ACCREDIA
ENTE ITALIANO DI ACCREDITAMENTO

Con il patrocinio di

UNI
UN MONDO FATTO BENE

Convegno

Convegno annuale del **Dipartimento Certificazione e Ispezione 2026**

17/18/19 marzo 2026

Dall’AI alla Cybersecurity: standards, accreditamenti e certificazioni per un approccio affidabile e responsabile

Tavola rotonda

18/03/2026

Lo stato dell’arte

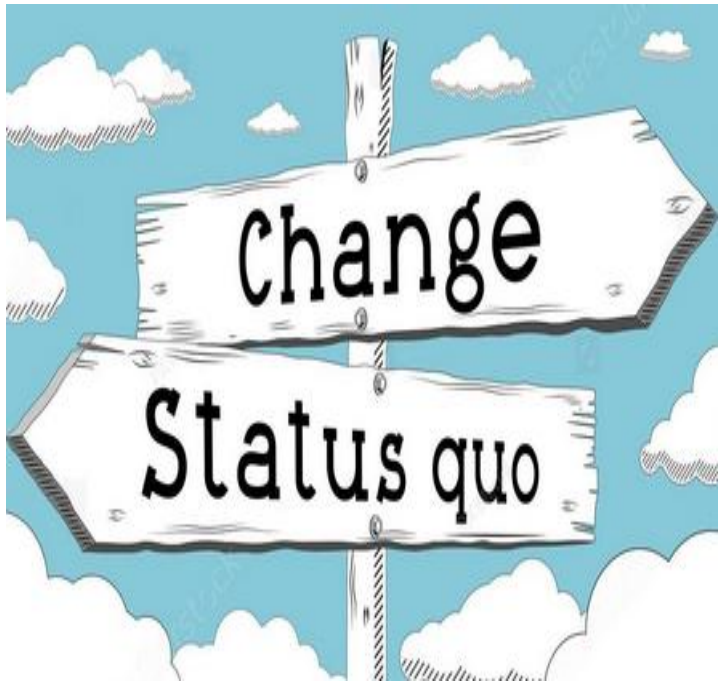
Perimetro normativo

Ad oggi l’UE si è dotata di un mosaico regolatorio su sicurezza, resilienza digitale e fiducia nei sistemi ICT

- CSA
- NIS2
- DORA
- CRA
- AI Act

Obiettivi comuni:

1. **Sicurezza, resilienza e fiducia**
2. **Approccio *risk-based* e proporzionalità**
3. **Governance, Autorità e supervisione**
4. **Valutazione di conformità e standard**
5. ***Supply chain* e *value chain***
6. **Diritti fondamentali e consumatori**



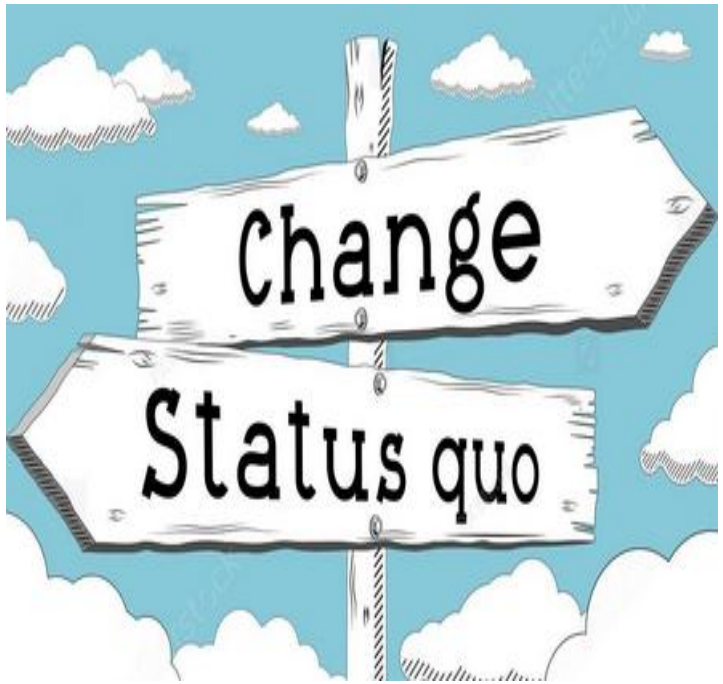
ACCREDIA
ENTE ITALIANO DI ACCREDITAMENTO

Lo stato dell’arte

Il ruolo della Valutazione della conformità

Operativamente la valutazione della conformità può avere almeno quattro funzioni:

1. **Prevenzione**, attraverso controlli esterni e la creazione di consapevolezza nelle Organizzazioni.
2. **Riduzione del rischio**, perché obbliga a trattare cybersecurity e robustezza come requisiti da progettare, validare e testare.
3. **Fiducia**, perché consente dichiarazioni di conformità, marcatura CE e maggiore leggibilità per clienti, partner e autorità.
4. **Interoperabilità**, ENISA evidenzia che AI Act e Cybersecurity Act dovrebbero funzionare in armonia per evitare duplicazioni e rendere più coerente il sistema di assurance



ACCREDIA
ENTE ITALIANO DI ACCREDITAMENTO

Lo stato dell’arte

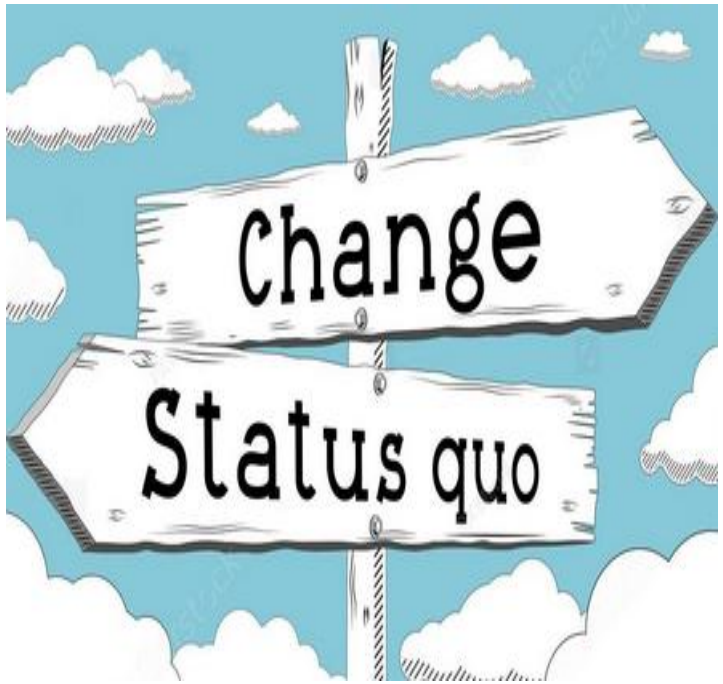
Minacce cyber abilitate dall’AI

Minacce Attuali (ACN 2023-2024)

- Incremento significativo: attacchi DDoS e ransomware verso PA centrale, trasporti, servizi finanziari
- Numeri CSIRT Italia 2023: 1.400+ eventi cyber, 300+ incidenti
- Trend 2024: ulteriore crescita segnalata (2000+ eventi, 570+ incidenti)

Minacce Emergenti

- Intelligenza artificiale applicata in chiave offensiva
- Frammentazione delle famiglie ransomware
- Hacktivismo mirato a infrastrutture critiche
- Deepfake e phishing potenziato dall’AI



ACCREDIA
ENTE ITALIANO DI ACCREDITAMENTO

Lo stato dell’arte

Scadenze

NIS2	• Dal 1° gennaio 2026 sono decorsi gli obblighi di notifica degli incidenti significativi. • Entro il 31 ottobre 2026: implementazione delle misure di sicurezza di base, secondo la prassi operativa richiamata nelle linee guide ACN.
CRA	• Dal 11 giugno 2026 si applica il quadro sulla notifica degli organismi di valutazione della conformità. • Dal 11 settembre 2026 si applicano gli obblighi di segnalazione di vulnerabilità attivamente sfruttate e incidenti gravi. Piena applicazione dal 11 dicembre 2027.
AI Act	• 2 agosto 2026: entra in applicazione la maggior parte delle norme, inclusi i sistemi ad alto rischio Allegato III • 2 agosto 2027: si applicano le norme per l’IA ad alto rischio Allegato I. *In attesa di approvazione Omnibus*

Il caso di Martha Root

L’attacco in diretta durante il Chaos Communication Congress ad Amburgo del 29.12.2025

Combinando l’uso di chatbot AI realistici, l’analisi automatizzata delle conversazioni, web scraping e metodi OSINT Martha ha cancellato **3 siti web estremisti** il tutto in diretta e in piena condivisione dello schermo

L'operazione ha incluso la modifica delle password admin, l'eliminazione dei server e l'estrazione di circa **8.000 profili utente e 100 GB di dati**. I comandi Python eseguiti live sullo schermo hanno suscitato applausi entusiastici dal pubblico

- *La legittimità morale di un’azione coincide mai con la sua liceità?*
- *Se un’infrastruttura digitale ospita odio o minacce, chi ha il diritto di fermarla?*

Fonte: Cybernews.com

Panel

Massimo De Felice
Presidente ACCREDIA

Andrea Billet
Direttore Centrale del Servizio Certificazione e Vigilanza ACN

Giovanni Melardi
Responsabile sistemi di gestione AgID

Alessandro Armando
Direttore Cybersecurity National Lab

Daniele Nardi
Membro Comitato di gestione Laboratorio Nazionale di Artificial Intelligence and Intelligent Systems

Ruggero Lensi
Direttore Generale UNI

Antonio Romeo
Dirigente Area Innovazione e Digitale Unioncamere

ACCREDIA
ENTE ITALIANO DI ACCREDITAMENTO

Con il patrocinio di

UNI
UN MONDO FATTO BENE

Grazie per aver partecipato!