1. FRAMEWORK DI SICUREZZA INFORMATICA E COMPLIANCE

Standard internazionali di sicurezza

ISO/IEC 27001 e famiglia 27000:

- **Definizione**: standard internazionale per gestione sicurezza informazioni
- **Scopo**: fornire framework per implementare, mantenere e migliorare un ISMS (Information Security Management System)
- **Struttura famiglia ISO 27000**:
  - **ISO 27000**: panoramica e vocabolario
  - **ISO 27001**: requisiti per ISMS (certificabile)
  - **ISO 27002**: controlli di sicurezza
  - **ISO 27005**: gestione rischio
  - **ISO 27017/27018**: sicurezza cloud
- **Componenti ISO 27001**:
  - Approccio basato sul rischio
  - Leadership e impegno
  - Pianificazione
  - Operatività
  - Valutazione prestazioni
  - Miglioramento
- **Ciclo PDCA**:
  - **Plan**: stabilire politiche e obiettivi
  - **Do**: implementare controlli
  - **Check**: monitorare e revisionare
  - **Act**: mantenere e migliorare

NIST Cybersecurity Framework:

- **Definizione**: framework volontario sviluppato dal National Institute of Standards and Technology (USA)
- **Struttura**:
  - **Core**: funzioni, categorie, sottocategorie
  - **Implementation Tiers**: livelli di maturità
  - **Profile**: allineamento business-sicurezza
- **Funzioni Core**:
  - **Identify**: comprensione rischi e asset

    - **Protect**: implementazione salvaguardie
    - **Detect**: identificare eventi di sicurezza
    - **Respond**: azioni post-incidente
    - **Recover**: ripristino capacità
- **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

Common Criteria (ISO/IEC 15408):

- **Definizione**: standard per valutazione sicurezza prodotti IT
- **Componenti**:
    - **Protection Profile (PP)**: requisiti indipendenti dall'implementazione
    - **Security Target (ST)**: requisiti specifici di un prodotto
    - **Target of Evaluation (TOE)**: prodotto valutato
- **Evaluation Assurance Levels (EAL)**:
    - **EAL1**: test funzionale
    - **EAL2**: test strutturale
    - **EAL3**: test metodico
    - **EAL4**: progettazione metodica
    - **EAL5**: progettazione semi-formale
    - **EAL6**: verifica semi-formale
    - **EAL7**: verifica formale
- **Applicazioni**: dispositivi di rete, sistemi operativi, smart card

2. IMPLEMENTAZIONE PRATICA DELLA SICUREZZA

Dall'implementazione tecnica alla conformità normativa

Gap Analysis e Risk Assessment:

- **Gap Analysis**:
    - **Definizione**: confronto stato attuale vs. stato desiderato
    - **Metodologia**:
        1. Definire stato target (requisiti)
        2. Valutare stato attuale
        3. Identificare gap
        4. Sviluppare piani d'azione
    - **Tipologie**: tecnica, organizzativa, documentale
- **Risk Assessment**:

- **Approcci**:
  - **Qualitativo**: scale alto/medio/basso
  - **Quantitativo**: calcoli numerici (ALE = SLE × ARO)
  - **Ibrido**: combinazione dei due
- **Processo**:
  1. Identificazione asset
  2. Identificazione minacce e vulnerabilità
  3. Analisi probabilità e impatto
  4. Determinazione livello rischio
  5. Controlli di mitigazione

Security Controls Implementation:

- **Categorie di controlli**:
  - **Per tipologia**: tecnici, amministrativi, fisici
  - **Per funzione**: preventivi, detective, correttivi
- **Mappatura controlli-standard**:
  - **ISO 27001 Annex A**: 114 controlli in 14 domini
  - **NIST SP 800-53**: controlli in 20 famiglie
  - **CIS Controls**: 20 controlli critici
- **Gestione documentazione**:
  - **Politiche**: obiettivi generali
  - **Standard**: requisiti specifici
  - **Procedure**: istruzioni dettagliate
  - **Evidenze**: prove di implementazione
- **Principi di sicurezza**:
  - **Defense-in-depth**: stratificazione controlli
  - **Least privilege**: diritti minimi
  - **Segregation of duties**: separazione compiti
  - **Need-to-know**: accesso solo alle info necessarie

Audit di sicurezza e compliance:

- **Tipi di audit**:
  - **Interno**: condotto dall'organizzazione
  - **Esterno**: condotto da terze parti
  - **Certificazione**: per ottenere certificazioni
  - **Penetration testing**: simulazione attacchi
- **Processo di audit**:
  - **Pianificazione**: scope, obiettivi, criteri
  - **Raccolta evidenze**: interviste, test, documenti

    - **Analisi**: valutazione conformità
    - **Reporting**: risultati e raccomandazioni
    - **Follow-up**: verifica azioni correttive
- **Tecniche di verifica**:
    - **Document review**: analisi documenti
    - **Interview**: colloqui col personale
    - **Observation**: osservazione diretta
    - **Technical testing**: verifiche tecniche
- **Gestione non conformità**:
    - Classificazione per gravità
    - Root cause analysis
    - Piani di remediation
    - Verifica efficacia azioni correttive

3. GDPR E PROTEZIONE DATI PERSONALI (PARTE 1)

Overview del GDPR e principi fondamentali

Definizione e ambito:

- **GDPR**: Regolamento (UE) 2016/679
- **In vigore**: dal 25 maggio 2018
- **Applicabilità**: organizzazioni che trattano dati di cittadini UE
- **Extraterritorialità**: si applica anche a organizzazioni extra-UE

Principi fondamentali:

- **Liceità, correttezza e trasparenza**:
    - Trattamento su base legale
    - Informative chiare e comprensibili
    - No trattamenti nascosti
- **Limitazione della finalità**:
    - Scopi specifici, espliciti, legittimi
    - No utilizzo per finalità incompatibili
- **Minimizzazione dei dati**:
    - Solo dati necessari allo scopo
    - No raccolte eccessive
- **Esattezza**:
    - Dati accurati e aggiornati
    - Rettifica o cancellazione di dati inesatti
- **Limitazione della conservazione**:
    - Conservazione solo per il tempo necessario

    - Definizione periodi di retention
- **Integrità e riservatezza**:
    - Protezione da trattamenti non autorizzati
    - Misure tecniche e organizzative adeguate
- **Accountability**:
    - Responsabilizzazione del titolare
    - Capacità di dimostrare conformità

Ruoli chiave:

- **Titolare del trattamento (Controller)**: determina finalità e mezzi
- **Responsabile del trattamento (Processor)**: tratta per conto del titolare
- **Interessato (Data subject)**: persona fisica identificata o identificabile
- **DPO (Data Protection Officer)**: supervisiona 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 a gravità, durata, natura dell'infrazione
- Diritto al risarcimento per gli interessati

Privacy by Design e Privacy by Default

Privacy by Design:

- **Definizione**: integrare protezione dati nella progettazione
- **Principi chiave**:
    1. Proattivo, non reattivo
    2. Privacy come impostazione predefinita
    3. Privacy incorporata nella progettazione
    4. Funzionalità completa (somma positiva)
    5. Sicurezza end-to-end
    6. Visibilità e trasparenza
    7. Rispetto per la privacy dell'utente

Privacy by Default:

- **Definizione**: impostazioni predefinite con massima protezione
- **Implementazioni**:
    - Raccolta solo dati necessari
    - Limitazione accesso ai dati
    - Opt-out per servizi non essenziali

    - Conservazione limitata
    - Minima condivisione dati

Approcci tecnici:

- **Data minimization**: raccolta minima di dati
- **Pseudonymization**: sostituzione identificatori con pseudonimi
- **Anonymization**: rendere impossibile l'identificazione
- **Encryption**: protezione dati tramite cifratura
- **Access controls**: limitazione accesso in base a necessità
- **Audit trails**: registrazione accessi e modifiche

4. GDPR E PROTEZIONE DATI PERSONALI (PARTE 2)

Implementazione tecnica dei diritti degli interessati

Diritto di accesso:

- **Implementazione**: sistema centralizzato di recupero dati
- **Requisiti tecnici**:
    - Capacità di estrarre tutti i dati di un individuo
    - Formati machine-readable
    - Inclusione di dati diretti e indiretti
- **Sfide**: dati distribuiti, formati eterogenei
- **Soluzioni**: data inventory, data mapping, sistemi SAR

Diritto di rettifica:

- **Implementazione**: meccanismi per correggere dati inesatti
- **Requisiti tecnici**:
    - Tracciabilità delle modifiche
    - Propagazione aggiornamenti tra sistemi
- **Sfide**: sincronizzazione sistemi diversi
- **Soluzioni**: single source of truth, master data management

Diritto alla cancellazione (diritto all'oblio):

- **Implementazione**: processi di eliminazione completa
- **Requisiti tecnici**:
    - Identificazione di tutti i dati collegati
    - Gestione dei backup
- **Sfide**: eliminazione dai backup senza compromettere integrità
- **Soluzioni**: tokenization, encryption con distruzione chiavi

Diritto alla limitazione del trattamento:

- **Implementazione**: sistemi per contrassegnare dati con restrizioni
- **Requisiti tecnici**:
  - Flag nei database
  - Controlli d'accesso granulari
- **Sfide**: garantire non-utilizzo dei 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 (XML, JSON)
  - Completezza dati
- **Sfide**: interoperabilità tra sistemi diversi
- **Soluzioni**: API standardizzate, formati di interscambio

Diritto di opposizione al trattamento automatizzato:

- **Implementazione**: meccanismi per esclusione da processi automatici
- **Requisiti tecnici**:
  - Opt-out da profiling
  - Intervento umano
- **Sfide**: identificazione decisioni automatizzate
- **Soluzioni**: human-in-the-loop, review processes

Data breach: rilevamento, gestione e notifica

Definizione data breach:

- Violazione di sicurezza che comporta:
  - Distruzione, perdita, modifica
  - Divulgazione non autorizzata
  - Accesso non autorizzato a dati personali

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
  - Esfiltrazioni dati
  - Comportamenti anomali utenti

Procedure di gestione:

- **Fase 1: Contenimento**:
  - Isolamento sistemi compromessi
  - Blocco accessi non autorizzati
  - Preservazione prove forensi
- **Fase 2: Valutazione**:
  - Identificazione dati compromessi
  - Determinazione gravità
  - Valutazione rischi per interessati
- **Fase 3: Remediation**:
  - Eliminazione causa
  - Ripristino sistemi
  - Implementazione controlli aggiuntivi
- **Fase 4: Documentazione**:
  - Registrazione azioni intraprese
  - Cronologia dettagliata
  - Lezioni apprese

Notifica:

- **All'Autorità di controllo**:
  - Entro 72 ore dalla scoperta
  - Descrizione natura violazione
  - Categorie e numero di interessati
  - Conseguenze probabili
  - Misure adottate o proposte
- **Agli interessati**:
  - Quando la violazione presenta rischio elevato
  - Linguaggio chiaro e semplice
  - Contatti DPO
  - Misure di mitigazione

Registro delle violazioni:

- Documentazione di tutte le violazioni
- Indipendentemente dall'obbligo di notifica
- Dettagli su circostanze, effetti, rimedi

5. IDENTITÀ DIGITALE E AUTENTICAZIONE

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

Evoluzione dei sistemi:

1. **Password semplici**: vulnerabili a brute force, social engineering
2. **Password policy**: lunghezza, complessità, rotazione
3. **Password manager**: generazione e gestione sicura
4. **2FA**: password + secondo fattore
5. **MFA**: combinazione di 3+ fattori
6. **Autenticazione adattiva**: basata su comportamento/rischio
7. **Passwordless**: eliminazione password

Tecnologie per autenticazione forte:

- **OTP (One-Time Password)**:
  - **HOTP**: basato su contatore
  - **TOTP**: basato su timestamp
  - **Distribuzione**: SMS, email, app
- **Hardware token**:
  - Token fisici (Yubikey, RSA SecurID)
  - Smart card
  - Security keys (FIDO2)
- **Mobile authentication**:
  - Push notification
  - App authenticator
  - QR code scanning
- **Biometria**:
  - Impronte, volto, iride

    - Voce
    - Comportamentale (keystroke dynamics)

Standard e protocolli:

- **FIDO2/WebAuthn**: autenticazione crittografica
- **OAuth 2.0**: framework autorizzazione
- **OpenID Connect**: identità su OAuth 2.0
- **SAML**: Security Assertion Markup Language
- **JWT**: JSON Web Token

Single Sign-On e sistemi federati

Single Sign-On (SSO):

- **Definizione**: autenticazione unica per più applicazioni
- **Vantaggi**:
    - Migliore user experience
    - Gestione centralizzata
    - Riduzione password fatigue
    - Maggiore sicurezza
- **Tipi di SSO**:
    - **Enterprise SSO**: interno all'organizzazione
    - **Web SSO**: applicazioni web
    - **Federated SSO**: tra organizzazioni diverse
- **Funzionamento**:
    1. Autenticazione su IdP o SP
    2. Generazione token/ticket
    3. Propagazione token alle applicazioni
    4. Validazione e accesso

Identity Federation:

- **Definizione**: condivisione identità tra organizzazioni
- **Componenti**:
    - **Identity Provider (IdP)**: gestisce autenticazione
    - **Service Provider (SP)**: fornisce servizi
    - **Protocolli di federazione**: standard di scambio
- **Meccanismi di trust**:
    - **Bilateral**: accordi diretti
    - **Hub and spoke**: entità centrale
    - **Web of trust**: relazioni multiple

- **Implementazioni**:
  - **SAML federations**: educative (eduGAIN)
  - **Social login**: Google, Facebook, Apple
  - **Enterprise federation**: B2B, supply chain

Protocolli federativi:

- **SAML**:
  - Standard XML per scambio dati
  - Architettura IdP/SP
  - Assertion contenenti attributi
  - Diffuso in ambito enterprise
- **OAuth 2.0**:
  - Framework di autorizzazione
  - Delega accesso via token
  - Grant types per diversi scenari
  - Base per federazione
- **OpenID Connect (OIDC)**:
  - Layer identità su OAuth 2.0
  - ID token (JWT)
  - UserInfo Endpoint per attributi

Sfide e considerazioni:

- **Privacy**: minimizzazione dati condivisi
- **Session management**: durata, invalidazione, logout
- **Incident response**: compromissione identità
- **Vendor lock-in**: dipendenza da provider
- **Regulatory compliance**: conformità tra domini

6. FIRMA DIGITALE E PKI

Infrastruttura a chiave pubblica (PKI)

Definizione e componenti:

- **PKI**: framework per creare, gestire, distribuire, utilizzare certificati digitali
- **Certificato digitale**: documento che associa chiave pubblica a identità
- **CA (Certificate Authority)**: ente che emette certificati
- **RA (Registration Authority)**: verifica identità
- **VA (Validation Authority)**: verifica validità
- **Subscriber**: entità che usa il certificato

- **Relying party**: entità che si affida al certificato

Architettura PKI:

- **Root CA**: massimo livello, generalmente offline
- **Intermediate CA**: emettono per conto della Root
- **Issuing CA**: emettono per utenti finali
- **Cross-certification**: relazioni tra CA diverse
- **Bridge CA**: interconnessione tra domini

Formato certificati X.509:

- **Versione**: formato (tipicamente v3)
- **Numero seriale**: identificativo univoco
- **Algoritmo di firma**: usato dalla CA
- **Emittente**: nome CA
- **Validità**: Not Before, Not After
- **Soggetto**: identità titolare
- **Chiave pubblica**: algoritmo e valore
- **Estensioni**: usi, vincoli, CRL, AIA
- **Firma digitale**: firma della CA

Certificate Revocation:

- **CRL**: Certificate Revocation List
- **OCSP**: Online Certificate Status Protocol
- **OCSP Stapling**: risposta allegata
- **Motivi revoca**: compromissione, cessazione, sostituzione

Applicazioni:

- **TLS/SSL**: sicurezza web
- **Code signing**: firma software
- **Email sicura**: S/MIME
- **Documenti firmati**: PDF, XML
- **Smart card**: autenticazione
- **IPsec**: VPN

eIDAS e normativa italiana

eIDAS:

- **Definizione**: Regolamento UE n. 910/2014
- **Obiettivi**: mercato unico digitale europeo

- **Ambito**: identità, firme, sigilli, marcatura temporale
- **Principio di non discriminazione**: validità forma elettronica
- **Mutuo riconoscimento**: sistemi notificati

Livelli di firma elettronica:

- **Semplice**: dati allegati ad altri dati
- **Avanzata (FEA)**: requisiti di identificazione e controllo
- **Qualificata (FEQ)**: avanzata con dispositivo sicuro e certificato qualificato
- **Sigillo elettronico**: equivalente per persone giuridiche

Prestatori di servizi fiduciari:

- **Qualified TSP**: autorizzati a livello nazionale
- **Supervisione**: organismi designati
- **EU Trusted Lists**: elenchi prestatori qualificati
- **Servizi**: CA, timestamping, conservazione, PEC

Normativa italiana:

- **CAD (Codice dell'Amministrazione Digitale)**:
  - D.Lgs. 82/2005
  - Documenti informatici
  - Domicilio digitale
  - Pagamenti elettronici
- **PEC (Posta Elettronica Certificata)**:
  - Valore legale raccomandata A/R
  - Gestori accreditati AgID
- **SPID (Sistema Pubblico di Identità Digitale)**:
  - Tre livelli di sicurezza
  - Identity provider accreditati
  - Notificato sotto eIDAS
- **CIE (Carta d'Identità Elettronica)**:
  - Documento con chip
  - Autenticazione forte
  - Compatibile con eIDAS

Evoluzione:

- **eIDAS 2.0**: European Digital Identity
- **Wallet digitale europeo**: gestione credenziali
- **Identità decentralizzata (SSI)**: controllo utente
- **Interoperabilità**: sistemi nazionali

7. RESPONSIBLE DISCLOSURE E BUG BOUNTY

Principi della responsible disclosure

Definizione:

- Processo etico per segnalare vulnerabilità
- Bilanciamento tra sicurezza pubblica e tempo per correggere
- Minimizzazione rischi da exploit

Modelli di disclosure:

- **Full disclosure**: pubblicazione immediata
- **Non-disclosure**: nessuna divulgazione
- **Coordinated disclosure**: collaborazione con vendor
- **Responsible disclosure**: tempo ragionevole per patch

Timeline tipica:

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

Best practice:

- **Comunicazione sicura**: PGP/canali crittati
- **Proof of concept**: dimostrare senza danneggiare
- **Minimizzazione dettagli sensibili**: no exploit pubblici
- **Documentazione chiara**: prerequisiti, impatto
- **CVE assignment**: codifica vulnerabilità
- **Esclusione dati sensibili**: no PII

Considerazioni legali:

- **CFAA (USA)**: rischi responsabilità
- **EU Cybersecurity Act**: supporto responsible disclosure
- **Safe harbor**: protezioni per researcher
- **Terms of service**: violazioni potenziali
- **NDA**: accordi non divulgazione
- **Autorizzazione**: esplicita vs. implicita

Bug bounty programs

Definizione:

- Programmi che premiano la scoperta di vulnerabilità
- Modello crowdsourced di security testing
- Incentivazione responsible disclosure

Tipi di programmi:

- **Pubblici**: aperti a tutti
- **Privati**: solo invitati
- **Ongoing**: costanti
- **Time-boxed**: competizioni limitate
- **Self-hosted**: gestione diretta
- **Platform-based**: tramite piattaforme

Piattaforme principali:

- **HackerOne**: enterprise e government
- **Bugcrowd**: ampia gamma
- **Intigriti**: europea, compliance
- **Synack**: Red team gestito
- **Open Bug Bounty**: vulnerabilità web
- **YesWeHack**: piattaforma europea

Struttura tipica:

- **Scope**: sistemi inclusi
- **Out-of-scope**: aree escluse
- **Reward table**: ricompense per severità
- **Rules of engagement**: limiti dei test
- **Safe harbor**: protezioni legali
- **Reporting guidelines**: formato report
- **SLA**: tempi risposta

Modelli di ricompensa:

- **Pay-per-vulnerability**: pagamento per bug
- **Tiered rewards**: basate su CVSS
    - Critical: $5,000-$50,000+
    - High: $1,000-$10,000
    - Medium: $500-$2,500
    - Low: $100-$500

- **Bonus**: report alta qualità
- **Recognition**: hall of fame

Benefici e sfide:

- **Benefici**:
  - Talenti globali
  - Pagamento per risultati
  - Complemento a security testing
  - Miglioramento continuo
  - Trasparenza
- **Sfide**:
  - Gestione volume report
  - Budget
  - Requisiti legali
  - Triaging

8. ETHICAL HACKING E NORMATIVE SULLA SECURITY RESEARCH

Framework legali per security testing

Legislazione europea:

- **NIS Directive 2**:
  - Supporto alla disclosure
  - Protezioni per researcher
  - Armonizzazione approcci
- **EU Cybersecurity Act**:
  - Framework certificazione
  - Supporto ENISA
  - Standardizzazione
- **GDPR**:
  - Implicazioni per test con dati personali
  - Data breach notification
  - Security by design

Legislazione italiana:

- **Codice Penale art. 615-ter**: accesso abusivo
- **D.Lgs. 231/2001**: responsabilità enti
- **Perimetro di sicurezza nazionale cibernetica**:

- Regole specifiche per testing

Safe harbor provisions:

- **Definizione**: protezioni per researcher in buona fede
- **Elementi**:
  - Scopo e limitazioni
  - Requisiti disclosure
  - Impegni reciproci
  - Non-prosecution

Caveat legali:

- **Autorizzazione**: esplicita, documentata
- **Jurisdictional issues**: leggi diverse
- **Danni collaterali**: responsabilità
- **Limitazioni contrattuali**: ToS, EULA, NDA
- **Asset di terze parti**: complicazioni supply chain

Distinzione tra hacking etico e criminale

Definizioni:

- **Hacker** (originale): innovatore tecnologico
- **White hat**: ethical hacker
- **Grey hat**: area grigia, senza intenti malevoli
- **Black hat**: hacker criminale

Elementi distintivi:

Aspetto	Ethical Hacking	Criminal Hacking
Autorizzazione	Esplicita	Assente
Intento	Migliorare sicurezza	Profitto, danno
Disclosure	Responsible disclosure	Vendita exploit
Impatto	Limitato, controllato	Potenzialmente illimitato
Compenso	Legittimo	Illecito
Metodologia	Documentata	Stealth

Confini etici e legali:

- **Ethical hacking formale**: pentest autorizzato
- **Security research**: analisi sistemi pubblici

- **Academic research**: avanzamento conoscenza
- **Grey area**: research senza autorizzazione
- **Illegale**: data theft, ransomware

Professionalizzazione:

- **Certificazioni**: CEH, OSCP, CREST
- **Formazione**: corsi specializzati, CTF
- **Carriere**: penetration tester, red team
- **Standard**: codici etici
- **Community**: conferenze (DEF CON, Black Hat)

Ruolo degli ethical hacker nella società:

- **Scoperta vulnerabilità**: prima degli attaccanti
- **Bug bounty ecosystem**: modello economico sostenibile
- **Security awareness**: sensibilizzazione
- **Trasparenza**: pressione su vendor
- **Evoluzione standard**: miglioramento pratiche