SCHEMA RIASSUNTIVO · MATERIA

Informatica di base

Nozioni essenziali per concorsi: hardware, software, reti, sicurezza, posta elettronica.

Studia questa materia sul sito →

8 argomenti · 53 lezioni

Lezioni principali

Concetti base di informatica per il concorso

Hardware, software, reti, sicurezza, posta elettronica: i fondamentali richiesti.

SPID, CIE, CNS: l'identità digitale nella PA

Per accedere ai servizi digitali della PA servono strumenti di identità: SPID, CIE (Carta d'Identità Elettronica), CNS (Carta Nazionale dei Servizi). Ciascuno ha caratteristiche e livelli di sicurezza.

Sicurezza informatica di base: password, phishing, ransomware

La cybersecurity di base per la PA include misure tecniche e comportamentali per proteggere sistemi, dati e operatori. Aspetti chiave: 1) Password robuste e personali: lunghezza, complessità, univocità, no condivisione; 2) 2FA/MFA dove disponibile; 3) Phishing: riconoscere email sospette, non cliccare link, non aprire allegati non attesi, segnalare all'IT; 4) Ransomware: backup off-line, antivirus aggiornato, formazione; 5) Aggiornamenti software regolari; 6) Blocco schermo quando ci si allontana; 7) Logout a fine giornata; 8) No credenziali condivise (mai); 9) Riconoscimento social engineering (telefonate sospette, finti superiori, urgenze artificiose); 10) Segnalazione tempestiva di incidenti all'IT + DPO + eventualmente CSIRT-Italia. Per la PL: target frequente di phishing istituzionale; cura nelle banche dati interforze; conoscenza dei rischi specifici (ransomware, accessi abusivi); cooperazione con IT comunale + Polizia Postale per casi gravi.

Reti e Internet: fondamentali

Comprendere cos'è una rete e come funziona Internet è base per i concorsi: LAN/WAN, protocollo TCP/IP, indirizzi IP, DNS, HTTP/HTTPS.

PEC: come funziona tecnicamente

La PEC (Posta Elettronica Certificata, D.P.R. 68/2005 + CAD artt. 6, 48) è il sistema italiano di posta elettronica con valore legale. Caratteristiche tecniche: trasmissione cifrata tra gestori PEC accreditati AgID, ricevute opponibili (accettazione + consegna), busta di trasporto in formato standard. Valore legale: la PEC produce ricevute opponibili e ha valore legale nei casi previsti, soprattutto verso soggetti dotati di domicilio digitale. La consegna nella casella PEC perfeziona la notifica indipendentemente dalla lettura. Per la PL: strumento essenziale per notifiche, comunicazioni con valore legale, trasmissione atti tra PA. Verifica dell'indirizzo PEC nelle banche dati pubbliche (INI-PEC, INAD, IPA) prima dell'invio per evitare errori. Differenza con email ordinaria: PEC ha valore legale, email no.

Fondamenti di informatica

Hardware e software — componenti del computer

Il computer è composto da hardware (componenti fisici: CPU, RAM, storage, scheda madre, GPU, periferiche) e software (programmi: sistema operativo, applicativi, driver). CPU esegue istruzioni; RAM memoria volatile; storage (SSD/HDD) memoria permanente; periferiche input (tastiera, mouse) e output (monitor, stampante). Conoscere i componenti aiuta a capire prestazioni, manutenzione e acquisti informati. Base per ogni utilizzo professionale.

Il sistema operativo — Windows di base

Il sistema operativo (SO) gestisce hardware e software. Windows è il più diffuso nelle PA italiane. Elementi chiave: desktop (schermata principale), barra delle applicazioni, menu Start, Esplora file (cartelle/file), Pannello di controllo / Impostazioni, task manager. File: nome + estensione (.docx, .pdf). Cartelle: organizzazione gerarchica. Shortcut tastiera accelerano produttività. Sicurezza: password, blocco schermo.

File e cartelle — organizzazione dati

Organizzare file e cartelle efficacemente è fondamentale. Principi: gerarchia chiara, nomi significativi, struttura standardizzata. Nomi file: descrittivi, data se rilevante, no caratteri speciali. Cartelle: per progetto, anno, tipologia. Ricerca: con Esplora file o motore integrato. Ordinamento: nome, data, tipo, dimensione. Compressione zip per riduzione dimensioni/invio. Attenzione: caratteri illegali (\/:?\"|).

Reti e Internet — concetti di base

Le reti connettono dispositivi. LAN (Local Area Network): ufficio, casa. WAN (Wide Area Network): aree estese. Internet: rete globale. WiFi: connessione wireless. Ethernet: via cavo. Router/modem: collegano al provider. IP: identifica dispositivi. DNS: traduce nomi in indirizzi. Cloud: dati su server remoti. Principali: sicurezza (VPN, firewall), prestazioni (velocità), affidabilità.

Browser e navigazione web

Il browser è il programma per navigare su Internet. Più diffusi: Chrome (Google), Edge (Microsoft), Firefox (Mozilla), Safari (Apple). Elementi: barra URL, schede, segnalibri, cronologia, download. HTTPS: sito sicuro (lucchetto). Cookie: piccoli dati siti. Password: salvataggio automatico (da usare con cautela). Estensioni: funzionalità aggiuntive. Privacy: modalità incognito.

Email e PEC — comunicazione digitale

L'email è strumento fondamentale di comunicazione. Componenti: indirizzo (nome@dominio), oggetto, corpo, allegati. Client: Outlook, Thunderbird, webmail. PEC (Posta Elettronica Certificata): equivale a raccomandata AR per valore legale. Obbligatoria per imprese e PA. Galateo email: oggetto chiaro, grammatica corretta, firma. Attenzione: phishing, spam, virus. Archiviazione importante.

Password e sicurezza di base

Le password sono la prima difesa dei tuoi dati. Requisiti: lunghezza (12+ caratteri), complessità (maiuscole, minuscole, numeri, simboli), unicità (diversa per ogni servizio), segretezza. Autenticazione a due fattori (2FA): sicurezza aggiuntiva. Password manager per gestire molte password. Attenzione: non condividere, non scrivere in chiaro, non riutilizzare. Phishing: mai inserire password da link email sospette.

Stampa, scansione, digitalizzazione

Gestire documenti cartacei e digitali è routine PA. Stampanti: locali o di rete; laser (veloce) o inkjet; multifunzione (stampa, scansione, copia, fax). Scansioni: OCR per testo modificabile; PDF/A per archiviazione. Risoluzione: 300 DPI standard. Digitalizzazione: processo PA di dematerializzazione. Formati: PDF per condivisione, PDF/A per archivio, TIFF per alta qualità. Firma digitale su PDF generato.

Office e strumenti digitali PA

Word e Writer — videoscrittura

I word processor (Microsoft Word, LibreOffice Writer) sono strumenti fondamentali per creare e formattare documenti. Funzioni principali: digitazione, formattazione (font, grassetto, stili), paragrafi (allineamento, indentazione), tabelle, immagini, intestazioni/piè, stampa unione per invii massivi. Salvataggio: .docx (Word), .odt (Writer), .pdf per condivisione. Revisioni per collaborazione. Essenziali per PA: verbali, relazioni, corrispondenza.

Excel e Calc — fogli di calcolo

I fogli di calcolo (Excel, LibreOffice Calc) gestiscono dati in righe e colonne. Celle con riferimenti (A1, B2). Formule iniziano con =. Funzioni comuni: SOMMA, MEDIA, CONTA, SE, CERCA.VERT. Grafici per visualizzare dati. Formattazione celle (numeri, date, valuta). Ordinamento e filtri. Tabelle pivot per analisi. Essenziali per PA: statistiche, bilanci, gestione dati. Esportazione PDF o CSV per interoperabilità.

PowerPoint e presentazioni

Le presentazioni (PowerPoint, LibreOffice Impress, Google Slides) comunicano idee tramite slide (diapositive) sequenziali. Elementi: titolo, testo, immagini, grafici, video, animazioni, transizioni. Temi predefiniti per coerenza. Modalità presentazione a schermo intero. Esportazione: PPTX, PDF, video. Principi: meno è più (poche parole per slide), contrasto, coerenza. Usi PA: comunicazione istituzionale, formazione, conferenze.

SPID e CIE — identità digitale

L'identità digitale italiana si articola in SPID, CIE e CNS (CAD art. 64). SPID (Sistema Pubblico di Identità Digitale): credenziali con 3 livelli di sicurezza; normalmente gratuito per il cittadino nei livelli ordinari, salvo condizioni dei singoli gestori (alcuni gestori applicano costi per servizi premium o livelli alti). CIE (Carta di Identità Elettronica): documento fisico con chip NFC; per uso digitale richiede lettore NFC o app CieID + PIN (rilasciato all'emissione). CNS (Carta Nazionale dei Servizi): smart card con certificato digitale; richiede lettore smart card + software specifico; usata per servizi specifici (fisco, sanità, ecc.). eIDAS 2.0 (Reg. UE 2024/1183): in implementazione l'EU Digital Identity Wallet (in Italia: ITwallet). Per la PA: SPID e CIE sono i principali strumenti per cittadini per accesso ai servizi online (App IO, portali, ecc.).

Firma digitale — come funziona

La firma digitale è equivalente giuridico della firma autografa, ma più sicura. Si basa su crittografia asimmetrica (chiave pubblica + privata). Certificato qualificato: rilasciato da CA (Certification Authority) accreditate. Formati: PAdES (PDF), CAdES (generico .p7m), XAdES (XML). Strumenti: token USB, smart card + lettore, firma remota (HSM). Uso PA: documenti, contratti, processo civile telematico. Obbligatoria per dirigenti e atti formali.

PagoPA — pagamenti digitali verso la PA

Il PagoPA (Pagamenti Pubblica Amministrazione) è il sistema unico nazionale per pagare verso PA. Gestito da PagoPA SpA. Cittadini pagano tributi, multe, tasse, servizi. Modalità: home banking, carte, app IO, tabaccai, Poste. Obbligatorio per tutte le PA dal 2021. Codice CBILL (IUV) identifica pagamento. Tracciabilità totale. Ricevuta automatica. PL: verbali CDS pagabili via PagoPA.

Amministrazione Trasparente — portale web

L'Amministrazione Trasparente (D.Lgs. 33/2013) è la sezione obbligatoria del sito web di ogni PA italiana che pubblica dati e atti per finalità di trasparenza e accountability. Sezioni obbligatorie: organizzazione, personale, contributi e sussidi, bandi e gare, performance, opere pubbliche, attività e procedimenti, ecc. Per la PL: dati statistici di attività della PL possono essere pubblicati nel rispetto di

Sicurezza, privacy, PL digitale

Cybersecurity — minacce e difese

La cybersecurity è la protezione di sistemi informatici da attacchi. Minacce principali: virus (si moltiplicano), trojan (nascosti), ransomware (cripta dati per riscatto), spyware, adware, worm, rootkit. Attacchi: phishing (email fraudolente), brute force (password), DDoS (sovraccarico), zero-day. Difese: antivirus aggiornati, firewall, backup, aggiornamenti, formazione, 2FA. PL: attenzione a banche dati, credenziali, dispositivi mobili.

Privacy e GDPR applicata

La privacy applicata all'informatica è cruciale per la PA. Sintesi (la materia è approfondita nella specifica materia Privacy/GDPR): principi base in ambito IT: 1) Password robuste e personali, 2FA dove possibile; 2) Banche dati: accesso solo per finalità di servizio, con tracciamento; 3) Email: cifratura per dati sensibili, attenzione a destinatari, no condivisione di credenziali; 4) Allegati: firmati digitalmente per atti formali, no dati eccedenti; 5) Stampa documenti: con cura (no stampe abbandonate in stampante), distruzione sicura quando non più necessari (trituratore). Reati specifici: art. 615-ter c.p. (accesso abusivo), 326 c.p. (rivelazione segreto), 167 D.Lgs. 196/2003 (trattamento illecito). Per la PL: cura quotidiana nei trattamenti; coordinamento con DPO comunale; formazione obbligatoria. Approfondimenti: vedere materia specifica Privacy/GDPR per dettagli su categorie dati, basi giuridiche, GDPR vs LED, diritti interessato, data breach.

Intelligenza Artificiale — concetti base

L'Intelligenza Artificiale (IA) è un campo dell'informatica che sviluppa sistemi capaci di simulare aspetti dell'intelligenza umana. Tipologie: IA generativa (es. ChatGPT, immagini), IA per riconoscimento (volti, oggetti, voce), IA decisionale, sistemi predittivi. Reg. UE 2024/1689 (AI Act): regolamento europeo sull'IA, in vigore progressivamente (parti dal 2025-2027); classifica i sistemi IA per livelli di rischio (proibiti, alto rischio, rischio limitato, minimo). Per la PA: l'uso dell'IA nella PA richiede cautela, verifica umana, tutela dati e rispetto delle regole europee. Aree di applicazione potenziale: assistenti virtuali per cittadini, analisi di documenti, supporto decisionale (sempre con verifica umana). Cura: no decisioni automatiche su persone senza supervisione, trasparenza nei processi, tutela dei dati personali (GDPR), valutazione di impatto. Per la PL: argomento di sfondo culturale; eventuali strumenti IA usati con cautela (es. analisi targhe, rilevamento anomalie ZTL); decisioni operative restano umane.

Social media istituzionali

I social media sono canali di comunicazione PA verso cittadini. Principali: Facebook (grande pubblico), Instagram (giovani, visuale), LinkedIn (professionale), YouTube (video), X/Twitter (news). PA usa per: informazioni, trasparenza, coinvolgimento. Policy chiare su contenuti, tono, gestione commenti. Attenzione: privacy cittadini, diffamazione, crisis management. AGID linee guida. PL: profili ufficiali Corpo, contenuti educativi e trasparenti.

PL digitalizzazione e banche dati

La digitalizzazione della Polizia Locale comporta l'uso di strumenti informatici e banche dati per l'attività operativa. Banche dati tipiche per la PL: ANPR (anagrafe nazionale), MCTC (motorizzazione: veicoli, patenti), PRA/ACI (proprietà veicoli), ANIA (coperture assicurative veicoli), portali comunali (ZTL, gestionale verbali, anagrafe locale, SUAP), catasto se autorizzati. Eventuali banche dati interforze (es. SDI/CED) secondo autorizzazioni, qualifiche e convenzioni (accesso non automatico per la PL e dipendente da regolamenti specifici). Strumenti operativi: palmari, verbali digitali, fotografie nel rispetto privacy e regolamenti interni del Corpo. Body-cam e dispositivi mobili: se previsti da regolamenti e DPIA (non strumento standard senza base regolamentare). Principi fondamentali: accesso solo se autorizzati + per

CAD, documento informatico e firme

CAD — Codice dell'Amministrazione Digitale

Il CAD (Codice dell'Amministrazione Digitale, D.Lgs. 82/2005) è la legge fondamentale della digitalizzazione della PA italiana. Disciplina: documento informatico e suo valore giuridico, firme elettroniche (semplice, avanzata, qualificata, digitale), PEC e domicilio digitale (artt. 3-bis, 6-bis, 6-quater), pagamenti elettronici (PagoPA), servizi online della PA, identità digitale (SPID, CIE), protocollo informatico, conservazione digitale, accessibilità. Modifiche progressive: D.Lgs. 217/2017, D.L. 76/2020, D.L. 77/2021. Principi cardine: equivalenza giuridica del documento digitale, dovere di digitalizzazione delle PA, diritto del cittadino all'uso delle tecnologie. AgID (Agenzia per l'Italia Digitale) coordina l'attuazione. Per la PL: cornice normativa per atti digitali, PEC, SEND, App IO, banche dati.

Documento informatico — valore legale

Il documento informatico (CAD artt. 20-23) è la rappresentazione digitale di atti, fatti o dati giuridicamente rilevanti. Tipologie: 1) Documento informatico originale (nato digitale, es. atto sottoscritto digitalmente); 2) Copia informatica di documento analogico (es. scansione di un atto cartaceo); 3) Copia analogica di documento informatico (es. stampa di un atto digitale, con attestazione di conformità del pubblico ufficiale); 4) Duplicato informatico (riproduzione digitale informaticamente identica). Valore giuridico: il documento informatico ha piena efficacia se conforme al CAD (firma digitale, conservazione, ecc.). Per la PL: i verbali e gli atti possono essere nativamente digitali; le copie cartacee possono essere notificate previa attestazione di conformità del pubblico ufficiale.

Firme elettroniche: semplice, avanzata, qualificata, digitale

Il CAD (artt. 24-32) e il Reg. UE 910/2014 (eIDAS) disciplinano le firme elettroniche con tre livelli di sicurezza crescente: 1) Firma elettronica semplice (FES): qualsiasi metodo elettronico (es. spunta su click, foto firma); valore probatorio limitato; 2) Firma elettronica avanzata (FEA): identifica con certezza il firmatario, è collegata univocamente, è creata con strumenti che il firmatario controlla, garantisce integrità del documento; 3) Firma elettronica qualificata (FEQ): FEA basata su certificato qualificato + dispositivo qualificato (es. smartcard, USB token); equivalente alla firma autografa autenticata. Firma digitale: è una FEQ italiana basata su certificati qualificati. Formati: PAdES (per PDF), CAdES (formato .p7m), XAdES (XML). Per la PL: la firma digitale è strumento essenziale per atti, ordinanze, comunicazioni con valore legale.

Marca temporale

La marca temporale (CAD art. 41 + Linee guida AgID) è un servizio che attribuisce data e ora certa a un documento informatico, attestando la sua esistenza in un momento specifico. Funzione: 1) prova dell'esistenza del documento prima di una certa data; 2) conservazione della validità della firma digitale anche dopo la scadenza del certificato (se la marca è apposta prima della scadenza); 3) antidatazione prevenuta. Soggetti: erogata da TSA (Time Stamping Authority) qualificate, accreditate AgID. Tecnologia: cifratura asincrona; il documento viene "marcato" con timestamp ufficiale + firma del TSA. Formati: timestamp integrato nel file (PAdES) o separato (.tsr). Valore probatorio: piena efficacia giuridica fino a querela di falso. Per la PL: utile per atti con effetti differiti, contrattualistica, conservazione documenti per termini lunghi.

Conservazione digitale

La conservazione digitale (CAD artt. 43-44 + Linee guida AgID 2020) è il processo che garantisce la conservazione nel tempo dei documenti informatici mantenendo: integrità (non alterabilità), autenticità (riconoscibilità del firmatario/origine), leggibilità (formati standard utilizzabili nel tempo), disponibilità (recuperabilità). Differenza con

Protocollo, PEC e SEND

Protocollo informatico

Il protocollo informatico (CAD artt. 50 ss. + D.P.R. 445/2000) è il sistema digitale di registrazione dei documenti in entrata e in uscita della PA. Funzione: garantire data certa, identificare in modo univoco ogni documento, tracciare il flusso documentale. Contenuto della registrazione: numero di protocollo (univoco e progressivo), data e ora di registrazione, mittente (per documenti in entrata) o destinatario (per documenti in uscita), oggetto del documento, classificazione (in base al titolario di archivio del Comune), fascicolazione (collegamento al fascicolo del procedimento). Obbligatorio per atti formali (entrata/uscita); non obbligatorio per comunicazioni interne (di norma con sistema separato di "movimento interno"). Per la PL: tutti gli atti formali (verbali, ordinanze, comunicazioni esterne) sono protocollati; cura nella corretta registrazione.

Fascicolo informatico

Il fascicolo informatico (CAD art. 41 + D.P.R. 445/2000 art. 64) è la raccolta digitale dei documenti relativi a un singolo procedimento amministrativo. Funzione: organizzare in modo strutturato tutti gli atti che compongono il procedimento (istanze, verbali, ordinanze, comunicazioni, ricorsi, ecc.). Contenuto: documenti protocollati + comunicazioni interne pertinenti + atti del procedimento. Caratteristiche: identificazione univoca (numero fascicolo), tracciabilità completa (storia del procedimento), accesso controllato (solo personale autorizzato), conservazione congiunta con il procedimento. Distinzione: protocollo singolo registra ogni documento; fascicolo li raggruppa per procedimento. Per la PL: ogni procedimento (sanzionatorio, di accertamento, ecc.) ha proprio fascicolo informatico; cura nella completezza + chiusura del fascicolo a procedimento concluso.

Domicilio digitale: INI-PEC, INAD, IPA

Il domicilio digitale (CAD art. 3-bis) è l'indirizzo elettronico (PEC) che funge da domicilio legale per le notifiche e comunicazioni della PA. Banche dati pubbliche: 1) INI-PEC (Indice Nazionale degli Indirizzi PEC delle imprese e professionisti, gestito da InfoCamere): obbligatorio per imprese (iscrizione CCIAA) e professionisti iscritti agli ordini; 2) INAD (Indice Nazionale dei Domicili Digitali delle persone fisiche, gestito da AgID, operativo dal 6 luglio 2023): volontario per cittadini che attivano il domicilio digitale via SPID/CIE/CNS; 3) IPA (Indice delle Pubbliche Amministrazioni, gestito da AgID): per enti pubblici. Uso PA: prima di una notifica/comunicazione, la PA verifica nelle banche dati l'esistenza del domicilio digitale del destinatario; se presente, invio via PEC con valore legale. Per la PL: notifica verbali a società/professionisti via INI-PEC; cittadini con INAD; comunicazioni ad altre PA via IPA.

PEC: ricevute e valore legale

La PEC (Posta Elettronica Certificata, D.P.R. 68/2005) è il sistema italiano di posta elettronica con valore legale. Caratteristiche: trasmissione cifrata, ricevute opponibili a terzi, conservazione legale. Ricevute principali: 1) Ricevuta di accettazione: emessa dal gestore PEC del mittente, conferma che la PEC è stata accettata per l'invio; 2) Ricevuta di consegna: emessa dal gestore PEC del destinatario, conferma che la PEC è arrivata nella casella (anche se non letta). Busta di trasporto: messaggio "wrapper" che contiene il messaggio originale + ricevute (formato .eml). Allegati: file allegati al messaggio originale. Differenza con email ordinaria: PEC ha valore legale (equivalente raccomandata A/R verso domicilio digitale), email ordinaria no. Per la PL: PEC strumento essenziale per notifiche, comunicazioni con valore legale, trasmissione atti.

SEND — Piattaforma Notifiche Digitali

La SEND (Servizio Notifiche Digitali) è la piattaforma nazionale per le notifiche digitali della PA, gestita da PagoPA S.p.A. Funzione: sistema unico per inviare notifiche con valore legale, integrato con altri servizi nazionali. Funzionamento: la PA carica l'atto sulla SEND; la piattaforma

Servizi PA, credenziali e banche dati

PagoPA e IUV — pagamenti digitali PA

Il PagoPA è il sistema nazionale dei pagamenti elettronici verso la PA (CAD art. 5 + L. 89/2014). Funzione: standardizzare e tracciare i pagamenti dei cittadini alle PA. Componenti: 1) IUV (Identificativo Univoco di Versamento): codice univoco di ogni avviso di pagamento; 2) Avviso di pagamento: documento PDF con QR code + IUV + importo + dati PA; 3) Ricevuta telematica (RT): rilasciata a pagamento avvenuto, prova legale del pagamento. Modalità di pagamento: app bancaria, home banking, ATM, sportelli postali, tabaccai abilitati, App IO. Per la PL: pagamento delle multe CdS + sanzioni amministrative; tracciabilità automatica; riconciliazione rapida. La SEND integra automaticamente l'avviso PagoPA con la notifica.

App IO — App ufficiale dei servizi pubblici

L'App IO è l'applicazione mobile ufficiale dei servizi pubblici italiani, gestita da PagoPA S.p.A. Funzioni: 1) Notifiche dalle PA (avvisi, comunicazioni, scadenze); 2) Pagamenti integrati via PagoPA; 3) Servizi comunali (es. iscrizione asili, certificati, ZTL); 4) Accesso ai servizi PA con SPID/CIE; 5) Documenti (es. certificati digitali, IO Italia). Integrazione SEND: notifiche degli atti formali della PA visibili in app + pagamento integrato. Vantaggi: unico punto di accesso ai servizi PA + comunicazioni rapide. Per la PL: il cittadino riceve in App IO l'avviso di un verbale CdS notificato via SEND; può pagare in app con un click via PagoPA. Diffusione: progressiva tra cittadini (milioni di utenti); progressiva integrazione di Comuni e PA.

SPID, CIE, CNS — identità digitale

L'identità digitale italiana si articola in tre principali strumenti: 1) SPID (Sistema Pubblico di Identità Digitale): credenziali (username + password + eventuali codici/app); 3 livelli di sicurezza (1: solo password — basilare; 2: password + codice OTP — standard; 3: dispositivo crittografico — alto); normalmente gratuito per il cittadino nei livelli ordinari, salvo condizioni dei singoli gestori; 2) CIE (Carta di Identità Elettronica): documento fisico chip + servizi digitali; richiede lettore NFC o app CieID per uso online; livelli di sicurezza simili a SPID; 3) CNS (Carta Nazionale dei Servizi): smart card con certificato digitale; richiede lettore smart card + software; usata per servizi specifici (es. firma, sanità, fisco). Uso: accesso servizi PA online (App IO, portali, servizi nazionali). Identità digitale europea (eIDAS 2.0): portafoglio digitale UE in implementazione progressiva.

Sicurezza delle credenziali nella PA

La sicurezza delle credenziali nella PA è un aspetto cruciale per evitare data breach e accessi abusivi. Principi: 1) Password personali e robuste: lunghezza minima, complessità, cambiata periodicamente, mai condivisa; 2) 2FA / MFA (autenticazione a due/più fattori): password + codice OTP o app; raccomandata per accessi sensibili; 3) Divieto di condivisione delle credenziali con colleghi (anche per "fare prima"); 4) Blocco schermo quando ci si allontana dalla postazione (Win+L); 5) Logout alla fine del lavoro; 6) Accessi tracciati (log) per audit; 7) Riconoscimento phishing: non cliccare link sospetti, no fornire credenziali via email; 8) Aggiornamento software e antivirus. Conseguenze violazioni: disciplinare + responsabilità penale (art. 615-ter c.p. accesso abusivo, fino 5 anni se PU). Per la PL: cura nelle banche dati interforze, gestionali verbali, sistemi sensibili.

Banche dati della Polizia Locale

Le banche dati utilizzate dalla Polizia Locale sono numerose e ciascuna ha regole specifiche di accesso. Banche dati tipiche per la PL: 1) ANPR (Anagrafe Nazionale Popolazione Residente) — per dati anagrafici cittadini; 2) MCTC (Motorizzazione Civile e Trasporti) — per veicoli, patenti, revisioni; 3) PRA/ACI (Pubblico Registro Automobilistico) — per proprietà veicoli; 4) ANIA — banca dati coperture assicurative veicoli; 5) Portali comunali: ZTL, gestione verbali, anagrafe locale, SUAP, catasto se autorizzati; 6) Eventuali banche dati interforze secondo

Sicurezza, formati file, accessibilità

Reati informatici di base

I reati informatici sono fattispecie penali specifiche per condotte illecite nel mondo digitale, particolarmente rilevanti per la PA. Reati principali: 1) Art. 615-ter c.p. (accesso abusivo a sistema informatico): punisce chi si introduce abusivamente in un sistema protetto; fino 3 anni, 1-5 anni se commesso da PU/IPS; 2) Art. 635-bis ss. c.p. (danneggiamento informatico): danneggiamento di informazioni, sistemi, comunicazioni; fino 4 anni; 3) Art. 640-ter c.p. (frode informatica): alterazione di sistema informatico per profitto; fino 5 anni; 4) Art. 167 D.Lgs. 196/2003 (trattamento illecito di dati personali): per profitto/danno; fino 3 anni; 5) Art. 326 c.p. (rivelazione segreti d'ufficio): per PU/IPS che rivela info riservate; fino 3 anni. Concorso: spesso più reati insieme. Per la PL: rischio diretto per accesso abusivo banche dati + rivelazione segreti.

Phishing e social engineering

Il phishing è la tecnica fraudolenta che cerca di ottenere credenziali, dati o azioni dagli utenti tramite comunicazioni ingannevoli (email, SMS, telefonate). Il social engineering è l'ingannare le persone usando aspetti psicologici. Tipologie tipiche: 1) Email falsa che impersona banca, fornitore, PA; 2) Link malevoli che simulano siti reali; 3) Allegati pericolosi (PDF, ZIP, file Office con macro) che installano malware; 4) Finti fornitori che chiedono dati o pagamenti urgenti; 5) Finti superiori gerarchici che chiedono trasferimenti urgenti (CEO fraud); 6) SMS phishing (smishing) e vishing (telefonico). Cosa fare in caso di sospetto: NON cliccare, NON aprire allegati, NON rispondere; verificare con il presunto mittente tramite altro canale; segnalare all'IT; cancellare. Per la PL: target frequente per phishing istituzionale; cura nel riconoscimento.

Ransomware nella PA

Il ransomware è un tipo di malware che cifra i dati dei sistemi infettati e richiede un riscatto (in cripto-valuta) per restituire l'accesso. Effetti: blocco delle attività della PA, perdita dei dati, danno economico e reputazionale, possibile data breach. Vie di infezione: phishing (email con allegato malevolo), vulnerabilità software non aggiornate, accessi remoti compromessi (RDP). Prevenzione: backup regolari e testati (offline o cloud sicuro), formazione del personale, antivirus aggiornato, sistemi patchati, segmentazione rete. In caso di infezione: NON pagare il riscatto (di norma), NON improvvisare, disconnettere subito i sistemi compromessi dalla rete, segnalare immediatamente all'ufficio IT + DPO + CSIRT-Italia (Computer Security Incident Response Team), notifica al Garante se dati personali (entro 72h). Ricorso ai backup è la soluzione preferita. Per la PL: rischio elevato, cura nelle prevenzioni.

Gestione allegati e formati file

I formati file principali nella PA: 1) PDF (Portable Document Format): standard per documenti finali, supporta firma digitale (PAdES); 2) PDF/A: variante per archiviazione a lungo termine, formato preferito per conservazione digitale; 3) DOCX/ODT: documenti Word/LibreOffice modificabili; 4) XLSX/ODS: fogli di calcolo; 5) CSV: dati tabellari semplici (testo separato da virgole), per scambio dati; 6) ZIP/RAR: archivio compresso, può contenere più file; 7) JPG/PNG: immagini; 8) MP4: video. File eseguibili pericolosi: .exe, .scr, .bat, .vbs, .cmd, .ps1 — possono installare malware; MAI aprire se non da fonte certa. File Office con macro (.docm, .xlsm): possono contenere codice malevolo, alert al apertura. Per la PA: prediligere PDF/A per archiviazione, DOCX per lavoro corrente; diffidare di allegati eseguibili anche da mittenti apparentemente legittimi.

Accessibilità dei documenti digitali

L'accessibilità digitale (L. 4/2004 "Stanca" + D.Lgs. 106/2018 + L. 67/2006) è l'obbligo per la PA di rendere i propri siti web e documenti digitali utilizzabili da tutti, inclusi cittadini con disabilità (visiva, uditiva, motoria, cognitiva). Strumenti di accessibilità: 1) PDF accessibili

Mappa concettuale

Informatica di base · argomenti e lezioni collegate

Informatica di base

Lezioni principali

- **Concetti base di informatica per il concorso**

  Hardware, software, reti, sicurezza, posta elettronica: i fondamentali richiesti.

- **SPID, CIE, CNS: l'identità digitale nella PA**

  Per accedere ai servizi digitali della PA servono strumenti di identità: SPID, CIE (Carta d'Identità Elettronica), CNS (Carta Nazionale dei Servizi). Ciascuno ha caratteristiche e livelli di sicurezza.

- **Sicurezza informatica di base: password, phishing, ransomware**

  La cybersecurity di base per la PA include misure tecniche e comportamentali per proteggere sistemi, dati e operatori. Aspetti chiave: 1) Password robuste e personali: lunghezza, complessità, univocità, no condivisione; 2) 2FA/MFA dove disponibile; 3) Phishing: riconoscere email sospette, non cliccare link, non aprire allegati non attesi, segnalare all'IT; 4) Ransomware: backup off-line, antivirus aggiornato, formazione; 5) Aggiornamenti software regolari; 6) Blocco schermo quando ci si allontana; 7) Logout a fine giornata; 8) No credenziali condivise (mai); 9) Riconoscimento social engineering (telefonate sospette, finti superiori, urgenze artificiose); 10) Segnalazione tempestiva di incidenti all'IT + DPO + eventualmente CSIRT-Italia. Per la PL: target frequente di phishing istituzionale; cura nelle banche dati interforze; conoscenza dei rischi specifici (ransomware, accessi abusivi); cooperazione con IT comunale + Polizia Postale per casi gravi.

- **Reti e Internet: fondamentali**

  Comprendere cos'è una rete e come funziona Internet è base per i concorsi: LAN/WAN, protocollo TCP/IP, indirizzi IP, DNS, HTTP/HTTPS.

- **PEC: come funziona tecnicamente**

  La PEC (Posta Elettronica Certificata, D.P.R. 68/2005 + CAD artt. 6, 48) è il sistema italiano di posta elettronica con valore legale. Caratteristiche tecniche: trasmissione cifrata tra gestori PEC accreditati AgID, ricevute opponibili (accettazione + consegna), busta di trasporto in formato standard. Valore legale: la PEC produce ricevute opponibili e ha valore legale nei casi previsti, soprattutto verso soggetti dotati di domicilio digitale. La consegna nella casella PEC perfeziona la notifica indipendentemente dalla lettura. Per la PL: strumento essenziale per notifiche, comunicazioni con valore legale, trasmissione atti tra PA. Verifica dell'indirizzo PEC nelle banche dati pubbliche (INI-PEC, INAD, IPA) prima dell'invio per evitare errori. Differenza con email ordinaria: PEC ha valore legale, email no.

Fondamenti di informatica

Hardware e software — componenti del computer

Il computer è composto da hardware (componenti fisici: CPU, RAM, storage, scheda madre, GPU, periferiche) e software (programmi: sistema operativo, applicativi, driver). CPU esegue istruzioni; RAM memoria volatile; storage (SSD/HDD) memoria permanente; periferiche input (tastiera, mouse) e output (monitor, stampante). Conoscere i componenti aiuta a capire prestazioni, manutenzione e acquisti informati. Base per ogni utilizzo professionale.

Il sistema operativo — Windows di base

Il sistema operativo (SO) gestisce hardware e software. Windows è il più diffuso nelle PA italiane. Elementi chiave: desktop (schermata principale), barra delle applicazioni, menu Start, Esplora file (cartelle/file), Pannello di controllo / Impostazioni, task manager. File: nome + estensione (.docx, .pdf). Cartelle: organizzazione gerarchica. Shortcut tastiera accelerano produttività. Sicurezza: password, blocco schermo.

File e cartelle — organizzazione dati

Organizzare file e cartelle efficacemente è fondamentale. Principi: gerarchia chiara, nomi significativi, struttura standardizzata. Nomi file: descrittivi, data se rilevante, no caratteri speciali. Cartelle: per progetto, anno, tipologia. Ricerca: con Esplora file o motore integrato. Ordinamento: nome, data, tipo, dimensione. Compressione zip per riduzione dimensioni/invio. Attenzione: caratteri illegali (\/:?\"|).

Reti e Internet — concetti di base

Le reti connettono dispositivi. LAN (Local Area Network): ufficio, casa. WAN (Wide Area Network): aree estese. Internet: rete globale. WiFi: connessione wireless. Ethernet: via cavo. Router/modem: collegano al provider. IP: identifica dispositivi. DNS: traduce nomi in indirizzi. Cloud: dati su server remoti. Principali: sicurezza (VPN, firewall), prestazioni (velocità), affidabilità.

Browser e navigazione web

Il browser è il programma per navigare su Internet. Più diffusi: Chrome (Google), Edge (Microsoft), Firefox (Mozilla), Safari (Apple). Elementi: barra URL, schede, segnalibri, cronologia, download. HTTPS: sito sicuro (lucchetto). Cookie: piccoli dati siti. Password: salvataggio automatico (da usare con cautela). Estensioni: funzionalità aggiuntive. Privacy: modalità incognito.

Email e PEC — comunicazione digitale

L'email è strumento fondamentale di comunicazione. Componenti: indirizzo (nome@dominio), oggetto, corpo, allegati. Client: Outlook, Thunderbird, webmail. PEC (Posta Elettronica Certificata): equivale a raccomandata AR per valore legale. Obbligatoria per imprese e PA. Galateo email: oggetto chiaro, grammatica corretta, firma. Attenzione: phishing, spam, virus. Archiviazione importante.

Password e sicurezza di base

Le password sono la prima difesa dei tuoi dati. Requisiti: lunghezza (12+ caratteri), complessità (maiuscole, minuscole, numeri, simboli), unicità (diversa per ogni servizio), segretezza. Autenticazione a due fattori (2FA): sicurezza aggiuntiva. Password manager per gestire molte password. Attenzione: non condividere, non scrivere in chiaro, non riutilizzare. Phishing: mai inserire password da link email sospette.

Stampa, scansione, digitalizzazione

Gestire documenti cartacei e digitali è routine PA. Stampanti: locali o di rete; laser (veloce) o inkjet; multifunzione (stampa, scansione, copia, fax). Scansioni: OCR per testo modificabile; PDF/A per archiviazione. Risoluzione: 300 DPI standard. Digitalizzazione: processo PA di dematerializzazione. Formati: PDF per condivisione, PDF/A per archivio, TIFF per alta qualità. Firma digitale su PDF generato.

Backup e sicurezza dei dati

Il backup è la copia di sicurezza di dati e file, fondamentale per protezione contro perdita di dati (guasti hardware, malware, errori, disastri). Tipologie: completo (tutti i dati), incrementale (solo modifiche), differenziale, snapshot. Regola 3-2-1: 3 copie dei dati, 2 supporti diversi, 1 off-site. Per la PA: backup centralizzato gestito dall'IT del Comune; il singolo dipendente deve salvare nei percorsi ufficiali dell'ente, non solo su chiavette o cloud personali. Strumenti raccomandati: cartelle di rete del Comune, cloud comunale, sistemi gestionali con backup automatico. Cosa evitare: file su desktop personale del PC, USB personali, cloud privato (Google Drive, Dropbox personale), email come archivio. Recupero: in caso di perdita, IT recupera da backup centralizzato. Per la PL: verbali, foto, documenti operativi salvati nei sistemi gestionali del Comune o cartelle di rete dedicate; mai su strumenti personali.

Competenze digitali — framework europeo

Le competenze digitali sono essenziali nella PA moderna. DigComp (Digital Competence Framework) UE identifica 5 aree: 1. Informazione e data literacy, 2. Comunicazione e collaborazione, 3. Creazione di contenuti digitali, 4. Sicurezza, 5. Problem solving. Livelli: base, intermedio, avanzato, altamente specializzato. Italia: PNRR promuove alfabetizzazione. AGID coordina. Formazione continua per PA. Certificazioni: ECDL/ICDL, EIPASS.

Office e strumenti digitali PA

Word e Writer — videoscrittura

I word processor (Microsoft Word, LibreOffice Writer) sono strumenti fondamentali per creare e formattare documenti. Funzioni principali: digitazione, formattazione (font, grassetto, stili), paragrafi (allineamento, indentazione), tabelle, immagini, intestazioni/piè, stampa unione per invii massivi. Salvataggio: .docx (Word), .odt (Writer), .pdf per condivisione. Revisioni per collaborazione. Essenziali per PA: verbali, relazioni, corrispondenza.

Excel e Calc — fogli di calcolo

I fogli di calcolo (Excel, LibreOffice Calc) gestiscono dati in righe e colonne. Celle con riferimenti (A1, B2). Formule iniziano con =. Funzioni comuni: SOMMA, MEDIA, CONTA, SE, CERCA.VERT. Grafici per visualizzare dati. Formattazione celle (numeri, date, valuta). Ordinamento e filtri. Tabelle pivot per analisi. Essenziali per PA: statistiche, bilanci, gestione dati. Esportazione PDF o CSV per interoperabilità.

PowerPoint e presentazioni

Le presentazioni (PowerPoint, LibreOffice Impress, Google Slides) comunicano idee tramite slide (diapositive) sequenziali. Elementi: titolo, testo, immagini, grafici, video, animazioni, transizioni. Temi predefiniti per coerenza. Modalità presentazione a schermo intero. Esportazione: PPTX, PDF, video. Principi: meno è più (poche parole per slide), contrasto, coerenza. Usi PA: comunicazione istituzionale, formazione, conferenze.

SPID e CIE — identità digitale

L'identità digitale italiana si articola in SPID, CIE e CNS (CAD art. 64). SPID (Sistema Pubblico di Identità Digitale): credenziali con 3 livelli di sicurezza; normalmente gratuito per il cittadino nei livelli ordinari, salvo condizioni dei singoli gestori (alcuni gestori applicano costi per servizi premium o livelli alti). CIE (Carta di Identità Elettronica): documento fisico con chip NFC; per uso digitale richiede lettore NFC o app CieID + PIN (rilasciato all'emissione). CNS (Carta Nazionale dei Servizi): smart card con certificato digitale; richiede lettore smart card + software specifico; usata per servizi specifici (fisco, sanità, ecc.). eIDAS 2.0 (Reg. UE 2024/1183): in implementazione l'EU Digital Identity Wallet (in Italia: ITwallet). Per la PA: SPID e CIE sono i principali strumenti per cittadini per accesso ai servizi online (App IO, portali, ecc.).

Firma digitale — come funziona

La firma digitale è equivalente giuridico della firma autografa, ma più sicura. Si basa su crittografia asimmetrica (chiave pubblica + privata). Certificato qualificato: rilasciato da CA (Certification Authority) accreditate. Formati: PAdES (PDF), CAdES (generico .p7m), XAdES (XML). Strumenti: token USB, smart card + lettore, firma remota (HSM). Uso PA: documenti, contratti, processo civile telematico. Obbligatoria per dirigenti e atti formali.

PagoPA — pagamenti digitali verso la PA

Il PagoPA (Pagamenti Pubblica Amministrazione) è il sistema unico nazionale per pagare verso PA. Gestito da PagoPA SpA. Cittadini pagano tributi, multe, tasse, servizi. Modalità: home banking, carte, app IO, tabaccai, Poste. Obbligatorio per tutte le PA dal 2021. Codice CBILL (IUV) identifica pagamento. Tracciabilità totale. Ricevuta automatica. PL: verbali CDS pagabili via PagoPA.

Amministrazione Trasparente — portale web

L'Amministrazione Trasparente (D.Lgs. 33/2013) è la sezione obbligatoria del sito web di ogni PA italiana che pubblica dati e atti per finalità di trasparenza e accountability. Sezioni obbligatorie: organizzazione, personale, contributi e sussidi, bandi e gare, performance, opere pubbliche, attività e procedimenti, ecc. Per la PL: dati statistici di attività della PL possono essere pubblicati nel rispetto di privacy, segreto d'ufficio e obblighi specifici di pubblicazione (non tutti i dati operativi sono pubblicabili). Da oscurare: dati sanitari, di minori, giudiziari, eccedenti, dati che rivelino disagio sociale (artt. 26-27 D.Lgs. 33/2013). Durata pubblicazione: di regola 5 anni (art. 8). Vigilanza: ANAC + AgID. Sanzioni per omessa pubblicazione (artt. 46-47). Diritto di accesso civico del cittadino per atti non pubblicati.

Videoconferenze — Teams, Zoom, Meet

Le videoconferenze sono ormai standard di lavoro. Piattaforme: Microsoft Teams (integrato Office 365), Zoom, Google Meet, Cisco Webex. Funzioni: audio/video, chat, condivisione schermo, registrazione, breakout rooms. Requisiti: webcam, microfono, cuffie, connessione stabile. Galateo: mute quando non si parla, camera a richiesta, presentarsi. Sicurezza: password meeting, waiting room. Usi PA: riunioni, formazione, eventi pubblici.

Cloud storage e sincronizzazione

Il cloud storage è la memorizzazione di file su server remoti accessibili via internet, con sincronizzazione automatica tra dispositivi. Servizi popolari: Google Drive, Microsoft OneDrive, Dropbox, iCloud, Apple, ecc. Per la PA: non usare cloud personali non autorizzati per dati d'ufficio. I dati d'ufficio devono essere conservati solo su strumenti approvati dall'ente (cloud comunale, server interno, sistemi conformi). Verifica: conformità GDPR del provider, localizzazione dei dati (preferibilmente UE), accordo DPA con il fornitore, certificazioni di sicurezza. Cloud nazionale (PSN — Polo Strategico Nazionale): progetto italiano per cloud sovrano della PA. Rischi del cloud personale: data breach, perdita di controllo dei dati, violazione GDPR, sanzioni. Per la PL: foto operative, verbali, file di lavoro solo su strumenti dell'ente (non su Google Drive personale, WhatsApp, ecc.).

Sicurezza, privacy, PL digitale

Cybersecurity — minacce e difese

La cybersecurity è la protezione di sistemi informatici da attacchi. Minacce principali: virus (si moltiplicano), trojan (nascosti), ransomware (cripta dati per riscatto), spyware, adware, worm, rootkit. Attacchi: phishing (email fraudolente), brute force (password), DDoS (sovraccarico), zero-day. Difese: antivirus aggiornati, firewall, backup, aggiornamenti, formazione, 2FA. PL: attenzione a banche dati, credenziali, dispositivi mobili.

Privacy e GDPR applicata

La privacy applicata all'informatica è cruciale per la PA. Sintesi (la materia è approfondita nella specifica materia Privacy/GDPR): principi base in ambito IT: 1) Password robuste e personali, 2FA dove possibile; 2) Banche dati: accesso solo per finalità di servizio, con tracciamento; 3) Email: cifratura per dati sensibili, attenzione a destinatari, no condivisione di credenziali; 4) Allegati: firmati digitalmente per atti formali, no dati eccedenti; 5) Stampa documenti: con cura (no stampe abbandonate in stampante), distruzione sicura quando non più necessari (trituratore). Reati specifici: art. 615-ter c.p. (accesso abusivo), 326 c.p. (rivelazione segreto), 167 D.Lgs. 196/2003 (trattamento illecito). Per la PL: cura quotidiana nei trattamenti; coordinamento con DPO comunale; formazione obbligatoria. Approfondimenti: vedere materia specifica Privacy/GDPR per dettagli su categorie dati, basi giuridiche, GDPR vs LED, diritti interessato, data breach.

Intelligenza Artificiale — concetti base

L'Intelligenza Artificiale (IA) è un campo dell'informatica che sviluppa sistemi capaci di simulare aspetti dell'intelligenza umana. Tipologie: IA generativa (es. ChatGPT, immagini), IA per riconoscimento (volti, oggetti, voce), IA decisionale, sistemi predittivi. Reg. UE 2024/1689 (AI Act): regolamento europeo sull'IA, in vigore progressivamente (parti dal 2025-2027); classifica i sistemi IA per livelli di rischio (proibiti, alto rischio, rischio limitato, minimo). Per la PA: l'uso dell'IA nella PA richiede cautela, verifica umana, tutela dati e rispetto delle regole europee. Aree di applicazione potenziale: assistenti virtuali per cittadini, analisi di documenti, supporto decisionale (sempre con verifica umana). Cura: no decisioni automatiche su persone senza supervisione, trasparenza nei processi, tutela dei dati personali (GDPR), valutazione di impatto. Per la PL: argomento di sfondo culturale; eventuali strumenti IA usati con cautela (es. analisi targhe, rilevamento anomalie ZTL); decisioni operative restano umane.

Social media istituzionali

I social media sono canali di comunicazione PA verso cittadini. Principali: Facebook (grande pubblico), Instagram (giovani, visuale), LinkedIn (professionale), YouTube (video), X/Twitter (news). PA usa per: informazioni, trasparenza, coinvolgimento. Policy chiare su contenuti, tono, gestione commenti. Attenzione: privacy cittadini, diffamazione, crisis management. AGID linee guida. PL: profili ufficiali Corpo, contenuti educativi e trasparenti.

PL digitalizzazione e banche dati

La digitalizzazione della Polizia Locale comporta l'uso di strumenti informatici e banche dati per l'attività operativa. Banche dati tipiche per la PL: ANPR (anagrafe nazionale), MCTC (motorizzazione: veicoli, patenti), PRA/ACI (proprietà veicoli), ANIA (coperture assicurative veicoli), portali comunali (ZTL, gestionale verbali, anagrafe locale, SUAP), catasto se autorizzati. Eventuali banche dati interforze (es. SDI/CED) secondo autorizzazioni, qualifiche e convenzioni (accesso non automatico per la PL e dipendente da regolamenti specifici). Strumenti operativi: palmari, verbali digitali, fotografie nel rispetto privacy e regolamenti interni del Corpo. Body-cam e dispositivi mobili: se previsti da regolamenti e DPIA (non strumento standard senza base regolamentare). Principi fondamentali: accesso solo se autorizzati + per finalità di servizio + tracciamento accessi (log) + rispetto privacy (GDPR + LED). Conseguenze abuso: triplice responsabilità (disciplinare + civile + penale art. 615-ter c.p.).

App IO — servizi al cittadino

L'App IO è l'app ufficiale della Repubblica Italiana per accedere a servizi PA. Gestita da PagoPA SpA. Accesso: SPID o CIE. Funzioni: notifiche PA, pagamenti PagoPA, documenti (green pass storicamente), servizi integrati. Notifiche digitali (SEND): equivalgono a raccomandata. Cashback/bonus storici. Crescita: 30+ milioni utenti. Vantaggi: unico punto, sicurezza, gratuità. Obiettivo: cittadinanza digitale per tutti.

Accessibilità digitale e inclusione

L'accessibilità digitale permette a tutti (inclusi disabili) di usare strumenti IT. L. 4/2004 Stanca: siti PA accessibili obbligatori. WCAG (Web Content Accessibility Guidelines) standard internazionale, livelli A/AA/AAA. AGID linee guida attuative. Elementi: testo alternativo immagini, contrasto, tastiera (no solo mouse), screen reader. PA obbligate: sito, documenti, servizi. Dichiarazione accessibilità annuale. Sanzioni per non conformità. PL: documenti accessibili, comunicazioni inclusive.

Smart working — strumenti digitali

Il smart working (lavoro agile) richiede strumenti digitali specifici. Hardware: PC/notebook aziendale, webcam, cuffie, connessione stabile. Software: VPN per rete aziendale, videoconferenza (Teams), collaborazione (cloud storage), chat (Teams, Slack). Sicurezza: 2FA, antivirus, password forti. Organizzazione: postazione dedicata, pause, diritto disconnessione. PA: priorità genitori, L. 104, fragili (D.L. 80/2021). Policy aziendale chiara.

Futuro della digitalizzazione PA

La digitalizzazione PA avanza rapidamente grazie a PNRR (Piano Nazionale Ripresa Resilienza) con miliardi € investiti. Obiettivi 2026: cittadinanza digitale, servizi accessibili, interoperabilità PA. Cloud first: PSN (Polo Strategico Nazionale) per dati strategici. AI: adozione responsabile. Interoperabilità: PDND (Piattaforma Digitale Nazionale Dati). Identità digitale: evoluzione EUDI Wallet UE. Competenze digitali: target 70% cittadini base. PL: evoluzione continua hardware, software, AI.

CAD, documento informatico e firme

CAD — Codice dell'Amministrazione Digitale

Il CAD (Codice dell'Amministrazione Digitale, D.Lgs. 82/2005) è la legge fondamentale della digitalizzazione della PA italiana. Disciplina: documento informatico e suo valore giuridico, firme elettroniche (semplice, avanzata, qualificata, digitale), PEC e domicilio digitale (artt. 3-bis, 6-bis, 6-quater), pagamenti elettronici (PagoPA), servizi online della PA, identità digitale (SPID, CIE), protocollo informatico, conservazione digitale, accessibilità. Modifiche progressive: D.Lgs. 217/2017, D.L. 76/2020, D.L. 77/2021. Principi cardine: equivalenza giuridica del documento digitale, dovere di digitalizzazione delle PA, diritto del cittadino all'uso delle tecnologie. AgID (Agenzia per l'Italia Digitale) coordina l'attuazione. Per la PL: cornice normativa per atti digitali, PEC, SEND, App IO, banche dati.

Documento informatico — valore legale

Il documento informatico (CAD artt. 20-23) è la rappresentazione digitale di atti, fatti o dati giuridicamente rilevanti. Tipologie: 1) Documento informatico originale (nato digitale, es. atto sottoscritto digitalmente); 2) Copia informatica di documento analogico (es. scansione di un atto cartaceo); 3) Copia analogica di documento informatico (es. stampa di un atto digitale, con attestazione di conformità del pubblico ufficiale); 4) Duplicato informatico (riproduzione digitale informaticamente identica). Valore giuridico: il documento informatico ha piena efficacia se conforme al CAD (firma digitale, conservazione, ecc.). Per la PL: i verbali e gli atti possono essere nativamente digitali; le copie cartacee possono essere notificate previa attestazione di conformità del pubblico ufficiale.

Firme elettroniche: semplice, avanzata, qualificata, digitale

Il CAD (artt. 24-32) e il Reg. UE 910/2014 (eIDAS) disciplinano le firme elettroniche con tre livelli di sicurezza crescente: 1) Firma elettronica semplice (FES): qualsiasi metodo elettronico (es. spunta su click, foto firma); valore probatorio limitato; 2) Firma elettronica avanzata (FEA): identifica con certezza il firmatario, è collegata univocamente, è creata con strumenti che il firmatario controlla, garantisce integrità del documento; 3) Firma elettronica qualificata (FEQ): FEA basata su certificato qualificato + dispositivo qualificato (es. smartcard, USB token); equivalente alla firma autografa autenticata. Firma digitale: è una FEQ italiana basata su certificati qualificati. Formati: PAdES (per PDF), CAdES (formato .p7m), XAdES (XML). Per la PL: la firma digitale è strumento essenziale per atti, ordinanze, comunicazioni con valore legale.

Marca temporale

La marca temporale (CAD art. 41 + Linee guida AgID) è un servizio che attribuisce data e ora certa a un documento informatico, attestando la sua esistenza in un momento specifico. Funzione: 1) prova dell'esistenza del documento prima di una certa data; 2) conservazione della validità della firma digitale anche dopo la scadenza del certificato (se la marca è apposta prima della scadenza); 3) antidatazione prevenuta. Soggetti: erogata da TSA (Time Stamping Authority) qualificate, accreditate AgID. Tecnologia: cifratura asincrona; il documento viene "marcato" con timestamp ufficiale + firma del TSA. Formati: timestamp integrato nel file (PAdES) o separato (.tsr). Valore probatorio: piena efficacia giuridica fino a querela di falso. Per la PL: utile per atti con effetti differiti, contrattualistica, conservazione documenti per termini lunghi.

Conservazione digitale

La conservazione digitale (CAD artt. 43-44 + Linee guida AgID 2020) è il processo che garantisce la conservazione nel tempo dei documenti informatici mantenendo: integrità (non alterabilità), autenticità (riconoscibilità del firmatario/origine), leggibilità (formati standard utilizzabili nel tempo), disponibilità (recuperabilità). Differenza con archiviazione: l'archiviazione è il deposito ordinato dei documenti; la conservazione a norma è un processo certificato che garantisce valore probatorio. Soggetti: Responsabile della conservazione (interno alla PA), eventuale Conservatore esterno accreditato (servizio commerciale qualificato). Strumenti: marche temporali periodiche, hash, formati standard (PDF/A, XML), pacchetti di archiviazione, manuali di conservazione. Per la PL: atti digitali (verbali, ordinanze) richiedono conservazione a norma per mantenere valore legale negli anni successivi.

Protocollo, PEC e SEND

Protocollo informatico

Il protocollo informatico (CAD artt. 50 ss. + D.P.R. 445/2000) è il sistema digitale di registrazione dei documenti in entrata e in uscita della PA. Funzione: garantire data certa, identificare in modo univoco ogni documento, tracciare il flusso documentale. Contenuto della registrazione: numero di protocollo (univoco e progressivo), data e ora di registrazione, mittente (per documenti in entrata) o destinatario (per documenti in uscita), oggetto del documento, classificazione (in base al titolario di archivio del Comune), fascicolazione (collegamento al fascicolo del procedimento). Obbligatorio per atti formali (entrata/uscita); non obbligatorio per comunicazioni interne (di norma con sistema separato di "movimento interno"). Per la PL: tutti gli atti formali (verbali, ordinanze, comunicazioni esterne) sono protocollati; cura nella corretta registrazione.

Fascicolo informatico

Il fascicolo informatico (CAD art. 41 + D.P.R. 445/2000 art. 64) è la raccolta digitale dei documenti relativi a un singolo procedimento amministrativo. Funzione: organizzare in modo strutturato tutti gli atti che compongono il procedimento (istanze, verbali, ordinanze, comunicazioni, ricorsi, ecc.). Contenuto: documenti protocollati + comunicazioni interne pertinenti + atti del procedimento. Caratteristiche: identificazione univoca (numero fascicolo), tracciabilità completa (storia del procedimento), accesso controllato (solo personale autorizzato), conservazione congiunta con il procedimento. Distinzione: protocollo singolo registra ogni documento; fascicolo li raggruppa per procedimento. Per la PL: ogni procedimento (sanzionatorio, di accertamento, ecc.) ha proprio fascicolo informatico; cura nella completezza + chiusura del fascicolo a procedimento concluso.

Domicilio digitale: INI-PEC, INAD, IPA

Il domicilio digitale (CAD art. 3-bis) è l'indirizzo elettronico (PEC) che funge da domicilio legale per le notifiche e comunicazioni della PA. Banche dati pubbliche: 1) INI-PEC (Indice Nazionale degli Indirizzi PEC delle imprese e professionisti, gestito da InfoCamere): obbligatorio per imprese (iscrizione CCIAA) e professionisti iscritti agli ordini; 2) INAD (Indice Nazionale dei Domicili Digitali delle persone fisiche, gestito da AgID, operativo dal 6 luglio 2023): volontario per cittadini che attivano il domicilio digitale via SPID/CIE/CNS; 3) IPA (Indice delle Pubbliche Amministrazioni, gestito da AgID): per enti pubblici. Uso PA: prima di una notifica/comunicazione, la PA verifica nelle banche dati l'esistenza del domicilio digitale del destinatario; se presente, invio via PEC con valore legale. Per la PL: notifica verbali a società/professionisti via INI-PEC; cittadini con INAD; comunicazioni ad altre PA via IPA.

PEC: ricevute e valore legale

La PEC (Posta Elettronica Certificata, D.P.R. 68/2005) è il sistema italiano di posta elettronica con valore legale. Caratteristiche: trasmissione cifrata, ricevute opponibili a terzi, conservazione legale. Ricevute principali: 1) Ricevuta di accettazione: emessa dal gestore PEC del mittente, conferma che la PEC è stata accettata per l'invio; 2) Ricevuta di consegna: emessa dal gestore PEC del destinatario, conferma che la PEC è arrivata nella casella (anche se non letta). Busta di trasporto: messaggio "wrapper" che contiene il messaggio originale + ricevute (formato .eml). Allegati: file allegati al messaggio originale. Differenza con email ordinaria: PEC ha valore legale (equivalente raccomandata A/R verso domicilio digitale), email ordinaria no. Per la PL: PEC strumento essenziale per notifiche, comunicazioni con valore legale, trasmissione atti.

SEND — Piattaforma Notifiche Digitali

La SEND (Servizio Notifiche Digitali) è la piattaforma nazionale per le notifiche digitali della PA, gestita da PagoPA S.p.A. Funzione: sistema unico per inviare notifiche con valore legale, integrato con altri servizi nazionali. Funzionamento: la PA carica l'atto sulla SEND; la piattaforma verifica automaticamente se il destinatario ha domicilio digitale (PEC in INAD/INI-PEC); in caso affermativo invia via PEC; in caso negativo la SEND gestisce la raccomandata cartacea tramite Poste Italiane. Integrazioni: avviso di notifica su App IO (notifica visibile in app); pagamento integrato con PagoPA; accesso digitale alle prove di notifica con SPID/CIE. Vantaggi: tracciabilità completa, conservazione digitale, riduzione costi. Adozione: la SEND è la piattaforma nazionale per le notifiche digitali della PA; l'adozione dipende dai processi di integrazione degli enti e dalle norme applicabili.

Servizi PA, credenziali e banche dati

PagoPA e IUV — pagamenti digitali PA

Il PagoPA è il sistema nazionale dei pagamenti elettronici verso la PA (CAD art. 5 + L. 89/2014). Funzione: standardizzare e tracciare i pagamenti dei cittadini alle PA. Componenti: 1) IUV (Identificativo Univoco di Versamento): codice univoco di ogni avviso di pagamento; 2) Avviso di pagamento: documento PDF con QR code + IUV + importo + dati PA; 3) Ricevuta telematica (RT): rilasciata a pagamento avvenuto, prova legale del pagamento. Modalità di pagamento: app bancaria, home banking, ATM, sportelli postali, tabaccai abilitati, App IO. Per la PL: pagamento delle multe CdS + sanzioni amministrative; tracciabilità automatica; riconciliazione rapida. La SEND integra automaticamente l'avviso PagoPA con la notifica.

App IO — App ufficiale dei servizi pubblici

L'App IO è l'applicazione mobile ufficiale dei servizi pubblici italiani, gestita da PagoPA S.p.A. Funzioni: 1) Notifiche dalle PA (avvisi, comunicazioni, scadenze); 2) Pagamenti integrati via PagoPA; 3) Servizi comunali (es. iscrizione asili, certificati, ZTL); 4) Accesso ai servizi PA con SPID/CIE; 5) Documenti (es. certificati digitali, IO Italia). Integrazione SEND: notifiche degli atti formali della PA visibili in app + pagamento integrato. Vantaggi: unico punto di accesso ai servizi PA + comunicazioni rapide. Per la PL: il cittadino riceve in App IO l'avviso di un verbale CdS notificato via SEND; può pagare in app con un click via PagoPA. Diffusione: progressiva tra cittadini (milioni di utenti); progressiva integrazione di Comuni e PA.

SPID, CIE, CNS — identità digitale

L'identità digitale italiana si articola in tre principali strumenti: 1) SPID (Sistema Pubblico di Identità Digitale): credenziali (username + password + eventuali codici/app); 3 livelli di sicurezza (1: solo password — basilare; 2: password + codice OTP — standard; 3: dispositivo crittografico — alto); normalmente gratuito per il cittadino nei livelli ordinari, salvo condizioni dei singoli gestori; 2) CIE (Carta di Identità Elettronica): documento fisico chip + servizi digitali; richiede lettore NFC o app CieID per uso online; livelli di sicurezza simili a SPID; 3) CNS (Carta Nazionale dei Servizi): smart card con certificato digitale; richiede lettore smart card + software; usata per servizi specifici (es. firma, sanità, fisco). Uso: accesso servizi PA online (App IO, portali, servizi nazionali). Identità digitale europea (eIDAS 2.0): portafoglio digitale UE in implementazione progressiva.

Sicurezza delle credenziali nella PA

La sicurezza delle credenziali nella PA è un aspetto cruciale per evitare data breach e accessi abusivi. Principi: 1) Password personali e robuste: lunghezza minima, complessità, cambiata periodicamente, mai condivisa; 2) 2FA / MFA (autenticazione a due/più fattori): password + codice OTP o app; raccomandata per accessi sensibili; 3) Divieto di condivisione delle credenziali con colleghi (anche per "fare prima"); 4) Blocco schermo quando ci si allontana dalla postazione (Win+L); 5) Logout alla fine del lavoro; 6) Accessi tracciati (log) per audit; 7) Riconoscimento phishing: non cliccare link sospetti, no fornire credenziali via email; 8) Aggiornamento software e antivirus. Conseguenze violazioni: disciplinare + responsabilità penale (art. 615-ter c.p. accesso abusivo, fino 5 anni se PU). Per la PL: cura nelle banche dati interforze, gestionali verbali, sistemi sensibili.

Banche dati della Polizia Locale

Le banche dati utilizzate dalla Polizia Locale sono numerose e ciascuna ha regole specifiche di accesso. Banche dati tipiche per la PL: 1) ANPR (Anagrafe Nazionale Popolazione Residente) — per dati anagrafici cittadini; 2) MCTC (Motorizzazione Civile e Trasporti) — per veicoli, patenti, revisioni; 3) PRA/ACI (Pubblico Registro Automobilistico) — per proprietà veicoli; 4) ANIA — banca dati coperture assicurative veicoli; 5) Portali comunali: ZTL, gestione verbali, anagrafe locale, SUAP, catasto se autorizzati; 6) Eventuali banche dati interforze secondo autorizzazioni, qualifiche e convenzioni (es. SDI/CED, accesso non automatico per la PL e dipendente da regolamenti specifici). Principio fondamentale: accesso solo se autorizzati + per finalità di servizio + tracciamento accessi (log) + rispetto privacy. Per la PL: cautela rinforzata, formazione obbligatoria.

Sicurezza, formati file, accessibilità

Reati informatici di base

I reati informatici sono fattispecie penali specifiche per condotte illecite nel mondo digitale, particolarmente rilevanti per la PA. Reati principali: 1) Art. 615-ter c.p. (accesso abusivo a sistema informatico): punisce chi si introduce abusivamente in un sistema protetto; fino 3 anni, 1-5 anni se commesso da PU/IPS; 2) Art. 635-bis ss. c.p. (danneggiamento informatico): danneggiamento di informazioni, sistemi, comunicazioni; fino 4 anni; 3) Art. 640-ter c.p. (frode informatica): alterazione di sistema informatico per profitto; fino 5 anni; 4) Art. 167 D.Lgs. 196/2003 (trattamento illecito di dati personali): per profitto/danno; fino 3 anni; 5) Art. 326 c.p. (rivelazione segreti d'ufficio): per PU/IPS che rivela info riservate; fino 3 anni. Concorso: spesso più reati insieme. Per la PL: rischio diretto per accesso abusivo banche dati + rivelazione segreti.

Phishing e social engineering

Il phishing è la tecnica fraudolenta che cerca di ottenere credenziali, dati o azioni dagli utenti tramite comunicazioni ingannevoli (email, SMS, telefonate). Il social engineering è l'ingannare le persone usando aspetti psicologici. Tipologie tipiche: 1) Email falsa che impersona banca, fornitore, PA; 2) Link malevoli che simulano siti reali; 3) Allegati pericolosi (PDF, ZIP, file Office con macro) che installano malware; 4) Finti fornitori che chiedono dati o pagamenti urgenti; 5) Finti superiori gerarchici che chiedono trasferimenti urgenti (CEO fraud); 6) SMS phishing (smishing) e vishing (telefonico). Cosa fare in caso di sospetto: NON cliccare, NON aprire allegati, NON rispondere; verificare con il presunto mittente tramite altro canale; segnalare all'IT; cancellare. Per la PL: target frequente per phishing istituzionale; cura nel riconoscimento.

Ransomware nella PA

Il ransomware è un tipo di malware che cifra i dati dei sistemi infettati e richiede un riscatto (in cripto-valuta) per restituire l'accesso. Effetti: blocco delle attività della PA, perdita dei dati, danno economico e reputazionale, possibile data breach. Vie di infezione: phishing (email con allegato malevolo), vulnerabilità software non aggiornate, accessi remoti compromessi (RDP). Prevenzione: backup regolari e testati (offline o cloud sicuro), formazione del personale, antivirus aggiornato, sistemi patchati, segmentazione rete. In caso di infezione: NON pagare il riscatto (di norma), NON improvvisare, disconnettere subito i sistemi compromessi dalla rete, segnalare immediatamente all'ufficio IT + DPO + CSIRT-Italia (Computer Security Incident Response Team), notifica al Garante se dati personali (entro 72h). Ricorso ai backup è la soluzione preferita. Per la PL: rischio elevato, cura nelle prevenzioni.

Gestione allegati e formati file

I formati file principali nella PA: 1) PDF (Portable Document Format): standard per documenti finali, supporta firma digitale (PAdES); 2) PDF/A: variante per archiviazione a lungo termine, formato preferito per conservazione digitale; 3) DOCX/ODT: documenti Word/LibreOffice modificabili; 4) XLSX/ODS: fogli di calcolo; 5) CSV: dati tabellari semplici (testo separato da virgole), per scambio dati; 6) ZIP/RAR: archivio compresso, può contenere più file; 7) JPG/PNG: immagini; 8) MP4: video. File eseguibili pericolosi: .exe, .scr, .bat, .vbs, .cmd, .ps1 — possono installare malware; MAI aprire se non da fonte certa. File Office con macro (.docm, .xlsm): possono contenere codice malevolo, alert al apertura. Per la PA: prediligere PDF/A per archiviazione, DOCX per lavoro corrente; diffidare di allegati eseguibili anche da mittenti apparentemente legittimi.

Accessibilità dei documenti digitali

L'accessibilità digitale (L. 4/2004 "Stanca" + D.Lgs. 106/2018 + L. 67/2006) è l'obbligo per la PA di rendere i propri siti web e documenti digitali utilizzabili da tutti, inclusi cittadini con disabilità (visiva, uditiva, motoria, cognitiva). Strumenti di accessibilità: 1) PDF accessibili (PDF/UA): struttura semantica, ordine di lettura, testo alternativo per immagini, etichette per moduli; 2) Testo alternativo (alt text) per immagini: descrive l'immagine per chi non la vede; 3) Contrasto adeguato (testo/sfondo); 4) Titoli strutturati (H1, H2, H3) per navigazione; 5) Documenti leggibili da screen reader (lettori vocali); 6) Sottotitoli e trascrizioni per video. Obblighi PA: documenti pubblicati accessibili (sito web, App IO, ecc.); AgID linee guida. Sanzioni: AgID controlla, eventuali sanzioni amministrative. Per la PL: documenti pubblici (avvisi, ordinanze, comunicati) devono essere accessibili.

Schema basato sui contenuti pubblicati sulla piattaforma. Verifica sempre le fonti normative ufficiali.