# 1. Framework di sicurezza informatica e compliance

## 1.1 Standard internazionali di sicurezza

### 1.1.1 ISO/IEC 27001 e famiglia 27000

- **Definizione e scopo**:
  - Standard internazionale per la gestione della sicurezza delle informazioni
  - Fornisce un framework sistematico per implementare, mantenere e migliorare continuamente un ISMS (Information Security Management System)
  - Pubblicato dall'International Organization for Standardization (ISO) e dall'International Electrotechnical Commission (IEC)
- **Struttura della famiglia ISO 27000**:
  - **ISO/IEC 27000**: Panoramica e vocabolario
  - **ISO/IEC 27001**: Requisiti per un ISMS (certificabile)
  - **ISO/IEC 27002**: Codice di pratiche per i controlli di sicurezza
  - **ISO/IEC 27005**: Gestione del rischio per la sicurezza delle informazioni
  - **ISO/IEC 27017/27018**: Sicurezza nel cloud computing
  - **ISO/IEC 27032**: Cybersecurity
  - **ISO/IEC 27701**: Estensione per la gestione delle informazioni sulla privacy
- **Principali componenti ISO 27001**:
  - **Approccio basato sul rischio**: identificazione, analisi e trattamento del rischio
  - **Leadership e impegno**: responsabilità del management
  - **Pianificazione**: obiettivi di sicurezza e piani per raggiungerli
  - **Supporto**: risorse, competenze, consapevolezza, comunicazione
  - **Operatività**: pianificazione e controllo operativo
  - **Valutazione delle prestazioni**: monitoraggio, misurazione, analisi
  - **Miglioramento**: azioni correttive e miglioramento continuo
- **Ciclo PDCA (Plan-Do-Check-Act)**:
  - **Plan**: stabilire politiche, obiettivi, processi e procedure
  - **Do**: implementare e operare l'ISMS
  - **Check**: monitorare e revisionare l'ISMS
  - **Act**: mantenere e migliorare l'ISMS
- **Processo di certificazione**:
  - Analisi preliminare e gap analysis
  - Implementazione del sistema
  - Audit interno
  - Audit di certificazione (stage 1 e 2)

- Mantenimento e ricertificazione (audit periodici)

### 1.1.2 NIST Cybersecurity Framework

- **Definizione e scopo**:
  - Framework volontario sviluppato dal National Institute of Standards and Technology (USA)
  - Progettato per migliorare la gestione del rischio di cybersecurity nelle infrastrutture critiche
  - Applicabile a organizzazioni di ogni dimensione e settore
  - Focus su risultati di business e sicurezza
- **Struttura del framework**:
  - **Core**: funzioni, categorie, sottocategorie e riferimenti informativi
  - **Implementation Tiers**: livelli di maturità nell'implementazione
  - **Profile**: allineamento delle attività di business con gli obiettivi di sicurezza
- **Funzioni principali (Core)**:
  - **Identify (Identificare)**: comprensione del contesto, asset, rischi
    - Asset management, business environment, governance, risk assessment
    - Sviluppo di una comprensione organizzativa per gestire il rischio di cybersecurity
  - **Protect (Proteggere)**: implementazione di salvaguardie
    - Identity management, awareness training, data security, protective technology
    - Sviluppo e implementazione di controlli di sicurezza appropriati
  - **Detect (Rilevare)**: attività per identificare eventi di sicurezza
    - Anomalies and events, continuous monitoring, detection processes
    - Sviluppo e implementazione di attività per identificare tempestivamente incidenti
  - **Respond (Rispondere)**: azioni a seguito di un incidente
    - Response planning, communications, analysis, mitigation, improvements
    - Sviluppo e implementazione di attività per agire in caso di incidente
  - **Recover (Ripristinare)**: ripristino delle capacità
    - Recovery planning, improvements, communications
    - Sviluppo e implementazione di piani per la resilienza e il ripristino
- **Implementation Tiers**:
  - **Tier 1**: Partial - processi ad hoc e reattivi
  - **Tier 2**: Risk Informed - processi approvati ma non integrati
  - **Tier 3**: Repeatable - processi formali e integrati
  - **Tier 4**: Adaptive - processi che si adattano basandosi su lezioni apprese
- **Vantaggi del framework**:
  - Linguaggio comune per la sicurezza informatica

- Approccio basato sul rischio e orientato al business
- Flessibilità e scalabilità
- Complementare ad altri standard (es. ISO 27001)
- Evoluzione continua (aggiornato regolarmente)

### 1.1.3 Common Criteria for IT Security Evaluation (ISO/IEC 15408)

- **Definizione e scopo**:
  - Standard internazionale per la valutazione della sicurezza dei prodotti IT
  - Fornisce un framework per specificare requisiti di sicurezza e valutare prodotti
  - Riconoscimento reciproco tra paesi firmatari (CCRA - Common Criteria Recognition Arrangement)
  - Livello di garanzia progressivo e adattabile alle esigenze
- **Componenti principali**:
  - **Protection Profile (PP)**: set di requisiti indipendenti dall'implementazione
  - **Security Target (ST)**: requisiti specifici per un prodotto particolare
  - **Target of Evaluation (TOE)**: prodotto o sistema sottoposto a valutazione
  - **Evaluation Assurance Level (EAL)**: livello di rigore della valutazione (da 1 a 7)
- **Livelli EAL**:
  - **EAL1**: Functionally tested - analisi funzionale e test
  - **EAL2**: Structurally tested - analisi strutturale e test
  - **EAL3**: Methodically tested and checked - test metodico
  - **EAL4**: Methodically designed, tested and reviewed - progettazione metodica
  - **EAL5**: Semiformally designed and tested - progettazione semi-formale
  - **EAL6**: Semiformally verified design and tested - verifica semi-formale
  - **EAL7**: Formally verified design and tested - verifica formale
- **Processo di valutazione**:
  - Definizione del Security Target
  - Valutazione da parte di un laboratorio accreditato
  - Supervisione dell'autorità di certificazione nazionale
  - Rilascio del certificato
- **Applicazioni comuni**:
  - Dispositivi di rete (router, firewall)
  - Sistemi operativi e software di sicurezza
  - Smart card e dispositivi crittografici
  - Sistemi per infrastrutture critiche

## 1.2 Dall'implementazione tecnica alla conformità normativa

### 1.2.1 Gap Analysis e Risk Assessment

- **Gap Analysis**:
  - **Definizione**: processo di confronto tra stato attuale e stato desiderato
  - **Metodologia**:
    1. Definire lo stato target (requisiti normativi/standard)
    2. Valutare lo stato attuale
    3. Identificare le lacune (gap)
    4. Sviluppare piani d'azione
  - **Tipologie**:
    - Gap analysis tecnica (infrastrutture, configurazioni)
    - Gap analysis organizzativa (processi, procedure)
    - Gap analysis documentale (politiche, standard)
- **Risk Assessment**:
  - **Definizione**: processo sistematico di identificazione e valutazione dei rischi
  - **Approcci metodologici**:
    - **Qualitativo**: basato su scale descrittive (alto/medio/basso)
    - **Quantitativo**: basato su calcoli numerici (es. ALE = SLE × ARO)
    - **Ibrido**: combinazione dei due approcci
  - **Fasi del processo**:
    1. Identificazione degli asset e valutazione
    2. Identificazione delle minacce e vulnerabilità
    3. Analisi della probabilità e impatto
    4. Determinazione del livello di rischio
    5. Identificazione e prioritizzazione dei controlli
- **Relazione con la compliance**:
  - Il risk assessment alimenta la gap analysis
  - Prioritizzazione degli interventi basata sul rischio
  - Approccio risk-based per l'allocazione delle risorse
  - Documentazione dei rischi residui accettati

## 1.2.2 Security Controls Implementation

- **Categorie di controlli di sicurezza**:
  - **Controlli tecnici**: hardware/software (firewall, IDS, crittografia)
  - **Controlli amministrativi**: politiche, procedure, standard
  - **Controlli fisici**: barriere, controllo accessi, allarmi
  - **Controlli preventivi**: impediscono eventi di sicurezza
  - **Controlli detective**: rilevano eventi di sicurezza
  - **Controlli correttivi**: limitano l'impatto di eventi
- **Mappatura controlli-standard**:
  - **ISO 27001 Annex A**: 114 controlli in 14 domini

    - **NIST SP 800-53**: centinaia di controlli in 20 famiglie
    - **CIS Controls**: 20 controlli critici (prioritizzati)
    - **COBIT**: framework per governance IT e controlli
- **Gestione della documentazione**:
    - **Politiche di sicurezza**: obiettivi e direzione generali
    - **Standard**: requisiti specifici e misure obbligatorie
    - **Procedure**: istruzioni dettagliate passo-passo
    - **Linee guida**: consigli e best practices
    - **Evidence**: prove dell'implementazione dei controlli
- **Approccio alla security technology**:
    - **Defense-in-depth**: stratificazione dei controlli
    - **Least privilege**: diritti minimi necessari
    - **Segregation of duties**: separazione dei compiti
    - **Need-to-know**: accesso solo alle info necessarie
    - **Security-by-design**: sicurezza integrata dallo sviluppo

### 1.2.3 Audit di sicurezza e compliance

- **Tipi di audit**:
    - **Audit interno**: condotto dall'organizzazione stessa
    - **Audit di seconda parte**: condotto da partner/fornitori
    - **Audit di terza parte**: condotto da enti indipendenti
    - **Audit di certificazione**: per ottenere certificazioni
    - **Penetration testing**: simulazione di attacchi reali
- **Processo di audit**:
    - **Pianificazione**: definizione scope, obiettivi, criteri
    - **Raccolta evidenze**: interviste, osservazioni, test
    - **Analisi**: valutazione conformità, identificazione gap
    - **Reporting**: documentazione risultati e raccomandazioni
    - **Follow-up**: verifica implementazione azioni correttive
- **Tecniche di verifica**:
    - **Document review**: analisi di politiche e procedure
    - **Interview**: colloqui con personale chiave
    - **Observation**: osservazione diretta dei processi
    - **Sampling**: esame di un campione rappresentativo
    - **Technical testing**: verifiche tecniche e configurazioni
    - **Compliance checking**: verifica conformità a requisiti
- **Gestione delle non conformità**:
    - Classificazione per gravità
    - Root cause analysis

    - Piani di remediation
    - Monitoraggio dell'implementazione
    - Verifica dell'efficacia delle azioni correttive

### 1.2.4 Penetration Testing

- **Definizione**: processo autorizzato di simulazione di attacchi per identificare vulnerabilità
- **Tipologie**:
    - **Black box**: nessuna conoscenza preventiva
    - **White box**: completa conoscenza dell'infrastruttura
    - **Gray box**: conoscenza parziale
    - **External**: simulazione di attacchi dall'esterno
    - **Internal**: simulazione di attacchi dall'interno
    - **Focused**: mirato a sistemi/applicazioni specifiche
- **Metodologia PTES (Penetration Testing Execution Standard)**:
    1. **Pre-engagement**: definizione scope, autorizzazioni, limitazioni
    2. **Intelligence gathering**: raccolta informazioni target
    3. **Threat modeling**: identificazione potenziali vettori di attacco
    4. **Vulnerability analysis**: identificazione vulnerabilità
    5. **Exploitation**: sfruttamento vulnerabilità
    6. **Post exploitation**: mantenimento accesso, escalation privilegi
    7. **Reporting**: documentazione risultati e raccomandazioni
- **Strumenti comuni**:
    - **Reconnaissance**: Shodan, Maltego, theHarvester
    - **Scanning**: Nmap, Nessus, OpenVAS
    - **Exploitation**: Metasploit, Burp Suite, OWASP ZAP
    - **Password attacks**: Hashcat, John the Ripper
    - **Wireless testing**: Aircrack-ng, Kismet
- **Rapporto con la compliance**:
    - Requisito esplicito in molti standard (PCI DSS, ISO 27001)
    - Evidenza di due diligence nella sicurezza
    - Valutazione dell'efficacia dei controlli implementati
    - Identificazione di vulnerabilità non rilevate da audit tradizionali

## 1.3 Documentation e certificazione della sicurezza

### 1.3.1 Struttura documentale per un sistema di gestione della sicurezza

- **Piramide documentale**:
    - **Livello 1 - Politiche**: dichiarazioni di alto livello su intenti e direzione

    - **Livello 2 - Standard**: requisiti specifici per l'implementazione delle politiche
    - **Livello 3 - Procedure**: istruzioni dettagliate
    - **Livello 4 - Work Instructions**: guida passo-passo per attività specifiche
    - **Livello 5 - Records**: evidenze e registrazioni
- **Documenti chiave per ISO 27001**:
    - **Information Security Policy**: documento principale approvato dal management
    - **Statement of Applicability (SoA)**: controlli selezionati e giustificazioni
    - **Risk Assessment Report**: metodologia e risultati della valutazione rischi
    - **Risk Treatment Plan**: azioni per mitigare i rischi identificati
    - **Internal Audit Program**: pianificazione e risultati degli audit interni
    - **Management Review Minutes**: riesame periodico dell'ISMS
    - **Incident Management Procedure**: gestione incidenti di sicurezza
- **Caratteristiche di una buona documentazione**:
    - **Chiara e concisa**: facilmente comprensibile
    - **Pertinente**: focalizzata sulle esigenze dell'organizzazione
    - **Accessibile**: disponibile a chi ne ha bisogno
    - **Aggiornata**: rivista e modificata regolarmente
    - **Approvata**: formalmente autorizzata dal livello appropriato
    - **Versionata**: gestione delle modifiche e dello storico

## 1.3.2 Processo di certificazione

- **Fasi della certificazione ISO 27001**:
    1. **Scelta dell'ente certificatore**: accreditato secondo ISO/IEC 17021
    2. **Pre-assessment** (opzionale): valutazione preliminare
    3. **Stage 1 audit**: revisione documentale e preparazione
    4. **Gap remediation**: correzione delle non conformità identificate
    5. **Stage 2 audit**: valutazione dell'implementazione e dell'efficacia
    6. **Certification**: emissione del certificato (validità 3 anni)
    7. **Surveillance audits**: verifiche annuali di mantenimento
    8. **Recertification**: rinnovo completo dopo 3 anni
- **Tipi di non conformità**:
    - **Major**: violazione significativa di un requisito dello standard
    - **Minor**: deviazione limitata che non compromette l'efficacia
    - **Observation**: potenziale area di miglioramento, non non-conformità
- **Vantaggi della certificazione**:
    - **Vantaggio competitivo**: dimostrazione di impegno verso la sicurezza
    - **Conformità normativa**: base per rispettare molti requisiti legali
    - **Miglioramento interno**: miglioramento processi e riduzione rischi
    - **Fiducia stakeholders**: clienti, partner, fornitori, investitori

    - **Riduzione costi incidenti**: prevenzione di violazioni e perdite
- **Costi e risorse**:
    - Implementazione sistema (consulenza, formazione)
    - Miglioramenti tecnologici e organizzativi
    - Costi di certificazione (audit, tariffa ente)
    - Personale dedicato (Security Officer, audit team)
    - Mantenimento e miglioramento continuo

### 1.3.3 Gestione continua della compliance

- **Ciclo di gestione della compliance**:
    - **Plan**: identificazione requisiti e pianificazione
    - **Implement**: implementazione di controlli e misure
    - **Monitor**: verifica e misurazione dell'efficacia
    - **Report**: comunicazione a stakeholder
    - **Improve**: miglioramento continuo
- **Gestione degli aggiornamenti**:
    - Monitoraggio modifiche normative
    - Analisi impatto sui controlli esistenti
    - Aggiornamento documentazione e controlli
    - Comunicazione dei cambiamenti
    - Verifica dell'efficacia post-modifiche
- **Strumenti di supporto**:
    - **GRC platforms**: Governance, Risk and Compliance
    - **SIEM**: Security Information and Event Management
    - **Compliance dashboards**: monitoraggio in tempo reale
    - **Automated compliance checking**: verifica automatizzata
    - **Documentation management systems**: gestione documentale
- **Key Performance Indicators (KPI)**:
    - Percentuale di conformità ai controlli
    - Numero e gravità delle non conformità
    - Tempo medio di risoluzione
    - Copertura degli audit
    - Livello di maturità dei controlli

# 2. Legislazione sulla protezione dei dati e privacy

## 2.1 GDPR e implicazioni tecniche

### 2.1.1 Panoramica del GDPR

- **Definizione e ambito**:
  - Regolamento (UE) 2016/679 (General Data Protection Regulation)
  - In vigore dal 25 maggio 2018
  - Applicabile a tutte le organizzazioni che trattano dati di cittadini UE
  - Armonizza le normative sulla protezione dati in tutta l'UE
  - Extraterritorialità: si applica anche a organizzazioni extra-UE
- **Principi fondamentali**:
  - **Liceità, correttezza e trasparenza**: trattamento dati legittimo e comprendibile
  - **Limitazione della finalità**: dati raccolti per scopi specifici
  - **Minimizzazione dei dati**: solo i dati necessari
  - **Esattezza**: dati accurati e aggiornati
  - **Limitazione della conservazione**: conservati solo per il tempo necessario
  - **Integrità e riservatezza**: protezione da trattamenti non autorizzati
  - **Responsabilizzazione (accountability)**: dimostrare la conformità
- **Ruoli chiave**:
  - **Titolare del trattamento (Controller)**: determina finalità e mezzi
  - **Responsabile del trattamento (Processor)**: tratta dati per conto del titolare
  - **Interessato (Data subject)**: persona fisica identificata o identificabile
  - **DPO (Data Protection Officer)**: supervisiona la conformità
  - **Autorità di controllo**: autorità pubblica di vigilanza (es. Garante Privacy)
- **Sanzioni**:
  - Fino a 20 milioni di Euro o 4% del fatturato globale annuo
  - Proporzionali alla gravità, durata e natura dell'infrazione
  - Rimedi giudiziari e diritto al risarcimento per gli interessati

### 2.1.2 Privacy by Design e Privacy by Default

- **Privacy by Design**:
  - **Definizione**: integrare la protezione dei dati fin dalla progettazione
  - **Principi chiave**:
    1. Proattivo, non reattivo; preventivo, non correttivo
    2. Privacy come impostazione predefinita
    3. Privacy incorporata nella progettazione
    4. Funzionalità completa (somma positiva, non somma zero)
    5. Sicurezza end-to-end
    6. Visibilità e trasparenza
    7. Rispetto per la privacy dell'utente
- **Privacy by Default**:
  - **Definizione**: impostazioni predefinite che garantiscono massima protezione
  - **Implementazioni pratiche**:

        - Raccolta solo dei dati strettamente necessari
        - Limitazione dell'accesso ai dati personali
        - Impostazione predefinita opt-out per servizi non essenziali
        - Conservazione limitata nel tempo
        - Minimizzazione della condivisione dati
- **Approcci tecnici**:
    - **Data minimization**: raccolta e conservazione dei soli dati necessari
    - **Pseudonymization**: sostituzione di identificatori diretti con pseudonimi
    - **Anonymization**: rendere impossibile l'identificazione della persona
    - **Encryption**: protezione dei dati tramite cifratura
    - **Access controls**: limitazione dell'accesso in base al principio di necessità
    - **Audit trails**: registrazione degli accessi e modifiche

### 2.1.3 Implementazione tecnica dei diritti degli interessati

- **Diritto di accesso**:
    - **Implementazione**: sistema centralizzato di recupero dei dati personali
    - **Requisiti tecnici**: capacità di estrarre tutti i dati relativi a un individuo specifico
    - **Sfide**: dati distribuiti su sistemi diversi, formati eterogenei
    - **Soluzioni**: data inventory, data mapping, sistemi di subject access request
- **Diritto di rettifica**:
    - **Implementazione**: meccanismi per correggere dati inesatti
    - **Requisiti tecnici**: tracciabilità delle modifiche, propagazione aggiornamenti
    - **Sfide**: sincronizzazione tra sistemi diversi
    - **Soluzioni**: single source of truth, sistemi master data management
- **Diritto alla cancellazione (diritto all'oblio)**:
    - **Implementazione**: processi di eliminazione completa e irreversibile
    - **Requisiti tecnici**: identificazione di tutti i dati collegati, inclusi backup
    - **Sfide**: eliminazione dai backup senza compromettere l'integrità
    - **Soluzioni**: tokenization, encryption con distruzione chiavi, strumenti di data erasure
- **Diritto alla limitazione del trattamento**:
    - **Implementazione**: sistemi per contrassegnare i dati con restrizioni d'uso
    - **Requisiti tecnici**: flag nei database, controlli d'accesso granulari
    - **Sfide**: garantire che nessun processo utilizzi i dati "limitati"
    - **Soluzioni**: data tagging, attribute-based access control
- **Diritto alla portabilità dei dati**:
    - **Implementazione**: capacità di esportare dati in formato strutturato
    - **Requisiti tecnici**: formati standard, machine-readable
    - **Sfide**: interoperabilità tra sistemi diversi
    - **Soluzioni**: API standardizzate, formati di interscambio (XML, JSON)

- **Diritto di opposizione al trattamento automatizzato**:
  - **Implementazione**: meccanismi per esclusione da processi automatici
  - **Requisiti tecnici**: opt-out dai sistemi di profiling/decisioni automatizzate
  - **Sfide**: identificazione di tutte le decisioni automatizzate
  - **Soluzioni**: human-in-the-loop, review processes, consent management

### 2.1.4 Data breach: rilevamento, gestione e notifica

- **Definizione di data breach**:
  - Violazione di sicurezza che comporta accidentalmente o illecitamente:
    - Distruzione, perdita, modifica
    - Divulgazione non autorizzata
    - Accesso a dati personali trasmessi, conservati o trattati
- **Rilevamento**:
  - **Tecnologie di monitoraggio**:
    - SIEM (Security Information and Event Management)
    - DLP (Data Loss Prevention)
    - EDR (Endpoint Detection and Response)
    - NBA (Network Behavior Analysis)
    - File integrity monitoring
  - **Indicatori di compromissione**:
    - Attività di rete anomale
    - Accessi non autorizzati
    - Modifiche non autorizzate a file/database
    - Esfiltrazioni di dati
    - Comportamenti anomali degli utenti
- **Procedure di gestione**:
  - **Fase 1: Contenimento**:
    - Isolamento dei sistemi compromessi
    - Blocco degli accessi non autorizzati
    - Preservazione delle prove forensi
  - **Fase 2: Valutazione**:
    - Identificazione dei dati compromessi
    - Determinazione della gravità
    - Valutazione dei rischi per gli interessati
  - **Fase 3: Remediation**:
    - Eliminazione della causa
    - Ripristino dei sistemi
    - Implementazione di controlli aggiuntivi
  - **Fase 4: Documentazione**:

        - Registrazione di tutte le azioni intraprese
        - Cronologia dettagliata
        - Lezioni apprese
- **Notifica**:
    - **All'Autorità di controllo**:
        - Entro 72 ore dalla scoperta (se rischio per diritti/libertà)
        - Descrizione della natura della violazione
        - Categorie e numero approssimativo di interessati
        - Conseguenze probabili
        - Misure adottate o proposte
    - **Agli interessati**:
        - Quando la violazione presenta un rischio elevato
        - Linguaggio chiaro e semplice
        - Contatti del DPO o altro punto di contatto
        - Misure che possono adottare per mitigare i rischi
    - **Esenzioni dalla notifica agli interessati**:
        - Dati criptati o resi inintelligibili
        - Misure successive che scongiurano il rischio
        - Sforzo sproporzionato (comunicazione pubblica)
- **Registro delle violazioni**:
    - Documentazione di tutte le violazioni
    - Indipendentemente dall'obbligo di notifica
    - Dettagli su circostanze, effetti e rimedi
    - A disposizione dell'Autorità di controllo

## 2.2 Sicurezza dei dati nei diversi contesti

### 2.2.1 Dati sanitari: requisiti specifici e protocolli dedicati

- **Classificazione dei dati sanitari**:
    - **Dati sanitari**: stato di salute fisica o mentale
    - **Dati genetici**: caratteristiche ereditate o acquisite
    - **Dati biometrici**: caratteristiche fisiche, fisiologiche, comportamentali
- **Requisiti normativi specifici**:
    - **GDPR Art. 9**: categoria speciale di dati con protezione rafforzata
    - **HIPAA** (USA): standard per privacy e sicurezza informazioni sanitarie
    - **D.Lgs. 101/2018**: adeguamento italiano al GDPR per dati sanitari
    - **Fascicolo Sanitario Elettronico**: normativa specifica (D.L. 179/2012)
- **Misure tecniche e organizzative**:
    - **Controllo accessi avanzato**: strong authentication, RBAC, break-glass

    - **Crittografia end-to-end**: per la trasmissione di dati sensibili
    - **Data segregation**: separazione fisica o logica dei dati sanitari
    - **Anonimizzazione/pseudonimizzazione**: per statistiche e ricerca
    - **Audit trail completo**: chi ha avuto accesso a cosa e quando
- **Standard tecnici di settore**:
    - **HL7 FHIR**: standard per interoperabilità dati sanitari
    - **DICOM**: standard per gestione immagini mediche
    - **IHE**: profili di integrazione per sanità digitale
    - **OpenEHR**: standard per EHR (Electronic Health Records)
    - **ISO 27799**: sicurezza informatica in sanità
- **Casi d'uso specifici**:
    - **Telemedicina**: sicurezza delle comunicazioni remote
    - **Dispositivi medici connessi**: IoMT (Internet of Medical Things)
    - **Ricerca medica**: bilanciamento tra accesso ai dati e privacy
    - **Apps salute e fitness**: data minimization e trasparenza
    - **Genetica e genomica**: protezione dati altamente sensibili

## 2.2.2 Dati finanziari: standard di settore (PCI DSS)

- **Payment Card Industry Data Security Standard (PCI DSS)**:
    - **Definizione**: standard di sicurezza per proteggere dati delle carte di pagamento
    - **Applicabilità**: qualsiasi organizzazione che memorizza, elabora o trasmette dati di carte
    - **Amministrazione**: PCI Security Standards Council (creato da Visa, Mastercard, Amex, Discover, JCB)
    - **Livelli di merchant**: classificazione basata sul volume di transazioni
- **12 requisiti principali PCI DSS**:
    1. **Rete sicura**: firewall e router configurati per proteggere i dati
    2. **Password sicure**: no default dei vendor, password robuste
    3. **Protezione dati**: crittografia dei dati dei titolari di carta
    4. **Trasmissione cifrata**: cifratura su reti pubbliche
    5. **Antimalware**: uso e aggiornamento regolare
    6. **Sviluppo sicuro**: sistemi e applicazioni sicuri
    7. **Restrizione accessi**: principio del need-to-know
    8. **Autenticazione**: ID unici per ogni persona con accesso
    9. **Restrizione accesso fisico**: ai dati dei titolari di carta
    10. **Monitoraggio**: tracking e logging di tutti gli accessi
    11. **Test regolari**: di sicurezza di sistemi e processi
    12. **Policy di sicurezza**: documentata e mantenuta
- **Tecnologie e pratiche chiave**:

    - **Tokenization**: sostituzione del PAN con token non sensibile
    - **P2PE (Point-to-Point Encryption)**: cifratura dal punto di acquisizione
    - **Network segmentation**: isolamento dell'ambiente cardholder data
    - **Vulnerability scanning**: almeno trimestralmente
    - **Penetration testing**: almeno annualmente
    - **File integrity monitoring**: per rilevare modifiche non autorizzate
- **Processo di validazione**:
    - **Self-Assessment Questionnaire (SAQ)**: per merchant di livello inferiore
    - **Report on Compliance (ROC)**: per livelli superiori, eseguito da QSA
    - **Vulnerability scans trimestrali**: da ASV approvato
    - **Attestation of Compliance (AOC)**: certificazione di conformità
- **Relazione con altre normative**:
    - Complementare a GDPR per dati finanziari
    - Overlap con SOX per aziende quotate
    - Sinergie con ISO 27001 per gestione sicurezza
    - Requisiti specifici per servizi di pagamento (PSD2)

### 2.2.3 Dati dei minori: tutele aggiuntive e responsabilità

- **Framework normativo**:
    - **GDPR Art. 8**: consenso dei minori e autorizzazione genitoriale
    - **COPPA** (USA): Children's Online Privacy Protection Act
    - **Age Appropriate Design Code** (UK): design di servizi per minori
    - **D.Lgs. 101/2018**: specificazioni sulla protezione dei minori
- **Requisiti specifici**:
    - **Età del consenso**: 16 anni (modificabile dagli Stati membri fino a 13)
    - **Verifica dell'età**: meccanismi efficaci ma proporzionati
    - **Informativa**: linguaggio chiaro e comprensibile per i minori
    - **Autorizzazione genitoriale**: verifica affidabile
    - **Best interest**: considerazione preminente in tutte le decisioni
- **Misure tecniche**:
    - **Age verification**: soluzioni tecniche per verifica età (non documenti)
    - **Parental dashboard**: controllo genitoriale sulle attività
    - **Privacy settings**: impostazioni elevate di default
    - **Geofencing**: limitazioni basate sulla localizzazione
    - **Content filtering**: protezione da contenuti inappropriati
    - **Profiling restrictions**: limitazioni alla profilazione
- **Design considerations**:
    - **Privacy by default**: impostazioni più restrittive
    - **No dark patterns**: no manipolazione per condivisione eccessiva

    - **Limited data collection**: strettamente necessaria
    - **Transparency**: spiegazioni adatte all'età
    - **Limited retention**: tempi di conservazione minimi
    - **Right to erasure**: cancellazione facilitata
- **Conseguenze delle violazioni**:
    - Sanzioni economiche maggiorate
    - Danni reputazionali significativi
    - Possibili risvolti penali
    - Responsabilità civile verso famiglie

# 3. Identità digitale e fiducia nelle reti

## 3.1 Sistemi di autenticazione e autorizzazione

### 3.1.1 Evoluzione dei sistemi di autenticazione

- **Fattori di autenticazione**:
    - **Conoscenza** (something you know): password, PIN, pattern
    - **Possesso** (something you have): token, smart card, device
    - **Inerenza** (something you are): biometria, comportamento
    - **Luogo** (somewhere you are): geolocalizzazione
    - **Tempo** (when you authenticate): orari consentiti
- **Dai semplici username/password ai sistemi moderni**:
    1. **Password semplici**: vulnerabili a brute force, social engineering
    2. **Password policy**: lunghezza, complessità, rotazione
    3. **Password manager**: generazione e gestione sicura
    4. **Autenticazione a due fattori (2FA)**: password + secondo fattore
    5. **Autenticazione multi-fattore (MFA)**: combinazione di 3+ fattori
    6. **Autenticazione adattiva/contestuale**: basata su comportamento/rischio
    7. **Autenticazione passwordless**: eliminazione completa delle password
- **Tecnologie per autenticazione forte**:
    - **OTP (One-Time Password)**:
        - HOTP (HMAC-based): basato su contatore
        - TOTP (Time-based): basato su timestamp
        - Distribuzione via SMS, email, app dedicata
    - **Hardware token**:
        - Token fisici (Yubikey, RSA SecurID)
        - Smart card e lettori
        - USB security keys (FIDO2, WebAuthn)
    - **Mobile authentication**:
        - Push notification

        - Mobile app authenticator
        - QR code scanning
    - **Biometria**:
        - Impronte digitali, riconoscimento facciale, iride
        - Riconoscimento vocale
        - Comportamentale (keystroke dynamics, mouse movements)
- **Standard e protocolli**:
    - **FIDO2/WebAuthn**: autenticazione forte basata su crittografia asimmetrica
    - **OAuth 2.0**: framework per autorizzazione
    - **OpenID Connect**: livello di identità su OAuth 2.0
    - **SAML**: Security Assertion Markup Language
    - **JWT**: JSON Web Token

### 3.1.2 Single Sign-On e sistemi federati

- **Single Sign-On (SSO)**:
    - **Definizione**: autenticazione unica per accedere a più applicazioni
    - **Vantaggi**:
        - Miglior user experience (una sola password da ricordare)
        - Gestione centralizzata degli accessi
        - Riduzione password fatigue
        - Miglior sicurezza (password più robuste, MFA centralizzato)
    - **Tipi di SSO**:
        - **Enterprise SSO**: all'interno di un'organizzazione
        - **Web SSO**: per applicazioni web
        - **Federated SSO**: tra organizzazioni diverse
    - **Funzionamento**:
        1. Autenticazione su service provider (SP) o identity provider (IdP)
        2. Generazione token/ticket che certifica l'identità
        3. Propagazione token alle applicazioni integrate
        4. Validazione token e concessione accesso
- **Identity Federation**:
    - **Definizione**: condivisione delle identità tra organizzazioni diverse
    - **Componenti**:
        - **Identity Provider (IdP)**: gestisce le identità e l'autenticazione
        - **Service Provider (SP)**: fornisce servizi basati sulle identità
        - **Protocolli di federazione**: meccanismi standardizzati di scambio
    - **Meccanismi di trust**:
        - **Bilateral**: accordi diretti tra due entità
        - **Hub and spoke**: entità centrale gestisce trust relationship

        - **Web of trust**: relazioni tra più entità
    - **Implementazioni comuni**:
        - **SAML federations**: educative (eduGAIN), ricerca (InCommon)
        - **Social login**: Google, Facebook, Apple come IdP
        - **Enterprise federation**: B2B, supply chain
- **Protocolli federativi**:
    - **SAML (Security Assertion Markup Language)**:
        - Standard XML per scambio dati autenticazione/autorizzazione
        - Architettura IdP/SP
        - Assertion contenenti attributi utente
        - Diffuso in ambito enterprise
    - **OAuth 2.0**:
        - Framework di autorizzazione (non autenticazione)
        - Delega accesso tramite token
        - Grant types per diversi scenari
        - Base per molti sistemi di federazione
    - **OpenID Connect (OIDC)**:
        - Layer di identità su OAuth 2.0
        - Aggiunge autenticazione standardizzata
        - ID token (JWT) con claims
        - Scambio attributi utente via UserInfo Endpoint
- **Sfide e considerazioni**:
    - **Privacy e data sharing**: minimizzazione dati condivisi
    - **Session management**: durata, invalidazione, propagazione logout
    - **Incident response**: gestione compromissione identità federate
    - **Vendor lock-in**: dipendenza da provider specifici
    - **Regulatory compliance**: conformità normativa attraverso domini

### 3.1.3 Biometria e sfide etiche

- **Tecnologie biometriche principali**:
    - **Fisiologiche**:
        - **Impronte digitali**: minuzie, pattern
        - **Riconoscimento facciale**: punti di riferimento, geometria
        - **Scansione iride/retina**: pattern unici dell'occhio
        - **Geometria della mano**: dimensioni, forma
        - **DNA**: sequenza genetica
    - **Comportamentali**:
        - **Firma dinamica**: pressione, velocità, accelerazione
        - **Keystroke dynamics**: modalità di digitazione

        - **Gait analysis**: modo di camminare
        - **Voice recognition**: caratteristiche vocali
        - **Behavioral analytics**: pattern di utilizzo
- **Funzionamento dei sistemi biometrici**:
    1. **Enrollment**: acquisizione caratteristica biometrica
    2. **Feature extraction**: identificazione caratteristiche distintive
    3. **Template creation**: creazione modello di riferimento
    4. **Storage**: memorizzazione sicura del template
    5. **Matching**: confronto con nuove acquisizioni
    6. **Decision**: accettazione o rifiuto
- **Metriche di performance**:
    - **FAR (False Acceptance Rate)**: autenticazione erronea di un impostore
    - **FRR (False Rejection Rate)**: rifiuto erroneo di utente legittimo
    - **EER (Equal Error Rate)**: punto in cui FAR=FRR
    - **CER (Crossover Error Rate)**: simile a EER
    - **FTE (Failure to Enroll)**: impossibilità di registrare un utente
    - **FTA (Failure to Acquire)**: impossibilità di acquisire il campione
- **Considerazioni etiche e privacy**:
    - **Immutabilità**: caratteristiche non modificabili (a differenza delle password)
    - **Revocabilità**: difficoltà di "cambiare" biometria compromessa
    - **Consenso informato**: comprensione dell'acquisizione e utilizzo
    - **Sorveglianza di massa**: potenziali abusi per tracking
    - **Discriminazione**: bias negli algoritmi (età, etnia, condizioni mediche)
    - **Centralizzazione**: rischi di data breach di database biometrici
- **Mitigazioni tecniche**:
    - **Template protection**: trasformazione irreversibile
    - **Biometric encryption**: protezione crittografica
    - **Cancellable biometrics**: trasformazione revocabile
    - **Local processing**: elaborazione su dispositivo
    - **Liveness detection**: prevenzione spoofing
    - **Multimodal biometrics**: combinazione di più caratteristiche
- **Normativa applicabile**:
    - **GDPR Art. 9**: dati biometrici come categoria speciale
    - **Leggi nazionali**: limiti specifici all'uso della biometria
    - **Standard ISO/IEC 24745**: protezione dei dati biometrici
    - **Principi di proporzionalità**: giustificazione dell'uso

## 3.2 Firma digitale e validità legale

### 3.2.1 Infrastruttura a chiave pubblica (PKI)

- **Definizione e componenti**:
  - **PKI**: insieme di hardware, software, persone, policy e procedure per creare, gestire, distribuire, utilizzare, archiviare e revocare certificati digitali
  - **Certificato digitale**: documento elettronico che associa una chiave pubblica a un'identità
  - **CA (Certificate Authority)**: ente che emette certificati
  - **RA (Registration Authority)**: verifica identità dei richiedenti
  - **VA (Validation Authority)**: verifica validità certificati
  - **Subscriber**: entità che richiede e utilizza il certificato
  - **Relying party**: entità che si affida al certificato
- **Architettura PKI**:
  - **Root CA**: CA di massimo livello, generalmente offline
  - **Intermediate CA**: emettono certificati per conto della Root CA
  - **Issuing CA**: emettono certificati per utenti finali
  - **Cross-certification**: relazioni di fiducia tra CA diverse
  - **Bridge CA**: facilita interconnessione tra domini PKI
- **Formato certificati X.509**:
  - **Versione**: versione del formato (tipicamente v3)
  - **Numero seriale**: identificativo univoco
  - **Algoritmo di firma**: algoritmo usato dalla CA
  - **Emittente**: nome della CA
  - **Validità**: periodo di validità (Not Before, Not After)
  - **Soggetto**: identità del titolare
  - **Informazioni chiave pubblica**: algoritmo e valore
  - **Estensioni**: usi del certificato, vincoli, CRL, AIA
  - **Firma digitale**: firma della CA sull'intero certificato
- **Certificate Revocation**:
  - **CRL (Certificate Revocation List)**: elenco certificati revocati
  - **OCSP (Online Certificate Status Protocol)**: verifica stato in tempo reale
  - **OCSP Stapling**: allegare risposta OCSP firmata
  - **Motivi di revoca**: compromissione chiave, cessazione operatività, sostituzione
- **Applicazioni**:
  - **TLS/SSL**: sicurezza connessioni web
  - **Code signing**: firma di software
  - **Email sicura**: S/MIME
  - **Documenti firmati**: PDF, XML
  - **Smart card**: autenticazione forte
  - **IPsec**: VPN e comunicazioni sicure

## 3.2.2 eIDAS e normativa italiana

- **eIDAS (electronic IDentification Authentication and Signature)**:
  - **Definizione**: Regolamento UE n. 910/2014 su identificazione elettronica e servizi fiduciari
  - **Obiettivi**: creare un mercato unico digitale europeo
  - **Ambito**: identità digitale, firme elettroniche, sigilli, marcatura temporale, servizi di recapito, autenticazione siti web
  - **Principio di non discriminazione**: non negazione di effetti giuridici per forma elettronica
  - **Mutuo riconoscimento**: dei sistemi di identità digitale notificati
- **Livelli di firma elettronica**:
  - **Firma elettronica semplice**: dati in forma elettronica allegati a altri dati (es. firma su tablet)
  - **Firma elettronica avanzata (FEA)**: requisiti aggiuntivi di identificazione e controllo
  - **Firma elettronica qualificata (FEQ)**: firma avanzata creata con dispositivo sicuro e certificato qualificato
  - **Sigillo elettronico**: equivalente della firma ma per persone giuridiche
- **Prestatori di servizi fiduciari (Trust Service Providers)**:
  - **Qualified TSP**: riconosciuti e autorizzati a livello nazionale
  - **Supervisione**: da parte di organismi designati dagli Stati membri
  - **EU Trusted Lists**: elenchi pubblici dei prestatori qualificati
  - **Servizi regolamentati**: CA, timestamping, conservazione, PEC
- **Normativa italiana**:
  - **CAD (Codice dell'Amministrazione Digitale)**:
    - **D.Lgs. 82/2005** e successive modifiche
    - Disciplina documenti informatici e firme elettroniche
    - Domicilio digitale
    - Pagamenti elettronici
  - **PEC (Posta Elettronica Certificata)**:
    - Specificità italiana (ora evoluta in REM sotto eIDAS)
    - Valore legale equiparato a raccomandata A/R
    - Gestori accreditati presso AgID
  - **SPID (Sistema Pubblico di Identità Digitale)**:
    - Sistema di identità digitale italiano
    - Tre livelli di sicurezza
    - Identity provider accreditati
    - Notificato sotto eIDAS
  - **CIE (Carta d'Identità Elettronica)**:
    - Documento d'identità con chip
    - Autenticazione forte per servizi online
    - Compatibile con eIDAS

- **Evoluzione e sfide**:
  - **eIDAS 2.0**: proposta di aggiornamento (European Digital Identity)
  - **Wallet digitale europeo**: gestione credenziali
  - **Identità decentralizzata (SSI)**: maggior controllo per l'utente
  - **Interoperabilità**: tra diversi sistemi nazionali
  - **Tecnologie emergenti**: blockchain, mobile ID

## 3.2.3 PEC e comunicazioni certificate

- **Posta Elettronica Certificata (PEC)**:
  - **Definizione**: sistema email che fornisce prova legale dell'invio e della consegna
  - **Base normativa**: CAD (D.Lgs. 82/2005), DPR 68/2005
  - **Equiparazione**: valore legale della raccomandata con ricevuta di ritorno
  - **Caratteristiche distintive**:
    - Autenticazione mittente/destinatario
    - Integrità del messaggio
    - Certificazione temporale
    - Non ripudiabilità
    - Tracciabilità completa
- **Architettura del sistema PEC**:
  - **Gestore mittente**: certifica l'invio e genera ricevuta di accettazione
  - **Gestore destinatario**: certifica la ricezione e genera ricevuta di consegna
  - **Indice pubblico gestori (IGPEC)**: registro dei gestori accreditati
  - **Indice nazionale domicili digitali (INAD)**: registro indirizzi PEC
- **Ricevute e notifiche**:
  - **Ricevuta di accettazione**: conferma presa in carico dal gestore mittente
  - **Ricevuta di consegna**: conferma consegna nella casella destinatario
  - **Avviso di non accettazione**: per messaggi non conformi
  - **Avviso di mancata consegna**: impossibilità di recapito entro 24h
  - **Busta di trasporto**: contiene messaggio originale e dati certificazione
- **Caratteristiche tecniche**:
  - **Firma digitale** su ricevute e messaggi
  - **Marcatura temporale**
  - **Protocollo S/MIME** per integrità e non ripudio
  - **Crittografia** per confidenzialità (TLS)
  - **Log** di tutte le operazioni (conservati per 30 mesi)
- **Evoluzione verso REM (Registered Electronic Mail)**:
  - **eIDAS**: standard europeo per servizi elettronici di recapito certificato
  - **Differenze PEC-REM**: interoperabilità europea, requisiti tecnici
  - **Migrazione**: conversione del sistema italiano verso standard europeo

    - **Timeline**: periodo transitorio di coesistenza
- **Obblighi e utilizzi**:
    - **PA**: obbligo di domicilio digitale
    - **Imprese e professionisti**: obbligo iscrizione INI-PEC
    - **Cittadini**: facoltà di eleggere domicilio digitale
    - **Utilizzi principali**: comunicazioni ufficiali con PA, notifiche legali, contrattualistica, fatturazione elettronica

# 3.3 Fiducia digitale ed evoluzione dei sistemi di identità

## 3.3.1 Trust model tradizionali vs. decentralizzati

- **Trust model tradizionali (centralizzati)**:
    - **Hierarchical trust**: struttura piramidale (PKI tradizionale)
        - Singolo punto di fiducia (Root CA)
        - Trust cascade verso il basso
        - Vulnerabilità: compromissione root compromette intero sistema
    - **Federated trust**: fiducia tra domini diversi
        - Bridge CA o cross-certification
        - Identity providers federati
        - Delegation of trust
        - Vulnerabilità: complessità gestionale, dipendenza da terze parti
    - **Web of trust**:
        - Approccio peer-to-peer alla fiducia (PGP)
        - Firme reciproche tra utenti
        - Trust path attraverso rete sociale
        - Vulnerabilità: difficile scaling, isole di fiducia
- **Trust model decentralizzati/distribuiti**:
    - **Blockchain-based**:
        - Consenso distribuito
        - Immutabilità del ledger
        - Disintermediazione
        - Smart contracts per automazione trust
        - Vulnerabilità: 51% attack, governance, scalabilità
    - **Self-Sovereign Identity (SSI)**:
        - Utente al centro e proprietario dell'identità
        - Relazioni bilaterali di fiducia
        - Credenziali verificabili (VCs)
        - Separazione identity provider / attribute provider
        - Vulnerabilità: gestione chiavi, recovery meccanisms

- **Elementi di comparazione**:

| | Aspetto | Modelli tradizionali |
|---|---|---|
| | Controllo | Centralizzato/federato |
| | Resilienza | Single point of failure |
| | Governance | Top-down |
| | Scalabilità | Limitata da ente centrale |
| | Privacy | Intermediari necessari |
| | Usabilità | Semplice per utente |
| | Revoca | Meccanismi centralizzati |
| | Costo | Licenze, manutenzione |

- **Casi d'uso emergenti**:
  - **Digital credentials**: certificati di istruzione, licenze
  - **Supply chain**: tracciabilità e autenticità prodotti
  - **Healthcare**: controllo accessi dati sanitari
  - **Government services**: identità digitale per servizi pubblici
  - **IoT & Smart Cities**: autenticazione dispositivi
  - **DeFi (Decentralized Finance)**: servizi finanziari senza intermediari

## 3.3.2 Self-Sovereign Identity (SSI)

- **Definizione e principi**:
  - **SSI**: paradigma in cui individui o organizzazioni hanno controllo completo sulla propria identità digitale
  - **Principi chiave** (Christopher Allen, 2016):
    1. **Esistenza**: identità separata dai provider
    2. **Controllo**: utenti controllano la propria identità
    3. **Accesso**: accesso ai propri dati
    4. **Trasparenza**: sistemi e algoritmi verificabili
    5. **Persistenza**: identità a lungo termine
    6. **Portabilità**: non legata a singolo provider
    7. **Interoperabilità**: ampia applicabilità
    8. **Consenso**: condivisione dati solo con consenso
    9. **Minimizzazione**: disclosure selettiva
    10. **Protezione**: diritti garantiti
- **Componenti architetturali**:
  - **DID (Decentralized Identifiers)**:
    - Identificatori persistenti globalmente univoci
    - Indipendenti da registry centrali

        - Controllati da possessori di chiavi
        - Formato: did:[method]:[method-specific-id]
        - Risoluzione in DID Document
    - **Verifiable Credentials (VC)**:
        - Attestazioni digitali crittograficamente verificabili
        - Emissi da issuer a holder
        - Verificabili da verifier senza contattare issuer
        - Struttura: metadata, claims, proofs
        - Supporto per Zero-Knowledge Proofs
    - **Decentralized Identity Hubs/Agents**:
        - Software per gestione identità e credenziali
        - Wallet per storage credenziali
        - Interfaccia per autorizzazioni
        - Middleware per interazioni
    - **Verifiable Data Registry**:
        - Blockchain o ledger distribuito
        - Memorizza DID, schema, revocation info
        - Non memorizza dati personali
        - Garantisce immutabilità e non-censurabilità
- **Standard e implementazioni**:
    - **W3C DID Standard**: specifiche per identificatori decentralizzati
    - **W3C Verifiable Credentials**: formato per credenziali
    - **DIF (Decentralized Identity Foundation)**: interoperabilità
    - **Hyperledger Indy/Aries**: framework per SSI su blockchain
    - **Sovrin**: rete pubblica di identità basata su Hyperledger
    - **uPort/Serto**: implementazione su Ethereum
    - **Microsoft ION**: implementazione su Bitcoin
- **Vantaggi e limiti**:
    - **Vantaggi**:
        - Privacy by design
        - Resistenza alla censura
        - Eliminazione intermediari
        - Riduzione honeypot di dati
        - Usability potenzialmente superiore
    - **Sfide**:
        - Gestione chiavi complessa
        - Recovery procedure
        - Interoperabilità tra sistemi
        - Assenza framework legali completi

        - Adozione di massa

### 3.3.3 Evoluzioni tecnologiche e normative dei sistemi di identità

- **Tendenze tecnologiche**:
    - **Mobile ID**: identità basata su dispositivi mobili
        - SIM-based authentication
        - Mobile signature
        - Secure elements e TEE (Trusted Execution Environment)
        - NFC per interazioni fisiche
    - **Biometria comportamentale**:
        - Continuous authentication
        - Behavioral analytics
        - Keystroke/touch dynamics
        - Autenticazione passiva
    - **Passwordless authentication**:
        - FIDO2/WebAuthn per autenticazione senza password
        - Public-key cryptography su dispositivi utente
        - Authenticator roaming vs platform
        - Push authentication
    - **Zero-Knowledge Proofs (ZKP)**:
        - Dimostrazione di un fatto senza rivelare informazioni
        - Selective disclosure di attributi
        - Age verification senza rivelare data nascita
        - Dimostrazione di appartenenza a gruppo
- **Sviluppi normativi**:
    - **eIDAS 2.0 / European Digital Identity Wallet**:
        - Proposta di regolamento (COM/2021/281)
        - Wallet digitale europeo
        - Identità elettronica verificabile
        - Interoperabilità obbligatoria
        - Riconoscimento transfrontaliero
    - **Digital Identity Trust Framework**:
        - Framework nazionali di fiducia
        - Governance per ecosistemi di identità
        - Certificazione di provider
        - Trust mark e schemi di accreditamento
    - **Regulatory Sandboxes**:
        - Ambienti controllati per sperimentazione
        - Deroghe temporanee a regolamentazione

        - Test di nuove tecnologie di identità
        - Collaborazione regolatori-innovatori
- **Tensioni e bilanciamenti**:
    - **Privacy vs. KYC/AML**: requisiti di identificazione vs anonimato
    - **Sovranità nazionale vs. standardizzazione**: approcci locali vs globali
    - **Controllo statale vs. autodeterminazione**: sorveglianza vs autonomia
    - **Semplicità vs. sicurezza**: usabilità vs protezioni avanzate
    - **Legacy systems vs. innovazione**: retrocompatibilità vs nuovi paradigmi
- **Convergenza digitale-fisico**:
    - **Smart borders**: automated border control
    - **Mobile driving license**: patente digitale standard ISO
    - **Digital travel credentials**: passaporti digitali
    - **Contactless identity verification**: verifica a distanza
    - **IoT identity**: autenticazione dei "things"

# 4. Responsabilità e etica nella sicurezza informatica

## 4.1 Responsible disclosure e bug bounty

### 4.1.1 Principi della responsible disclosure

- **Definizione**:
    - Processo etico di segnalazione vulnerabilità che bilancia:
        - Diritto del pubblico alla sicurezza e all'informazione
        - Tempo necessario per correggere la vulnerabilità
        - Limitazione potenziali danni da exploit
- **Modelli di disclosure**:
    - **Full disclosure**: pubblicazione immediata e completa
        - Vantaggi: massima trasparenza, pressione su vendor
        - Svantaggi: rischio sfruttamento prima del patch
    - **Non-disclosure**: nessuna divulgazione pubblica
        - Vantaggi: zero rischio di sfruttamento pubblico
        - Svantaggi: nessuna pressione per correzioni, dipendenza da vendor
    - **Coordinated disclosure**: collaborazione con vendor/CERT
        - Vantaggi: tempo per patch, protezione utenti
        - Svantaggi: possibili ritardi, compromessi necessari
    - **Responsible disclosure**: disclosure pubblica dopo tempo ragionevole
        - Vantaggi: bilanciamento sicurezza/trasparenza
        - Svantaggi: definizione "ragionevole" soggettiva
- **Timeline tipica**:

1. **Scoperta**: identificazione vulnerabilità
2. **Notifica iniziale**: contatto con vendor/CERT
3. **Verifica**: conferma del problema
4. **Periodo di correzione**: tempo per sviluppo patch (60-90 giorni tipici)
5. **Pubblicazione coordinata**: release patch e dettagli vulnerabilità
6. **Disclosure pubblica**: pubblicazione dettagli tecnici
7. **Post-disclosure**: monitoraggio adozione patch

- **Best practice**:
  - **Protocollo di comunicazione sicuro**: PGP/canali crittati
  - **Proof of concept**: dimostrare senza causare danni
  - **Minimizzazione dettagli sensibili**: evitare exploit code pubblico
  - **Documentazione chiara**: prerequisiti, impatto, riproduzione
  - **CVE assignment**: codifica standard della vulnerabilità
  - **Esclusione dati sensibili**: no PII o dati cliente
  - **Rispetto policy del vendor**: se ragionevoli
- **Considerazioni legali**:
  - **Computer Fraud and Abuse Act** (USA): rischi di responsabilità
  - **EU Cybersecurity Act**: supporto responsible disclosure
  - **Safe harbor**: protezioni legali per security researcher
  - **Terms of service**: violazioni potenziali durante test
  - **NDA**: accordi di non divulgazione
  - **Autorizzazione**: esplicita vs. implicita

### 4.1.2 Bug bounty programs

- **Definizione**:
  - Programmi che premiano economicamente la scoperta di vulnerabilità nei sistemi informatici
  - Modello crowdsourced di security testing
  - Incentivazone della responsible disclosure
  - "Pagare i cappelli bianchi invece di subire i cappelli neri"
- **Tipi di programmi**:
  - **Pubblici**: aperti a tutti i ricercatori
  - **Privati**: solo ricercatori invitati
  - **Ongoing**: costanti nel tempo
  - **Time-boxed**: competizioni limitate (CTF, hackathon)
  - **Self-hosted**: gestiti direttamente dall'organizzazione
  - **Platform-based**: tramite piattaforme dedicate
- **Piattaforme principali**:
  - **HackerOne**: focus su enterprise e government

    - **Bugcrowd**: ampia gamma di programmi
    - **Intigriti**: europea, forte in compliance
    - **Synack**: Red team gestito per enterprise
    - **Open Bug Bounty**: focus su web vulnerabilities
    - **YesWeHack**: piattaforma europea
- **Struttura tipica**:
    - **Scope**: sistemi/applicazioni inclusi nel programma
    - **Out-of-scope**: aree escluse
    - **Reward table**: ricompense basate su severità
    - **Rules of engagement**: limiti dei test (no DoS, social engineering)
    - **Safe harbor**: protezioni legali per tester
    - **Reporting guidelines**: formato e contenuto report
    - **SLA**: tempi di risposta e validazione
- **Modelli di ricompensa**:
    - **Pay-per-vulnerability**: pagamento per ogni bug valido
    - **Tiered rewards**: basate su CVSS o classificazione interna
        - Critical: $5,000-$50,000+
        - High: $1,000-$10,000
        - Medium: $500-$2,500
        - Low: $100-$500
    - **Bonus**: per report di alta qualità, exploit chain
    - **Recognition**: hall of fame, swag, punti reputation
    - **First-to-find**: solo prima segnalazione valida
- **Benefici e sfide**:
    - **Benefici**:
        - Accesso a talenti globali diversificati
        - Pagamento solo per risultati
        - Complemento a security testing tradizionale
        - Miglioramento continuo
        - Signal di trasparenza e fiducia
    - **Sfide**:
        - Gestione volume report e duplicati
        - Budget e prevedibilità costi
        - Requisiti legali e regolamentari
        - Competizione per ricercatori di qualità
        - False positive e triaging

## 4.2 Normative sulla security research

### 4.2.1 Framework legali per security testing

- **Legislazione europea**:
  - **NIS Directive 2 (2022/2555)**:
    - Supporto alla cooperazione sulla disclosure
    - Protezioni per security researcher
    - Armonizzazione approcci nazionali
  - **EU Cybersecurity Act (2019/881)**:
    - Framework per certificazione cybersecurity
    - Supporto ENISA a coordinated disclosure
    - Standardizzazione pratiche
  - **GDPR (2016/679)**:
    - Implicazioni per test con dati personali
    - Data breach notification
    - Accountability e security by design
- **Legislazione italiana**:
  - **Codice Penale**: art. 615-ter (accesso abusivo)
  - **D.Lgs. 231/2001**: responsabilità enti
  - **Perimetro di sicurezza nazionale cibernetica**:
    - Framework per asset critici
    - Regole specifiche per testing
- **Legislazione comparata**:
  - **USA**: CFAA (Computer Fraud and Abuse Act)
    - Criticato per eccessiva ampiezza
    - Riforme per safe harbor researcher
  - **UK**: Computer Misuse Act
    - Autorizzazione come difesa
    - Guidance CPS per public interest
  - **Paesi Bassi**: approccio pionieristico
    - Framework responsible disclosure
    - Protezioni esplicite per researcher
- **Safe harbor provisions**:
  - **Definizione**: protezioni legali per security researcher in buona fede
  - **Elementi tipici**:
    - Scopo e limitazioni test autorizzati
    - Requisiti di responsible disclosure
    - Impegni reciproci researcher/organizzazione
    - Non-prosecution agreement
  - **Implementazioni**:
    - Corporate vulnerability disclosure policy
    - Bug bounty terms and conditions

        - Framework governativi (es. DoD Vulnerability Disclosure Policy)
- **Caveat legali**:
    - **Autorizzazione**: esplicita, documentata, scope definito
    - **Jurisdictional issues**: applicabilità leggi diverse
    - **Danni non intenzionali**: responsabilità potenziale
    - **Limitazioni contrattuali**: ToS, EULA, NDA
    - **Asset di terze parti**: supply chain complications

## 4.2.2 Bilanciamento tra sicurezza e innovazione

- **Tensioni fondamentali**:
    - **Security vs. usabilità**: controlli rigidi vs. esperienza utente
    - **Regolamentazione vs. agilità**: compliance vs. time-to-market
    - **Transparenza vs. protezione**: full disclosure vs. security by obscurity
    - **Centralizzazione vs. decentralizzazione**: controllo vs. resilienza
- **Approcci di policy**:
    - **Risk-based approach**: regolamentazione proporzionale al rischio
    - **Regulatory sandboxes**: spazi sicuri per sperimentazione
    - **Voluntary standards**: framework flessibili non coercitivi
    - **Public-private partnership**: collaborazione stato-imprese
    - **International harmonization**: standard globali
- **Innovazione nella cybersecurity**:
    - **Security automation**: riduzione overhead manuale
    - **AI/ML per difesa**: rilevamento anomalie, threat intelligence
    - **DevSecOps**: integrazione sicurezza nello sviluppo
    - **Secure-by-design**: principi di progettazione intrinsecamente sicuri
    - **Zero Trust**: modello di sicurezza senza perimetri fissi
- **Case study**:
    - **GDPR impact**:
        - Effetti su privacy by design
        - Standardizzazione controlli
        - Impatto su modelli business
    - **IoT security**:
        - Mancanza standard iniziale
        - Evoluzione approcci regolamentari
        - Bilanciamento time-to-market e sicurezza
    - **Open source security**:
        - Vulnerabilità supply chain
        - Log4j come wake-up call
        - Modelli sostenibili per sicurezza condivisa

# 4.3 Ethical hacking e hacking civico

## 4.3.1 Distinzione tra hacking etico e criminale

- **Definizioni e contesto storico**:
  - **Hacker** (originale): innovatore tecnologico, problem-solver
  - **Cracker/Black hat**: hacker con intenti criminali
  - **White hat**: ethical hacker, security professional
  - **Grey hat**: operante in area grigia, senza autorizzazione ma senza intenti malevoli
- **Elementi distintivi**:

| | Aspetto | Ethical Hacking |
|---|---|---|
| | **Autorizzazione** | Esplicita |
| | **Intento** | Migliorare sicurezza |
| | **Disclosure** | Responsible disclosure |
| | **Impatto** | Limitato, controllato |
| | **Compenso** | Legittimo (stipendio, bug bounty) |
| | **Metodologia** | Documentata, riproducibile |
| | **Framework** | Standard (OWASP, PTES, NIST) |

- **Confini etici e legali**:
  - **Ethical hacking formale**: pentest autorizzato, bug bounty
  - **Security research**: analisi di sistemi/prodotti pubblici
  - **Academic research**: documenti per avanzamento conoscenza
  - **Grey area**: independent security research senza autorizzazione
  - **Chiaramente illegale**: data theft, ransomware, attacchi DoS
- **Professionalizzazione dell'ethical hacking**:
  - **Certificazioni**: CEH, OSCP, CREST, GPEN
  - **Formazione e accademia**: corsi specializzati, CTF
  - **Carriere**: penetration tester, red team, bug hunter
  - **Standard professionali**: codici etici (ISC², ISACA)
  - **Community**: conferenze (DEF CON, Black Hat, CODEBLUE)
- **Strumenti comuni e differenze di utilizzo**:

| | Strumento | Uso etico |
|---|---|---|
| | **Port scanner** | Test con autorizzazione |
| | **Vulnerability scanner** | Identified permitted targets |
| | **Packet sniffer** | Analisi reti autorizzate |
| | **Password cracker** | Test resilienza password |

| | Strumento | Uso etico |
|---|---|---|
| | **Exploitation framework** | PoC con limiti |
| | **Social engineering** | Simulazioni concordate |

## 4.3.2 Ruolo degli ethical hacker nella società

- **Contributi positivi**:
  - **Scoperta vulnerabilità**: identificazione problemi prima degli attaccanti
  - **Bug bounty ecosystem**: modello economico sostenibile per sicurezza
  - **Security awareness**: sensibilizzazione pubblica
  - **Trasparenza**: pressione su vendor per correzioni
  - **Evoluzione standard**: miglioramento continuo pratiche sicurezza
- **Ruoli professionali**:
  - **Penetration tester**: simulazione attacchi controllati
  - **Red teamer**: simulazione avversari reali
  - **Security researcher**: ricerca vulnerabilità
  - **Bug hunter**: partecipazione programmi bug bounty
  - **Security educator**: formazione e divulgazione
  - **Security evangelist**: promozione best practice
- **Considerazioni etiche**:
  - **Dual-use research**: ricerca con potenziale uso dannoso
  - **Disclosure of weaponizable bugs**: quando e come pubblicare
  - **Target selection**: considerazioni su impatto sociale
  - **Collateral damage**: rischi di danni non intenzionali
  - **Knowledge responsibility**: responsabilità per competenze acquisite
- **Evoluzione del ruolo**:
  - **Da outsider a insider**: integrazione nella sicurezza mainstream
  - **Da individui a community**: collaborazione e standard condivisi
  - **Da generalisti a specialisti**: focus su domini specifici
  - **Da tecnici a strategici**: ruolo sempre più ampio nelle organizzazioni
  - **Da reattivi a proattivi**: spostamento verso secure by design

## 4.3.3 Hacking per il bene comune: casi di studio

- **Civic hacking**:
  - **Definizione**: utilizzo di competenze hacking per beneficio pubblico
  - **Differenze da hacktivist**: rispetto delle leggi, costruttivo vs. disruptive
  - **Ambiti d'azione**: governi aperti, trasparenza, open data
  - **Modelli organizzativi**: hackathon civici, Code for All, lab civici
- **Caso 1: Sicurezza sanitaria**:

    - **MedSec e pacemaker vulnerabili**:
        - Scoperta vulnerabilità gravi in dispositivi impiantabili
        - Dilemma etico sulla disclosure
        - Impatto su policy FDA e sicurezza dispositivi medicali
        - Miglioramento standard industria
- **Caso 2: Sicurezza elettorale**:
    - **DEF CON Voting Village**:
        - Test annuale macchine elettorali
        - Scoperta numerose vulnerabilità
        - Miglioramento trasparenza processi elettorali
        - Influenza su regolamentazioni e certificazioni
- **Caso 3: Trasporto pubblico**:
    - **Karsten Nohl e vulnerabilità MIFARE**:
        - Reverse engineering smart card trasporti
        - Dimostrazione rischi per sistemi pubblici
        - Transizione verso soluzioni più sicure
        - Miglioramento security design
- **Caso 4: Sicurezza consumer**:
    - **Project Zero di Google**:
        - Team dedicato alla ricerca vulnerabilità
        - Strict disclosure timeline
        - Miglioramento ecosistema sicurezza
        - Pressione su vendor per aggiornamenti rapidi
- **Impatto e lezioni**:
    - **Awareness pubblica**: sensibilizzazione su rischi digitali
    - **Trasparenza forzata**: superamento "security by obscurity"
    - **Miglioramento standard**: evoluzione requisiti minimi
    - **Modello replicabile**: framework per ricerca responsabile
    - **Bilanciamento interessi**: pubblico vs. commerciale

# Conclusione

Lo studio degli standard di sicurezza informatica, delle normative sulla protezione dei dati e dell'evoluzione dei sistemi di identità digitale evidenzia l'importanza crescente di un approccio strutturato e conforme alla sicurezza nelle organizzazioni moderne.

La compliance normativa non deve essere vista come un semplice obbligo burocratico, ma come un'opportunità per implementare un framework di gestione della sicurezza solido ed efficace. L'adozione di standard internazionali come ISO 27001 e NIST CSF fornisce una base metodologica fondamentale per proteggere gli asset informativi.

Parallelamente, l'evoluzione dei sistemi di identità digitale, dalla tradizionale PKI alle emergenti tecnologie decentralizzate come SSI, dimostra come il panorama della sicurezza sia in costante trasformazione, richiedendo un continuo aggiornamento delle competenze e delle strategie.

Le considerazioni etiche legate alla security research e all'ethical hacking sottolineano inoltre la dimensione umana e sociale della cybersecurity: le competenze tecniche devono essere bilanciate da un solido framework etico e legale che garantisca che l'innovazione tecnologica proceda nel rispetto dei diritti fondamentali e della sicurezza collettiva.

In definitiva, la sicurezza informatica moderna richiede un approccio olistico che combini competenze tecniche, consapevolezza normativa, sensibilità etica e visione strategica: solo integrando queste diverse dimensioni è possibile costruire sistemi digitali realmente sicuri, resilienti e rispettosi dei diritti degli utenti.