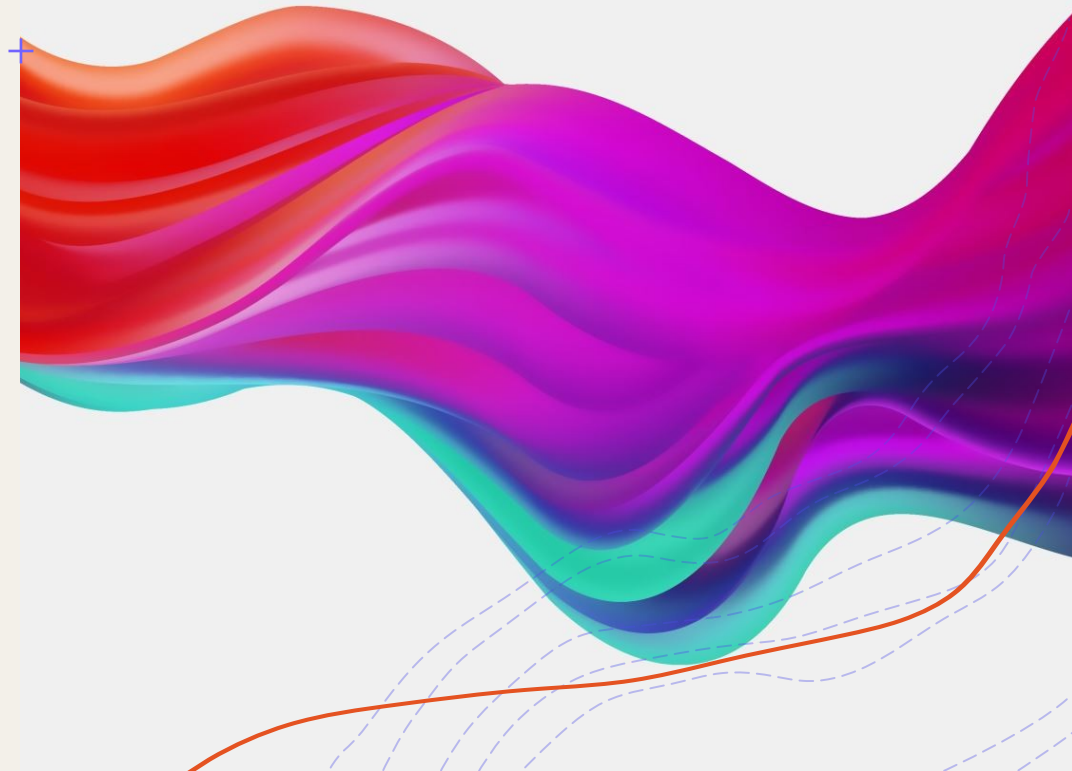


Framework di sicurezza e compliance normativa Educazione Civica e Sistemi e Reti

Albertin Riccardo

Classe 4D

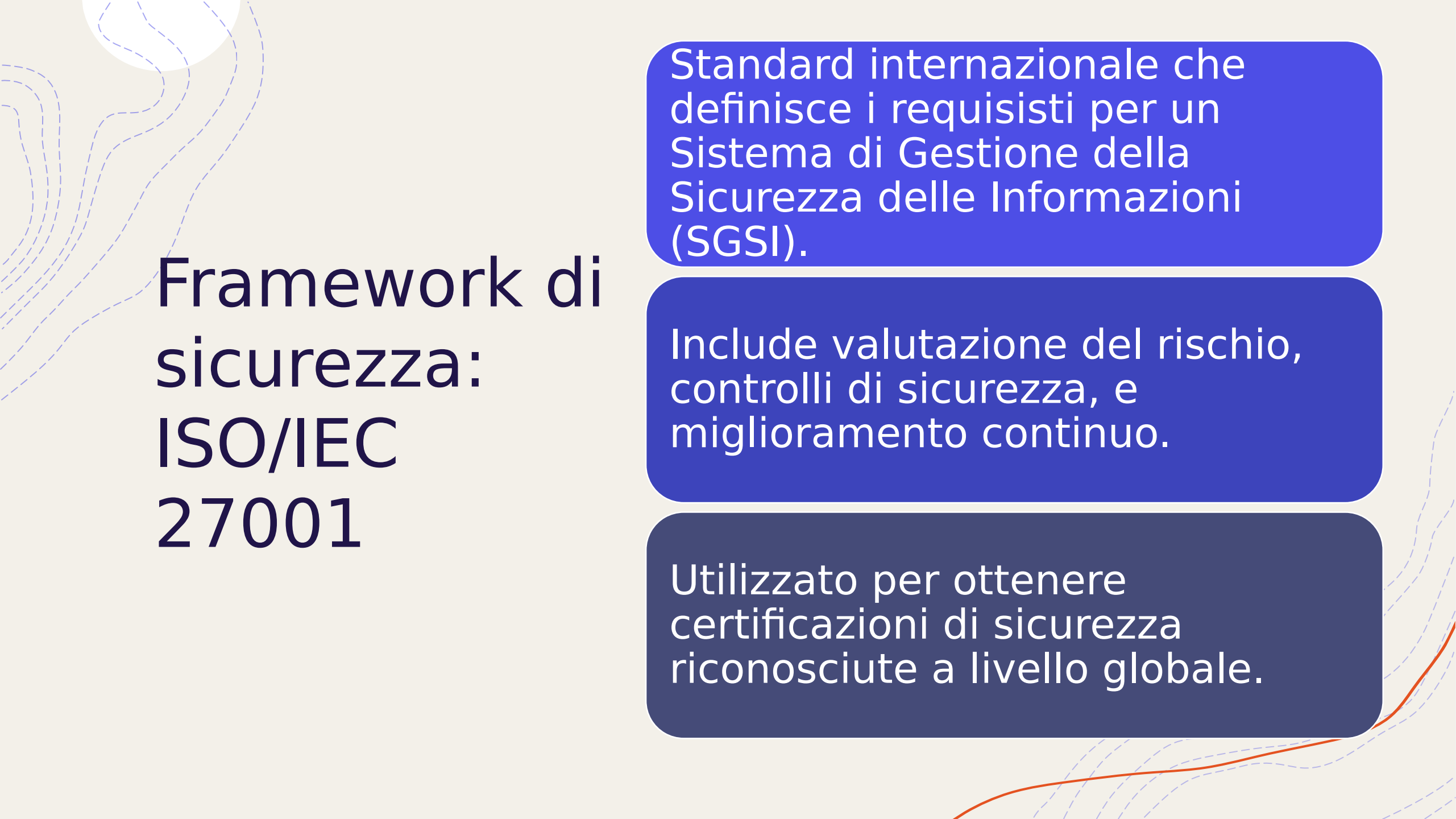


Introduzione al contesto

La sicurezza informatica è un pilastro fondamentale per il funzionamento di sistemi digitali affidabili.

Con la crescente quantità di dati trattati e le minacce sempre più avanzate, diventa cruciale adottare framework di sicurezza molto efficaci.

Le normative europee e internazionali spingono le organizzazioni ad allinearsi a standard riconosciuti.

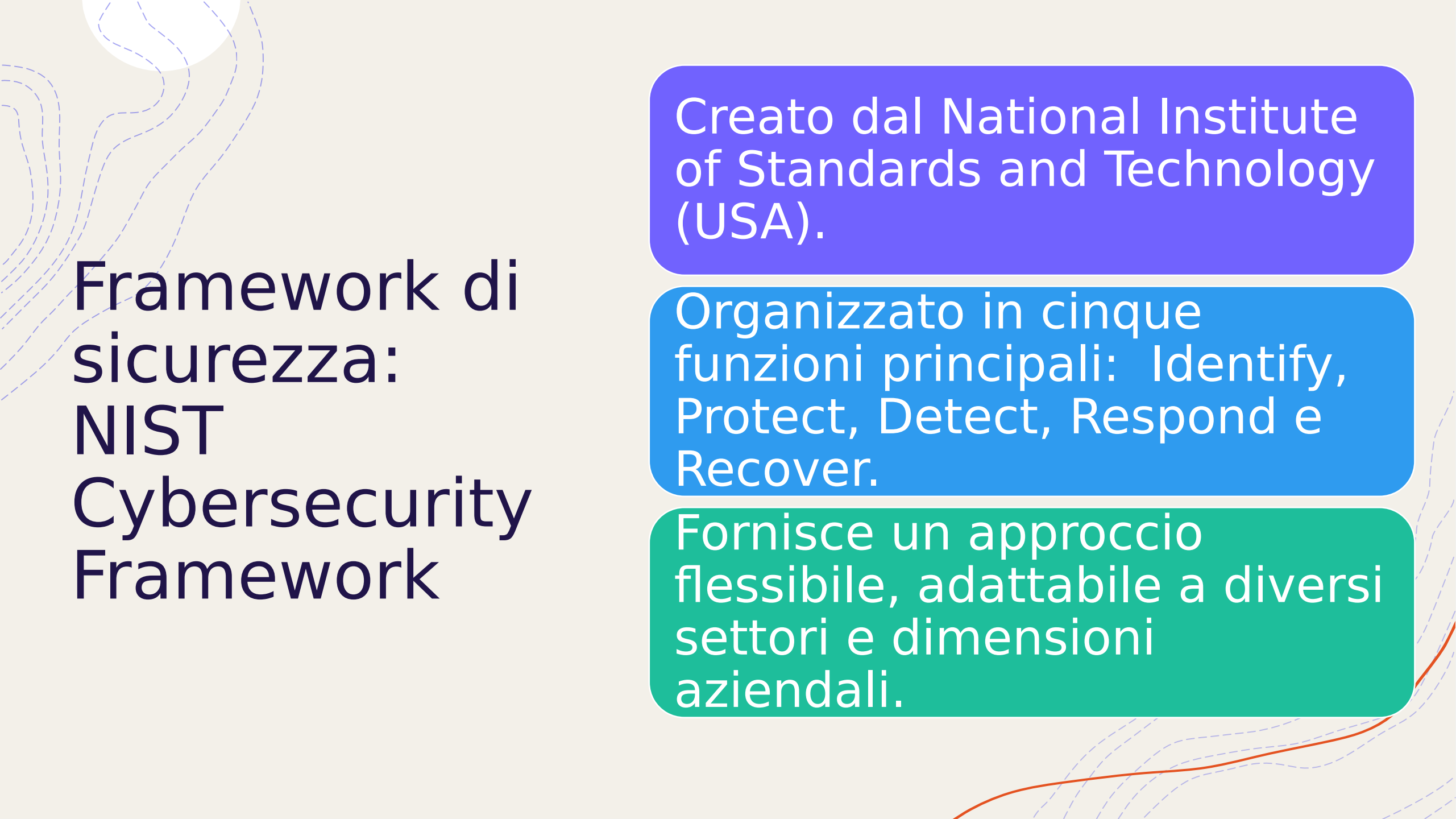


Framework di sicurezza: ISO/IEC 27001

Standard internazionale che definisce i requisiti per un Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

Include valutazione del rischio, controlli di sicurezza, e miglioramento continuo.

Utilizzato per ottenere certificazioni di sicurezza riconosciute a livello globale.



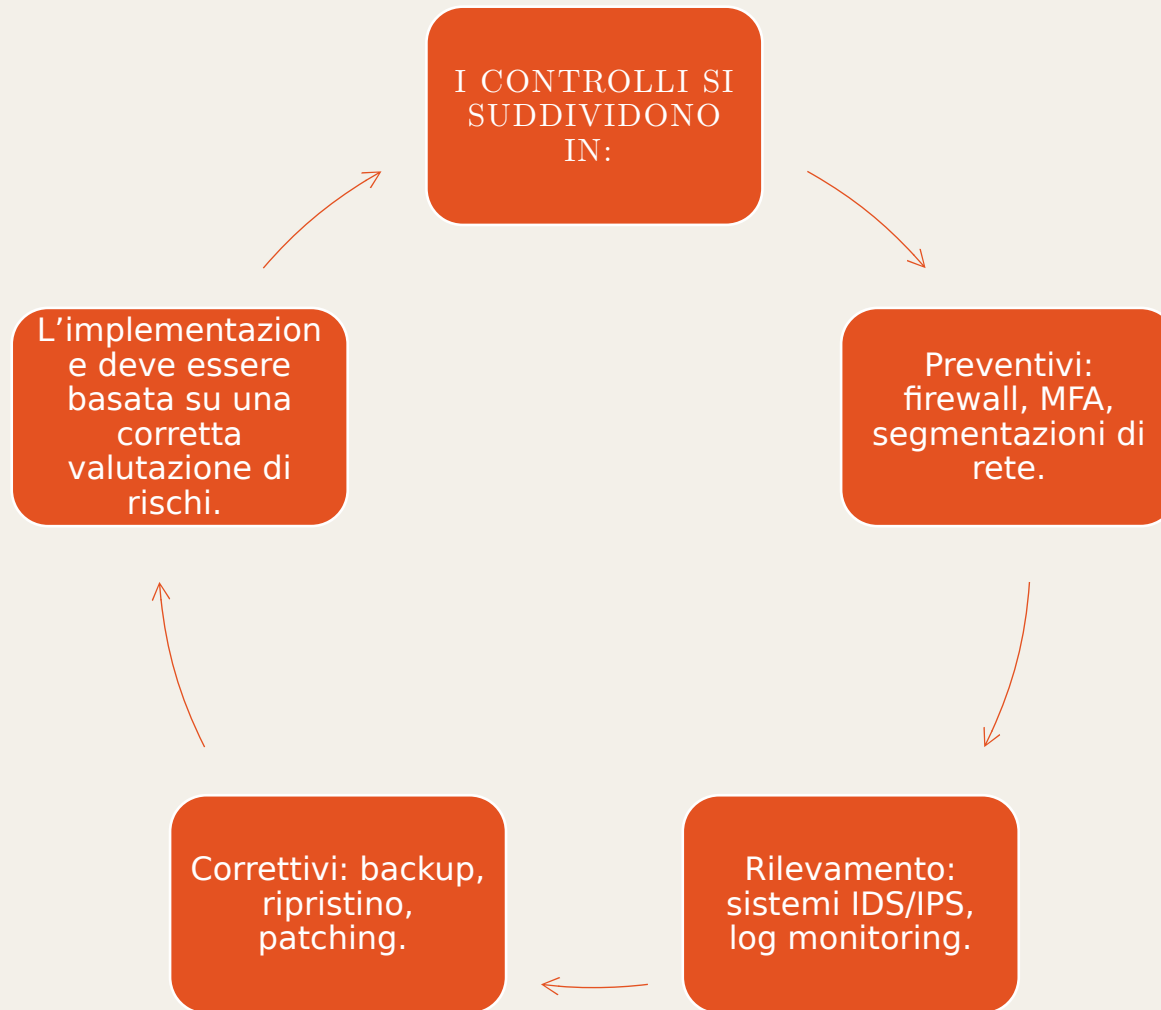
Framework di sicurezza: NIST Cybersecurity Framework

Creato dal National Institute of Standards and Technology (USA).

Organizzato in cinque funzioni principali: Identify, Protect, Detect, Respond e Recover.

Fornisce un approccio flessibile, adattabile a diversi settori e dimensioni aziendali.

Controlli di sicurezza





Crittografia e protocolli

La crittografia è essenziale per la riservatezza e l'integrità dei dati.

Protocolli come HTTPS, TLS e VPN proteggono i dati in transito.

L'uso di chiavi pubbliche e private permette autenticazione sicura e firma digitale.

Mappatura normativa

Le normative (es. GDPR) impongono requisiti di sicurezza precisi.

È utile creare una matrice che mappi i requisiti normativi ai controlli tecnici implementati.

Esempio: crittografia dei dati personali e misure per garantirne la disponibilità.

Caso studio: implementazione ISO 27001



UNA PMI DECIDE DI
ADOTTARE ISO 27001
PER MIGLIORARE LA SUA
SICUREZZA.



FASI: VALUTAZIONE DEI
RISCHI, DEFINIZIONE DEI
CONTROLLI, FORMAZIONE,
AUDIT INTERNO.



RISULTATO: MAGGIORE
PROTEZIONE DEI DATI E
POSSIBILITÀ DI ACCEDERE
A MERCATI
REGOLAMENTATI.

Aspetti normative ed etici

Le organizzazioni devono rispettare leggi come GDPR, NIS2, Cyber Resilience Act.

Importante bilanciare la sicurezza con diritti fondamentali come la privacy.

Gli operatori IT hanno una responsabilità professionale e legale.

Sfide e opportunità future

Sfide:

- Minacce in evoluzione (es. ransomware)

- Complessità normativa

Opportunità:

- Intelligenza artificiale per il rilevamento minacce

- Automazione dei controlli di compliance

Diagramma Architetture: Sicurezza in Rete



Esempio di architettura sicura:



- Firewall perimetrale



- VPN per accesso remoto



- Segmentazione LAN con VLAN



- IDS/IPS per rilevamento intrusioni



- Server crittografati (TLS, dischi cifrati)



- Backup off-site



- Logging centralizzato e SIEM

Raccomandazioni e best practices

- Approccio basato sul rischio
- Formazione continua del personale
- Revisione regolare dei controlli di sicurezza
- Documentazione chiara e auditabile

Conclusioni

I framework come ISO 27001 e NIST CSF aiutano a strutturare la sicurezza informatica in modo efficace.

L'integrazione tra aspetti tecnici, normativi ed etici è fondamentale.

La sicurezza è un processo continuo, non un obiettivo statico.

Riferimenti

- ISO.org

- NIST.gov

- GDPR.eu

- ENISA (Agenzia europea per la cybersicurezza)

- Documentazione aziendale e casi studio