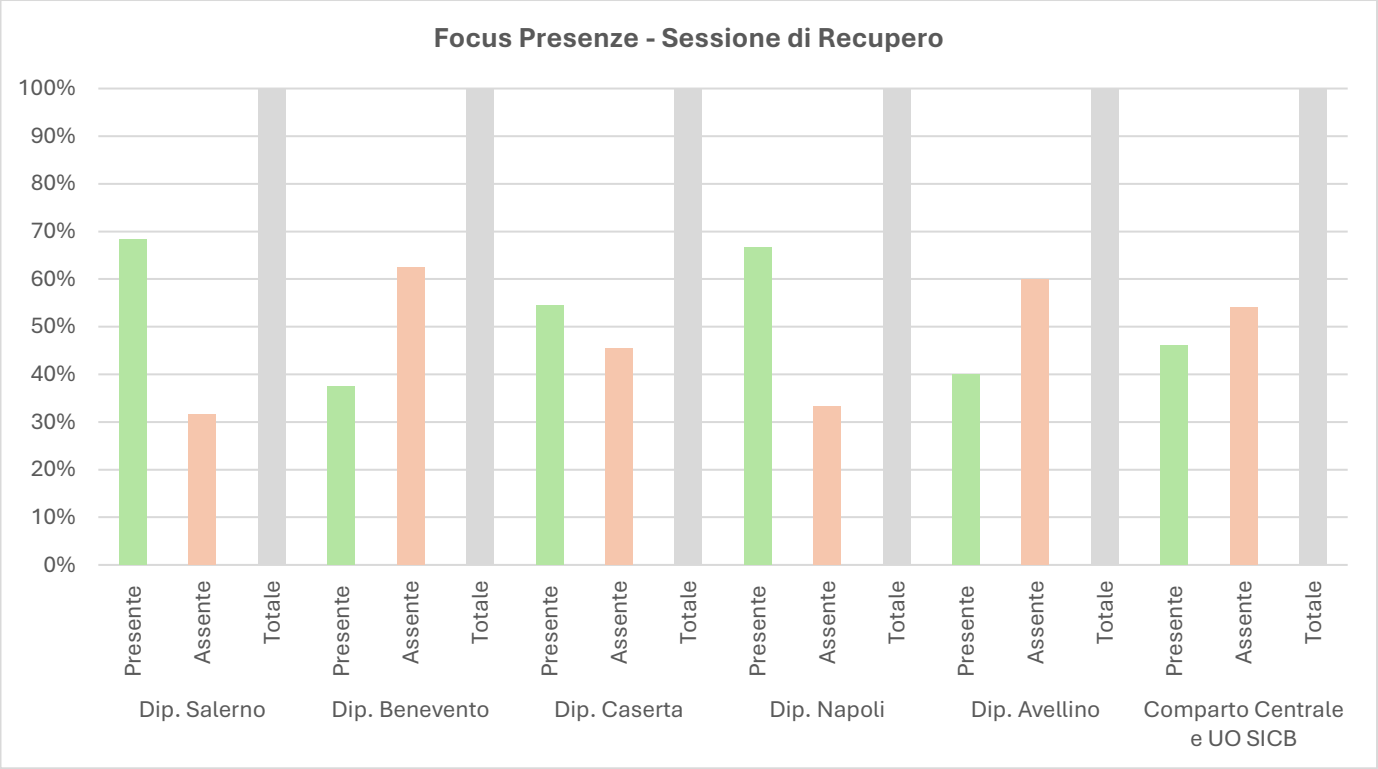
Si segnala che le 195 risorse assenti nelle sessioni di riferimento hanno successivamente avuto la possibilità di partecipare ad una sessione di recupero online, di cui di seguito si riportano le numeriche:



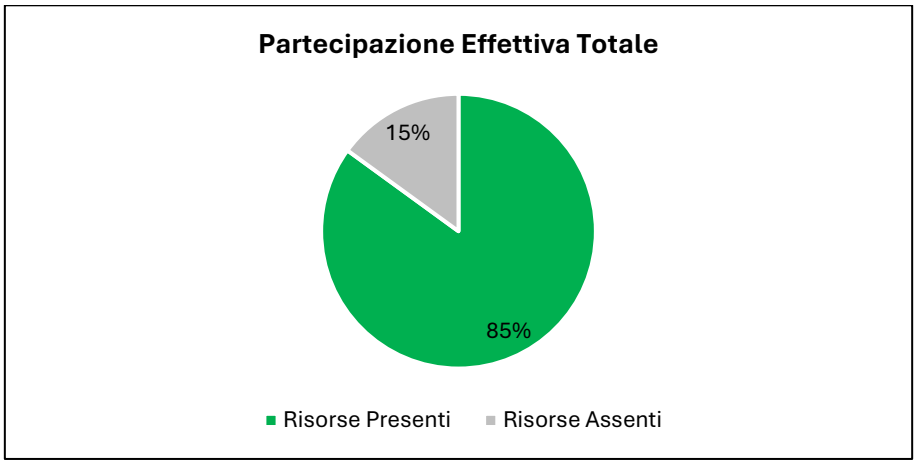
In virtù del fatto che la sessione di recupero è stata composta da risorse risultate assenti e/o da risorse che hanno richiesto esplicitamente la partecipazione a tale sessione[2], di seguito si riporta un focus relativo alle presenze alla suddetta sessione.

In particolare, dal grafico seguente si potrà evincere la suddivisione dei presenti/assenti alla sessione di recupero, rispetto al totale dei convocati, per ciascuna risorsa dei Dipartimenti Provinciali, UOC SICB e Struttura Centrale:

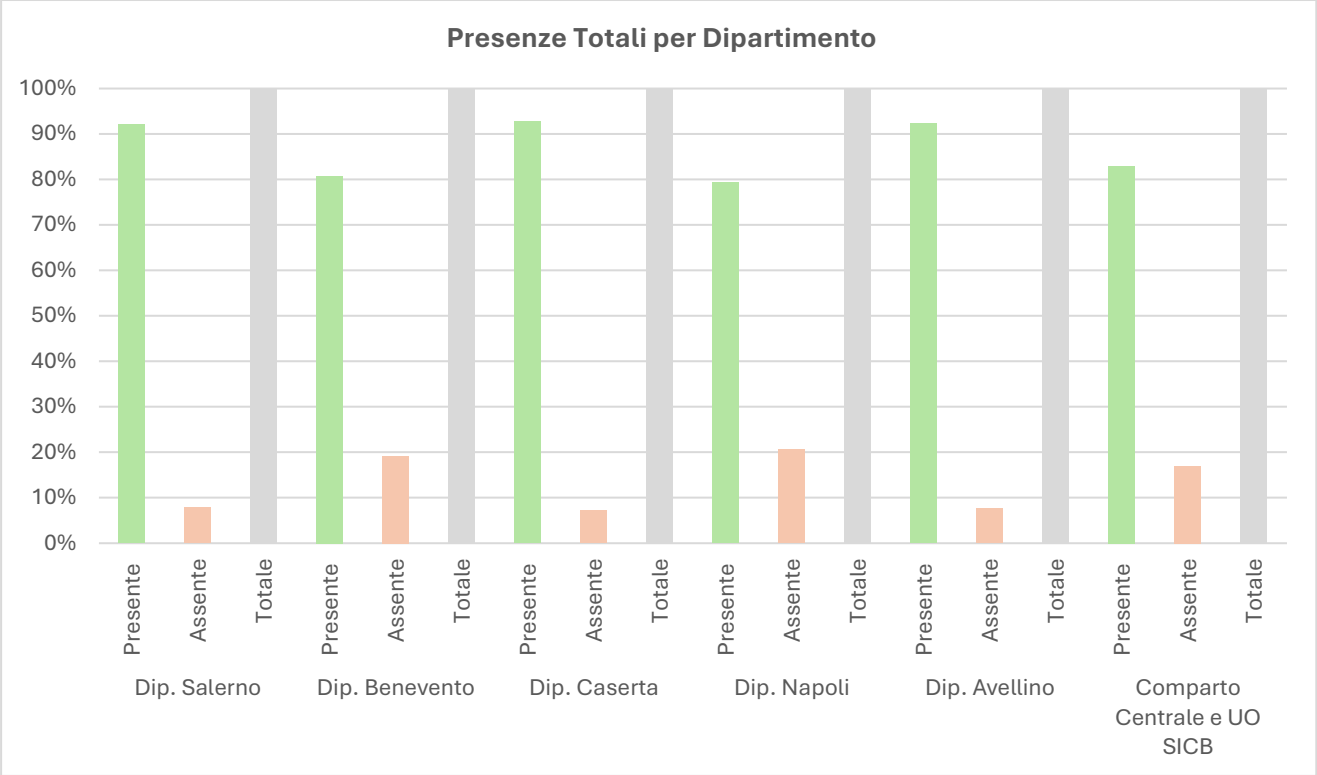
[2] Si riporta che alcuni dei Dipendenti del Dipartimento di Napoli, per esigenze di natura logistico/ organizzative, sono stati inclusi direttamente all'interno della sessione di recupero.



Con la sessione di recupero, la **partecipazione generale del personale di Comparto agli eventi formativi proposti è salita all'85%,** con un totale di 482 risorse presenti e 85 risorse assenti sul totale dei Dipendenti coinvolti:



Di seguito si riporta graficamente la percentuale di partecipazione **totale** alle sessioni erogate, in relazione ad ogni singola risorsa dei Dipartimenti Provinciali, UOC SICB e Struttura Centrale:



4 Conclusioni

L'attività ha visto l'adesione e l'impegno attivo di tutti i Dipendenti coinvolti, Dirigenti e Comparto, e grazie al supporto continuo del Management e dei Referenti Interni sono state **raggiunte percentuali di partecipazione molto elevate**, anche rispetto a numeriche rilevanti.

Tale risultato non solo evidenzia l'interesse e l'impegno dei partecipanti verso le tematiche della Cybersicurezza, ma sottolinea anche l'importanza di investire nella formazione continua per affrontare le sfide sempre più complesse del mondo digitale: la consapevolezza acquisita durante il corso rappresenta un primo passo fondamentale per i Dipendenti e per l'Agenzia, nell'ottica di contribuire a creare un ambiente di lavoro più sicuro e resiliente.

Il Referente per la Cybersicurezza
dott. Massimo Di Guida

Il Responsabile Progetto PNRR
dott.ssa Loredana La Via