Progetto PNRR M1C1 | 1.5 – Cybersecurity
“Assessment e potenziamento della resilienza cyber di ARPAC”
Calendario attività formative
Potenziamento della Cybersecurity del Personale Amministrativo, del Personale IT, e del Comitato di Crisi
Anno 2025

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. Calendario

2.1 Personale Amministrativo

Di seguito si riporta il calendario delle sessioni di formazione erogate verso il Personale Amministrativo dell'Agenzia.

Le sessioni, a cui hanno partecipato 66 risorse dell'Agenzia, sono state erogate in presenza, e hanno avuto come oggetto l'introduzione al processo di Business Impact Analysis e della Continuità Operativa.

Numero Sessione	Data
Sessione 1 – BIA	1° luglio 2025 (10:00-13:00)
Sessione 2 - BIA	8 luglio 2025 (10:00-13:00)

2.2 Personale IT

Di seguito si presenta il calendario delle quattro sessioni formative rivolte al personale dell'U.O. Sistemi Informativi e Informatici, finalizzate a rafforzare le competenze in ambito di sicurezza informatica. Le attività hanno riguardato: la gestione degli incidenti di sicurezza e l'analisi approfondita di tre Playbook specifici dedicati rispettivamente agli scenari di crisi di malware, data breach e phishing.

Numero Sessione	Data
Sessione 1 – Gestione Incidenti	18 settembre 2025 (10:00-13:00)
Sessione 2 – Playbook Malware/Ransomware	25 settembre 2025 (10:00-13:00)
Sessione 3 – Playbook Data Breach	2 ottobre 2025 (10:00-13.00)
Sessione 4 – PlayBook Phishing	9 ottobre 2025 (10:00-13:00)

2.3 Comitato di Crisi

In data 4 novembre 2025 è stata condotta una sessione operativa della durata complessiva di quattro ore e trenta minuti, dedicata all'esecuzione di un'esercitazione di tipo "Table Top". Tale attività ha avuto come obiettivo principale la simulazione di uno scenario di incidente informatico reale, sconosciuto ai partecipanti, al fine di testare e valutare in modo approfondito le modalità di risposta e gestione adottate dall'Agenzia in caso di potenziali eventi di sicurezza informatica.

L'esercitazione ha coinvolto un totale di tredici risorse, rappresentanti i membri del Comitato di Crisi dell'ARPAC, che hanno partecipato attivamente alla simulazione, contribuendo con le proprie competenze e responsabilità specifiche. L'iniziativa ha permesso di analizzare criticamente le procedure operative esistenti, identificare eventuali criticità e aree di miglioramento, nonché rafforzare la capacità di coordinamento e reazione dell'Agenzia di fronte a possibili minacce informatiche.

Questa attività rientra nell'ambito delle misure preventive e di gestione del rischio adottate dall'Agenzia per garantire la continuità operativa e la tutela delle informazioni sensibili, in linea con le normative vigenti in materia di sicurezza informatica e protezione dei dati.

Il Referente per la cybersicurezza
Dott. Massimo Di Guida

Il Responsabile Progetto PNRR
Dott.ssa Loredana La Via