DESCRIZIONE DEL PROGETTO

Questo progetto integrato permette di ottenere una valutazione unica sia per **Sistemi e Reti** che per **Educazione Civica**, attraverso lo sviluppo di una presentazione tecnica o un elaborato scritto che analizzi gli aspetti di sicurezza informatica avanzata, standard di compliance e responsabilità professionale nell'ambito delle tecnologie di rete.

Il lavoro dovrà integrare le competenze tecniche acquisite durante il corso (protocolli di rete, sicurezza, crittografia, livello applicativo) con una riflessione critica sugli aspetti normativi, etici e di responsabilità sociale legati alla sicurezza informatica e alla protezione dei dati.

OBIETTIVI

Competenze tecniche (Sistemi e Reti)

- Dimostrare comprensione approfondita degli standard e framework di sicurezza
- Analizzare criticamente le soluzioni tecniche per la protezione delle reti e dei dati
- Valutare l'implementazione di controlli di sicurezza in contesti specifici
- Collegare i concetti di crittografia e protocolli sicuri alle applicazioni pratiche

Competenze di cittadinanza (Educazione Civica)

- Comprendere il quadro normativo sulla protezione dei dati e sicurezza informatica
- Analizzare le implicazioni etiche delle tecnologie di sicurezza
- Valutare il bilanciamento tra sicurezza, privacy e accessibilità
- Riflettere sulla responsabilità professionale degli operatori IT

TRACCE DISPONIBILI

Gli studenti sceglieranno **UNA** delle seguenti tracce:

TRACCIA 1: Framework di sicurezza e compliance normativa

- **Aspetti tecnici**:
  - Analisi comparativa di standard di sicurezza (ISO 27001, NIST CSF)
  - Implementazione tecnica di controlli di sicurezza
  - Gap analysis e risk assessment metodologie
  - Audit e certificazione di sicurezza
- **Aspetti di Educazione Civica**:
  - Evoluzione normativa della sicurezza informatica
  - Responsabilità legale delle organizzazioni
  - Bilanciamento tra compliance e innovazione

- Trasparenza e accountability nelle politiche di sicurezza

TRACCIA 2: GDPR e protezione dei dati nelle infrastrutture di rete

- **Aspetti tecnici**:
  - Implementazione tecnica della Privacy by Design
  - Soluzioni per la protezione dei dati in transito e a riposo
  - Gestione tecnica dei data breach
  - Architetture a supporto dei diritti degli interessati
- **Aspetti di Educazione Civica**:
  - Diritti fondamentali alla privacy e protezione dati
  - Bilanciamento tra sicurezza e privacy
  - Asimmetrie informative e potere dei dati
  - Implicazioni globali delle normative europee

TRACCIA 3: Identità digitale, autenticazione e fiducia nelle reti

- **Aspetti tecnici**:
  - Evoluzione dei sistemi di autenticazione e autorizzazione
  - Infrastrutture a chiave pubblica (PKI) e firma digitale
  - Single Sign-On e identity federation
  - Biometria e nuove tecnologie di autenticazione
- **Aspetti di Educazione Civica**:
  - Identità digitale come diritto fondamentale
  - Inclusività e accessibilità dei sistemi di identità
  - Sovranità digitale e controllo dell'identità
  - Fiducia digitale e democrazia elettronica

TRACCIA 4: Ethical Hacking, Responsible Disclosure e Bug Bounty

- **Aspetti tecnici**:
  - Metodologie di penetration testing e security assessment
  - Protocolli di responsible disclosure
  - Architettura e gestione dei programmi di bug bounty
  - Strumenti e tecniche di ethical hacking
- **Aspetti di Educazione Civica**:
  - Etica hacker e responsabilità professionale
  - Framework legali per la security research
  - Bilanciamento tra trasparenza e sicurezza

- Collaborazione pubblico-privato nella cybersecurity

FORMATO E REQUISITI

Il progetto può essere sviluppato in **uno** dei seguenti formati:

Opzione 1: Presentazione tecnica (da esporre alla classe)

- **Numero slide**: 12-18 slide
- **Durata**: 12-15 minuti di presentazione + 5 minuti Q&A
- **Formato**: PowerPoint o Google Slides
- **Struttura**:
  1. Titolo e overview
  2. Introduzione al contesto normativo/tecnico
  3. Analisi approfondita degli aspetti tecnici
  4. Implementazione pratica di soluzioni
  5. Case study dettagliato
  6. Implicazioni etiche/sociali/normative
  7. Sfide e opportunità future
  8. Raccomandazioni e best practices
  9. Conclusioni e riferimenti

Opzione 2: Relazione tecnica (da esporre alla classe commentandone le scelte)

- **Lunghezza**: 10-12 pagine (esclusi copertina, indice e bibliografia)
- **Formato**: PDF, Times New Roman 12pt, interlinea 1,5
- **Struttura**:
  1. Abstract
  2. Introduzione al contesto
  3. Framework teorico
  4. Analisi tecnica approfondita
  5. Mapping tra aspetti tecnici e normativi
  6. Case study
  7. Implicazioni etiche e sociali
  8. Raccomandazioni
  9. Conclusioni
  10. Bibliografia

REQUISITI TECNICI

1. **Approfondimento tecnico** che dimostri padronanza degli argomenti avanzati studiati

2. **Almeno un diagramma architetturale** che illustri l'implementazione della soluzione analizzata
3. **Almeno una matrice** di mappatura tra requisiti normativi/etici e controlli tecnici
4. **Riferimenti espliciti** agli standard del settore studiati
5. **Almeno un caso studio reale** documentato con fonti attendibili
6. **Analisi critica** delle soluzioni proposte, con vantaggi e limiti
7. **Riferimenti bibliografici** accurati, aggiornati e pertinenti

CRITERI DI VALUTAZIONE

Criterio	Peso	Descrizione
Comprensione degli Standard	30%	Accurata interpretazione dei framework di sicurezza, corretta applicazione dei requisiti normativi, comprensione delle relazioni tra controlli e compliance
Implementazione Tecnica	30%	Dettaglio delle soluzioni tecniche proposte, analisi della loro efficacia, mappatura concreta tra requisiti e controlli implementativi
Analisi delle Problematiche	20%	Identificazione di gap e sfide nell'implementazione, analisi critica dei limiti degli standard, proposte innovative per migliorare la conformità
Qualità dell'Elaborato	20%	Per presentazioni: organizzazione logica, efficacia comunicativa, gestione domande tecniche Per paper: struttura metodologica, precisione terminologica, documentazione adeguata

TIMELINE

- **Assegnazione progetto**: Prima settimana di maggio
- **Scelta della traccia**: Entro una settimana dall'assegnazione
- **Consegna abstract/outline**: Metà maggio (facoltativo, per feedback)
- **Consegna finale/Presentazione**: Prima settimana di giugno

SUGGERIMENTI PER LO SVILUPPO

1. **Focalizzati su uno standard specifico** o sul confronto mirato tra due framework complementari
2. **Elabora un caso di studio realistico** che dimostri l'applicazione pratica dei requisiti
3. **Crea una matrice di mappatura** tra requisiti normativi e controlli tecnici implementabili
4. **Analizza criticamente** l'efficacia dei controlli proposti in relazione alle minacce attuali
5. **Considera gli aspetti multidisciplinari** tra sicurezza tecnica, compliance normativa ed etica

6. **Evidenzia le tensioni** tra diversi requisiti (es. sicurezza vs usabilità, privacy vs funzionalità)
7. **Proponi soluzioni innovative** che bilancino i diversi aspetti analizzati

SUPPORTO

Per chiarimenti e supporto durante lo sviluppo del progetto:

- Orario di ricevimento: da definire
- Email: g.rovesti@gferraris.it
- Materiali di riferimento disponibili sul registro elettronico

---