

 **QUIZ** commentati

Concorsi

RIPAM

Assistenti amministrativi

2913

(**3997** Assistenti
per le P.A.)

600

(**1100** Ministero
della **difesa**)

QUIZ COMMENTATI

per la **prova scritta**

NLD
CONCORSI

40. Risposta corretta: c)

Il **SUAP**, disciplinato dal **D.P.R. 160/2010**, costituisce il **canale telematico unico** attraverso cui imprese e cittadini possono gestire tutte le **procedure amministrative** necessarie per l'avvio, la modifica o la cessazione di un'attività produttiva, a prescindere dal settore coinvolto. In questa prospettiva, il SUAP rappresenta uno **strumento fondamentale di semplificazione**, che consente di centralizzare l'interlocuzione con la Pubblica Amministrazione, riducendo **tempi burocratici** e **oneri procedurali**, e promuovendo una **gestione digitale integrata** dei procedimenti.

L'affermazione contenuta nella lettera (C) coglie pienamente l'essenza istituzionale del SUAP, in quanto ne descrive la funzione di **sportello unico digitale** per l'intero ciclo autorizzativo delle attività economiche. Diversamente, la descrizione come **portale di commercio elettronico** (A) è del tutto estranea alla finalità pubblica dello sportello, che non opera nel mercato ma nell'ambito regolatorio. Allo stesso modo, l'idea che il SUAP sia un **ufficio della Camera di Commercio con funzioni di assistenza legale** (B) risulta impropria: sebbene le Camere di Commercio possano gestire i SUAP per conto dei Comuni, non sono titolari delle sue funzioni istituzionali. Infine, identificare il SUAP con un **sistema informatico del Ministero dell'Economia e delle Finanze** (D) confonde ambiti e competenze, attribuendo erroneamente al SUAP un ruolo nel settore **tributario**, che non gli compete.

41. Risposta corretta: c)

L'**IT Wallet**, istituito con il **D.I n. 19/2024** e disciplinato dalla **Legge n. 56/2024**, costituisce un tassello chiave nella strategia nazionale di **digitalizzazione dei documenti personali**. Integrato all'interno dell'**app IO**, consente ai cittadini di **gestire in formato digitale documenti ufficiali** come la **patente di guida**, la **tessera sanitaria** e la **carta europea della disabilità**, direttamente dal proprio smartphone, con un livello di sicurezza elevato e in pieno rispetto della normativa sulla **protezione dei dati personali**.

L'architettura del sistema è fondata su **protocolli di cifratura, autenticazione forte e controllo individuale delle informazioni**, garantendo così la **riservatezza** e il **pieno potere decisionale dell'utente**. È possibile scegliere quali documenti caricare, condividerli solo quando necessario, ed esercitare un controllo puntuale sull'intero ciclo di vita digitale delle credenziali custodite (C). Si tratta di un approccio che unisce **innovazione tecnologica** e **tutela della privacy**, coerente con le linee guida del **Regolamento eIDAS 2.0** e con il progetto di identità digitale europea.

Non trova riscontro, invece, l'idea che il Wallet abbia già **sostituito integralmente i documenti cartacei** (B): il sistema è attualmente **complementare**, pensato per affiancare le versioni fisiche in una fase iniziale di transizione digitale, in attesa della completa interoperabilità e di un quadro normativo armonizzato a livello europeo.

Limitare la funzione del Wallet alla **sola archiviazione di certificati scolastici** (A) non rende giustizia all'ambizione del progetto, che mira a **digitalizzare i principali documenti identificativi** e abilitare un uso esteso in ambiti pubblici e privati.

Infine, sostenere che il servizio sia **riservato a un ipotetico "SPID di livello 3"** (D) è privo di fondamento tecnico: SPID si articola su **tre livelli di sicurezza**, ma **non distingue gli utenti in classi di accesso**, e l'uso dell'IT Wallet non è subordinato a una classificazione esclusiva.

42. Risposta corretta: b)

Il principio della **confidenzialità** (B) è uno dei pilastri della **sicurezza dei dati personali**, come stabilito dagli artt. 5 e 32 del **Regolamento UE 2016/679 (GDPR)**. Questo principio impone che i dati trattati siano **protetti da accessi non autorizzati**, mediante l'adozione di misure tecniche e organizzative adeguate, come autenticazione forte, crittografia e controllo degli accessi. Si tratta di un aspetto essenziale soprattutto per le **pubbliche amministrazioni**, che gestiscono quotidianamente dati particolarmente sensibili. L'**integrità** (A) garantisce che le informazioni non vengano modificate in modo improprio o accidentale. La **disponibilità** (C) tutela il diritto degli interessati ad accedere ai dati quando necessario, mentre la **tracciabilità** (D) riguarda la

possibilità di **ricostruire le operazioni effettuate** su un sistema, contribuendo alla responsabilizzazione, ma non è sinonimo di riservatezza.

43. Risposta corretta: c)

Le **misure minime di sicurezza ICT** (C), definite nella **Circolare AgID 2/2017**, costituiscono un insieme di accorgimenti tecnici e organizzativi che **ogni amministrazione pubblica** è tenuta ad adottare per garantire un livello base di sicurezza dei propri sistemi. Tali misure includono, tra l'altro, la **protezione perimetrale**, il **backup periodico dei dati**, la gestione sicura delle **identità digitali** e il **monitoraggio degli accessi**. Questi requisiti sono vincolanti per tutte le PA e rappresentano il primo livello della **strategia nazionale per la cybersicurezza**. Gli **audit esterni** (A) sono importanti, ma non costituiscono un obbligo minimo per tutte le amministrazioni. La **cifratura** (B) è raccomandata nei casi in cui i dati trattati siano particolarmente sensibili, ma non è richiesta in maniera sistematica. Il **piano triennale** (D), pur essendo uno strumento strategico previsto dall'AgID, non ha natura tecnica e non sostituisce le misure minime.

44. Risposta corretta: d)

Il **Computer Security Incident Response Team (CSIRT Italia)**, istituito presso l'Agenzia per la Cybersicurezza Nazionale (ACN), rappresenta il punto di riferimento per la **gestione e il coordinamento delle attività di risposta agli incidenti informatici** (B). La sua missione è supportare enti pubblici e operatori di servizi essenziali nel fronteggiare **cyber attacchi**, **vulnerabilità critiche e violazioni dei dati**, assicurando il contenimento e la risoluzione tempestiva degli eventi. Fornisce **supporto tecnico**, dirama **allerta tempestive**, gestisce **banche dati sulle minacce emergenti** e promuove la **resilienza cibernetica** del Paese. Non rientra tra i suoi compiti la **promozione culturale** (A), la **normativa documentale** (C) né tantomeno la **gestione operativa di SPID** (D), che è affidata a soggetti autorizzati da AgID.

45. Risposta corretta: c)

L'**art. 37 del GDPR** stabilisce che tutte le **autorità e gli organismi pubblici**, senza distinzione in base al tipo di trattamento effettuato, sono **tenuti a designare un Responsabile della Protezione dei Dati (RPD)** (C). Questa figura è incaricata di vigilare sulla **conformità normativa** e di fungere da punto di contatto con l'Autorità Garante, promuovendo una **gestione trasparente e corretta dei dati personali**. L'obbligo vale anche in assenza di trattamenti particolari o su larga scala. Il riferimento ai **dati biometrici** (A) è solo parzialmente rilevante e non modifica l'obbligatorietà generale per la PA. L'affermazione secondo cui la nomina sarebbe necessaria **in ogni caso** (B) è eccessivamente ampia, poiché nel settore privato è vincolata alla natura e alla portata del trattamento. Non serve, infine, alcuna **richiesta da parte del Garante** (D) per attivare tale obbligo: si tratta di un adempimento diretto e generalizzato.

46. Risposta corretta: c)

La **L. 23 settembre 2025, n. 132**, nel quadro della **Legge quadro sull'intelligenza artificiale**, assegna espressamente all'**Agenzia per la cybersicurezza nazionale** un ruolo centrale di **vigilanza** sui sistemi di intelligenza artificiale, comprendente anche **attività ispettive e sanzionatorie**, in coerenza con la normativa nazionale e dell'**Unione europea** e con quanto previsto dall'**AI Act**. La novità consiste nell'estensione delle competenze dell'ACN oltre la tradizionale tutela delle **infrastrutture critiche**, includendo in modo strutturato la supervisione dei sistemi di IA sotto il profilo della **cybersicurezza**, nonché la promozione del loro sviluppo in tale ambito. Le altre opzioni non sono corrette perché riducono o alterano il perimetro delle attribuzioni normative: l'ACN non svolge solo funzioni di promozione dell'innovazione (A), non è limitata a un ruolo meramente consultivo (B) e non assorbe integralmente le competenze dell'AgID, che restano distinte e complementari, in particolare in materia di **notifica**, **valutazione**, **accreditamento** e **monitoraggio** dei soggetti incaricati di verificare la conformità dei sistemi di intelligenza artificiale (D).