La sicurezza e la qualità dei dati

Domenico Natale
Commissione UNINFO SC7

Agenda

- Il mondo ISO 2012
- Le linee guida dei siti web delle PA
- Raccomandazioni sul Cloud nella PA
- La qualità del sw ISO 25010
- La qualità dei dati ISO 25012
- IT Service quality model ISO 25011
- Conclusione

Il mondo ISO 2012…

* L'ISO (International Organization for Standardization) è la più grande organizzazione del mondo per lo sviluppo di standard internazionali. Ha sviluppato 19.000 standard e ne pubblica ogni anno circa 1.000

* ISO è un network di istituti nazionali di 164 Paesi con un segretariato centrale a Ginevra che coordina il sistema. Gli esperti lavorano su internet e si riuniscono due volte l'anno

* www.iso.org e www.uni.com
* www.jtc1-sc7.org e www.uninfo.polito.it

ISO Plenary meeting 2012

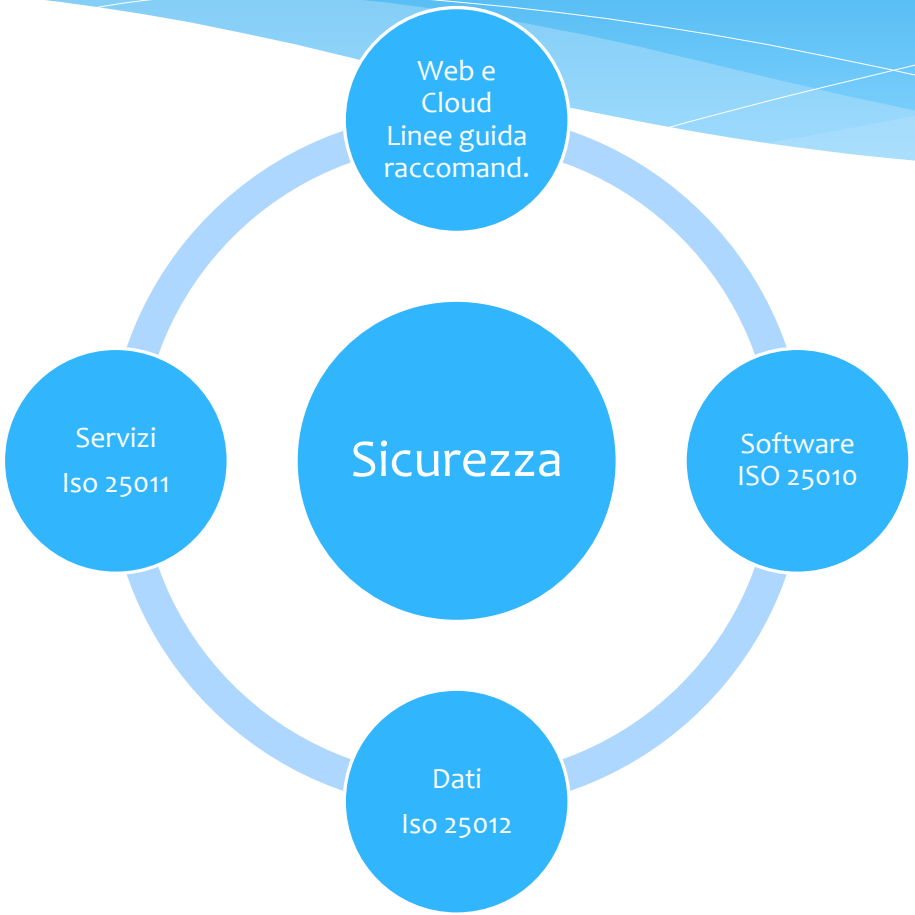
UNINFO: TECNOLOGIE INFORMATICHE E LORO APPLICAZIONI
ENTE di NORMAZIONE FEDERATO all'UNI

Information Technology	Telematica per i trasporti - ITS
Mpeg	Codifiche - RFID
Sicurezza/Security	Applicazioni
Ingegneria del Software	Informazioni Geografiche
Open Source	Telecomunicazioni
Accessibilità	Automazione Industriale
Applicazioni distribuite	Linguaggi
Smart Cards	Learning Technologies
Biometrica	Apparecchiature e Supporti
Sistemi Bancari	Documenti ed elementi di informazione
E-business	

Orientamenti standard ISO 2012

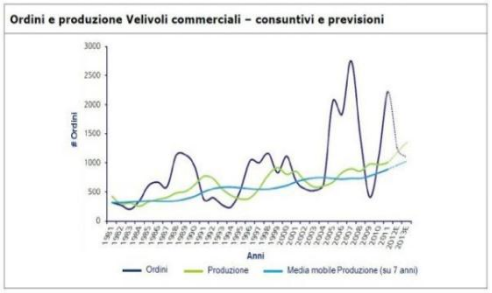
Standard di processo	Standard di prodotto
ISO/IEC 9001 ISO/IEC 12207 ISO/IEC 15288 ISO/IEC 27001	ISO/IEC 25000, 25010*, 25012**
ISO/IEC 14143 ISO/IEC 15939	ISO/IEC 25021, 25022*, 25023*, 25024**
ISO/IEC 20000 (è focalizzato su requisiti e linee guida per l'IT "Service management system" con una prospettiva di processo più che con un intento di valutazione della performance finale; fornisce un'ottima base per la qualità del servizio, ma non l'assicura)	ISO/IEC 25011*** (caratteristiche di qualità del servizio)

Sicurezza: il punto comune della qualità



Priorità della sicurezza

La sicurezza informatica è causa ed effetto della qualità dei dati ed è una priorità data la pervasività dell'informatica nei settori della pubblica utilità



Le linee guida dei siti web delle PA…

* Pubblicate su www.digitpa.gov.it/fruibilita-del-dato/accessibilita per il 2011

* Integrate con il CAD 2010 e Delibere CiVIT *(Commissione per la Valutazione, la Trasparenza e l'Integrità delle Amministrazioni pubbliche)*

* Finalizzate al processo di sviluppo dei servizi online e all'offerta di informazioni di qualità rivolte al cittadino

Le linee guida dei siti web delle PA

Principi di usabilità	Declinazioni (sintesi)
Percezione	Informazioni e comandi sempre disponibili e percettibili
Comprensibilità	Informazioni e comandi facili da capire e da usare
Operabilità	Consentire scelte immediate necessarie al raggiungimento dell'obiettivo
Coerenza	I simboli, i messaggi e le azioni devono avere lo stesso significato in tutto il sito
Tutela della salute	Salvaguardare il benessere psico-fisico dell'utente

Le linee guida dei siti web delle PA

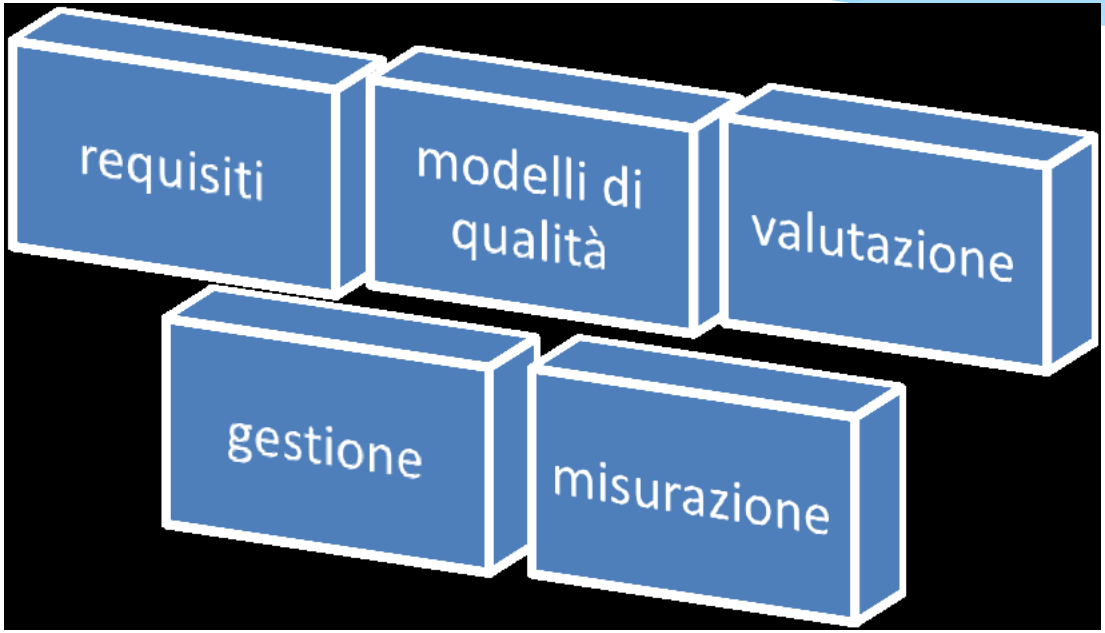
Principi	Declinazioni (sintesi)
Sicurezza	**Fornire transazioni e dati affidabili, gestiti con adeguati livelli di sicurezza**
Trasparenza	Comunicare all'utente lo stato, gli effetti delle azioni compiute
Facilità di apprendimento	Utilizzo di facile e rapido apprendimento
Aiuto e documentazione	Le funzionalità di aiuto devono essere di facile reperimento e collegate alle azioni svolte
Tolleranza agli errori	Fare in modo di prevenire gli errori e poter porvi rimedio
Gradevolezza	Mantenere l'interesse dell'utente
Flessibilità	Tener conto delle preferenze individuali e dei contesti

Raccomandazioni sul Cloud nella PA

* mantenimento del controllo sui dati del titolare del trattamento (data protection)
* individuazione dei dati adeguati per il cloud
* controllo della ridondanza e allineamento
* garanzia riservatezza (dati sensibili e giudiziari)
* crittografia
* backup
* competenze di territorialità (europea e extraeuropea)
* accordi negoziali-contrattuali e responsabilità

(Pubblicate su www.digitpa.gov.it)

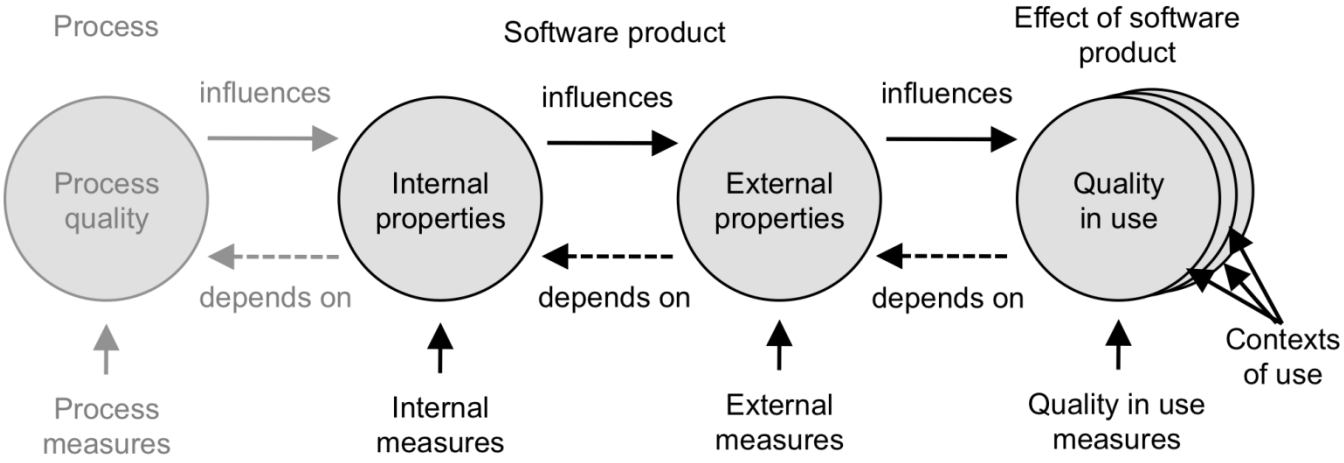
Progetto ISO serie 25000



La qualità ISO 25010

* Definita nello standard ISO come:
  * Qualità interna, verificabile con ispezioni o strumenti di proprietà statiche sul codice informatico
  * Qualità esterna, verificabile da tecnici con test dinamici esclusivamente in ambienti simulati
  * Qualità in uso, verificabile in ambiente reali (o anche simulati) con la partecipazione di utenti (primari, secondari, indiretti) che enfatizzano le difficoltà o la facilità di interazione utente-computer

La qualità ISO 25010 © ISO



Qualità interna/esterna ISO 25010

Applicativa	Tecnica
Idoneità funzionale	Efficienza
Manutenibilità	Compatibilità
Usabilità	Affidabilità
	Sicurezza *
	Portabilità

Sicurezza*
Riservatezza, integrità, non ripudio, tracciabilità, autenticità

Sicurezza ISO 25010

Security
degree to which a product or system protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization:

confidentiality
degree to which a product or system ensures that data are accessible only to those authorized to have access

integrity
degree to which a system, product or component prevents unauthorized access to, or modification of, computer programs or data

non-repudiation
degree to which actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later

accountability
degree to which the actions of an entity can be traced uniquely to the entity

authenticity
degree to which the identity of a subject or resource can be proved to be the one claimed

Qualità in uso ISO 25010

Efficacia	Efficienza	Soddisfazione	Assenza e attenuazione rischi	Copertura del contesto
Efficacia	Efficienza	Utilità	**Economici**	Completezza
		Fiducia	**Per le persone**	Flessibilità
		Piacere	**Danno ambientale**	
		Comodità		

Assenza e attenuazione dei rischi

Quality in use model
Quality in use is the degree to which a product or system can be used by specific users to meet their needs to achieve specific goals with effectiveness, efficiency, freedom from risk and satisfaction in specific contexts of use:

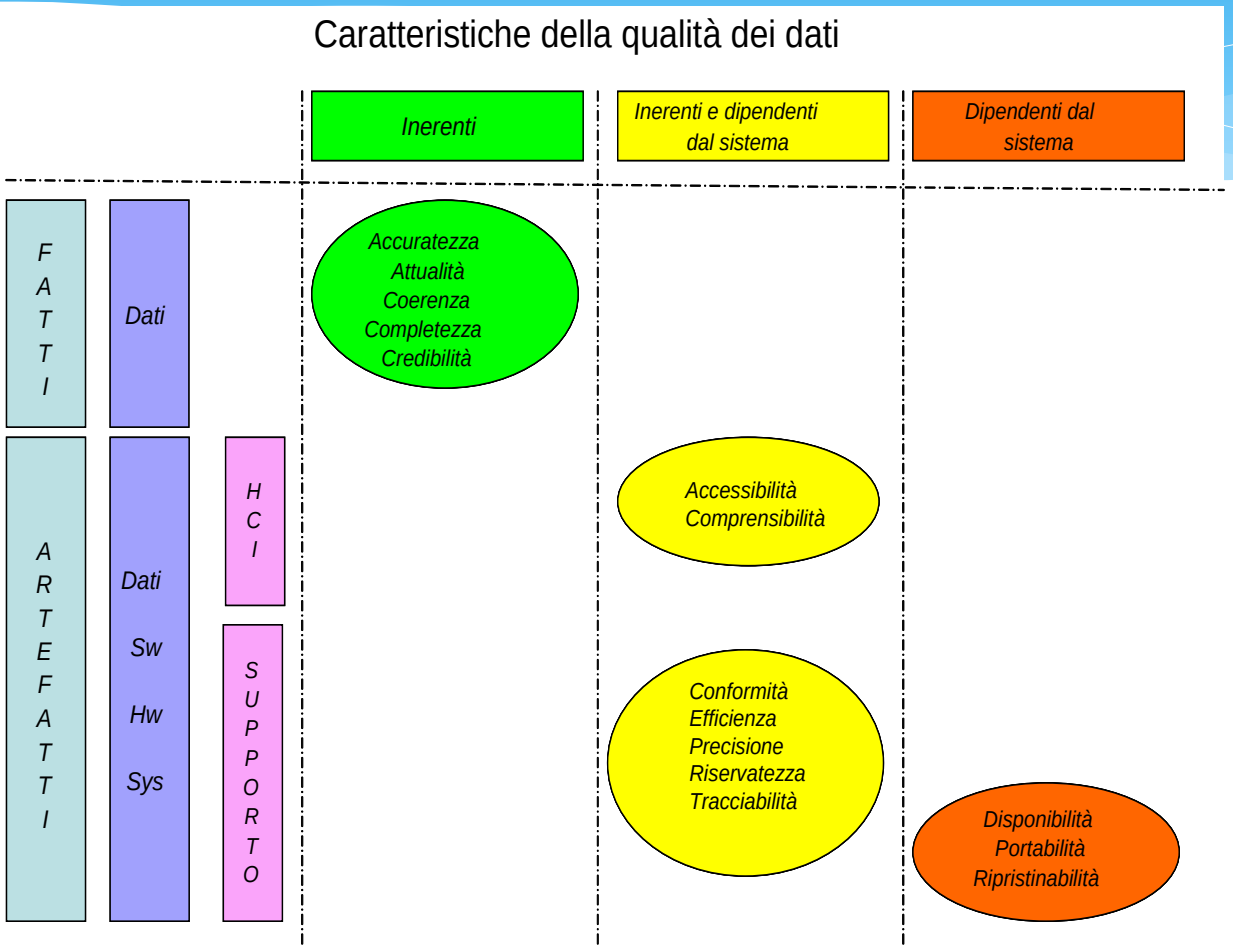
freedom from risk
degree to which a product or system mitigates the potential risk to economic status, human life, health, or the environment

economic risk mitigation
degree to which a product or system mitigates the potential risk to financial status, efficient operation, commercial property, reputation or other resources in the intended contexts of use

health and safety risk mitigation
degree to which a product or system mitigates the potential risk to people in the intended contexts of use

environmental risk mitigation
degree to which a product or system

Qualità dei dati ISO 25012



Sicurezza nella qualità dei dati

Integrity
property of safeguarding the accuracy and completeness of assets

Compliance
The degree to which data has attributes that adhere to standards, conventions or regulations in force and similar rules relating to data quality in a specific context of use.

Confidentiality
The degree to which data has attributes that ensure that it is only accessible and interpretable by authorized
users in a specific context of use.

Traceability
The degree to which data has attributes that provide an audit trail of access to the data and of any changes
made to the data in a specific context of use.

Recoverability
The degree to which data has attributes that enable it to maintain and preserve a specified level of operations
and quality, even in the event of failure, in a specific context of use.

IT service quality model ISO 25011

* Partecipano al progetto:
  * Cina (National Body propositore)
  * Giappone
  * Lussemburgo
  * Usa
  * Italia
* Stato di avanzamento NWI approvato in Korea dopo: ricerca di mercato, studio di precedenti standard ISO, test in 9 città della Cina, confronto «face to face» in Mumbai nel 2011

Termini e definizioni

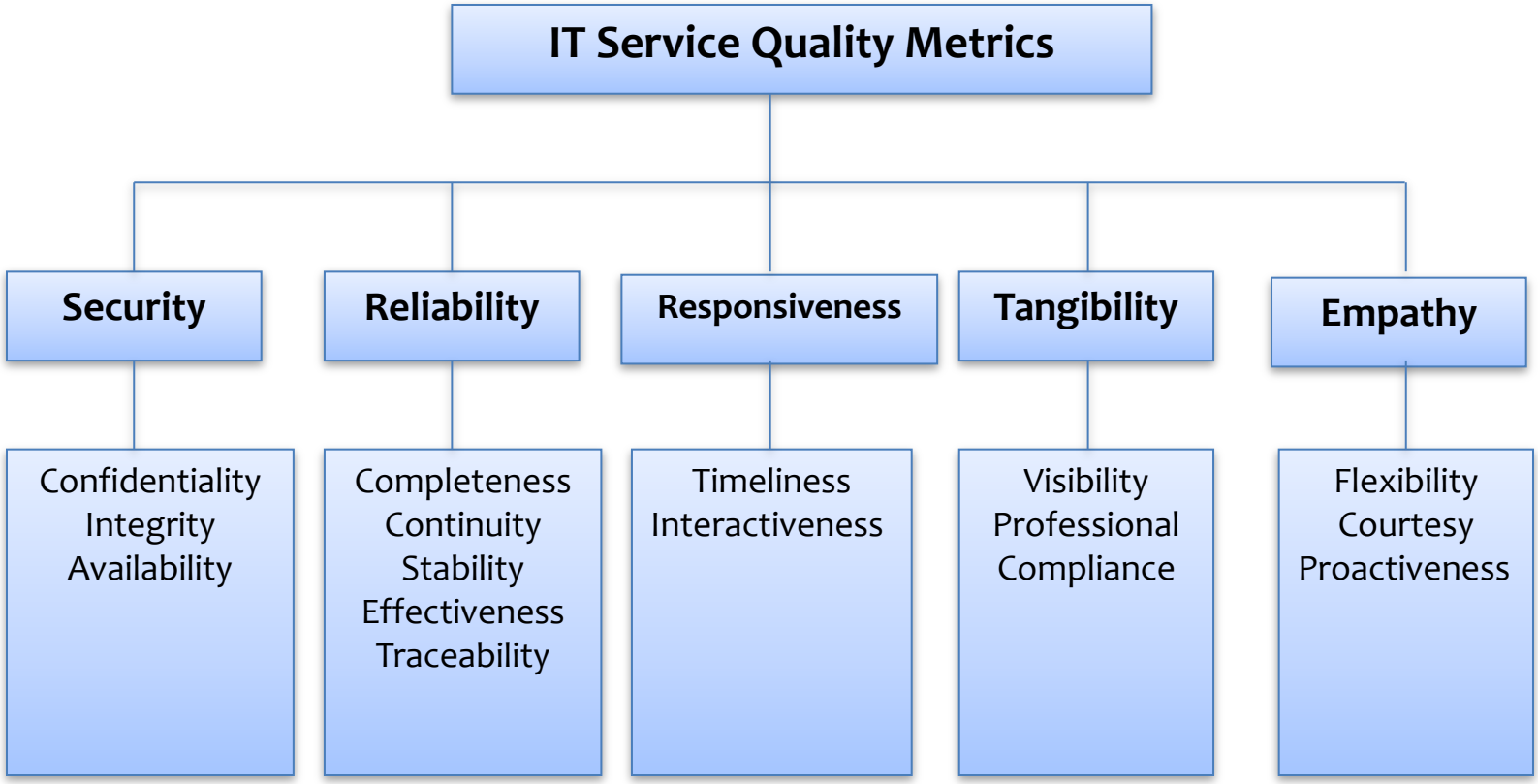
* Servizio: mezzo per fornire un valore per il cliente, facilitando i risultati che il cliente vuole raggiungere [ISO 20000]

* Servizio IT: servizio basato su applicazione IT che usa strumenti per sostenere le attività commerciali e amministrative dei clienti

* Qualità: totalità delle caratteristiche di un'entità che soddisfa la capacità di soddisfare esigenze esplicite o implicite [ISO 8402]

* Qualità Servizio IT: grado in cui le caratteristiche inerenti il servizio IT soddisfano le esigenze dell'utente

Detailed IT Service Quality Metrics (Draft © ISO)



Detailed IT Service Quality Metrics (Draft © ISO)

* Security
  * Confidentiality
  * Integrity
  * Availability
* Reliability
* Responsiveness
* Tangibility
* Empaty

Conclusione

Il concetto di sicurezza va esaminato da un punto di vista non solo del processo, ma anche del prodotto già trattato in diversi standard e linee guida tra cui:

* Linee guida dei siti web della PA
* Raccomandazioni sul Cloud computing nella PA
* ISO/IEC 25010 «Software and System quality model»
* ISO/IEC 25012 «Data quality Model»
* NWI ISO/IEC 25011 «IT Service quality model»