

Obiettivo: Adozione e messa a sistema della governance della cybersicurezza di Arpal attraverso il potenziamento delle modalità di prevenzione e gestione degli incidenti informatici e la formazione del personale.

Indicatore: % misure attuate nell'ambito del finanziamento PNRR dedicato

Target: 1) >90% - 0,8) fra 75% e 90% - 0,6) fra 60% e 74% - 0) <60%

Il progetto "CYBER ARPAL" è stato approvato dall'Agenzia per la Cybersicurezza Nazionale (ACN) nell'ambito dell'Avviso pubblico n. 8/2024 (Investimento 1.5 "Cybersecurity" del PNRR).

L'obiettivo è potenziare la resilienza cyber dell'Agenzia Regionale per la Protezione dell'Ambiente Ligure (ARPAL), con un finanziamento integrale di € 1.474.930,00.

ARPAL interviene su tutte le linee di azione previste (dalla Governance e programmazione, alla Gestione del rischio e degli incidenti, fino alla Sicurezza delle applicazioni e delle reti).

Il progetto, avviato a fine 2024, è in linea con quanto previsto e lo stato di avanzamento complessivo stimato è a oltre l'80%. Prevede entro la fine del 2025 interventi nelle seguenti macro-aree:

- Analisi della postura di sicurezza e definizione di un piano di potenziamento.
- Miglioramento dei processi e dell'organizzazione.
- Formazione e aumento della consapevolezza del personale.
- Progettazione e sviluppo di nuovi sistemi e tecnologie.

Tra le attività già avviate figurano l'acquisizione di una piattaforma di e-learning, corsi di formazione specialistica, servizi di Vulnerability Assessment e Penetration Test, l'adesione al Polo Strategico Nazionale (PSN) e il potenziamento di apparati di sicurezza perimetrale.

Le attività delineate nel progetto sono 21, in alcuni casi a livello esecutivo sono state ulteriormente spaccettate. Tra loro poi molte sono interconnesse.

Per semplicità le riportiamo di seguito con lo stato di avanzamento "mediato" sulle attività di dettaglio che le compongono.

Riga	Intervento	Tipologia di intervento	Attività	Stato avanzamento
ACN8_1_A	1. Governance e programmazione cyber	A. Analisi della postura di sicurezza e definizione di un piano di potenziamento	Attività di Security Posture Assessment in relazione al Framework Nazionale per la Cyber Security e la Data Protection	60 %
ACN8_1_B	1. Governance e programmazione cyber	B. Miglioramento dei processi e dell'organizzazione	Security Awareness and Training	60%
ACN8_1_C	1. Governance e programmazione cyber	C. Formazione e miglioramento della consapevolezza delle persone	Corsi di formazione, infografiche, campagne di phishing	100%
ACN8_1_D	1. Governance e programmazione cyber	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Attività di Vulnerability Assessment e Penetration Test sulle componenti infrastrutturali e relativa reportistica	70%
ACN8_2_B	2. Gestione del rischio cyber e della continuità operativa	B. Miglioramento dei processi e dell'organizzazione	Procedure per la gestione in tempo reale di minacce e anomalie comportamentali e delle minacce, migliorando la visibilità della sicurezza e la conformità normativa	50%

ACN8_2_C	2. Gestione del rischio cyber e della continuità operativa	C. Formazione e miglioramento della consapevolezza delle persone	Formazione per il personale tecnico	100%
ACN8_2_D1	2. Gestione del rischio cyber e della continuità operativa	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Implementazione sistemi di backup, Soluzioni Digital Risk Protection Service, Sandbox	50%
ACN8_2_D2	2. Gestione del rischio cyber e della continuità operativa	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Servizi NDR	40%
ACN8_3_C	3. Gestione e risposta agli incidenti di sicurezza	C. Formazione e miglioramento della consapevolezza delle persone	Formazione diffusa e awareness	80%
ACN8_3_D	3. Gestione e risposta agli incidenti di sicurezza	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Potenziamento apparati di sicurezza perimetrale e aggiornamento apparati di rete	70%
ACN8_4_B	4. Gestione delle identità digitali e degli accessi logici	B. Miglioramento dei processi e dell'organizzazione	Identity & Access Management personalizzato	30%
ACN8_4_C	4. Gestione delle identità digitali e degli accessi logici	C. Formazione e miglioramento della consapevolezza delle persone	Formazione diffusa sulle modalità di accesso ai sistemi	80%
ACN8_4_D1	4. Gestione delle identità digitali e degli accessi logici	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Network Access Control comprensivo di servizi professionali	70%
ACN8_4_D2	4. Gestione delle identità digitali e degli accessi logici	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Revisione dei sistemi di accesso fisico alle sedi e alle stanze	50%
ACN8_5_A	5. Sicurezza delle applicazioni, dei dati e delle reti	A. Analisi della postura di sicurezza e definizione di un piano di potenziamento	Analisi approfondita della postura applicativa e infrastrutturale delle reti di monitoraggio e dei software di raccolta dati gestionali	50%
ACN8_5_B	5. Sicurezza delle applicazioni, dei dati e delle reti	B. Miglioramento dei processi e dell'organizzazione	Implementazione di sistema di difesa delle applicazioni web e API da minacce	60%
ACN8_5_C	5. Sicurezza delle applicazioni, dei dati e delle reti	C. Formazione e miglioramento della consapevolezza delle persone	Formazione specifica agli amministratori delle reti di monitoraggio anche con riferimento alla direttiva NIST/NIS2	80%
ACN8_5_D1	5. Sicurezza delle applicazioni, dei dati e delle reti	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Acquisizione di sistemi per la gestione della sicurezza fisica delle stazioni delle reti di monitoraggio	70%
ACN8_5_D2	5. Sicurezza delle applicazioni, dei dati e delle reti	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Aggiornamento dei software gestionali in ottemperanza alla direttiva NIST/NIS2	70%
ACN8_5_D3	5. Sicurezza delle applicazioni, dei dati e delle reti	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Protezione degli apparati OT, monitoraggio delle trasmissioni e dei relativi dati	70%
			PROGETTO	87.6%