Certificazioni di sicurezza

Cesare Gallotti

Milano, 18 gennaio 2018

Cesare Gallotti

Agenda

- La certificazione dei sistemi di gestione per la sicurezza delle informazioni;
- La certificazione della sicurezza dei prodotti;
- La certificazione privacy;
- Gli organismi di certificazione.

Cesare Gallotti

- Lavora dal 1999 nel campo della sicurezza delle informazioni, della qualità e della gestione dei servizi IT.
- Ha condotto numerosi 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 e ISO 9001. Ha progettato ed erogato corsi di Quality Assurance e di certificazione Lead Auditor ISO/IEC 27001 e ITIL Foundation.
- Tra gli attestati di studio e i titoli professionali, si segnalano: le certificazioni CEPAS Lead Auditor ISO/IEC 27001, IRCA Lead Auditor 9001:2008, CISA, ITIL Expert e CBCI, la qualifica come Lead Auditor ISO/IEC 20000 e ISO 22301 e il perfezionamento postlaurea in "Computer Forensics e investigazioni digitali".
- E' capodelegazione del WG1 del comitato italiano ISO/IEC SC27 in UNINFO.
- Riferimenti:
  - Web: www.cesaregallotti.it
  - Blog: blog.cesaregallotti.it
  - Twitter: @cesaregallotti

Ma prima... cos'è una certificazione?

- In parole povere la certificazione funziona così:
  - qualcuno (ente di normazione) stabilisce dei requisiti per un'organizzazione o una persona o un prodotto o un servizio o un processo e li scrive in uno *standard di requisiti* o *specifica*;
  - qualcuno (auditor o gruppo di auditor) verifica che un'organizzazione o una persona o un prodotto o un servizio o un processo soddisfi i requisiti stabiliti;
  - se i requisiti sono soddisfatti è emesso un *certificato* con scritto: "l'organizzazione, la persona, ecc... soddisfa i requisiti specificati dal documento (o standard) X".
- Per molte certificazioni sono stati stabiliti dei meccanismi per assicurare che il processo (normazione, audit, certificazione) sia il più possibile oggettivo e affidabile (per esempio, chi stabilisce i requisiti, chi può condurre gli audit, chi verifica l'operato degli auditor, eccetera).

I sistemi di gestione per la sicurezza delle informazioni (ossia le certificazioni di sicurezza delle informazioni per le organizzazioni; ossia la ISO/IEC 27001)

Informazioni

- Informazione: conoscenza o dati che hanno significato e valore.
- Le informazioni possono esistere in molte forme. Possono essere stampate o scritte su carta, gestite con strumenti informatici, trasmesse via posta o con mezzi elettronici, presentate in film o fotografie o dette in conversazioni.
- Qual è la differenza tra dati e informazioni?
  - T. S. Eliot, The rock, 1934
  - Where is the wisdom we have lost in knowledge?
    Where is the knowledge we have lost in information?

Sicurezza delle informazioni

- Il mantenimento della loro (ISO/IEC 27000)
  - riservatezza (le informazioni non sono rese disponibili o note a individui, entità o processi non autorizzati);
  - integrità (accuratezza e completezza);
  - disponibilità (accessibilità e usabilità su richiesta di un'entità autorizzata, secondo i tempi previsti).
- Altre proprietà da preservare (normalmente incluse nella "integrità"):
  - efficacia (utilità per l'utilizzatore);
  - affidabilità (verità e credibilità; anche sinonimo di accuratezza);
  - autenticità (essere chi o cosa è dichiarato);
  - conformità (coerente con le normative e i regolamenti applicabili);
  - non ripudiabilità (capacità di provare che un evento o un'azione e le entità che lo hanno originato, se dichiarato è accaduto).

Sistema di gestione per la sicurezza delle informazioni

Il sistema di gestione per la sicurezza delle informazioni (SGSI) è quello « certificabile » ISO/IEC 27001.

Il SGSI è: parte del sistema di gestione complessivo per

- stabilire,
- attuare,
- monitorare,
- riesaminare,
- mantenere,
- migliorare

la sicurezza delle informazioni.

*Insieme di elementi **interrelati e interagenti** per **stabilire** obiettivi di sicurezza delle informazioni e **raggiungerli**.*

Sistema di gestione per la sicurezza delle informazioni

- Il sistema di gestione per la sicurezza delle informazioni (SGSI) è quello « certificabile » ISO/IEC 27001.
- Un sistema di gestione è: l'insieme di elementi interrelati e interagenti per stabilire obiettivi di sicurezza delle informazioni e raggiungerli.
- Il SGSI è la parte del sistema di gestione complessivo per
  - stabilire,
  - attuare,
  - monitorare,
  - riesaminare,
  - mantenere,
  - migliorare

  la sicurezza delle informazioni.

Due leggi di sicurezza delle informazioni

Principio di Schneier:

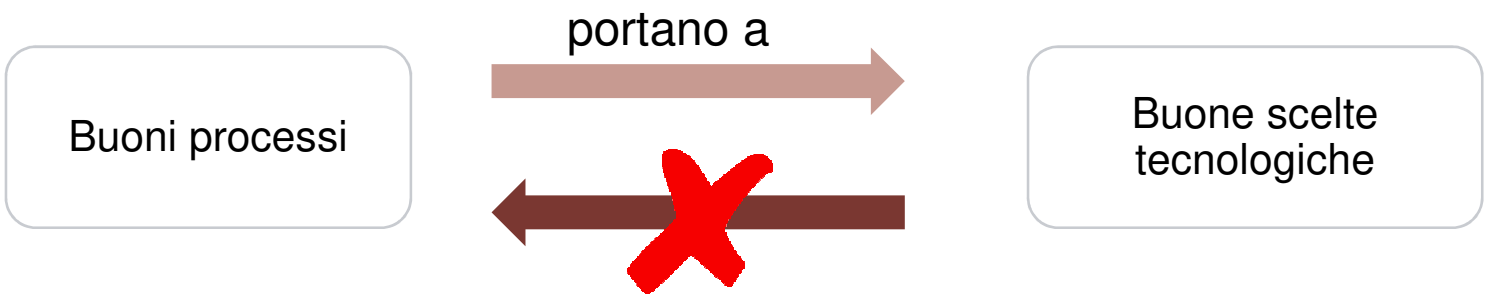
la sicurezza è una catena: è forte come il suo anello più debole.

Corollario di Mitnick:

l'anello più debole sono le persone

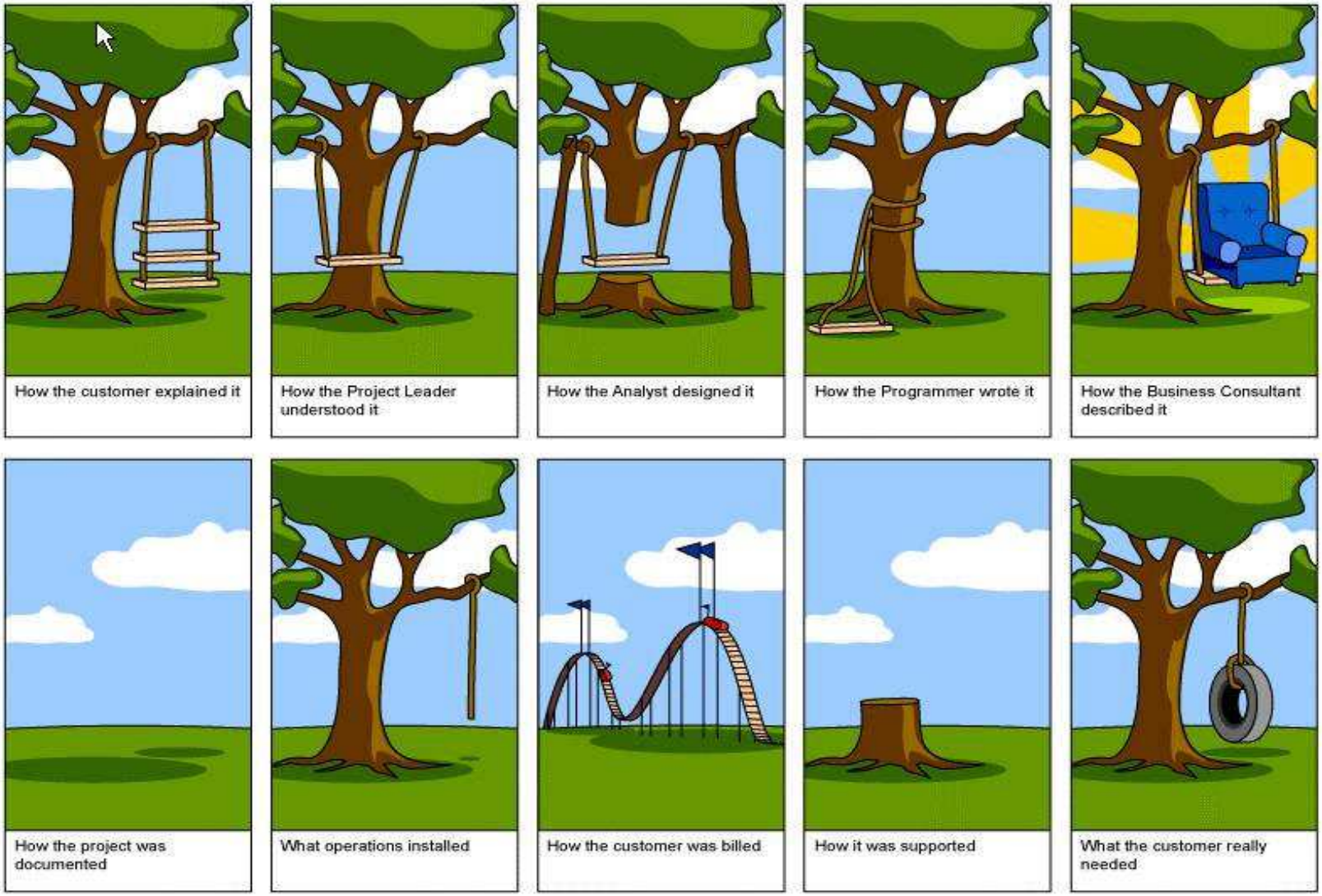
Sistema di gestione per la sicurezza delle informazioni

La sicurezza si basa sulla buona gestione



Processi per: scegliere, attuare, mantenere.

Processi per scegliere



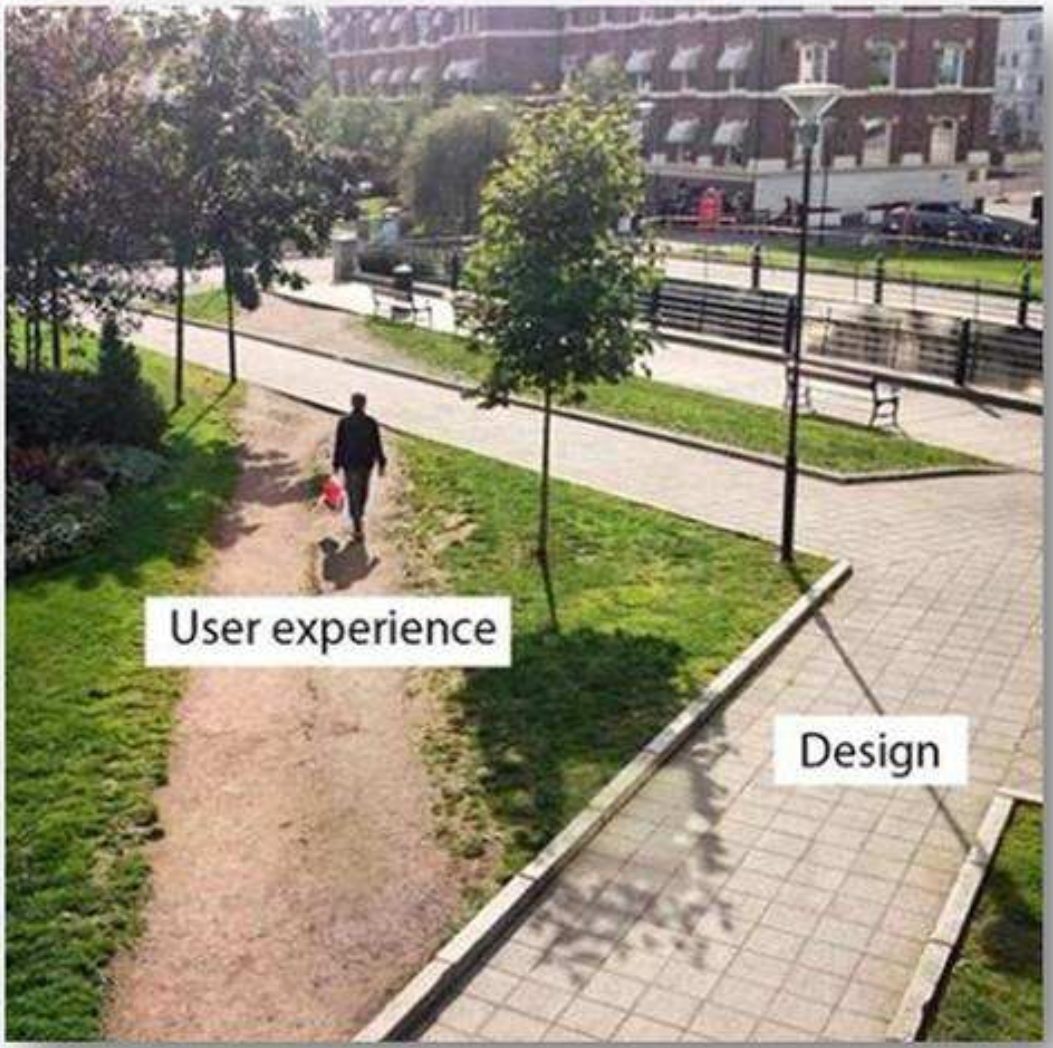
Processi per attuare

Prodotti comprati e mai usati

Ritardi (es. 1386-1965)

Processi per mantenere (1/2)

Processi per mantenere (2/2)



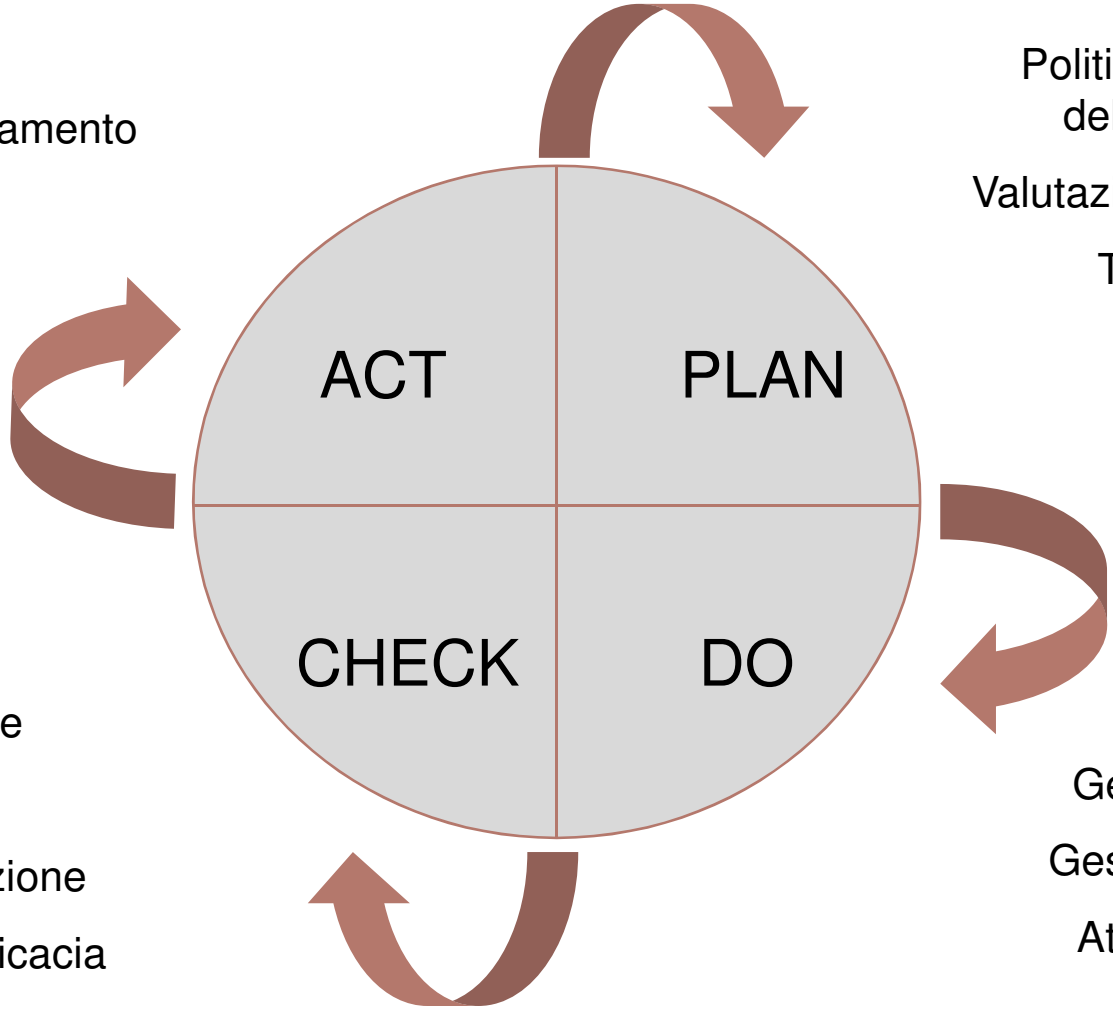
Ciclo PDCA e requisiti di sistema

Leadership

Azioni correttive

Azioni di miglioramento

Aggiornamenti



Politica di sicurezza delle informazioni

Valutazione del rischio

Trattamento del rischio

Verifiche tecniche

Audit interni

Riesame di direzione

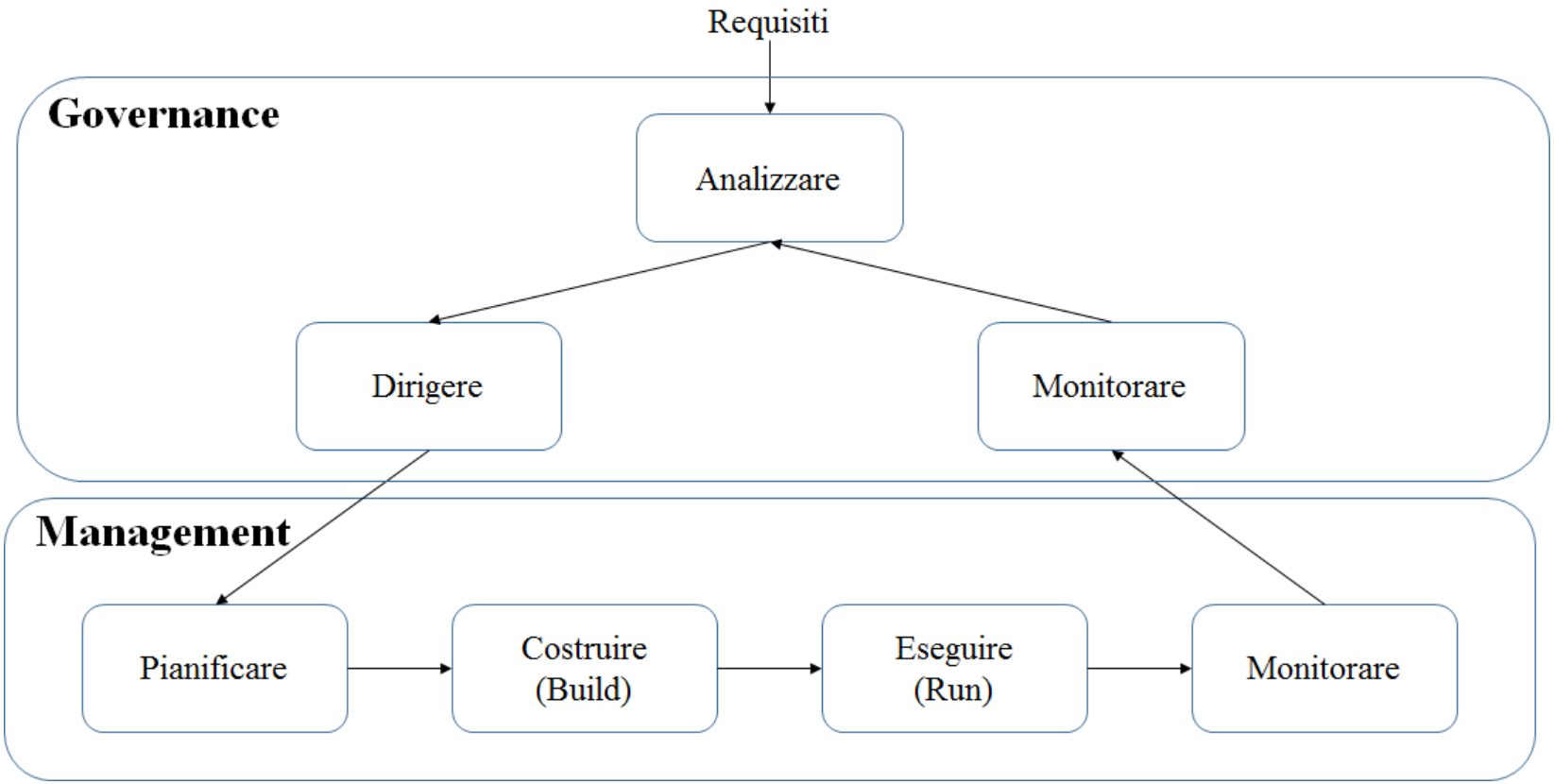
Valutazioni di efficacia

Gestire le risorse

Gestire documenti

Attuare i controlli

Governance

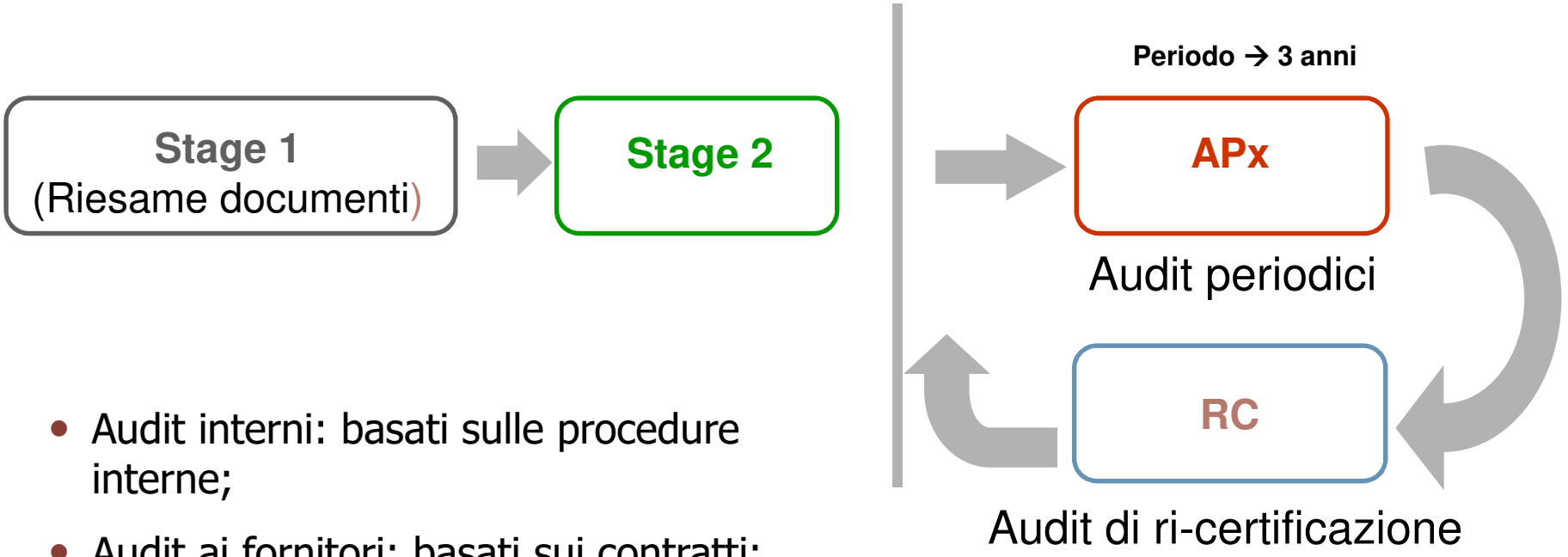


- Ma è possibile governare senza capire come si gestisce?

Le norme della serie ISO/IEC 27000

- ISO/IEC 27001 – Requisiti per un sistema di gestione per la sicurezza delle informazioni.
- ISO/IEC 27002 – Guida ai controlli di sicurezza delle informazioni.
- ISO/IEC 27000 - Termini e definizioni.
- ISO/IEC 27003 – Guida all'interpretazione.
- ISO/IEC 27004 – Monitoraggi e misurazioni.
- ISO/IEC 27005 – Gestione del rischio.
- ISO/IEC 27006 – Per gli Organismi di certificazione.
- Standard sector-specific:
  - ISO/IEC 27010 per le TLC;
  - ISO/IEC 27019 per il settore energy;
  - altri.

Processo di audit di certificazione



- Audit interni: basati sulle procedure interne;
- Audit ai fornitori: basati sui contratti;
- Audit di certificazione: basati su standard.

La certificazione della sicurezza dei prodotti

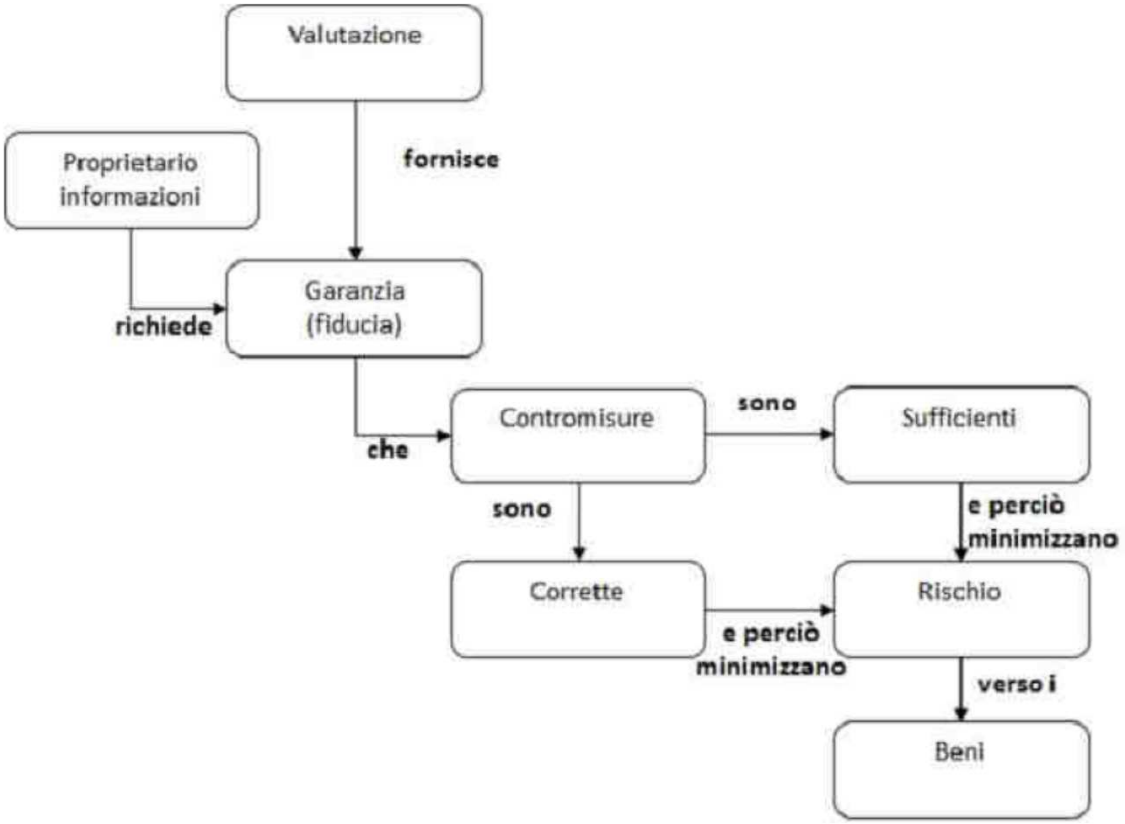
I Common Criteria

- Lo standard di riferimento per la certificazione dei prodotti è denominato " Common Criteria for Information Technology Security Evaluation".
- I Common Criteria sono stati recepiti a livello internazionale come ISO/IEC 15408.
- Lo standard prevede:
  - sette livelli di garanzia crescenti, da EAL1 (Evaluation Assurance Level) a EAL7;
  - livelli di garanzia dipendenti dall'estensione e formalità della documentazione usata in fase di analisi e sviluppo, nonché dalle modalità seguite nello sviluppo;
  - l'esecuzione di analisi tecniche e test:
  - tutti i livelli superiori al primo richiedono la collaborazione degli sviluppatori.
- Fino al livello EAL4 vi è un accordo sottoscritto da 26 Paesi, denominati CCRA (Common Criteria Recognition Agreement) per riconoscere mutuamente le certificazioni.

Qualche definizione

- Oggetto di Valutazione (OdV) o Target of Evaluation (TOE): prodotto o sistema da certificare;
- Protection Profile o Profilo di Protezione (PP): documento che riporta i requisiti di sicurezza per una tipologia di prodotti o sistemi.
  - Esempi sono i Protection Profile per firewall e database management system.
- Security Target (o Target di sicurezza o Traguardo di Sicurezza): documento relativo ad uno specifico OdV; può fare riferimento ad uno o più Protection Profile.

Concetti


Valutazione
fornisce
Proprietario informazioni
richiede
Garanzia (fiducia)
che
Contromisure
sono
Sufficienti
sono
e perciò minimizzano
Corrette
e perciò minimizzano
Rischio
verso i
Beni

Gli schemi di certificazione

- Uno schema è relativo ai prodotti e sistemi correlati alla sicurezza nazionale e alle informazioni classificate, regolato dal DPCM dell'11 aprile 2002.
- Uno schema è relativo alla sicurezza "commerciale" (richiamato anche dalle norme che regolamento la firma digitale e i dispositivi utilizzati per apporla sui documenti), regolato dal DPCM del 30 ottobre 2003.
  - vedere anche www.ocsi.isticom.it.

Qualche riflessione

- La certificazione di un prodotto o sistema richiede tempi lunghi e costi elevati.
- I prodotti certificati vanno usati nella configurazione prevista (che non sempre è quella predefinita e non sempre è adeguata alle esigenze dell'utilizzatore).
- Non sempre la certificazione riflette la complessità del prodotto (classico caso è la certificazione di Windows Server 2008 rispetto al PP CAPP, che non prevede attacchi da parte di malintenzionati).
- In Italia si ha più specializzazione nell'integrazione di prodotti e quindi in pochi potrebbero ottenere certificazioni superiori a EAL 3.

Certificazioni di prodotti specifici

- Per i prodotti crittografici è necessario fare riferimento alle FIPS 140-2.
- Le normative per i dispositivi medici (da marcare CE) richiedono anche la valutazione della sicurezza informatica.

La certificazione privacy

La certificazione privacy per il GDPR

- Considerando 100: Dovrebbe essere incoraggiata l'istituzione di meccanismi di certificazione e sigilli nonché marchi di protezione dei dati che consentano di valutare rapidamente il livello di protezione dei dati dei prodotti e servizi.
- Art. 42, par. 1: Incoraggiano l'istituzione di meccanismi di certificazione nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al GDPR dei trattamenti.
- Par. 5: La certificazione è rilasciata dagli OdC o dalla DPA competente in base ai criteri approvati dalla DPA o dal Board.
- Art. 43, par. 1: Gli organismi di certificazione sono accreditati da (opzione):
  - la DPA competente;
  - dall'organismo nazionale di accreditamento (regolamento CE n. 765/2008) secondo la EN ISO/IEC 17065:2012 (relativa ai prodotti, processi e servizi) e i requisiti aggiuntivi stabiliti dalla DPA competente.

NOTA: gli articoli del GDPR qui sono stati riassunti.

Dove è citata?

- Art. 24 par. 3: L'adesione ai codici di condotta o al meccanismo di certificazione **può** essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.
- Art. 25 par. 3: Il meccanismo di certificazione può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 [attuare in modo efficace i principi di protezione dei dati] e 2 [trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento] del presente articolo.
- Art. 28 par. 5: L'adesione da parte del responsabile del trattamento a un codice al meccanismo di certificazione può essere utilizzata come elemento per dimostrare le garanzie sufficienti.
- Art. 32 par. 3: L'adesione a un codice di condotta ol meccanismo di certificazione può essere utilizzata come elemento per dimostrare di garantire un livello di sicurezza adeguato al rischio.

NB: testo adattato.

Ma anche i codici di condotta

- Art. 40: Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici di condotta.
- Art. 41 (par. 1): il controllo della conformità con un codice di condotta può essere effettuato da un organismo in possesso del livello adeguato di competenze riguardo al contenuto del codice e del necessario accreditamento a tal fine dell'autorità di controllo competente.
- Art. 41 (par. 3): L'autorità di controllo competente presenta al comitato il progetto di criteri per l'accreditamento dell'organismo.
- Art 41 (par. 4): un organismo adotta le opportune misure in caso di violazione del codice da parte di un titolare del trattamento o responsabile del trattamento. Esso informa l'autorità di controllo competente di tali misure e dei motivi della loro adozione.

Riflessioni sui codici di condotta

- Sono in corso analisi dei progetti di accreditamento dei soggetti che dovrebbero controllare l'adozione di codici di condotta?
- Conviene, ad un'organizzazione, che l'organismo di controllo informi il Garante per la privacy in caso di non conformità?

Le certificazioni delle persone?

- La posizione più comune è che gli articoli del GDPR relativi alla certificazione non includono le persone.
- In Spagna è stato pubblicato a luglio 2017 uno schema relativo al profilo del DPO.
- In Italia nel 2017 è stata pubblicata la UNI 11697 dal titolo “Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza".

Cos’è un trattamento?

- Un trattamento è un:
  - prodotto;
  - processo;
  - servizio?
- Dal considerando 100, si deduce che è un servizio.

Esempi di certificazione di servizio

- Centri di contatto multicanale (norme EN 15838:2010 e UNI 11200:2010)
  - Regolamento Accredia RT-22;
  - la EN 15838 include il ciclo PDCA (strategia, attività operative, riesami periodici, gestione del miglioramento);
- Erogazione di corsi di formazione;
- Vigilanza (norma UNI 10891);
- Centri di monitoraggio e ricezione allarmi (EN 50518 e UNI 11068);
- Fornitori di servizi eIDAS;
  - i requisiti consigliano l'adozione della ISO/IEC 27001;
- Fornitori di servizi di conservazione "a norma" (richiesta la certificazione ISO/IEC 27001);
- Fornitori di servizi SPID (richiesta la certificazione ISO/IEC 27001).

Esempi di certificazione di prodotto

- Attualmente "lo" schema di certificazione della sicurezza dei prodotti informatici è costituito dalla ISO/IEC 15408 (Common Criteria);
  - richiede l'attuazione di processi molto simili (e forse più rigorosi) di quelli richiesti dai sistemi di gestione per la qualità.
- Gli schemi di certificazione di prodotto sono tanti, tra cui:
  - Regolamento Reg. CE 303/2008 (apparecchiature con gas fluorurati);
  - Direttiva PED (per i recipienti in pressione);
  - Direttiva MED (dispositivi medici).
- In molti casi è richiesto un sistema di gestione (per la qualità), anche se non necessariamente certificato.

La certificazione

- Alcuni schemi di certificazione di prodotti, processi o servizi possono comprendere
  - prove iniziali;
  - ispezioni;
  - valutazione dei sistemi di gestione per la qualità, seguite dalla sorveglianza che tiene conto del SGQ e delle prove o ispezioni su campioni prelevati dalla produzione e dal libero mercato.
  - prove iniziali e prove di sorveglianza;
  - solo prove di tipo.

Iniziative italiane

- Il 18 ottobre è stato attivato un gruppo di lavoro per la redazione di una "Prassi di riferimento UNI" dal titolo "Linee guida per la gestione dei dati personali in ambito ICT secondo il Regolamento europeo EU 679/2016 (GDPR)
  - non uno standard di requisiti certificabili;
  - solo per l'ICT (comunque molto importante);
  - comunque un punto di riferimento;
  - prevista la pubblicazione per aprile 2018.
- La norma UNI 11697 del 2017, "Profili professionali relativi al trattamento e alla protezione dei dati personali";
  - riguarda DPO, Manager privacy, Specialista privacy, Valutatore privacy;
  - alcuni registri stanno promuovendo schemi di certificazione professionali basati sulle bozze di questa norma (non ancora disponibili gli accreditamenti).

Previsioni (personali) sulle certificazioni privacy (1/2)

- Non risultano allo studio delle DPA degli schemi condivisi per i servizi.
- C'è interesse sulla ISO/IEC 27552 (estensione della ISO/IEC 27001), ma sarà forse pubblicata solo a fine 2019;
  - si potrebbe trovare una via per cui una norma relativa ai sistemi di gestione possa essere trattata come relativa a servizi;
  - è comunque necessario non prevedere la certificazione come relativa al solo trattamento, ma con impatti su tutta l'organizzazione del titolare o del *processor*.
- Sicuramente alcuni enti promuovono schemi "proprietari" non promossi da alcuna DPA (non secondo criteri approvati da alcuna DPA);
  - vedere anche il comunicato GPD e Accredia del 19 luglio 2017: *in Italia non è ancora stato stabilito dal Legislatore nazionale a chi spetti il ruolo di ente di accreditamento ai fini del regolamento, né sono stati definiti i "requisiti aggiuntivi" per l'accreditamento degli organismi di certificazione.*

Previsioni (personali) sulle certificazioni privacy (2/2)

- Alcuni schemi sono promossi solo da una DPA (e quindi con valore reale solo in un Paese);
  - Label CNIL (dal 2011; 12 per la label Gouvernance e 1 per la label relativa ai servizi);
  - EuroPriSe (dal 2008, meno di 50 "seals" per prodotti, servizi, siti web);
  - ePrivacy Seal (dal 2011, circa 200 "seals" per prodotti).
- Gli schemi per la certificazione di prodotti;
  - solitamente sono molto complessi da realizzare in ambito IT e molto onerosi da certificare;
  - forse alcuni schemi nazionali, meno onerosi dei Common Criteria, si imporranno sul mercato europeo generale.
- Troppi faranno pressioni perché uno schema di "certificazione privacy" sia approvato, ma alcune strade sono percorribili già oggi:
  - prevedere audit condotti da persone competenti (non necessariamente di OdC);
  - pubblicizzare le misure di sicurezza adottate.

Gli organismi di certificazione

Gli attori

- Gli enti di normazione (quelli ufficiali sono regolamentati dal Regolamento europeo 1025/2012) emettono norme;
  - possono essere enti nazionali (UNI e UNINFO, BSI, DIN, eccetera);
  - possono essere enti internazionali (CEN, ISO, IEC);
  - possono essere enti privati (tutti possono scrivere norme!);
- Gli organismi di accreditamento sorvegliano le attività di certificazione;
  - accreditano (e verificano) gli organismi di certificazione secondo norme specifiche;
  - si riconoscono mutualmente;
  - in Europa rispondono al Regolamento europeo 765/2008.
- Gli organismi di certificazione;
  - certificano le organizzazioni o i prodotti, processi e servizi;
  - selezionano gli auditor;
- Le organizzazioni... si vorrebbero certificare;
  - la certificazione deve avvenire rispetto a norme specifiche.

Gli organismi di certificazione

- Sono stabilite regole per gli OdC. Per esempio in merito a:
  - modalità di conduzione degli audit;
  - verifiche sulla conduzione degli audit;
  - mantenimento dei certificati (sorveglianza, verifiche in occasione di modifiche);
  - gestione dei reclami;
  - trasparenza e imparzialità;
  - competenze del personale.

Regolamenti

- Gli Organismi di accreditamento (soprattutto in Italia!) pubblicano requisiti ulteriori a quelli delle norme ISO per gli OdC.
- Gli Organismi di certificazione devono pubblicare un regolamento relativo alle attività di certificazione dei prodotti, processi e servizi.
- Il regolamento dettaglia alcuni processi generali (p.e. gestione dei reclami dei clienti).
- Il regolamento dettaglia come sono svolti gli audit:
  - numero e tipo di verifiche di certificazione, sorveglianza e ri-certificazione;
  - modalità di condivisione del rapporto;
  - tipo di rilievi (classificazione delle non conformità) e loro gestione (p.e. a fronte di non conformità gravi è necessario un audit straordinario entro poche settimane).

FINE

Diverse indicazioni sono state raccolte dal Webinar

“Aggiornamento sulle certificazioni collegate al GDPR"

di Fabio Guasconi (Bl4ckSwan S.r.l.)

messo a disposizione da gli Osservatori Digital Innovation del Politecnico di Milano e il Clusit (Associazione Italiana per la Sicurezza Informatica).

Gli errori sono di Cesare Gallotti