CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

CYBER FACTORY 4.0

1-15
MARZO
2026

IN EVIDENZA

ANSA, 11 MARZO 2026

In Italia il 9,6% dei cyber attacchi mondiali, IA moltiplicatore di rischio

L'Italia si conferma un bersaglio del cyber crimine: nel 2025 si è verificato il 9,6% degli incidenti mondiali, in aumento del 42% sul 2024. Sono i dati del Rapporto Clusit 2026. Il 28% degli incidenti ha colpito il settore governativo-militare-forze dell'ordine, in crescita in valore assoluto del 290% rispetto al 2024.

LEGGI TUTTO

CYBER 4.0

CYBER 4.0, 12 MARZO 2026

Affrontare le sfide della cybersecurity: nel 2026 tornano i seminari promossi dal MIMIT e Cyber 4.0

Il Centro di Competenza Cyber 4.0, in collaborazione con il Ministero delle Imprese e del Made in Italy e con la Scuola Superiore di Specializzazione in Telecomunicazioni, promuove anche per il 2026 un ciclo di seminari in modalità webinar dedicato all'aggiornamento professionale sui temi della sicurezza informatica. Rivolto a lavoratori del settore pubblico e privato, il percorso formativo si articola in sei appuntamenti distribuiti nel corso dell'anno, ciascuno dedicato a un ambito strategico della trasformazione digitale.

LEGGI TUTTO

CYBER 4.0, 12 MARZO 2026

Progetto ESII – AI a supporto dei team SOC nell'investigazione degli incidenti

La crescente complessità degli ambienti digitali rende la gestione degli incidenti di sicurezza un'attività sempre più critica per i SOC, chiamati a interpretare grandi volumi di alert e a individuare rapidamente anomalie e correlazioni significative. In questo contesto nasce ESII (Early Security Incident Investigation), un progetto cofinanziato da Cyber 4.0 nell'ambito delle proprie attività di promozione dell'innovazione e di trasferimento tecnologico.

LEGGI TUTTO

IN ITALIA

ACN, 10 MARZO 2026

La cybersicurezza nelle politiche dell'UE: in ACN la relazione di Roberto Viola

Si è tenuta il 9 marzo 2026, presso la sede dell'Agenzia per la cybersicurezza nazionale (ACN), la riunione del Nucleo per la cybersicurezza (NCS), presieduta da Bruno Frattasi, Direttore generale dell'Agenzia per la cybersicurezza nazionale, con la partecipazione di Roberto Viola, Direttore generale della DG CONNECT (Direzione Generale per le Reti di Comunicazione, i Contenuti e le Tecnologie) della Commissione Europea.

LEGGI TUTTO

TORINO CLICK, 12 MARZO 2026

Torino, l'AI Hub accelera la collaborazione tra Africa ed Europa sull'intelligenza artificiale

Torino è stata oggi il palcoscenico di un importante evento internazionale dedicato all'innovazione e alla cooperazione nel campo dell'intelligenza artificiale tra Africa ed Europa. L'iniziativa, intitolata "Shaping AI Futures Across Africa and Europe", ha riunito innovatori africani dell'AI, leader industriali italiani ed europei e rappresentanti istituzionali, con l'obiettivo di costruire nuove partnership per lo sviluppo sostenibile delle tecnologie digitali.

LEGGI TUTTO

ACN, 3 MARZO 2026

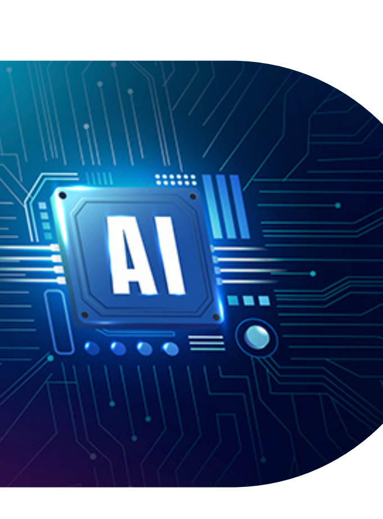
Buone pratiche di cybersicurezza: il vademecum per i dipendenti della PA - on line il nuovo programma

L'offerta formativa di Syllabus si arricchisce di un nuovo percorso formativo afferente all'ambito tematico Transizione digitale, dal titolo "Buone pratiche di cybersicurezza: il vademecum per i dipendenti della PA". Sviluppato dal Dipartimento della funzione pubblica – DFP in collaborazione con l'Agenzia per la Cybersicurezza Nazionale - ACN, il programma mira a elevare il livello di sicurezza digitale della Pubblica Amministrazione, accrescendo la consapevolezza del personale attraverso 12 indicazioni pratiche, semplici e concrete contenute in un Vademecum curato dall'ACN e dal DFP. La comprensione di queste buone pratiche di cybersecurity non è solo un dovere tecnico-procedurale per tutti i dipendenti pubblici, ma un'esigenza strategica per la gestione proattiva delle sfide digitali.

LEGGI TUTTO

AGID, 12 MARZO 2026

Linee guida su IA nella PA: al via la consultazione pubblica su sviluppo e procurement



Da oggi e fino all'11 aprile sono in consultazione pubblica le "Linee Guida per lo sviluppo di sistemi di Intelligenza Artificiale nella pubblica amministrazione" e le "Linee Guida per il procurement di IA nella Pubblica Amministrazione" adottate con la Determinazione n.43/2026. Previste dal Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026, le linee guida di AgID per l'acquisto e lo sviluppo di sistemi di IA nella pubblica amministrazione sono emanate seguendo l'iter previsto all'articolo 71 del Codice dell'Amministrazione Digitale (CAD).

LEGGI TUTTO

CYBERSECURITY ITALIA, 25 FEBBRAIO 2026

Roma Capitale, inaugurata la nuova sala operativa per la sicurezza cyber. Gualtieri: "Le minacce crescono ma lavorando in sinergia si possono contrastare tutte"

"Lavoriamo sin dal primo anno della nostra amministrazione sulla sicurezza cyber dei cittadini di Roma, fino alla realizzazione di questa sala, che lavora in stretta collaborazione con l'ACN". Così il Sindaco Roberto Gualtieri che ha presenziato all'inaugurazione della sala operativa del Cyber Security Operations Center (CSOC) presso la sede della Città metropolitana di Roma Capitale. "La sala", ha aggiunto Gualtieri, "consentirà di rendere davvero sicure le comunicazioni di tutti i dipendenti. Senza tralasciare, allo stesso tempo, anche i servizi per i cittadini. Si tratta di un'infrastrutturale strategica di sicurezza fondamentale per la vita di Roma".

LEGGI TUTTO

NEWS INTERNAZIONALI

ICT SECURITY MAGAZINE, 12 MARZO 2026

Cyber Proxies: capacità cibernetiche degli attori non statali filo-iraniani

Gli attori non statali filo-iraniani sfruttano i cyber proxies come strumenti strategici per proiettare potere, condurre operazioni cibernetiche e perseguire obiettivi politici regionali. Questo testo inaugura una serie di approfondimenti sul tema Cyber Proxies. Capacità Cibernetiche degli Attori Non Statali Filo-Iraniani, analizzando come l'Iran coordini reti di proxy, dall'organizzazione di Hezbollah e Hamas fino alle unità cyber dedicate, per espandere la propria influenza e influenzare dinamiche geopolitiche complesse. La lettura offre un quadro chiaro e dettagliato delle infrastrutture, delle strategie operative e delle metodologie impiegate, introducendo i lettori al mondo dei cyber proxies filo-iraniani.

LEGGI TUTTO

INTERFACE, MARCH 6, 2026

The UN's New Global Mechanism on Cybersecurity, March 2026

March 2026 will mark a milestone for international cybersecurity policy: all 193 UN Member States will convene in New York to launch the UN's first permanent Global Mechanism. Agreed at the final session of the second UN Open-ended Working Group (OEWG) in July 2025, the Global Mechanism on Developments in the Field of ICTs in the Context of International Security and Advancing Responsible State Behaviour in the Use of ICTs (Global Mechanism) will begin its work with an organizational session on March 30-31, 2026.

LEGGI TUTTO

AP NEWS, MARCH 3, 2026

Iranian strikes on Amazon data centers highlight industry's vulnerability to physical disasters

Damage to three Amazon Web Services facilities in the Middle East from Iranian drone strikes highlights the rapid growth of data centers in the region, as well as the industry's vulnerability to conflict. The company's cloud computing division, Amazon Web Services, said late Monday that two data centers in the United Arab Emirates were "directly struck" and another facility in Bahrain was also damaged after a drone landed nearby.

LEGGI TUTTO

ECCC, MARCH 13, 2026

New ECCC call for proposals under the Horizon Europe Programme is open for applications

The call for proposals from Horizon Europe - Work Programme 2026-2027 Civil Security for Society (HORIZON-CL3-2026-02-CS-ECCC - Cybersecurity) implemented by the ECCC covers the following topics:
Approaches and tools for security in software and hardware development and assessment (HORIZON-CL3-2026-02-CS-ECCC-01, EUR 20 million). This topic aims to develop innovative tools, methods, and processes to secure the entire ecosystem of software and hardware development.

LEGGI TUTTO

EUROPOL, MARCH 4, 2026

Major data leak forum dismantled in global action against cybercrime forum

A major online forum for stolen data has been dismantled following an international operation coordinated by Europol.
The forum, known as LeakBase, had established itself as a central hub in the cybercrime ecosystem, specialising in the trade of leaked databases and so-called "stealer logs" – archives of stolen credentials harvested through infostealer malware. Accessible on the open web and operating in English, the platform combined elements of a forum and discussion board, enabling cybercriminals to buy, sell and exchange compromised data.

LEGGI TUTTO

CARNEGIE EUROPE, MARCH 10, 2026

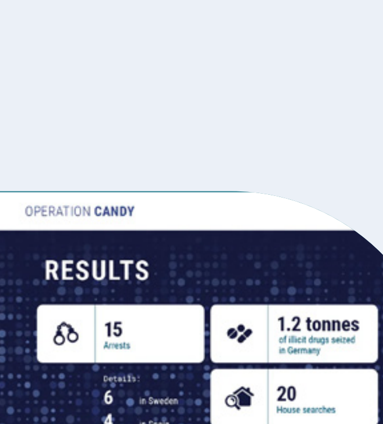
Resetting Cyber Relations with the United States

For more than two decades, successive U.S. administrations treated the UN as a necessary—if imperfect—venue for shaping global expectations of state behavior in cyberspace. The United States was a principal architect of the UN cyber framework, supporting the applicability of international law to cyberspace, articulating confidence-building measures, and defending multistakeholder engagement. Historically, U.S. international engagement in various cyber processes was driven by a strategic logic that combined normative leadership with institutional investment. In the past decade, Washington was instrumental in establishing the Global Forum on Cyber Expertise (GFCE), setting up the International Counter Ransomware Initiative (CRI), and promoting the Budapest Convention on Cybercrime. However, this posture has become increasingly unsettled since U.S. President Donald Trump's return to power. The 2025 U.S. National Security Strategy reflects a more instrumental view of multilateral institutions, including the UN. Engagement is no longer justified primarily by long-term order-shaping considerations and alliances but by short-term strategic return, cost efficiency, and perceived alignment with the administration's worldviews and narrowly defined national interests.

LEGGI TUTTO

EUROPOL, MARCH 6 2026

From a small Swedish town to a global crime network: international operation strikes top-tier organised crime



The seizure of two mobile phones in a small Swedish town exposed a resilient criminal architecture stretching across Europe, Asia and Australia. On 4 March, coordinated actions in Spain, Sweden and Thailand struck key nodes of this network, building on earlier operational activity in Australia.

LEGGI TUTTO

REUTERS, MARCH 11, 2026

Exclusive: Foreign hacker in 2023 compromised Epstein files held by FBI, source and documents show

A foreign hacker compromised files relating to the FBI's investigation of the late sex offender Jeffrey Epstein during a break-in at the bureau's New York Field Office three years ago, according to a source familiar with the matter and recently published Justice Department documents reviewed by Reuters.
The details of who accessed a server at the FBI's New York Field Office, including the allegation that a foreign hacker was involved, are being reported here for the first time.

LEGGI TUTTO

DARK READING, MARCH 6, 2026

North Korean APTs Use AI to Enhance IT Worker Scams

While threat actors across the board struggle to meaningfully upgrade their cyberattacks with artificial intelligence (AI), North Korean threat actors are making more practical use of the same technology to perpetuate their classic IT worker scams.
In a new report, Microsoft's threat intelligence team described how two clusters of malicious actors tied to the Democratic People's Republic of Korea (DPRK) — "Jasper Sleet" and "Coral Sleet" — use AI in a variety of ways to improve the scale and precision of their fraudulent campaigns, enabling "sustained, large-scale misuse of legitimate access" to organizations that don't know better.

LEGGI TUTTO

LAC4, MARCH 13, 2026

Strengthening Cyber Space in Latin America and the Caribbean with the EU CyberNet Cyber Hygiene Platform

As part of LAC4's ongoing commitment to the digital transformation of Latin America and the Caribbean, the LAC4 together with EU CyberNet project expands the EU CyberNet Cyber Hygiene Platform to Guatemala and makes it readily available to all LAC4 members to improve cyber capabilities across all government officials and organisations.

LEGGI TUTTO

Nuove Pubblicazioni

Sistema di Informazione per la Sicurezza della Repubblica, Relazione annuale Intelligence 2026, 2 marzo 2026

Whitehouse, President Trump's Cyber Strategy for America, March 6, 2026

Rusi, Brief, Bold and Beautiful? Reactions on the US National Cyber Strategy, March 16,2026

CISA, Known Exploited Vulnerabilities Catalog, March 2026

Eventi

UNISA, Salerno Winter School on Internet Governance, 23-27 marzo 2026, Salerno.

MIMIT, SSSCLT e Cyber 4.0, "Data power: governance, sicurezza e difesa della proprietà intellettuale", aprile 2026, webinar online.

Cybercrime Conference, 6 -7 Maggio 2026, Auditorium della Tecnica, Roma

Forum Cyber 4.0, 3-4 Giugno 2026, The Dome Luiss, Roma

Cyber FACTory 4.0 è una newsletter con cadenza bisettimanale.
Le notizie sono selezionate per attinenza alle attuali aree di interesse di Cyber 4.0 e non rappresentano posizioni ufficiali del Centro di Competenza.
Ricevi questo contenuto in quanto hai preso parte alle attività del Centro.
Per ulteriori informazioni, contributi, iscrizioni o rimozioni da questa lista di distribuzione, contattare: **comunicazione@cyber40.it**

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER