FONDAZIONE PIEMONTE INNOVA

CYBERSECURITY E PA: l'importanza di modelli adattivi

La ***Palestra dell'Innovazione*** dei piccoli comuni in Piemonte e l'esperienza ***Piattaforma Città*** del Cluster Nazionale Smart Communities

Luca Mancino

Forum Cyber 4.0
Roma, 4-5 giugno 2025

FONDAZIONE PIEMONTE INNOVA

Fondazione Piemonte Innova - già Torino Wireless - è un **partenariato pubblico-privato** che abilita **l'innovazione e la doppia transizione**, digitale ed energetica, delle imprese e degli enti del terzo settore, affiancando le **pubbliche amministrazioni** per lo sviluppo di progetti di **innovazione**, sostenibili e replicabili, e **strategie di digitalizzazione.**

Smart Communities Tech
Italian Technology Cluster for Smart Communities

Il Cluster Smart Communities Tech - uno dei dodici Cluster Tecnologici Nazionali del MUR - è il **riferimento** per lo **sviluppo intelligente e sostenibile** di comunità e territori in Italia, utilizzando **l'innovazione tecnologica come strumento strategico.** Ne fanno parte 250+ Enti tra Regioni, Città, Università e OR, imprese.

Cyber e PA: "una questione di dimensioni"

FONDAZIONE PIEMONTE INNOVA

nelle GRANDI CITTÀ

ELEVATA DIGITALIZZAZIONE
le **grandi quantità di dati** sensibili che vengono raccolte da piattaforme e sensori sono fondamentali per alimentare i servizi digitali

INTERCONNESSIONI E INFRASTRUTTURE CRITICHE
le **interdipendenze tra i sistemi** aumentano la vulnerabilità delle PA, con potenziali gravi effetti a catena sui servizi cittadini nel caso di un attacco

GOVERNANCE PIÙ EFFICACE
il tema della sicurezza informatica deve essere **compreso e gestito** alle Amministrazioni per dialogare al meglio con i fornitori di soluzioni tecnologiche e scegliere quelle più affidabili

nei PICCOLI COMUNI

DIGITALIZZAZIONE CRESCENTE
soprattutto grazie a risorse PNRR, **anche le PAL stanno affrontando la transizione digitale**

MINORE CONSAPEVOLEZZA
i dati annuali sul numero di attacchi informatici in Italia evidenziano che **nessun ente può ritenersi completamente al sicuro**

VULNERABILITÀ DIFFUSA
la **scarsità di personale adeguatamente formato** per prevenire e gestire il rischio cyber aumenta la pericolosità anche di minacce minori e i possibili disservizi ai cittadini a seguito di un attacco

Comune di Torino hackerato

(15 novembre 2021 > servizi sospesi fino a 15 giorni)

Comune di Pisa hackerato

(Corriere della Sera, 19 maggio 2025)

CORRIERE DELLA SERA

CORRIERE FIORENTINO

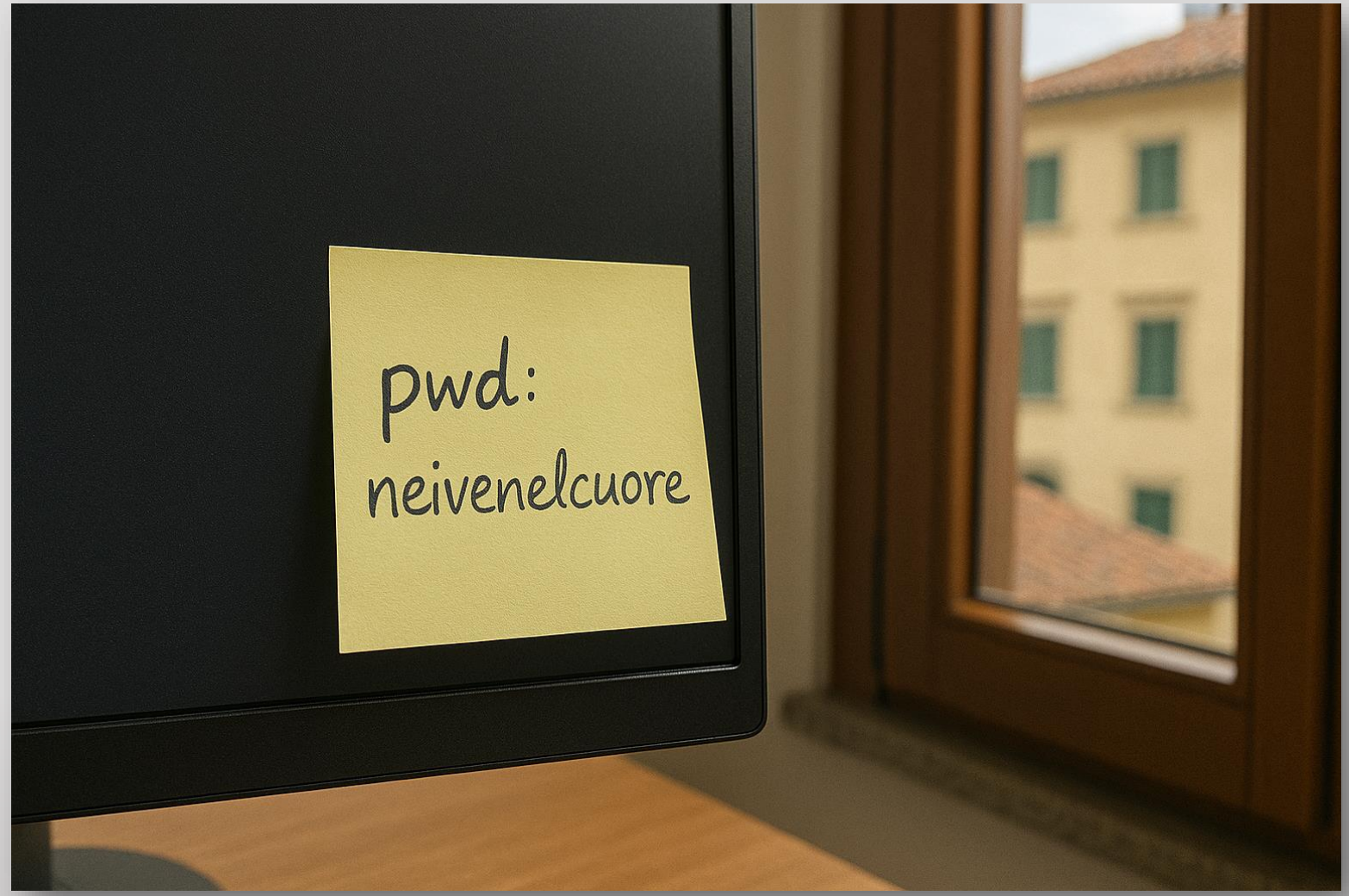
Attacco hacker al Comune di Pisa: dati sottratti e diffusi in rete, chiesto un riscatto

di Luca Lunedì

L'attacco informatico avvenuto il 10 maggio scorso. La notizia, diffusa dal gruppo consiliare Una città in Comune, è stata confermata dall'amministrazione. Sarebbe stato chiesto un riscatto: «Indagini in corso»

Comune di Neive

(PiemonteDigitale2030, marzo 2024)



PIATTAFORMA CITTÀ

Il ***Cluster Smart Communities Tech*** come **aggregatore di servizi, attività e buone pratiche** e **punto di incontro e confronto** stabile e continuativo tra città, imprese e mondo della ricerca

Tavoli di lavoro per raccogliere gli esempi di smart cities più innovativi e creare un **modello** che faccia da **guida per lo sviluppo intelligente e sostenibile** dei Comuni in tutta Italia

Stabilire un modello nazionale

Favorire la collaborazione

Facilitare lo **scambio di idee, esperienze e buone pratiche** relative ai progetti per la smart city **in ottica di replicabilità**

Promuovere le iniziative locali in corso affinché le **aziende italiane possano individuare opportunità di investimento**, favorendo i programmi di ricerca e sviluppo

Incoraggiare l'innovazione industriale

Il Cluster SmartCommunitiesTech (SCT) è parte del sistema italiano Cluster Tecnologici Nazionali

Smart COMMUNITIES Tech
Italian Technology Cluster for Smart Communities

100+
città coinvolte
sui tavoli di lavoro

Più di un terzo
città del Mezzogiorno

Piattaforma Città
promuove la collaborazione
per aumentare la replicabilità
e l'impatto dei programmi di innovazione
in tutta Italia

Valle d'Aosta
Aosta

Piemonte
Alessandria
Bardonecchia
C.M. Torino
Cuneo
Torino
San Giorgio Canavese

Liguria
Genova

Toscana
Carmignano
C.M. Firenze
Firenze
Massa
Pisa
Pistoia
Siena

Sardegna
Cagliari
Oristano

Trentino-Alto Adige
San Candido
Trento

Lombardia
Brugherio
Cantù
Como
Corsico
Lecco
Legnano
Magenta
Mantova
Piacenza
Rho
Segrate

Emilia-Romagna
Castel San Pietro Terme
Bologna
Ferrara
Fidenza
Imola
Modena
Monfalcone
Parma
Piacenza
Reggio Emilia
Rimini
Sassuolo

Lazio
Frosinone
Roma

Umbria
Assisi
Gualdo Tadino
Perugia
Terni

Campania
Benevento

Sicilia
Catania
C.M. Catania
Palermo

Calabria
C.M. Reggio Calabria
Cosenza

Friuli-Venezia Giulia
Azzano Decimo
Cividale del Friuli
Pordenone
Trieste
Udine

Veneto
Mira
Padova
Valdagno
Vicenza

Abruzzo
L'Aquila
Pescara
Teramo

Molise
Campobasso

Puglia
Lecce
Provincia di Lecce
Regione Puglia
Nardò
Otranto
Surbo
Taranto

Basilicata
Grassano
Matera
Montescaglioso
Pisticci
Pomarico
Venosa

Smart COMMUNITIES PiattaformaCittà
Smart COMMUNITIES Tech Italian Technology Cluster for Smart Communities
MUR

Il Cluster SmartCommunitiesTech (SCT) è parte del sistema italiano Cluster Tecnologici Nazionali

piemonte digitale 2030

Il programma d'azione di **Regione Piemonte** che, insieme a **CSI Piemonte** e **Fondazione Piemonte Innova**, **supporta e accompagna i Comuni nel percorso di trasformazione digitale e sostenibile**, agevolando il processo di innovazione.

1

Incontro con ogni Comune in presenza presso la loro sede, per **raccogliere le necessità** sui temi "digitalizzazione/innovazione", utilizzando anche lo strumento del **Digital Maturity Assessment (DMA)** basato su standard di indagine europei

Assessment Digitale

2

Attraverso una ricerca desktop su Open Data e database di Fondazione Piemonte Innova, **mappatura dello stato dell'arte di infrastrutture e competenze digitali** già attive o sviluppate dai Comuni. A ogni Ente viene restituito un documento strutturato in 11 sezioni

Fascicolo Digitale e database

3

Percorso di crescita delle competenze interne alla PA attraverso workshop formativi - in presenza - rivolti agli amministratori locali e al personale degli Enti su tematiche quali digitalizzazione interna, cybersecurity e GDPR, Piano Triennale ICT, comunicazione, ecc.

I martedì dell'Innovazione

SUPPORTO CONCRETO AI COMUNI SULLE TEMATICHE DELL'INNOVAZIONE

STRUMENTO INTERATTIVO DI DATA DISCOVERY

FORMAZIONE E CATALOGO BEST PRACTISE PER REPLICABILITÀ SUL TERRITORIO

200+ Comuni incontrati nel 2023 e 2024

I "nuovi" riferimenti normativi sulla cyber per la PA

FONDAZIONE PIEMONTE INNOVA

I punti di contatto sulla cybersecurity tra **legge 90/2024** e **Direttiva (UE) 2022/2555 (NIS2)**

Notifica di incidenti informatici	**Entro 24 ore dall'evento una prima notifica** di carattere generale ed **entro 72 ore una notifica più completa** (a valle di istruttoria per acquisire elementi causali e essenziali dell'incidente informatico) **Necessità di individuare un referente con specifiche professionalità e competenze in materia**, un profilo tecnico – anche appartenente all'UTD - cui è affidato il compito di sovraintendere ai sistemi e alle reti
Governance e gestione del rischio cyber	**Sensibilizzare le PA** ad individuare al loro interno soggetti responsabili dell'applicazione delle normative e a **implementare misure di gestione del rischio che prevengano o almeno governino rischi da incidente informatico**
Principio «by Design»	Introdurre sistemi di gestione che non si limitino a un set di misure minime di sicurezza, ma rispondano a **criteri di adeguatezza e proporzionalità alle dimensioni e alla tipologia di ente pubblico**
Rischio cyber applicato al Procurement	Legge 90/2024: regole di **predisposizione degli atti di gara e selezione dell'offerta più rigide** di quelle del codice dei contratti pubblici NIS 2: obbligo di contemplare misure di gestione del rischio cyber per assicurare la **sicurezza della catena di approvvigionamento**, compresi aspetti relativi alla sicurezza riguardanti rapporti tra ogni soggetto e i suoi fornitori

SICUREZZA INFORMATICA

Piano Triennale per l'Informatica nella PA (2024-26, aggiornamento 2025) - Capitolo 7

FONDAZIONE PIEMONTE INNOVA

ob 7.1 adottare una governance della cybersicurezza diffusa nella PA

7.1.1 – identificazione di un modello, con ruolo e responsabilità, di gestione della cybersicurezza
7.1.2 – definizione del framework documentale a supporto della gestione cyber

ob 7.2 gestire i processi di approvvigionamento IT coerentemente con i requisiti di sicurezza definiti

7.2.1 – definizione del framework documentale a supporto del processo di approvvigionamento IT
7.2.2 – definizione delle modalità di monitoraggio del processo di approvvigionamento IT

ob 7.3 gestione e mitigazione del rischio cyber

7.3.1 – definizione del framework per la gestione del rischio cyber
7.3.2 – definizione delle modalità di monitoraggio del rischio cyber

ob 7.4 potenziare le modalità di prevenzione e gestione degli incidenti informatici

7.4.1 – definizione del framework documentale relativo alla gestione degli incidenti
7.4.2 – definizione delle modalità di verifica e aggiornamento dei piani di risposta agli incidenti

ob 7.5 implementare attività strutturate di sensibilizzazione cyber del personale

7.5.1 – definizione dei piani di formazione in ambito cyber
7.5.2 – adozione di strumenti atti alla formazione in ambito cyber

FONDAZIONE PIEMONTE INNOVA

ANCONA

SecurityAN è il progetto con cui l'Amministrazione Comunale affronterà un importante **adeguamento informatico**, investendo primariamente sulla **formazione** di tutto il personale, con ulteriori corsi sulla sicurezza informatica specifica per i tecnici adibiti alla gestione dei sistemi informatici. Grazie alla **simulazione di attacchi** phishing, spear-phishing e whaling, si procederà inoltre ad analizzare la **postura di sicurezza dell'Ente**, con l'obiettivo di definire un **piano di potenziamento** efficace e di aggiornamento relativamente al disaster recovery.

CITTÀ METROPOLITANA di GENOVA

CYBER-CMGE coinvolge 29 Comuni della Città Metropolitana nell'**implementazione di tecnologie avanzate** per il miglioramento della protezione delle reti (tra cui la segmentazione del traffico di rete), nell'**ammodernamento degli apparati di rete** a servizio dell'infrastruttura metropolitana e nella **crescita delle competenze** in materia di sicurezza informatica con un percorso di formazione specialistica del personale IT. Il **Centro Operativo di Sicurezza** (SOC) sarà inoltre **esteso** agli enti territoriali attualmente sprovvisti, garantendo così un controllo costante degli attacchi.

MODENA

Con il programma **Modena Smart Security**, il Comune sta lavorando al potenziamento delle misure di sicurezza online e alla formazione del personale al fine di aumentare la consapevolezza delle minacce e migliorare le procedure interne di prevenzione e gestione del rischio.

Tra le iniziative previste, il Comune supporta la **Cyber Security Academy**, corso di specializzazione universitaria per la formazione di esperti di cybersecurity per la protezione dei dati e delle persone nella PA, nel mondo delle imprese e nella città connessa. Il percorso si svolge in collaborazione con il Centro di Ricerca Interdipartimentale sulla Sicurezza dell'Università degli Studi di Modena e Reggio e nei prossimi anni sarà ospitato dal Modena Data Center.

NOVARA

NO.V.A.R.A. (Novara Vulnerability Assessment Risk Analysis) PRESIDIUM IT SECURITATIS è il progetto che, all'interno della più ampia strategia di innovazione Novara Futura, mira a rafforzare l'**infrastruttura digitale** del Comune attraverso l'implementazione delle azioni - sia in materia di **soluzioni tecnologiche**, sia in merito alla riorganizzazione dei **processi interni** - individuate dal Framework nazionale per la Cybersecurity e la Data protection, le cui Linee guida sono frutto della collaborazione tra Enti pubblici, imprese e mondo accademico.

FONDAZIONE PIEMONTE INNOVA

PERUGIA

Perugia Data Safe mira a rafforzare la sicurezza informatica e la resilienza cyber del Comune attraverso un insieme di azioni sinergiche, guidate dalla consapevolezza che un attacco ad una Pubblica Amministrazione comunale mette in pericolo non solo la privacy dei cittadini, ma anche il tessuto economico locale. Il progetto si sviluppa su numerose attività, dall'**analisi delle vulnerabilità** e dalla definizione di **piani di miglioramento** per la sicurezza, a **percorsi di formazione del personale**, all'implementazione di strumenti per la **gestione degli accessi** e delle identità digitali, e all'installazione di **sistemi di protezione**, firewall e infrastrutture per il disaster recovery.

Il punto di vista dei piccoli Comuni*

Evidenze dal programma PiemonteDigitale2030

FONDAZIONE PIEMONTE INNOVA

ritiene che **garantire la sicurezza delle informazioni non sia una priorità strategica** per lo sviluppo del proprio Ente

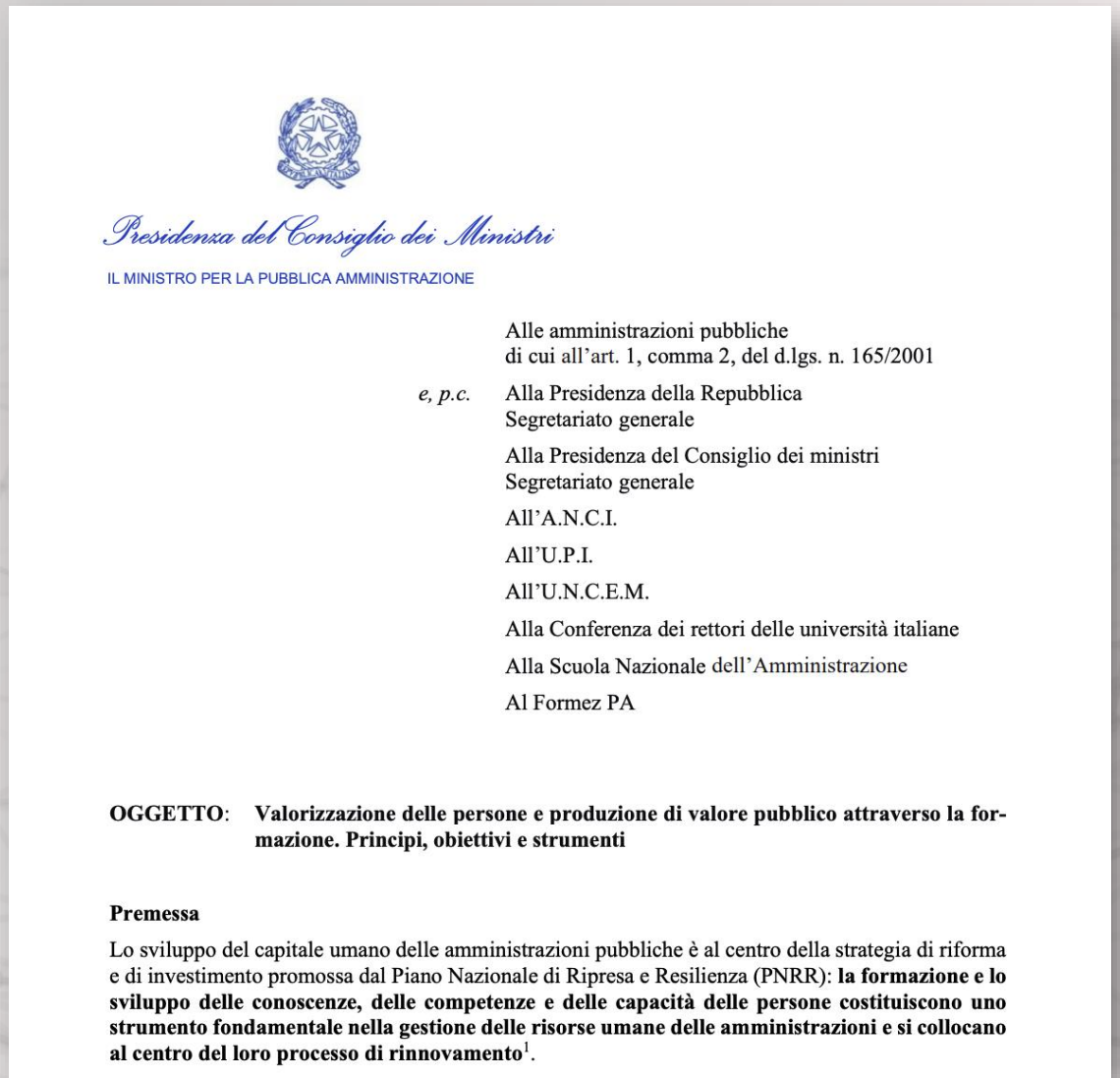
ritiene **poco importante investire in tecnologie e crescita delle competenze interne** per la gestione dei processi di cybersecurity

*I dati si riferiscono a 216 Comuni piemontesi intervistati nel 2024

Direttiva in materia di formazione del 14 gennaio 2025

Obiettivo: 40 ore di formazione annue per ogni dipendente pubblico

Nel gennaio 2025, Zangrillo ha emanato una direttiva che stabilisce l'obbligo di **40 ore di formazione all'anno** per ciascun dipendente pubblico, a partire dal 2025. Questo provvedimento mira a promuovere una cultura dell'apprendimento continuo, migliorare le competenze del personale e aumentare l'efficacia delle istituzioni pubbliche.



Presidenza del Consiglio dei Ministri

IL MINISTRO PER LA PUBBLICA AMMINISTRAZIONE

Alle amministrazioni pubbliche
di cui all'art. 1, comma 2, del d.lgs. n. 165/2001

e, p.c. Alla Presidenza della Repubblica
Segretariato generale

Alla Presidenza del Consiglio dei ministri
Segretariato generale

All'A.N.C.I.

All'U.P.I.

All'U.N.C.E.M.

Alla Conferenza dei rettori delle università italiane

Alla Scuola Nazionale dell'Amministrazione

Al Formez PA

OGGETTO: **Valorizzazione delle persone e produzione di valore pubblico attraverso la formazione. Principi, obiettivi e strumenti**

Premessa

Lo sviluppo del capitale umano delle amministrazioni pubbliche è al centro della strategia di riforma e di investimento promossa dal Piano Nazionale di Ripresa e Resilienza (PNRR): **la formazione e lo sviluppo delle conoscenze, delle competenze e delle capacità delle persone costituiscono uno strumento fondamentale nella gestione delle risorse umane delle amministrazioni e si collocano al centro del loro processo di rinnovamento**[1].

Accademia e Syllabus
e poi formazione specifica, da ACN a PerForma PA

Syllabus

Formazione personalizzata in modalità e-learning per rafforzare le conoscenze, svilupparne di nuove e aumentare la capacità digitale delle Pubbliche Amministrazioni

- **SICUREZZA**

  PROTEGGERE I DISPOSITIVI → conoscere l'esistenza e i rischi connessi agli attacchi informatici e saperli prevenire attraverso l'adozione delle necessarie precauzioni (a partire dalle più semplici)

  PROTEGGERE I DATI PERSONALI E LA PRIVACY → conoscere e saper applicare la normativa vigente sulla protezione dei dati personali, declinando gli adempimenti connessi alla tutela dei dati personali nell'ambito delle attività della PAL

- **CYBERSICUREZZA: SVILUPPARE LA CONSAPEVOLEZZA NELLA PA**

  illustrare concetti chiave relativi alla cybersecurity, sviluppando nel dipendente pubblico la consapevolezza delle azioni individuali che possono esporre l'amministrazione ad attacchi informatici attraverso l'identificazione delle principali sfide, lo sviluppo di competenze di prevenzione e gestione del rischio e la conoscenza del ruolo dell'Agenzia per la Cybersicurezza Nazionale (ACN) e della Strategia Nazionale di Cybersicurezza

Accademia dei Comuni digitali

Capacity building a supporto dei processi di trasformazione digitale nella PA, con particolare riferimento ai Comuni

- **SICUREZZA INFORMATICA E PROTEZIONE DEI DATI PERSONALI – livello INTRODUTTIVO**

  PRATICHE ESSENZIALI PER LA SICUREZZA DIGITALE NELLA PA → sviluppare competenze essenziali per proteggere i dati e garantire la sicurezza dell'ente, a partire da gestione delle password, riconoscimento delle e-mail di phishing e aggiornamento di software e dispositivi

  INTRODUZIONE ALLA LEGGE SULLA CYBERSICUREZZA NAZIONALE E SUI REATI INFORMATICI → fornire un quadro complessivo sulla nuova disciplina, approfondendo gli obblighi di notifica in caso d'incidente

- **SICUREZZA INFORMATICA E PROTEZIONE DEI DATI PERSONALI – APPROFONDIMENTO**

  GUIDA ALL'IMPLEMENTAZIONE DELLA DIRETTIVA NIS 2 → definire il contesto della normativa e il panorama di applicazione, le misure e gli obblighi di notifica

  PRIVACY BY DESIGN: TEORIA E PRATICA PER PROGETTARE SERVIZI A NORMA GDPR → sviluppare e consolidare competenze per una progettazione attenta al trattamento dei dati personali anche attraverso l'analisi di alcuni provvedimenti del Garante della Privacy

FONDAZIONE PIEMONTE INNOVA

Forum Cyber 4.0
Roma, 4-5 giugno 2025

GRAZIE!

Luca Mancino

luca.mancino@piemonteinnova.it

linkedin.com/in/luca-mancino