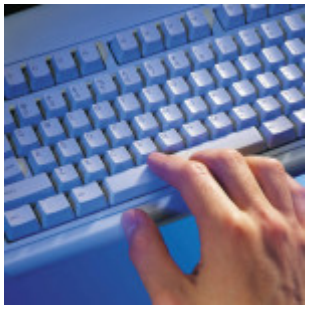
La nuova edizione della norma ISO 27002 (seconda parte)



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.

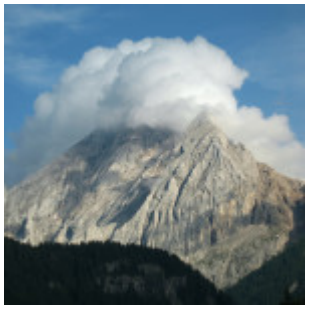
Naturalmente sull'argomento esiste la norma specifica UNI EN ISO 22301:2014 – *Sicurezza della società – Sistemi di gestione della continuità operativa – Requisiti.*

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*.

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.

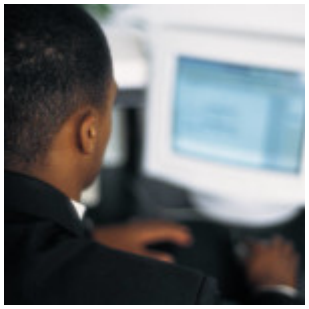
In linea generale parlare di dati poco sicuri nel *cloud* perché si teme che qualcuno possa "guardarci dentro" non ha molto senso: a parte che bisognerebbe valutare quale livello di sicurezza ci si aspetta per ogni tipo di dato (si veda il precedente articolo sulla valutazione dei rischi per la sicurezza 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.

Il cloud computing e la PMI

Cloud Computing: è utilizzabile da un'impresa di piccole dimensioni? Quali benefici potrebbe portare? Forum, Wiki, Social Network, Blog possono migliorare il lavoro dei dipendenti? In quali ambiti sono applicabili?

Quali attività dell'impresa potrebbero essere supportate da applicazioni mobile? Con quali benefici? Quali sono gli ostacoli da superare in fase di adozione?

Come aumentare l'efficacia delle attività di marketing attraverso le tecnologie digitali ed i social media? Quali risultati concreti è possibile ottenere grazie al *Mobile Marketing*?

Queste domande sono state utilizzate per promuovere un seminario sull'argomento nell'ambito di una nota fiera che si svolge in questo periodo e sono le domande che un responsabile di una piccola e media impresa o di uno studio professionale potrebbe chiedersi a proposito del *cloud computing*. Sicuramente in questo periodo il cloud computing è molto popolare e parecchi eventi ed alcune riviste trattano l'argomento sotto diversi aspetti. Ovviamente se con l'autunno si parla di "*cloud*" (in inglese letteralmente "nuvola") non è solo un fatto atmosferico, considerando che alcuni importanti produttori di hardware e di software stanno proponendo soluzioni applicative al riguardo (tanto per restare in cielo Microsoft propone "Azur") e che la spinta commerciale – in un periodo di vendite non esaltanti – è abbastanza forte.

Francamente le prospettive e le possibilità, anche per le piccole e medie imprese egli studi professionali, sono molto interessanti, soprattutto dal punto di vista del rapporto costi-benefici.

Per una disamina dettagliata ed indipendente sul *cloud computing* (che cos'è? Come si attua? Quali sono le soluzioni sul mercato?) rimando ad un bell'articolo apparso su PC Professionale del mese di ottobre (anche la rivista INARCOS ha recentemente pubblicato un bell'articolo sull'argomento), mediante il quale i neofiti

dell’argomento potranno capire di cosa si tratta.

Personalmente vorrei sottolineare alcuni pregi e difetti delle implementazioni “cloud” per le organizzazioni oggetto di questo articolo.

Se da un lato le soluzioni proposte di gestione di sistemi informatici non operanti all’interno del perimetro dell’azienda presenta alcuni vantaggi inconfutabili, soprattutto per una piccola organizzazione.

Acquistare un servizio che comprenda l’impiego di server remoti e software applicativi utilizzabili via internet in modo sicuro può avere dei costi abbordabili e certi rispetto ad analoghe soluzioni interne che non possono esaurirsi nell’acquisto di hardware e licenze software e nella relativa installazione, ma devono considerare servizi di manutenzione che – in mancanza di personale interno di adeguata competenza (la stragrande maggioranza dei casi per le piccole organizzazioni) – devono essere acquistati esternamente con costi che facilmente lievitano a fronte di esigenze particolari. In questi casi molte piccole realtà, al fine di spendere poco, si affidano allo “smanettone di turno”, auspicalmente un “bravo ragazzo” esperto di computer, che però non è in grado di fornire un assistenza continuativa adeguata, talvolta sparisce dalla circolazione (spesso questi soggetti sono anche “un po’ matti”) e, se succedono guai grossi, senza assistenza qualificata il personale interno potrebbe non riuscire a lavorare proficuamente per un certo periodo di tempo (ad es. non riuscire ad accedere ad internet o alla posta elettronica, non lavorare su una determinata postazione con problemi, ecc.). Naturalmente in questo modo i sistemi non sono sempre aggiornati come dovrebbero (patch e service pack vengono installate solo occasionalmente durante le visite del tecnico esterno), la sicurezza (anti malware e firewall, backup) non è gestita a dovere in modo continuativo, insomma non c’è da stare tranquilli. Viceversa il servizio “cloud” potrebbe fornire adeguate garanzie in questo senso e l’ubicazione remota dei dati potrebbe fornire quella sicurezza aggiuntiva che spesso non viene ricercata nei backup dalle piccole organizzazioni (vengono periodicamente conservati backup dei dati fuori dall’azienda per scongiurare gli effetti di eventi catastrofici, quali terremoti o inondazioni, o di furti dell’hardware e dei supporti?).

Il *software as a service* (detto SaaS) via internet può essere fruito da qualsiasi postazione dotata di accesso alla rete, teoricamente in qualunque parte del mondo, soddisfacendo così le esigenze di mobilità di manager e professionisti, ma anche di agenti e rappresentanti che potrebbero ad esempio inserire gli ordini direttamente nel gestionale già a casa del cliente, riducendo così tempi, costi e possibili errori di trascrizione.

Attraverso servizi “*cloud*” (non solo software, ma anche infrastrutture di rete, fornite da remoto) è possibile gestire meglio i rapporti con i clienti ed i partner che – mediante collegamento via web sicuro – possono accedere ai dati che li riguardano e ricevere/trasmettere informazione in tempi più brevi senza

necessariamente avere un supporto da parte di personale dell'organizzazione. Ovviamente questo è ottenibile anche con applicazioni web installate su server aziendali aperti verso l'esterno, ma i vantaggi del *cloud* sono in questo caso quelli esposti in precedenza (stabilità, aggiornamento e sicurezza della piattaforma gestita da personale competente). Detto dei vantaggi passiamo ora agli svantaggi o aspetti negativi del *cloud computing*, naturalmente sempre per piccole organizzazioni.

Il problema principale è costituito dal fatto che per usufruire dei servizi *cloud* occorre un collegamento ad internet e pure veloce. Sembra una banalità, ma sono venuto a conoscenza di situazioni reali nelle quali il collegamento non è costante come prestazioni durante tutto l'arco della giornata, anzi è inaccettabile per alcune ore (mi riferisco ad una zona industriale poco distante da un piccolo centro abitato, non ad un paesino fra i monti) ed anche di collegamenti assenti (in un'area ad elevata urbanizzazione) per periodi prolungati (alcuni giorni) o intermittenti nel corso della giornata per lunghi periodi (settimane). In questi ultimi casi occorre sopperire con una connessione di backup (chiavetta USB, se disponibile il collegamento su rete 3G) e non tutti i servizi potrebbero essere disponibili, quindi il collegamento a internet deficitario può creare importanti danni all'azienda "cloud", tanto più gravi quanto più sono i servizi "in the cloud". Provate ad immaginare un sistema ERP che funziona solo se c'è il collegamento ad internet: in assenza di connessione l'azienda si blocca con conseguenti costi improduttivi (personale che non lavora, ordini che non vengono processati, ecc.) e perdita di immagine verso i clienti. Occorre tener presente che se da un lato i servizi di *cloud computing* a pagamento arrivano a garantire dei livelli di affidabilità (disponibilità del servizio, sicurezza dei dati) elevatissimi, dall'altro i provider di servizi internet e telefono del nostro paese danno poche garanzie al riguardo in caso di guasto: ben che vada garantiscono l'intervento entro 48 ore, ma se il problema non si scopre i tempi si possono allungare e vengono riconosciuti risarcimenti danni ridicoli (comparabili con il costo dei canoni del servizio).

Dunque il *digital divade* ed i problemi di connessione sono i principali ostacoli alla diffusione del *cloud computing*.

Poi viene il problema della sicurezza dei dati, declinato (ISO 27000 *docet*) in termini di riservatezza, integrità e disponibilità. Su questo aspetto bisogna verificare i contratti di servizio che, per una piccola azienda, potrebbero risultare ostici e sulla riservatezza bisogna fidarsi.

Alcuni imprenditori italiani sono restii ad affidarsi anche semplicemente ad un servizio di *storage in the cloud* proprio per timore che qualcuno vada a curiosare fra i suoi dati (quando magari non ha il benché minimo controllo su quello che potrebbe accadere all'interno della sua azienda).

Accanto a questo potrebbero esserci problemi di *compliance* normativa (ad es. legge sulla privacy), talvolta di difficile interpretazione se il server che custodisce i

nostri dati (e dei nostri clienti e fornitori) è collocato in un paese extra UE o non si sa dove.

Infine, senza fare terrorismo, parliamo di sabotaggi e di terrorismo. Se i dati delle aziende si spostassero sempre più "*in the cloud*" a qualcuno potrebbe venir voglia di sabotare questi dati attraverso tecniche di *hacking* e quindi di bloccare la produttività di moltissime imprese, causando danni ingenti all'economia globale. Provate a pensare se qualche terrorista riuscisse ad impossessarsi dei dati gestiti da multinazionali come Google, Microsoft o Amazon.

Ma il freno alla diffusione del *cloud computing* non deve essere la paura, ne lo slancio deve essere il costo basso o addirittura nullo. Occorre effettuare un'adeguata valutazione dei rischi di caso in caso per decidere di rivolgersi a servizi di questo tipo ed a livello di *risk management* aziendale le nostre piccole imprese non sono certo dei fenomeni! Da un lato ci sono le finte paure, con gradi di rischio minimi perché la probabilità che si verifichino è bassissima e gli effetti si possono prevenire o mitigare con adeguate contromisure. Dall'altro ci sono rischi reali che vengono sottovalutati, accecati magari dalla parola gratis, che contraddistingue molti servizi. Infatti lo sviluppo di molti servizi gratuiti su internet, dalle Google Apps ai vari servizi di backup e *storage on line*, da Microsoft Live ai *tool* di collaborazione *on-line* oppure ai social network professionali come Linkedin o Viadeo, è principalmente dovuto al fatto che spesso i servizi di base sono gratis e molte aziende italiane ci si buttano a pesce senza sapere neanche quali garanzie è in grado di fornire il servizio. Ovviamente i servizi gratis ed il mondo open source non potrebbero sopravvivere senza che nessuno paghi per il lavoro delle persone. Ciò può avvenire o attraverso la pubblicità oppure mediante servizi aggiuntivi più professionali a pagamento. Pensate cosa accadrebbe se domani Facebook ci dicesse che non è più gratis, ma che ad ogni utente – per continuare ad operare sulla piattaforma di social network più diffusa nel mondo – verrà richiesto un minimo obolo, diciamo 1 euro al mese….

Cito un esempio: recentemente la piattaforma NING (un misto fra un sito web ed un social network ristretto) ha deciso di non offrire più i servizi gratis e, molto onestamente, ha proposto servizi a pagamento ed ha permesso ad ogni iscritto di scaricarsi i propri contenuti qualora non volesse aderire ai servizi a pagamento.

Non vorrei essere frainteso, tanto di cappello ai numerosi servizi *free* come Google Apps o altri che potrebbero migliorare la vita lavorativa di piccole organizzazioni che però non sanno usarli perché nessuno ha detto loro che esistono e come fare per utilizzarli. Il miglioramento dell'efficienza aziendale (e dei piccoli studi professionale) passa anche attraverso l'utilizzo consapevole di strumenti web per la gestione delle attività (calendari, appuntamenti, progetti, documenti) e la comunicazione con l'esterno (sito web, blog, newsletter, forum,…), però occorre che tutto ciò venga pianificato con criterio dall'imprenditore, magari con il supporto di personale competente ed indipendente che sappia indirizzare nel modo giusto le scelte imprenditoriali, senza farsi condizionare dall'enfasi della spinta

promozionale di alcuni player che operano sul mercato e che magari hanno già un piede in azienda con altri prodotti o da voci provenienti da colleghi e concorrenti che operano in realtà con esigenze e problematiche diverse.