Le regole applicative della UNI EN ISO 9001:2015

L’adeguamento delle aziende alla norma UNI EN ISO 9001:2015 prosegue a rilento con il solito approccio italiano “qual è la scadenza? Settembre 2018? Bene, cominciamo a pensarci a Giugno 2018 perché poi ci sono le ferie!”

Forse senza sapere che ben difficilmente si riuscirà a migrare in tempo utile, senza perdere la certificazione almeno per qualche mese; se non altro perché gli Organismi di Certificazione non avranno modo di gestire un’elevata mole di adeguamenti negli ultimi mesi del periodo di transizione. Oltre al fatto che se l’adeguamento non viene effettuato in occasione di un rinnovo o di una sorveglianza si spenderà di più.

Ma quali sono i **requisiti aggiuntivi per le aziende italiane** che vogliono recepire questa normativa? Sia in fase di transizione dalla vecchia norma ISO 9001:2008, sia come nuova certificazione di qualità?

Quali sono i contenuti dell’**Appendice C della UNI EN ISO 9001:2015 (versione italiana)** che dovrebbero aiutare le imprese del nostro Paese a recepire nel modo corretto questa norma?

Visto il tenore della nuova norma, infatti, noi italiani abbiamo bisogno di **regole più chiare**, espresse in termini di **obblighi e doveri** (“l’organizzazione DEVE”), senza troppe frasi del tipo “se ritenuto necessario”, “quando necessario”, “conservare informazioni documentate affinché si possa avere fiducia del fatto che…”, “le informazioni documentate che l’organizzazione determina necessarie per…” e così via.

Vediamo sinteticamente quali sono queste regole applicative che dovrebbero agevolare anche il compito dell’auditor dell’Organismo di Certificazione, evitando inutili discussioni su cosa richiede la norma e cosa dovrebbe effettivamente essere presente per dimostrare la conformità del sistema di gestione per la qualità.

1. Se l’organizzazione migra dalla versione 2008 della ISO 9001 avrà un **Manuale Qualità** ed anche se esso non è espressamente richiesto dalla ISO 9001:2015 farà

meglio a tenerselo. Naturalmente revisionandolo e rendendolo più snello, evitando inutili ridondanze con le procedure. Perché comunque il Manuale rappresenta il vertice della c.d. "piramide della documentazione", il documento di maggior sintesi che richiama documenti più di dettaglio (è un po' come il "*main program*" che richiama le varie "*subroutine*" dei programmi software). Del resto eliminando il Manuale, comunque dovremo documentare la Politica, i Processi ed altro…. dove li mettiamo se non nel manuale? Le aziende che pensano in futuro di certificarsi secondo la normativa del settore automotive IATF 16949:2016 considerino che tale standard richiede il manuale qualità.

2. Le **procedure** chi ce le ha se le tenga e chi è di nuova certificazione ci pensi bene a non predisporle. L'evoluzione dell'organizzazione aziendale negli ultimi 20-30 anni è andata sempre verso la definizione in forma documentata delle modalità di svolgimento delle attività, per definire regole precise che devono essere seguite da tutti, per evitare il caos ove ciascuno fa quello che gli pare. Se non ci sono procedure e istruzioni documentate nelle aziende italiane non solo si tende ad interpretare i processi in modo "personalizzato", secondo quello che il singolo ritiene meglio, ma i nuovi nell'incarico non hanno modo di imparare a ricoprire il ruolo perché l'addestramento è sempre scarso e non trovano regole scritte precise su cosa fare e cosa non fare. Ovviamente ci sono casi e casi: in determinate situazioni l'operatività è guidata dai sistemi informativi e, pertanto, non è facile portare a termine attività in modo diverso, per cui dettagliare troppo non serve.
3. L'**analisi del contesto dell'organizzazione** e la **valutazione dei rischi** sono da documentare. Infatti se suddette attività devono essere riesaminate periodicamente (ad esempio in occasione del riesame di direzione) come facciamo a ricordarci quello che abbiamo detto sull'argomento un anno o sei mesi fa se non scriviamo nulla? Quale imprenditore o Direttore Generale riesce ad analizzare il contesto interno ed esterno della propria organizzazione, identificare e valutare i rischi oralmente nello stesso modo a distanza di tempo, senza nemmeno tenersi una traccia scritta? Dal momento che poi le azioni pianificate per affrontare rischi ed opportunità devono essere documentate con tanto di responsabilità, tempi e valutazione dell'efficacia che senso ha documentare le azioni, ma non i rischi che le hanno scaturite?
4. La norma ISO 9001:2015 non richiede più il **Rappresentante della Direzione**, che in molte realtà coincideva con la figura del Responsabile Qualità (ce se diverso dal rappresentante della Direzione non era richiesto neanche prima): non ha nessun senso eliminare il Responsabile Qualità. Alcuni imprenditori che non hanno ben compreso la questione hanno cominciato a dire: "ma allora possiamo eliminare il responsabile qualità, con quello che costa!". In un mondo perfetto nel quale la Qualità è patrimonio di tutti e tutti applicano la norma in modo adeguato il Responsabile Qualità potrebbe effettivamente non servire, ma nelle nostre aziende italiane chi fa e fa fare le cose che servono per mantenere la certificazione senza il Responsabile Qualità? Oggi in molte realtà il Responsabile Qualità non solo svolge più attività di quelle di sua stretta pertinenza, ma costringe gli altri (responsabili di funzione, Direzione ed altri) a fare il loro dovere. Bisognerebbe alzargli lo stipendio, altro che

eliminare la figura!

5. La norma prevede che sia l'organizzazione a determinare "cosa è necessario monitorare e misurare", come e quando farlo per ottenere risultati validi. Ora più di prima è necessario identificare **indicatori** pertinenti con gli obiettivi ed in grado di misurare l'efficacia – se non anche l'efficienza – dei processi. Le aziende non pensino che questa libertà possa permettere loro di decidere gli indicatori a loro convenienza: l'aumento di fatturato per il processo commerciale e il numero assoluto delle non conformità per la produzione non sono indicatori sufficienti a misurare suddetti processi e gli obiettivi di nessuna azienda.
6. La norma non prevede più le **azioni preventive**, ma le azioni finalizzate a migliorare l'efficacia e l'efficienza del Sistema e dei suoi processi sono state rinforzate. Le azioni preventive, ovvero quelle azioni finalizzate ad evitare il verificarsi di non conformità potenziali, sono solo un "di cui" delle azioni di miglioramento: chiamiamole così, non solo AP.

In conclusione la norma ISO 9001:2015 deve essere vista con lo spirito giusto dalle aziende italiane, dimenticandosi di quello che è stato fatto in passato, per evitare di buttare via tempo e denaro per un adeguamento forzoso che non porterebbe alcun vantaggio nel tempo all'impresa. Sarà compito anche degli auditor degli Organismi di Certificazione cercare di far capire alle aziende il reale significato di questa norma, ma bisognerà vedere se avranno tempo e voglia per farlo, soprattutto se osteggiati da rappresentanti dell'azienda e consulenti che affermeranno che la norma non richiede un manuale, non richiede delle procedure e non è prescrittiva per tante altre attività. Il rischio, in tal caso, è che l'auditor alzi bandiera bianca e dica "fate un po' quello che volete… se non avete capito voi a cosa servono certe cose…".

A proposito l'Appendice C della UNI ISO 9001:2015 italiana non esiste, ma è meglio far finta che le regola sopra esposte esistano veramente.

Come e quando migrare alla ISO 9001:2015?

Ad oggi sono molte le organizzazioni certificate ISO 9001:2008 che non hanno ancora adeguato il loro sistema di gestione per la qualità alla nuova ISO 9001:2015. Anche se il termine per effettuare il passaggio alla nuova norma è abbastanza lontano (15/09/2018) i tempi per effettuare una migrazione efficace ed efficiente non sono abbondanti per molte imprese, infatti sarebbe opportuno effettuare la migrazione in occasione di un **rinnovo della certificazione** oppure di una **visita di sorveglianza/mantenimento** al fine di contenere i costi di certificazione.

Questo perché in occasione degli audit di rinnovo l'Organismo di Certificazione già deve verificare tutti i processi dell'organizzazione e la documentazione di sistema, dunque i costi aggiuntivi sono minimi, se non addirittura nulli.

Negli audit di sorveglianza richiedere l'adeguamento alla ISO 9001:2015 potrebbe essere un po' più oneroso, ma per quelle organizzazioni che hanno la scadenza del certificato oltre la data limite per l'adeguamento (14 settembre 2018) questa è l'occasione migliore per passare alla nuova norma.

Visto che ormai il 2016 è passato, resta di fatto poco più di un anno e mezzo, ovvero solo una o due visite dell'Organismo di Certificazione – a seconda dei casi – per effettuare il passaggio, che comunque dovrà avvenire durante un audit svolto con congruo anticipo rispetto alla data limite sopra indicata, per consentire all'Ente di sbrigare tutte le pratiche necessarie per il rinnovo del certificato in ISO 9001:2015.

Le organizzazioni che avranno la visita dell'Organismo di Certificazione nella seconda parte dell'anno avranno solo una occasione per rinnovare il loro certificato secondo queste modalità.

Rimandare eccessivamente può portare a costi aggiuntivi, infatti sarebbe necessario richiedere una visita straordinaria nell'estate 2018 (probabilmente prima della chiusura per ferie di agosto) per rinnovare in tempo il certificato, consci del fatto che lasciare scadere il certificato vorrà dire perdere di fatto la certificazione ISO 9001 e, quindi, dover intraprendere l'iter dal principio per riottenere la certificazione di qualità. In questi casi sicuramente ci sarebbero costi aggiuntivi.

Ma quale sono le ragioni dell'evidente attendismo di molte imprese nell'effettuare il passaggio? Le principali motivazioni possono probabilmente riassumersi nelle seguenti:

- Posticipare i costi di adeguamento (organismo di certificazione, consulenza,

impegno interno,…);
- Incertezza sul mantenimento della certificazione oltre la scadenza del certificato;
- Incertezza sul futuro dell'organizzazione;
- Timore sull'impatto dell'adeguamento nell'organizzazione interna.

Sicuramente la prospettiva nel breve termine di molte piccole imprese è sui processi primari essenziali (produzione, commerciale) e viene evitato tutto ciò che porta impegno e costi su altri processi, soprattutto in realtà sottodimensionate in termini di risorse. Evidentemente non è stata adeguatamente compresa la portata di questa norma e del **sistema di gestione per la qualità come reale strumento di gestione**, **di controllo e di miglioramento di tutta l'azienda**. Un po' di paura nell'affrontare un cambiamento normativo non indifferente come quello del 2008 completa il quadro di parecchie organizzazioni.

Le interpretazioni sbagliate sulla nuova norma ISO 9001:2015 non mancano, da quelle eccessivamente "terroristiche" (requisiti molto più difficili da soddisfare) a quelle eccessivamente semplicistiche (si può buttare via il manuale e tutte le procedure ed anche rottamare il responsabile qualità).

Le linee guida UNI-Conforma, la linea guida ISO/TS 9002:2016 da poco pubblicata ed altri documento potrebbero aiutare nella corretta interpretazione dei requisiti.

L'approccio corretto – a mio parere – dovrebbe essere quello di pianificare l'adeguamento per tempo, allocando le risorse necessarie al progetto. Purtroppo molte organizzazioni chiedono e continueranno a chiedere "*quanto costa passare alla nuova norma*?", "*quanto tempo ci si mette?*". A queste domande non c'è una risposta univoca corretta e rivolgersi al tal consulente piuttosto che ad altri solo perché promette costi e tempi inferiori è un grave errore che molti imprenditori commetteranno.

Costi e **tempi** per l'adeguamento dipendono da svariati fattori:

- Il sistema qualità è stato mantenuto aggiornato alla realtà aziendale oppure è obsoleto, modificato solo a fronte di rilievi dell'organismo di certificazione?
- I processi sono adeguatamente descritti oppure sono delineati in modo minimale e generico?
- Vengono sistematicamente calcolati e monitorati indicatori idonei a misurare le prestazioni dei processi oppure sono gestiti solo pochi indici standard poco aderenti alla realtà aziendale?
- La Direzione vuole semplicemente mantenere il certificato con il minimo sforzo oppure vuole sfruttare questo strumento per tenere sotto controllo l'organizzazione e cercare di migliorare?

Dalle risposte a queste domande si può capire meglio il lavoro che sarà da fare.

Situazioni con organizzazioni vicine alle prime parti delle domande sopra riportate sarebbero difficilmente certificabili secondo la nuova norma ISO 9001:2015, ma probabilmente lo saranno ugualmente ingannando se stesse. Il risparmio di tempi e costi nell'adeguamento potrà essere pagato in futuro mantenendo prassi obsolete e non efficienti, contrarie al vero spirito della norma.

Il tanto vituperato appesantimento della norma sulla certificazione di qualità, soprattutto dal punto di vista documentale, in realtà non esiste, a maggior ragione ora che bisogna "mantenere le informazioni documentate che servono". Il problema che molti detrattori della ISO 9001 non si rendono conto che molte evidenze (informazioni documentate) servono anche a cautelarsi quando qualcosa va storto (gestione dei rischi).

Di fatto molte piccole e medie imprese italiane sono lontane dai principi ispiratori della nuova norma sui sistemi di gestione per la qualità, ma non è detto che per ottenere la certificazione serva essere completamente in linea con essi, il percorso di miglioramento potrebbe essere più lungo, la verifica di passaggio alla ISO 9001:2015 potrebbe evidenziare molti rilievi, ma pian piano le carenze potranno essere eliminate e l'azienda potrà essere condotta su principi di gestione migliori di quelli attuali, secondo standard internazionali riconosciuti.

Operativamente la maggior parte dei sistemi qualità ISO 9001:2008 necessiterà delle seguenti attività:

- **Formazione del personale** sulla norma ISO 9001:2015;
- Identificazione e descrizione del **contesto dell'organizzazione**;
- **Valutazione dei rischi** di business (generali e specifici dei vari processi aziendali), attività che passa attraverso l'identificazione dei rischi, la loro ponderazione e la definizione delle misure da porre in essere per il loro trattamento;
- Revisione della **mappatura dei processi** (il livello di approfondimento dipende dallo stato del sistema qualità esistente);
- Rivalutare l'insieme di indicatori da monitorare (anche in questo caso dipende da cosa esiste attualmente);
- Revisione della **documentazione del sistema qualità** esistente: sicuramente il manuale qualità andrà per lo meno snellito, procedure e istruzioni saranno da aggiornare per riferimenti obsoleti, per recepire le azioni di trattamento dei rischi, per aggiornarle alla realtà aziendale e migliorarle in ottica di efficacia ed efficienza;
- Sottoporre ad **audit interno** il sistema di gestione per la qualità secondo le prassi abituali;

- Effettuare un **riesame della direzione** sul sistema di gestione per la qualità che recepisca i nuovi elementi.

L'eliminazione di documenti di tipo procedurale e il non tener evidenza documentale di talune attività (analisi del contesto, valutazione dei rischi, …) sono false semplificazioni, adatte solo a chi sa recitare senza leggere il copione, ovvero ad organizzazioni che hanno ben chiaro il proprio contesto organizzativo, i propri rischi, le azioni attuate per mitigarli, le procedure aziendali e tutte le prassi da adottare a tutti i livelli dell'organizzazione.

Le attività da completare potrebbero essere non eccessivamente impegnative e non tutte devono necessariamente essere completate prima della visita di certificazione.

Se in qualche caso l'impegno appare eccessivamente gravoso è perché probabilmente non è stato fatto nulla o quasi negli anni scorsi per mantenersi aggiornati. L'inadeguatezza della gestione attuale rispetto ai requisiti della norma ISO 9001:2015 e l'elevato gap da colmare per raggiungere la conformità con la nuova norma dovrebbe far riflettere la Direzione sul fatto che la gestione aziendale non è andata al passo coi tempi.

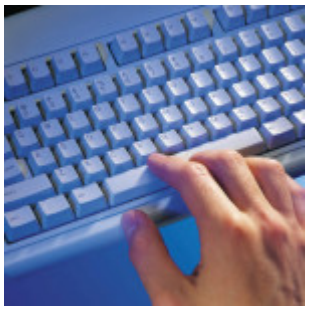
Esempi di questa situazione si possono trovare quando:

- risulta difficoltoso correlare strategie, politiche ed obiettivi aziendali;
- risulta estremamente impegnativo individuare e soprattutto calcolare indicatori idonei a misurare gli obiettivi e le prestazioni dei processi in termini di efficacia ed efficienza;
- emergono rischi importanti non adeguatamente gestiti;
- emergono carenze di risorse umane e delle relative competenze necessarie;
- emerge che la conoscenza organizzativa ed il know-how aziendale non è curato e tutelato adeguatamente;
- risultano carenze dal punto di vista tecnologico: hardware e software obsoleti, strumenti inadeguati, ecc.

In tutti questi casi la nuova norma ISO 9001:2015 può rappresentare un **valido strumento e stimolo per migliorare l'efficacia e l'efficienza interna**, molto più che costituire un obbligo certificativo.

La nuova edizione della norma ISO

27002 (seconda parte)



In questo articolo (cfr. precedente articolo) passiamo ad esaminare la seconda parte della norma La norma UNI CEI ISO/IEC 27002:2014 – *Raccolta di prassi sui controlli per la sicurezza delle informazioni* (che sostituisce la ISO 27002:2005).

12 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.
- **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.

Questi elementi nella precedente versione della norma erano in gran parte all'interno della sezione 10 "*Communications and Operations Management*" (ma la gestione delle vulnerabilità tecniche era, invece, al paragrafo 12.6, per puro caso lo stesso della versione attuale della norma), il quale comprendeva anche i controlli del punto 13 seguente.

13 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, …).
- **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.

14 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.
- **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).

15 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.

16 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).

17 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.*

18 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*.

Le novità della UNI ISO 27001:2014

La norma ISO 27001 pubblicata nel 2013 è stata tradotta in italiano e convertita in norma UNI nel marzo 2014 come UNI CEI ISO/IEC 27001:2014 – *Tecnologie informatiche – Tecniche per la sicurezza – Sistemi di gestione per la sicurezza delle informazioni – Requisiti*. Essa specifica i requisiti per stabilire, attuare, mantenere e migliorare in modo continuo un **sistema di gestione per la sicurezza delle informazioni** nel contesto di un'organizzazione, includendo anche i requisiti per **valutare e trattare i rischi** relativi alla sicurezza delle informazioni adattati alle necessità dell'organizzazione.

La nuova ISO 27001 non riporta termini e definizioni, ma richiama la ISO 27000.2014 (scaricabile gratuitamente da http://www.iso27001security.com/html/27000.html e curiosamente venduta dall'UNI a € 138) per tutti i termini utilizzati nelle norme della serie ISO 27k.

Si segnala che nel capitolo introduttivo della ISO 27001 è scomparso il paragrafo "Approccio per processi", sebbene venga sottolineata l'importanza che il sistema di gestione per la sicurezza delle informazioni sia parte integrante dei processi e

della struttura gestionale complessiva dell'organizzazione.

La norma ISO 27001 riprende la nuova struttura di tutte le norme sui sistemi di gestione e, pertanto, al capitolo 4 tratta il "contesto dell'organizzazione". In questo capitolo viene esposto che per **comprendere l'organizzazione e il suo contesto** (4.1) occorre determinare i fattori esterni ed interni pertinenti alle finalità dell'organizzazione stessa e che influenzano la sua capacità di conseguire i risultati previsti per il proprio sistema di gestione per la sicurezza delle informazioni e che per **comprendere le necessità e le aspettative delle parti interessate** (4.2) occorre individuare le parti interessate al sistema di gestione per la sicurezza delle informazioni ed i requisiti delle stesse attinenti ad esso.

Anche la determinazione del **campo di applicazione del Sistema di Gestione per la Sicurezza delle Informazioni** (SGSI o ISMS, *Information Security Management System*) è un'attività inerente la comprensione dell'organizzazione ed il suo contesto. In questo ambito l'organizzazione deve determinare i **confini di applicabilità** del sistema di gestione per la sicurezza delle informazioni ISO 27001 al fine di stabilirne il campo di applicazione, in modo analogo a quanto avveniva nella versione precedente della norma, considerando anche i **fattori esterni ed interni** ed i **requisiti delle parti interessate** esposti ai paragrafi precedenti.

Il capitolo 5 **"Leadership"** rispecchia anch'esso la nuova struttura delle norme sui sistemi di gestione. In esso, al paragrafo 5.1, viene indicato quali modalità l'alta direzione deve attuare per dimostrare leadership e impegno nei riguardi del sistema di gestione per la sicurezza delle informazioni. In analogia con altri sistemi di gestione, l'alta direzione deve stabilire **politica** ed **obiettivi**, mettere a disposizione le **risorse necessarie** per l'attuazione del SGSI, **comunicare** l'importanza di **un'efficace gestione della sicurezza delle informazioni** e dell'essere **conforme ai requisiti** del SGSI stesso; deve, inoltre, assicurare che il SGSI ISO 27001 consegua i risultati previsti, fornire guida e sostegno al personale per contribuire all'efficacia del sistema di gestione della sicurezza delle informazioni e, naturalmente, deve promuovere il miglioramento continuo.

Il paragrafo 5.2 tratta della **politica per la sicurezza delle informazioni** per la quale i requisiti sono analoghi a quelli presenti negli altri sistemi di gestione: naturalmente la politica deve essere documentata, comunicata all'interno dell'organizzazione ed essere disponibile a tutte le parti interessate.

Anche il paragrafo 5.3 – che riguarda **ruoli, responsabilità e autorità nell'organizzazione** – è molto simile a quanto riportato nelle altre norme sui sistemi di gestione; in particolare, il fatto che la l'alta direzione debba assegnare responsabilità e autorità per assicurare che il sistema di gestione per la sicurezza delle informazioni sia conforme ai requisiti della norma e per riferire alla direzione stessa sulle prestazioni del sistema di gestione per la sicurezza delle informazioni, se non definisce la **nomina di un responsabile per il sistema di gestione della sicurezza delle informazioni** poco ci manca. Pur non essendo richiesto

un rappresentante della direzione (non lo era neanche nella versione 2005 ISO e 2006 UNI della norma) viene rafforzato il concetto che è necessario assegnare responsabilità precise, all'interno o all'esterno dell'organizzazione (consulente), per garantire la conformità del SGSI.

Il capitolo 6 "**Pianificazione**" tratta, nel paragrafo 6.1, quali azioni occorre attuare per affrontare **rischi ed opportunità**. Infatti sulla base di quanto emerso dall'analisi del contesto dell'organizzazione occorre determinare i rischi e le opportunità che è necessario affrontare per assicurare che il sistema possa conseguire i risultati previsti, possa prevenire, o almeno ridurre, gli effetti indesiderati e realizzare il miglioramento continuo. Le **azioni per affrontare rischi ed opportunità** devono essere **pianificate**, così come le modalità per **integrare ed attuare** le azioni stesse nei processi del proprio sistema di gestione per la sicurezza delle informazioni e per **valutare l'efficacia** di tali azioni.

La **valutazione dei rischi relativi alla sicurezza delle informazioni** è trattata al paragrafo 6.1.2, dove sono riportati i requisiti per il **processo di valutazione del rischio** relativo alla sicurezza delle informazioni. Il processo di valutazione del rischio dovrà comprendere le seguenti attività

- Stabilire e mantenere i criteri di rischio relativo alla sicurezza.
- Assicurare che le ripetute valutazione del rischio producano risultati coerenti, validi e confrontabili tra loro (il metodo usato deve essere ripetibile e riproducibile con risultati coerenti come se fosse un dispositivo di misurazione sotto conferma metrologica).
- Identificare i rischi relativi alla sicurezza.
- Analizzare i rischi individuati, valutando le possibili conseguenze che risulterebbero se tali rischi si concretizzassero e valutando la verosimiglianza realistica di concretizzarsi dei rischi identificati, ovvero la probabilità che essi accadono, e, infine, determinando i livelli di rischio.
- Ponderare i rischi comparando i risultati dell'analisi dei rischi con i criteri stabiliti e definendo le priorità di trattamento dei rischi precedentemente valutati.

Naturalmente **la valutazione dei rischi deve essere documentata.**

Il **trattamento del rischio** relativo la sicurezza delle informazioni (6.1.3) deve essere definito ed applicato attraverso un processo del tutto similare a quello stabilito nella versione precedente della norma, anche se esposto in modo differente. Oltre a selezionare l'opzione di trattamento dei rischi consuete occorre determinare i controlli necessari per attuare le opzioni selezionate per il trattamento del rischio, tenendo presente controlli riportati nell'appendice A e meglio dettagliati nella norma ISO 27002 (anch'essa tradotta finalmente in italiano come UNI CEI ISO/IEC 27002:2014 – *Tecnologie informatiche – Tecniche per la sicurezza – Raccolta di prassi sui controlli per la sicurezza delle informazioni*) al fine di non omettere controlli che potrebbero essere necessari.

Resta la necessità di redigere una **Dichiarazione di Applicabilità** che riporti:

- i controlli selezionati come necessari (che siano attuati o meno) e la relativa giustificazione per l'inclusione;
- i controlli presenti nell'Appendice A della ISO 27001 stessa eventualmente esclusi con le giustificazioni per la loro esclusione
- i controlli selezionati attualmente applicati.

Quest'ultimo punto costituisce una novità nel testo della norma che chiarisce e sancisce una prassi comunemente adottata dagli Organismi di Certificazione, ovvero quella di accettare una dichiarazione di applicabilità di determinati controlli di sicurezza la cui attuazione è stata pianificata, ma deve ancora venire.

Infine occorre predisporre un **piano di trattamento dei rischi** relativi alla sicurezza delle informazioni che dovrà essere approvato dalla Direzione, comprendente anche l'accettazione dei rischi residui che si è deciso di non trattare.

Anche questo **processo di trattamento del rischio dovrà essere documentato**.

Il sistema di gestione per la sicurezza delle informazioni ISO 27001 dovrà porsi degli **obiettivi** e **pianificare le azioni adeguate per conseguirli** (paragrafo 6.2). Le caratteristiche degli obiettivi sono le stesse degli altri sistemi di gestione (devono essere coerenti con la politica, misurabili, ecc.).

La pianificazione delle azioni poste in essere per conseguire gli obiettivi per la sicurezza delle informazioni deve comprendere le **azioni** pianificate, le **risorse** necessarie, le **responsabilità**, i **tempi** di completamento delle azioni, e le **modalità** di **valutazione dei risultati**.

Il capitolo 7 "**Supporto**" non presenta novità significative rispetto all'analogo capitolo delle altre norme relative ad altri sistemi di gestione. Pertanto i paragrafi **Risorse** (7.1), **Competenza** (7.2) Consapevolezza (7.3) e **Comunicazione** (7.4) non presentano sorprese di sorta, ma solo una esplicitazione più chiara rispetto al passato di cosa ci si dovrebbe attendere da un sistema di gestione per la sicurezza delle informazioni.

Il paragrafo 7.5 "**Informazioni documentate**" con i suoi sotto paragrafi descrive i requisiti relativi a **documenti** e **registrazioni,** secondo la dizione delle precedenti norme sui sistemi di gestione. Anche in questo caso i requisiti non presentano novità rispetto al passato, ma solo un diverso ordine di esposizione ed una maggior chiarezza nel descrivere che cosa ci si aspetta da un sistema di gestione documentato.

Non sono richieste procedure particolari, né un manuale del sistema di gestione ISO 27001, ma solo le informazioni documentate indicate nei vari punti della norma.

Il capitolo 8 “**Attività operative**” dispone requisiti relativi ai punti:

- pianificazione e controlli operativi (8.1);
- valutazione del rischio relativo la sicurezza delle informazioni (8.2);
- trattamento del rischio relativo la sicurezza delle informazioni (8.3).

In questo capitolo non ci sono novità rispetto alla versione precedente della norma, ma solo una riscrittura secondo la nuova struttura delle norme sui sistemi di gestione di quanto era già prescritto in passato. I contenuti, in verità, sono alquanto scarni, infatti viene prescritto di mantenere sotto controllo i processi operativi dell’organizzazione (processo produttivo o erogazione del servizio, approvvigionamenti, commerciale, ecc.) attraverso l’attuazione di tutti i controlli di sicurezza pianificati, monitorando ogni cambiamento e rivalutando periodicamente i rischi secondo le modalità già descritte nei paragrafi deò capitolo 6.

Il capitolo 9 “**Valutazione delle prestazioni**”, riporta i requisiti per il **monitoraggio**, la **misurazione**, **l’analisi** e la **valutazione** (9.1) del SGSI, per gli **audit** interni (9.2) e per il **riesame della direzione** (9.3). Anche in questo capitolo non sono presenti novità sostanziali rispetto alla precedente versione della norma, ma solo una riscrittura del testo in modo più chiaro. In particolare viene indicata la necessità di monitorare e misurare l’efficacia dell’attuazione dei controlli di sicurezza e tutti i processi che forniscono evidenza del buon funzionamento del SGSI.

Nel capitolo 10 “**Miglioramento**” sono trattate **non conformità**, **azioni correttive** e **miglioramento continuo**. Anticipando quello che avverrà per la prossima versione della norma ISO 9001:2015, si rileva l’eliminazione delle requisito riguardante le **azioni preventive** che vanno a confluire insieme a tutte le azioni di miglioramento non legate a non conformità o incidenti sulla sicurezza delle informazioni.

È curioso il fatto che mentre nella versione precedente la norma ISO 27001 non dedicava un paragrafo alle non conformità, che venivano citate nel testo, ma erano citati anche gli **incidenti** per la sicurezza delle informazioni, questa nuova versione non tratta gli incidenti – se non nei controlli dell’appendice A – e dedica il paragrafo 10.1 alle non conformità ed alle azioni correttive attuate per eliminarle.

Si ricorda che ACCREDIA ha disposto che Tutte le certificazioni emesse sotto accreditamento a fronte della ISO/IEC 27001:2005 dovranno essere ritirate entro il 1° ottobre 2015; oltre tale data potranno sussistere solo certificazioni secondo la nuova ISO 27001:2013. Pertanto restano pochi mesi per convertire i vecchi SGSI alla nuova norma. Probabilmente la stragrande maggioranza delle organizzazioni con SGSI certificato o certificando ISO 27001 dispongono già della certificazione ISO 9001 per la qualità, ma la nuova norma ISO 9001:2015, la cui struttura è allineata alla ISO 27001:2013 deve ancora essere ufficialmente emessa.

Il consiglio per le organizzazioni che si stanno adeguando alla 27001:2013 è quello di strutturare il sistema di gestione integrato secondo il nuovo schema, dunque allineare anche il sistema di gestione per la qualità sulla base delle indicazioni disponibili dalla bozza di ISO 90001:2015. Così facendo si avrà un sistema di gestione integrato ISO 9001-27001 omogeneo e meglio gestibile nell'immediato.

Questo probabilmente comporterà ristrutturare il manuale del sistema di gestione, anche se non esplicitamente richiesto dalla nuova norma, al fine di mantenere una continuità con il passato e garantire il controllo su tutta la documentazione del sistema di gestione.

Le modifiche al SGSI non sono sostanziali e riguardano più che altro i 114 controlli di sicurezza dell'appendice A e della ISO 27002 che naturalmente impattano sul trattamento dei rischi e sulla Dichiarazione di Applicabilità (*Statement of Applicability*, SoA).

La certificazione SSAE 16 per i servizi in outsourcing

Oggi le imprese tendono ad **esternalizzare molti processi ed attività secondarie** al fine di ottimizzarne i costi e la qualità del servizio risultante che, se svolto da personale specializzato, è spesso superiore a quella ottenibile con personale interno.

Alcune di queste attività – ad esempio la gestione delle paghe e del personale, l'acquisizione di documenti e dati in formato digitale e la relativa archiviazione sostitutiva, la gestione contabile e fiscale, i servizi informatici, ecc. – prevedono la **gestione di informazioni critiche dal punto di vista della** riservatezza e degli aspetti legali e di compliance ad essi correlati.

Per questo motivo alcune aziende internazionali – multinazionali o grandi gruppi con sedi all'estero, in particolare negli Stati Uniti – richiedono, alle loro filiali o consociate italiane, evidenza della **buona gestione dei servizi affidati in outsourcing**.

Per le aziende soggette a tale standard la **Sezione 404 del Sarbanes-Oxley Act (SOX)**

richiede che i fornitori di servizi in outsourcing siano provvisti di una particolare certificazione, il **Report SSAE 16**, per **garantire che controlli e processi interni siano appropriati alla gestione delle informazioni dei propri clienti**.

La crescente richiesta di **servizi in outsourcing** pone, quindi, l'esigenza da parte delle organizzazioni che forniscono servizi in outsourcing delle tipologie sopra elencate (payroll, contabilità, gestione documentale, …) di fornire ai propri clienti e ad altri soggetti un rapporto di revisione completo sui sistemi di controllo e sui processi, al fine di assicurare che i servizi erogati alla clientela siano sicuri e conformi a uno standard riconosciuto.

La **certificazione SSAE no. 16** è il nuovo standard per effettuare la reportistica sui controlli nelle aziende di servizi – sostituendo la precedente SAS no. 70 – e risponde alla domanda crescente di disporre di regole conformi a standard internazionali riconosciuti in tutto il mondo, migliorativi rispetto ad una semplice certificazione ISO 9001.

Il report SSAE 16 (*Statement on Standards for Attestation Engagements no. 16*) viene rilasciato da auditor indipendenti qualificati dall'AICPA (dall'*American Institute of Certified Public Accountants)* dopo un articolato processo di analisi dei processi interni, confronto degli stessi con un'apposita matrice di controlli che produrrà una *gap analysis* la quale costituirà il punto di partenza per portare, attraverso l'introduzione di idonei controlli ed apposita documentazione procedurale, alle verifiche di efficacia dei controlli implementati atti a garantire l'adeguatezza degli stessi e delle informazioni processate.

Il report SSAE 16 costituisce un'esaustiva fotografia del funzionamento dell'organizzazione di servizi e dei controlli implementati per garantire non solo la conformità del servizio, ma anche la sicurezza nella gestione dei dati elaborati.

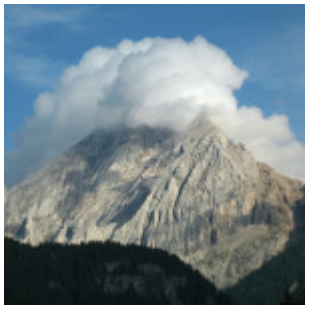
Il processo che porta alla certificazione SSAE 16 comprende una dettagliata **mappatura dei processi organizzativi** e dei **flussi informativi** che permette di effettuare la **mappatura degli obiettivi di controllo, delle criticità e dei rischi**, finalizzata alla **valutazione dei rischi** (*risk assessment*), imprescindibile punto di partenza per qualsiasi **sistema di controllo interno**.

Sebbene questo schema SSAE 16 ricalchi per alcuni elementi la certificazione ISO 9001 e la certificazione ISO 27001, esso presenta una valenza particolare in determinati settori e costituisce il logico completamente in un percorso di miglioramento e di qualificazione dell'organizzazione di servizi nei confronti del cliente.

Tale certificazione, si ribadisce, è rivolta in particolare alle seguenti organizzazioni di servizi:

- Servizi di gestione paghe del personale
- Acquisizione dati e documenti in formato digitale
- Conservazione sostitutiva
- Servizi contabili e fiscali
- Servizi di assistenza e sviluppo software.

Cosa hanno in comune privacy, cloud computing e business continuity?



In precedenti articoli (Il cloud computing e la PMI, i sistemi di gestione della sicurezza delle informazioni, ISO 22301 e la business continuity, le novità sulla privacy) abbiamo affrontato tutti questi argomenti che, indubbiamente, hanno un unico filo conduttore.

Oggi molte aziende, fra cui anche numerose PMI, hanno dati "nel *cloud*", ovvero memorizzati in risorse fisiche non collocate all'interno dell'azienda, bensì su internet, magari senza rendersene conto. Infatti, oltre a veri e propri servizi *cloud* erogati da fornitori specializzati, molte PMI utilizzano servizi di archiviazione gratuiti quali SkyDrive, Dropbox o Google Drive in maniera non strutturata, in quanto sono propri reparti o uffici o addirittura singoli collaboratori che, per praticità, hanno pensato di sfruttare suddetti *tool* di archiviazione remota.

In altri casi alcune organizzazioni utilizzano software via web che memorizzano i dati su server remoti, magari presso il fornitore del software (spesso si tratta di Saas, *Software as a Service*).

Tra i principali aspetti negativi che hanno generato diffidenza sull'archiviazione nel *cloud* c'è sicuramente la **sicurezza dei dati**, declinata in termini di **riservatezza**. Molti imprenditori, infatti, hanno la sensazione che alcuni dati riservati (informazioni commerciali, proprietà intellettuale relativa a progetti, ecc.) debbano rimanere in azienda per paura che qualcuno li possa consultare.

Normalmente una PMI, specialmente una piccola impresa, non effettua un'adeguata **valutazione dei rischi** che corre e, pertanto, valuta questo argomento a sensazione, piuttosto che con fatti concreti. Quali sono infatti i rischi reali?

In una logica di *Risk Assessment*, naturalmente, ogni impresa fa storia a se; bisogna conoscere quali dati vorrebbe mettere sul cloud, qual è il livello di riservatezz**a** che tali dati devono avere, se si tratta di dati sensibili, quali **procedure di backup** sono implementate, di che tipo di **connessione internet** si dispone e così via.

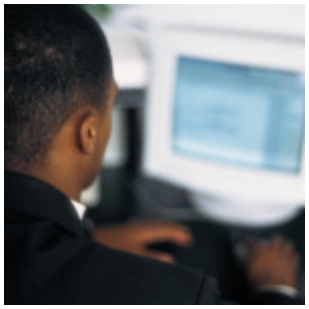
In linea generale parlare di dati poco sicuri nel *cloud* perché si teme che qualcuno possa "guardarci dentro" non ha molto senso: a parte che bisognerebbe valutare quale livello di sicurezza ci si aspetta per ogni tipo di dato (si veda il precedente articolo sulla valutazione dei rischi per la sicurezza delle informazioni), oggi molti *repository* di dati nel *cloud* forniscono ampie garanzie di sicurezza, soprattutto se sono gestiti da importanti player del settore, quali Microsoft, Google, Amazon, ecc.

Se, come al solito, decliniamo il termine **Sicurezza** in **Riservatezza**, **Integrità** e **Disponibilità** (ISO 27000 *docet*) e valutiamo nel complesso **il livello di rischio che incombe sui dati nel cloud**, vediamo che, a fronte di un **livello di riservatezza più che adeguato** (i dati di una PMI nel cloud normalmente sono sufficientemente protetti da sguardi indiscreti, grazie alle misure di sicurezza informatica che i fornitori più seri offrono ormai per *default*), certamente superiore a quello che si può ottenere all'interno dell'azienda stessa (dove potrebbero esserci soggetti interessati a curiosare dove non dovrebbero) la garanzia di **integrità dei dati** è più che buona, ma sulla **disponibilità** degli stessi occorre fare qualche riflessione.

Su quest'ultimo aspetto incide non solo l'affidabilità del fornitore di servizi *cloud* e dell'infrastruttura di cui dispone, ma anche la **connessione internet** che, ancora ogg,i non è sicuramente adeguata in molte imprese italiane, sia per **velocità**, sia per **continuità del servizio**. È proprio questo l'anello di congiunzione con la **continuità operativa**, più elegantemente detta ***business continuity***.

Infine la **privacy**, ovvero la **protezione dei dati personali** con la relativa legge italiana (D.Lgs 196/2003) ed il **nuovo Regolamento Europeo** che sarà emanato

probabilmente il prossimo anno. In questo ambito un Parere della Commissione Europea del 2012 ha per il momento fugato molti dubbi sulle garanzie legali che un'impresa dovrebbe richiedere al proprio fornitore di servizi cloud per essere tranquilla di non incorrere in pesanti problemi legali.



Probabilmente molti **contratti** che regolamentano la fornitura di servizi *cloud* (spesso mascherati sotto la fornitura di *software as a service*) non cautelano adeguatamente l'organizzazione che, non dimentichiamolo, è **titolare del trattamento dei dati** memorizzati in un server chissà dove. È prassi consolidata, infatti, di numerosi fornitori di SaaS di spostare i database dei propri clienti nello spazio web più conveniente per rapporto qualità/prezzo, non importa se in Canada o in Australia In tali situazioni le aziende non dovrebbero dimenticare che come titolari del trattamento sono i **responsabili di fronte alla legge su eventuali inosservanze del Codice della Privacy** e che "esportare" i dati personali fuori dalla Comunità Europea non è sempre possibile, come minimo occorre richiedere il consenso dell'interessato.

Dunque quali interrogativi deve porsi un'azienda coscienziosa prima di affidare i propri dati al *cloud*?

Vediamo i principali, fermo restando che solo dopo una precisa valutazione dei rischi si può determinare quali aspetti sono più critici in ogni singola realtà.

1. Il contratto con il fornitore mi garantisce adeguatamente rispetto alla normativa sulla privacy?
2. Il livello di riservatezza necessario sui dati è adeguatamente garantito da misure di sicurezza dichiarate contrattualmente dal fornitore?
3. La disponibilità dei dati garantita contrattualmente (SLA) è adeguata alle mie esigenze?
4. Posso rientrare in possesso dei miei dati quando voglio e senza costi eccessivi?
5. Il fornitore è sufficientemente affidabile? Si serve di subfornitori egualmente affidabili e resi noti contrattualmente?
6. In caso di perdita dei dati quali sistemi di *disaster recovery* mi garantiscono di rientrare operativo nel più breve tempo possibile? Tale tempo è coerente con le mie esigenze operative?
7. So esattamente in quale stato o area geografica sono memorizzati i miei dati?
8. Ho considerato tutti i possibili fattori di rischio che possono incombere sulla mia continuità operativa?
9. Ho definito gli obiettivi di disponibilità del servizio e di *business continuity* in caso di situazione di crisi?
10. Sono in grado di monitorare il comportamento del fornitore ed eventualmente sottoporlo ad audit sul rispetto dei vincoli contrattuali?

Oggi esistono molti sistemi per garantirsi un futuro tranquillo con i dati nel

cloud, ad esempio seguendo i principi ed i metodi indicati dalle **norme della famiglia ISO 27000** (ISO 27001 che riporta i requisiti di un **sistema di gestione della sicurezza delle informazioni** certificabile, ISO 27002 che riporta le *best practices*, ovvero i controlli che possono essere messi in atto, ISO 27005 che è la linea guida per il *risk assessment*, …) includendovi i requisiti cogenti per la privacy in vigore in Italia ed in Europa. Se il problema di mantenere una certa continuità operativa costituisce un fattore critico si può adottare la metodologia esposta nella ISO 22301 ed in altri standard e linee guida sull'argomento.

Mediante gli stessi sistemi ci si può garantire in modo adeguato nei confronti del fornitore, ad esempio esaminando il contratto con un supporto legale competente, verificare se il fornitore dispone di certificazioni ISO 9001, ISO 27001, ISO 22301 oppure dispone di un Report SSAE 16 ("*Statement on Standards for Attestation Engagements*" n. 16 , standard AICPA per il reporting sui controlli alle organizzazioni che forniscono servizi in outsourcing, richiesto dalle aziende soggette al *Sarbanes-Oxley Act* o SOX, Sezione 404).

Se ascoltiamo quello che ci raccontano gli esperti di sicurezza informatica che relazionano nei frequenti seminari o convegni sull'argomento non c'è certo da stare tranquilli nemmeno all'interno della propria azienda (tra *ransomware* e *data leakage* ogni tanto nascono minacce sempre più terrificanti per il futuro delle nostre imprese, senza dimenticare il comportamento dei collaboratori disonesti) e, quindi, un cloud consapevole può veramente essere una buona cosa.

Dall'altra parte la *software house* che fornisce applicazioni *web-based* con l'opzione di memorizzare i dati, anziché su un server interno all'azienda, su un server remoto (ovvero nel *cloud*) dovrebbe prendere in considerazione tutti gli aspetti sopra esposti, sia al fine di fornire un servizio pienamente conforme alle normative applicabili e di piena soddisfazione di tutte le esigenze del cliente, sia al fine di non incorrere in problemi legali nel caso in cui qualcosa andasse storto, anche solo a causa del proprio fornitore di servizi cloud. Dunque valutare quali tipi di dati verranno archiviati nel cloud dai propri clienti e quali garanzie forniscono i fornitori di spazio di archiviazione a cui ci si rivolge (le **caratteristiche di un data center sicuro** sono state esposte in un articolo apparso lo scorso anno sulla rivista INARCOS).

In conclusione, come per qualsiasi decisone o progetto strategico, le aziende (clienti e fornitori) dovrebbero valutare con adeguate competenze la situazione nel suo complesso ed i rischi che si potrebbe correre. Purtroppo tali competenze, informatiche, legali e gestionali spesso non sono presenti in piccole realtà poco strutturate che, quindi, rischiano di incorrere in problemi significativi e se poi trattano dati sensibili, in particolare dati sanitari, potrebbero veramente incorrere in perdite economiche e di immagine molto importanti.

Una metodologia di valutazione dei rischi per la sicurezza delle informazioni

La norma UNI CEI ISO 27001 (*Sistemi di gestione della sicurezza delle informazioni – Requisiti*), recentemente pubblicata in nuova versione 2013 dall'ISO, richiede una valutazione preliminare dei rischi sulla sicurezza delle informazioni (punto 4.2.1) al fine di implementare un sistema di gestione della sicurezza delle informazioni idoneo a trattare i rischi che l'organizzazione effettivamente corre in merito all'Information Security.

Gli approcci possibili alla valutazione dei rischi possono essere diversi ed i metodi per effettuare il cosiddetto ***Risk Assessment*** possono variare di caso in caso, in funzione della dimensione, della complessità e del tipo di organizzazione che si sta esaminando.

La ISO 27005 (*Information security risk management*) è il principale riferimento per la gestione del rischio in ambito sicurezza delle informazione, ma anche altre norme quali la ISO 31000 (*Risk management – Principles and guidelines*) – recepita in Italia come UNI ISO 31000 (Gestione del rischio – Principi e linee guida) – e ISO 31010 (*Risk management – Risk assessment techniques*) possono essere prese a riferimento.

Vediamo un esempio di possibile approccio alla gestione del rischio finalizzato a preparare una valutazione dei rischi sulla sicurezza delle informazioni.

Il processo di **gestione dei rischi** comprende le seguenti fasi, descritte nel seguito:

1) Identificazione dei rischi

2) Analisi e ponderazione dei rischi

3) Identificazione e valutazione delle opzioni per il trattamento dei rischi

4) Scelta degli obiettivi di controllo ed i controlli per il trattamento dei rischi

5) Accettazione dei rischi residui.

Le attività suddette vengono descritte nel **Rapporto di valutazione dei rischi** (*Risk assessment report*).

L'**identificazione dei rischi** che incombono sulla sicurezza delle informazioni avviene attraverso:

a) L'identificazione degli asset significativi all'interno del SGSI: tale attività avviene come descritto nella procedura *Identificazione e valutazione degli asset*.

b) La valorizzazione ai fini del SGSI degli asset rilevati: tale attività avviene come descritto nella procedura *Identificazione e valutazione degli asset*. La valorizzazione degli asset in termini di riservatezza, integrità e disponibilità avviene per singolo asset oppure per gruppi di asset omogenei ai fini del SGSI; nel seguito in entrambe le situazioni si utilizzerà il termine *asset* intendendosi anche "raggruppamento di *asset*".

c) Identificazione delle minacce/pericoli che incombono sugli asset: tale attività viene svolta valutando le minacce note della letteratura e quelle ipotetiche specifiche in relazione ai servizi svolti dall'organizzazione. Le minacce vengono associate agli asset (e quindi alle informazioni che essi gestiscono) e vengono valorizzate in una scala da 1 a 3 (Bassa, Media, Alta). La stessa minaccia può assumere un livello di gravità diverso a seconda dell'asset cui si applica..

d) Identificazione delle vulnerabilità: tale attività viene svolta valutando le vulnerabilità note della letteratura, quelle ufficiali comunicate da fonti autorevoli e quelle ipotetiche specifiche in relazione ai servizi svolti dall'organizzazione. Le vulnerabilità vengono associate agli asset (e quindi alle informazioni che essi gestiscono) e vengono valorizzate in una scala da 1 a 3 (Bassa, Media, Alta). La stessa vulnerabilità può assumere un livello di gravità diverso a seconda dell'asset cui si applica.

e) Identificazione degli impatti o conseguenze che la perdita dei requisiti di riservatezza, integrità e disponibilità possono avere sugli asset. Le conseguenze del concretizzarsi di una minaccia in grado di sfruttare una vulnerabilità vengono anch'esse valorizzate attraverso la formula seguente:

Impatto = Valore Asset x Gravità Minaccia x Gravità Vulnerabilità.

L'analisi e ponderazione dei rischi per la sicurezza delle informazioni identificati avviene attraverso:

a) La valutazione della probabilità che si verifichino i singoli rischi identificati nella fase precedente. La probabilità di accadimento di un rischio

avviene considerando gli **incidenti** verificatisi in passato e statistiche eventualmente disponibili. L'assegnazione di una livello di probabilità attraverso una scala qualitativa avviene secondo il seguente schema:

Valore	Descrizione	Esempio
1	Mai verificatosi ma possibile	Non è mai accaduto nella storia dell'organizzazione
2	Raro	Accaduto una volta all'anno
3	Periodico	Accaduto circa 3 volte l'anno
4	Regolare	Accaduto circa una volta al mese
5	Frequente	Si verifica settimanalmente

b) Determinazione dell'indice di esposizione al rischio moltiplicando la gravità dell'impatto per la probabilità. Il risultato ottenuto sarà un valore da 3 a 81.

c) Definizione dei criteri di accettazione dei rischi: si stabilisce un livello minimo di tolleranza dei rischi al di sotto del quale i rischi vengono accettati ed al di sopra del quale i rischi devono essere trattati con azioni mirate.

Relativamente alla **identificazione e valutazione delle opzioni per il trattamento dei rischi, per i rischi** che si è deciso di trattare, in ordine decrescente dal maggiore al minore, vengono scelte delle azioni di mitigazione del rischio, che possono consistere nelle seguenti opzioni:

- Ridurre il rischio attraverso l'applicazione di obiettivi di controllo e controlli preventivi e correttivi, finalizzati alla riduzione degli effetti (impatto) del verificarsi del rischio e/o alla riduzione della probabilità che si verifichi.
- Evitare il rischio attraverso l'applicazione di obiettivi di controllo e controlli finalizzati ad evitare che si concretizzino le situazioni che permettono al rischio di concretizzarsi, ovvero ridurre a zero la probabilità che l'incidente paventato si verifichi.
- Trasferire il rischio attraverso la stipula di polizze assicurative oppure l'esternalizzazione a fornitori di processi ed attività con la relativa presa in carico da parte del fornitore dei relativi rischi.

Tali azioni vengono documentate nel **Piano di trattamento dei rischi**. Esso deve definire le singole azioni da intraprendere, i tempi e le relative responsabilità e risorse per gestire i singoli rischi. L'efficacia delle azioni pianificate porterà ad un ricalcolo della valutazione dei rischi, ottenendo nuovi indici.

La **scelta degli obiettivi di controllo e dei controlli per il trattamento dei rischi** da attuare avviene in base dall'elenco dei controlli applicabili definito a partire dai controlli identificati a livello normativo (norme della famiglia ISO 27000) a

cui si possono aggiungere altri controlli ritenuti utili.

I controlli vengono ritenuti applicabili o non applicabili, se applicabili possono essere attuati in modo completo o parziale. L'applicazione dei controlli può infatti essere ritenuta conveniente solo su alcuni processi/attività, in funzione della diversa esposizione al rischio che possiedono le varie attività svolte dall'organizzazione.

L'attuazione del **piano di trattamento dei rischi** porta all'**accettazione dei rischi residui**, ovvero ad evidenziare i rischi residui ritenuti accettabili, dato dall'insieme dei rischi valutati accettabili in sede di prima valutazione dei rischi ed i rischi residui trattati dalle azioni contenute nel **piano di trattamento dei rischi**.

Il piano di trattamento dei rischi riporta le seguenti informazioni:

1) Elenco dei rischi da trattare;

2) Descrizione delle relazioni fra il rischio e l'azione di trattamento del rischio prescelta;

3) Descrizione delle relazioni fra il rischio e gli obiettivi di controllo ed i controlli selezionati per gestire il rischio.

Lo scopo della procedura *Identificazione e valutazione degli asset* (predisposta con riferimento alla ISO 27005 – *Information technology – Security techniques – Information security risk management – Annex B – Identification and valuation of assets and impact assessment*) dovrebbe essere quello di definire le modalità operative e le responsabilità per l'effettuazione e l'aggiornamento del censimento dei beni (*asset*) aziendali e la relativa valutazione, in termini di riservatezza, integrità e disponibilità delle stesse. In essa vengono stabiliti:

- la classificazione degli asset;
- l'identificazione di ogni asset che ha impatto sulla sicurezza delle informazioni;
- la valutazione quantitativa di ogni asset in relazione alla sua importanza per la sicurezza delle informazioni.

La **classificazione degli asset** potrebbe distinguere due categorie principali di asset:

1. Asset primari: processi/attività ed informazioni;
2. Asset di supporto: hardware, software, reti, personale, sito, struttura organizzativa.

Gli asset possono essere delle seguenti tipologie:

1. *Information asset*: dati digitali e non digitali, sistemi operativi, software applicativo, beni intangibili (conoscenza, marchi, brevetti, …).
2. *Asset fisici*: infrastruttura IT, Hardware, Sistemi di controllo, Servizi IT.
3. *Risorse Umane*: dipendenti, collaboratori esterni e consulenti.

L'**identificazione** e ed il **censimento degli asset** aziendali (*asset inventory*) ha lo scopo di identificare i requisiti di sicurezza (riservatezza, integrità e disponibilità) degli stessi e valutarne possibili vulnerabilità.

Ad ogni *information asset* deve essere associato un valore in termini di **Riservatezza**, **Integrità** e **Disponibilità**; tale valore viene espresso in termini qualitativi attraverso l'attribuzione di un livello di importanza (Basso, Medio, Alto) a cui è associato un valore numerico crescente (1,2,3).

Ad ogni *asset* di supporto o *asset* non informativo (risorse fisiche e risorse umane) viene associato un valore in termini di criticità dell'asset, dato dalla somma dei valori di importanza dei requisiti *dell'asset* in termini di Riservatezza, Integrità, Disponibilità in funzione delle informazioni che esso gestisce. Dunque l'importanza di una risorsa per la sicurezza dipende dai requisiti di Riservatezza, Integrità e Disponibilità, espressi in livelli (Basso/Medio/Alto) a cui corrisponde il valore 1/2/3.

Di conseguenza il valore associato all'asset potrà variare da un minimo di 3 (Riservatezza=Basso + Integrità=Basso + Disponibilità=Basso) ad un massimo di 9 (Riservatezza=Alto + Integrità=Alto + Disponibilità=Alto).

Poiché gli asset possono essere di diversi tipi (risorse fisiche e risorse umane), la metodologia di valutazione dei requisiti di sicurezza delle informazioni è differente per ogni tipo di asset.

Il Valore *dell'Asset* in termini di sicurezza delle informazioni viene utilizzato nel ***Risk Assessment*** in combinazione con:

- le minacce che incombono sugli *asset* che possono sfruttare le vulnerabilità rilevate degli *asset* stessi;
- la probabilità che la minaccia si concretizzi in un incidente di sicurezza (delle informazioni);
- la gravità dell'impatto associato all'incidente.

Decreto anticorruzione ed impatti sul D.Lgs 231

La Legge n. 190 del 6/11/2012 (cosiddetta “legge anticorruzione”), entrata in vigore lo scorso 28/11/2012, riformula e punisce più severamente alcuni reati, quali la concussione e la corruzione, che potenzialmente possono interessare coloro che intrattengono rapporti commerciali con le P.A..

La Legge 190/2012 introduce inoltre il nuovo reato di “corruzione fra privati”, che comporta, oltre alle sanzioni penali a carico degli esponenti apicali delle società e dei loro subordinati nonché di coloro che li corrompono, la responsabilità amministrativa della società alla quale appartengono i corruttori, ai sensi del D.Lgs. n. 231/2001.

E’ dunque necessario aggiornare le valutazioni dei rischi predisposte ai sensi del suddetto D.Lgs 231/2001 e, conseguentemente, apportare le modifiche necessarie al relativo Modello Organizzativo. Inoltre alcune organizzazioni, che prima avevano valutato inesistente il rischio di corruzione di una P.A. poichè non trattano affari con essa, ora, con l’inserimento del reato di corruzione fra privati nell’elenco dei reati per cui si applica il D.Lgs 231, dovranno valutare attentamente se la non attuazione di un Modello Organizzativo 231 è ancora una scelta corretta.