Norme tecniche per la sicurezza informatica

23 febbraio 2023

UNINFO

Relatore

Fabio GUASCONI

- ✓ Presidente del CT 510 di **UNINFO** "Sicurezza"
- ✓ Direttivo **CLUSIT**
- ✓ Esperto **SBS**
- ✓ Esaminatore UNI 11697
- ✓ Certificazioni CISA, CISM, PCI-QSA/3DS/QPA/P2PE/CPSA, ITIL, PRINCE2, ISFS, LA 27001/22301/27701/9001, LI 27001, DPO UNI 11697
- ✓ Co-fondatore di **Bl4ckswan** S.r.l.

UNINFO

Sicurezza Informatica? Cybersecurity?

Information security (sicurezza delle informazioni):
Tutela della riservatezza, integrità e disponibilità dell'informazione.

- **Riservatezza:** Proprietà di essere accessibile e usabile a richiesta di un'entità autorizzata
- **Integrità:** Proprietà relativa all'accuratezza e alla completezza
- **Disponibilità:** Proprietà di essere accessibile e usabile a richiesta di un'entità autorizzata

Cybersecurity
Tutela di persone, società, organizzazioni e nazioni dai **rischi cyber**
[Safeguarding of people, society, organizations and nations from **cyber risks**]

- **Rischi Cyber (Cyber risks)** Il rischio cyber è associato alla possibilità che le minacce sfruttino le vulnerabilità nel cyberspazio e quindi causino danni alle entità nel cyberspazio
- **Cyberspazio (Cyber space)** Ambiente digitale interconnesso di reti, servizi, sistemi, persone, processi, organizzazioni e ciò che risiede nell'ambiente digitale o lo attraversa

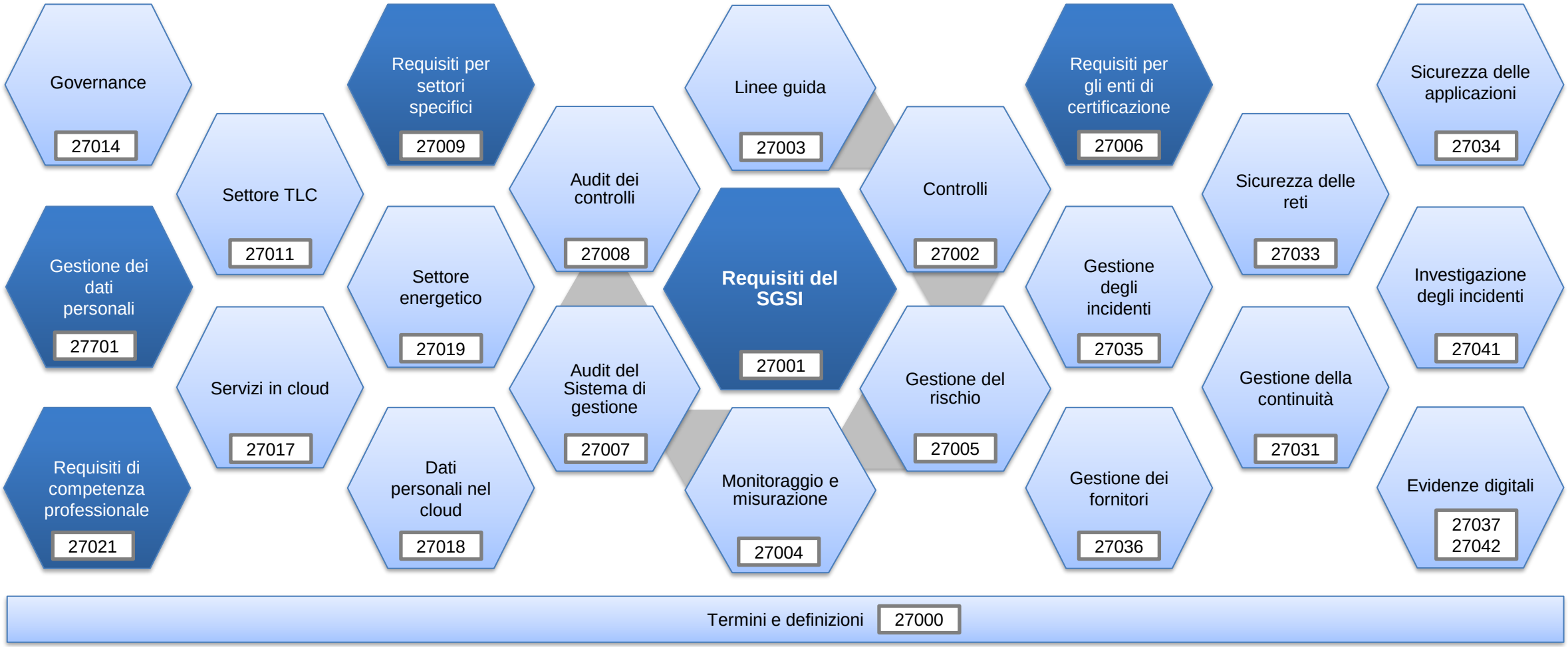
ISO/IEC 27001

La norma ISO/IEC 27001 rappresenta il punto di riferimento internazionale, quando si parla di information security, che descrive le best practice per un SGSI (Sistema di Gestione per la Sicurezza delle Informazioni).

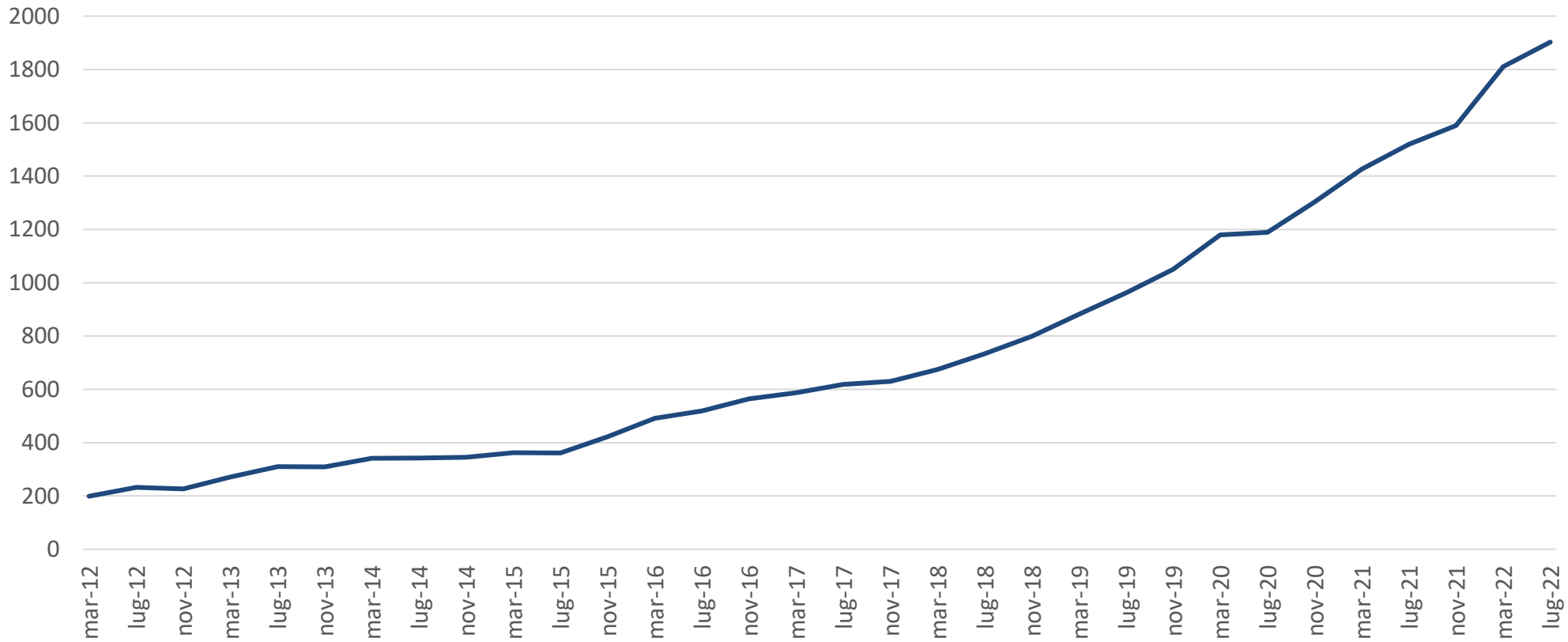
- Applicabile a realtà di ogni dimensione
- Circa 20 anni di esistenza sul mercato
- Ambito definibile a piacimento
- Approccio ciclico (**PDCA**)
- High-level structure tipica dei nuovi sistemi di gestione
- E' basata sulla gestione del rischio
- Costituisce un framework completo
- Dice **cosa fare**, non come farlo
- Rivolto al miglioramento continuo
- E' un riferimento universale e **certificabile**

UNINFO

Processi (e famiglia) ISO/IEC 27001



Certificazioni ISO/IEC 27001



Fonte: **Accredia**

UNINFO

ISO/IEC 27001, perché utilizzarla?

Offre un' "**ancora**" terminologica e metodologica condivisa nel mondo in un ambito continuamente in evoluzione

Il bacino di **risorse** ad essa collegate sul mercato è estremamente ampio

Permette un approccio "**intelligente**" e non solo prescrittivo a questi temi

Si **integra** perfettamente con gli altri sistemi di gestione, con il tema della protezione dei dati personali (27701) e con la gestione del rischio a livello d'impresa

E' una norma adottata a livello **europeo** dal CEN ed ufficialmente tradotta anche in Italiano

Famiglia 22100

Questa famiglia di norme sulla **sicurezza dei macchinari (safety of machinery)** si compone di:

- *Part 1: How ISO 12100 relates to type-B and type-C standards*
- *Part 2: How ISO 12100 relates to ISO 13849-1*
- *Part 3: Implementation of ergonomic principles in safety standards*
- ***Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects***
- *Part 5: Implications of artificial intelligence machine learning*

Queste norme, e in particolare la parte 4, sono state create perchè la serie ISO 12100, incentrata sulla **safety**, non è esaustiva, ad esempio: non indirizza attacchi e minacce intenzionali.

La parte 4 mira a valutare i rischi di IT Security durante tutte le fasi del ciclo di vita delle machine, partendo dale 5 fasi del cybersecurity framework (**identify, protect, detect, respond, recover**)

Famiglia 22100, safety vs security

	Safety of machinery	IT-Security (cyber security)
Objectives	injury/accident prevention, health (avoidance of harm)	availability, integrity, confidentiality
Conditions (risks, methods, measures)	transparent (obvious)	not obvious (not shared with machinery user)
Dynamics	rather static field (intended use, reasonable foreseeable misuse)	highly dynamic field; moving target (intentional manipulation, criminal intent)
Risk reduction (mitigation) measures	mainly by machine manufacturer at a dedicated time (when providing the machine for the first use)	by various actors (machine manufacturer, integrator, machine user, service provider) at any time along the overall life cycle

- I problemi di IT SECURITY possono generare problematiche di SAFETY (e viceversa)
- Le misure di IT SECURITY (sarabbe interessante usare quelle della 27002) possono essere adottate da:
  - **Manufacturer**
  - **Integrator**
  - **End users**

Comparativa

ISO/IEC 27001	ISO 22100
Certificabile	Non certificabile
Generalista	Specifica per le macchine
Comprende un insieme esaustivo di misure di sicurezza	Ha un insieme esemplificativo di misure di sicurezza
E' diffusa ed ampiamente adottata	E' relativamente recente
Si integra con altri sistemi di gestione	Si integra con la gestione della safety e con il cybersecurity framework

E' possibile prendere il meglio di entrambe le norme?

Conclusioni

1

Esistono norme tecniche importanti sulla sicurezza, non serve reinventare la ruota quando si può viaggiare sulle spalle dei giganti

2

La tecnologia da sola non è la risposta ai problemi di sicurezza informatica / delle informazioni / cyber, la sua governance è indispensabile

3

La sicurezza della progettazione e manutenzione delle macchine sarà sempre più un parametro importante sul mercato

Contatti

fabio.guasconi@bl4ckswan.com