Oltre la sicurezza tecnica: lo scudo della dimostrabilità

Come trasformare la conformità NIS2 in un vantaggio dimostrabile

18 marzo 2026

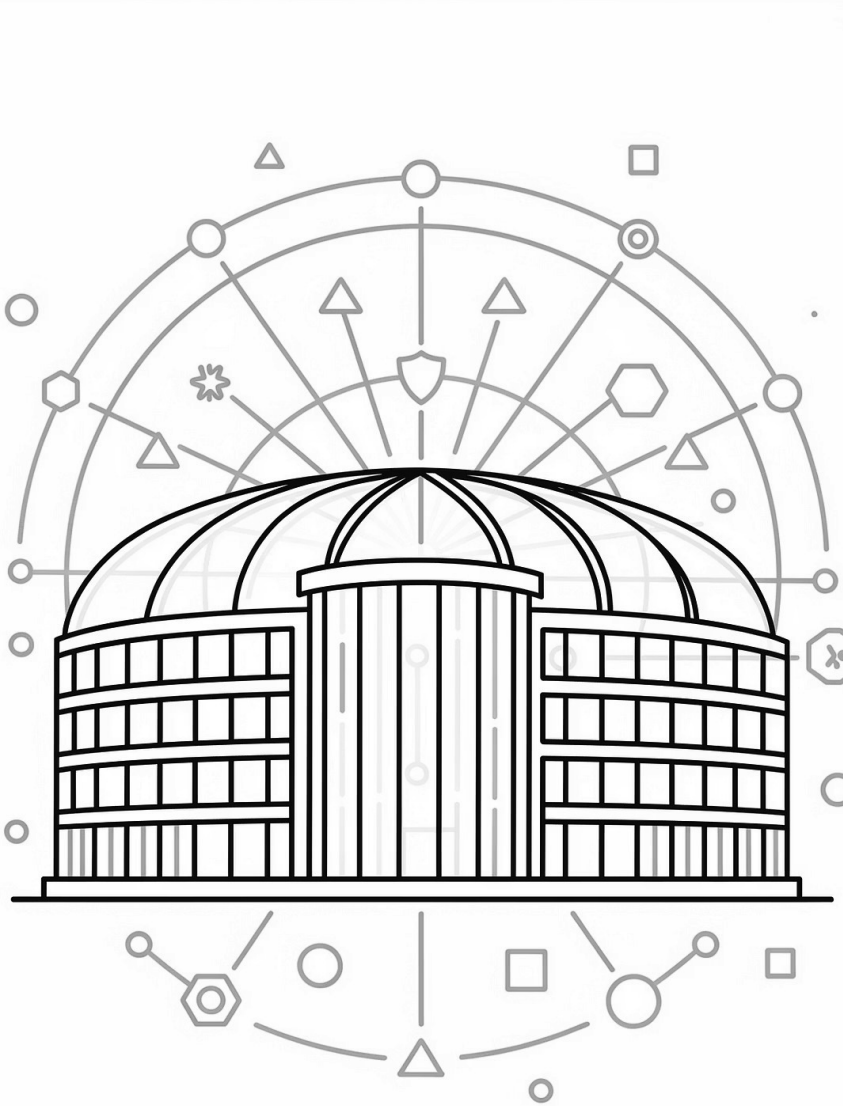
SMART FLOW
COMPLIANCE • DATA PROTECTION
CERTIFICAZIONI • SOSTENIBILITÀ

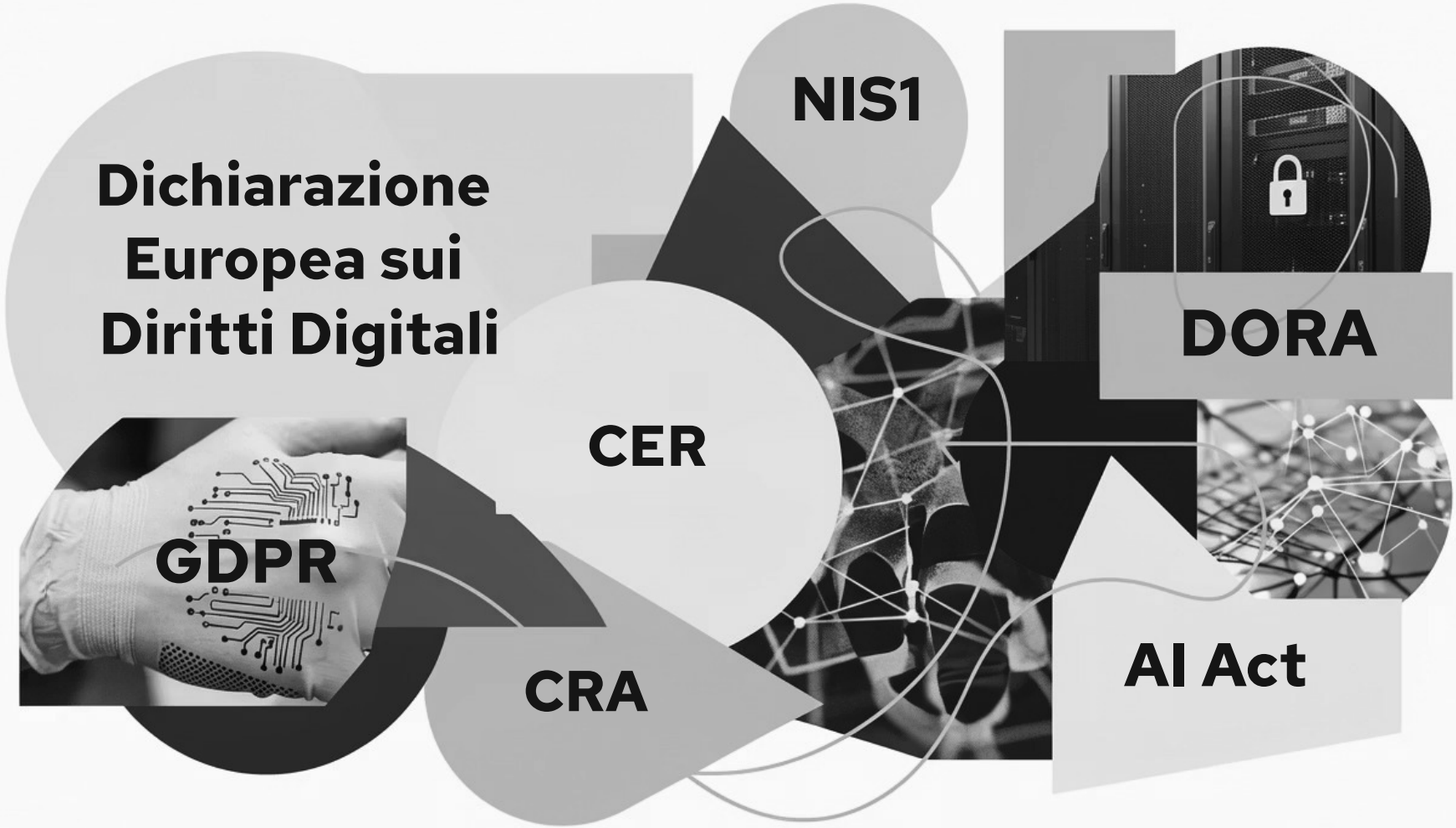
SOCIO SOSTENITORE 2026

Cosa è la NIS2

Dal 16 ottobre 2024 è in vigore la nuova direttiva Network and Information Security (NIS2), recepita con il D.Lgs. 4 settembre 2024, n. 138.

La direttiva mira a **garantire l'innalzamento del livello di sicurezza informatica** del tessuto produttivo e delle Pubbliche Amministrazioni, in armonia con gli altri Stati membri dell'Unione Europea.




Dichiarazione Europea sui Diritti Digitali
NIS1
DORA
CER
GDPR
CRA
AI Act

Gli adempimenti operativi fondamentali

1

Identificazione

Classificarsi come soggetto importante o essenziale secondo i criteri NIS2

2

Piattaforma ACN

Accreditarsi sulla piattaforma dedicata ACN e aggiornare le proprie informazioni ogni anno

3

Nuovi Obblighi

Sicurezza informatica, notifica degli incidenti, responsabilizzazione, formazione e supply chain

4

Ruolo CSIRT

Identificare il riferimento CSIRT e adeguarsi ai requisiti progressivamente rilasciati da ACN

Tutto questo non basta se non si può provarlo.
La conformità senza dimostrabilità rappresenta un rischio.

www.menti.com

Codice: **5627 0286**

La rivincita degli informatici

I membri degli **organi direttivi** sono **responsabili dell'approvazione** delle misure di gestione dei rischi e **della supervisione** della loro implementazione.

Cybersecurity vs Compliance

Cybersecurity

- **Focus:** Protezione tecnica e operativa dei sistemi, delle reti e dei dati.
- **Obiettivo:** Prevenire, rilevare, e mitigare attacchi informatici e vulnerabilità.
- **Domanda chiave:** "Siamo protetti da potenziali minacce?"

Compliance

- **Focus:** Adeguamento ai requisiti legali, normativi e contrattuali (es. NIS2).
- **Obiettivo:** Dimostrare l'esistenza e l'efficacia delle misure di sicurezza implementate.
- **Domanda chiave:** "Possiamo provare la nostra protezione e l'aderenza alle norme?"

> La NIS2 enfatizza che la cybersecurity non è solo una questione di efficacia, ma di **dimostrabilità** continua e verificabile.

Cybersecurity vs Compliance

L'imperativo della dimostrabilità nella compliance

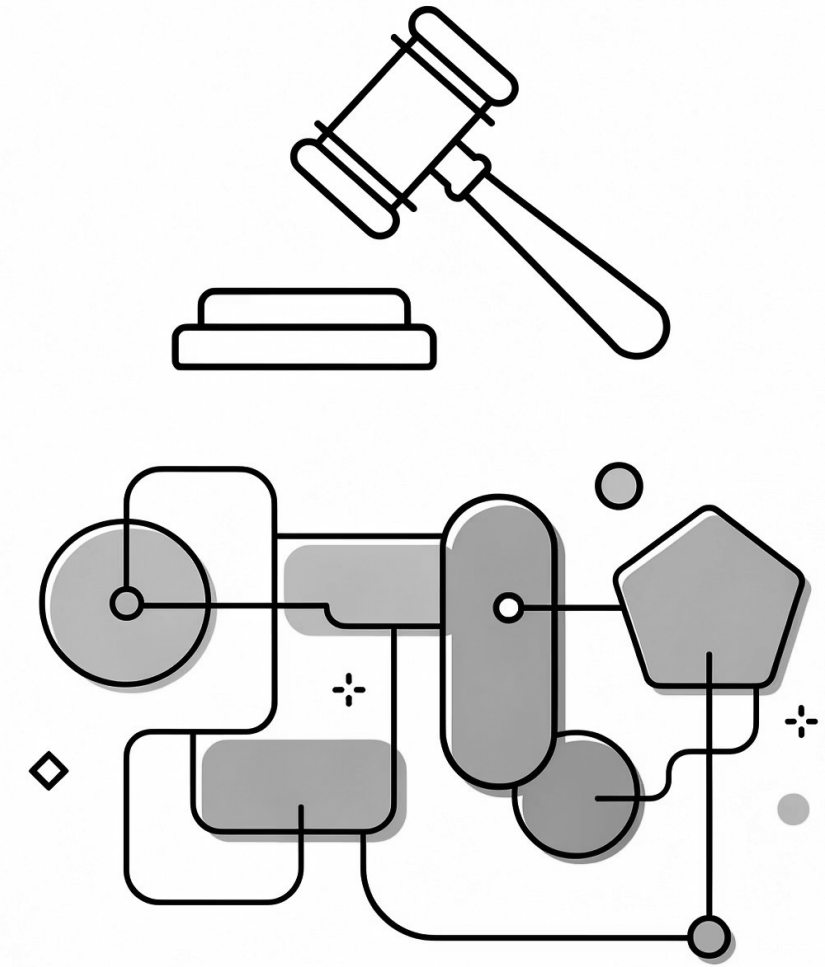
Al di là delle singole scadenze normative, emerge un principio universale: **ogni obbligo converge su un fondamento comune — la dimostrabilità**. Non basta più applicare la regola: bisogna renderne l'applicazione evidente e inconfutabile.

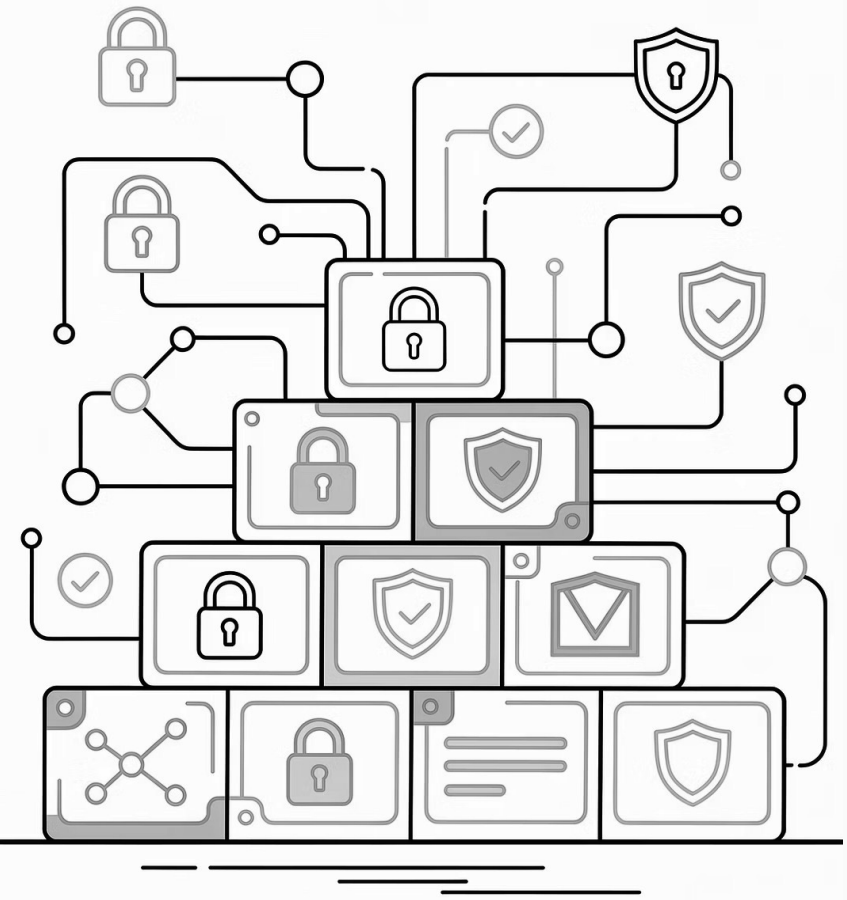
~~INNOCENTE~~

INADEMPIENTE

fino a prova contraria

> Si inverte la logica giuridica tradizionale: in caso di ispezione o incidente, l'assenza di documentazione e di una tracciabilità immutabile delle decisioni umane (chi ha autorizzato, quando e perché) equivale automaticamente a una **presunzione di colpevolezza e negligenza**.





ISO 27001: La Base per la Compliance NIS2

Per le organizzazioni, lo standard internazionale ISO/IEC 27001:2022 rappresenta un **blueprint metodologico collaudato**, coprendo tra il 70% e l'80% dei requisiti della direttiva NIS2.

L'adozione di un Sistema di Gestione della Sicurezza delle Informazioni (ISMS) basato sulla ISO 27001 permette di costruire una base di conformità solida, riducendo significativamente gli sforzi di implementazione per soddisfare i mandati legali specifici della NIS2.

La strategia della "Difesa Documentale"

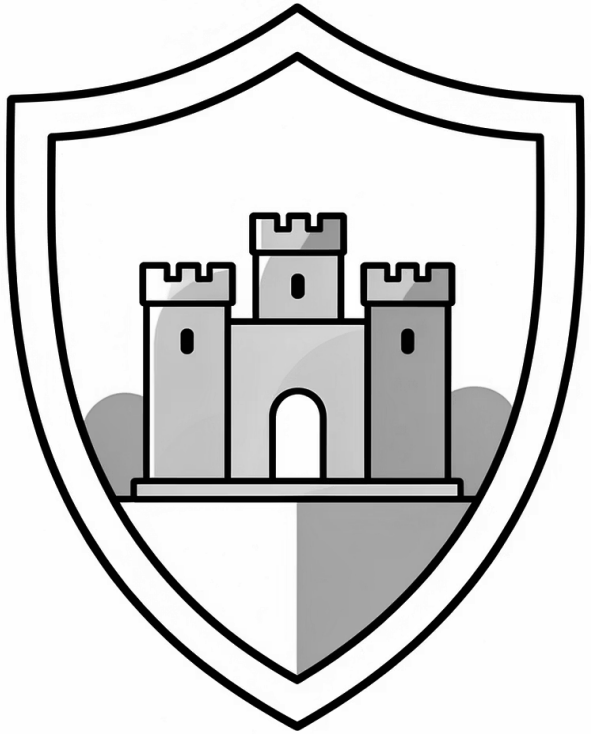
> La vera sfida non è solo bloccare le minacce, ma costruire uno **scudo di accountability** che trasformi la conformità operativa in evidenza legale inattaccabile.

Tracciare le decisioni

Audit log immutabili di ogni azione autorizzativa

Dimostrare la conformità

Evidenza legale pronta per ispezioni e audit



LA TRAPPOLA OPERATIVA

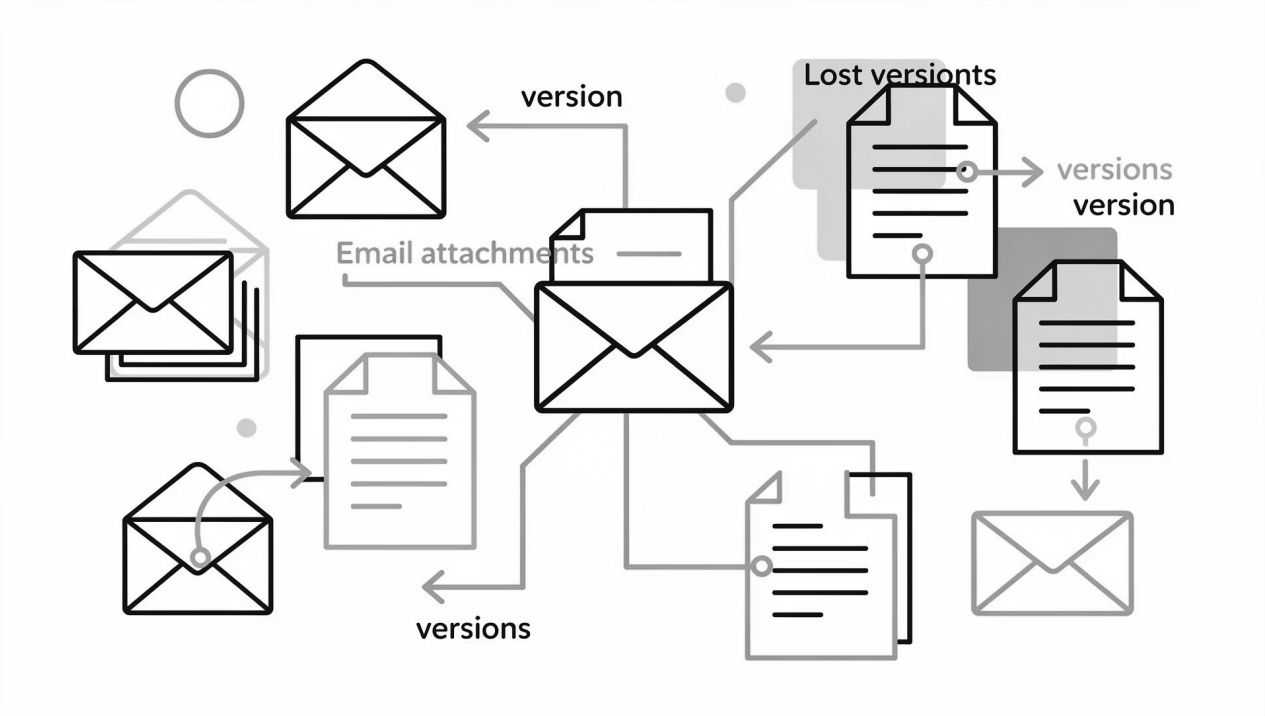
L'illusione di Excel ed email

Documenti modificabili = prove invalide

Gestire la governance su file Word ed Excel crea **"buchi neri"** nella sicurezza: sono documenti modificabili, privi di audit log e **incapaci di fornire una prova valida** in caso di ispezione da parte del regolatore.

LA TRAPPOLA OPERATIVA

Versioni via email: l'ultima approvata è un mistero



Quale versione è quella ufficiale?

Collaborare su bozze via email rende **impossibile identificare con certezza** l'ultima versione approvata di un documento. In un contesto di audit, l'ambiguità documentale si traduce automaticamente in **esposizione al rischio**.

LA TRAPPOLA OPERATIVA

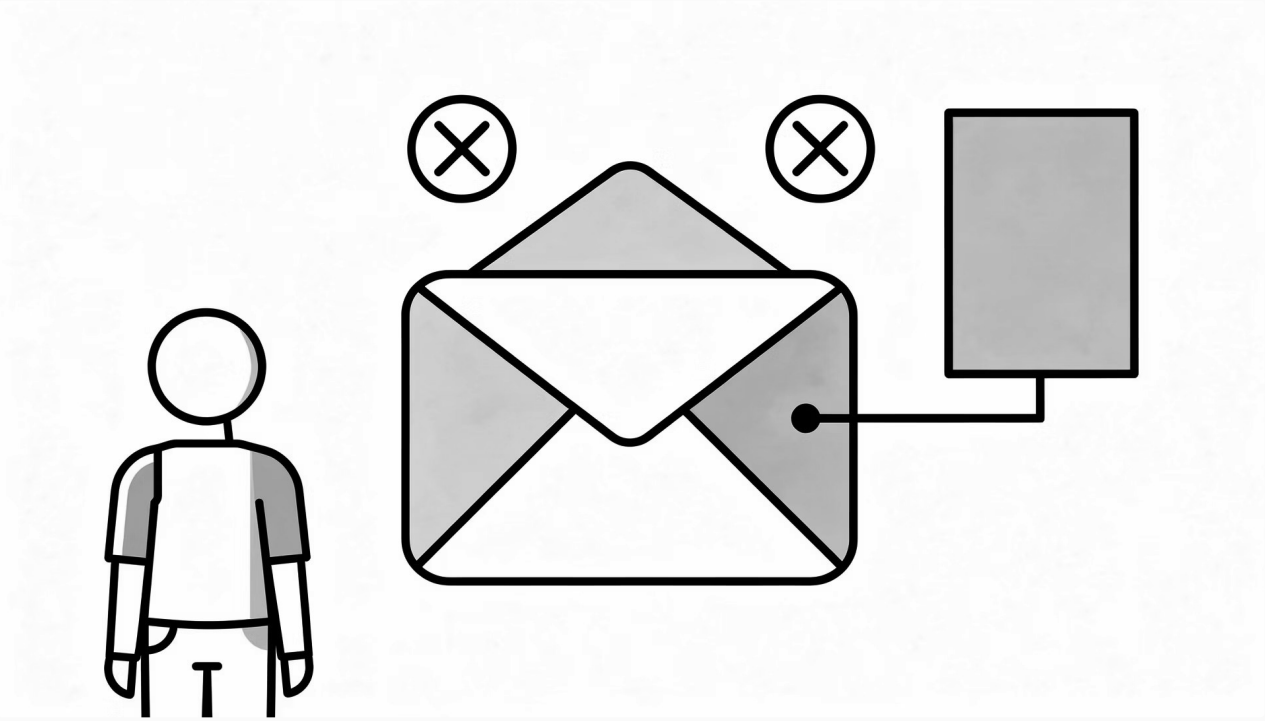
Canali non strutturati: decisioni invisibili

Senza traccia non è mai accaduto

Coinvolgere i colleghi tramite canali non strutturati significa **operare senza traccia**: le decisioni vengono prese, ma agli occhi del regolatore **non sono mai esistite**. Ogni accordo informale è un rischio potenziale.

LA TRAPPOLA OPERATIVA

Un PDF inviato non è una prova



Formazione senza timestamp è formazione inesistente

Inviare un PDF via email non prova nulla. Senza un **log digitale** che registri l'azione di lettura (click) e il momento esatto (timestamp), non si può dimostrare che il dipendente sia stato effettivamente **formato o informato**.

La soluzione: tenere traccia di decisioni e azioni

La vera dimostrabilità va ben oltre la semplice esistenza di un documento. Richiede la **capacità inconfutabile di tracciare ogni decisione e azione umana** all'interno del sistema di compliance, trasformando ogni passaggio in un'evidenza verificabile.

Tracciabilità delle Decisioni

Ogni autorizzazione, approvazione e scelta chiave deve essere registrata in modo immutabile, con data, ora e identificativo dell'autore.

Audit Trail delle Azioni

Ogni interazione con i processi e documenti di compliance – dalla lettura alla modifica – deve lasciare una traccia digitale verificabile.

Integrazione Sistemica

È fondamentale adottare strumenti che colleghino in modo nativo e sicuro documenti, persone e processi in un ecosistema digitale unico e auditabile.

CASE STUDY

L'esperienza di FHP Holding portuale

Le sfide affrontate

Definire chiaramente i ruoli e mettere ordine nella documentazione, centralizzandola per garantire un ambiente lavorativo all'insegna della **tranquillità e della sicurezza operativa**.

I benefici ottenuti

Un supporto guidato passo a passo verso l'automazione, con la serenità di **processi interamente tracciati** e pronti per qualsiasi ispezione.

Stefano Perfetti – Chief Technology & Marketing Officer, FHP Holding portuale

CASE STUDY

Il risultato: processi tracciati, dirigenza serena

Documentazione centralizzata

Tutti i documenti in un unico repository strutturato, accessibile e versionato

Ruoli definiti

Responsabilità chiare per ogni attore, tracciate e verificabili in ogni momento

Automazione guidata

Percorso step-by-step verso l'automazione dei processi di compliance

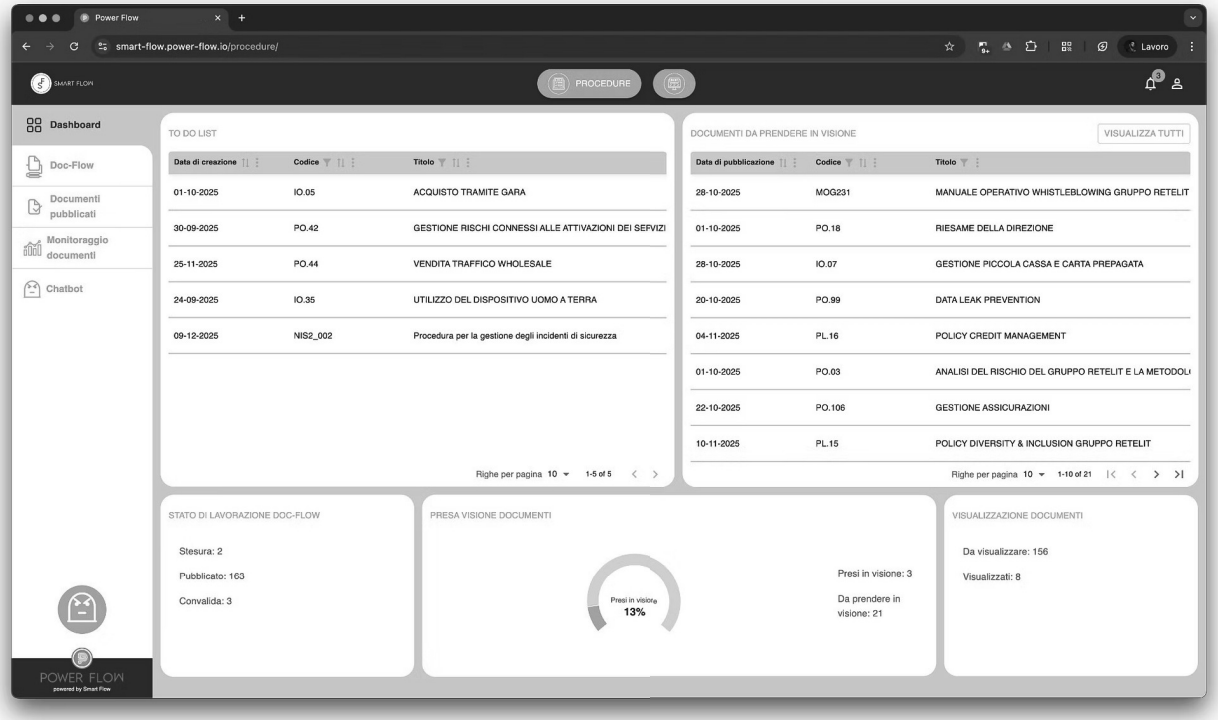
Tracciabilità completa

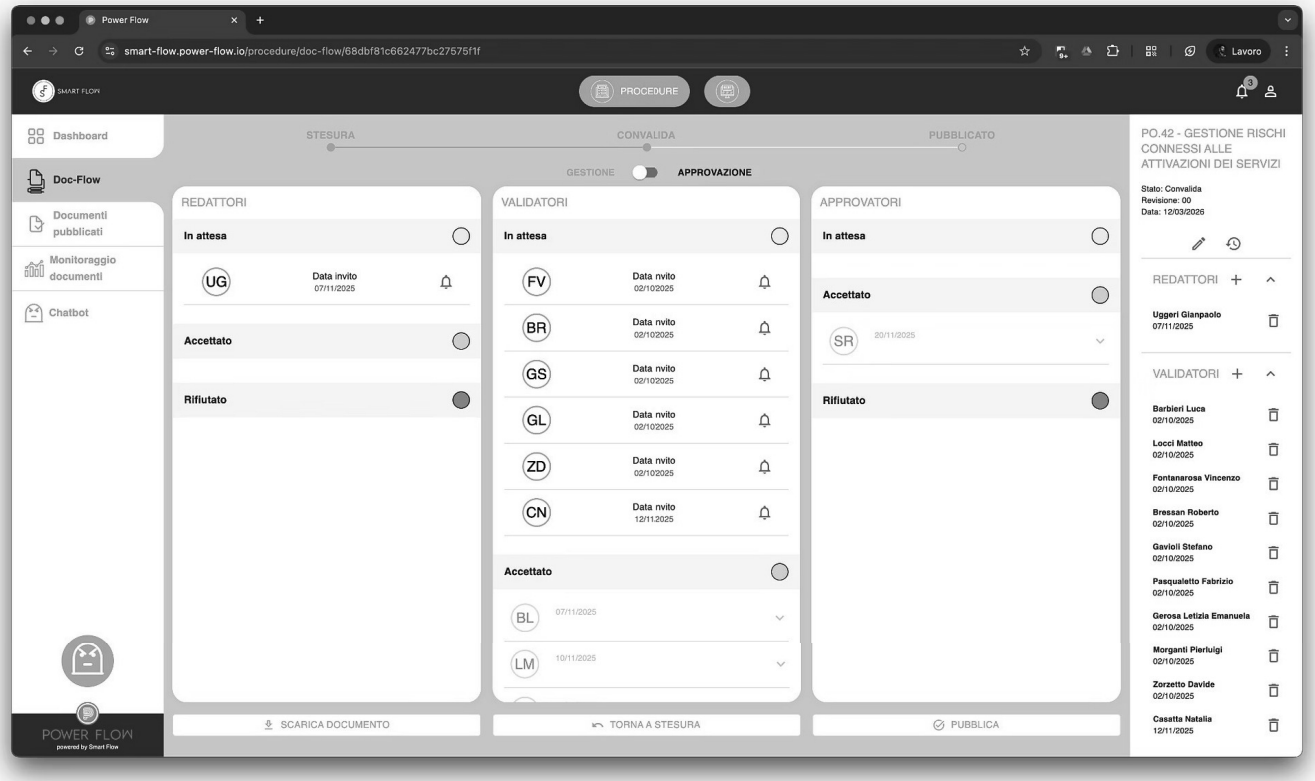
Ogni azione registrata con timestamp immutabile, pronta per l'audit

POWER FLOW PROCEDURE

To-do list: il cuore operativo della compliance

La to-do list integrata permette di assegnare, tracciare e chiudere ogni adempimento normativo con piena visibilità su stato e responsabilità.





POWER FLOW PROCEDURE

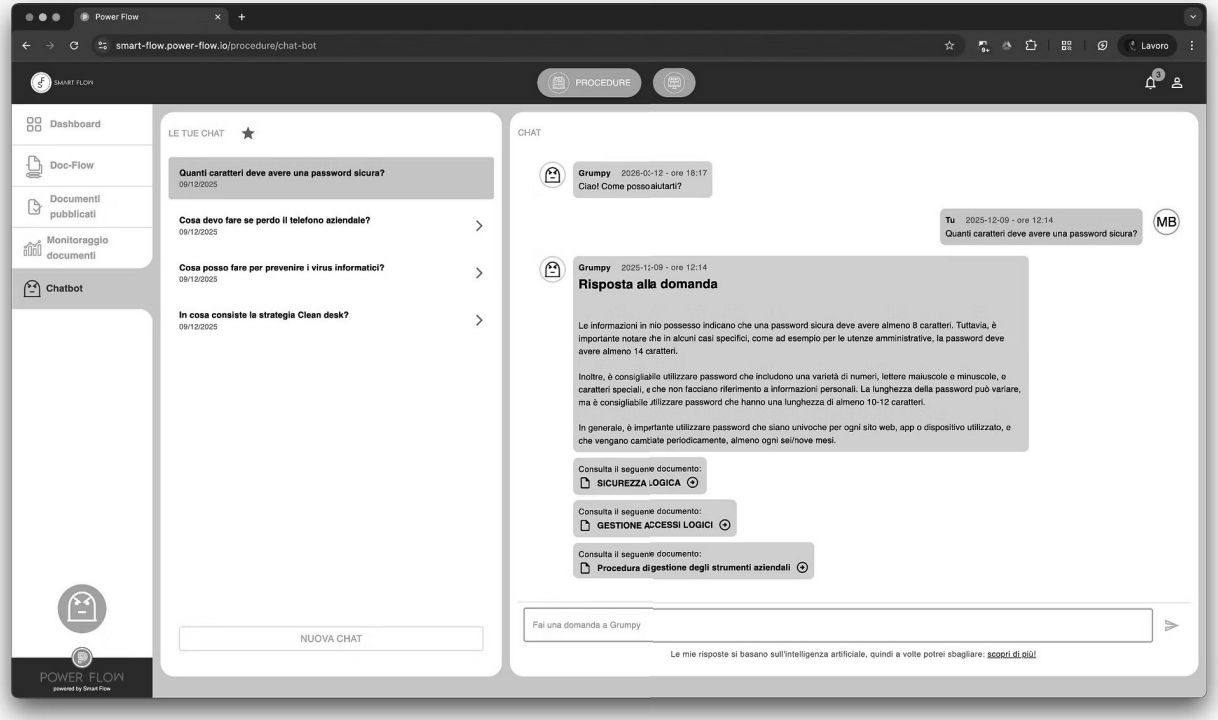
Il processo di approvazione tracciato

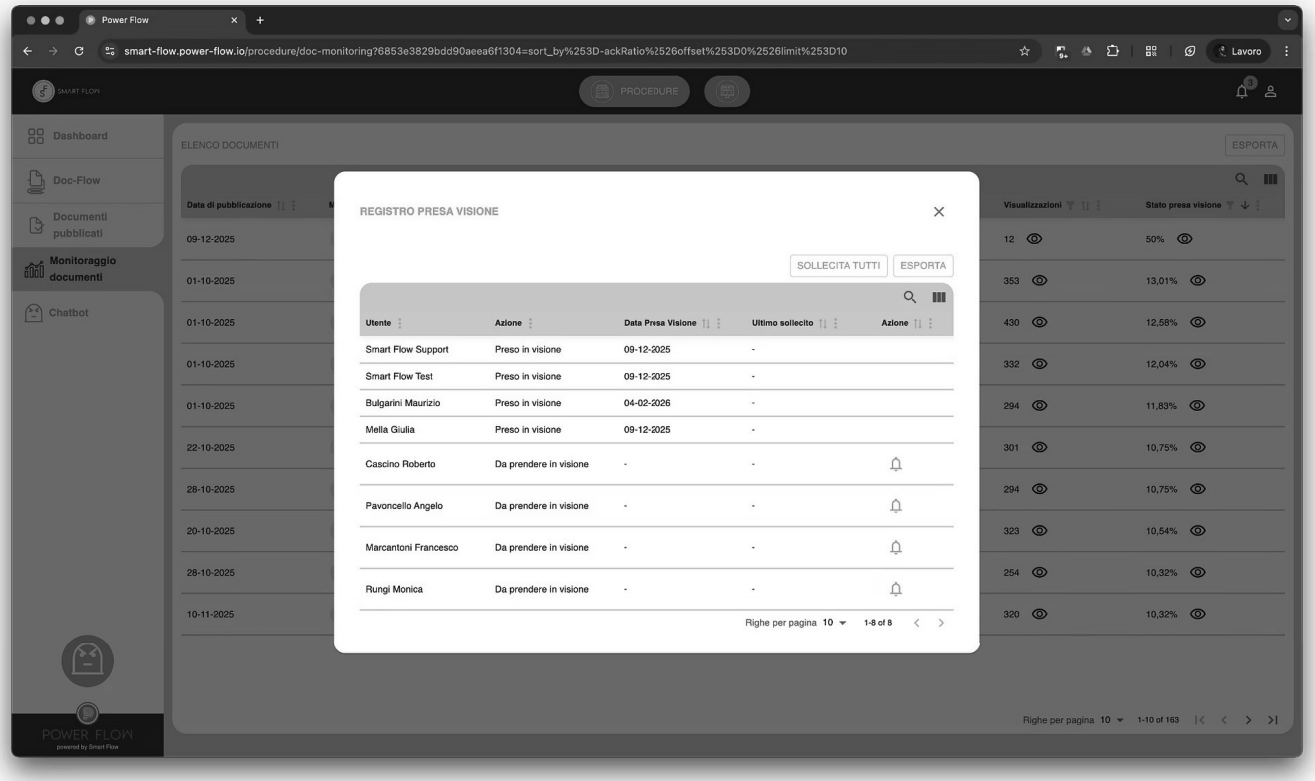
Ogni approvazione segue un workflow strutturato: chi ha autorizzato, quando e con quale ruolo. Un audit trail immutabile che trasforma ogni decisione in evidenza documentale.

POWER FLOW PROCEDURE

Grumpy: il chatbot che guida la compliance

Grumpy è l'assistente AI integrato nella piattaforma: risponde a domande normative, guida gli utenti nei processi e riduce il carico cognitivo dei team di compliance.





POWER FLOW PROCEDURE

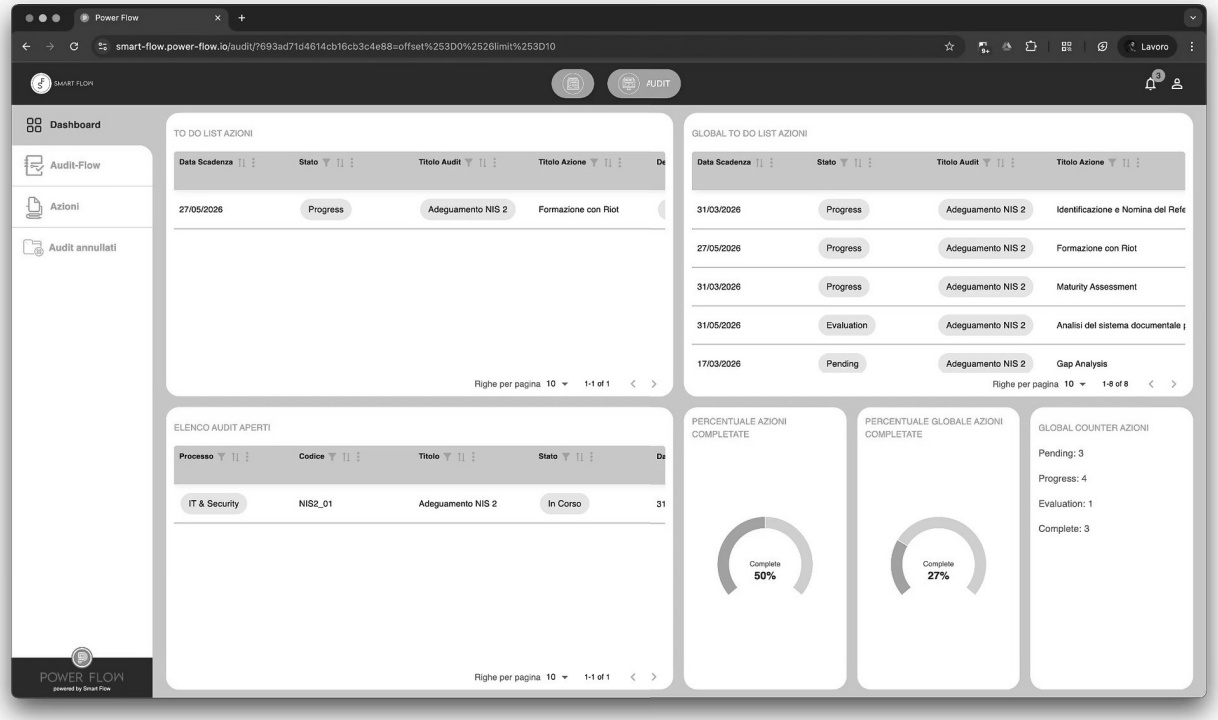
Il registro di presa visione

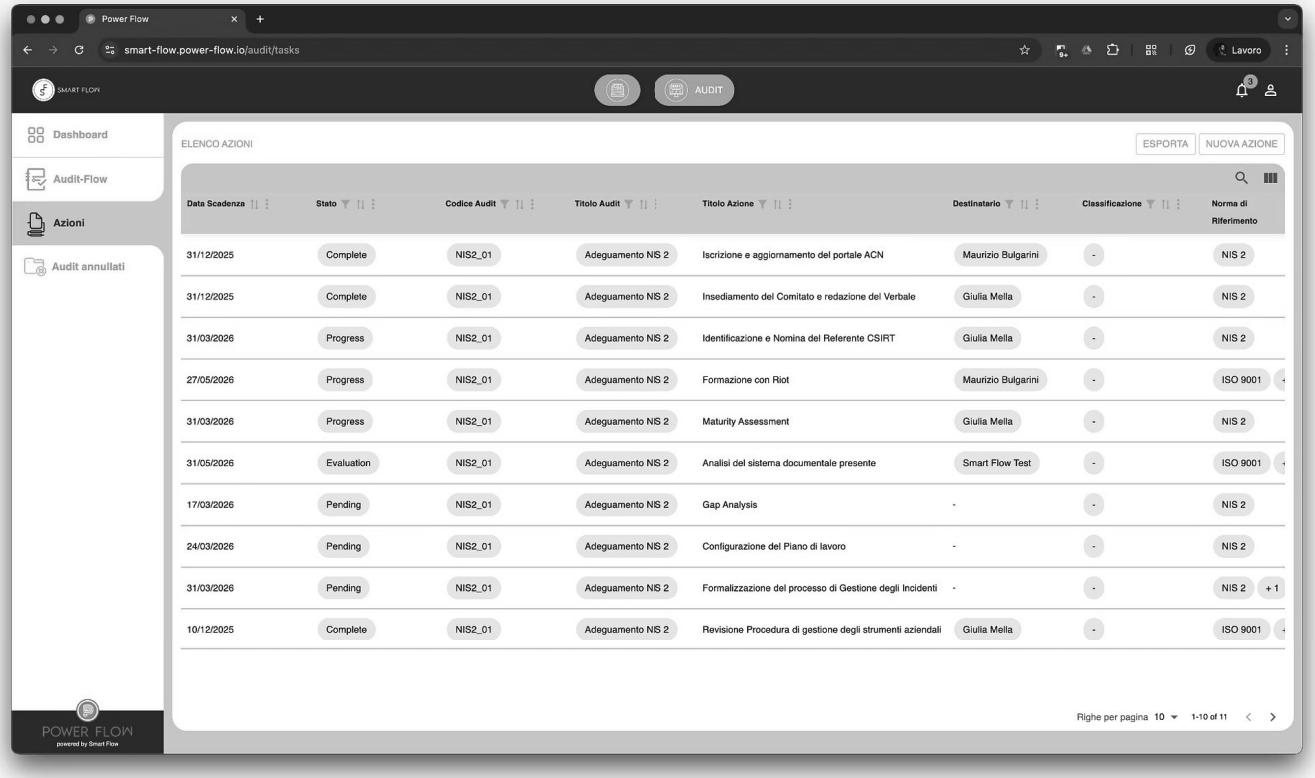
Ogni dipendente legge e conferma la presa visione di policy e procedure. Il sistema registra timestamp e identità digitale: la formazione diventa finalmente **dimostrabile**.

POWER FLOW AUDIT

La dashboard: visibilità totale sullo stato di compliance

Una dashboard unificata offre una visione in tempo reale dello stato di ogni adempimento, con alert, scadenze e KPI di conformità sempre aggiornati.





POWER FLOW AUDIT

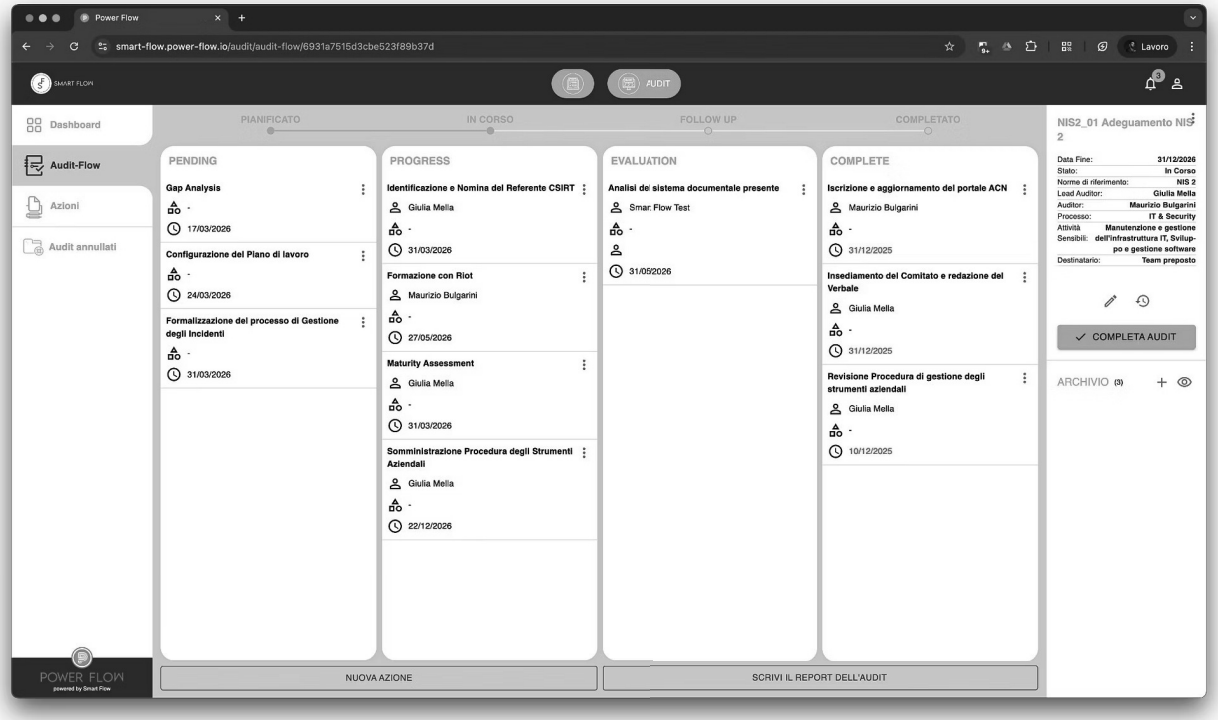
To-do list audit: priorità e scadenze sotto controllo

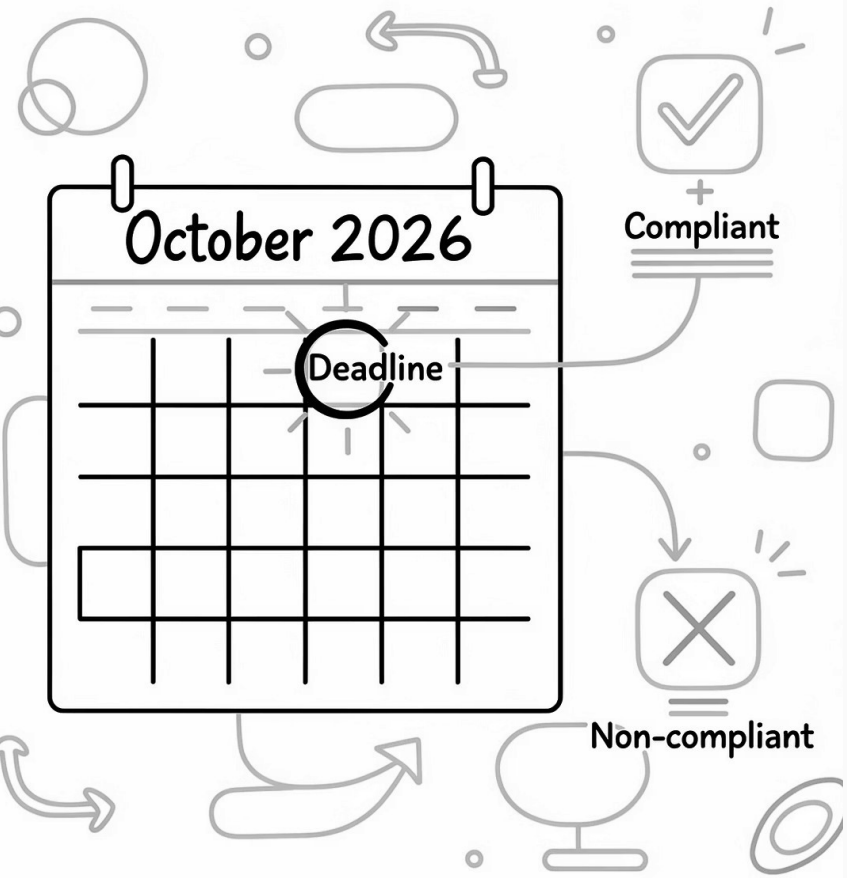
Il modulo audit organizza le attività di verifica in liste operative strutturate, con assegnazione di responsabilità, scadenze e stato di completamento tracciato.

POWER FLOW AUDIT

Il piano di lavoro: roadmap verso la piena conformità

Il piano di lavoro integrato traduce i requisiti NIS2 in attività concrete, con milestone misurabili e responsabilità assegnate — dalla diagnosi iniziale alla piena compliance certificabile.





Sei confidente che entro ottobre 2026 sarai compliant con la normativa NIS2?

Il tempo stringe. La scadenza si avvicina e ogni mese senza un sistema strutturato di dimostrabilità è un mese di esposizione al rischio.
La domanda non è se adeguarsi, ma quando iniziare.

Chi siamo

Smart Flow – Torino, dal 2016

Nati dalla confluenza di competenze ed esperienze maturate in grandi aziende italiane e internazionali, siamo oggi **partner strategico per la Digital Transformation** di aziende di ogni settore.

Siamo specializzati in:

- Compliance, governance e certificazioni GDPR
- Digitalizzazione e ottimizzazione dei processi
- Consulenza HR e ICT Governance
- Protezione dei dati e NIS2 / AI Act

Per una **consulenza conoscitiva gratuita**, scrivi a **marketing@smart.flow.it**

Il nostro impegno

Smart Flow contribuisce a una **crescita positiva del mondo del lavoro**, allineandosi agli obiettivi europei di rispetto dell'ambiente e delle risorse.

Per un **digitale etico e sicuro**, mettiamo a disposizione oltre un decennio di esperienza operativa.

Grazie!

Visita il nostro sito a basso impatto ambientale

www.smart-flow.it

Corso Quintino Sella, 102 · 10132 Torino · +39 011 1911 5338 ·
hello@smart-flow.it

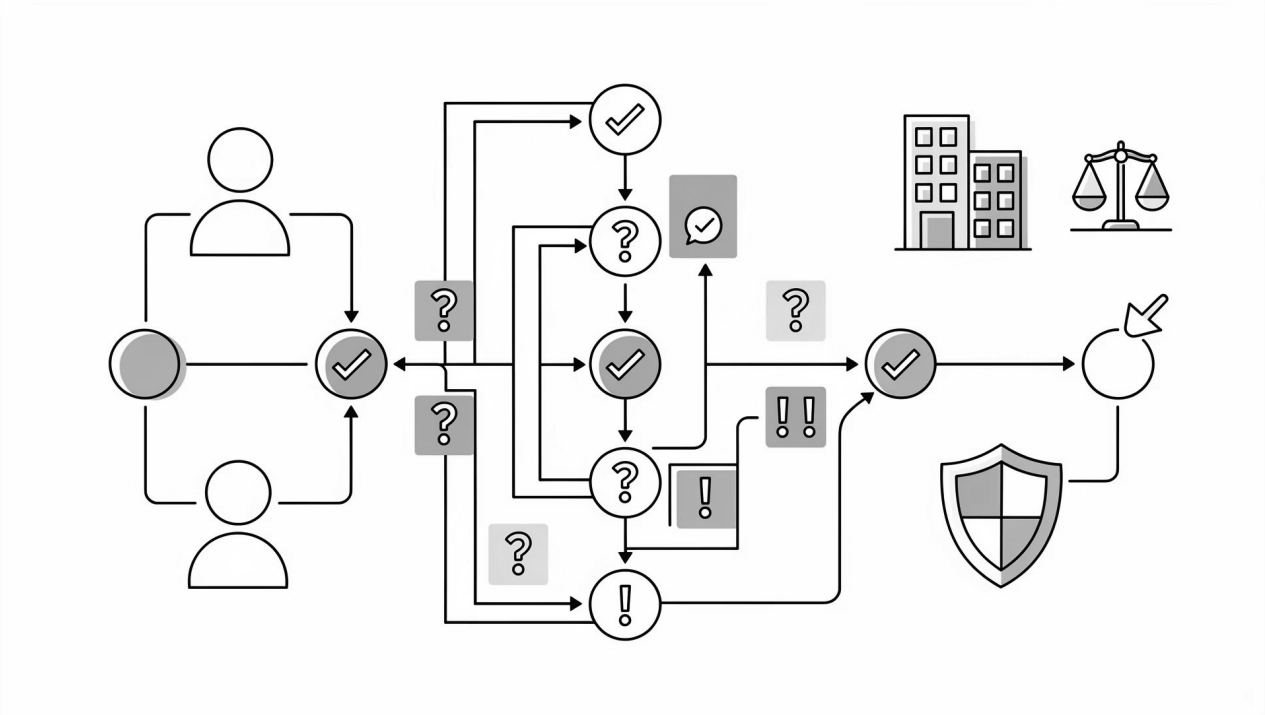
Che competenze sono necessarie?

Un contesto operativo complesso

Sono richieste **competenze multidisciplinari** per governare le incombenze normative. La situazione è caratterizzata da:

- Norme, regolamenti, progetti e urgenze che si sovrappongono senza una prioritizzazione chiara
- Difficoltà nell'allineare team legali, IT e di business
- Escalation della **responsabilità dirigenziale** verso i vertici aziendali

Dalla sicurezza alla dimostrabilità



Il nuovo paradigma

L'assenza di una **tracciabilità delle decisioni umane** — chi ha autorizzato, quando, perché — equivale ormai a una **negligenza sanzionabile** agli occhi del regolatore.

Non si tratta più solo di avere i processi corretti: si tratta di poter dimostrare, in modo immutabile e verificabile, che quei processi sono stati effettivamente seguiti.

La risposta strategica UE

La direttiva NIS2 potenzia la resilienza europea di fronte a minacce cyber divenute strumenti chiave nei conflitti ibridi e nella competizione globale.

1

Geopolitica Cyber

Il web è teatro di potere statale e spionaggio: la resilienza sistemica è ormai vitale per la sovranità.

2

Minacce mirate

Attori statali colpiscono settori strategici (logistica, telecomunicazioni) per mappare vulnerabilità e sottrarre dati.

3

AI e Crimine

Il crimine si professionalizza: l'uso di IA in attacchi offensivi (phishing, deepfake) esige difese adattive immediate.

Cybersecurity vs Compliance

Non vorrai mica aspettare il primo incidente per scoprire cosa devi fare per segnalarlo (in 24 ore)