Progetto PNRR M1C1 I 1.5 – Cybersecurity

” Assessment e potenziamento della resilienza cyber di ARPAC”

Calendario attività formative

Potenziamento della Cybersecurity & Data Protection Awareness dei dipendenti agenziali

Anno 2025

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 Aziendali, oltre che in relazione all'identità digitale di ogni singola persona coinvolta.

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 Agenzia per la Cybersicurezza Nazionale (ACN) 379907 del 24 dicembre 2025 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 si riporta il calendario delle attività formative svolte nonché il macro-contenuto del programma per le attività che hanno coinvolto il personale Dirigente, il Personale del Comparto della Struttura Centrale e il Personale dei Dipartimenti Provinciali dislocati sul territorio, comprensivo anche della U.O.C. Siti Contaminati e Bonifiche.

Programma e Calendario Formativo

Al fine di definire un programma formativo consistente per il Personale aziendale è stata effettuata un'attività di pianificazione e di raccolta delle informazioni relative alle esigenze formative dei Dipendenti di ARPAC. Di conseguenza, il materiale utilizzato è stato focalizzato su aspetti generali relativi alla sicurezza delle informazioni e cybersecurity e con approfondimenti ad-hoc su tematiche verticali connesse alle buone prassi di igiene informatica. 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 e 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;
- **Definizione di nuovi processi interni,** ove è stata fornita una panoramica sullo stato delle attività intraprese dall'Agenzia per migliorare la propria postura Cyber, con particolare focus sulla revisione e l'aggiornamento delle policy e delle procedure interne;
- **Pratiche di igiene Informatica,** ove sono state analizzate, a titolo esemplificativo, le principali best practices relative alla navigazione online, scelta della password e sicurezza dei dispositivi per identificare le aree di miglioramento necessarie per garantire la sicurezza delle informazioni. Sono stati anche 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 e a seguire le best practices.

A valle della definizione del materiale formativo è stata programmata l'erogazione delle attività con sedute formative differenziate sulla base delle esigenze di ciascuna area inclusa, in particolare mediante:

- **Workshop in aula**: sessioni interattive condotte da esperti, che offrono opportunità di discussione e 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.

Tale approccio ibrido ha garantito che il Personale ARPAC, indipendentemente dalla loro posizione o orario di lavoro, potessero avere la possibilità di partecipare attivamente alla formazione. Di seguito si riporta la calendarizzazione delle attività eseguite nel periodo di riferimento:

❖ Personale Dirigente – I Edizione

Numero sessione	Data	Modalità di erogazione
Sessione 1 – mattina	14 Marzo 2025	Workshop in aula
Sessione 2 - pomeriggio		
Sessione Recupero	19 Marzo 2025	Sessione di formazione da remoto

❖ Personale Dirigente – II Edizione

Numero sessione	Data	Modalità di erogazione
Sessione 1 – mattina	7 Ottobre 2025	Workshop in aula
Sessione 2 - pomeriggio		
Sessione Recupero	14 Ottobre 2025	Sessione di formazione da remoto

❖ Personale dei Dipartimenti, comprensivo anche della U.O.C. Siti Contaminati e Bonifiche, e personale del Comparto centrale

Area	Numero sessione	Data	Modalità di erogazione
Dipartimento di Salerno	Sessione 1 – mattina	24 Marzo 2025	Sessione di formazione da remoto
	Sessione 2 - pomeriggio		
Dipartimento di Benevento	Sessione 1 – mattina	28 Marzo 2025	Workshop in aula
	Sessione 2 - pomeriggio		
Dipartimento di Caserta	Sessione 1 – mattina	01 Aprile 2025	Workshop in aula
	Sessione 2 - pomeriggio		
Dipartimento di Napoli	Sessione 1 – mattina	07 Aprile 2025	Workshop in aula
	Sessione 2 - pomeriggio		
Dipartimento di Avellino	Sessione 1 – mattina	09 Aprile 2025	Sessione di formazione da remoto
	Sessione 2 - pomeriggio		

Area	Numero sessione	Data	Modalità di erogazione
Comparto Centrale e U.O. Siti Contaminati e Bonifiche	Sessione 1 – mattina	14 Aprile 2025	Sessione di formazione da remoto
	Sessione 2 - pomeriggio		
Sessione Recupero	Sessione singola	16 Aprile 2025	Sessione di formazione da remoto

Il Referente per la Cybersicurezza

dott. Massimo Di Guida

Il Responsabile Progetto PNRR

dott.ssa Loredana La Via