ITHUM
it's for human

In partnership with

ict academy
Certified IT Specialist Community & Academy Programs
www.ict-academy.it

GIOVEDÌ 18 DICEMBRE 2025 - ORE 17:00

ISO/IEC 27701:2025

La gestione della privacy tra sicurezza delle informazioni e resilienza digitale

In collaborazione con lexant STUDIO LEGALE

Gerardo GISO (Lexant) - Avvocato, Consulente Privacy e DPO

Francesco NESTA - Data Protection Officer Regione Umbria, ARPAL Umbria e PUNTOZERO s.c.a.r.l.

Agenda:

- **17.00** Presentazione
- **17.10** Speech
- **17.40** Feedback / Prossime iniziative
- **18:00** Q&A e saluti finali

Relatori:

Francesco NESTA - Data Protection Officer Regione Umbria, ARPAL Umbria e PUNTOZERO s.c.a.r.l.

Antonio Gerardo GISO - Avvocato, Consulente Privacy & ICT Law Data Protection Officer

Presenta e Modera:

Marco CIAMPI – Founder & CEO at ITHUM – LinkedIn

Evento Linkedin

Know your Speaker

Francesco NESTA

Data Protection Officer Regione Umbria, ARPAL Umbria e PUNTOZERO s.c.a.r.l.

francesco.nesta@tin.it

LinkedIn

Know your Speaker

Antonio Gerardo GISO

Avvocato, Consulente Privacy & ICT Law
Data Protection Officer

lexant STUDIO LEGALE

gerardo.giso@lexant.it

LinkedIn

Introduzione

La ISO/IEC 27701:2025 quale **maturazione dello standard**.

Passare da una "estensione" a uno "standard autonomo" non è solo una questione formale: la gestione della privacy, sebbene intrinsecamente legata alla sicurezza delle informazioni, ha una sua dignità strutturale, i suoi processi di rischio specifici e i suoi stakeholder (i PII Principals) che richiedono un'attenzione dedicata.

- **Differenza chiave** → la versione 2019 era un "modulo aggiuntivo" da installare alla 27001, la versione 2025 è un edificio che sta in piedi da solo, pur condividendo le stesse fondamenta architettoniche (HLS) degli altri standard ISO.
- **Consiglio per affrontare la transizione** → partire dall'**Allegato A** della nuova norma e mappare l'attuale SoA. Troverete che molti controlli sono stati consolidati, rendendo la gestione potenzialmente più snella, ma richiedendo una **ri-mappatura documentale attenta**.

ISO/IEC 27701:2025 da "estensione" a "standard autonomo"

Struttura "Appoggiata" alla ISO 27001

Non ha una struttura completa, ma estende le ciausole della ISO 27001.

Dipendenza Diretta

Costruita come documento "settoriale", con ISO 27001 e 27002 come prerequisiti normativi.

Struttura HLS Completa e Autonoma

Adotta la struttura standard (clausole 4-10) per una facile integrazione con altri sistemi.

Autonomia Normativa

Il riferimento primario diventa ISO/IEC 29100 (Privacy framework).

Integrazione tramite Allegati

Le relazioni con GDPR e altre norme sono gestite tramite mapping informativi.

Evoluzione 2019 - 2025

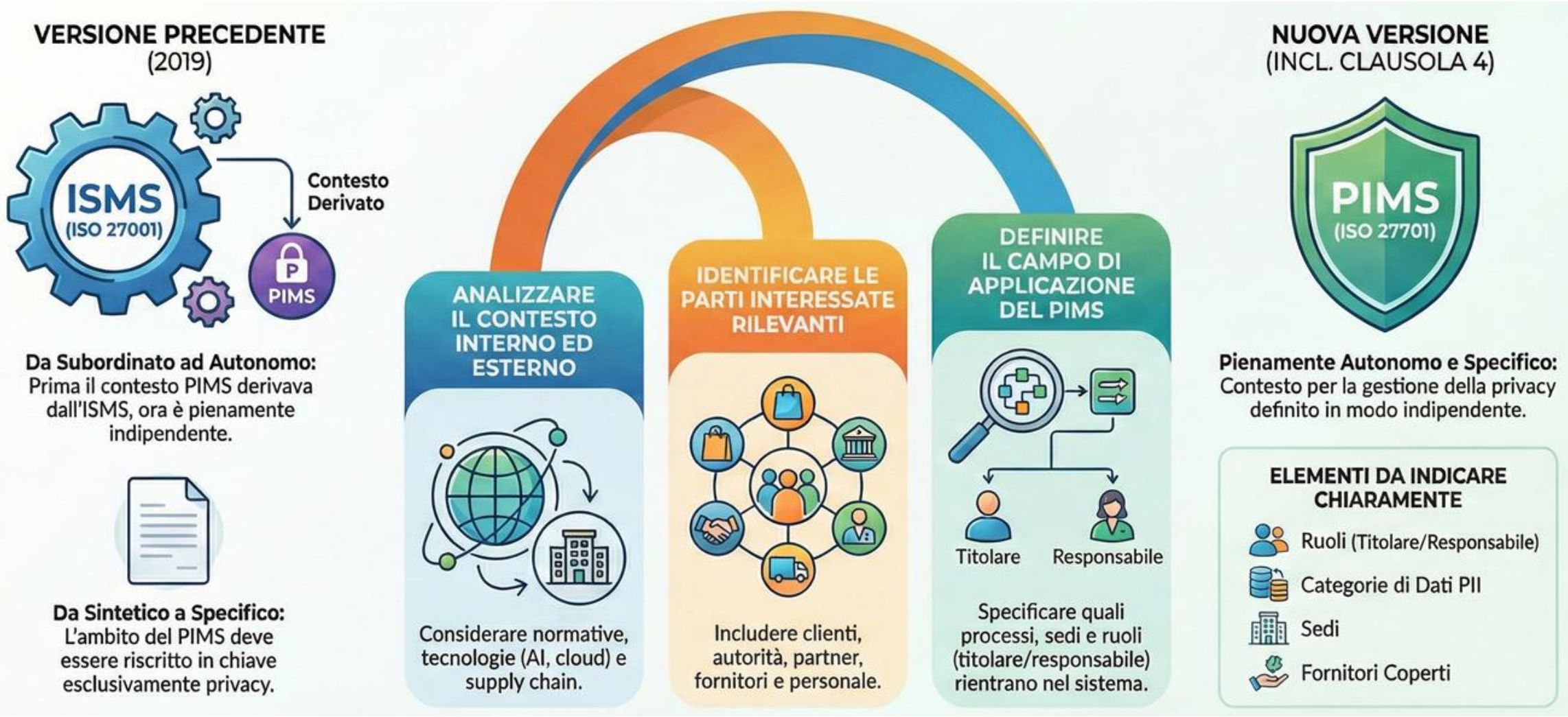
27701/2019 appoggiata alla 27001

- clausola 5: requisiti PIMS collegati alla 27001;
- clausola 6: guida collegata alla 27002;
- clausole 7–8: requisiti specifici per titolari e responsabili;
- Annex A–B: PII Controllers & Processors
- Annex C–F: mapping e linee guida.

27701/2025 struttura HLS

- clausola 4: Contesto dell'organizzazione
- clausola 5: Leadership
- clausola 6: Pianificazione
- clausola 7: Supporto
- clausola 8: Operatività
- clausola 9: Valutazione delle prestazioni
- clausola 10: Miglioramento
- Annex A–B: PII Controllers & Processors + Sicurezza
- Annex C–F: Mapping e corrispondenze

Contesto & Leadership



Rick based approach privacy

APPROCCIO 2019: Rischio Privacy come "Layer" Aggiuntivo

Sicurezza Informatica (ISO 27001)

La gestione del rischio privacy era un'estensione della valutazione del rischio di sicorezza (ISO 27001).

APPROCCIO 2025: Rischio Privacy come Processo Autonomo

Definire Criteri di Rischio Specifici

Valutare il rischio per i diritti e le libertà degli interessati in base al tipo di dati e al contesto.

Collegare le Valutazioni d'Impatto

Integrare in modo stretto DPIA, TIA e la valutazione generale del rischio PIMS.

Costruire una "Statement of Applicability" (SoA) PIMS

Giuatificare formalmente l'inclusione o l'esclusione del controlli previsti dall'Annex A.

Supporto & Informazioni documentate

Privacy Risk Process, Assessment, Treatment

Prima (Approccio 2019)

Requisiti Sparpagliati

I requisiti operativi per titolari e responsabili erano distribuiti tra varie clausole e annex.

Forte Dipendenza dall'ISMS

L'approccio precedente presupponeva un Sistema di Gestione della Sicurezza (ISMS) già operativo.

Oggi (Approccio Attuale)

Clausola 8: Processo Autonomo

Tutta l'operatività privacy è ora centralizzata e progettata come un unico processo PIMS.

Annex A & B: Struttura dei Controlli

A (Elenco Controlli)
Ferniscono l'elenco normativo del controlli (A).

B (Guida Pratica)
e la guida pratica all'Implementazione (B).

Vantaggi:

Permette di creare un SoA PIMS "pulito" ed evitare duplicazioni con il SoA 27001.

Performance Misurabile

Ciclo di Miglioramento Continuo nella Privacy

Allegati della ISO 27701:2025

Allegato A:
Il "Cosa Fare"

Contiene l'elenco dei controlli normativi per Titolari (Controller) e Responsabili (Processor).

Allegato B:
Il "Come Farlo"

Fornisce la guida pratica all'implementazione dei controlli richiesti.

Allegato E:
Mapping per Cloud e Dati Sensibili

Utile per allinearsi agli standard ISO 27018 (cloud) e 29151 (protezione PII).

Allegato C:
Mapping con ISO 29100

Allinea i controlli PIMS ai principi del privacy framework ISO.

Allegato D:
Mapping con il GDPR

Una "bussola operativa" che collega i requisiti della norma agli articoli del GDPR.

Allegato F:
Guida alla Transizione 2019 -> 2025

Strumento essenziale per la gap analysis, mostrando come sono stati riorganizzati i controlli.

Annex 27701:2025

Oltre alle clausole, la vera forza operativa della 27701:2025 sta negli Annex:

- **Annex A** – il contenitore unico dei controlli normativi (ovvero "cosa dovete fare"). È diviso in tre tabelle:
  - **Tabella A.1:** Controlli per PII Controllers.
  - **Tabella A.2:** Controlli per PII Processors.
  - **Tabella A.3:** Controlli di sicurezza delle informazioni comuni a entrambi.
- **Annex B** – la guida all'implementazione (ovvero "come farlo"), assorbendo di fatto il contenuto delle vecchie clausole 7 e 8.
- **Annex C** – Mapping con **ISO/IEC 29100**: consente di allineare i controlli PIMS ai principi del privacy framework ISO.
- **Annex D** – Mapping con il **GDPR**: mostra la corrispondenza tra requisiti/controlli 27701 e articoli chiave del regolamento (es. art. 30, 32, 35). Non crea equivalenze legali, ma è una **bussola operativa** utilissima per DPIA, registri, misure tecniche.
- **Annex E** – Mapping con **ISO/IEC 27018** (cloud privacy) e **ISO/IEC 29151** (PII protection): prezioso per chi lavora con cloud, dati sanitari, grandi piattaforme.
- **Annex F** – Corrispondenza con **ISO/IEC 27701:2019**: è lo **strumento principale per la gap analysis di transizione**, perché mostra come requisiti e controlli della 2019 sono stati riorganizzati nella 2025, quali sono stati accorpati, quali spostati nell'ambito della sicurezza, quali non più necessari.

Cosa fare adesso: tre passi per la transizione

1. **Rivedere lo “scheletro” del PIMS alla luce delle clausole 4–10**

- aggiornare campo di applicazione, politica privacy, ruoli, schema del risk assessment e del risk treatment privacy;
- verificare che il PIMS sia descritto come **sistema autonomo**, non come appendice della 27001.

2. **Ricostruire il SoA PIMS usando Annex A/B e Annex F**

- partire dal SoA attuale;
- usare Annex F per vedere dove sono finiti i vecchi requisiti 2019;
- costruire un SoA PIMS 2025 che richiami in modo ordinato i controlli Annex A/B e, dove necessario, rinvii alle misure 27001/27002.

3. **Definire 5–7 KPI privacy e integrarli nel ciclo di audit e riesame**

- tempi risposta diritti, numero reclami, esito DPIA, numero breach e near miss, stato azioni correttive;
- portarli sistematicamente nel riesame di direzione, così che il PIMS diventi parte del governo aziendale, non solo del fascicolo certificazione.

Grazie per l'attenzione!

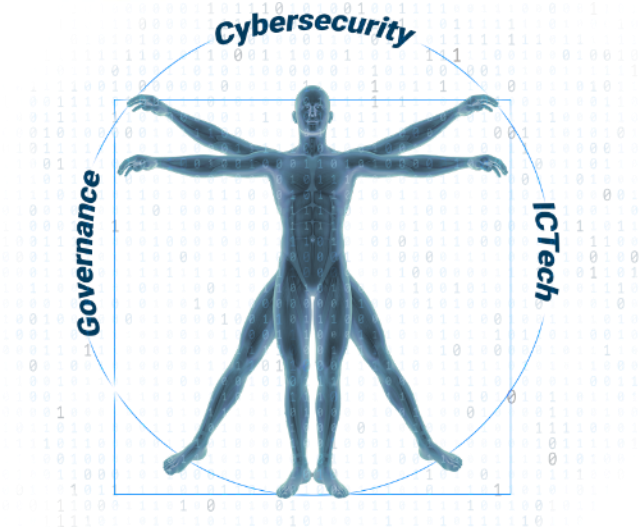
QUESTIONARIO

- ❑ Gradimento
- ❑ Newsletter

Scrivere a eventi@ithum.it per:

- ✓ Attestato di partecipazione
- ✓ Slide proiettate
- ✓ Informazioni varie
- ✓ Registrazione

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

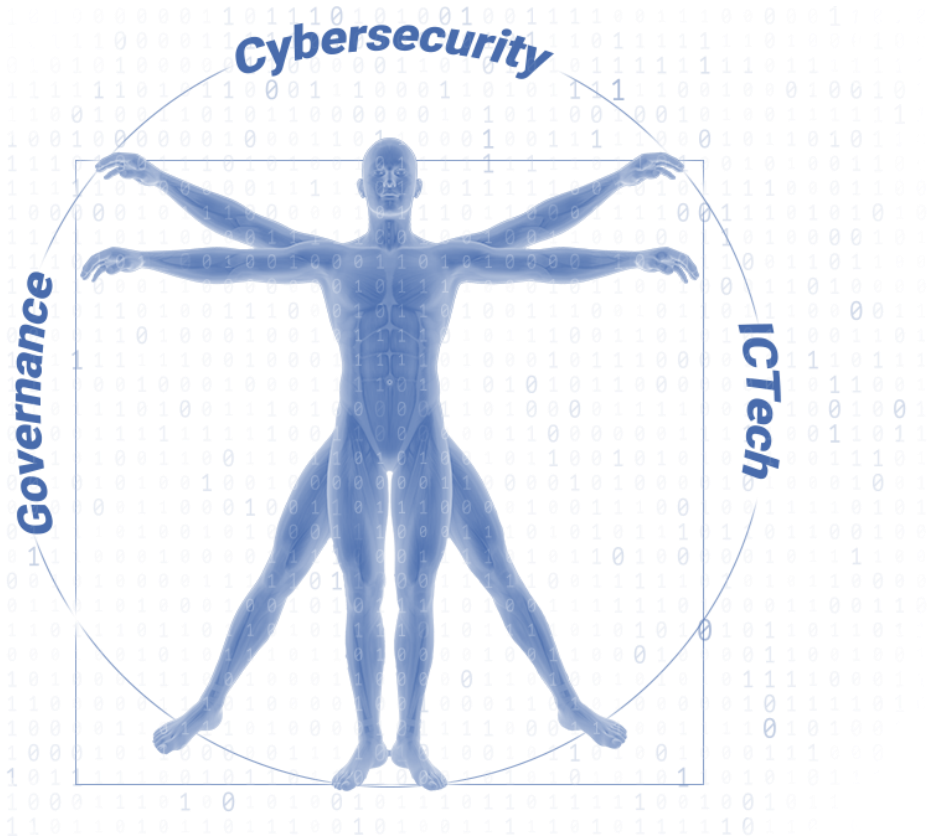
ITHUM
it's for human

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

Via Cristoforo Colombo, 149
00147 Roma (RM) Italy

informazioni@ithum.it

www.ithum.it



Corsi correlati

ISO/IEC 27017-27018
Codici di condotta per il controllo e la protezione delle informazioni in cloud

Inizio corso: 20 gennaio 2026

ISO/IEC 27001
Sicurezza delle informazioni

Inizio corso: 9 marzo 2026

Data Protection Officer (DPO)

Inizio corso: *in definizione*

Privacy Manager

Inizio corso: *in definizione*

Privacy Specialist

Inizio corso: *in definizione*

Privacy Engineer

Inizio corso: *in definizione*

Privacy Auditor

Inizio corso: *in definizione*

ITHUM
it's for human

Q&A