compet-e

ITHUM
it's for human

Approved by

ict academy

Giovedì 12 dicembre 2024 - ore 17:00

NATALE CON LA NIS 2

La nuova direttiva europea sulla sicurezza di reti e sistemi informativi

Piermaria SAGLIETTO
Founder & CEO Compet-e

Agenda:

- **17:00** Presentazione
- **17:10** Speech
- **17:45** Feedback / Prossime iniziative
- **17:50** Dibattito - Q&A
- **18:15 (circa)** Saluti

Relatori:

Piermaria SAGLIETTO – (LinkedIn)

Presenta e Modera:

ITHUM

Evento LinkedIn

Know your Speaker

Piermaria SAGLIETTO

Founder & CEO Compet-e

p. saglietto@compet-e.it

LinkedIn: piermaria-saglietto-7130b419/

Network and Information System Security

I soggetti coinvolti - 1/2

SETTORI ALTA CRITICITÀ (Allegato I)

- Settore Energetico: elettrico, oil and gas, riscaldamento, idrogeno
- Settore Trasporti: aereo, nautico, ferroviario e stradale
- Settore Bancario e Finanziario
- Settore Sanitario: assistenza sanitaria, laboratori analisi, produttori di dispositivi medicali, ricerca
- Settore Acqua e acque reflue
- Settore Infrastrutture digitali: gestori di domini, Cloud Computing, distribuzione contenuti, comunicazione
- Gestione dei servizi TIC (business-to-business)
- Pubblica Amministrazione
- Settore Spaziale

ALTRI SETTORI CRITICI (Allegato II)

- Settore Servizi postali e di corriere
- Settore Trattamento dei rifiuti
- Settore Chimico: produzione e distribuzione
- Settore Alimentare: produzione, trasformazione e distribuzione
- Settore Fabbricazione: macchinari in genere, apparecchiature elettriche, elettronica, computer, mezzi di trasporto
- Servizi digitali: social network, motori di ricerca, mercati online
- Ricerca scientifica

I soggetti coinvolti – 2/2

SETTORI DELLA PA (Allegato III)

- Amministrazioni centrali
- Amministrazioni regionali
- Amministrazioni locali (città metropolitane, città >100K ab., capoluoghi regione, ASL)
- Altri settori PA (ex: servizi assistenziali ricreativi culturali, enti di ricerca, etc...)

ULTERIORI SETTORI (Allegato IV)

- Trasporto pubblico locale
- Società in-house, società partecipate e società a controllo pubblico (d.lgs.19 agosto 2016, n. 175).
- Soggetti nel campo di istruzione che operano attività di ricerca
- Etc...

Criteri per comprendere a chi si applica (d.lgs.138/2024)

Per le imprese degli allegati I e II si deve applicare un secondo criterio.

Raccomandazione n. 2003/361/CE.
In base al numero di **dipendenti e al fatturato/volume di affari** si classificano le imprese/enti in:

- **Microimpresa**: <10 dipendenti e fatturato annuo/totale di bilancio < 2 milioni di euro;
- **Piccola impresa**: < 50 dipendenti e fatturato annuo/totale di bilancio <10 milioni di euro;
- **Media impresa**: < 250 dipendenti e fatturato annuo < 50 milioni di euro / totale di bilancio < 43 milioni di euro;
- **Grandi imprese**: la casistica rimanente.

Secondo la normativa europea, il requisito di piccola/media impresa soddisfatto se solo uno dei parametri (dipendenti o fatturato) è oltre la soglia.

Comprendere il criterio dimensionale

Il calcolo numero dei dipendenti e fatturato varia se l'impresa è **autonoma**, **associata** o **collegata con altre imprese**.

Imprese Autonome → <u>non possiede</u> partecipazioni del 25% o più in altre imprese e nessun'altra impresa possiede una quota del 25% o più nella stessa.
In questo caso:

- N° dipendenti: conteggio dei dipendenti diretti
- Fatturato e totale bilancio: dell'impresa stessa (no aggregazioni con altre)

Imprese Associate → possiede partecipazione del 25% o più (ma < 50%) in un'altra impresa o a sua volta posseduta nella stessa misura da un'altra impresa.

- N° dipendenti: dipendenti imprese associate (proporzionale % partecipazione) + dipendenti diretti
- Fatturato e totale bilancio: proporzionale % partecipazione

***Esempio**: Se l'impresa **A** detiene il **30%** dell'impresa **B**, si aggiungerà il **30%** dei **dipendenti**, del fatturato e del totale di bilancio di **B** ai dati di **A**.*

Quando rientra il criterio dimensionale?

Regola generale.
Il 2° criterio applicato ai soggetti dell'Allegato I e Allegato II (art. 3 co. 2 d.lgs.138/2024).
Se si superano i massimali per le piccole imprese → **NIS2**.

Eccezioni.
No criterio dimensionale per:

- Fornitori di reti/servizi comunicazione elettronica al pubblico
- Prestatori servizi fiduciari (ex. firma elettronica)
- Gestori registri nomi di dominio
- Fornitori dei servizi di registrazione nomi di dominio
- Soggetti critici (direttiva CER infrastrutture critiche europee)

Imprese collegate a soggetti NIS2 se (art. 3 co. 10 d.lgs.138/2024):

a) adottano decisioni o influenza dominante su questi in ambito sicurezza informatica;
b) detengono o gestiscono i sistemi informativi di questi;
c) gestiscono sicurezza informatica o servizi TIC di questi

Clausola di salvaguardia

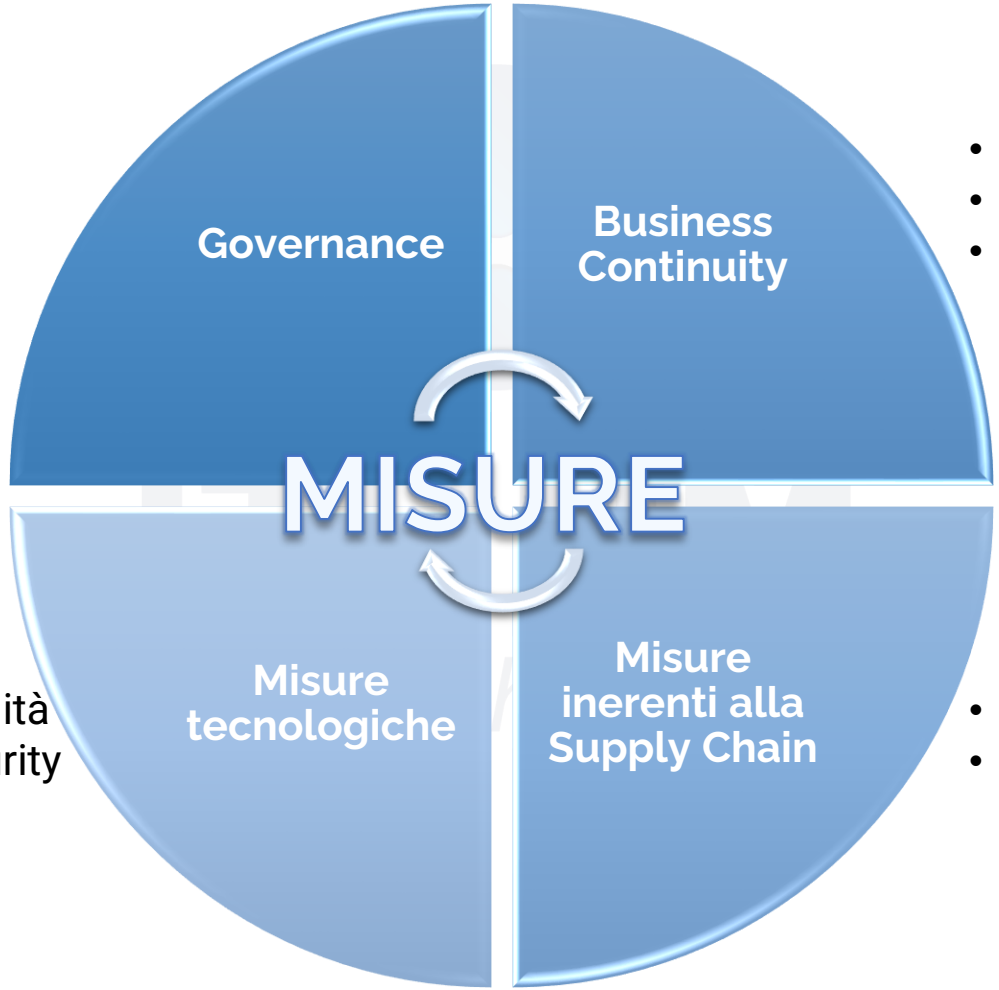
D.lgs. 138/2024, art. 3, co. 4
Soggetto **media o grande impresa** (art.2 dell'allegato Raccomandazione **2003/361/CE): art.6, par. 2** salvo che **ciò non sia proporzionato**, tenuto anche conto **dell'indipendenza del soggetto** dalle sue **imprese collegate** in **termini di sistemi informativi e di rete** che utilizza nella fornitura dei suoi servizi e in termini di servizi che fornisce.

Art. 40, co. 1, lettera a)
ACN propone DPCM con criteri per applicazione clausola salvaguardia (art.3, co. 4)

FAQ 1.6 di ACN
Qualora il **soggetto ritenga che ciò non sia proporzionato** [...] potrà richiedere deroga (NIS, art.3, co. 4)
Esclude: imprese associate o collegate dal calcolo del numero di dipendenti, fatturato e bilancio)
…in presenza di specifici criteri stabiliti dal DPCM su clausola di salvaguardia

Gli adempimenti dei soggetti essenziali e importanti

- Governo dei rischi
- Governo degli incidenti
- Consapevolezza/Formazione



- Backup e ripristino
- Piani di continuità e loro test
- Gestione delle crisi

- Presidio e gestione delle vulnerabilità
- Igiene di base in ambito cybersecurity
- Crittografia e cifratura
- Verifiche, test e audit
- Autenticazione a più fattori

- Gestione dei rapporti con fornitori
- Gestioni dei rischi legati ai fornitori e forniture

Gli adempimenti - focus su art. 24

Policy **analisi dei rischi** e **sicurezza sistemi informativi**

Sistemi **gestione incidenti** Cyber: maggiori obblighi segnalazione

Misure di **Business Continuity**, quali il Backup evoluto, il Disaster Recovery, il **Crisis Management**

Gli obblighi in termini di Cybersecurity coinvolgono tutta la **Supply Chain**, anche i fornitori

Soluzioni di Autenticazione a più Fattori (MFA) o autenticazione continua, comunicazioni vocali, video e testo protette e sistemi di comunicazione emergenziali interni protetti, ove opportuno

La sicurezza acquisizione, sviluppo e manutenzione di reti e sistemi informativi, compresa la gestione e **divulgazione vulnerabilità**

Policy e procedure su uso **crittografia** e/o cifratura crittografica

Policy (anche **Audit e Test)** di valutazione efficacia delle misure di **gestione del rischio Cybersecurity**

Pratiche **igiene informatica di base** [i.e., regole fondamentali per garantire la cybersecurity] e **Formazione su sicurezza informatica**

Misure **sicurezza delle risorse umane, politiche di controllo accessi** e **gestione Asset**

Necessario incorporare misure di **Cybersecurity Risk Management** nei **rapporti contrattuali** con fornitori e *Service provider*

Come prepararsi

Valutazione del Campo di Applicazione

- Determinare se l'organizzazione rientra nel campo di applicazione
- Identificare quali specifiche categorie di entità si applicano (operatori di servizi essenziali, fornitori di servizi digitali…)

Analisi dei Gap

- Effettuare un'analisi dei gap rispetto ai requisiti della NIS2
- Identificare le aree di non conformità
- Definire una strategia di adeguamento

Miglioramento delle Misure di Sicurezza

Implementare o migliorare le misure tecniche e organizzative per proteggere le reti e i sistemi informativi includendo:

- sicurezza informatica
- resilienza fisica
- gestione della sicurezza della supply chain

Come prepararsi

Piani di Risposta agli Incidenti e di Recupero

- Sviluppare/aggiornare piani di risposta incidenti e recupero post attacco informatico
- Regolari esercitazioni di simulazione

Formazione e Consapevolezza

- Formazione e sensibilizzazione
- Aggiornamento del personale

Collaborazione e Condivisione

- Partecipazione iniziative di condivisione informazioni e collaborazione
- Contatti con autorità di regolamentazione e organismi di sicurezza nazionali pertinenti

Monitoraggio Continuo e Valutazione periodica

- Processi di monitoraggio continuo misure di sicurezza e valutazione periodica efficacia delle politiche e delle procedure di sicurezza
- Revisioni, audit interni/esterni di verifica conformità NIS2

“Se ho la 27001 sono a posto per la NIS2?”

NIS2 & ISO 27001 - Punti di contatto e differenze

ISO 27001

- **Obiettivo**: fornire alle organizzazioni guida per proteggere informazioni con approccio sistematico basato sul rischio.
  - ✓ Garantire la riservatezza, l'integrità e la disponibilità delle informazioni;
  - ✓ Migliorare continuamente la sicurezza delle informazioni.

NIS2

- **Obiettivo**: garantire maggiore sicurezza informatica per infrastrutture critiche dell'UE.
  - ✓ Rafforzare la cooperazione tra Stati membri.
  - ✓ Migliorare la resilienza dei servizi essenziali.

Applicabilità

- ISO 27001 è uno standard internazionale applicabile a **qualsiasi organizzazione**.
- NIS2 è una direttiva dell'UE rivolta a **specifici settori.**

Volontarietà

- ISO 27001 è una **certificazione volontaria**, utile per dimostrare l'impegno nella sicurezza informatica.
- NIS2 è **obbligatoria** per le organizzazioni che operano nei settori regolamentati.

Ambito geografico

- ISO 27001 ha **applicazione globale**, senza vincoli geografici.
- NIS2 è **limitata ai paesi dell'Unione Europea**, con focus sulla cooperazione transfrontaliera.

I vantaggi della sinergia

- **Supporto alla conformità**: Le organizzazioni con ISO 27001 facilitano conformità ai requisiti di sicurezza della NIS2, grazie a processi già in atto per gestione rischio.
- **Resilienza rafforzata**: La combinazione di ISO 27001 e dei requisiti di sicurezza operativa NIS2 offre protezione più robusta contro minacce informatiche.
- **Coordinamento efficace**: ISO 27001 come prova concreta dell'efficacia delle misure di sicurezza implementate, semplificando audit e ispezioni imposte da NIS2.

QUINDI

- **ISO 27001 e NIS2 sono strumenti complementari**
- L'integrazione di entrambi gli approcci permette alle organizzazioni di raggiungere un'elevata resilienza informatica e di essere in regola con le normative europee.

Come essere conformi?

Decreto di esecuzione 2024/2690 e Linee Guida Enisa

REGOLAMENTO DI ESECUZIONE (UE) 2024/2690
DELLA COMMISSIONE
del 17 ottobre 2024

recante modalità di applicazione della direttiva (UE) 2022/2555 sui i requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza […]

Pubblicato sulla Gazzetta ufficiale dell'unione Europea

- Requisiti tecnici e metodologici misure per la gestione dei rischi in materia di cyber sicurezza previsti da NIS2;
- Definizione «Incidente *significativo*" secondo NIS2

IMPLEMENTING GUIDANCE

On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures.

Consultazione pubblica aperta da ENISA dal 07/11 al 09/12

Una «declinazione tecnica» del regolamento di esecuzione n°2690/2024 della Commissione NIS2.

- **Indicazioni pratiche su come attuare un requisito** (art. 21 NIS2, da cui art. 24 d.gls.138/2024) o aspetti critici da considerare;
- **Esempi di prove di conformità** utili a dimostrare la conformità norme richieste;
- **Suggerimenti supplementari** su aspetti aggiuntivi da considerare per rafforzare ulteriormente la sicurezza;
- **Mappature con standard internazionali (ISO/IEC e NIST)** e framework nazionali, per facilitare integrazione requisiti.

Timeline – le principali scadenze

Entro il 31 dicembre 2024

Assessment

1 gennaio – 28 febbraio 2025

Registrazione su **piattaforma digitale** (ACN)

31 marzo 2025

Redazione elenco ACN
(soggetti essenziali e soggetti importanti)

1 aprile – 15 aprile 2025

Comunicazione elenco ACN

15 aprile – 31 maggio 2025

I soggetti dovranno **fornire ulteriori informazioni richieste dalla normativa**

Dal 1 gennaio 2026

Adempimento obbligo di notifica degli incidenti

Dal 1 ottobre 2026

Adempimento obblighi:

- organi di amministrazione e direttivi
- in materia di misure di sicurezza
- di raccolta e mantenimento banca dati di registrazione dei nomi di dominio (ove applicabile)

Reg Tech

Governance, Risk & Compliance (GRC)

Con competenze tecnologiche e di dominio funzionale, supportiamo i clienti nell'**affrontare le esigenze settore compliance**.

- **Privacy GDPR** | *Regolamento 2016/679*
- **Sicurezza delle informazioni** | *ISO 27001*
- **NIS2** | *Network & Information System Security*
- **Log & asset management** | *Log degli amministratori di sistema*

- **Responsabilità amministrativa** | *D.lgs 231/2001*
- **Prevenzione della corruzione** | *ISO 37001*
- **Whistleblowing** | *Gestione delle segnalazioni*
- **Sicurezza sul lavoro** | *D.lgs. 81/08*

- **Antiriciclaggio** | *Anti Money-Laundering*
- **DORA** | *Digital Operational Resilience Act*

Software

Piattaforma GRC

GRC CORA è la piattaforma di GRC **sviluppata dal nostro team** per la gestire la compliance in modo *smart*.

Consulenza

normativa

Il nostro team formato da **risorse estremamente specializzate**, con elevata esperienza in materia, costantemente aggiornati e formati per offrire la migliore consulenza.

Formazione

in aula e online

Abbiamo sviluppato diversi **corsi di formazione** che eroghiamo in aula o online, in base alle esigenze di ogni realtà.

GRC CORA

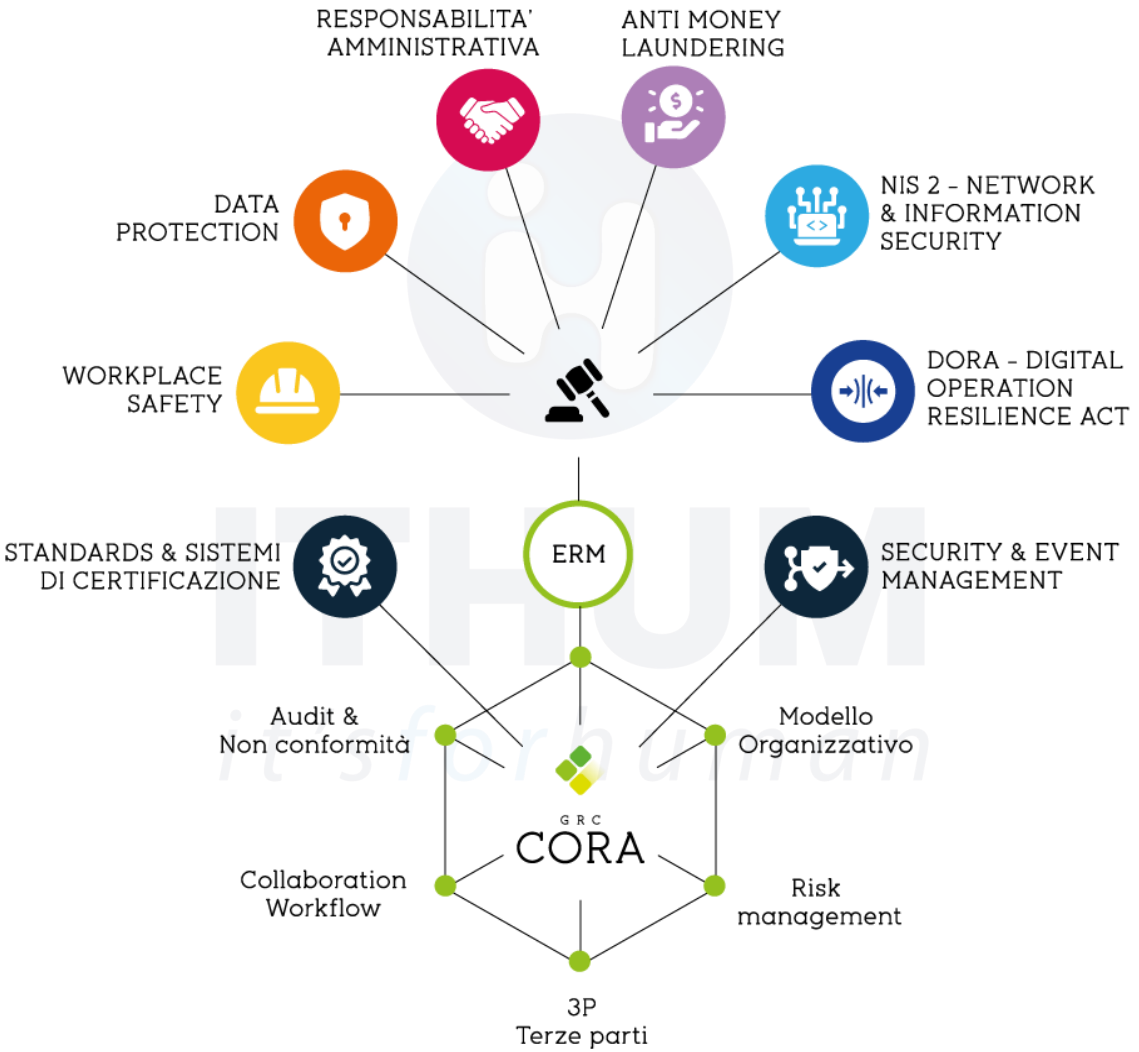
Compliance made **smart**

Dashboard
Analytics & KPI

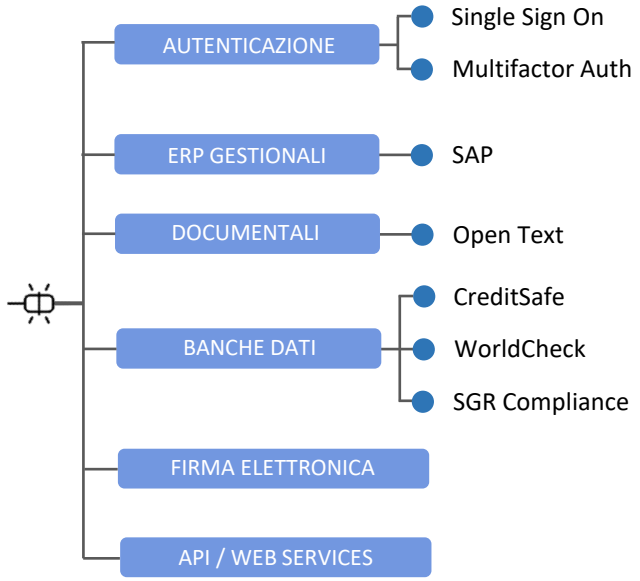
Top
Management

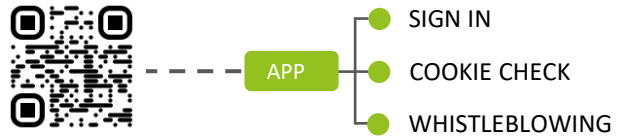
Referenti
di business

Team
di funzione



On premise
SaaS
Cloud Marketplace





Grazie per l'attenzione!

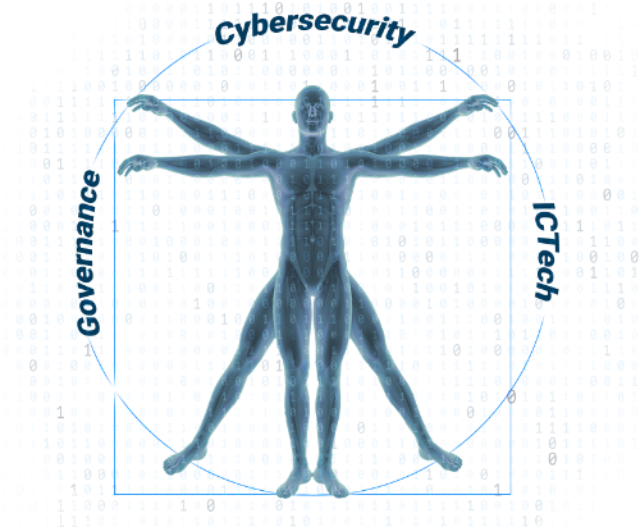
QUESTIONARIO

- ❑ Gradimento
- ❑ Newsletter

Scrivere a eventi@ithum.it per:

- ✓ Attestato di partecipazione
- ✓ Slide proiettate
- ✓ Registrazione
- ✓ Altre informazioni

ITHUM
it's for human



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

Founded in **2005**
by ICT professionals

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

Collaborative & strategic approach
to build Value

Cyber Security

- IT Security
  - Attacks & Warfare
  - Defence & Analysis
  - Secure Coding
  - Operation Technology Security
- Governance & Management
- Intelligence & Social
- Investigation & Forensic
- Regulatory Compliance
- Artificial Intelligence

Governance

- National & International Standards
  - Information Security
  - Artificial Intelligence
  - Business Continuity
  - Quality
  - IT Services
  - Anti-Bribery
  - Environment Social Government
  - Privacy GDPR
  - Professional Profiles UNI/EN (ICT & HR)
- Project Management & Framework
- Job Safety & Security
- Management & Soft skills

ICTech

- IT & Operative Systems
- Networking & DevNet
- Cloud & Virtualization
- Containers
  - Docker
  - Kubernetes
- Blockchain
- Development & Programming
- Industry 4.0 (IoT, Big Data, AR)
- Artificial Intelligence, Deep & Machine Learning

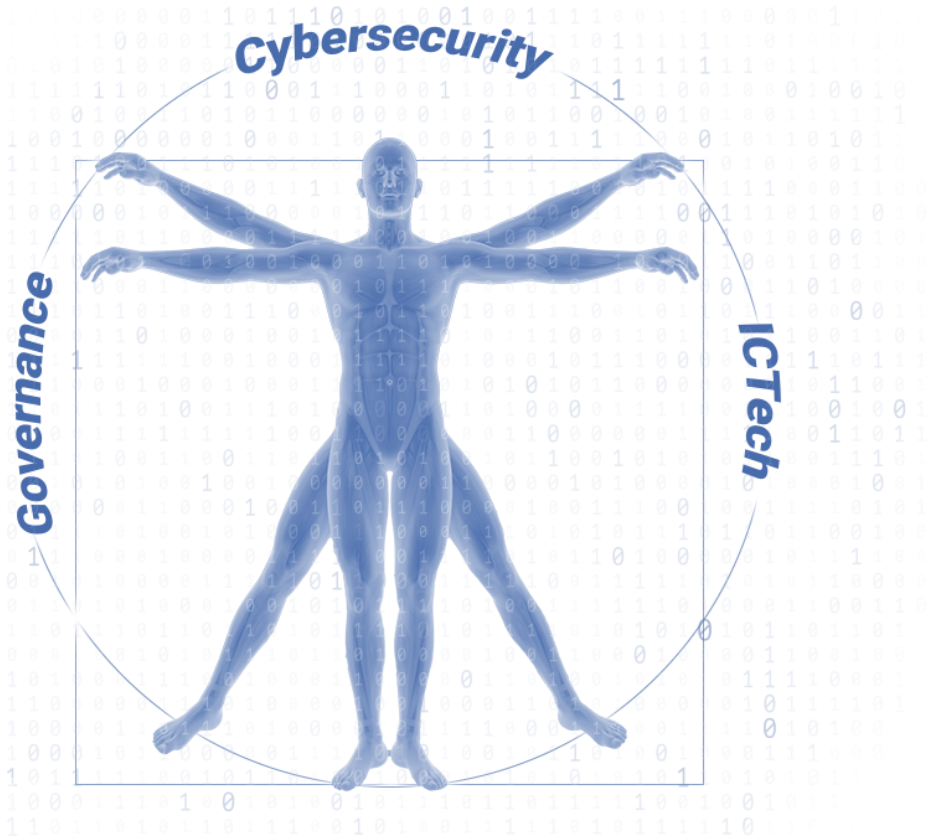
ITHUM
it's for human

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

Via Cristoforo Colombo, 149
00147 Roma (RM) Italy

informazioni@ithum.it

www.ithum.it



Opportunità correlate

Formazione

NIS 2

Inizio corso: 21 marzo 2025

Compliance Normativa

Inizio corso: 27 gennaio 2025

Consulenza

GAP Analysis NIS 2

Verifica perimetro di applicazione e redazione Report (entro il 31 dicembre)

Consulenza multi-compliance

Privacy, Sicurezza informazioni, Business Continuity, Qualità, Responsabilità amministrativa, DORA…)

Software *GRC CORA*

Software di gestione compliance

Scrivere a nis2@ithum.it per ulteriori informazioni

Q&A