



# DOCUMENTO GUIDA CYBERSECURITY

**ING. LAURA CASTELLANI**  
**PRESIDENTE COMMISSIONE CYBERSECURITY CDTI**  
**ROMA 19 MARZO 2026**



## DOCUMENTO GUIDA CYBERSECURITY

### Obiettivo del documento

Costituire una guida operativa per PMI e piccoli Enti della PA, una guida che sia semplice e permetta di poter mettere in atto tutte le azioni necessarie previste dalle normative nazionali in tema di cybersecurity

### Struttura logica del documento

Il documento segue un percorso che parte dalla normativa vigente e dalle strategie e arriva alla capacità operativa e alle prospettive future.

Il tutto seguendo una visione integrata di norme, processi, tecnologia, persone e scenari evolutivi.

### Modalità di costruzione del documento

All'interno della Commissione Cybersecurity i singoli membri scelgono di sviluppare una parte del documento in una logica bottom-up collaborativa



## INDICE DEL DOCUMENTO – CAPITOLI E AREE TEMATICHE

### Cornice regolatoria e strategica

Il Capitolo 1 definisce obblighi e pressioni esterne che rendono la cybersecurity una priorità imprescindibile per aziende e filiere.

### Governance e compliance

Il Capitolo 2 trasforma obblighi in responsabilità interne, chiarendo ruoli, framework e KPI per la resilienza.

### Parte operativa e abilitante

I Capitoli 3 e 4 propongono strumenti, procedure e tecnologie per difendere il perimetro digitale e adeguarsi.

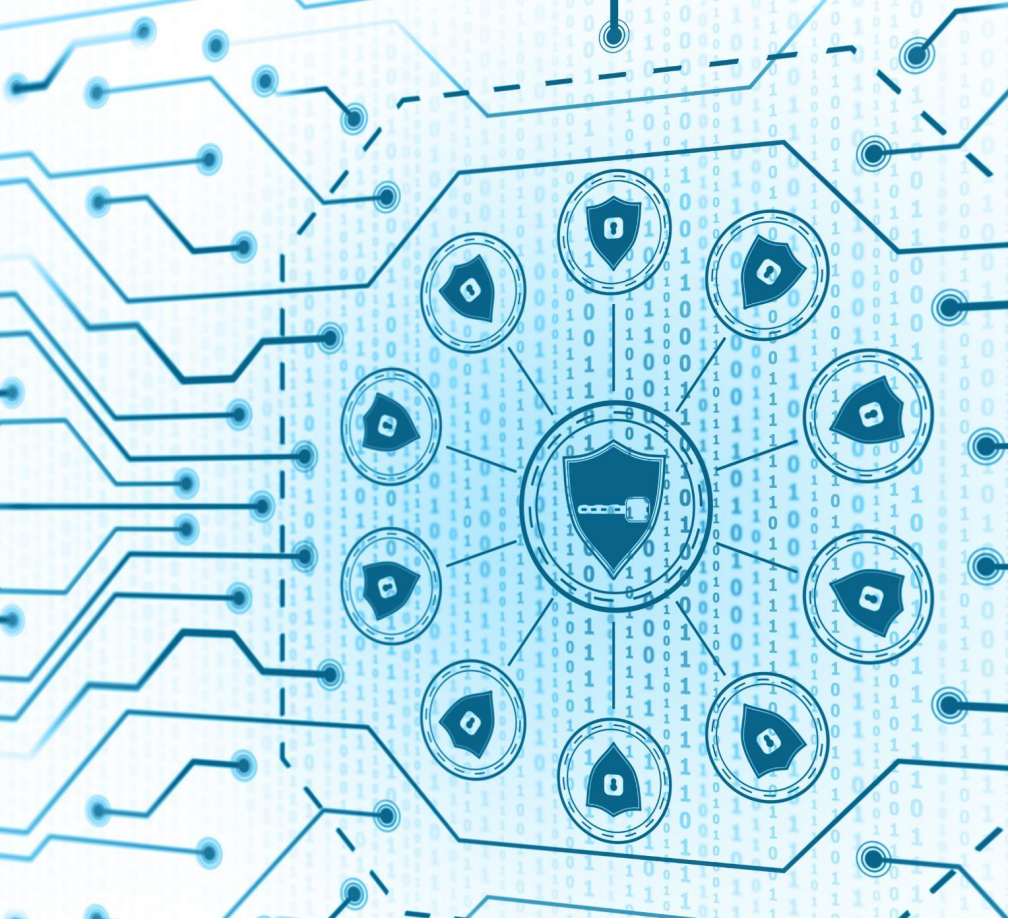
### Capitoli verticali e trasversali

Il Capitolo 5 tratta i settori critici e casi di studio (energia e infrastrutture critiche, sanità e PA locali, industria manifatturiera e supply chain, servizi finanziari e digitali)

Il Capitolo 6 tratta il tema importante della formazione sul tema

Il Capitolo 7 definisce i toolkit operativi e gli strumenti di compliance messi a disposizione

Il Capitolo 8 parla del futuro della Cybersecurity con riferimento anche al quantum e agli impatti dell' AI.



## **INTRODUZIONE – TARGET E PERCHÉ È CRUCIALE OGGI**

### **Target principale**

Il manuale si rivolge a dirigenti ICT, CISO e manager dell'innovazione con focus decisionale.

### **Rischi e impatti**

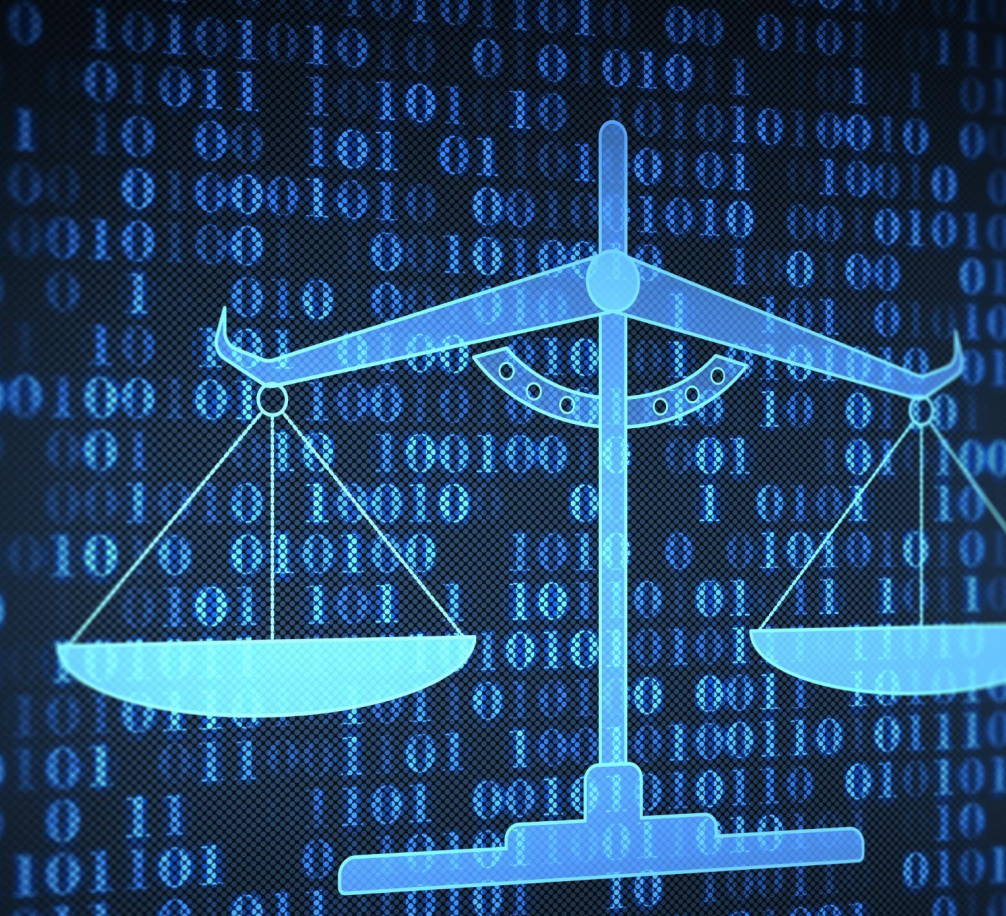
La digitalizzazione aumenta i rischi su continuità operativa, dati e reputazione aziendale.

### **Opportunità e vantaggi**

Investire in cybersecurity crea fiducia, qualità del servizio e vantaggi competitivi.

### **Responsabilità e governance**

La governance deve definire ruoli, risorse e garantire trasparenza, soprattutto in incidenti.



## **CAPITOLO 1 – SCENARIO NORMATIVO E STRATEGICO**

### Direttiva NIS2 e filiere critiche

La sicurezza si estende a ecosistemi e supply chain, richiedendo gestione del rischio e continuità dei servizi essenziali.

### Cyber Resilience Act e sicurezza by design

La sicurezza by design diventa obbligatoria per prodotti e servizi digitali, integrando sicurezza nel ciclo di vita.

### AI Act e gestione del rischio AI

L'AI introduce nuovi rischi e richiede valutazione, documentazione e controllo sistematico, specie in processi critici.

### Convergenza tra sicurezza e privacy

GDPR e Data Governance Act uniscono sicurezza e privacy, proteggendo dati e gestendo accessi e tracciabilità.



## CAPITOLO 2 – GOVERNANCE E MODELLI DI COMPLIANCE

### Leadership e decisioni strategiche

Le decisioni chiave sulla cybersecurity coinvolgono il board e la leadership, non solo il team IT.

### Framework di governance condivisi

L'adozione di standard riconosciuti evita frammentazioni e facilita un linguaggio comune tra i team.

### Misurabilità con KPI e risk management

I KPI aiutano a misurare la reale capacità di prevenzione, rilevazione e risposta agli incidenti.

### Accountability e ruoli chiari

Definire responsabilità tra CISO, CRO e altri ruoli previene sovrapposizioni e vuoti di governance.



## CAPITOLO 3 – STRUMENTI PER L'ADEGUAMENTO

### Autovalutazione di maturità

Il modello CDTI consente di misurare la maturità attuale prima di investire, creando una baseline condivisa tra i manager.

### Matrice rischi e impatti

La matrice collega requisiti normativi agli impatti organizzativi, definendo chi fa cosa e quali processi cambiano.

### Policy e procedure essenziali

Policy e procedure definiscono comportamenti attesi e modalità operative per garantire coerenza e gestione efficace.

### Reporting e comunicazione

Il reporting strutturato prepara canali e responsabilità, essenziali per comunicazioni tempestive in caso di incidenti.



## **CAPITOLO 4 – TECNOLOGIA E DIFESA OPERATIVA**

### Misure Tecniche e Organizzative

Le TOMs combinano tecnologia, processi e responsabilità per una difesa operativa efficace e monitorata quotidianamente.

### Architetture Zero Trust e Segmentazione

Zero Trust e segmentazione di rete riducono il rischio sistemico e migliorano la resilienza operativa aziendale.

### Cyber Threat Intelligence e SOC Evoluto

Un SOC evoluto integra tecnologia, persone e processi per migliorare rilevazione e risposta alle minacce.

### Strumenti Open-Source e Soluzioni di Mercato

La scelta di strumenti flessibili e sostenibili unisce opzioni open-source e soluzioni commerciali per la sicurezza.



## **CAPITOLO 5 – SETTORI CRITICI E CASI STUDIO**

### **Energia e infrastrutture critiche**

La cybersecurity in energia e infrastrutture assicura continuità operativa e sicurezza fisica, prevenendo impatti collettivi.

### **Sanità e Pubblica Amministrazione**

Protezione dati sensibili e continuità di servizi in sanità e PA locale sono fondamentali per la sicurezza delle persone.

### **Industria manifatturiera e supply chain**

La sicurezza della supply chain coinvolge fornitori e logistica, moltiplicando i rischi e richiedendo governance robusta.

### **Servizi finanziari e digitali**

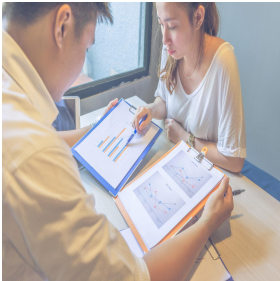
I servizi finanziari richiedono controlli rigorosi, antifrode e gestione efficiente degli incidenti per proteggere le transazioni.

# CAPITOLO 6 – PERSONE E CULTURA DELLA SICUREZZA



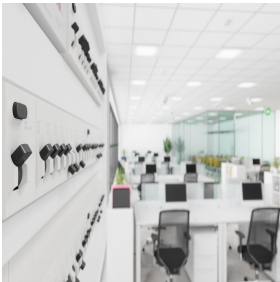
## Formazione continua e sensibilizzazione

La formazione deve essere continua, adattata ai ruoli e mirata a ridurre errori e riconoscere minacce come il phishing.



## Ruolo delle metacompetenze

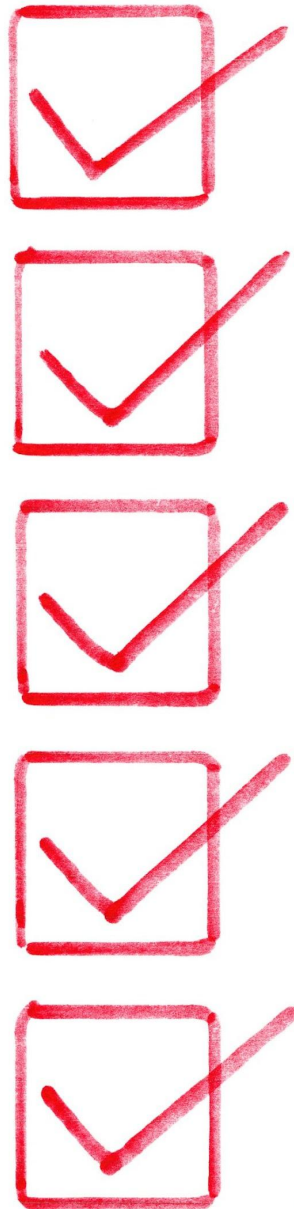
Le competenze trasversali come pensiero critico e gestione del cambiamento sono essenziali per la sicurezza digitale efficace.



## Gestione del fattore umano e insider threats

È fondamentale bilanciare controlli di accesso e monitoraggio per prevenire minacce interne involontarie o malevoli.

# CAPITOLO 7 – CHECKLIST E TOOLKIT OPERATIVI



## Checklist di conformità normativa

Le checklist facilitano la verifica degli obblighi NIS2, CRA e AI Act, supportando audit e controlli tracciabili.

## Template e modelli di policy

Template standardizzati riducono tempi e incoerenze, facilitando un linguaggio comune e aggiornamenti rapidi.

## Strumenti gratuiti e risorse

Accesso a tool e risorse gratuite aiuta organizzazioni a costruire maturità sostenibile e integrare soluzioni di mercato.

## Benefici trasversali del toolkit

Il toolkit accelera il time-to-compliance, riduce dipendenze e favorisce collaborazione tra funzioni aziendali.



## **CAPITOLO 8 – FUTURO DELLA CYBERSECURITY**

### Quantum computing e crittografia

Il quantum computing richiede aggiornamenti crittografici per proteggere dati sensibili a lungo termine.

### Impatto AI generativa

L'AI genera automazione ma può amplificare attacchi, richiedendo controlli e governance adeguati.

### Scenari geopolitici e cyberwarfare

La cybersecurity è influenzata da tensioni geopolitiche, richiedendo attenzione alla resilienza e collaborazione.

### Raccomandazioni strategiche

Strategie per governance, assessment, capacità operative e monitoraggio continuo della cybersecurity.