Gli standard EN 50600 e ISO/IEC TS 22237 per i data center

Per i data center sono molto note le norme dell'Uptime institute e l'ANSI TIA-942.

L'**Uptime insititute** certifica i data center sulla base delle loro caratteristiche di disponibilità. La certificazione può essere data su quattro livelli (*tier*), corrispondenti a caratteristiche architetturali sempre più rigorose e, di conseguenza, a sempre più elevati livelli di disponibilità del data center (fino al 99,99% per il Tier IV). L'ultima versione del *"Tier Standard: Topology"* è del 2018.

L'**ANSI TIA-942**, dal titolo *"Telecommunications Infrastructure Standard for Data Centers"*, la cui revisione B è del 2017, è un documento dell'ente di standardizzazione statunitense ANSI. Anch'esso prevede quattro livelli a cui un data center può aspirare.

Più recentemente, anche l'**Europa** ha voluto sviluppare standard relativi ai data center e promuoverli a livello internazionale. Questo articolo vuole quindi elencare rapidamente i lavori oggi pubblicati e proporre una sintetica riflessione sulle possibilità di certificazione collegate a questi standard.

Serie ISO/IEC 22237

La serie ISO/IEC 22237 reca il titolo *"Data centre facilities and infrastructures"* ed è composta dalle seguenti parti:

- ISO/IEC TS 22237-1:2018 – Part 1: General concepts;
- ISO/IEC TS 22237-2:2018 – Part 2: Building construction;
- ISO/IEC TS 22237-3:2018 – Part 3: Power distribution;

- ISO/IEC TS 22237-4:2018 – Part 4: Environmental control;
- ISO/IEC TS 22237-5:2018 – Part 5: Telecommunications cabling infrastructure;
- ISO/IEC TS 22237-6:2018 – Part 6: Security systems;
- ISO/IEC TS 22237-7:2018 – Part 7: Management and operational information.

La prima parte stabilisce i **criteri** per dimostrare una conformità "generale" a queste norme:

1. condurre una valutazione del rischio (la stessa ISO/IEC TS 22237-1 riporta alcune linee guida molto sintetiche, proponendo un approccio qualitativo su scale di 4 valori per verosimiglianza e conseguenza);
2. identificare una classe di disponibilità (la norma ne prevede 4) sulla base della valutazione del rischio (e realizzare quanto necessario, anche considerando i requisiti previsti per le componenti nelle parti 3, 4 e 5);
3. identificare una classe di protezione (la norma ne prevede 4) sulla base della valutazione del rischio (e realizzare quanto necessario, anche considerando i requisiti di protezione specificati dalle parti 2, 3, 4 e 6);
4. identificare un appropriato livello di capacità energetica (e realizzare quanto necessario);
5. applicare alcuni specifici principi di progettazione.

I **principi di progettazione** includono:

- un processo composto delle fasi di strategia, obiettivi, specifiche, proposta di progetto, decisione, progetto funzionale, approvazione, progettazione finale e pianificazione, contrattualistica, costruzione, esercizio;
- i principi necessari a raggiungere i livelli di disponibilità stabiliti (automazione, autonomia, tolleranza ai guasti, manutenibilità, assegnazione di

priorità, ridondanza, robustezza, scalabilità, semplicità);
- il concetto di efficace elettrocompatibilità per ridurre i rischi relativi ai disturbi elettromagnetici e dovuti a fulmini;
- l'uso di zone di sicurezza fisica;
- l'efficienza energetica.

È possibile anche dimostrare la conformità delle singole componenti ai requisiti delle norme specializzate, ossia le parti dalla 2 alla 6.

La parte 6, sui **sistemi di sicurezza**, si concentra su quelli per la protezione da accessi non autorizzati, incendi, eventi ambientali originati all'interno del data center ed eventi ambientali originati all'esterno del data center (esclusi gli incendi).

La parte 7 riguarda il sistema di gestione del data center e può essere vista come cappello delle altre norme, visto che ne ricorda i principi lungo il ciclo di vita del data center stesso.

È possibile dimostrare la conformità anche rispetto alla parte 7:

a) attuando una strategia basata sui requisiti di business;
b) attuando regole e procedure relative all'esercizio, alla gestione degli incidenti, della sicurezza e dei clienti (la norma descrive le caratteristiche di questi processi);
c) monitorando degli indicatori di efficacia dell'uso dell'energia;
d) attuando regole di gestione degli asset, di controllo ambientale, del ciclo di vita, dell'energia.

Sembra quindi che la serie ISO/IEC 22237 offra sette possibili certificazioni. Forse troppe, ma forse necessarie per poterle attuare nelle fasi del ciclo di vita più idonee al singolo data center e per dare la giusta evidenza ad un aspetto invece

che a un altro.

Serie EN 50600

La serie di **standard europei** EN 50600 include un gruppo di 7 documenti (la parte 1 e la parte 2, a sua volta suddivisa in sei sotto-parti) che possono essere considerati le versioni precedenti di quelli della serie ISO/IEC 22237, come è facilmente intuibile anche dai titoli:

- EN 50600-1 – Part 1: General concepts;
- EN 50600-2-1 – Part 2-1: Building construction;
- EN 50600-2-2 – Part 2-2: Power distribution;
- EN 50600-2-3 – Part 2-3: Environmental control;
- EN 50600-2-4 – Part 2-4: Telecommunications cabling infrastructure;
- EN 50600-2-5 – Part 2-5: Security systems;
- EN 50600-3-1 – Part 2-6: Management and operational information.

Tutte le norme sopra riportate sono state pubblicate tra il 2012 e il 2016.

La serie EN 50600 comprende altre norme. La parte 4 è costituita dalle seguenti 3 norme, pubblicate nel 2016:

- EN 50600-4-1 – Part 4-1: Overview of and general requirements for key performance indicators;
- EN 50600-4-2 – Part 4-2: Power Usage Effectiveness;
- EN 50600-4-3 – Part 4-3: Renewable Energy Factor.

La prima norma non è significativa, mentre le altre due trattano compiutamente due parametri oggi ritenuti molto importanti nell’ambito della sostenibilità energetica.

Ultima serie del gruppo è la 99, dedicata ad alcune **raccomandazioni**:

- CLC/TR 50600-99-1:2017 – Part 99-1: Recommended practices for energy management;

- PD CLC/TR 50600-99-2:2018 – Part 99-2: Recommended practices for environmental sustainability;
- DS/CLC/TR 50600-99-3:2018 – Part 99-3: Guidance to the application of EN 50600 series.

Conclusioni sulle certificazioni

Ad oggi, le certificazioni gestite dall'Uptime Institute e quelle per dimostrare la conformità all'ANSI TIA-942 sono molto note, anche se richiedono un notevole impegno da parte dei richiedenti.

Le certificazioni relative alle norme EN 50600 e ISO/IEC 22237 sono ancora poco diffuse e offerte da pochi organismi di certificazione, senza uno schema di accreditamento condiviso. Si tratta però di standard costruiti anche per essere più flessibili di quelli americani. Bisogna quindi vedere se in futuro si imporranno come riferimento – anche grazie al **Cybersecurity Act** – e come la flessibilità con cui è possibile certificarsi sarà usata e recepita.

Articolo a cura di **Cesare Gallotti**

Lavora dal 1999 nel campo della sicurezza delle informazioni, della qualità e della gestione dei servizi IT.

Ha condotto progetti di consulenza per la pubblica amministrazione e per il settore privato. Opera, sia in Italia che all'estero, come Lead Auditor ISO/IEC 27001, ISO 9001, ISO/IEC 200000 e ISO 22301. Ha progettato ed erogato corsi di Quality Assurance e di certificazione Lead Auditor ISO/IEC 27001 e ITIL Foundation.

Tra gli attestati si segnalano: le certificazioni AICQ SICEV Lead Auditor ISO/IEC 27001, IRCA Lead Auditor 9001, CISA, ITIL Expert e CBCI, la qualifica come Lead Auditor ISO/IEC 20000 e il perfezionamento postlaurea in "Computer Forensics e investigazioni digitali".

E’ capodelegazione del WG1 del comitato italiano ISO/IEC SC27 in UNINFO.

Ha pubblicato il libro, aggiornato nel 2017, “Sicurezza delle informazioni: valutazione del rischio; i sistemi di gestione; la norma ISO/IEC 27001:2013”.

Cura la pubblicazione, dal 2008, della newsletter “IT Service management news” (http://www.cesaregallotti.it/Newsletter.html).

Web: www.cesaregallotti.it; Blog: blog.cesaregallotti.it

https://www.ictsecuritymagazine.com/articoli/gli-standard-en-50600-e-iso-iec-ts-22237-per-i-data-center/