Progetto Innovazione e Digitalizzazione per Rafforzare la Sicurezza dei Dati Ambientali di ISPRA

Protezione dei dati e delle informazioni ambientali

Ing. Simona Ciattoni responsabile unità di missione Innovazione Digitale e Semplificazione

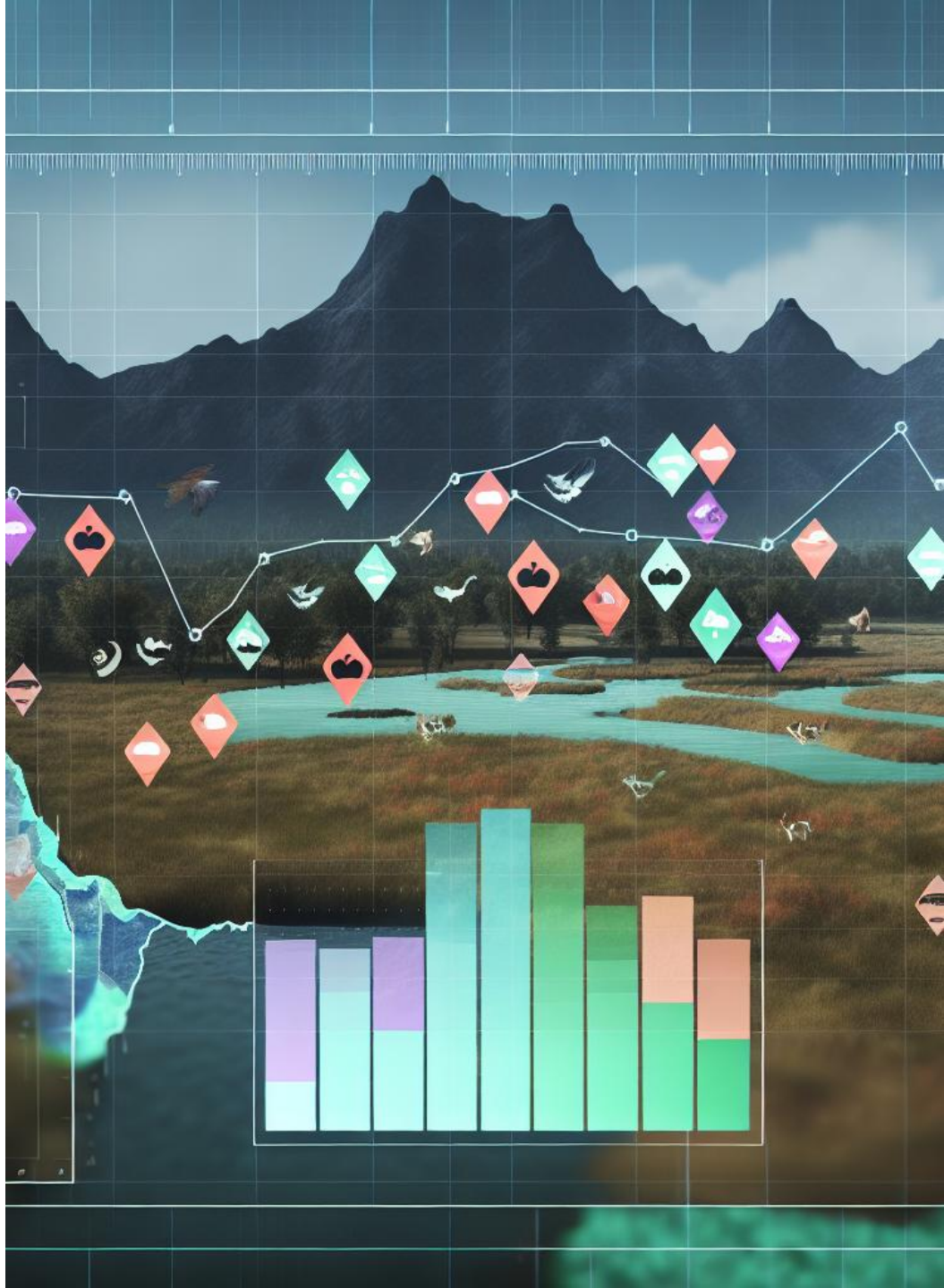
Dott. Guido Scatena responsabile sezione Reti e Sicurezza Telematica

Banca Dati di Indicatori Territoriali e Ambientali ISPRA

- La **banca dati di indicatori territoriali e ambientali ISPRA, con oltre 300 dataset e servizi ambientali connessi, rappresenta la più completa raccolta di dati sullo stato dell'ambiente in Italia**.

- Collaborazione: Questo patrimonio informativo è realizzato e curato in collaborazione con le Agenzie regionali e delle province autonome per la protezione dell'ambiente, che insieme costituiscono il Sistema Nazionale per la Protezione dell'Ambiente (SNPA).

- Accessibilità: Deve essere accessibile a una vasta gamma di soggetti, sia pubblici che privati per scopi:
  - Politiche ambientali
  - Pianificazione territoriale
  - Monitoraggio locale
  - Ricerca scientifica
  - Campagne di sensibilizzazione
  - Promozione dello sviluppo sostenibile.



Oltre la semplice raccolta e archiviazione dei dati ambientali

La Nostra Missione nella Gestione dei Dati Ambientali è un impegno verso l'efficienza e la trasparenza

Obbligo di garantire

- Disponibilità: dati e servizi sempre disponibili per gli utenti autorizzati
- Affidabilità: dati integri e non soggetti a manomissioni
- Accessibilità: facilmente accessibili e comprensibili grazie a formati interoperabili.

La Nostra Missione nella Gestione dei Dati Ambientali

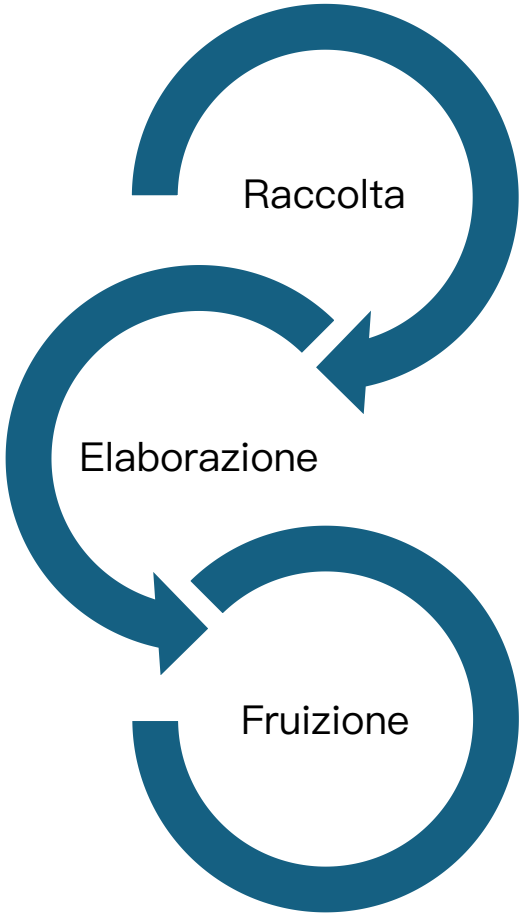
In un era di **minacce Cibernetiche** in continua evoluzione.

Necessario mettere in atto **misure di sicurezza** adeguate per far si che i **dati** ed i servizi siano non solo **accurati**, ma che non siano stati alterati, siano disponibili quando necessarie e protetti da accessi non autorizzati.

Esigenze ancora più stringenti quando i dati sono sensibili (GDPR). Nei sistemi ambientali possono esserci ad esempio dati sulla salute umana.

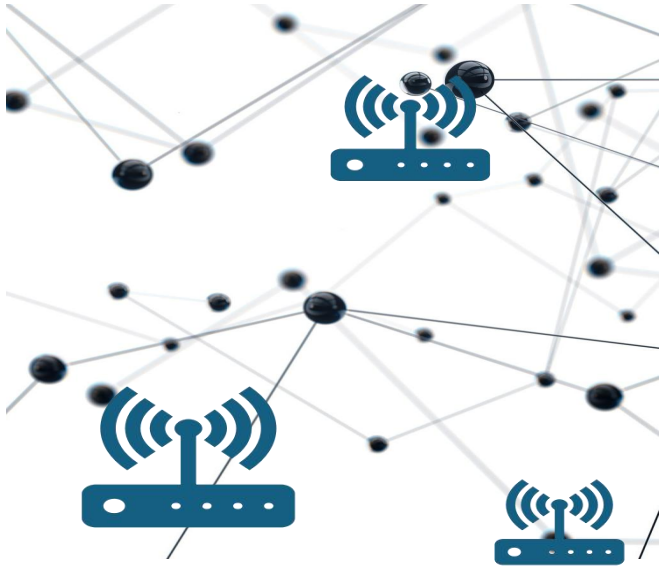
La Nostra Missione nella Gestione dei Dati Ambientali

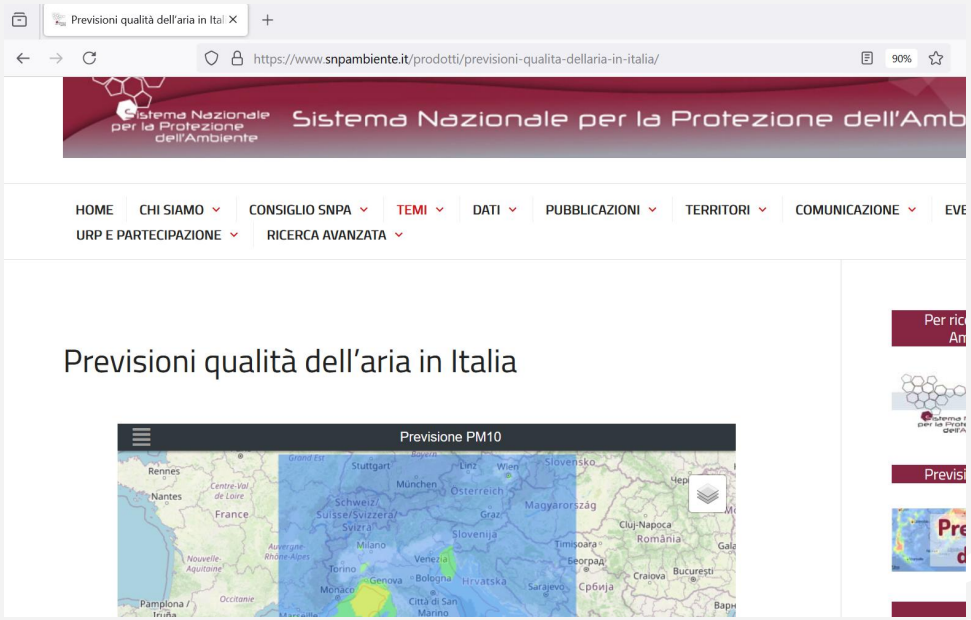
Sicurezza deve essere assicurata per ogni fase del ciclo di vita del dato



Scenari

Utilizzo di reti di monitoraggio ambientale che fa uso di sensori IoT distribuiti sul territorio e connessi in rete per raccogliere informazion in tempo reale.

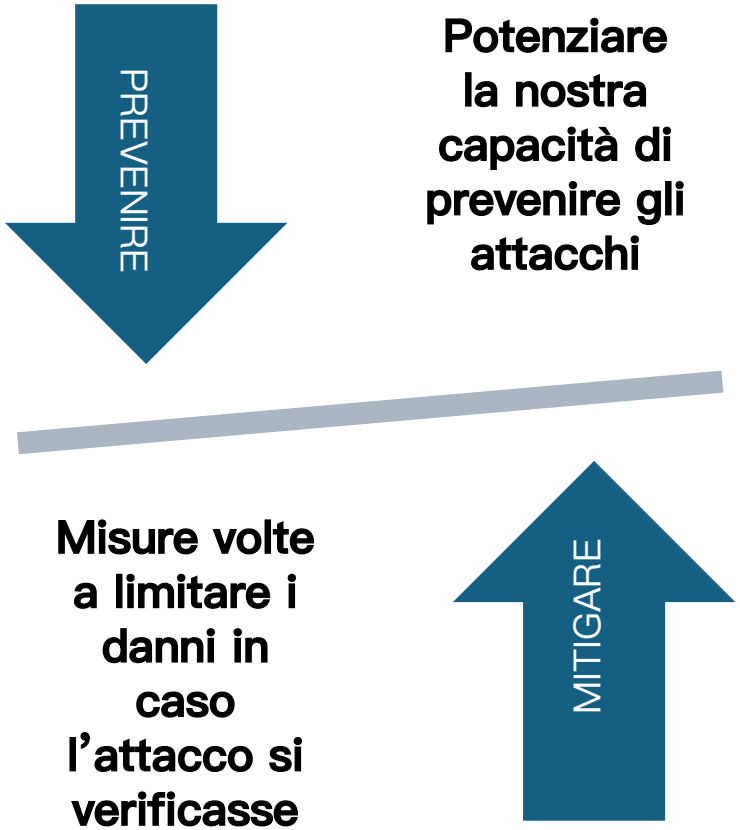




Dispositivi IoT apparentemente insignificanti possono mettere a rischio informazioni sensibili

Le piattaforme che gestiscono grandi quantità di dati territoriali e ambientali rappresentano un obiettivo appetibile per i criminali

La Nostra Visione Strategica come proteggere dati e servizi



Prima sfida: Scarsa consapevolezza interna del rischio cyber.

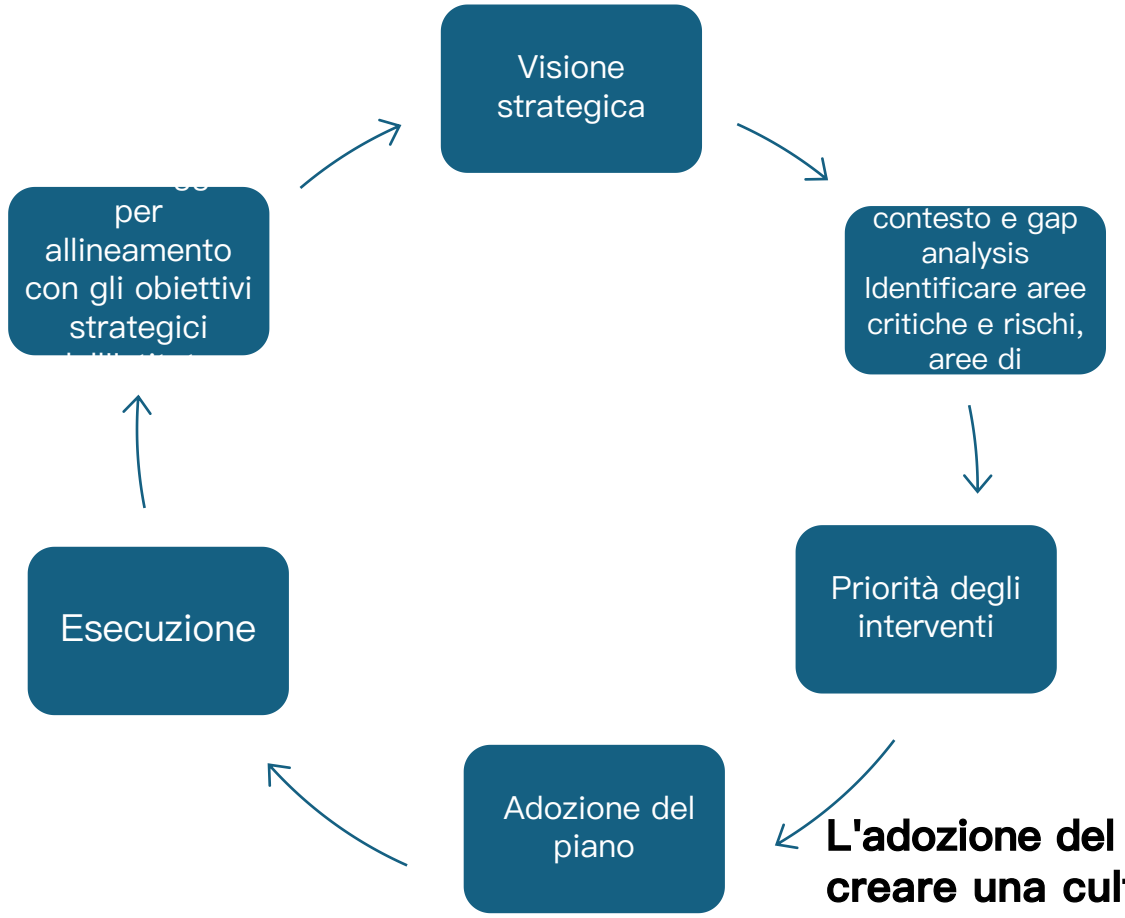
Approccio: prima azione, si è deciso di definire la visione strategica della sicurezza informatica dell'Istituto, basata su un approccio proattivo e a lungo termine.

Obiettivo: Creare una cultura interna di sicurezza che promuova la consapevolezza e la responsabilità.

Principi della strategia cybersecurity Ispra

Allineamento con Obiettivi Organizzativi	Integrare la sicurezza informatica negli obiettivi strategici dell'organizzazione, garantendo che le decisioni di sicurezza supportino il business.
Comprensione dei Rischi	Effettuare una valutazione dettagliata delle minacce e vulnerabilità, considerando sia i rischi interni che esterni.
Definizione di Politiche e Procedure	Stabilire un quadro normativo chiaro tramite lo sviluppo di politiche e procedure di gestione dei dati e delle risorse.
Investimenti in Tecnologia e Formazione	Destinare risorse a tecnologie di sicurezza e formazione continua per il personale.
Monitoraggio e Aggiornamento Continuo	Impegnarsi in un monitoraggio costante e revisioni periodiche delle strategie per adattarsi alle nuove minacce.
Cultura della Sicurezza	Promuovere una cultura aziendale in cui ogni dipendente riconosca l'importanza della sicurezza informatica.
Collaborazione e Condivisione delle Informazioni	Favorire la collaborazione con altre organizzazioni per la condivisione di informazioni sulle minacce e best practices

Piano per la Cybersicurezza



Questo approccio consente all'istituto adattare in modo dinamico la propria capacità di reazione e protezione di fronte ai rapidi cambiamenti del contesto, del panorama tecnologico e normativo, valutando continuamente il rischio e bilanciando le azioni preventive con le azioni di mitigazione in risposta agli attacchi.

L'adozione del piano sottolinea la volontà dei vertici dell'Istituto di creare una cultura interna della sicurezza, sensibilizzando tutti i dipendenti e promuovendo la collaborazione con altre organizzazioni, sia a livello nazionale che internazionale, per migliorare continuamente le pratiche di sicurezza informatica

Ostacoli e Opportunità

Ostacoli:

- Carenza di competenze tecniche interne.
- Limitate risorse economiche.

Opportunità:

- **Strategia Nazionale di Cybersicurezza**, il piano del governo italiano che mira a rafforzare la protezione dei dati e delle infrastrutture critiche del paese contro le minacce informatiche, grazieanche a fondi specifici (**Fondo per l'attuazione della Strategia nazionale di cybersicurezza** per aumentare l'autonomia tecnologica e rafforzare la sicurezza dei sistemi informativi nazionali– **Fondo per la gestione della cybersicurezza** per la gestione operativa della sicurezza)

ISPRA in collaborazione con ACN ha presentato il progetto *Intervento di innovazione e digitalizzazione per rafforzare la sicurezza dei dati e indicatori territoriali–ambientali strategici gestiti da ISPRA*

Il Progetto

- Finanziamento triennale (2024–2026) (decreto del Presidente Del Consiglio Dei Ministri 8 Luglio 2024 G.U. 04/09/2024) .
- Prevede una serie di azioni che mirano sia a prevenire il rischio di incidenti, sia a mitigare i danni in caso di loro verificarsi, intervenendo su aggiornamenti tecnologici sulla gestione strategica della sicurezza (governance) e l'accrescimento delle competenze

Misure previste

Governance della Sicurezza

- Definizione e Aggiornamento delle Policy Viene implementato un set di politiche di sicurezza che regolano accessi, protezione dei dati e gestione dei rischi che sono periodicamente aggiornate per allinearsi alle nuove normative e minacce emergenti
- Modello di Governance Strategica che definisce una chiara suddivisione di ruoli e responsabilità, garantendo che tutte le unità dell'Istituto abbiano compiti definiti in termini di sicurezza.
- Analisi del Rischio e BIA
- Compliance Normativa

Prevenzione

- Rafforzamento del controllo degli accessi, accedono solo utenti autorizzati con dispositivi autorizzati e che possono accedere solo alle risorse per le quali sono stati autorizzati,
- Penetration test: simulazioni di attacchi informatici per valutare la sicurezza dei sistemi IT, identificare vulnerabilità e azioni correttive e/o di mitigazione;
- Vulnerability Assessment: processo che identifica e valuta le debolezze in sistemi informatici. Trovare le falle prima che vengano sfruttate.

Mitigazione dei Danni

- Piano di Gestione degli Incidenti che definisce procedure standardizzate per la gestione degli incidenti, con la suddivisione chiara di ruoli e responsabilità.
- SOC (security operation center) un centro tecnologico con team dedicato che H24 sorveglia costantemente il traffico di rete e i sistemi IT, rilevando in tempo reale eventuali anomalie o minacce e garantisce una reazione rapida e centralizzata alle minacce

Crescita delle Competenze e Consapevolezza

- Trasferimento di Know how al personale tecnico
- Campagne di Security Awarenes e Phishing: Formazione periodica dei dipendenti per aumentare la consapevolezza sui rischi informatici, e simulazioni di attacchi prontezza del personale e fornire feedback in tempo reale.

CONCLUSIONI

- L'integrazione di piattaforme digitali avanzate per l'analisi e la condivisione degli indicatori territoriali e ambientali richiede una robusta infrastruttura di cybersecurity, una governance solida e competenze specializzate. È essenziale garantire la protezione dei dati, la sicurezza degli accessi e la prevenzione di attacchi informatici, trovando un equilibrio tra trasparenza e sicurezza. Solo così sarà possibile creare un ecosistema digitale resiliente, rafforzare la fiducia nei sistemi di monitoraggio e promuovere la partecipazione pubblica e la governance ambientale.
- In un contesto globale in cui le minacce alla sicurezza dei dati ambientali sono in continua evoluzione, è fondamentale che le istituzioni lavorino insieme per affrontare queste sfide comuni. La sicurezza dei dati ambientali non è solo una responsabilità di singoli enti, ma un obiettivo condiviso che richiede un impegno collettivo.
- auspichiamo pertatno una possibilità di collaborazione, con l'EEA ,e con l'intera rete Eionet

In tema cybersecurity: avere risorse e intelligence condivise migliora le posizioni di sicurezza di organizzazioni e Stati per l'obiettivo finale di proteggere le persone

CONCLUSIONI

- L'integrazione di piattaforme digitali avanzate per l'analisi e la condivisione degli indicatori territoriali e ambientali richiede una robusta infrastruttura di cybersecurity, una governance solida e competenze specializzate.
- È essenziale garantire la protezione dei dati, la sicurezza degli accessi e la prevenzione di attacchi informatici, trovando un equilibrio tra trasparenza e sicurezza.
- Solo così sarà possibile creare un ecosistema digitale resiliente, rafforzare la fiducia nei sistemi di monitoraggio e promuovere la partecipazione pubblica e la governance ambientale.
- In un contesto globale in cui le minacce alla sicurezza dei dati ambientali sono in continua evoluzione, è fondamentale che le istituzioni lavorino insieme per affrontare queste sfide comuni.
- La sicurezza dei dati ambientali non è solo una responsabilità di singoli enti, ma un obiettivo condiviso che richiede un impegno collettivo.

Auspichiamo una possibilità di collaborazione, con l'EEA e con l'intera rete Eionet, in tema cybersecurity avere risorse e intelligence condivise migliora le posizioni di sicurezza di organizzazioni e Stati per l'obiettivo finale di proteggere le persone