Progetto "CYBER ARPAL"

Potenziamento della resilienza cyber dell'Agenzia Regionale per la Protezione dell'Ambiente Ligure

Il progetto CYBER ARPAL, finanziato nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR) Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" (Avviso 08/2024), è stato portato interamente a compimento. L'iniziativa ha visto un investimento complessivo di € 1.474.930,00, finalizzato a trasformare la postura di sicurezza dell'Agenzia e a proteggere l'integrità dei dati, critici non solo per la tutela del territorio ma anche per la sanità pubblica e la protezione civile.

Grazie alla collaborazione strategica con Liguria Digitale e al coinvolgimento di partner istituzionali e privati di valore, ARPAL si può considerare un ente resiliente e tecnologicamente all'avanguardia. Il progetto CYBER ARPAL non ha solo messo in sicurezza l'infrastruttura ICT, ma ha consolidato una vera e propria cultura della sicurezza all'interno dell'organizzazione, garantendo l'affidabilità e la disponibilità costante delle informazioni ambientali-sanitarie e di protezione civile.

L'attuazione ha riguardato cinque macro-aree di intervento, tutte completate con successo:

- Governance e Programmazione Cyber: ARPAL ha completato un'estesa valutazione della propria postura di sicurezza, analizzando vulnerabilità e minacce per allinearsi alle migliori pratiche del settore. Parallelamente, è stato avviato un programma di miglioramento dei processi organizzativi e di revisione della conformità normativa, affiancato da servizi di Security Awareness e Incident Readiness. Un pilastro fondamentale del completamento di questo intervento è stata la formazione del personale, mirata a elevare la consapevolezza interna su temi critici quali il phishing e la gestione sicura delle credenziali, riducendo così il rischio derivante dal fattore umano.
- Gestione del rischio cyber e della continuità operativa: ARPAL ha completato il potenziamento dei sistemi dedicati alla resilienza operativa, adottando un approccio olistico per garantire la protezione dei processi critici. Le attività hanno portato all'implementazione di strumenti di rilevazione in tempo reale di minacce e anomalie comportamentali, migliorando sensibilmente la visibilità sulla sicurezza e la conformità normativa.
- Gestione e risposta agli incidenti di sicurezza: l'Agenzia ha completato il potenziamento delle proprie capacità di reazione, superando le limitazioni derivanti dalla carenza di personale con competenze verticali attraverso l'adozione di protocolli definiti e nuove tecnologie. Le attività hanno compreso una revisione critica delle politiche e delle procedure esistenti, adeguandole alle recenti evoluzioni normative e ai nuovi assetti organizzativi dell'Ente.
- Gestione delle identità digitali e degli accessi logici: l'Agenzia ha completato la transizione verso un modello di gestione degli accessi evoluto, superando i sistemi basati su singolo fattore per adottare un approccio Zero Trust. È stata inoltre attivata la piattaforma NAC (Network Access Control), che permette di regolare l'accesso alla rete in base all'identità verificata e allo stato dei dispositivi. In linea con l'obiettivo di rafforzamento della resilienza, l'intervento ha incluso il potenziamento della sicurezza fisica delle sedi tramite sistemi di monitoraggio degli ingressi, l'utilizzo di chiavi elettroniche e badge, assicurando così un controllo capillare e integrato degli accessi sia logici che fisici agli asset dell'ente.
- Sicurezza di Reti e Applicazioni: l'Agenzia ha portato a compimento il potenziamento della sicurezza perimetrale e applicativa, con un focus particolare sulla protezione della rete di rilevamento della qualità dell'aria e della rete freatimetrica distribuite sul territorio (IoT/OT). La superficie d'attacco, ampliata dalla capillarità dei dispositivi remoti, è stata messa in sicurezza attraverso l'adozione di tecnologie per il monitoraggio dei flussi di comunicazione e l'installazione di nuovi firewall, sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS). In questo contesto, è stato inoltre sviluppato il rifacimento dell'OMIRL, garantendo una piattaforma tecnologica più robusta e sicura per la gestione dei dati meteo-idrologici.

Il progetto CYBER ARPAL si è concluso con il raggiungimento del 100% degli obiettivi prefissati riportati nella tabella in calce. L'impatto migliorativo è tangibile in tutte le funzioni del Cybersecurity Framework: dalla consapevolezza degli asset (Identify) alla robustezza delle misure preventive (Protect), fino alla capacità di monitoraggio proattivo (Detect) e alla reattività operativa (Respond).

In definitiva, l'investimento del PNRR non ha rappresentato solo un aggiornamento infrastrutturale, ma ha generato un mutamento strutturale nella gestione del rischio: l'Agenzia è oggi in grado di proteggere l'integrità dei dati ambientali e meteo-idrologici con standard di sicurezza elevati, garantendo un servizio affidabile, trasparente e resiliente di fronte alle sfide del panorama cyber attuale.

Direzione Amministrativa - Settore ICT
Via Bombrini 8 – 16149 Genova
PEC: arpal@pec.arpal.liguria.it
ict@arpal.liguria.it - www.arpal.liguria.it
C.F. e P.IVA 01305930107

Riga	Intervento	Tipologia di intervento	Attività
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
ACN8_1_B	*1. Governance e programmazione cyber*	B. Miglioramento dei processi e dell'organizzazione	Security Awareness and Training
ACN8_1_C	*1. Governance e programmazione cyber*	C. Formazione e miglioramento della consapevolezza delle persone	Corsi di formazione, infografiche, campagne di phishing
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
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
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
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
ACN8_2_D2	*2. Gestione del rischio cyber e della continuità operativa*	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Servizi NDR
ACN8_3_C	*3. Gestione e risposta agli incidenti di sicurezza*	C. Formazione e miglioramento della consapevolezza delle persone	Formazione diffusa e awareness
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

Direzione Amministrativa - Settore ICT
Via Bombrini 8 – 16149 Genova
PEC: arpal@pec.arpal.liguria.it
ict@arpal.liguria.it - www.arpal.liguria.it
C.F. e P.IVA 01305930107

ACN8_4_B	*4. Gestione delle identità digitali e degli accessi logici*	B. Miglioramento dei processi e dell'organizzazione	Identity & Access Management personalizzato
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
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
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
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
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
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
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
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 (OMIRL)
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

Il Responsabile per la Transizione Digitale

(Enrica Bongio)

Enrica Bongio
ARPAL
Dirigente
15.05.2026 16:56:02 GMT+02:00

Direzione Amministrativa - Settore ICT
Via Bombrini 8 – 16149 Genova
PEC: arpal@pec.arpal.liguria.it
ict@arpal.liguria.it - www.arpal.liguria.it
C.F. e P.IVA 01305930107