ITHUM
it's for human

21 febbraio 2024 - Ore 17:00

INNOVAZIONE RESPONSABILE:

L'IA al Crocevia di Cybersecurity, Sostenibilità e Resilienza

Relatore:
Fabrizio CIRILLI
InfoSec e CybersSec Advisor

Agenda

- 17.00: Presentazione
- 17.10: Speech
- 17.45: Corso qualifica
- 17.50 Dibattito - Q&A
- 18:15 (circa): Saluti

Relatore: Fabrizio CIRILLI

Moderatore: Marco CIAMPI

Scrivere a eventi@ithum.it per:
- Attestato di partecipazione finale
- Slide
- Registrazione
- Info corso

ITHUM
it's for human

Innovare responsabilmente in un quadro normativo in continua evoluzione, non perdendo di vista la resilienza e la cybersecurity, garantendo la sostenibilità delle soluzioni

Innovazione e sostenibilità: un ossimoro?

Innovare è un must

Assicurare la sostenibilità delle scelte è una necessità

Come conciliarle con Resilienza e Cybersecurity?

Utilizzando un set di norme ISO costruite per armonizzare e integrare questi temi

ITHUM
it's for human

Il quadro normativo

Il quadro normativo

Regolamenti e direttive EU

- NIS2
- DORA
- Cyber Resilience Act
- Impronta ambientale dei big data
- AI Act
- Mercati digitali
- Rischi criptovalute
- European Chip Act
- …
- https://www.europarl.europa.eu/news/it/headlines/security/20221103STO48002/criminalita-informatica-nuove-misure-dell-ue-per-rafforzare-la-cibersicurezza

In sintesi, potremmo dire che andiamo verso una ***sicurezza sostenibile*** delle persone, delle infrastrutture, dei dati

ENISA e l'IA

PUBLICATION

Cybersecurity and privacy in AI - Forecasting demand on electricity grids

This report allows better assessment of the reality that artificial intelligence brings its own set of threats, which consequently insists on the search for new security measures to counter them. Finally, it should be noted that this guide strongly emphasises privacy issues in the same way as cybersecurity issues, privacy being one of the most important challenges facing society today. Security and privacy are intimately related, but both equally important, and a balance must be made specific to each use. As a result, as seen in this report, efforts to optimise security and privacy can often come at the expense of system performance.

Published on Jun 7, 2023

PRESS RELEASE

EU Elections at Risk with Rise of AI-Enabled Information Manipulation

The 11th edition of the Threat Landscape of the European Union Agency for Cybersecurity (ENISA) highlights the disruptive impacts of AI chatbots and AI-enabled manipulation of information.

Published on Oct 19, 2023

PUBLICATION

Cybersecurity of AI and Standardisation

The overall objective of the present document is to provide an overview of standards (existing, being drafted, under consideration and planned) related to the cybersecurity of artificial intelligence (AI), assess their coverage and identify gaps in standardisation. It does so by considering the specificities of AI, and in particular machine learning, and by adopting a broad view of cybersecurity, encompassing both the 'traditional' confidentiality–integrity–availability paradigm and the broader concept of AI trustworthiness. Finally, the report examines how standardisation can support the implementation of the cybersecurity aspects embedded in the proposed EU regulation laying down harmonised rules on artificial intelligence (COM(2021) 206 final) (draft AI Act).

Published on Mar 14, 2023

PUBLICATION

Cybersecurity and privacy in AI - Medical imaging diagnosis

This report allows better assessment of the reality that artificial intelligence brings its own set of threats, which consequently insists on the search for new security measures to counter them. Finally, it should be noted that this guide strongly emphasises privacy issues in the same way as cybersecurity issues, privacy being one of the most important challenges facing society today. Security and privacy are intimately related, but both equally important, and a balance must be made specific to each use. As a result, as seen in this report, efforts to optimise security and privacy can often come at the expense of system performance.

Published on Jun 7, 2023

PUBLICATION

Multilayer Framework for Good Cybersecurity Practices for AI

In this report, we present a scalable framework to guide NCAs and AI stakeholders on the steps they need to follow to secure their AI systems, operations and processes by using existing knowledge and best practices and identifying missing elements. The framework consists of three layers (cybersecurity foundations, AI-specific cybersecurity and sector-specific cybersecurity for AI) and aims to provide a step-by-step approach on following good cybersecurity practices in order to build trustworthiness in their AI activities.

Published on Jun 7, 2023

PUBLICATION

Artificial Intelligence and Cybersecurity Research

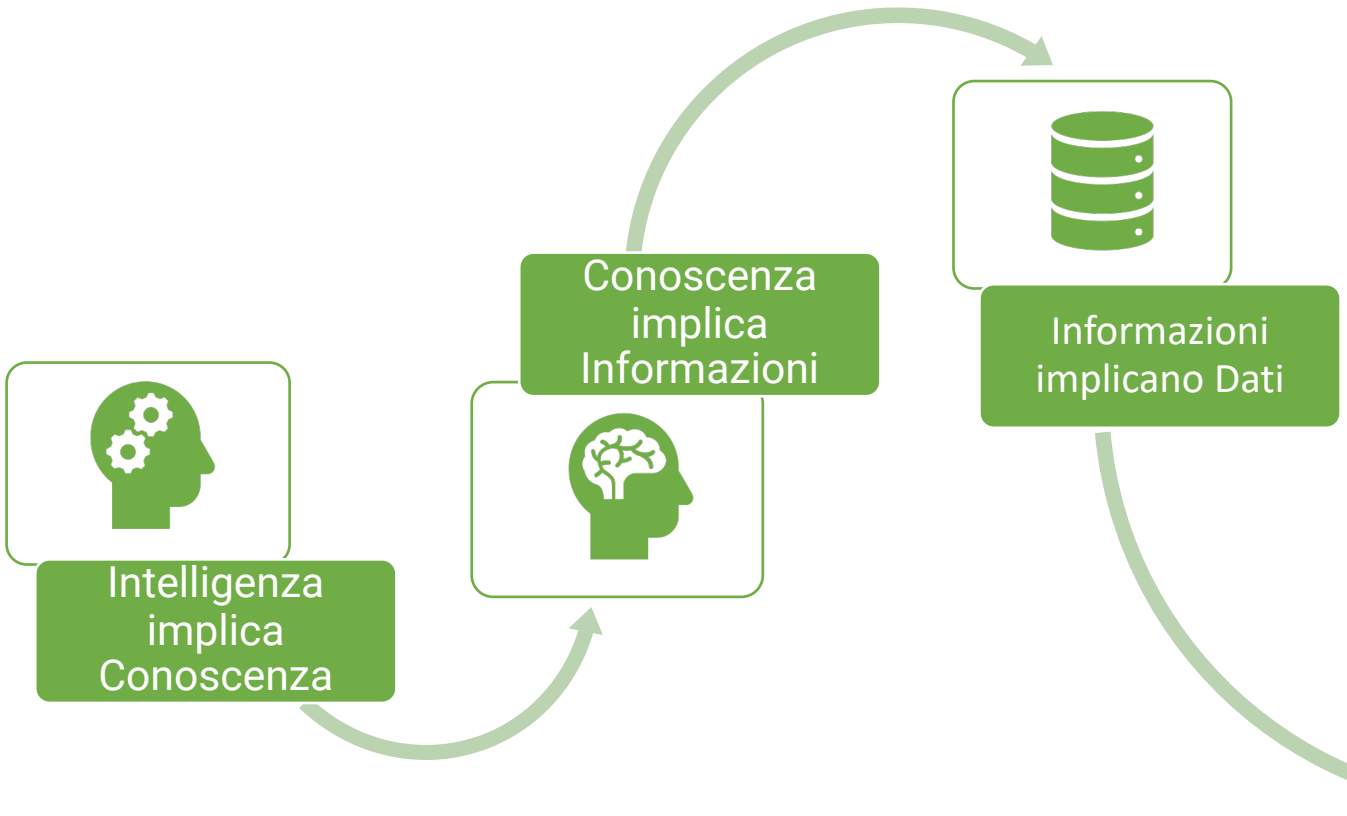
The aim of this study is to identify needs for research on AI for cybersecurity and on securing AI, as part of ENISA's work in fulfilling its mandate under Article 11 of the Cybersecurity Act . This report is one of the outputs of this task. In it we present the results of the work carried out in 2021 and subsequently validated in 2022 and 2023 with stakeholders, experts and community members such as the ENISA AHWG on Artificial Intelligence . ENISA will make its contribution through the identification of five key research needs that will be shared and discussed with stakeholders as proposals for future policy and funding initiatives at the level of the EU and Member States.

Published on Jun 7, 2023

ITHUM
it's for human

L'innovazione sostenibile

La conoscenza come strumento di cambiamento e innovazione



Andiamo quindi verso uno Strategic Intelligence Management (ISO 56006:2021)

- identificare nuove opportunità di business e alleanze
- aumento del vantaggio competitivo
- anticipare rischi e incertezze
- consentire opportunità di trasferimento tecnologico
- prevedere i fattori trainanti sociali, politici, tecnologici e commerciali
- ricercare segnali deboli per anticipare il cambiamento
- superare le barriere che limitano la creazione di valore
- attuare un approccio strutturato alla risoluzione dei problemi.

Conoscenza e sicurezza dei dati

Fondamentale è la **conoscenza che deriva dalle informazioni** (da *proteggere come patrimonio*) costituite di dati (che devono essere *affidabili*)

- Costruire dataset affidabili
- Proteggere le informazioni (dati e programmi)
- Costruire le conoscenze necessarie (umane e dell'AI)

In questo scenario la disponibilità dei dati è quasi scontata, **la sicurezza si sposta verso la cybersecurity e nuove caratteristiche** dei dati:

- Riservatezza
- Integrità
- Non ripudio
- Accountability
- Autenticità
- Intervenibilità (capacità di intervenire, per evitare che un sistema di intelligenza artificiale arrechi danni o generi pericoli)

L'attenzione ai Bias e alla correttezza è molto alta nell'ambito dell'IA, tanto da aver prodotto standard appositi:

- ISO/IEC TR 24027:2021 — Bias in AI systems and AI aided decision making
- ISO/IEC TR 24028:2020 - Panoramica sull'affidabilità nell'intelligenza artificiale

ITHUM
it's for human

Intelligenza Artificiale

IA affidabili

L’affidabilità ricopre un ruolo fondamentale ed è basata su:

- **Robustezza**, capacità di mantenere il livello di prestazioni, come previsto dagli sviluppatori, in qualsiasi circostanza
- **Affidabilità**, capacità di un sistema o di un'entità al suo interno di svolgere le funzioni richieste alle condizioni stabilite per un determinato periodo di tempo
- **Resilienza**, capacità del sistema di ripristinare rapidamente le condizioni operative a seguito di un incidente
- **Controllabilità**, proprietà di un sistema di IA, significa che un agente esterno possa intervenire nel suo funzionamento
- **Spiegabilità**, proprietà di un sistema di IA, significa che i fattori importanti che influenzano una decisione possono essere espressi in un modo comprensibile per gli esseri umani
- **Prevedibilità**, proprietà di un sistema di IA, significa che consente ipotesi affidabili da parte delle parti interessate
- **Trasparenza**, supporta gli obiettivi del sistema incentrati sull’uomo ed è un argomento di ricerca e discussione continua
- **Bias e correttezza**, è ciò che consente ai sistemi di machine learning di giudicare che una situazione è diversa da un’altra e di comportarsi diversamente di conseguenza. In quanto tale, il pregiudizio (bias) è fondamentale per il processo di apprendimento automatico e per adattare il comportamento alla particolare situazione in questione

I principi dell'IA

Etica: l'IA deve essere sviluppata e utilizzata in modo etico, rispettando i diritti umani e le libertà fondamentali.

Trasparenza: l'IA deve essere trasparente e comprensibile, in modo che gli utenti possano comprenderne i meccanismi e le implicazioni.

Responsabilità: l'IA deve essere responsabile, in modo che gli sviluppatori e gli utenti possano essere ritenuti responsabili delle sue azioni.

Qualità: l'IA deve essere di alta qualità, in modo da soddisfare i requisiti degli utenti e ridurre al minimo i rischi.

Continuo miglioramento: l'IA deve essere in continuo miglioramento, in modo da poter affrontare le sfide emergenti e migliorare le sue prestazioni.

Caratteristiche e particolarità della ISO/IEC 42001

Basata su HLS del 2021

Struttura simile alla ISO/IEC 27001

Climate change

Valutazione impatti

Valutazione e trattamento dei rischi

SoA

2 Annex Normativi (controlli e implementazione dei controlli)

Richiamo a numerosi standard ISO a supporto (di cui almeno 4 necessari per la corretta applicazione della norma) e al documento NIST AI Risk Management Framework

In uscita la ISO/IEC 42006 per gli Organismi di Certificazione impegnati nella certificazione dei Sistemi di Gestione per l'IA

ITHUM
it's for human

Resilienza

Resilienza

La capacità di assorbire e adattarsi a un ambiente mutevole è determinata dalla ***capacità collettiva di anticipare, prepararsi e rispondere alle minacce e opportunità*** per ogni singola componente di un sistema

Le norme e la resilienza

Sebbene esista uno specifico set di norme che trattino la continuità (ISO 22301) e che esista una specifica linea guida sul tema (ISO 22316) oggi associamo la resilienza a scenari legati agli attacchi informatici

Così la resilienza diventa ***la capacità di resistere, rispondere e adattarsi a fronte di una violazione delle informazioni mantenendo la continuità di prodotti/servizi a livelli predefiniti (MBCO), per rientrare in condizioni normali in tempi rapidi (RTO), perdendo la quantità minima di informazioni (RPO) ed evitare il punto di non ritorno (MTPD).***

Ne è la riprova l'uscita quasi simultanea di **DORA** e **NIS2**

Le norme e la resilienza

Interessante notare che la ISO/IEC 27001, sebbene non sia una norma dedicata alla continuità o alla resilienza, ha da sempre come obiettivo:

Ridurre gli impatti, mantenendo la sicurezza delle informazioni, anche in caso di incidenti

È stato quindi facile per il mercato associare il binomio:

Sicurezza delle informazioni (ISO/IEC 27001)

Continuità di prodotti/servizi (ISO 22301)

Le due norme sono profondamente diverse ma possono operare in modo sinergico assicurando un elevato grado di integrazione e resilienza

Nel mondo dei servizi IT

- Nel mondo dei **servizi IT** esiste la ISO/IEC 20000-1 (basata su ITIL) che integra le due parti: sicurezza delle informazioni e continuità dei servizi IT (non sicurezza delle informazioni dell'azienda e continuità dell'azienda!)
- Il settore ICT ha da sempre questa innata capacità e tendenza ad integrare gli elementi

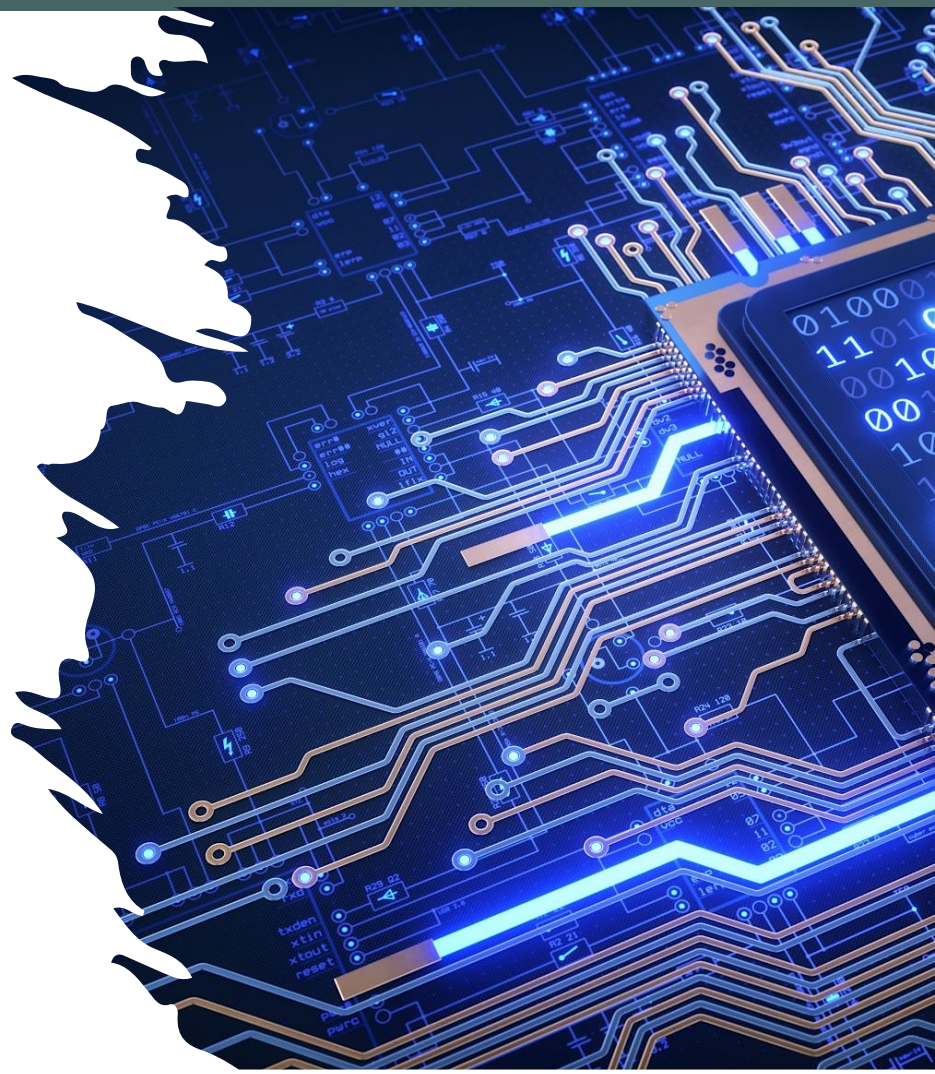
Il quadro delle norme

- In definitiva al momento possiamo sintetizzare il tutto con questo schema:

- Sistemi integrabili, creati per essere integrabili
- *La ISO/IEC 42001 per i sistemi di gestione per l'intelligenza artificiale propone una nuova prospettiva che ben si adatta a quanto stiamo descrivendo*

Una precisazione è d'obbligo

- Sicurezza informatica, sicurezza delle informazioni e cybersecurity NON sono sinonimi:
  - *Sicurezza informatica*, è sicurezza degli apparati, basata su ISO/IEC 15408, certificazioni dai laboratori ACN
  - *Sicurezza delle informazioni*, è sicurezza in termini di riservatezza, integrità e disponibilità dell'informazione, basata su ISO/IEC 27001, certificazione da organismi accreditati
  - *Cybersecurity*, basata su IEC 62443 (ISO/IEC TS 27110), associata a OT e sistemi di produzione, non ancora certificabile, ***salvaguarda le persone, la società, le organizzazioni e le nazioni dai rischi causati dalle cyber minacce che sfruttano l'ambiente digitale interconnesso di reti, servizi, sistemi e processi, mantenendo tali rischi ad un livello tollerabile***
- Talvolta i media creano miscellanee e usi impropri che possono fuorviare le imprese e i consumatori



Integrazione!

In conclusione

IL **CAMBIAMENTO** E LA **RESILIENZA** (INTESA COME CONTINUITÀ NELLA CYBERSECURITY) SI CONFERMANO ELEMENTI ESSENZIALI

LA **CONOSCENZA** MULTIDISCIPLINARE, CONDIVISA, BASATA SU DATI QUALITATIVAMENTE AFFIDABILI (IA) È LA CHIAVE PER L'**INNOVAZIONE** E IL **CAMBIAMENTO**

LE BARRIERE CONCETTUALI, TEORICHE, TECNICHE TENDONO A SGRETOLARSI CON L'USO DELL'IA PERMETTENDO INVECE **INTEGRAZIONI E CRESCITA ESPONENZIALE** GRAZIE ALLE CONOSCENZE

IN TUTTO QUESTO **L'ESSERE UMANO È AL CENTRO** DI TUTTI QUESTI SISTEMI E LA **SUA SALVAGUARDIA** È L'ELEMENTO ESSENZIALE DI CORRELAZIONE INSIEME ALLA **SOSTENIBILITÀ**

Grazie per l'attenzione!

QUESTIONARIO

- **Gradimento**
- **Privacy**
- **Newsletter**

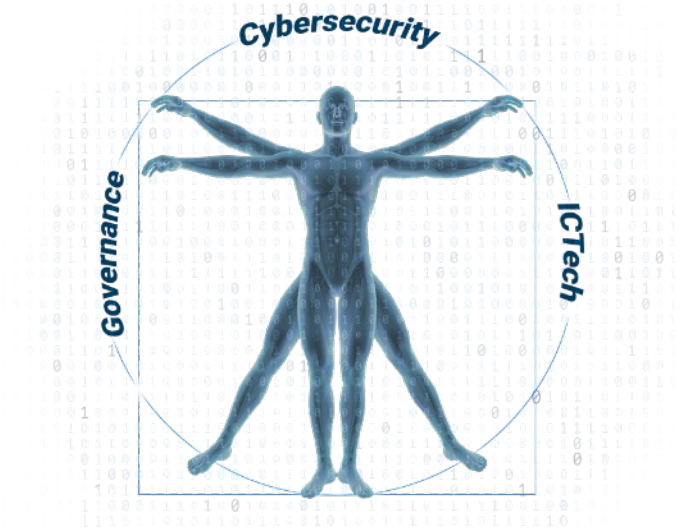
Scrivere a eventi@ithum.it per:

- Attestato partecipazione
- Slide
- Registrazione
- Info corso

ITHUM
it's for human

Founded in **2005**
by ICT professionals

Fields of interest:
Training & **Certifications**
Specialized **Consultancy**



HQ located **in Rome**
Active in Italy & Europe

Collaborative & strategic approach
to build Value

CYBER SECURITY

- IT Security
  - Attacks & Warfare
  - Defence & Analysis
  - Secure Coding
- Governance & Management
- Intelligence & Social
- Investigation & Digital Forensic

GOVERNANCE

- Management Systems ISO
  - Information Security, Business Continuity, Quality, ICT
  - Artificial Intelligence
  - Environment Social Government
- National & International Standards
  - Privacy GDPR
  - ICT Professional Profiles UNI/EN
  - HR Professional Profiles UNI
- Project Management & Framework
- Job Safety & Security
- Management & Soft skills

IT TECHNICIAN

- IT & OS Systems
- Cloud & Virtualization
- Development
- Industry 4.0
- Security DevNet
- DevOps

ithum.it

ITHUM
it's for human

(+39) 06 2158915
(+39) 06 86726329

Via Cristoforo Colombo, 149
00147 Roma (RM) Italy

informazioni@ithum.it

www.ithum.it