La Famiglia ISO 27000: Framework e Best Practices

Focus normativo su ISO/IEC 27001:2022 e ISO/IEC 27002:2022

Dalla Gestione del Rischio alla Sicurezza delle Informazioni

ISO 31000

Si prefigge di gestire il rischio nella sua accezione più generale. Fornisce linee guida generiche applicabili a qualsiasi tipo di rischio.

Famiglia ISO 27000

Una serie di norme dedicate specificamente alla sicurezza informatica.

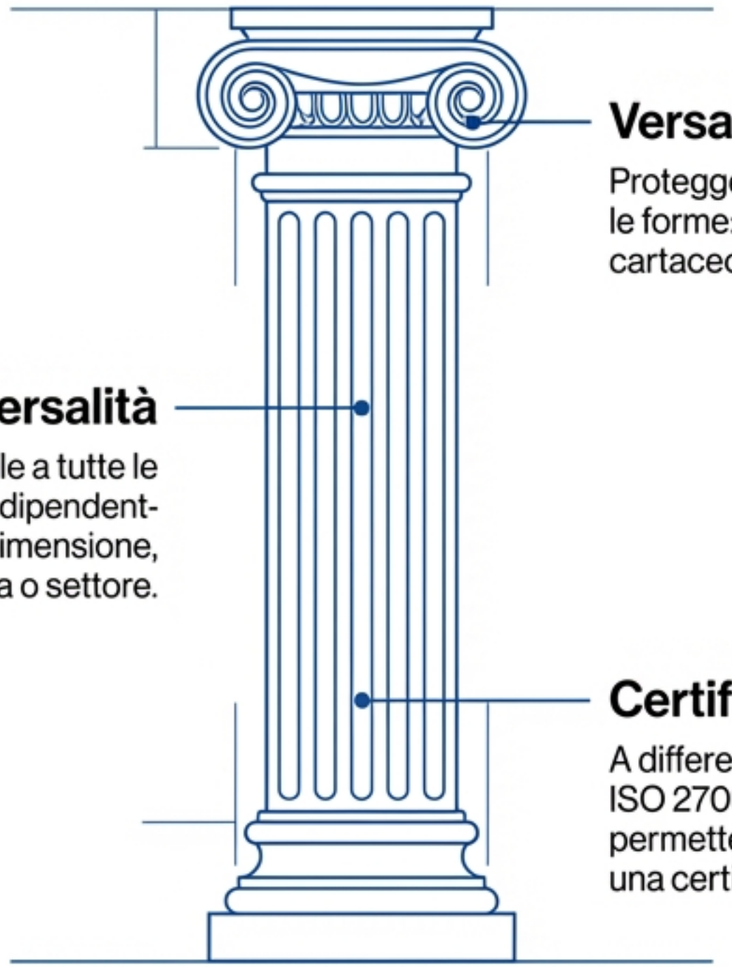
— Obiettivo: Proteggere le informazioni prodotte e mantenute da un ente.

Scope del Modulo: Analisi focalizzata esclusivamente su ISO 27001 (il pilastro) e ISO 27002 (le linee guida).

Il Pilastro Normativo: ISO/IEC 27001:2022

DEFINIZIONE

Lo standard internazionale che determina i requisiti per la creazione, manutenzione e sviluppo di un Information Security Management System (ISMS).



Versatilità dei Dati

Protegge le informazioni in tutte le forme: digitali, su supporto cartaceo o archiviate nel cloud.

Universalità

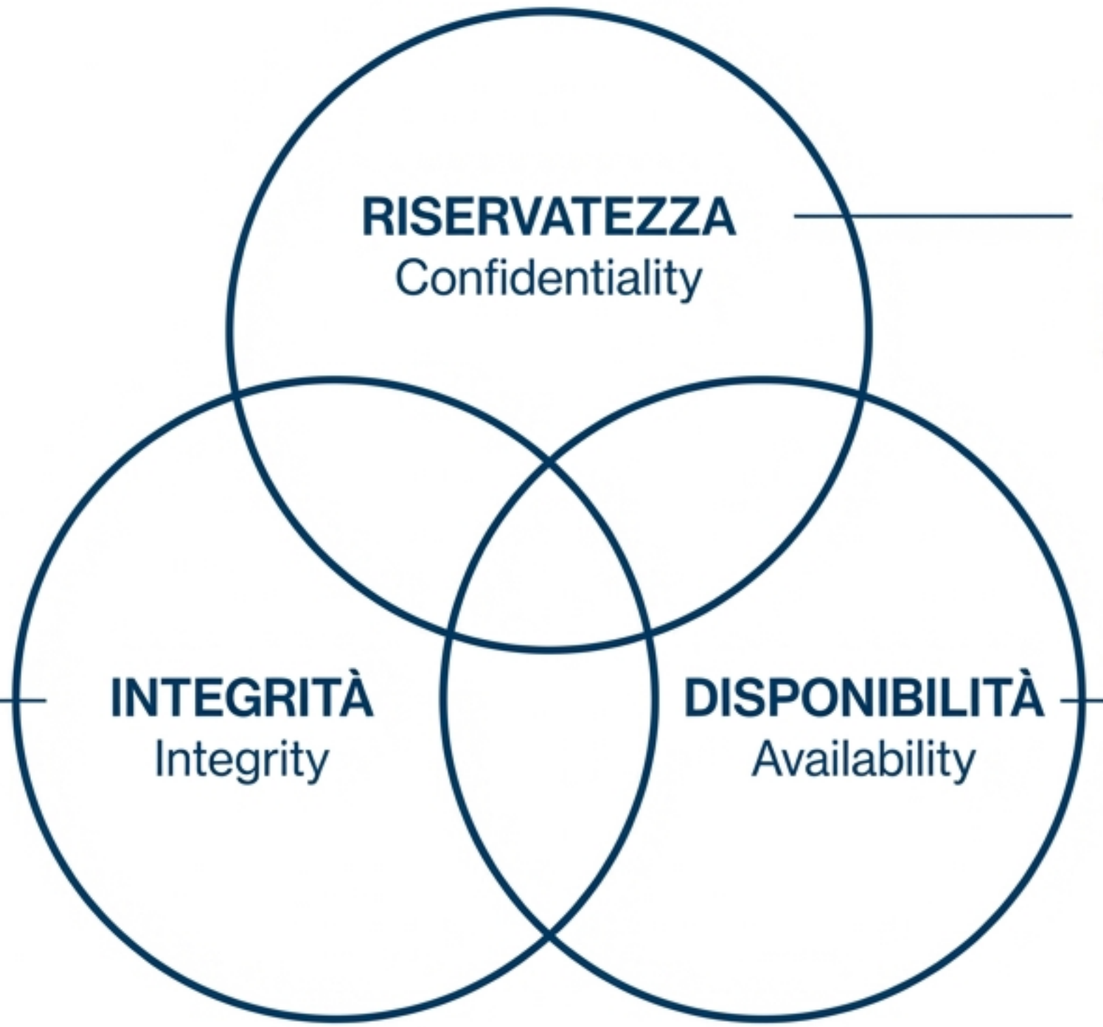
Applicabile a tutte le organizzazioni indipendent-temente da tipo, dimensione, natura o settore.

Certificabilità

A differenza della ISO 31000, la ISO 27001 è una norma che permette alle aziende di ottenere una certificazione ufficiale.

I Tre Punti Cardine: La Triade RID (CIA)

I principi fondamentali della norma.



Richiede che le informazioni siano rese inintelligibili a utenti non autorizzati. Chi non ha il permesso, non deve poter accedere.

Richiede che i dati rimangano uguali a se stessi nel tempo, senza subire alterazioni non autorizzate.

Richiede che l'accesso ai dati sia possibile rapidamente nel momento del bisogno.

La Necessità Strategica di un ISMS Robusto

Proteggere i sistemi informativi è diventato uno step cruciale per qualsiasi organizzazione, dal data center al singolo dispositivo in rete.

Espansione Superficie d'Attacco

Le 'porte' che gli attaccanti possono sfruttare per penetrare nei sistemi sono in continuo aumento.

Proliferazione dei Dispositivi

Inevitabile aumento del numero di device connessi e dell'IoT.

Impatto Post-Pandemico

Situazioni derivate dal Covid, come l'aumento dello smart working, hanno esposto maggiormente le reti aziendali.

I Benefici Operativi ed Economici

Resilienza e Sicurezza

- ✓ **Aumento della resistenza agli attacchi informatici.**
- ✓ **Protezione da rischi tecnologici e minacce comuni** (es. personale scarsamente informato).
- ✓ **Adattamento costante all'evoluzione delle minacce esterne.**

Efficienza e Cultura

- ↑ **Riduzione dei costi associati alla sicurezza nel lungo termine (approccio preventivo).**
- ↑ **Gestione dei rischi in modo economicamente conveniente.**
- ↑ **Coinvolgimento di tutti i dipendenti nell'adozione di controlli come pratica ordinaria.**

Distinzione Funzionale: ISO 27001 vs. ISO 27002

ISO/IEC 27001 (Il Framework)	ISO/IEC 27002 (Gli Strumenti)
• Specifica i **requisiti** per stabilire un ISMS. • È un documento **normativo**. • Prevede la **certificazione** dell'organizzazione.	• È una raccolta di **best practices** e codici di condotta. • Fornisce consigli per soddisfare i requisiti. • **Non prevede** la certificazione.

La Struttura della ISO/IEC 27002:2022

1. Persone

Controlli relativi alle risorse umane.

2. Fisici

Protezione degli oggetti fisici e delle strutture.

93

Controlli di Sicurezza Totali

3. Tecnologici

Misure tecniche e digitali.

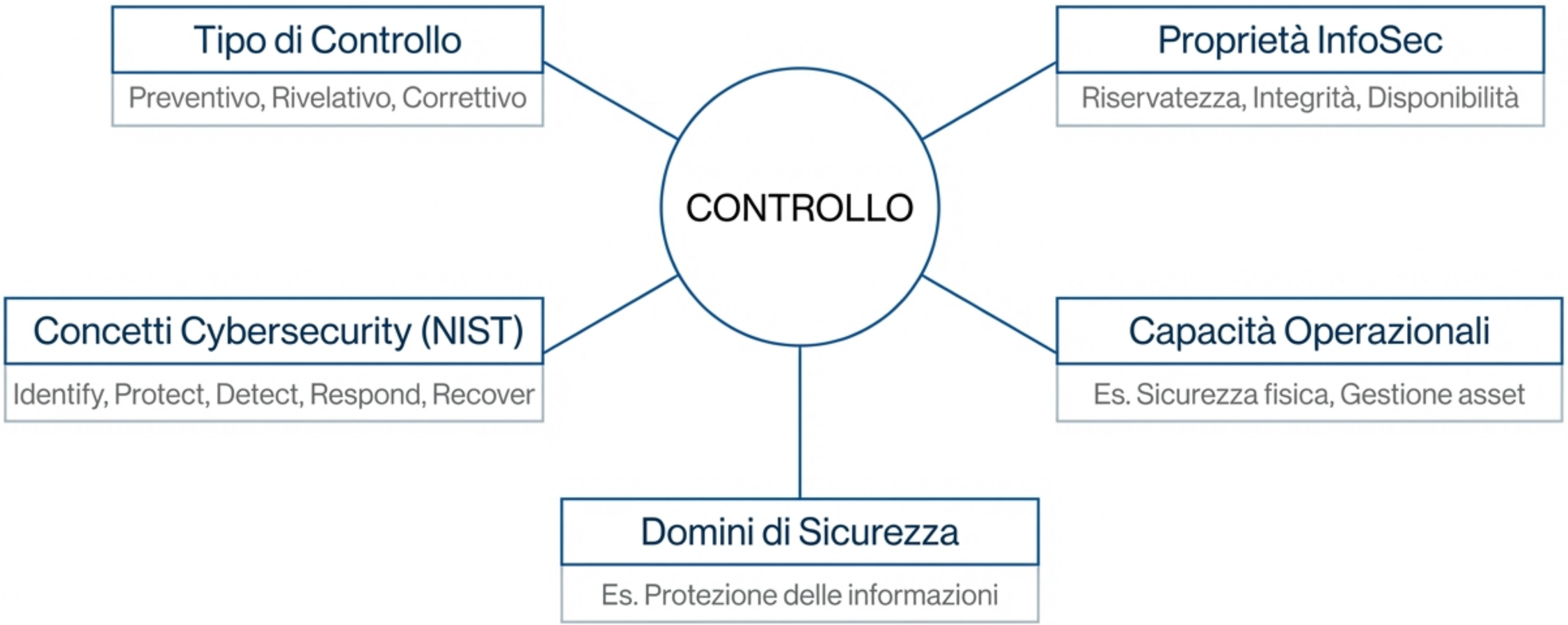
4. Organizzativi

Procedure e struttura dell’ente.

Tassonomia dei Controlli: Classificazione Temporale

Attributi dei Controlli di Sicurezza

I metadati che definiscono ogni controllo nella ISO 27002.



Caso Studio: Perimetri di Sicurezza

Controllo: Perimetri di Sicurezza

I perimetri di sicurezza dovrebbero essere definiti e utilizzati per proteggere le aree che contengono informazioni e altri asset associati.

Scopo: Prevenire l"accesso fisico non autorizzato, il danno e l"interferenza.

Tags

Tipo: Preventivo | Proprietà: CID (CIA) | Concetto: Protect | Capacità: Sicurezza Fisica

Conclusioni e Punti Chiave

1. **Sinergia Normativa**
   La ISO 27001 fornisce il framework di gestione (ISMS), mentre la ISO 27002 offre il catalogo pratico dei controlli.
2. **Adattabilità e Resilienza**
   Il sistema evolve con le minacce, adattandosi a nuove sfide come lo smart working.
3. **Approccio Olistico**
   La sicurezza non è solo tecnologica, ma include persone, perimetri fisici e processi organizzativi.
4. **Obiettivo Finale**
   Garantire costantemente Riservatezza, Integrità e Disponibilità delle informazioni aziendali.

Riferimenti Normativi

- ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
- ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls.
- ISO 31000:2018 - Risk management — Guidelines.