Corso di alta formazione sulla protezione dei dati personali

Responsabile della protezione dei dati (DPO)

Normative tecniche internazionali sulla sicurezza

Sistemi di gestione per la sicurezza delle informazioni:
ISO 27001:2013

Information security management systems

Ing. Andrea Cenni
Auditor ISDP 10003 - Protezione Dati Personali
Valutatore Privacy Uni 11697
andrea.cenni@studioingcenni.it | 328.7230906

Regolamento UE 679/2016 – Articolo 42
(«certificazione» - considerando 100)

1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di **certificazione della protezione dei dati** nonché di sigilli e marchi di protezione dei dati allo scopo di **dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento.** Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese.

Regolamento UE 679/2016 – Articolo 42

2. Oltre all'adesione dei titolari del trattamento o dei responsabili del trattamento soggetti al presente regolamento, i meccanismi, i sigilli o i marchi approvati ai sensi del paragrafo 5 del presente articolo, possono essere istituiti al fine di dimostrare la previsione di garanzie appropriate da parte dei titolari del trattamento o responsabili del trattamento non soggetti al presente regolamento ai sensi dell'articolo 3, nel quadro **dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali** alle condizioni di cui all'articolo 46, paragrafo 2, lettera f). Detti titolari del trattamento o responsabili del trattamento assumono l'impegno vincolante e azionabile, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati.

Regolamento UE 679/2016 – Articolo 42

3. La certificazione **è volontaria** e accessibile tramite una procedura **trasparente**.
4. La certificazione ai sensi del presente articolo **non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento** e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti a norma degli articoli 55 o 56.

Regolamento UE 679/2016 – Articolo 42

5. La certificazione ai sensi del presente articolo è rilasciata **dagli organismi di certificazione di cui all'articolo 43** o dall'autorità di controllo competente in base ai criteri approvati da tale autorità di controllo competente ai sensi dell'articolo 58, paragrafo 3, o dal comitato, ai sensi dell'articolo 63. Ove i criteri siano approvati dal comitato, ciò può risultare in una certificazione comune, il sigillo europeo per la protezione dei dati.

Regolamento UE 679/2016 – Articolo 42

6. Il titolare del trattamento o il responsabile del trattamento che sottopone il trattamento effettuato al meccanismo di certificazione **fornisce all'organismo di certificazione di cui all'articolo 43** o, ove applicabile, all'autorità di controllo competente **tutte le informazioni e l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione**.

Regolamento UE 679/2016 – Articolo 42

7. La certificazione è rilasciata al titolare del trattamento o responsabile del trattamento **per un periodo massimo di tre anni e può essere rinnovata alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti**. La certificazione è revocata, se del caso, dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente, a seconda dei casi, qualora non siano o non siano più soddisfatti i requisiti per la certificazione.
8. Il comitato raccoglie in un registro tutti i meccanismi di certificazione e i sigilli e i marchi di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato.

Regolamento UE 679/2016 – Articolo 43
(«Organismi di certificazione» – considerando da 166 a 168)

1. Fatti salvi i compiti e i poteri dell'autorità di controllo competente di cui agli articoli 57 e 58, gli organismi di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati, rilasciano e rinnovano la certificazione, dopo averne informato l'autorità di controllo al fine di consentire alla stessa di esercitare i suoi poteri a norma dell'articolo 58, paragrafo 2, lettera h), ove necessario. Gli Stati membri garantiscono che tali organismi di certificazione siano accreditati da uno o entrambi dei seguenti organismi:
   a) dall'autorità di controllo competente ai sensi degli articoli 55 o 56;
   b) dall'organismo nazionale di accreditamento designato in virtù **del regolamento (CE) n. 765/2008** del Parlamento europeo e del Consiglio (20) conformemente alla norma **ENISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente** ai sensi degli articoli 55 o 56.2.

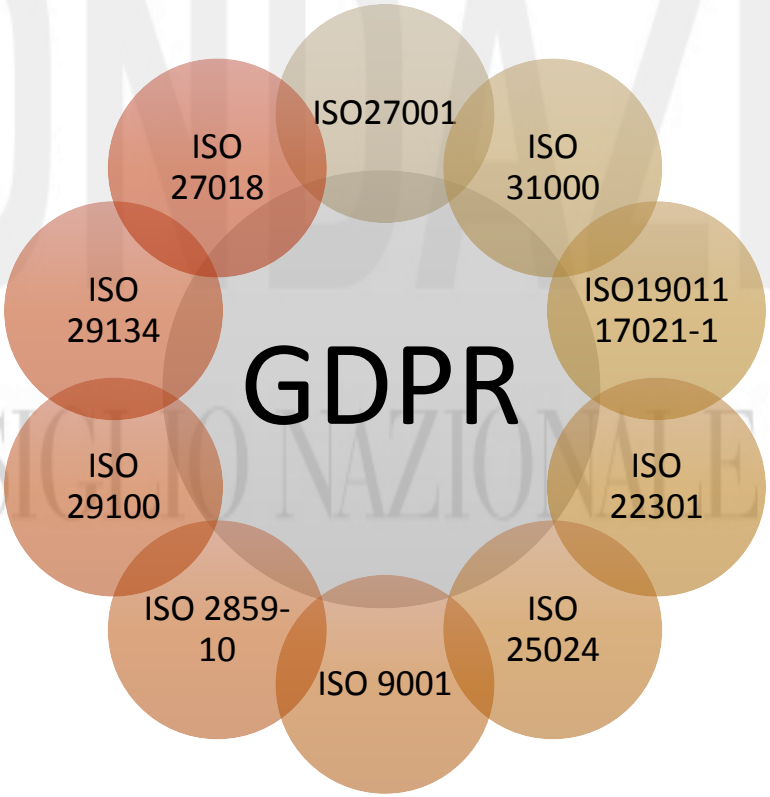
[…]

Regolamento UE 679/2016 – Articoli 42 e 43

- Quale certificazione? → **certificazione di processo/prodotto/servizio** secondo ISO 17065 NON di gestione (ISO 17021-1).
- Rispetto a quale norma o specifica? → **ACCREDIA + requisiti aggiuntivi AUTORITÀ GARANTE** (*"The Article 29 Working Party welcomes comments on the Guidelines on the accreditation of certification bodies (wp261). Such comments should be sent to the following address by 30 March 2018 at the latest".* http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614486).
- Cosa si certifica? La protezione dei dati trattati o il rispetto dell'intero Regolamento? → **la conformità al Regolamento. La conformità NON è un processo statico MA dinamico** (GDPR, art. 5(2): *"Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione») "*). Nel testo inglese: *"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."*

Nell'attesa …

Standard ISO utili alla compliance al GDPR



ISO 17065:2012

Requisiti per organismi che certificano prodotti, processi e servizi

SCOPO E CAMPO DI APPLICAZIONE

- La presente norma internazionale contiene requisiti per la competenza, il funzionamento coerente e l'imparzialità degli organismi di certificazione di prodotti, processi e servizi.
- Non è necessario che gli organismi di certificazione che operano in conformità alla presente norma internazionale offrano la certificazione di tutti i tipi di prodotti, processi e servizi.
- La certificazione di prodotti, processi e servizi è un'attività di valutazione di terza parte.
- Nella presente norma internazionale il termine "prodotto" può essere inteso come "processo" o "servizio", eccetto in quei casi ove vengano stabilite disposizioni distinte per "processi" o "servizi".

ISO 31000:2010

Gestione del rischio

SCOPO E CAMPO DI APPLICAZIONE

- La presente norma internazionale fornisce principi e linee guida generali sulla gestione del rischio.
- La presente norma internazionale può essere utilizzata da qualsiasi impresa pubblica, privata o sociale, associazione, gruppo o individuo e, pertanto, non è specifica per alcuna industria o settore.
- La presente norma internazionale può essere applicata lungo l'intera vita di un'organizzazione e ad un'ampia gamma di attività, incluse strategie e decisioni, operazioni, processi, funzioni, progetti, prodotti, servizi e beni.
- La presente norma internazionale può essere applicata a qualsiasi tipo di rischio, quale sia la sua natura, sia che essi abbiano conseguenze positive o negative.
- Sebbene la presente norma internazionale fornisca linee guida di applicazione generale, essa non intende promuovere l'uniformità della gestione del rischio tra le organizzazioni. La progettazione e l'attuazione di piani e strutture di riferimento di gestione del rischio richiedono di prendere in considerazione le differenti esigenze di una specifica organizzazione, i suoi particolari obiettivi, contesto, struttura, operazioni, processi, funzioni, progetti, prodotti, servizi, o beni e le specifiche prassi adottate.
- Tra gli scopi della presente norma internazionale vi è quello di essere utilizzata per armonizzare i processi della gestione del rischio nelle norme attuali e future. Essa fornisce un approccio comune a supporto di norme che riguardano rischi e/o settori specifici e non sostituisce tali norme.
- La presente norma internazionale non è destinata ad essere utilizzata a scopo di certificazione.

ISO 27001:2014

Sicurezza delle informazioni

SCOPO E CAMPO DI APPLICAZIONE

Generalità

- La presente norma internazionale è applicabile a tutte le tipologie di organizzazioni (per esempio, imprese commerciali, agenzie governative, organizzazioni senza scopo di lucro).
- La presente norma internazionale specifica i requisiti per stabilire, attuare, condurre, monitorare, riesaminare, mantenere attivo, aggiornato e migliorare un SGSI documentato all'interno di un contesto di rischi relativi al business complessivo dell'organizzazione. Essa specifica, inoltre, i requisiti per la realizzazione di controlli per la sicurezza personalizzati in base alle esigenze di singole organizzazioni o di parti delle medesime.
- Il SGSI è progettato per assicurare la selezione di controlli per la sicurezza adeguati e proporzionati, in grado di proteggere i beni informativi e dare fiducia alle parti interessate

Nota

- La ISO/IEC 17799 fornisce linee guida per l'attuazione che possono essere utilizzate nella progettazione dei controlli

ISO 27001:2014

Applicazione

- I requisiti specificati nella presente norma internazionale sono di carattere generale e predisposti per essere applicabili a tutte le organizzazioni, indipendentemente dalla tipologia, dimensione e natura. L'esclusione di qualunque requisito specificato nei punti 4, 5, 6, 7 e 8 non è accettabile se un'organizzazione vuole dichiarare la sua conformità alla presente norma internazionale.
- Qualsiasi esclusione dei controlli che si ritengano necessari a soddisfare i criteri di accettazione dei rischi necessita di essere giustificata e deve essere fornita evidenza che i rischi associati siano stati accettati dalle persone responsabili. Nel caso vengano esclusi alcuni controlli, le dichiarazioni di conformità alla presente norma non sono accettabili a meno che tali esclusioni siano ininfluenti verso la capacità e/o la responsabilità
- dell'organizzazione di fornire la sicurezza delle informazioni che soddisfi i requisiti di sicurezza stabiliti mediante la valutazione del rischio e le prescrizioni legali o regolamentari applicabili.

Nota

- Se un'organizzazione ha già operativo un sistema di gestione dei processi aziendali (per esempio riconducibile alla ISO 9001 o alla ISO 14001), nella maggior parte dei casi è preferibile soddisfare i requisiti della presente norma internazionale all'interno di tale preesistente sistema di gestione

ISO 19011:2012

- **Linee guida per audit di sistemi di gestione**
- **SCOPO E CAMPO DI APPLICAZIONE**

- La presente norma internazionale fornisce una guida sull'attività di audit di sistemi di gestione, compresi i principi dell'attività di audit, la gestione di un programma di audit e la conduzione degli audit di sistemi di gestione, così come una guida per la valutazione della competenza delle persone coinvolte nel processo di audit, inclusi il responsabile della gestione del programma di audit, gli auditor e i gruppi di audit.

ISO 17021-1:2015

Requisiti per gli organismi che forniscono audit e certificazione di sistemi di gestione

Parte 1: Requisiti

SCOPO E CAMPO DI APPLICAZIONE

- La presente parte della ISO/IEC 17021 contiene i principi ed i requisiti per la competenza, la coerenza e l'imparzialità degli organismi che forniscono audit e certificazione di tutti i tipi di sistemi di gestione.
- Gli organismi di certificazione, operanti secondo la presente parte della ISO/IEC 17021, non sono tenuti ad offrire tutti i tipi di certificazione di sistemi di gestione.
- La certificazione di sistemi di gestione è un'attività di valutazione della conformità di terza parte (vedere ISO/IEC 17000:2004, punto 5.5) e gli organismi che eseguono tale attività sono dunque organismi di valutazione della conformità di terza parte.

Nota

Esempi di gestione comprendono i sistemi di gestione ambientale, i sistemi di gestione per la qualità e i sistemi di gestione della sicurezza delle informazioni.

ISO 2859-10:2007

Procedimenti di campionamento nell'ispezione per attributi

Parte 10: Introduzione alla serie di norme ISO 2859 per il campionamento nell'ispezione per attributi

SCOPO E CAMPO DI APPLICAZIONE

- La presente parte della serie ISO 2859 fornisce una introduzione generale al campionamento per accettazione per attributi e un breve riassunto degli schemi e dei piani di campionamento per attributi utilizzati nelle ISO 2859-1, ISO 2859-2, ISO 2859-3, ISO 2859-4 ed ISO 2859-5, che descrivono specifiche tipologie di sistemi di campionamento per attributi.
- La norma fornisce inoltre una guida alla selezione del sistema d'ispezione appropriato da utilizzare in situazioni particolari

ISO 9001:2015

Gestione qualità

SCOPO E CAMPO DI APPLICAZIONE

Generalità

- La presente norma internazionale specifica i requisiti di un sistema di gestione per la qualità per un'organizzazione che:
  a) ha l'esigenza di dimostrare la propria capacità di fornire con regolarità un prodotto che soddisfi i requisiti del cliente e quelli cogenti applicabili;
  b) desidera accrescere la soddisfazione del cliente tramite l'applicazione efficace del sistema, compresi i processi per migliorare in continuo il sistema ed assicurare la conformità ai requisiti del cliente ed a quelli cogenti applicabili.

Nota

- Nella presente norma internazionale, il termine "prodotto" si applica solamente:
  a) al prodotto destinato al cliente o da esso richiesto;
  b) a qualunque elemento voluto risultante dai processi di realizzazione del prodotto.

Applicazione

- Tutti i requisiti della presente norma internazionale sono di carattere generale e previsti per essere applicabili a tutte le organizzazioni, indipendentemente da tipo, dimensione e prodotto fornito.
- Qualora alcuni requisiti della presente norma internazionale non possano essere applicati a causa della natura di un'organizzazione e del suo prodotto, può essere presa in considerazione la possibilità di una loro esclusione.

ISO 27018: 2014 (documento non ufficiale)

Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

- ISO 27018 è il primo standard a livello internazionale per garantire il rispetto dei principi e delle norme privacy, da parte dei providers di public cloud che se ne dotano: la norma, infatti, è specificamente indirizzata ai service providers di public cloud che elaborano dati personali (PII - Personally Identifiable Information) e che agiscano in qualità di Data (PII) Processor. Definisce delle linee guida basate su ISO / IEC 27002, prendendo in considerazione i requisiti normativi per la protezione dei dati personali che possono essere applicabili nel contesto del panorama dei rischi di sicurezza informatica di un fornitore di servizi public cloud. Trattandosi di Linee guida, la norma ISO27018 non è quindi una norma certificabile: è possibile ottenere un "Certificato di Conformità" rilasciato da un Ente Certificatore riconosciuto, a dimostrazione della capacità del Provider di assicurare la protezione dei dati personali. La norma si basa e rinforza i precedenti standard ISO/IEC 27001 e ISO/IEC 27002 in materia di Gestione della Sicurezza delle Informazioni, e stabilisce obiettivi di controllo, regole e procedure per implementare misure di protezione dei dati personali (PII) in conformità con i principi di privacy di ISO / IEC 29100, per i fornitori di servizi cloud. Ciò allo scopo di accrescere la fiducia verso i fornitori di cloud pubblico, fornendo indicazioni sugli obiettivi da raggiungere in termini di obblighi contrattuali e normativi, consentendo inoltre ai clienti di soddisfare i propri obblighi normativi sulla sicurezza dei dati.

ISO 27018: 2014 (documento non ufficiale)

Scopo

- Questo standard internazionale stabilisce obiettivi, controlli e linee guida di controllo comunemente accettati per l'attuazione di misure per proteggere le informazioni personali identificabili (PII) in conformità con i principi di riservatezza in ISO / IEC 29100 per l'ambiente pubblico di cloud computing.
- In particolare, questo standard internazionale specifica le linee guida basate su ISO / IEC 27002, prendendo in considerazione i requisiti normativi per la protezione delle PII che potrebbero essere applicabili all'interno del contesto degli ambienti a rischio per la sicurezza delle informazioni di un fornitore di servizi cloud pubblici.
- Questo standard internazionale è applicabile a tutti i tipi e dimensioni di organizzazioni, tra cui pubblico e società private, enti governativi e organizzazioni senza scopo di lucro che forniscono informazioni servizi di elaborazione come processori PII tramite cloud computing sotto contratto con altre organizzazioni.
- Le linee guida in questo Standard Internazionale potrebbero anche essere rilevanti per le organizzazioni che agiscono come PII controller; tuttavia, i PII controller potrebbero essere soggetti a ulteriori normative sulla protezione PII e obblighi, non applicabili ai processori PII. Questo standard internazionale non è destinato a coprire tali obblighi aggiuntivi.

ISO 22301:2014 (documento non ufficiale)

Societal security -- Business continuity management systems --- Requirements

- Lo standard ISO 22301 (Societal security — Business continuity management systems — Requirements) specifica i requisiti per progettare, implementare e gestire efficacemente un Sistema di gestione della continuità operativa. Il sistema di gestione della continuità operativa (business continuity management system o BCMS) enfatizza l'importanza di: comprendere le esigenze dell'organizzazione e le necessità per stabilire la politica e gli obiettivi di un sistema di gestione per la continuità del business; implementare e rendere operativi controlli e misure per gestire la capacità di un'intera organizzazione nella gestione delle interruzioni dell'operatività dovute a cause accidentali; monitorare e riesaminare le prestazioni e l'efficacia del sistema di gestione della continuità operativa del miglioramento continuo del BCMS basato su obiettivi misurabili. Si noti che anche la norma ISO/IEC 27031 "Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity" tratta la business continuity, ma nel contesto dell'ICT e delle tecniche di sicurezza strettamente correlata alla ISO 27001 che contiene i requisiti per la certificazione dei sistemi di gestione della sicurezza delle informazioni. La ISO 22301 evidenzia i componenti chiave del sistema di gestione della continuità operativa, peraltro presenti anche in altri sistemi di gestione. Tra essi la politica, le persone con le loro responsabilità definite, la gestione dei processi correlati a politica, pianificazione, attuazione ed operatività del BCMS, valutazione delle prestazioni, riesame della direzione e miglioramento, nonché la documentazione in grado di fornire evidenze verificabili tramite audit sul sistema di gestione della continuità operativa.

ISO 22301:2014 (documento non ufficiale)

Scopo

- Questo standard internazionale per la gestione della continuità operativa specifica i requisiti per pianificare, stabilire, implementare, operare, monitorare, rivedere, mantenere e migliorare continuamente un sistema di gestione documentato per proteggersi, ridurre la probabilità di insorgenza, prepararsi, rispondere e riprendersi dal disturbo di incidenti quando si presentano.
- I requisiti specificati nella presente norma internazionale sono generici e destinati a essere applicabili a tutte le organizzazioni, o parti di esse, indipendentemente dal tipo, dimensione e natura dell'organizzazione. L'estensione dell'applicazione di questi requisiti dipende dall'ambiente operativo e dalla complessità dell'organizzazione.
- Non è l'intento di questo standard internazionale implicare l'uniformità nella struttura di una business continuity management system (BCMS), ma per un'organizzazione che progetta una BCMS adeguata alle sue esigenze e che soddisfa i requisiti delle parti interessate. Questi bisogni sono modellati dal punto di vista legale, normativo, organizzativo e requisiti del settore, i prodotti e servizi, i processi impiegati, le dimensioni e la struttura dell'organizzazione e le esigenze delle parti interessate.
- Questo standard internazionale è applicabile a tutti i tipi e dimensioni di organizzazioni che lo desiderano
  - a) stabilire, attuare, mantenere e migliorare un BCMS,
  - b) garantire la conformità con la politica di continuità operativa dichiarata,
  - c) dimostrare la conformità agli altri,
  - d) richiedere la certificazione / registrazione del proprio BCMS da parte di un ente di certificazione di terze parti accreditato, o
  - e) effettuare un'autodeterminazione e un'autodichiarazione di conformità a questo standard internazionale.
- Questo standard internazionale può essere utilizzato per valutare la capacità di un'organizzazione di soddisfare le proprie esigenze di continuità e obblighi.

ISO 29100:2011

Information technology -- Security techniques -- Privacy framework

Scopo

- Questo standard internazionale fornisce un quadro sulla privacy che:
  a) specifica una terminologia sulla privacy comune;
  b) definisce gli attori e il loro ruolo nel trattamento delle informazioni personali identificabili (PII);
  c) descrive le considerazioni sulla tutela della privacy; e
  d) fornisce riferimenti a principi noti sulla privacy per la tecnologia dell'informazione.
- Questo standard internazionale è applicabile alle persone fisiche e alle organizzazioni coinvolte nella specificazione, procurare, progettare, progettare, sviluppare, testare, mantenere, amministrare e operare sistemi o servizi di tecnologia dell'informazione e della comunicazione in cui sono richiesti controlli sulla privacy per l'elaborazione delle PII.

ISO 29134:2017

Information technology -- Security techniques -- Guidelines for privacy impact assessment

Scopo

- Questo documento fornisce linee guida per
  a) un processo sulle valutazioni dell'impatto sulla privacy, e
  b) una struttura e il contenuto di un report PIA.
- È applicabile a tutti i tipi e dimensioni di organizzazioni, comprese le società pubbliche, le società private, enti governativi e organizzazioni senza scopo di lucro.
- Questo documento è rilevante per coloro che sono coinvolti nella progettazione o realizzazione di progetti, comprese le parti di sistemi operativi di elaborazione dati e servizi che elaborano le PII.

ISO 25024:2015

Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Measurement of data quality

- Questo standard internazionale definisce le misure di qualità dei dati per misurare quantitativamente i dati qualità in termini di caratteristiche definite in ISO / IEC 25012.
- Questo standard internazionale contiene quanto segue:
  a) un insieme di base di misure sulla qualità dei dati per ciascuna caratteristica;
  b) un insieme di base di entità bersaglio a cui sono applicate le misure di qualità durante il ciclo di vita dei dati;
  c) una spiegazione di come applicare le misure di qualità dei dati;
  d) una guida per le organizzazioni che definiscono le proprie misure per i requisiti di qualità dei dati e la valutazione.
- Comprende, come allegati informativi, una tavola sinottica di elementi di misura di qualità definiti in questo Standard internazionale (allegato A), una tabella delle misure di qualità associate a ciascuna misura di qualità elemento e obiettivo (allegato B), considerazioni su specifici elementi di misurazione della qualità (allegato C), un elenco di misure di qualità in ordine alfabetico (allegato D) e una tabella delle misure di qualità raggruppate da caratteristiche e entità bersaglio (allegato E).

ISO 25024:2015

- Questo standard internazionale può essere applicato a qualsiasi tipo di dati conservati in un formato strutturato all'interno di a sistema informatico utilizzato per qualsiasi tipo di applicazione.
- Le persone che gestiscono dati e servizi, inclusi i dati, sono i principali beneficiari delle misure di qualità.
- Questo standard internazionale è destinato a essere utilizzato da persone che hanno bisogno di produrre e / o utilizzare i dati misure di qualità nel rispetto delle loro responsabilità.
- Questo standard internazionale tiene conto di una vasta gamma di dati delle entità target.
- Può essere applicato in molti tipi di sistemi di informazione, ad esempio, come segue:
  a) sistema di informazione legacy;
  b) data warehouse;
  c) sistema informativo distribuito;
  d) sistema informativo cooperativo;
  e) World Wide Web.
- L'ambito non include quanto segue:
  a) rappresentazione della conoscenza;
  b) tecniche di data mining;
  c) significato statistico per campione casuale.

Dove possiamo applicare tutto questo …

Regolamento UE 679/2016

La ISO 31000 (gestione del rischio) permea l'intero Regolamento:

Articolo	Descrizione
art. 5 par. 1 lett. f), par 2	Principi applicabili al trattamento di dati personali e competenza del titolare
art. 24	Responsabilità del titolare del trattamento
Art. 25	Privacy by design e privacy by default
Art. 28 par. 3 lett. e)	Responsabile del trattamento
Art. 32	Sicurezza del trattamento
Art. 33 par. 3 lett. c)	Notifica di una violazione dei dati personali all'autorità di controllo
Art. 35 par. 1, 7 lett. c) e d)	Valutazione d'impatto sulla protezione dei dati
Art. 39 par 2	Compiti del responsabile della protezione dei dati
Art. 47 par. 2 lett. d)	Norme vincolanti d'impresa
Art. 49 par. 6	Deroghe in specifiche situazioni

Regolamento UE 679/2016 – Articolo 5

1. I dati personali sono:
   a) […]

   b) […]
   c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati») → ISO 25024 e tecniche di normalizzazione delle banche dati;
   d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza») → ISO 25024 (ex ante) e ISO 2859-10 (ex post);
   e) […]
   f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza») → ISO 27001.

Regolamento UE 679/2016 – Articolo 32

- 1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
  a) la pseudonimizzazione (→ ISO 25024) e la **cifratura** dei dati personali (→ **ISO 18033);**
  b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la **resilienza (→ ISO 22301)** dei sistemi e dei servizi di trattamento; → ISO 27001
  c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; → ISO 24762
  d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. → ISO 27008

Le ISO 27001 (e 27002) sono un ottimo punto di partenza

Standard di sicurezza famiglia serie 27000

Norme della famiglia 27000:

- ISO/IEC 27000:2016, Information security management systems — Overview and vocabulary
- ISO/IEC 27001:2013, Information security management systems — Requirements (UNI 27001:2014 - Sistemi di gestione della sicurezza delle informazioni – Requisiti)
- ISO/IEC 27002:2013, Code of practice for information security management (UNI 27002:2014 – Tecniche per la Sicurezza – Raccolta di prassi sui controlli per la sicurezza delle informazioni)

Standard di sicurezza famiglia serie 27000

Norme della famiglia 27000:

ISO/IEC 27003:2010, Information security management - System implementation guidance

ISO/IEC 27004:2016, Information security management - Measurement

ISO/IEC 27005:2011, Information security risk management

ISO/IEC 27006:2011, Requirements for bodies providing audit and certification of information security management systems

Standard di sicurezza famiglia serie 27000

Norme della famiglia 27000:

- ISO 27799:2016 - Health informatics — Information security management in health using ISO/IEC 27002
- ISO/IEC 27007:2011, Guidelines for information security management systems auditing
- ISO/IEC TR 27008:2011 - Guidelines for auditors on information security management systems controls
- ISO/IEC 27011:2008 - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

La certificazione ISO 27001

ISO 27001

- È la norma per la gestione della sicurezza delle informazioni
- Si basa sulla valutazione e gestione dei rischi
- Richiede una misurazione per la dimostrazione di efficacia

La pubblicazione della Norma Internazionale **ISO/IEC 27001:2005** ("*Information technology – Security techniques – Information security management systems – Requirements*") sulla Sicurezza delle Informazioni fu figlia delle norme britanniche BS 7779, parte prima e seconda, quindi ha visto la luce la ISO/IEC 17799:2000 ("*Information technology – Code of practice for information security management*"), successivamente revisionata nel 2005.

La certificazione ISO 27001

- La ISO/IEC 27001 copre naturalmente ogni tipo di organizzazione.
- Essa **specifica i requisiti per progettare, implementare, controllare, mantenere e migliorare un SGSI documentato**.

- Il SGSI delineato dalla ISO 27001 ha l'obiettivo di prevenire tutti i rischi dell'impresa legati alla sicurezza delle informazioni, anche attraverso l'implementazione di una serie di controlli indicati dalla norma.

La certificazione ISO 27001

Attualmente i certificati emessi da organismi accreditati SINCERT/ACCREDIA per sistemi di gestione della sicurezza delle informazioni (SGSI) sono circa 980, di cui però gran parte fanno riferimento a più siti della medesima organizzazione (ad es. Banche, RFI, Telecom, ecc.) ed alcuni di essi fanno capo ad organizzazioni che non hanno voluto dichiarare il proprio nominativo per ragioni di riservatezza.

La certificazione ISO 27001

L'impostazione dello standard ISO/IEC 27001 è coerente con quella del Sistema di Gestione per la Qualità ISO e con il *"Risk-Based Thinking"*; vengono infatti trattati argomenti quali:

- approccio per processi;
- politica per la sicurezza;
- identificazione;
- analisi dei rischi;
- valutazione e trattamento dei rischi;
- riesame e rivalutazione dei rischi;
- modello PDCA;
- utilizzo di procedure e di strumenti come audit interni;
- non conformità, azioni correttive, sorveglianza, miglioramento continuo.

La certificazione ISO 27001

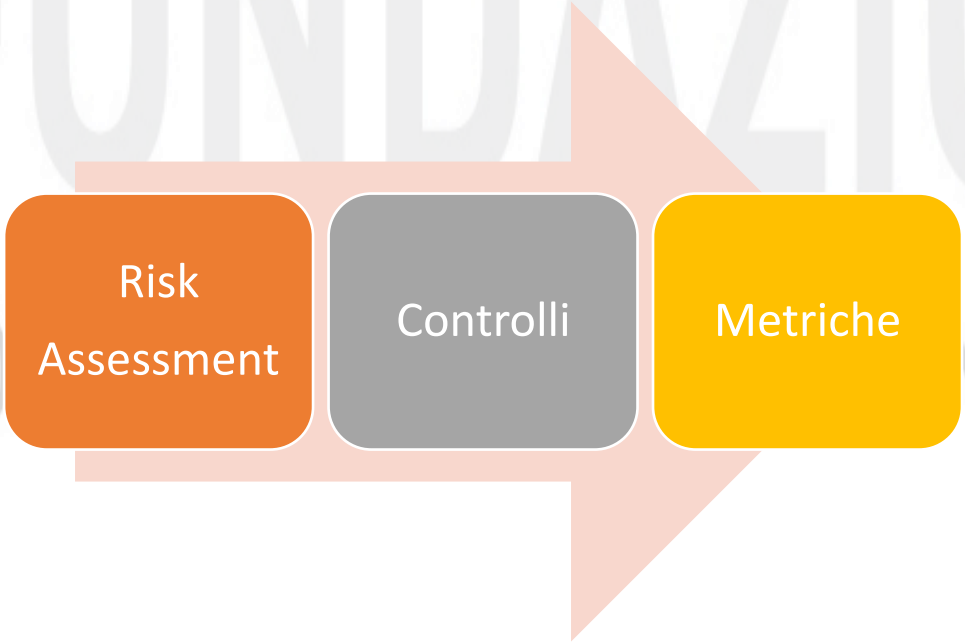
- Definizioni:
  - **Bene** (*asset*): Qualsiasi cosa cha abbia valore per l'organizzazione
  - **Disponibilità** (*availability*): Proprietà di essere accessibile e utilizzabile su richiesta di un'entità autorizzata
  - **Integrità** (*integrity*): Proprietà relativa alla salvaguardia dell'accuratezza e della completezza dei beni
  - **Riservatezza** (*confidentiality*): Proprietà per cui l'informazione non è resa disponibile o rivelata a individui, entità o processi non autorizzati

La certificazione ISO 27001

- Definizioni:
  - *Threat* (**Minaccia**) *potential cause of an unwanted incident, which may result in harm to a system or organization*
  - *Vulnerability* (**Vulnerabilità**) *weakness of an asset or control that can be exploited by a threat*

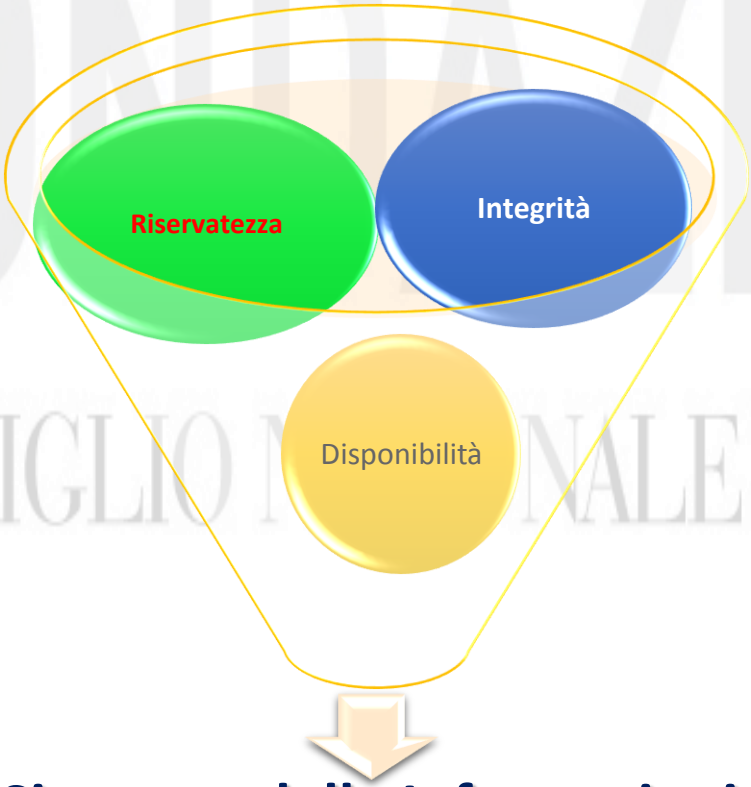
La certificazione ISO 27001

UNI CEI EN ISO 27001 – Concetti chiave



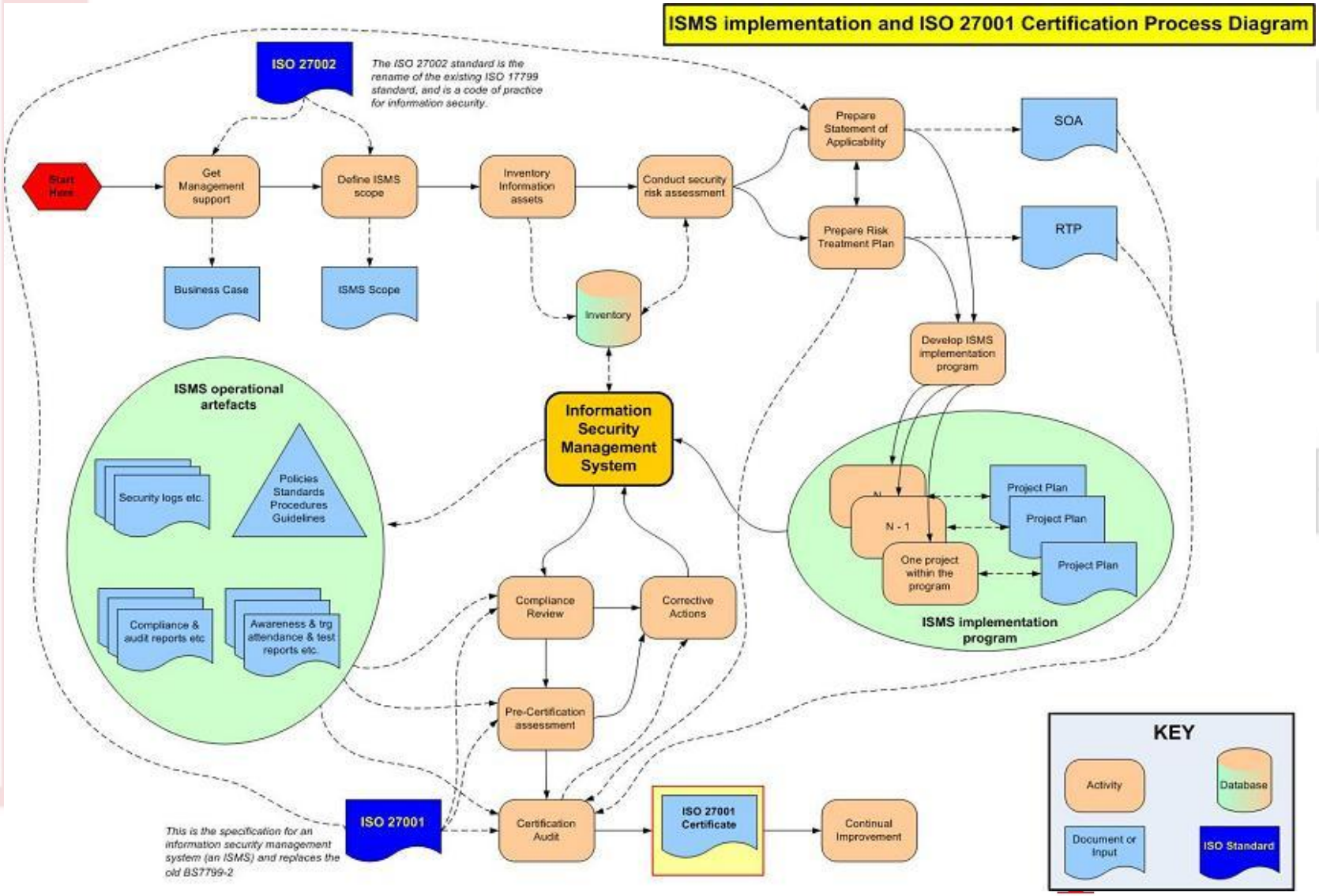
La certificazione ISO 27001: concetto di sicurezza delle informazioni

UNI CEI EN ISO 27001 – Concetti chiave



Sicurezza delle Informazioni

La ISO 27001 “Roadmap”



Il modello PDCA

- Analizzare e dare priorità ai rischi e alle opportunità dell'organizzazione:
  - cosa è accettabile?
  - cosa non è accettabile?
- Pianificare le azioni per annullare i rischi:
  - come posso evitare o eliminare il rischio?
  - come posso mitigare il rischio?
- Attuare un piano → intraprendere azioni
- Controllare l'efficacia delle azioni → funziona?
- Imparare dall'esperienza → miglioramento continuo

High Level Structure (HLS)

ANNEX SL

- Le Direttive ISO/IEC, Parte 1, Annesso SL, Appendice 2, definiscono la struttura di alto livello, identico testo base, termini comuni e comuni definizioni, destinati a formare, quando possibile, il nucleo delle future norme di sistemi di gestione, come la ISO 9001
- "Tutti i MSS (sia di tipo A che di tipo B) devono, in linea di principio, usare una struttura coerente, testo e terminologia comuni in modo che essi siano facili da utilizzare e reciprocamente compatibili. La guida e la struttura date nell'appendice 2 a questo Annex SL devono pure, in linea di principio essere seguiti (sulla base della risoluzione ISO/TMB 18/2012)"

La struttura delle norme sui sistemi di gestione

- 0 Introduzione
- 1 Scopo e campo di applicazione
- 2 Riferimenti normativi
- 3 Termini e definizioni
- 4 Contesto dell'organizzazione
- 5 Leadership
- 6 Pianificazione
- 7 Supporto
- 8 Attività operative
- 9 Valutazione delle prestazioni
- 10 Miglioramento

Struttura della norma ISO 27001

0. Introduzione
1. Scopo e Campo di applicazione

Sono capitoli introduttivi.
Il campo di applicazione definisce i risultati previsti del Sistema di Gestione.

2. Riferimenti normativi

Fornisce dettagli di norme o pubblicazioni di riferimento attinenti al particolare standard.

3. Termini e definizioni

Definisce i dettagli, i termini e le definizioni applicabili agli standard specifici in aggiunta a quelli comuni a tutti gli standard stessi.

Struttura della norma ISO 27001

4. Contesto dell'Organizzazione

PLAN

Si compone di quattro sotto requisiti.

4.1 Comprendere l'organizzazione e il suo contesto;

4.2 Comprendere le esigenze e le aspettative delle parti interessate;

4.3 Determinare il campo di applicazione del sistema di gestione;

4.4 Sistema di gestione per la qualità e relativi processi.

Il comma 4 definisce il Sistema di Gestione dell'Organizzazione identificando gli aspetti interni ed esterni che possono influire sui risultati attesi, tutte le parti interessate e le loro esigenze.

Documenta il campo di applicazione e imposta i confini del Sistema di Gestione in linea con gli obiettivi di business.

Struttura della norma ISO 27001

0	INTRODUZIONE
1	SCOPO E CAMPO DI APPLICAZIONE
2	RIFERIMENTI NORMATIVI
3	TERMINI E DEFINIZIONI
4	CONTESTO DELL'ORGANIZZAZIONE
4.1	Comprendere l'organizzazione e il suo contesto
4.2	Comprendere le necessità e le aspettative delle parti interessate
4.3	Determinare il campo di applicazione del sistema di gestione per la sicurezza delle informazioni
4.4	Sistema di gestione per la sicurezza delle informazioni

Struttura della norma ISO 27001

5. Leadership

PLAN

Comprende tre sotto requisiti:

5.1 Leadership e impegno;

5.2 Politica;

5.3 Ruoli, responsabilità e autorità nell'Organizzazione.

Viene, quindi, posto maggiore enfasi al ruolo della Leadership.

Ciò comporta che il Top Management ha ora una più rilevante responsabilità ed è maggiormente coinvolto nel governo del sistema di gestione.

È quindi necessario integrare i requisiti del sistema di gestione nel processi di core-business dell'Organizzazione garantendo che il sistema di gestione raggiunga i risultati attesi anche allocando le necessarie ed adeguate risorse.

Il Top Management ha anche la responsabilità di comunicare l'importanza del sistema di gestione aumentando la consapevolezza ed il coinvolgimento di tutti i dipendenti.

Struttura della norma ISO 27001

6. Pianificazione

PLAN

I sotto requisiti sono:

6.1 Azioni per affrontare i rischi e opportunità;

6.2 Obiettivi per la qualità e pianificazione per il loro raggiungimento.

In questo capitolo si pone particolare enfasi sull'approccio al rischio il Risk Based Thinking.

Dopo aver evidenziato rischi e opportunità nel cap. 4, diventa necessario stabilirne e pianificarne il trattamento quindi: chi, come e quando affronterà questi rischi.

Questo approccio proattivo va a sostituire l'azione preventiva e riducendo la necessità di conseguenti azioni correttive.

Attenzione viene posta agli obiettivi del sistema di gestione che dovrebbero essere misurabili, monitorati, comunicati, allineati alla politica della qualità e aggiornati quando necessario.

Struttura della norma ISO 27001

5 LEADERSHIP

5.1 Leadership e impegno

5.2 Politica

5.3 Ruoli, responsabilità e autorità nell'organizzazione

6 PIANIFICAZIONE

6.1 Azioni per affrontare rischi e opportunità

6.2 Obiettivi per la sicurezza delle informazioni e pianificazione per conseguirli

Struttura della norma ISO 27001

7. Supporto

DO

Il Capitolo riporta i seguenti sotto requisiti:

7.1 Risorse;

7.2 Competenza;

7.3 Consapevolezza;

7.4 Comunicazione;

7.5 Informazioni documentate.

Avendo già affrontato contesto, impegno e pianificazione, l'Organizzazione dovrà occuparsi di quelle attività di supporto necessarie alla soddisfazione degli obiettivi.

Questo comporta di porre attenzione alle risorse, alla comunicazione interna ed esterna, alle informazioni documentate che andranno a sostituire la documentazione e le registrazioni utilizzate in precedenza.

Struttura della norma ISO 27001

7 SUPPORTO

7.1 Risorse

7.2 Competenza

7.3 Consapevolezza

7,4 Comunicazione

7.5 Informazioni documentate

Struttura della norma ISO 27001

8. Attività operative

DO

Ha un sub requisito:

8.1 Pianificazione e Controllo operativi.

La maggior parte dei requisiti del sistema di gestione viene trattato all'interno di questo singolo requisito che copre sia i processi interni che quelli esterni anche in outsourcing includendo criteri adeguati per il controllo degli stessi ed anche metodi per la gestione dei cambiamenti sia quelli pianificati che quelli inattesi.

Struttura della norma ISO 27001

8 ATTIVITÀ OPERATIVE

8.1 Pianificazione e controllo operativi

8.2 Valutazione del rischio relativo alla sicurezza delle informazioni

8.3 Trattamento del rischio relativo alla sicurezza delle informazioni

Struttura della norma ISO 27001

9. Valutazione delle prestazioni

CHECK

Abbiamo tre sotto requisiti:

9.1 Monitoraggio, misurazione, analisi e valutazione;

9.2 Audit interni;

9.3 Riesame di direzione;

Qui si deve determinare cosa, come e quando le azioni intraprese devono essere monitorate, misurate, analizzate e valutate.

L'audit interno rappresenta quindi una parte importante di questo processo per garantire la conformità del sistema di gestione ai requisiti dell'Organizzazione e della norma che questo sia adeguatamente implementato e mantenuto.

Il riesame di direzione andrà poi ad effettuare la valutazione del fatto che il sistema di gestione sia adatto, adeguato ed efficace.

Struttura della norma ISO 27001

10. Miglioramento

ACT

Sono due i sotto requisiti:

10.1 Non conformità e azioni correttive;

10.2 Miglioramento continuo;

Si va quindi ad esaminare le modalità di gestione delle non conformità e delle azioni correttive.

Tenendo conto che durante l'attività dell'Organizzazione il contesto ed il mondo del lavoro sono in continua evoluzione talvolta non tutto può andare secondo i piani.

Andremo quindi ad esaminare i criteri ed i metodi adottati per affrontare e neutralizzare sia i rischi che le non conformità attraverso le azioni correttive intraprese nonché le strategie e le tecniche di miglioramento su base continuativa del sistema di gestione implementate.

Struttura della norma ISO 27001

9 VALUTAZIONE DELLE PRESTAZIONI

9.1 Monitoraggio, misurazione, analisi e valutazione

9.2 Audit interno

9.3 Riesame di direzione

10 MIGLIORAMENTO

10.1 Non conformità e azioni correttive

10.2 Miglioramento continuo

APPENDICE (normativa) A - OBIETTIVI DI CONTROLLO E CONTROLLI DI RIFERIMENTO

Obiettivi di controllo e controlli ← ISO 27002

8. Attività operative

8.1 Pianificazione e controllo operativi

- L'organizzazione deve pianificare, attuare e tenere sotto controllo i processi necessari per soddisfare i requisiti di sicurezza delle informazioni e per mettere in atto le azioni determinate al punto 6.1. L'organizzazione deve anche attuare i piani per conseguire gli obiettivi per la sicurezza delle informazioni determinati al punto 6.2.

8. Attività operative

- L'organizzazione deve le conservare informazioni documentate nella misura necessaria ad avere fiducia che i processi siano stati eseguiti come pianificato.
- L'organizzazione deve tenere sotto controllo le modifiche pianificate e riesaminare le conseguenze dei cambiamenti involontari, intraprendendo azioni per mitigare qualunque effetto negativo, per quanto necessario.
- L'organizzazione deve assicurare che i processi affidati all'esterno siano determinati e tenuti sotto controllo.

8. Attività operative

8.2 Valutazione del rischio relativo alla sicurezza delle informazioni

- L'organizzazione deve effettuare le valutazioni del rischio relativo alla sicurezza delle informazioni a intervalli pianificati o quando sono proposti o si verificano cambiamenti significativi, considerando i criteri stabiliti al punto 6.1.2 a).
- L'organizzazione deve conservare informazioni documentate sui risultati delle valutazioni del rischio relativo alla sicurezza delle informazioni.

8. Attività operative

8.3 Trattamento del rischio relativo alla sicurezza delle informazioni

L'organizzazione deve attuare il piano di trattamento del rischio relativo alla sicurezza delle informazioni.

L'organizzazione deve conservare informazioni documentate sui risultati del trattamento del rischio relativo alla sicurezza delle informazioni.

Concetto di rischio

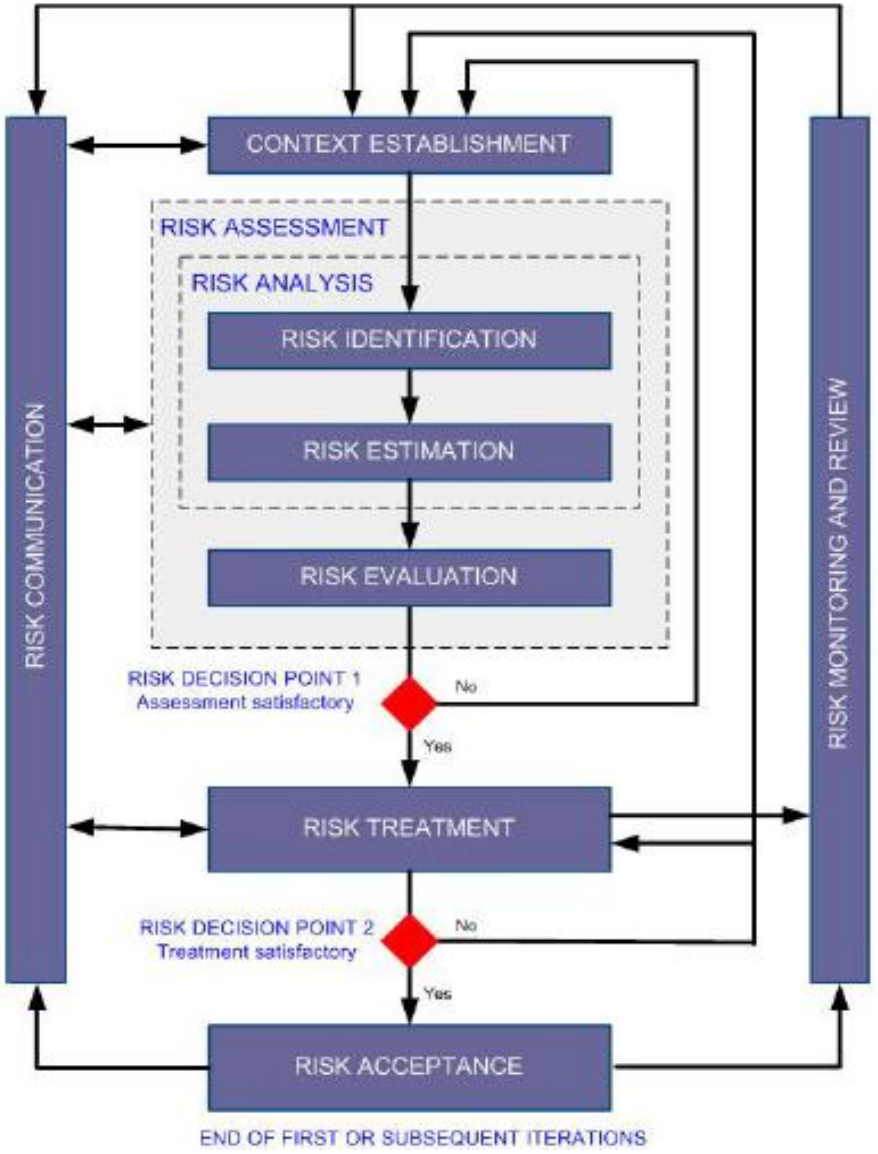
Definizioni:

- **rischio**: Effetto dell'incertezza sugli obiettivi.

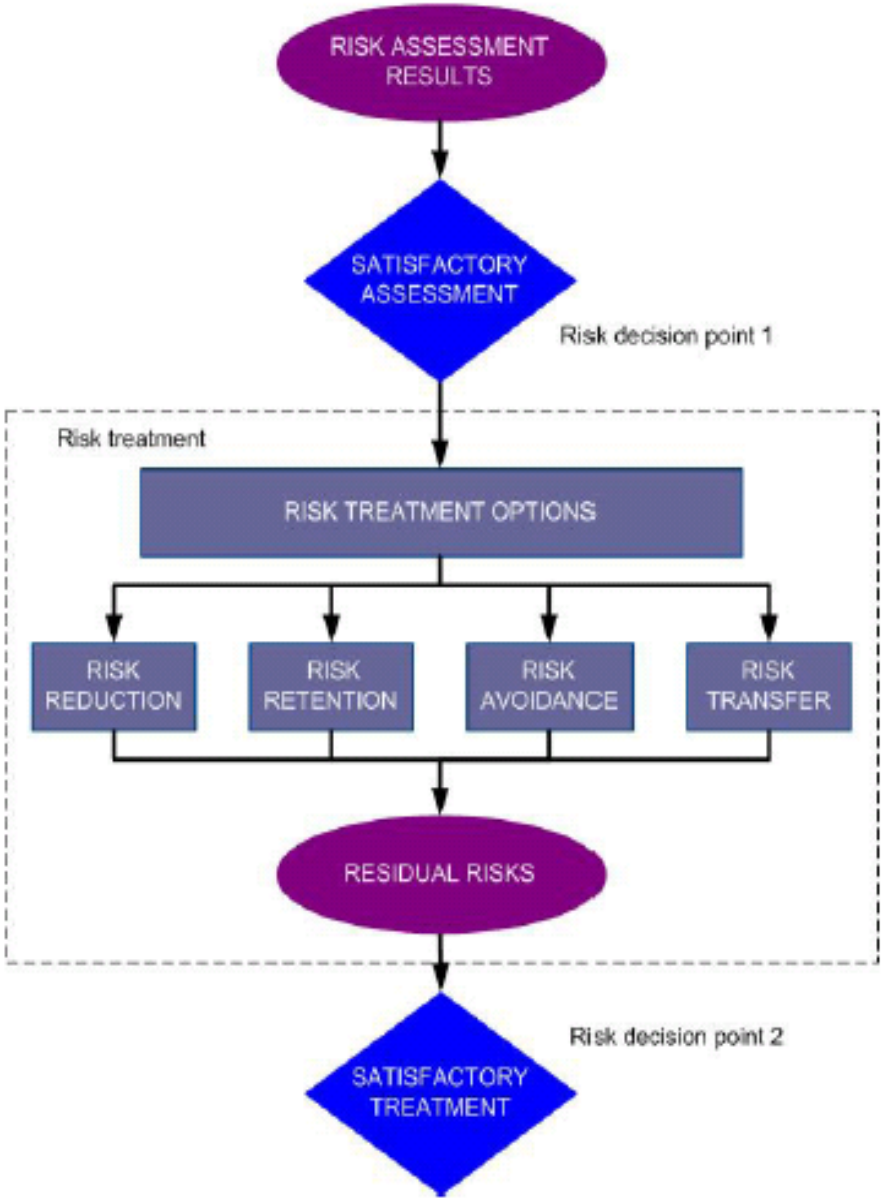
[Guida ISO 73:2009, definizione 1.1]

Incertezza → Rischio → Obiettivi

Schema del processo di valutazione (assessment) del rischio



Schema del processo di trattamento del rischio



ISO 27002: progettare e collaudare le contromisure in ambito sicurezza IT

La norma UNI CEI ISO/IEC 27002:2014 “Raccolta di prassi sui controlli per la sicurezza delle informazioni” (che sostituisce la ISO 27002:2005) è stata progettata per essere impiegata nelle organizzazioni che intendono implementare un sistema di gestione della sicurezza delle informazioni ISO 27001 e la prendono come riferimento per la scelta dei controlli di sicurezza da attuare.

Le *best practice* identificate dalla norma ISO 27002:2014 (UNI CEI ISO/IEC 27002:2014 - *Tecnologie informatiche - Tecniche per la sicurezza - Raccolta di prassi sui controlli per la sicurezza delle informazioni*) introducono 14 punti di controllo di sicurezza che riuniscono un totale di 35 categorie principali di sicurezza e 114 controlli.

Struttura della ISO 27002

- Ogni punto che definisce controlli di sicurezza contiene una o più categorie principali di sicurezza, al cui interno sono raggruppati i controllo relativi. Nella norma viene precisato che l'ordine dei punti è indipendente dalla loro importanza, infatti, a seconda delle circostanze, i controlli di sicurezza appartenenti ad uno o a tutti i punti di controllo potrebbero rivelarsi più o meno importanti ed ogni organizzazione che impiega la norma dovrebbe identificare i controlli applicabili al proprio interno, la loro importanza ed il loro impiego in ogni processo di business.
- Ogni **categoria principale** di controllo di sicurezza contiene:
  - L'**obiettivo di controllo** che dichiara cosa si vuole raggiungere
  - I **controlli** che possono essere applicati per raggiungere l'obiettivo di controllo.

Struttura della ISO 27002

- La descrizione dei controlli è strutturata come segue:

- Controllo: definisce nello specifico il controllo funzionale alla soddisfazione dell'obiettivo di controllo.
- Guida attuativa: fornisce informazioni più dettagliate per supportare l'attuazione del controllo. La guida può risultare completamente attinente o sufficiente a tutte le situazioni oppure potrebbe non soddisfare i requisiti specifici di controllo dell'organizzazione.
- Altre informazioni: fornisce informazioni aggiuntive che potrebbe essere necessario considerare, per esempio considerazioni legali e riferimenti ad altre norme. Nel caso non vi siano informazioni aggiuntive da considerare questa parte non è riportata nel testo.

A5 Politiche per la sicurezza delle informazioni

Al suo interno viene individuata la categoria “Indirizzi della direzione per la sicurezza delle informazioni” (5.1), in cui viene indicata la necessità di stabilire una politica per la sicurezza delle informazioni coerente con gli obiettivi e gli indirizzi dell’organizzazione in merito all’Information Security, anche in funzione del contesto di riferimento (mercato, esigenze dei clienti, leggi e regolamenti applicabili). Tale politica dovrà essere mantenuta aggiornata attraverso riesami periodici.

A5 Politiche per la sicurezza delle informazioni

❖**A5.1 Indirizzi della direzione per la sicurezza delle informazioni**

- A5.1.1 Politiche per la sicurezza delle informazioni
- A5.1.2 Riesame delle politiche per la sicurezza delle informazioni

Definizione di una policy per la protezione dei dati personali

A6 Organizzazione della sicurezza delle informazioni

In questa sezione sono definiti le seguenti categorie principali:

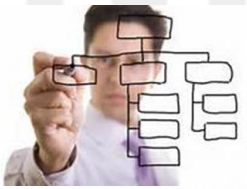
- **Organizzazione interna (6.1)**: è necessario definire tutti i ruoli e le responsabilità per la sicurezza delle informazioni, separazioni dei compiti, modalità di contatto con le autorità e con gruppi specialistici ed infine le modalità di gestione dei progetti con riferimento alla sicurezza delle informazioni.
- **Dispositivi portatili e telelavoro (6.2)**: in questa categoria sono raggruppati due controlli molto importanti che, forse, meriterebbero una trattazione separata, anche se poi i controlli relativi sono descritti in modo dettagliato. I dispositivi portatili da gestire e mantenere sotto controllo sono di diverse tipologie (notebook, tablet, smartphone, …) ed ognuna di essa meriterebbe una trattazione a sé, così come la proprietà del dispositivo (azienda, dipendente o collaboratore, o semplice visitatore) ed il tipo di impiego (esclusivamente aziendale, esclusivamente privato o misto come nel caso del BYOD, Bring Your Own Device). Per quanto riguarda il telelavoro occorre tenere sotto controllo diversi parametri ed aspetti di sicurezza fisica e logica, non trascurando il fatto che ora il telelavoro è inteso in senso più ampio rispetto alla precedente versione della norma.

A6 Organizzazione della sicurezza delle informazioni

- Quest'area è nel complesso più ridotta rispetto alla sezione 6 della precedente versione della norma che, tra l'altro, riportava la medesima categoria riferita a dispositivi portatili e telelavoro alla sezione 11, quella del controllo accessi. Del resto questa seconda categoria deve essere considerata in senso un po' più ampio perché la sicurezza dei dispositivi portatili e del telelavoro deve essere valutata insieme alla gestione delle connessioni Wi-Fi e degli accessi a siti web aziendali e ad eventuali servizi cloud.
- L'evoluzione tecnologica in questi ultimi 9 anni trascorsi dalla precedente versione della ISO 27002 ha fatto passi da gigante moltiplicando anche le possibili vulnerabilità e qualche citazione più specifica del problema del BYOD e dell'autenticazione a due fattori (2FA) sarebbe stata utile.

A6 Organizzazione della sicurezza delle informazioni

- **A6.1 Organizzazione interna**
  - A6.1.1 Ruoli e responsabilità per la sicurezza delle informazioni
  - A6.1.2 Separazione dei compiti
  - A6.1.3 Contatti con le autorità
  - A6.1.4 Contatti con gruppi specialistici
  - A6.1.5 Sicurezza delle informazioni nella gestione dei progetti
- **A6.2 Dispositivi portatili e telelavoro**
  - A6.2.1 Politica per i dispositivi portatili
  - A6.2.2 Telelavoro



A7 Sicurezza delle risorse umane

In questa sezione sono descritte le attività da considerare per garantire la sicurezza nella gestione del personale prima, durante ed al termine del rapporto di lavoro:

- **Prima dell'impiego** (7.1): in due controlli vengono esposte tutte le cautele da intraprendere al momento dell'assunzione di una persona o dell'incarico ad un collaboratore esterno, non solo accordi di riservatezza e clausole contrattuali sul futuro rapporto lavorativo, ma anche – per quanto reso possibile dalla legislazione applicabile – un'accurata indagine conoscitiva sul passato, lavorativo e non, del futuro dipendente/collaboratore.
- **Durante l'impiego** (7.2): nel corso della normale attività lavorativa viene data enfasi all'applicazione delle procedure stabilite e le responsabilità della Direzione nell'applicazione delle stesse, alla formazione-addestramento e sensibilizzazione del personale ed al ricorso ad eventuali processi disciplinari. Dunque regole da rispettare, ma anche motivazione ed incentivazione del personale, oltre che sanzioni a chi infrange le regole.

A7 Sicurezza delle risorse umane

- **Cessazione e variazione del rapporto di lavoro** (7.3): vengono presi in esame tutti gli aspetti e le attività da svolgere quando si chiude un rapporto di lavoro o avviene un'assegnazione ad altro incarico, come ad esempio il prolungamento della validità degli accordi di riservatezza, i passaggi di consegne e la comunicazione all'altro personale interessato della cessazione del rapporto di lavoro.

Qualche perplessità desta la traduzione UNI in quest'area: viene utilizzato il termine "soffiare" in senso di "soffiata", "spiata", "delazione", "informazione anonima su un comportamento non corretto" ed il termine "inazioni" probabilmente intendendo "omissioni" o il contrario di azioni, ovvero il "non agire".

A7 Sicurezza delle risorse umane

- ❖**A7.1** **Prima dell'impiego**
  - A7.1.1 Screening
  - A7.1.2 Termini e condizioni di impiego
- ❖**A7.2** **Durante l'impiego**
  - A7.2.1 Responsabilità della direzione
  - A7.2.2 Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni
  - A7.2.3 Processo disciplinare
- ❖**A7.3** **Cessazione e variazione del rapporto di lavoro**
  - A7.3.1 Cessazione o variazione delle responsabilità durante il rapporto di lavoro

A8 Gestione degli asset

In quest'area viene trattata la gestione degli asset (tradotti come "beni" nella precedente versione della norma ISO 27001) all'interno di tre categorie:

- **Responsabilità per gli asset** (8.1): tutti gli asset aziendali vanno inventariati, ne deve essere definito un responsabile e le regole per l'utilizzo e la gestione durante tutto il ciclo di vita.
- **Classificazione delle informazioni** (8.2): le informazioni dovrebbero essere classificate in funzione del livello di riservatezza richiesto e conseguentemente etichettate in funzione della loro classificazione. Le procedure per il trattamento degli asset dovrebbero essere una logica conseguenza della classificazione degli stessi e delle informazioni in essi trattate.
- **Trattamento dei supporti** (8.3): al fine di garantire riservatezza, integrità e disponibilità delle informazioni contenute nei supporti rimovibili (hard-disk esterni, chiavi USB, DVD, ecc.) occorre prevedere opportune procedure di gestione degli stessi durante tutto il loro ciclo di vita (impiego, dismissione, trasporto, ecc.).

Nella presente sezione – praticamente immutata rispetto alla corrispondente sezione 7 della precedente versione della norma, salvo l'aggiunta di due controlli – viene richiamata la classificazione degli asset finalizzata alla valutazione dei rischi contenuta nella **ISO 27005**.

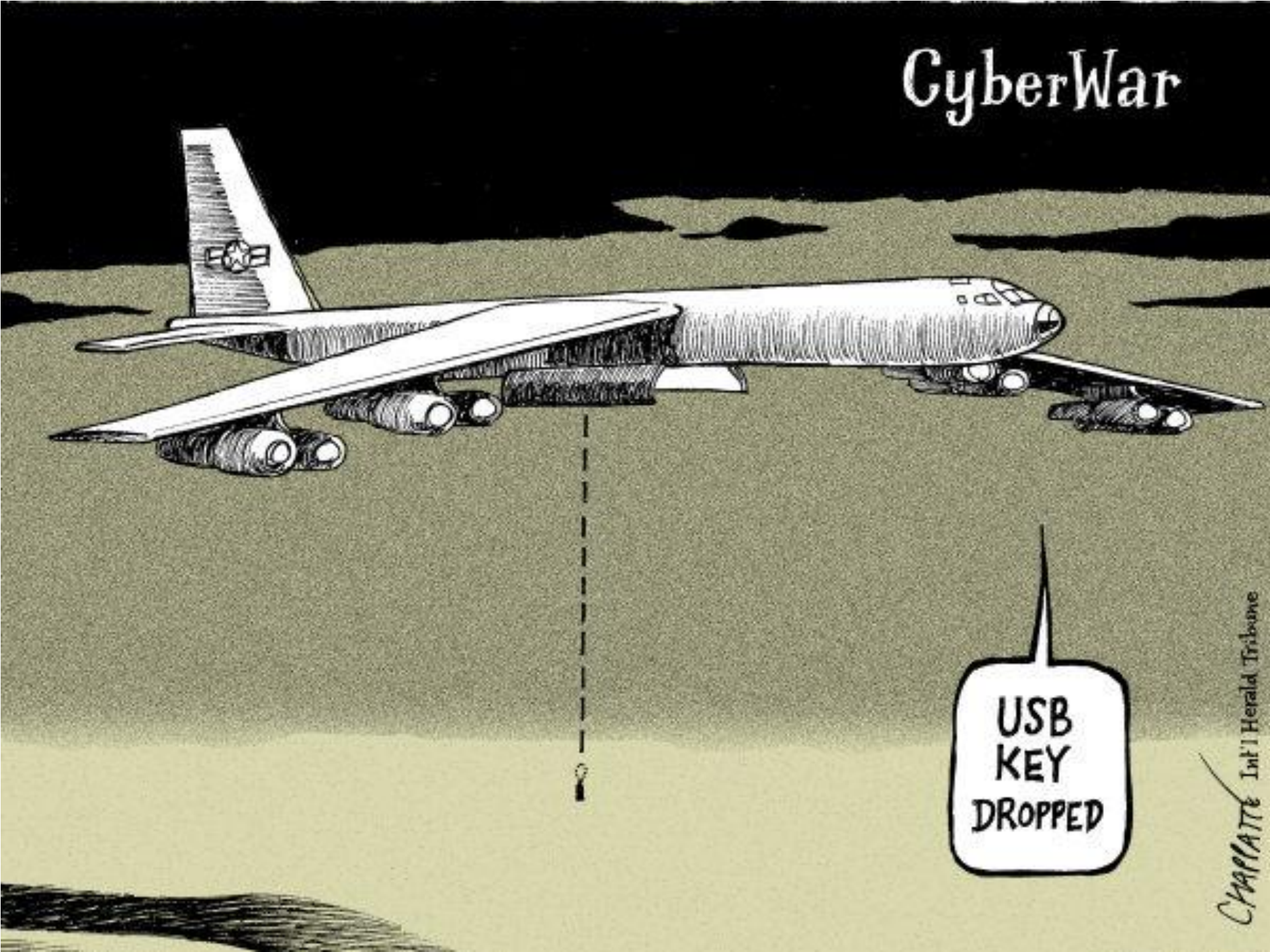
A8 Gestione degli asset

- **A8.1 Responsabilità per gli asset**
  - A8.1.1 Inventario degli asset
  - A8.1.2 Responsabilità degli asset
  - A8.1.3 Utilizzo accettabile degli asset
  - A8.1.4 Restituzione degli asset
- **A8.2 Classificazione delle informazioni**
  - A8.2.1 Classificazione delle informazioni
  - A8.2.2 Etichettatura delle informazioni
  - A8.2.3 Trattamento degli asset

A8 Gestione degli asset

❖ **A8.3 Gestione dei supporti rimovibili**

- A8.3.1 Gestione dei supporti rimovibili
- A8.3.2 Dismissione dei supporti
- A8.3.3 Trasporto dei supporti fisici


CyberWar
USB KEY DROPPED
CHAPPATTE Int'l Herald Tribune

A9 Controllo degli accessi

Questa sezione tratta l'importante aspetto del controllo degli accessi alle aree dove sono custodite informazioni, in formato digitale o su supporto cartaceo, sia dal punto di vista degli accessi fisici, sia dal punto di vista degli accessi logici ai sistemi informatici. Le categorie prese in esame sono le seguenti:

- **Requisiti di business per il controllo degli accessi** (9.1): occorre definire una politica di controllo degli accessi basata sull'accesso alle sole informazioni necessarie per svolgere il proprio lavoro (come impone anche la normativa sulla privacy in vigore in Italia) e regolamentare l'accesso alle reti (soprattutto evitare l'uso incontrollato delle reti Wi-Fi senza autenticazione utente).
- **Gestione degli accessi degli utenti** (9.2): è necessario regolamentare il processo di registrazione (tramite credenziali di autenticazione univoche) e de-registrazione degli utenti, la fornitura delle credenziali di accesso (provisioning), la gestione degli accessi privilegiati (ad es. quelli in qualità di "amministratore di sistema", cfr. apposita disposizione del Garante della Privacy), la gestione delle informazioni segrete per l'autenticazione (password, smartcard, ecc.), il riesame periodico dei diritti di accesso, la rimozione degli stessi al termine del rapporto (o la revisione in caso di cambio mansioni).
- **Responsabilità dell'utente** (9.3): è importante regolamentare ed istruire il personale sull'uso della password. Controllo degli accessi ai sistemi e alle applicazioni (9.4): è opportuno limitare l'accesso alle informazioni, predisporre procedure di log-on sicure, procedure di gestione delle password, limitare l'impiego di programmi di utilità privilegiati, limitare gli accessi al codice sorgente dei programmi.

A9 Controllo degli accessi

Nei controlli esposti sono illustrati molti principi di sicurezza delle informazioni abbastanza noti ai più, ma spesso non recepiti nelle PMI per scarsa competenza dei responsabili IT (spesso esterni), richieste di gestioni semplificate da parte degli utenti e dei responsabili, mancanza di consapevolezza da parte della Direzione e, soprattutto, la ricerca del minor costo nelle apparecchiature e nella formazione del personale. Per questo motivo molte regole basilari, ad esempio relative ad una corretta gestione della rete Wi-Fi (creazione di accessi "ospite" per gli esterni, impiego di autenticazioni per singolo utente tramite protocollo Radius o da pannello di controllo del router, segmentazione delle reti in Vlan, ecc.) e delle password (impiego di password complesse e memorizzate in modo sicuro tramite utility apposite, uso non promiscuo delle password, variazione delle password al primo accesso,…) spesso non vengono implementate.

A9 Controllo degli accessi

- **A9.1 Requisiti di business per il controllo degli accessi**
  - A9.1.1 Politica di controllo degli accessi
  - A9.1.2 Accesso alle reti e ai servizi di rete
- **A9.2 Gestione degli accessi degli utenti**
  - A9.2.1 Gestione degli accessi degli utenti
  - A9.2.2 Provisioning degli accessi degli utenti
  - A9.2.3 Gestione dei diritti di accesso privilegiato
  - A9.2.4 Gestione delle informazioni segrete di autenticazione degli utenti
  - A9.2.5 Riesame dei diritti di accesso degli utenti
  - A9.2.6 Rimozione o adattamento dei diritti di accesso

A9 Controllo degli accessi

- **A9.3 Responsabilità dell'utente**
  - A9.3.1 Utilizzo delle informazioni segrete di autenticazione
- **A9.4 Controllo degli accessi ai sistemi e alle applicazioni**
  - A9.4.1 Limitazione dell'accesso alle informazioni
  - A9.4.2 Procedure di log-on sicure
  - A9.4.3 Sistema di gestione delle password
  - A9.4.4 Uso di programmi di utilità privilegiati
  - A9.4.5 Controllo degli accessi al codice sorgente dei programmi

A10 Crittografia

- Questo punto di controllo prevede una sola categoria “Controlli crittografici” (10.1) all’interno della quale sono descritti due controlli inerenti la politica relativa all’impiego dei controlli crittografici e la gestione delle chiavi crittografiche. La trattazione è molto dettagliata e comprende diversi aspetti da non sottovalutare come cosa fare in caso di indisponibilità, temporanea o permanente, delle chiavi crittografiche. In Italia occorre considerare la normativa specifica sulla firma digitale e la gestione dei certificati tramite le certification authority accreditate. Viene richiamata la norma ISO/IEC 11770 per ulteriori informazioni sulle chiavi.
- Questa che era prima una categoria (cfr. punto 12.3 della norma ISO 27002:2005) ora è salito a livello di punto di controllo.

A10 Crittografia

❖**A10.1 Controlli crittografici**

- A10.1.1 Politica sull'uso dei controlli crittografici
- A10.1.2 Gestione delle chiavi

A11 Sicurezza fisica e ambientale

La sezione comprende due categorie:

- **Aree sicure** (11.1): devono essere definiti dei perimetri che delimitano aree con diversi livelli di sicurezza, nei quali occorre prevedere adeguate protezioni per prevenire accessi indesiderati e safety (viene citata la normativa antincendio), devono essere attivati sistemi di controllo e registrazione degli accessi alle aree sicure, devono essere implementate particolari misure di sicurezza fisica per proteggere aree chiave e devono essere adottate misure di protezione contro disastri e calamità naturali (incendi, alluvioni, terremoti, ecc.). Inoltre devono essere progettate ed attuate procedure per permettere il lavoro in aree sicure e protette e, infine, devono essere implementati controlli particolari nelle aree di carico/scarico materiali.
- **Apparecchiature** (11.2): particolari accorgimenti devono essere intrapresi per proteggere le apparecchiature impiegate (per elaborazione o archiviazione di informazioni in genere) rispetto ad accessi non consentiti o minacce di possibili danneggiamenti, anche provenienti dalle infrastrutture di supporto (connettività di rete, energia elettrica, gas, acqua, ecc.) o da carenze di sicurezza dei cablaggi. Inoltre le apparecchiature devono essere sottoposte a regolare manutenzione, dispositivi hardware e software devono essere mantenuti sotto controllo in caso di trasferimenti all'esterno dell'organizzazione, adottando, nel caso particolari misure di sicurezza ed in caso di dismissione di apparecchiature o supporti di memorizzazione le informazioni in essi contenute devono essere cancellate in modo sicuro. Infine è necessario definire istruzioni affinché le apparecchiature non siano lasciate incustodite quando con esse è possibile accedere ad informazioni riservate ed occorre definire politiche di "scrivania pulita" per prevenire la visione di informazioni riservate da parte di personale non autorizzato.

A11 Sicurezza fisica e ambientale

❖**A11.1 Aree sicure**

- A11.1.1 Perimetro di sicurezza fisica
- A11.1.2 Controlli di accesso fisico
- A11.1.3 Rendere sicuri uffici, locali e strutture
- A11.1.4 Protezione contro minacce esterne ed ambientali
- A11.1.5 Lavoro in aree sicure
- A11.1.6 Aree di carico e scarico

A11 Sicurezza fisica e ambientale

❖**A11.2 Apparecchiature**

- A11.2.1 Disposizione delle apparecchiature e loro protezione
- A11.2.2 Infrastrutture di supporto
- A11.2.3 Sicurezza dei cablaggi
- A11.2.4 Manutenzione delle apparecchiature
- A11.2.5 Trasferimento degli asset
- A11.2.6 Sicurezza delle apparecchiature e degli asset all'esterno delle sedi
- A11.2.7 Dismissione sicura o riutilizzo delle apparecchiature
- A11.2.8 Apparecchiature incustodite degli utenti
- A11.2.9 Politica di schermo e scrivania puliti

A12 Sicurezza delle attività operative

Questa area comprende ben 7 categorie:

- **Procedure operative e responsabilità** (12.1): devono essere predisposte procedure per documentare lo svolgimento di una serie di attività inerenti la sicurezza, occorre gestire i cambiamenti all'organizzazione e la capacità delle risorse (di storage, di banda, infrastrutturali ed anche umane), infine è necessario mantenere separati gli ambienti di sviluppo da quelli di produzione.
- **Protezione dal malware** (12.2): un solo controllo in questa categoria (protezione dal malware) che prescrive tutte le misure di sicurezza da attuare contro il malware. Non solo antivirus per prevenire ed eliminare malware, ma anche azioni di prevenzione tecnica e comportamentali (consapevolezza degli utenti).
- **Backup** (12.3): devono essere documentate ed attuate procedure di backup adeguate a garantire il ripristino dei dati in caso di perdita dell'integrità degli stessi e la continuità operativa (vedasi anche punto 17).
- **Raccolta di log e monitoraggio** (12.4): devono essere registrati, conservati e protetti i log delle attività degli utenti normali e di quelli privilegiati (si ricorda che per apposita disposizione del Garante Privacy italiano i log degli accessi in qualità di Amministratore di Sistema devono essere mantenuti in modo "indelebile" per almeno 6 mesi), occorre inoltre mantenere sincronizzati gli orologi dei sistemi con una fonte attendibile.

A12 Sicurezza delle attività operative

- **Controllo del software di produzione** (12.5): particolari attenzioni devono essere adottate nell'installazione ed aggiornamento del software di produzione (non solo per organizzazioni del settore ICT, banche o assicurazioni, ma anche per aziende manifatturiere!).
- **Gestione delle vulnerabilità tecniche** (12.6): viene fornita dalla norma un'ampia guida attuativa sulla gestione delle vulnerabilità tecniche conosciute (occorre mantenere un censimento dell'hardware e del relativo software installato su ogni elaboratore, installare le patch di sicurezza in modo tempestivo, mantenersi aggiornati sulle vulnerabilità di sicurezza conosciute, ecc.), oltre alle indicazioni sulla limitazione nell'installazione dei software (è opportuno, infatti, ridurre al minimo la possibilità per gli utenti di installare applicativi software autonomamente, anche se leciti come le utility gratuite che, a volte, possono essere il veicolo di adware o altre minacce alla sicurezza).
- **Considerazioni sull'audit dei sistemi informativi** (12.7): gli audit sui sistemi informativi dovrebbero avere un impatto ridotto sulle attività lavorative e le evidenze raccolte dovrebbero essere raccolte senza alterare i dati dei sistemi (accessi in sola lettura) e dovrebbero essere mantenute protette.

A12 Sicurezza delle attività operative

- **A12.1 Procedure operative e responsabilità**
  - A12.1.1 Procedure operative documentate
  - A12.1.2 Gestione dei cambiamenti
  - A12.1.3 Gestione della capacità
  - A12.1.4 Separazione degli ambienti di sviluppo, test e produzione
- **A12.2 Protezione dal malware**
  - A12.2.1 Controlli contro il malware

A12 Sicurezza delle attività operative

- ❖ **A12.3 Backup**
  - A12.3.1 Backup delle informazioni
- ❖ **A12.4 Raccolta di log e monitoraggio**
  - A12.4.1 Raccolta di log degli eventi
  - A12.4.2 Protezione delle informazioni di log
  - A12.4.3 Log di amministratori e operatori
  - A12.4.4 Sincronizzazione degli orologi

A12 Sicurezza delle attività operative

- **A12.5 Controllo del software di produzione**
  - A12.5.1 Installazione del software sui sistemi di produzione
- **A12.6 Gestione delle vulnerabilità tecniche**
  - A12.6.1 Gestione delle vulnerabilità tecniche
  - A12.6.2 Limitazioni all'installazione del software
- **A12.7 Considerazioni sull'audit dei sistemi informativi**
  - A12.7.1 Controlli per l'audit dei sistemi informativi

A13 Sicurezza delle comunicazioni

Questa sezione contiene due sole categorie:

- **Gestione della sicurezza della rete** (13.1): occorre adottare alcuni accorgimenti per garantire la sicurezza delle reti interne (responsabilità, autenticazioni, ecc.); viene anche citata la ISO/IEC 27033 nelle sue parti da 1 a 5 sulla sicurezza delle reti e delle comunicazioni per ulteriori informazioni. Deve, inoltre, essere gestita la sicurezza dei servizi di rete, compresi i servizi acquistati presso fornitori esterni, e la segregazione delle reti (separazione delle VLan, gestione delle connessioni Wi-Fi, ecc.).
- **Trasferimento delle informazioni** (13.2): occorre stabilire ed attuare politiche e procedure per il trasferimento delle informazioni con qualsiasi mezzo (posta elettronica, fax, telefono, scaricamento da internet, ecc.), nel trasferimento di informazioni con soggetti esterni occorre stabilire accordi sulle modalità di trasmissione, le informazioni trasmesse tramite messaggistica elettronica dovrebbero essere adeguatamente controllate e protette (non solo e-mail, ma anche sistemi EDI, instant messages, social network, ecc.) e, infine, occorre stabilire e riesaminare periodicamente accordi di riservatezza e di non divulgazione con le parti interessate.

I 7 controlli di quest'area sono sicuramente molto dettagliati e migliorano, oltre ad aggiornare, la precedente versione della norma, includendo controlli (un po' sparsi nella versione 2005 della ISO 27002) che recepiscono le nuove modalità di comunicazione, tra cui i social network, professionali e non.

A13 Sicurezza delle comunicazioni

- **A13.1 Gestione della sicurezza della rete**
  - A13.1.1 Controlli di rete
  - A13.1.2 Sicurezza dei servizi di rete
  - A13.1.3 Segregazione nelle reti
- **A13.2 Trasferimento delle informazioni**
  - A13.2.1 Politiche e procedure per il trasferimento delle informazioni
  - A13.2.2 Accordi per il trasferimento delle informazioni
  - A13.2.3 Messaggistica elettronica
  - A13.2.4 Accordi di riservatezza o di non divulgazione

A14 Acquisizione sviluppo e manutenzione dei sistemi

Quest'area tratta la sicurezza dei sistemi informativi impiegati per le attività aziendali e comprende tre categorie:

- **Requisiti di sicurezza dei sistemi informativi** (14.1): la sicurezza dei sistemi informativi- acquistati o sviluppati ad hoc – deve essere stabilita fin dall'analisi dei requisiti, deve essere garantita la sicurezza dei servizi applicativi che viaggiano su reti pubbliche (ad esempio attraverso trasmissioni ed autenticazioni sicure crittografate), infine occorre garantire la sicurezza delle transazioni dei servizi applicativi.
- **Sicurezza nei processi di sviluppo e supporto** (14.2): devono essere definite ed attuate politiche per lo sviluppo (interno o esterno all'organizzazione) sicuro dei programmi applicativi, devono essere tenuti sotto controllo tutti i cambiamenti ai sistemi (dagli aggiornamenti dei sistemi operativi alle modifiche dei sistemi gestionali), occorre effettuare un riesame tecnico sul funzionamento degli applicativi critici a fronte di cambiamenti delle piattaforme operative (sistemi di produzione, database, ecc.) e si dovrebbero limitare le modifiche (personalizzazioni) ai pacchetti software, cercando comunque di garantirne i futuri aggiornamenti. Inoltre dovrebbero essere stabiliti, documentati ed attuati principi per l'ingegnerizzazione sicura dei sistemi informatici e per l'impiego di ambienti di sviluppo sicuri. Nel caso in cui attività di sviluppo software fossero commissionate all'esterno, dovrebbero essere stabilite misure per il controllo del processo di sviluppo esternalizzato. Infine dovrebbero essere eseguiti test di sicurezza dei sistemi durante lo sviluppo e test di accettazione nell'ambiente operativo di utilizzo, prima di rilasciare il software.

A14 Acquisizione sviluppo e manutenzione dei sistemi

- **Dati di test** (14.3): i dati utilizzati per il test dovrebbero essere scelti evitando di introdurre dati personali ed adottando adeguate misure di protezione, anche al fine di garantirne la riservatezza.

Nel complesso i 13 controlli di questa sezione sono molto dettagliati e comprendono una serie di misure di sicurezza informatica ormai consolidate che riguardano tutti gli aspetti del ciclo di vita del software impiegato da un'organizzazione per la propria attività. Alcuni principi vanno commisurati ad una attenta valutazione dei rischi, poiché una stessa regola di sicurezza informatica (ad es. l'aggiornamento sistematico e tempestivo del software di base) potrebbe non garantire sempre l'integrità e la disponibilità dei sistemi (ad es. errori o malfunzionamenti introdotti dagli ultimi aggiornamenti di un sistema operativo).

A14 Acquisizione sviluppo e manutenzione dei sistemi

❖**A14.1 Requisiti di sicurezza dei sistemi informativi**

- A14.1.1 Analisi e specifica dei requisiti per la sicurezza delle informazioni
- A14.1.2 Sicurezza dei servizi applicativi su reti pubbliche
- A14.1.3 Protezione delle transazioni dei servizi applicativi

A14 Acquisizione sviluppo e manutenzione dei sistemi

❖**A14.2 Sicurezza nei processi di sviluppo e supporto**

- A14.2.1 Politica per lo sviluppo sicuro
- A14.2.2 Procedure per il controllo dei cambiamenti di sistema
- A14.2.3 Riesame tecnico delle applicazioni in seguito a cambiamenti nelle piattaforme operative
- A14.2.4 Limitazioni ai cambiamenti dei pacchetti software
- A14.2.5 Principi per l'ingegnerizzazione sicura dei sistemi
- A14.2.6 Ambiente di sviluppo sicuro

A14 Acquisizione sviluppo e manutenzione dei sistemi

- A14.2.7 Sviluppo affidato all'esterno
- A14.2.8 Test di sicurezza dei sistemi
- A14.2.9 Test di accettazione dei sistemi

❖**A14.3 Dati di test**

- A14.3.1 Protezione dei dati di test

A15 Relazioni con i fornitori

Questo punto di controllo tratta tutti gli aspetti di sicurezza delle informazioni che possono legati al comportamento dei fornitori. Sono state individuate due categorie:

- **Sicurezza delle informazioni nelle relazioni con i fornitori** (15.1): è necessario stabilire una politica ed accordi su tematiche inerenti la sicurezza delle informazioni con i fornitori che accedono agli asset dell'organizzazione; tali accordi devono comprendere requisiti per affrontare i rischi relativi alla sicurezza associati a prodotti e servizi nella filiera di fornitura dell'ICT (cloud computing compreso).
- **Gestione dell'erogazione dei servizi dei fornitori** (15.2): occorre monitorare – anche attraverso audit se necessario – e riesaminare periodicamente le attività dei fornitori che influenzano la sicurezza delle informazioni, nonché tenere sotto controllo tutti i cambiamenti legati alle forniture di servizi.

A15 Relazioni con i fornitori

❖**A15.1** **Sicurezza delle informazioni nelle relazioni con i fornitori**

- A15.1.1 Politica per la sicurezza delle informazioni nei rapporti con i fornitori
- A15.1.2 Indirizzare la sicurezza all'interno degli accordi con i fornitori
- A15.1.3 Filiera di fornitura per l'ICT

❖**A15.2** **Gestione dell'erogazione dei servizi dei fornitori**

- A15.2.1 Monitoraggio e riesame dei servizi dei fornitori
- A15.2.2 Gestione dei cambiamenti ai servizi dei fornitori

Contratti per servizi Cloud

A16 Gestione degli incidenti relativi alla sicurezza delle informazioni

L'area relativa agli incidenti sulla sicurezza delle informazioni (sezione 13 della precedente versione della norma) comprende una sola categoria (erano 2 nella precedente edizione):

- **Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti** (16.1): devono essere rilevati e gestiti tutti gli incidenti relativi alla sicurezza delle informazioni (viene qui richiamata la ISO/IEC 27035 – Information security incident management), ma anche rilevate ed esaminate tutte le segnalazioni di eventi relativi alla sicurezza che potrebbero indurre a pensare che qualche controllo è risultato inefficace senza provocare un vero e proprio incidente e pure tutte le possibili debolezze dei controlli messi in atto. In ogni caso ogni evento relativo alla sicurezza delle informazioni va attentamente valutato per eventualmente classificarlo come incidente vero e proprio o meno. Occorre poi rispondere ad ogni incidente relativo alla sicurezza delle informazioni in modo adeguato ed apprendere da quanto accaduto per evitare che l'incidente si ripeta. Infine dovrebbero essere stabilite procedure per la raccolta di evidenze relative agli incidenti e la successiva gestione (considerando anche eventuali azioni di analisi forense).

A16 Gestione degli incidenti relativi alla sicurezza delle informazioni

❖**A16.1 Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti**

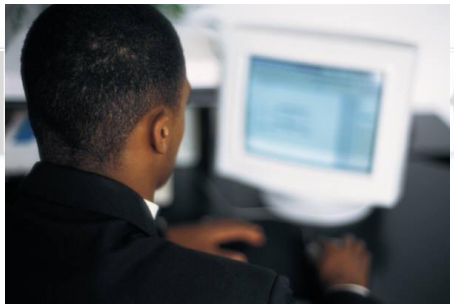
- A16.1.1 Responsabilità e procedure
- A16.1.2 Segnalazione degli eventi relativi alla sicurezza delle informazioni
- A16.1.3 Segnalazione dei punti di debolezza relativi alla sicurezza delle informazioni
- A16.1.4 Valutazione e decisione sugli eventi relativi alla sicurezza delle informazioni

Data breach

A16 Gestione degli incidenti relativi alla sicurezza delle informazioni

- A16.1.5 Risposta agli incidenti relativi alla sicurezza delle informazioni
- A16.1.6 Apprendimento dagli incidenti relativi alla sicurezza delle informazioni
- A16.1.7 Raccolta di evidenze

Electronic Evidence Guide



A17 Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa

In quest'area (corrispondente al punto 14 sella precedente versione della norma) viene trattata la business continuity in 5 controlli suddivisi in due categorie:

- **Continuità della sicurezza delle informazioni** (17.1): la continuità operativa per la sicurezza delle informazioni dovrebbe essere pianificata a partire dai requisiti per la business continuity, piani di continuità operativa (business continuity plan) dovrebbero essere attuati, verificati e riesaminati periodicamente.
- **Ridondanze** (17.2): per garantire la disponibilità (e la continuità operativa) occorre prevedere architetture e infrastrutture con adeguata ridondanza.

Naturalmente sull'argomento esiste la norma specifica UNI EN ISO 22301:2014 – Sicurezza della società – Sistemi di gestione della continuità operativa – Requisiti.

A17 Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa

❖**A17.1 Continuità della sicurezza delle informazioni**

- A17.1.1 Pianificazione della continuità della sicurezza delle informazioni
- A17.1.2 Attuazione della continuità della sicurezza delle informazioni
- A17.1.3 Verifica, riesame e valutazione della continuità della sicurezza delle informazioni
- **A17.2 Ridondanze**
- A17.2.1 Disponibilità delle strutture per l'elaborazione delle informazioni

A18 Conformità

Questo ultimo punto di controllo (era il punto 15 nella ISO 27002:2005) tratta la gestione della cosiddetta “compliance”, ovvero la conformità a leggi, regolamenti ed accordi contrattuali con i clienti. Sono identificate due categorie:

- **Conformità ai requisiti cogenti e contrattuali** (18.1): occorre innanzitutto identificare i requisiti cogenti, quindi attuare controlli per evitare di ledere i diritti di proprietà intellettuale, proteggere adeguatamente le registrazioni che permettono di dimostrare la conformità a tutti i requisiti cogenti, in particolare devono essere rispettati leggi e regolamenti sulla privacy (in Italia il D.lgs. 196/2003 in attesa del nuovo Regolamento Europeo, ma nella norma viene citata come riferimento la ISO/IEC 29100:2011 “Information technology – Security techniques — Privacy framework”). Infine occorre considerare eventuali limitazioni all’uso dei controlli crittografici vigenti in alcune nazioni.
- **Riesami della sicurezza delle informazioni** (18.2): dovrebbe essere svolto periodicamente un riesame indipendente sulla sicurezza delle informazioni dell’organizzazione, i processi di elaborazione delle informazioni e le procedure dovrebbero essere riesaminate periodicamente per valutarne la continua conformità ed adeguatezza alla politica ed alle norme ed infine dovrebbero essere eseguite delle verifiche tecniche della conformità dei sistemi informativi a politiche e standard di sicurezza (ad esempio penetration test e vulnerability assessment). Su quest’ultimo controllo si fa riferimento alla ISO/IEC TR 27008 – Guidelines for auditors on information security management systems controls.

A18 Conformità

❖**A18.1 Conformità ai requisiti cogenti e contrattuali**

- A18.1.1 Identificazione della legislazione applicabile e dei requisiti contrattuali
- A18.1.2 Diritti di proprietà intellettuale
- A18.1.3 Protezione delle registrazioni
- A18.1.4 Privacy e protezione dei dati personali
- A18.1.5 Regolamentazione sui controlli crittografici

A18 Conformità

❖**A18.2 Riesami della sicurezza delle informazioni**

- A18.2.1 Riesame indipendente della sicurezza delle informazioni
- A18.2.2 Conformità alle politiche e alle norme per la sicurezza
- A18.2.3 Verifica tecnica della conformità

Risorse

- Sito web http://www.iso27001security.com/ con possibilità di scaricare free Toolkit e ISO 27000
- Sito web ISO http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
- Sito web UNI www.uni.com
- Siti web di enti ed associazioni specializzate nella sicurezza delle informazioni: Clusit, NIST, AGID, OECD, ecc.

Proteggiamo l'IT ma …

Non dimentichiamoci della carta …

Grazie per l'attenzione

Ing. Andrea Cenni

Auditor ISDP 10003 - Protezione Dati Personali
Valutatore Privacy Uni 11697

andrea.cenni@studioingcenni.it

www.studioingcenni.it

Cell. 328 72 30 906