Finanziato dall'Unione europea NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

ARPAC CAMPANIA

Progetto PNRR M1C1 | 1.5 – Cybersecurity
“Assessment e potenziamento della resilienza cyber di ARPAC”

Potenziamento della Cybersecurity del Personale Amministrativo, del Personale IT, e del Comitato di Crisi
Relazione finale

INDICE

1. Introduzione

La formazione rappresenta un elemento fondamentale e imprescindibile per garantire la sicurezza, l'efficacia operativa e la resilienza di un'organizzazione moderna, soprattutto in un contesto tecnologico e normativo in continua evoluzione. Il presente calendario raccoglie le sessioni di formazione che Deloitte ha erogato presso l'Agenzia Regionale per la Protezione Ambientale della Campania (di seguito ARPAC) nell'ambito del Progetto PNRR M1C1 | 1.5 – Cybersecurity. Tali iniziative sono state rivolte al personale della U.O. Sistemi Informativi e Informatici, al Personale Amministrativo, e ai membri del Comitato di Crisi dell'Agenzia, con l'obiettivo di sviluppare competenze specifiche e una consapevolezza condivisa sui temi della sicurezza informatica e della gestione di tali rischi.

Le iniziative di formazione e sensibilizzazione hanno assunto un ruolo sempre più cruciale all'interno delle organizzazioni, soprattutto in considerazione delle recenti evoluzioni normative a livello nazionale ed europeo. Questi aggiornamenti legislativi stabiliscono infatti precisi obblighi e standard riguardanti la formazione in materia di cybersicurezza. In particolare, la Direttiva (UE) 2022/2555, il Decreto Legislativo 138/2024 e la determinazione n. 379907 dell'Agenzia per la Cybersicurezza Nazionale (ACN) del 24 dicembre 2025 sanciscono l'obbligo per gli organi direttivi di adottare e promuovere programmi formativi specifici, volti a rafforzare le competenze e la consapevolezza in ambito di sicurezza informatica, protezione delle informazioni e cybersicurezza. Tali requisiti normativi sottolineano l'importanza di un approccio strutturato e continuo alla formazione, che coinvolga tutti i livelli organizzativi, a partire dalla leadership, per garantire una gestione efficace e responsabile dei rischi digitali.

La formazione a 360 gradi è essenziale per creare una cultura della sicurezza diffusa e integrata, capace di prevenire e gestire efficacemente le minacce digitali, quali malware, ransomware e attacchi di ingegneria sociale. Per il Personale IT della U.O. Sistemi Informativi e Informatici, i corsi hanno approfondito aspetti tecnici fondamentali come la gestione degli incidenti in conformità con le normative vigenti (NIS2, D.Lgs. 138/2024, disposizioni dell'ACN) e l'utilizzo di Playbook specifici per la risposta a scenari quali Malware/Ransomware, Phishing e Data Breach. Parallelamente, il Personale Amministrativo ha potuto acquisire consapevolezza e competenze sulla Business Impact Analysis (BIA), strumento chiave per valutare e mitigare i rischi operativi. Infine, il Comitato di Crisi dell'Agenzia ha partecipato ad una esercitazione di Table Top il cui scopo è stato testarne la capacità decisionale e di risposta, sulla base di uno scenario di crisi ignoto, configuratosi poi come un attacco ransomware. Tale esercizio ha permesso di migliorare la capacità decisionale strategica e il coordinamento agenziale in situazioni emergenziali.

L'importanza di un percorso formativo continuo risiede nella necessità di mantenere aggiornate le competenze e di adattarsi rapidamente ai nuovi scenari di rischio, garantendo così una protezione efficace e proattiva dell'organizzazione. Attraverso un impegno costante nella formazione è possibile costruire una difesa solida, capace di integrare tecnologia, processi e persone, e di sostenere la crescita e la sicurezza dell'Agenzia nel lungo termine.

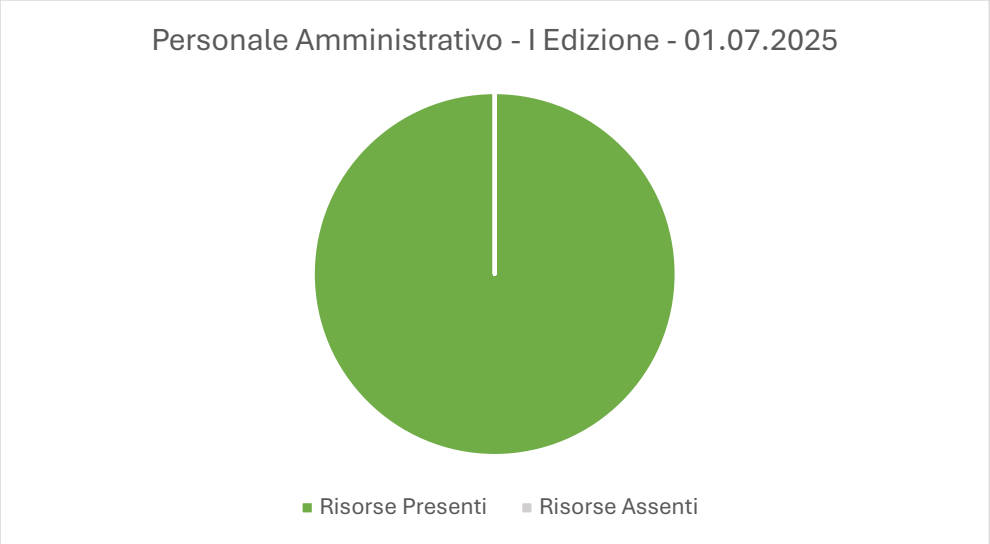
2. Formazione erogata

Nell'ambito dell'iniziativa progettuale PNRR M1C1 | 1.5 - Cybersecurity, in risposta al fabbisogno formativo rilevato presso l'ARPAC, è stato organizzato un ciclo di sessioni formative mirate, volto a rafforzare la consapevolezza, le competenze e la preparazione del personale in ambito cybersecurity. È emersa la necessità di incrementare il livello di consapevolezza e di competenza tecnica rispetto alle minacce cyber contemporanee, nonché di consolidare i processi organizzativi di risposta agli incidenti di sicurezza informatica e di continuità operativa. Tale esigenza è stata identificata sia in considerazione dell'evoluzione del panorama delle minacce informatiche, sia in risposta agli obblighi normativi nazionali ed europei in materia di cybersecurity e protezione dei dati.

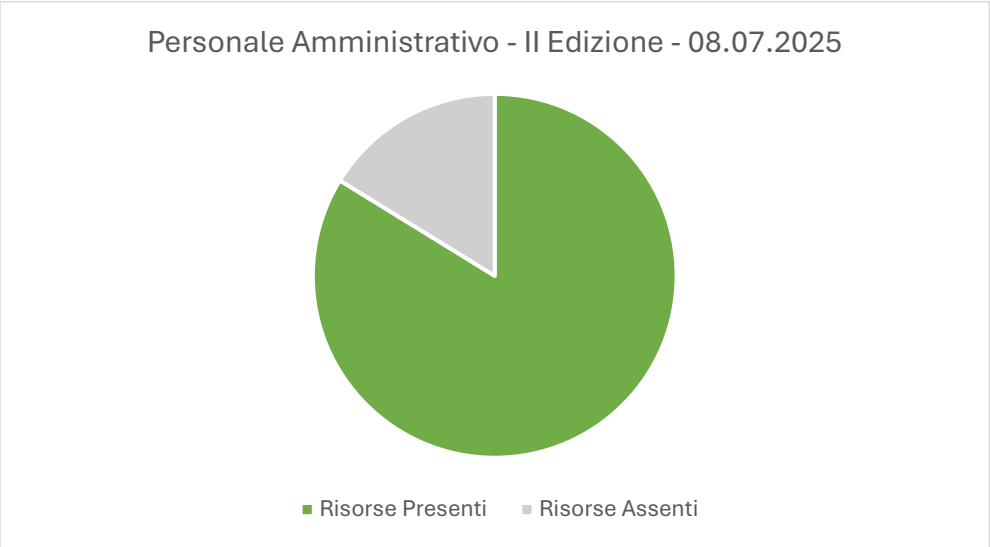
Il programma formativo è stato progettato e strutturato secondo un approccio differenziato e modulare, articolato in base alle diverse categorie di risorse operanti all'interno dell'Agenzia, con l'obiettivo di garantire una preparazione specifica e coerente con i rispettivi ruoli e responsabilità istituzionali. Il ciclo formativo ha coinvolto il Personale Amministrativo, il Personale Tecnico-Informatico appartenente all'Unità Operativa Sistemi Informativi e Informatici, nonché i componenti del Comitato di Crisi agenziale.

Tematiche affrontate durante la formazione:

- **Business Impact Analysis e Continuità Operativa** – Personale Amministrativo: le due sessioni dedicate al personale amministrativo hanno fornito una comprensione approfondita e dettagliata degli scenari che possono determinare interruzioni significative nella normale operatività dell'Agenzia. È stata illustrata la metodologia della Business Impact Analysis (BIA), strumento fondamentale per stimare e valutare l'impatto potenziale di tali interruzioni sui processi di business. Attraverso questo processo, è possibile prevedere le conseguenze operative e organizzative derivanti da eventi critici, identificando contestualmente le azioni prioritarie da intraprendere per mitigare i rischi. Inoltre, sono state approfondite le strategie di continuità operativa, con particolare riferimento alle modalità di redazione, agli obiettivi e all'importanza del Piano di Continuità Operativa (BCP) quale documento guida per garantire la resilienza e la ripresa tempestiva delle attività essenziali.



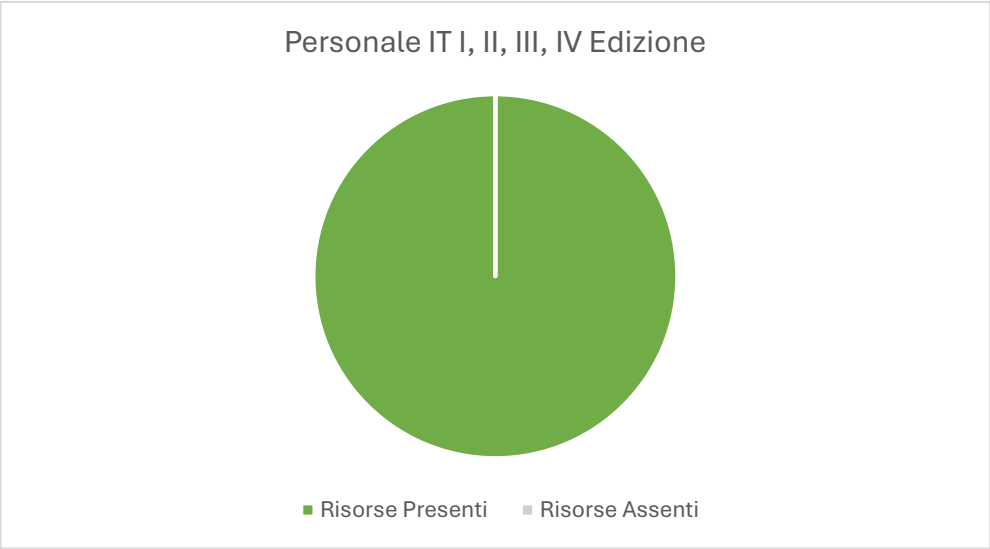
Alla prima sessione formativa per il Personale Amministrativo ha partecipato il 100% delle 35 risorse invitate.



Alla seconda sessione formativa per il Personale Amministrativo hanno partecipato 31 delle 37 risorse invitate, l'84% del totale.

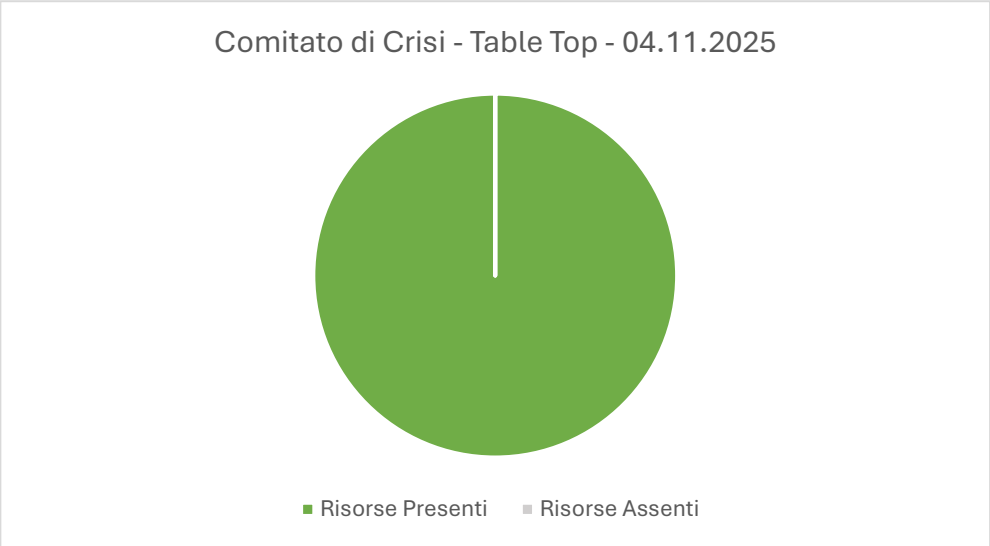
- **Gestione degli Incidenti di Sicurezza Informatica** – Personale IT (Unità Operativa Sistemi Informativi e Informatici): per il personale tecnico-informatico sono state erogate quattro sessioni formative specifiche, finalizzate a consolidare le competenze operative e procedurali necessarie per la gestione efficace degli incidenti di sicurezza informatica:
    - **Gestione Incidenti:** è stato illustrato in dettaglio il processo di gestione degli incidenti di sicurezza aggiornato in conformità con la Direttiva NIS2 e il D.Lgs. 138/2024, con particolare attenzione alla definizione dei ruoli e delle responsabilità, alle modalità di comunicazione interna ed esterna durante le fasi di emergenza, nonché alle procedure operative per la ripresa delle attività in sicurezza.
    - **Playbook Malware:** è stata fornita, illustrata e approfondita una guida pratica per l'identificazione tempestiva e l'isolamento dei sistemi compromessi da software dannoso, nonché per la rimozione efficace del malware e l'implementazione di strategie preventive volte a ridurre il rischio di future infezioni.
    - **Playbook Phishing:** sono state approfondite le metodologie per il riconoscimento di e-mail sospette e potenzialmente dannose, con particolare riguardo alla formazione continua del personale, all'adozione di filtri di sicurezza avanzati e alle procedure di risposta rapida per la gestione di sistemi eventualmente compromessi da attacchi di phishing.
    - **Playbook Data Breach:** è stata presentata una guida operativa per la gestione delle violazioni dei dati personali e sensibili, che ha coperto tutte le fasi fondamentali, dall'identificazione e contenimento dell'incidente, all'analisi e al recupero delle informazioni compromesse. Sono state inoltre illustrate le misure preventive da adottare, quali l'utilizzo di tecniche di crittografia, l'implementazione di controlli di accesso rigorosi, il monitoraggio continuo degli

eventi di sicurezza e la comunicazione tempestiva e trasparente con le parti interessate, in conformità con la normativa vigente.



Alle 4 sessioni di formazione ha partecipato il 100% delle 8 risorse invitate.

- **Esercitazione Table Top - Comitato di Crisi**: è stata condotta un'esercitazione di tipo Table Top, incentrata su uno scenario di attacco ransomware, con l'obiettivo di simulare un incidente reale e valutare in modo critico le modalità di risposta e gestione adottate dall'Agenzia. Questa attività ha rappresentato un'importante occasione per il Comitato di Crisi di consolidare le conoscenze teoriche acquisite durante il percorso formativo, testare l'efficacia dei processi di gestione della crisi informatica e sviluppare una maggiore consapevolezza operativa nella gestione di scenari di emergenza complessi. L'esercitazione ha altresì permesso di individuare eventuali aree di miglioramento, contribuendo così al rafforzamento complessivo della capacità di reazione e resilienza dell'Agenzia di fronte a minacce cyber.



Alla sessione di Table Top hanno preso parte 13 risorse, pari al 100% degli invitati, tenuto conto che due membri originariamente convocati sono stati sostituiti da personale qualificato in loro rappresentanza.

Il Referente per la cybersicurezza

Dott. Massimo Di Guida

Il Responsabile Progetto PNRR

Dott.ssa Loredana La Via