RPO e RTO: come progettare il disaster recovery

In questo articolo parleremo ancora di **business continuity**, ovvero di *business continuity plan* ed in particolare della progettazione delle procedure di ***disaster recovery***.

Molte organizzazioni che non predispongono un vero e proprio piano di continuità operativa (o *business continuity plan*, BCP), comunque hanno una **procedura di *disaster recovery***, più o meno evoluta. Purtroppo, però, questa attività viene delegata quasi interamente ai responsabili ICT senza coinvolgere il management, i responsabili dei processi primari di business ed in particolare di quelli più critici.

Non che i responsabili ICT non siano in grado di progettare una procedura di *disaster recovery* adeguata, ma spesso sono loro stessi che stabiliscono i requisiti di base del *disaster recovery*, ovvero implicitamente definiscono gli obiettivi **RTO** e **RPO** che dovrebbero essere alla base della procedura.

Riprendiamo le definizioni di questi indici, già esposte in precedenti articoli, per capire meglio di cosa si tratta.

- **Recovery Point Objective** (RPO) ovvero il punto (l'istante nel tempo) al quale le informazioni sono coerenti e possono essere ripristinate per consentire la ripresa delle attività (denominato anche *Maximum Data Loss*).
- **Recovery Time Objective** (RTO): periodo di tempo entro il quale i servizi erogati, la produzione, i servizi di supporto e le funzionalità operative devono essere ripristinati dopo l'incidente che ha generato la discontinuità.

Facciamo un esempio per comprendere meglio il significato degli indici sopra esposti.

Supponiamo che una piccola organizzazione che opera nel settore dei servizi, denominata ALFA srl, decida di effettuare un **backup incrementale** dei propri dati con frequenza giornaliera su un NAS interno, mantenendo le ultime 7 versioni dei dati e che poi, per cautelarsi a fronte di eventuali catastrofi naturali che potrebbero

rendere inutilizzabile il sistema informatico aziendale e tutti i backup salvati su NAS, effettui anche un **backup completo** su nastri DAT con cadenza settimanale. I nastri magnetici dell'ultimo backup settimanale sono conservati a casa del titolare, a 20 km di distanza dalla sede dell'azienda, il quale quando si porta via il backup restituisce quello della settimana precedente.

Qual è il valore di RPO e RTO per questa azienda?

Occorre distinguere fra diversi tipi di problemi (disastro):

1. Si tratta di un crash del sistema che ha comportato la perdita dei soli dati (eventualmente anche dei supporti di memorizzazione) oppure
2. Si tratta di un evento catastrofico che ha reso inutilizzabile l'intero server e l'infrastruttura informatica della sede di ALFA?

Evidentemente nel primo caso potrebbero essere sufficienti i backup su supporto NAS da ripristinare su un nuovo hard disk, reperibile in tempi brevi. Dunque il RTO potrebbe essere pari anche ad una sola giornata, dipende dal tempo che si impiega a ripristinare il sistema (tempi di acquisto dei nuovi supporti di memorizzazione, tempi di eventuale reinstallazione del sistema operativo del server e degli applicativi, ecc.). Il RPO invece è pari ad una giornata di lavoro o meno, a seconda dal tempo trascorso dall'ultimo backup giornaliero eseguito. In questo caso per valutare correttamente il RTO occorre capire quanto tempo si impiegherebbe a reinstallare il sistema, partendo dai supporti originali oppure da un'immagine del sistema creata attraverso l'impiego di macchine virtuali. Questa seconda soluzione, certamente più costosa della prima, potrebbe abbassare drasticamente il RPO.

Nel secondo caso il ripristino dell'operatività dipende anche dai danni generati alla sede dell'organizzazione: che si sia verificato un terremoto che ha reso inagibili i locali oppure un'alluvione i cui danni possano essere riparati entro qualche giorno o settimane la situazione può essere sensibilmente differente e il RTO, anche in questo caso può essere di alcuni giorni o settimane, indipendentemente dalla strategia di backup implementata. Il backup settimanale su nastro, conservato in un luogo sicuro (da valutare se la distanza dalla sede è sufficiente per garantire un'alta probabilità di evitare danni), garantirebbe un RPO di al massimo una settimana di dati persi.

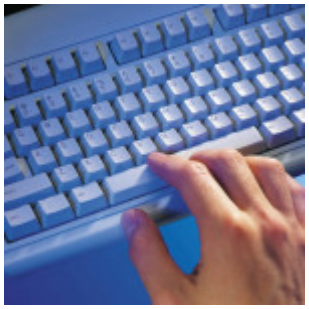
Bisogna capire se questi valori, di RPO e RTO, sono accettabili per l'organizzazione oppure le perdite, in termini di dati e di discontinuità operativa, mettono a repentaglio la sopravvivenza dell'azienda.

Ricordiamo che per alcune attività critiche il verificarsi di eventi disastrosi con RTO di settimane e di RPO di una settimana potrebbero portare a danni economici ingenti, non coperti da polizze assicurative (ritardi nella consegna di commesse con addebito di penali da parte del committente, perdita di commesse importanti, ecc.).

In questa seconda situazione occorrerebbe certamente un **sito di *disaster recovery***, ovvero un sito alternativo, geograficamente distante dalla sede principale dell'azienda, in grado di consentire la ripresa dell'attività in pochissimo tempo (ore, al massimo una giornata lavorativa) e la perdita dei dati di al massimo una giornata, dunque ottenendo un RTO = 1 giorno e RPO = 1 giorno. Ciò potrebbe essere ottenuto senza investimenti consistenti in una struttura gemella, ma dotandosi di una infrastruttura tecnologica in *cloud*.

In conclusione la procedura di *disaster recovery* dovrebbe essere progettata da personale competente (responsabile IT, consulenti esterni, …) basandosi su precisi input da parte della Direzione aziendale, derivanti da obiettivi di RPO e RTO ritenuti adeguati per l'organizzazione. La procedura di *disaster recovery* progettata avrà dei costi (che possono variare in base alle soluzioni scelte) che la Direzione dovrà mettere a budget per garantirsi gli obiettivi desiderati. Viceversa bisognerà migrare verso obiettivi meno ambiziosi di RPO e RTO, ma la Direzione deve essere consapevole di ciò. In caso di disastri, infatti, nessuno potrà accusare altri di non aver pensato alle giuste contromisure ed ognuno si assumerà le responsabilità che gli spettano.

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*.

La nuova edizione della norma ISO 27002 (prima parte)

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

Struttura della norma

La norma contiene **14 punti di controllo di sicurezza** (erano 11 nella precedente versione della norma) che riuniscono un totale di **35 categorie principali di sicurezza** (erano 39 nella versione precedente) e **114 controlli** (erano 133 nella versione precedente).

Ogni punto che definisce controlli di sicurezza contiene una o più categorie principali di sicurezza, al cui interno sono raggruppati i controllo relativi. Nella norma viene precisato che l'ordine dei punti è indipendente dalla loro importanza, infatti, a seconda delle circostanze, i controlli di sicurezza appartenenti ad uno o a tutti i punti di controllo potrebbero rivelarsi più o meno importanti ed ogni organizzazione che impiega la norma dovrebbe identificare i controlli applicabili al proprio interno, la loro importanza ed il loro impiego in ogni processo di business.

Ogni **categoria principale** di controllo di sicurezza contiene:

- L'**obiettivo di controllo** che dichiara cosa si vuole raggiungere
- I **controlli** che possono essere applicati per raggiungere l'obiettivo di controllo.

La descrizione dei controlli sono strutturate come segue:

- Controllo: definisce nello specifico il controllo funzionale alla soddisfazione dell'obiettivo di controllo.
- Guida attuativa: fornisce informazioni più dettagliate per supportare l'attuazione del controllo. La guida può risultare completamente attinente o sufficiente a tutte le situazioni oppure potrebbe non soddisfare i requisiti specifici di controllo dell'organizzazione.
- Altre informazioni: fornisce informazioni aggiuntive che potrebbe essere

necessario considerare, per esempio considerazioni legali e riferimenti ad altre norme. Nel caso non vi siano informazioni aggiuntive da considerare questa parte non è riportata nel testo.

Elenco dei controlli

I punti di controllo definiti dalla norma sono i seguenti:

5 POLITICHE PER LA SICUREZZA DELLE INFORMAZIONI

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

6 Organizzazione della sicurezza delle informazioni

In questa sezione sono definiti le seguenti categorie principali:

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

Quest'area è nel complesso più ridotta rispetto alla sezione 6 della precedente versione della norma che, tra l'altro, riportava la medesima categoria riferita a dispositivi portatili e telelavoro alla sezione 11, quella del controllo accessi. Del resto questa seconda categoria deve essere considerata in senso un po' più ampio perché la sicurezza dei dispositivi portatili e del telelavoro deve essere valutata insieme alla gestione delle connessioni wi-fi e degli accessi a siti web aziendali e ad eventuali servizi cloud.

Francamente ci si poteva aspettare qualcosa di più in quest'area ove al 6.2 l'evoluzione tecnologica in questi ultimi 9 anni trascorsi dalla precedente versione della ISO 27002 ha fatto passi da gigante moltiplicando anche le possibili vulnerabilità e qualche citazione più specifica del problema del BYOD e dell'autenticazione a due fattori (2FA) sarebbe stata gradita.

7 Sicurezza delle risorse umane

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

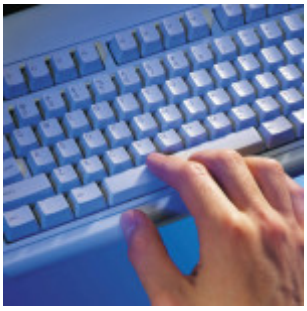
- **Prima dell'impiego (7.1)**: in due controlli vengono esposte tutte le cautele da intraprendere al momento dell'assunzione di una persona o dell'incarico ad un collaboratore esterno, non solo accordi di riservatezza e clausole contrattuali sul futuro rapporto lavorativo, ma anche – per quanto reso possibile dalla legislazione applicabile – un'accurata indagine conoscitiva sul passato, lavorativo e non, del futuro dipendente/collaboratore.
- **Durante l'impiego (7.2)**: nel corso della normale attività lavorativa viene data enfasi all'applicazione delle procedure stabilite e le responsabilità della Direzione nell'applicazione delle stesse, alla formazione-addestramento e sensibilizzazione del personale ed al ricorso ad eventuali processi disciplinari. Dunque regole da rispettare, ma anche motivazione ed incentivazione del personale, oltre che sanzioni a chi infrange le regole.
- **Cessazione e variazione del rapporto di lavoro (7.3)**: vengono presi in esame tutti gli aspetti e le attività da svolgere quando si chiude un rapporto di lavoro o avviene un'assegnazione ad altro incarico, come ad esempio il prolungamento della validità degli accordi di riservatezza, i passaggi di consegne e la comunicazione all'altro personale interessato della cessazione del rapporto di lavoro.

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

I contenuti sono analoghi a quelli della precedente versione della norma alla sezione 8, anche se i controlli sono in numero minore.

8 Gestione degli asset

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



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

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

9 Controllo degli accessi

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

- **Requisiti di business per il controllo degli accessi (9.1)**: occorre definire una politica di controllo degli accessi basata sull'accesso alle sole informazioni necessarie per svolgere il proprio lavoro (come impone anche la normativa sulla privacy in vigore in Italia) e regolamentare l'accesso alle reti (soprattutto evitare l'uso incontrollato delle reti wi-fi senza autenticazione utente).
- **Gestione degli accessi degli utenti (9.2)**: è necessario regolamentare il processo di registrazione (tramite credenziali di autenticazione univoche) e de-registrazione degli utenti, la fornitura delle credenziali di accesso (*provisioning*), la gestione degli accessi privilegiati (ad es. quelli in qualità di "amministratore di sistema", cfr. apposita disposizione del Garante della

Privacy), la gestione delle informazioni segrete per l'autenticazione (password, smartcard, ecc.), il riesame periodico dei diritti di accesso, la rimozione degli stessi al termine del rapporto (o la revisione in caso di cambio mansioni).
- **Responsabilità dell'utente (9.3)**: è importante regolamentare ed istruire il personale sull'uso della password.
- **Controllo degli accessi ai sistemi e alle applicazioni (9.4)**: è opportuno limitare l'accesso alle informazioni, predisporre procedure di log-on sicure, procedure di gestione delle password, limitare l'impiego di programmi di utilità privilegiati, limitare gli accessi al codice sorgente dei programmi.

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

Nel complesso sono presenti molti meno controlli rispetto alla precedente versione della norma alla sezione 11, ma i contenuti, opportunamente aggiornati, sono equivalenti.

10 Crittografia

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

Questa che era prima una categoria (cfr. punto 12.3 della norma ISO 27002:2005) ora è salito a livello di punto di controllo.

11 Sicurezza fisica e ambientale

La sezione comprende due categorie:

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

fine I parte ….continua…

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 privacy in Farmacia e nell'ambulatorio medico privato

La privacy dei privati cittadini utenti delle farmacie e dei piccoli ambulatori privati spesso è messa a repentaglio da una gestione non accurata delle regole stabilite dalla normativa al riguardo (D.Lgs 196/2003 – "Codice per la protezione dei dati personali") e da tutte le buone pratiche di gestione della sicurezza delle informazioni.

I titolari di **farmacie** ed **ambulatori medici** polifunzionali sono di fatto legali rappresentanti di imprese che, seppur di piccole dimensioni, raccolgono e gestiscono **dati personali sensibili** (in particolare dati sanitari relativi alla salute delle persone) di una **grande moltitudine di persone** fisiche e, come tali, sono tenuti a rispondere di fronte alla legge di tali gestioni.

In questi ultimi anni si è passati da una gestione prevalentemente cartacea dei dati personali sensibili raccolti da queste organizzazioni, ad una gestione elettronica di molte informazioni che riguardano la sfera privata delle persone, ovvero i **dati sanitari**.

Se pensiamo ad una farmacia moderna possiamo trovare molti **trattamenti di dati in formato digitale** che solo pochi anni fa non erano presenti: si passa dal ben noto scontrino fiscale parlante (sul quale ha molto disquisito il Garante della Privacy), generato e poi gestito da un sistema informatico, alla ricetta elettronica di recente introduzione, passando per una serie di servizi che le farmacie hanno introdotto da pochi anni: intolleranze alimentari, analisi della pelle, gestione referti esami diagnostici, preparazione di diete, fidelity card, e-commerce, ecc.. Ma anche servizi meno recenti come le prenotazioni di esami tramite CUP ASL o la Dispensazione per Conto vengono gestiti dalle farmacie, attraverso appositi portali dedicati, per conto dei clienti.

Ognuno di questi trattamenti di dati presenta vulnerabilità intrinseche per la sicurezza delle informazioni trasmesse: credenziali di accesso non sufficientemente difficili da individuare, scarsa protezione dei PC e dei Server da attacchi esterni, inadeguata protezione dei medesimi elaboratori in caso di furto e via dicendo.

Come le piccole organizzazioni di altri settori industriali o dei servizi, anche le farmacie non sono dotate di personale esperto nella gestione della sicurezza dei sistemi informatici e spesso il coinvolgimento dei fornitori esterni specializzati non è così sistemato (soprattutto per motivi di costo) da poter garantire una protezione adeguata.

RIPARBELLA C'È STATA ANCHE UNA LITE FRA UN CLIENTE E IL PERSONALE

«Non c'è privacy in farmacia»

– RIPARBELLA –

«C'ERANO già state diverse segnalazioni di cittadini infastiditi da una generale mancanza di privacy durante l'acquisto dei medicinali nella farmacia comunale — scrive Alessandro Lucibello Piani della lista civica "Insieme per cambiare» — e come spesso capita l'inerzia nel non cercare un rimedio fa si che le tensioni si acuiscano ed è di pochi giorni fa il caso di un acceso scontro verbale tra un cliente e gli addetti alla farmacia. Pur considerando la difficoltà di istituire nella piccola farmacia di Riparbella le obbligatorie e appropriate distanze di cortesia per rispettare la privacy dei cittadini resta comunque obbligatorio adottare soluzioni tali da prevenire, durante i colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute dei cittadini. Oltre ad esporre un cartello con la dicitura "Per il rispetto della riservatezza si prega la clientela di attendere il turno a debita distanza" le persone che non sono tenute per legge al segreto professionale non dovrebbero accedere dietro al banco negli orari di apertura, e ora è opportuno che si attivi subito il responsabile comunale intervenendo urgentemente per sensibilizzare tutti sul tema della privacy».

D'altro canto **dai computer delle farmacie transitano quantità di dati sensibili di gran linga superiori a quelle di altre piccole organizzazioni** e costituiscono il canale di consultazione di archivi di prenotazione di esami diagnostici di un elevatissimo numero di pazienti. Da qui la necessità di proteggere i sistemi informatici delle farmacie, sia da un punto di vista logico, sia fisico, in modo molto più attento rispetto ad un normale PC aziendale.

Anche i **piccoli ambulatori privati**, che ospitano medici che eseguono visite specialistiche ed esami diagnostici, ultimamente hanno trovato grande beneficio dall'utilizzo delle nuove tecnologie, nonostante la ritrosia all'utilizzo del computer da parte di numerosi medici. Tutto ciò, però, comporta **la necessità di proteggere adeguatamente i dati sensibili dei pazienti** che transitano in formato digitale in reti locali poco protette. In tali organizzazioni spesso non è nemmeno chiaro chi è il titolare del trattamento dati – il medico che visita il paziente o il centro medico – ed a chi vengono eventualmente delegate le responsabilità per i

trattamenti delegati ad altri.

In generale, nelle farmacie e nei piccoli centri medici, tutta la "parte informatica" è delegata a **fornitori specializzati** che talvolta non conoscono in modo preciso la normativa sulla privacy e sono **negligenti nel sottoscrivere le proprie assunzioni di responsabilità** a fronte delle attività eseguite; conseguentemente **tutte le responsabilità ricadono sul titolare del trattamento**, persona fisica o giuridica avente comunque un legale rappresentante, generalmente poco avvezzo a questioni informatiche.

Dal punto di vista normativo, poi, il passaggio da una **normativa italiana** – molto completa e severa per taluni aspetti, ma ormai **obsoleta** per quanto riguarda il **disciplinare tecnico delle misure minime di sicurezza** – ad un nuovo **Regolamento Europeo in fase di approvazione**, non fa che complicare le cose per le piccole organizzazioni che finora hanno avuto regole precise (password di almeno 8 caratteri variate ogni 3 mesi se si trattano dati sensibili, backup almeno ogni 7 giorni, aggiornamenti semestrali dei programmi software, assenza di idonee dichiarazioni di conformità dei fornitori, ecc.) con le quali confrontarsi. Il nuovo Regolamento, infatti, introdurrà la necessità di **valutare i rischi che si corrono dal punto di vista della sicurezza dei dati personali** e, conseguentemente, **progettare il sistema di gestione della privacy** in funzione delle reali esigenze di riservatezza, adottando misure di sicurezza adeguate (non solo "minime").

Inoltre l'attuale versione del Regolamento Europeo sulla Privacy in approvazione contiene l'obbligo per i titolari di dati personali di dotarsi – entro determinate condizioni – di un "***Privacy Officer***", ovvero di una persona, dotata di **adeguate competenze in materia di privacy e sicurezza dei dati**, **responsabile per la gestione della privacy** all'interno dell'organizzazione. Ma il limite attualmente stabilito per l'obbligo di nominare un Privacy Officer è legato al numero di dati personali gestiti (più di 5000 in un anno) che viene facilmente superato da una farmacia di medio volume di affari, ma non da numerose imprese industriali con oltre 50 dipendenti.

La ratio del nuovo Regolamento UE è evidentemente quella di **garantire migliore protezione dove esistono maggiori rischi**, sia per il numero di dati personali trattati, sia per la vulnerabilità dei sistemi.

Il **cambio di mentalità** di chi gestisce **piccole organizzazioni nel settore sanitario** non sarà facile, anche perché non ci saranno più regole precise da seguire per stare tranquilli, ma, oserei dire giustamente, **il Regolamento Europeo ribalterà la responsabilità di progettare un sistema di gestione della privacy adeguato sulle spalle degli imprenditori**. Molti di questi ultimi non saranno in grado di valutare in modo competente ed oggettivo quali misure adottare e dovranno fare attenzione a non credere alle "ricette preconfezionate" a basso costo che hanno già rovinato l'approccio alla privacy negli anni del ben noto **DPS** (Documento Programmatico sulla Sicurezza).

Già oggi il rischio di molte piccole organizzazioni del settore sanitario è quello di non essere conformi alla legislazione attuale sotto diversi aspetti (mancate nomine degli incaricati, mancanza di credenziali di autenticazione ai sistemi informatici adeguate e variate periodicamente, utilizzo troppo invasivo della videosorveglianza, archiviazione di dati privi di protezione, ecc.), figuriamoci domani se saranno i titolari del trattamento (ovvero i legali rappresentanti o direttori delle organizzazioni) a dover **decidere quali misure di sicurezza sono adeguate**! Il rischio concreto è quello di **sottovalutare il problema privacy**, come del resto è avvenuto dopo l'abolizione del DPS che non ha abolito tutti gli altri adempimenti!

Dimenticarsi di proteggere adeguatamente i dati personali dei propri clienti può comportare non solo **sanzioni civili** (e in alcuni casi anche reati penali) in caso di **ispezione da parte del nucleo Privacy della Guardia di Finanza** (oggi peraltro molto rare), ma anche, in caso di **richiesta di risarcimento danni da parte dell'interessato** i cui dati sensibili sono stati violati, ingenti perdite economiche. Talvolta, poi, la mancata diligenza del titolare del trattamento potrebbe portare anche al divieto di intraprendere relazioni commerciali con la Pubblica Amministrazione, riducendo o annullando di fatto la possibilità di operare.

Infine, oltre agli aspetti legati al rispetto della normativa cogente, esistono altri pericoli a cui è sottoposta una organizzazioni che gestisce in modo inconsapevole la sicurezza dei dati, ad esempio la **perdita di dati** e **l'indisponibilità di risorse per garantire la continuità del servizio** al cliente e, quindi, perdite economiche più o meno rilevanti in funzione della gravità dell'evento.

Altre risorse in rete:

- http://www.federfarmalombardia.it/documents/servizi/vademecum_privacy.pdf
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3533579
- http://www.federprivacy.it/forum/17-privacy-in-campo-sanitario/307-privacy-in-farmacia-e-negli-studi-medici.html
- http://www.federfarma.it/Edicola/Ultime-notizie/17-05-2014-07-30-18.aspx?feed=FederfarmaUltimeNotizie
- http://www.sicurezzamagazine.it/telecamere-nelle-farmacie/
- http://quellichelafarmacia.com/19493/sicurezza-farmacia-abuso-videosorveglianza-una-violazione-privacy/#sthash.RJlzvePR.dpbs

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**.

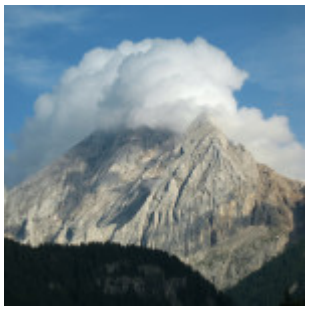
Sebbene questo schema SSAE 16 ricalchi per alcuni elementi la certificazione ISO 9001 e la certificazione ISO 27001, esso presenta una valenza particolare in determinati settori e costituisce il logico completamente in un percorso di miglioramento e di qualificazione dell'organizzazione di servizi nei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

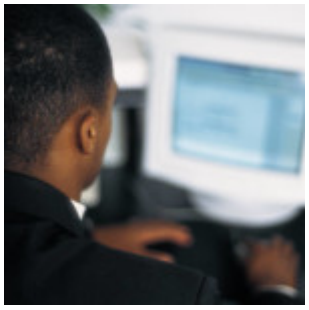
In linea generale parlare di dati poco sicuri nel *cloud* perché si teme che qualcuno

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.

La norma ISO 19011 sugli audit nei sistemi di gestione

La **UNI EN ISO 19011:2012 – Linee guida per audit di sistemi di gestione** pubblicata lo scorso anno, presenta alcune interessanti novità rispetto alla versione precedente del 2003, anche se nella sostanza i cambiamenti non impattano in modo significativo sul processo di audit.

Anzitutto già dal titolo si capisce che la norma è valida per qualsiasi tipo di audit su sistemi di gestione, non solo per quelli relativi a qualità ed ambiente (ISO 9001 e ISO 14001), ma – come era ovvio supporre – si adatta anche alla gestione degli audit per i sistemi di gestione sulla sicurezza delle informazioni ISO 27001, sulla sicurezza e salute sul lavoro, ecc.

Oltre ai soliti capitoli introduttivi presenti in tutte le norme ISO (Scopo e campo di applicazione, riferimenti normativi, termini e definizioni, ecc.) ed al capitolo "Principi dell'audit", la norma presenta due capitoli fondamentali:

- GESTIONE DI UN PROGRAMMA DI AUDIT
- SVOLGIMENTO DI UN AUDIT

La ISO 19011:2012 fa prevalentemente riferimento alla gestione degli audit di prima e seconda parte, ovvero agli audit interni e quelli eseguiti dal cliente sul fornitore, mentre per gli audit di parte terza (svolti dagli Organismi di Certificazione) il principale riferimento è diventato la ISO 17021:2011. Paradossalmente gli auditor degli organismi di certificazione su sistemi di gestione dovranno considerare questa norma come possibile linea guida, mentre i requisiti da osservare sono contenuti solo nella ISO 17021.

La norma introduce il concetto di **rischio associato all'attività di audit** di sistemi di gestione, ma l'approccio adottato riguarda sia il rischio che il processo di audit non raggiunga i propri obiettivi, sia l'eventualità che l'audit interferisca con le attività e i processi dell'organizzazione oggetto dell'audit, trascurando il fatto che l'audit può evidenziare comportamenti e prassi "rischiose" per l'organizzazione. Per rischiose intendo procedimenti rilevati (difformi o meno alle procedure stabilite) che possono portare a non conformità, nelle sue varie declinazioni: prodotti non conformi, incidenti (per la sicurezza delle informazioni), non conformità di sistema, ecc..

Le definizioni del capitolo 3 apportano lievi modifiche a quelle della precedente versione della norma. Si noti che il termine "verifica ispettiva" è completamente sparito da questa e dalle norme della famiglia ISO 9000, a favore del termine "audit" sebbene l'impiego della precedente terminologia sia rimasto nell'uso comune dei sistemi di gestione per la qualità ed anche alcuni organismi di certificazione continuino ad usarlo, mentre altri impongono alle aziende clienti l'aggiornamento della terminologia. Nella sostanza i due termini rimangono sinonimi e nulla vieta di citare il primo termine al posto del secondo nella propria documentazione di sistema.

In generale l'elenco dei termini e definizioni richiama più un audit di un ente di certificazione piuttosto che un audit interno di auna piccola impresa.

I **principi dell'audit** delineati dalla norma al capitolo 7 sono i seguenti:

a) **Integrità:** il fondamento della professionalità.

b) Presentazione imparziale: obbligo di elaborare rapporti veritieri e accurati.

c) Dovuta professionalità: l'applicazione di diligenza e di giudizio nel corso del l'attività di audit.

d) Riservatezza: sicurezza delle informazioni.

e) Indipendenza: la base per l'imparzialità dell'audit e l'obiettività delle conclusioni dell'audit.

f) Approccio basato sull'evidenza: il metodo razionale per raggiungere

conclusioni dell'audit affidabili e riproducibili in un processo di audit sistematico.

Probabilmente l'enfasi è eccessiva sull'integrità ed imparzialità dell'auditor, mentre uno dei principi fondamentali per svolgere un buon audit è la conoscenza dei processi sottoposti ad audit da parte dell'auditor che li verifica, ma sulla competenza degli auditor c'è un capitolo a parte (il settimo).

Riguardo all'indipendenza la norma cita che «*Per gli audit interni, gli auditor dovrebbero essere indipendenti dai responsabili operativi della funzione sottoposta ad audit*». Tale aspetto non viene sempre rispettato in molti sistemi di gestione certificati, con buona pace degli enti di certificazione, sebbene questa norma si esprima in termini condizionali ("dovrebbe").

Il **programma di audit** può anche comprendere informazioni e risorse necessarie quali:

- obiettivi del programma di audit e dei singoli audit;
- estensione/numero/tipo/durata/siti/pianificazione temporale degli audit;
- procedure del programma di audit;
- criteri di audit;
- metodi di audit;
- selezione dei gruppi di audit
- risorse necessarie (inclusi viaggi e alloggi);
- processi per la gestione della riservatezza, sicurezza delle informazioni, salute e sicurezza sul lavoro e quant'altro necessario.

Il programma di audit normalmente ha un orizzonte temporale di un anno e dovrebbe coprire tutte le aree/processi/unità operative/divisioni comprese nel sistema di gestione da sottoporre ad audit. Il diagramma di flusso riportato nella norma definisce alcuni passi fondamentali:

1. Definizione degli **obiettivi** del programma di audit.
2. Definizione del **programma di audit** (ruoli, responsabilità, competenze, estensione, ecc.).
3. **Attuazione** del programma di audit (obiettivi, metodi, assegnazione membri del gruppo di audit, registrazioni, ecc.).
4. **Monitoraggio** del programma di audit.
5. **Riesame e miglioramento** del programma di audit.

Nel punto 3 intervengono la **competenza degli auditor** e lo **svolgimento dell'audit**, trattati ai capitoli successorio

La norma ISO 19011 descrive in dettaglio i suddetti *step*; da ciò si comprende che un programma di audit non dovrebbe limitarsi ad un elenco di audit per aree o processi con periodi indicativi di svolgimento e definizioni di responsabili del gruppo di audit. Questo può essere sufficiente per una piccola realtà, mentre per un'azienda

più grande e strutturata, magari con alcune unità operative distaccate, potrebbe essere consigliabile sviluppare un programma di audit descrittivo, non solamente un "calendario di audit". Alcuni aspetti dovrebbero essere definiti e trattati più approfonditamente, ad esempio gli obiettivi (audit di conformità ad una norma oppure bisogna valutare il raggiungimento di determinati obiettivi di miglioramento?), i metodi (è opportuno pianificare audit a distanza?), l'estensione dei singoli audit, le tecnologie informatiche da impiegare e così via.

Anche i rischi di un programma di audit dovrebbero essere attentamente valutati: dedicare un tempo insufficiente a determinate aree o processi, oppure incaricare auditor non sufficientemente competenti per verificare certi processi, potrebbe comportare uno spreco di risorse oppure una riduzione dell'efficacia degli audit.

Un'attenta programmazione di questa fase può rendere il programma di audit più o meno efficace ed efficiente con conseguente impatto sui costi di tutta l'attività e benefici che ne derivano.

Anche la fase di attuazione del programma di audit richiede una pianificazione accurata di vari aspetti quali obiettivi, campo di applicazione, criteri e tempistiche dei singoli audit, nonché comunicazione ai soggetti interessati e disponibilità delle risorse necessarie per svolgere l'audit.

A volte anche una corretta gestione di aspetti logistici e di comunicazione sia agli auditor, sia ai soggetti auditati, di informazioni di interesse quali i risultati di precedenti audit, le tecnologie da verificare, informazioni relative alla sicurezza, ecc. possono evitare problemi in fase di svolgimento dell'audit.

La norma raccomanda la corretta gestione dei risultati degli audit e delle relative registrazioni (piani e rapporti di audit, rapporti di non conformità, azioni correttive, ecc.), compresa la dovuta riservatezza delle stesse.

Monitoraggio, riesame e miglioramento del programma di audit sono punti fondamentali per mantenere efficace ed efficiente il programma di audit anche attraverso modifiche scaturite dai risultati degli audit e da altri ritorni dal campo (ad es. *feedback* da parte delle persone auditate).

Il capitolo 6 "**Svolgimento dell'audit**" tratta tutti gli aspetti relativi all'esecuzione degli audit pianificati: dall'avvio dell'attività di audit con la presa di contatto del responsabile dell'audit con i responsabili delle attività auditate, alla preparazione dell'audit con la pianificazione dell'audit e la predisposizione dei documenti di lavoro (ad es. check-list), fino alla conduzione dell'audit ed alle attività conclusive (emissione e distribuzione del rapporto, chiusura dell'audit ed attività di *follow-up*).

La **fase preparatoria dell'audit** è molto importante per evitare poi di avere problemi successivamente o di trovarsi a non essere in grado di esaminare tutto ciò che si

avrebbe dovuto verificare. Questa fase è spesso svolta con frettolosità dagli organismi di certificazione che non hanno budget sufficienti per organizzare e preparare al meglio un audit in azienda; molto lavoro è affidato all'auditor che se conosce già l'azienda da precedenti visite riuscirà ad organizzarsi bene, viceversa si potrebbe rischiare di svolgere un audit troppo superficiale.

La predisposizione di un piano di audit che poi si sarà in grado di rispettare può agevolare i rapporti con il personale sottoposto a verifica, che non avrà scuse se non sarà pronto agli orari stabiliti e non potrà contestare il mancato rispetto degli orari pianificati.

La **conduzione** dell'audit vero e proprio inizia con la **riunione di apertura** o riunione iniziale che sostanzialmente non è molto diversa da quella descritta nelle precedenti versioni della norma. A seconda che si tratti di un audit di parte terza o di parte seconda, piuttosto che un audit interno, potrà variare il formalismo ed il tempo dedicato alla riunione di apertura. Anche se in organizzazioni di medio-piccole dimensioni e/o con una certa abitudine agli audit la riunione di apertura può risultare superflua è comunque opportuno confermare la programmazione degli orari delle interviste per assicurarsi che tutto si svolga senza intoppi.

Il riesame della documentazione dovrebbe essere previsto in molti audit per valutare la conformità delle regole stabilite ai criteri dell'audit (tipicamente una normativa di riferimento) prima di valutare se le procedure sono attuate in modo conforme.

Naturalmente in funzione degli esiti di eventuali audit precedenti, delle anomalie rilevate e delle azioni correttive intraprese dall'organizzazione auditata, questa fase preliminare all'avvio dell'audit vero e proprio sarà più o meno estesa.

La **comunicazione** fra i membri del gruppo di audit e fra questi e l'organizzazione soggetta a verifica è molto importante per rivalutare periodicamente l'avanzamento dell'audit e, in caso di necessità, riprogrammare attività anche riassegnando singoli compiti. La responsabilità principale di quest'attività è ovviamente del responsabile del team di audit.

Questo aspetto spesso viene mal gestito in alcuni audit di certificazione e così si finisce per dilungare eccessivamente la verifica o dedicare un tempo insufficiente alla verifica di processi importanti.

Se in alcuni casi è il piano di audit ad essere non ben progettato, in altri lo svolgimento dell'audit accumula ritardi che il team di audit non cerca di recuperare.

Infatti spesso il piano di audit rispecchia sequenze poco condivisibili (ad es. svolgere la verifica del riesame da parte della direzione all'inizio dell'audit piuttosto che alla fine quando l'auditor si sarà fatto un'idea migliore delle

prestazioni dei processi e dei relativi indicatori) oppure relega processi primari nell'ultimo quarto del tempo di audit, quando potrebbero essersi accumulati ritardi significativi ed il personale coinvolto potrebbe avere la necessità di uscire dall'azienda.

Viceversa anche con un piano ben progettato si possono registrare ritardi notevoli perdendosi in discussioni lunghissime con il personale dell'azienda; soprattutto nella prima parte della mattinata i tempi sono spesso molto allungati fra ritardi iniziali, chiacchere e caffè; come in qualsiasi attività lavorativa del resto.

L'assegnazione di ruoli e responsabilità a guide ed osservatori può riguardare soprattutto audit di parte terza (di certificazione) nei quali alcuni organismi richiedono esplicitamente che l'audit sia sempre accompagnato in azienda da personale incaricato, anche per motivi di sicurezza fisica e di riservatezza.

Il ruolo degli osservatori va confinato nel loro ambito: spesso i consulenti dell'azienda rispondono in vece dei responsabili dell'azienda (per colpa un po' dell'uno, un po' dell'altro) e questo non è consentito dai regolamenti ACCREDIA; in altri casi gli osservatori in addestramento dell'Organismo di Certificazione si spingono un po' troppo oltre i propri compiti e partecipano attivamente alla verifica ponendo domande ed esprimendo giudizi.

Riguardo alla **raccolta e verifica delle informazioni**, durante l'audit, dovrebbero essere raccolte informazioni verificabili tramite adeguato campionamento. Tali informazioni, se supportate da evidenza oggettiva, costituiscono delle **evidenze** (prove) che possono essere valutate in base ai criteri dell'audit e porteranno alle **risultanze dell'audit** che, opportunamente riesaminate, determineranno le **conclusioni dell'audit** (Conformità o non conformità del processo esaminato).

I metodi di raccolta delle informazioni comprendono interviste, osservazioni e riesame dei documenti, comprese le registrazioni (naturalmente di qualsiasi tipo e su qualsiasi supporto).

Su campionamento e metodi di raccolta delle informazioni la norma richiama i punti B.3, B.5, B6 e B.7 dell'Appendice B.

Riguardo al **campionamento**, esso viene distinto in campionamento basato su giudizio e campionamento statistico. Normalmente viene utilizzato solo quello del primo tipo, mentre il secondo mi sembra francamente impraticabile negli audit dei sistemi di gestione, salvo casi particolari nei quali vengono identificati a monte i macro-elementi potenzialmente esaminabili e, quindi, si stabilisce quali verificare nell'audit.

Una buona tecnica utilizzata nella pratica è quella di esaminare un certo numero di documenti o attività ed approfondire l'esame su altri elementi simili solo se si riscontrano non conformità.

Di fatto negli audit di certificazione il campionamento è scarsamente significativo dal punto di vista statistico. Facciamo un esempio: se un'azienda riceve 1000 ordini cliente all'anno e svolge 10 eventi formativi all'anno un campionamento omogeneo prevedrebbe che, a fronte della verifica di 2 registrazioni dell'addestramento/formazione (20% del totale), venissero esaminati 200 ordini cliente, cosa che in realtà non avviene mai.

La **produzione delle risultanze** dell'audit dovrebbe comprendere non conformità, conformità/buone prassi, opportunità di miglioramento e raccomandazioni per l'organizzazione. Le non conformità possono essere classificate in gradi di severità differenti.

La **preparazione delle conclusioni dell'audit** dovrebbe essere preceduta da una riunione del team di audit per riesaminare tutte le risultanze e concordare le conclusioni dell'audit. Inoltre dovrebbero essere trattate le cause radice delle non conformità e le azioni conseguenti richieste.

La **riunione di chiusura** dell'audit ha l'obiettivo di presentare i risultati dell'audit alla direzione dell'organizzazione ed ai responsabili delle funzioni/processi verificati. In essa dovrebbero essere discussi i rilievi ed eventuali divergenze fra il team di audit ed i responsabili dell'organizzazione dovrebbero essere risolte (ed in caso negativo comunque registrate), nonché le azioni da intraprendere post-audit.

Il **rapporto di audit** dovrebbe comprendere o fare riferimento a:

a) gli obiettivi dell'audit;

b) il campo di applicazione dell'audit, in particolare l'identificazione delle unità organizzative e funzionati o dei processi sottoposti ad audit;

c) l'identificazione del committente dell'audit;

d) l'identificazione del gruppo di audit e dei partecipanti all'audit della organizzazione oggetto dell'audit;

e) le date e i siti dove sono state condotte le attività di audit;

f) i criteri dell'audit;

g) le risultanze dell'audit e le relative evidenze;

h) le conclusioni del l'audit;

i) una dichiarazione sul grado in cui i criteri di audit sono stati soddisfatti.

Il rapporto di audit può anche includere o fare riferimento a:

- il piano di audit, compresa la pianificazione temporale;
- una sintesi del processo di audit (compreso qualsiasi ostacolo incontrato che può ridurre l'affidabilità del le conclusioni del l'audit);
- la conferma che gli obiettivi dell'audit sono stati raggiunti nell'ambito del campo di applicazione del l'audit, in conformità al piano di audit;
- qualsiasi area non coperta (sebbene compresa nel campo di applicazione dell'audit);
- una sintesi delle conclusioni dell'audit e delle principali risultanze dell'audit che le supportano;
- eventuali opinioni divergenti non risolte tra il gruppo di audit e l'organizzazione oggetto dell'audit;
- le opportunità di miglioramento, se specificate nel piano di audit;
- le buone prassi identificate;
- i piani concordati di azioni conseguenti, se presenti;
- una dichiarazione sulla natura riservata dei contenuti;
- qualsiasi implicazione per il programma di audit o per gli audit successivi;
- la lista di distribuzione del rapporto di audit.

La norma, infine, ricorda che il rapporto di audit può essere sviluppato prima della riunione di chiusura (cosa che avviene nella maggioranza dei casi).

La **distribuzione del rapporto di audit** potrebbe essere posticipata e comunque dovrebbe avvenire senza eccessivi ritardi indirizzandolo a coloro i quali era previsto nel piano che lo ricevessero.

La chiusura dell'audit avviene al termine di tutte le attività previste. La conservazione ed eventuale divulgazione dei rapporti dovrebbe avvenire secondo quanto concordato e riportato nelle procedure di riferimento, rispettando il livello di riservatezza richiesto.

La conduzione di azioni conseguenti all'audit riguarda l'attuazione di correzioni, azioni correttive o preventive e di miglioramento, eventualmente concordate in sede di audit, la cui efficacia potrà essere valutata in un audit successivo.

Il capitolo 7 della norma riguarda la **competenza e valutazione degli auditor**. Se la competenza viene determinata come ormai usuale nelle norme sui sistemi di gestione (istruzione, formazione/addestramento, conoscenze, esperienze, …), la determinazione e valutazione delle competenze di auditor e responsabili di gruppi di audit diventa un'attività molto articolata, descritta nella norma.

Oltre che competente l'auditor deve possedere alcune caratteristiche personali e comportamentali in linea con i principi dell'audit sopra esposti (comportamento etico, essere diplomatico, con mentalità aperta, ecc.).

Gli auditor dovrebbero possedere conoscenze ed abilità di carattere generale e specifiche per poter operare efficacemente nelle discipline per le quali sono impiegati (e vengono, dunque, qualificati), così come descritto nella norma. Tra le competenze a carattere generale che ogni auditor dovrebbe possedere ci sono conoscenze di carattere legale ed economico legate all' funzionamento delle imprese.

Per il responsabile del gruppo di audit sono richieste capacità aggiuntive e maggior esperienza nella conduzione di audit su sistemi di gestione.

I **metodi di valutazione dell'auditor** previsti dalla norma sono: riesame delle registrazioni, informazioni di ritorno dal campo, intervista, osservazioni del comportamento, esame (orale/scritto), riesame successivo all'audit (rapporto di audit, interviste con il responsabile del gruppo di audit, ecc.).

Infine la norma si concluse con due utili appendici:

- Appendice A: Guida ed esempi illustrativi delle conoscenze e abilità degli auditor specifiche della disciplina.
- Appendice B: Guida supplementare destinata agli auditor per la pianificazione e la conduzione di audit.

In conclusione si tratta di una norma di contenuti molto ampi, considerando anche le appendici appena citate. Ne consegue che la **preparazione di un auditor** che sia in grado di applicare le ormai note tecniche di audit, per rendere l'audit estremamente efficace e ad alto valore aggiunto, deve necessariamente comportare, oltre alla **lettura della norma e di altro materiale didattico** correlato, un certo numero di ore di **formazione frontale**, qualche **esercitazione pratica** ed un po' di **esperienza sul campo come osservatore**.

AVCpass: il nuovo sistema per la gestione dei documenti per le gare di appalto

L’art. 6 bis del D.lgs 163/2006, introdotto dall’art. 20, comma 1, lettera a), legge n. 35 del 2012 dispone che dal 1 gennaio 2013 le Stazioni Appaltanti ed Enti aggiudicatori possano verificare il possesso dei requisiti degli Operatori che partecipano alle gare pubbliche, esclusivamente tramite BDNCP (Banca dati nazionale dei contratti pubblici, istituita dall’art. 62 bis del Codice dell’Amministrazione Digitale di cui al decreto legislativo 7 marzo 2005, n. 82). La **Delibera attuativa n.111 del 20/12/2012 dell’Autorità di Vigilanza dei Contratti Pubblici (AVCP)** ha, tra l’altro, istituito il nuovo sistema di verifica dei requisiti attraverso la BDNCP, denominato ***AVCPASS***, dotato di apposite aree dedicate ad operatori economici e a stazioni appaltanti/enti aggiudicatori.

Il sistema AVCpass, infatti – come sancito dall’art. 2 della Delibera AVCpass del 20/12/2012 – permette, attraverso un’interfaccia web, rispettivamente alle Stazioni Appaltanti e agli Enti aggiudicatori l’acquisizione dei documenti a comprova del possesso dei requisiti di carattere generale, tecnico-organizzativo ed economico-finanziario per l’affidamento dei contratti pubblici ed agli Operatori Economici di inserire a sistema i documenti la cui produzione è a proprio carico ai sensi dell’art. 6-bis, comma 4, del Codice.

Uno dei moduli dei quali il sistema AVCpass si compone è il **Fascicolo Virtuale dell’Operatore Economico** che offre agli Operatori Economici la possibilità di creare un proprio *repository* dove collezionare i documenti utili da presentare in sede di partecipazione alle procedure di scelta del contraente per l’affidamento di contratti pubblici.

Le finalità del sistema sono quelle di **rendere molto più efficienti le procedure di gara per l’aggiudicazione di appalti pubblici**, permettendo così una notevole **riduzione dei costi da parte delle imprese** e degli altri soggetti partecipanti alle gare. Finora, infatti, chi partecipava a gare pubbliche spesso doveva produrre – per ogni gara – una serie di documenti amministrativi comprovanti il possesso di determinati requisiti amministrativi, organizzativi, tecnici e gestionali, generando così un’inutile spreco di risorse (costi vivi per l’acquisizione dei documenti, costi relativi al tempo impiegato dal personale per produrre i documenti, costi per la stampa di documenti, spese postali, ecc.). In più saranno i vari Enti Certificatori – dall’Agenzia delle Entrate a Infocamere, dall’INPS a Inarcassa – a dover fornire i documenti certificativi alla Stazione Appaltante in via completamente telematica. Anche la verifica del possesso dei requisiti richiesti da parte delle Stazioni Appaltanti dovrebbe essere più efficiente e garantire maggior trasparenza del processo di verifica e di aggiudicazione degli appalti pubblici.

A leggere la Delibera dell’AVCP del dicembre scorso – ed avendo ben noti gli sprechi di risorse per le imprese che partecipano ad appalti pubblici – viene da pensare perché non ci si è pensato prima, ma si sa come vanno queste cose in Italia. Vedremo comunque se il nuovo sistema AVCPass – introdotto gradualmente nel corso del 2013

fino a coprire tutti gli appalti pubblici a partire dal 1° gennaio 2014 – verrà applicato in modo adeguato.

Da parte delle imprese partecipanti c'è tutto l'interesse a far sì che il sistema funzioni al più presto, visti gli evidenti risparmi di costi, ma occorre verificare se gli Enti Pubblici saranno subito pronti ad utilizzare ed accettare il nuovo sistema AVCPass, che necessita di un cambiamento di mentalità non trascurabile. Infatti l'onere di produrre certificazioni ed attestazioni di dati già noti alla Pubblica Amministrazione, o facilmente reperibili via internet, si sposta dal soggetto partecipante alla gara alla PA ed agli Enti Certificatori dipendenti dallo Stato stesso. Gli esempi sono numerosi: si va dal Bilancio societario e relativo fatturato (fornito dall'Agenzia delle Entrate) alla regolarità contributiva (fornita da INPS, INAIL, Inarcassa, ecc.), dai certificati o attestazione di regolare esecuzione di precedenti lavori pubblici (forniti da altre P.A.) alla certificazione di qualità ISO 9001 (fornita da ACCREDIA, ma reperibile liberamente sul sito dell'Ente di Accreditamento). Inoltre gli Enti Pubblici dovranno evolvere dal punto di vista informatico, come del resto impone loro il **Codice dell'Amministrazione Digitale**.

Infatti il sistema AVCpass – nel rispetto delle regole del Codice dell'Amministrazione Digitale -obbligherà Stazioni Appaltanti ed Operatori Economici partecipanti alle gare ad utilizzare strumenti evoluti per garantire l'autenticità e l'inalterabilità dei documenti e delle registrazioni digitali, ovvero la **firma digitale** e la **posta elettronica certificata** (PEC), la cui diffusione è ancora limitata, sia da parte degli Operatori Economici, sia da parte degli Enti Pubblici, soprattutto riguardo al loro utilizzo (quasi tutti hanno PEC e firma digitale, ma "la tengono nel cassetto").

Dal punto di vista della trasparenza e della garanzia di regolarità del processo di aggiudicazione degli appalti la possibilità di avere false dichiarazioni sarà quasi azzerata in quanto dati quali fatturato, costo del personale, dati camerali, referenze di precedenti lavori, ecc. saranno forniti direttamente alla Stazione Appaltante dall'Ente preposto.

Infine all'Articolo 8 "Protezione dei dati personali e misure di sicurezza" della Delibera 111 vengono esposte le misure di sicurezza che verranno predisposte dall'AVCP per garantire **la sicurezza delle informazioni** gestite attraverso AVCPass. Ciò, se correttamente interpretato, comprende tutte le misure di prevenzione e di controllo necessarie a garantire la **Riservatezza** dei dati trattati, l'**Integrità** dei dati raccolti attraverso AVCpass e la **Disponibilità** continuativa del sistema AVCPass. Solo l'attuazione di misure di sicurezza fisica, logica, comportamentale e di piani di *business continuity* adeguati anche all'interno dell'AVCP e delle P.A. (in linea con le regole della norma ISO 27001) permetterà uno svolgimento delle procedure di aggiudicazione delle gare lineare, trasparente ed equo, eliminando i contenziosi che provocano dispendio di risorse da entrambe le parti (P.A. e partecipanti alle gare).

Al link seguente dell'AVCP sono disponibili alcuni moduli di formazione on-line sul sistema AVCpass: Formazione AVCPASS

Nel seguito si riporta un estratto della **Delibera 111 del 20/12/2012 dell'AVCP**.

Art. 1

Definizioni

1. Ai fini della presente delibera si intende per:

***– BDNCP**, la Banca dati nazionale dei contratti pubblici, istituita dall'art. 62 bis del Codice dell'Amministrazione Digitale di cui al decreto legislativo 7 marzo 2005, n. 82;*

***– OE**, Operatore Economico;*

***– AVCPASS**, l'Authority Virtual Company Passport, il servizio realizzato dall'Autorità per la verifica del possesso dei requisiti da parte degli OE;*

***– SIMOG**, il Sistema Monitoraggio Gare;*

***– CIG**, il Codice Identificativo Gara;*

***– PASSOE**, il documento che attesta che l'OE può essere verificato tramite AVCPASS;*

***– PEC**, la Posta elettronica certificata.*

Articolo 2

Oggetto ed ambito di applicazione

1. La presente delibera, in attuazione a quanto disposto dall'articolo 6-bis del Codice:

a) individua i dati concernenti la partecipazione alle gare e la valutazione delle offerte da inserire nella BDNCP al fine di consentire alle stazioni appaltanti/enti aggiudicatori di verificare il possesso dei requisiti degli operatori economici per l'affidamento dei contratti pubblici;

b) istituisce il nuovo sistema di verifica dei requisiti attraverso la BDNCP, denominato AVCPASS, dotato di apposite aree dedicate ad operatori economici e a stazioni appaltanti/enti aggiudicatori;

c) stabilisce i termini e le regole tecniche per l'acquisizione, l'aggiornamento e

la consultazione dei predetti dati.

2) Il sistema AVCPASS consente:

2.1. alle stazioni appaltanti/enti aggiudicatori, attraverso un'interfaccia web e le cooperazioni applicative con gli Enti Certificanti, l'acquisizione della documentazione comprovante il possesso dei requisiti di carattere generale, tecnico-organizzativo ed economico-finanziario per l'affidamento dei contratti pubblici;

2.2. agli operatori economici, tramite l'apposita area dedicata, di inserire a sistema i documenti la cui produzione è a proprio carico ai sensi dell'art. 6-bis, comma 4, del Codice. L'operatore economico può utilizzare tali documenti per ciascuna delle procedure di affidamento alle quali partecipa entro il periodo di validità del documento, così come dichiarato dall'operatore medesimo.

3. Per l'utilizzo del sistema AVCPASS:

3.1. la stazione appaltante/ente aggiudicatore, dopo la registrazione al sistema SIMOG, acquisisce, per ciascuna procedura di affidamento, il CIG, tramite il Responsabile del Procedimento; quest'ultimo indica il soggetto abilitato alla verifica dei requisiti;

3.2. l'operatore economico, dopo la registrazione al servizio AVCPASS, indica a sistema il CIG della procedura di affidamento cui intende partecipare. Il sistema rilascia un "PASSOE" da inserire nella busta contenente la documentazione amministrativa. Fermo restando l'obbligo per l'operatore economico di presentare le autocertificazioni richieste dalla normativa vigente in ordine al possesso dei requisiti per la partecipazione alla procedura di affidamento, il "PASSOE" rappresenta lo strumento necessario per procedere alla verifica dei requisiti stessi da parte delle stazioni appaltanti/enti aggiudicatori.

4. In attuazione dei commi 1 e 3, le stazioni appaltanti/enti aggiudicatori indicano nei documenti di gara che:

4.1. la verifica del possesso dei requisiti di carattere generale, tecnico-organizzativo ed economico-finanziario avviene, ai sensi dell'articolo 6-bis del Codice e della presente delibera attuativa, attraverso l'utilizzo del sistema AVCPASS, reso disponibile dall'Autorità, fatto salvo quanto previsto dal comma 3 del citato art. 6-bis;

4.2. tutti i soggetti interessati a partecipare alla procedura devono obbligatoriamente registrarsi al sistema accedendo all'apposito link sul Portale AVCP (Servizi ad accesso riservato – AVCPASS) secondo le istruzioni ivi contenute.

5. Il sistema AVCPASS si applica a tutte le tipologie di contratti disciplinate dal

Codice per le quali è previsto il rilascio del CIG attraverso il sistema SIMOG. Per gli affidamenti per i quali è consentito il rilascio del CIG in forma semplificata l'utilizzo della procedura di verifica prevista dall'art.6-bis del Codice comporta l'acquisizione del CIG attraverso il sistema SIMOG.

Articolo 3

Termini e regole tecniche di accesso al servizio

1. Il sistema AVCPASS è utilizzabile per le procedure di affidamento il cui CIG è richiesto a partire dal 1° gennaio 2013.

2. Coerentemente con quanto previsto dall'art. 77, comma 5, del Codice e dalla Circolare della Presidenza del Consiglio dei Ministri n. 1/2010, tutte le comunicazioni svolte nell'ambito del sistema AVCPASS sono effettuate tramite PEC. Pertanto, è necessario che ciascuno dei seguenti soggetti possieda un indirizzo PEC:

a) stazione appaltante/ente aggiudicatore (PEC relativa all'Area Organizzativa Omogenea di Protocollo di appartenenza);

b) Responsabile del Procedimento (casella PEC personale);

c) almeno un amministratore/legale rappresentante di ogni operatore economico (casella PEC personale dell'amministratore e casella PEC dell'operatore economico); nel caso di operatore economico persona fisica casella PEC personale;

d) eventuale delegato dall'operatore economico (casella PEC personale del delegato e casella PEC dell'operatore economico);

e) Presidente di Commissione e Commissari di gara chiamati ad operare tramite il sistema AVCPASS (casella PEC personale).

3. Coerentemente con quanto disposto dall'art. 21, comma 2, del Dlgs 82/2005 recante il Codice dell'Amministrazione Digitale e s.m.i., i documenti inseriti dagli operatori economici, devono essere firmati digitalmente dai soggetti di cui al comma 2, lettere c) e d). Pertanto tali soggetti devono dotarsi di un certificato di firma digitale, in corso di validità, rilasciato da un organismo incluso nell'elenco pubblico dei certificatori.

Articolo 4

Modalità operative

1. Per operare sul sistema AVCPASS, occorre registrarsi al servizio secondo le modalità descritte nel Manuale Utente pubblicato sul Portale dell'Autorità (Servizi

ad accesso riservato – AVCPASS).

2. Ai fini dell'utilizzo del sistema AVCPASS, i dati richiesti dal sistema SIMOG per il rilascio del CIG sono integrati con quelli riguardanti i requisiti di partecipazione e le modalità di comprova degli stessi da parte dell'operatore economico.

3. Le stazioni appaltanti/enti aggiudicatori nominano, nell'ambito di ogni procedimento di affidamento, il soggetto o i soggetti abilitati alla verifica dei requisiti.

4. L'accesso al sistema AVCPASS è consentito esclusivamente al Responsabile del Procedimento ed al soggetto abilitato alla verifica dei requisiti, a partire dalla scadenza del termine per la presentazione delle offerte, così come dichiarato sul sistema SIMOG.

5. Il Responsabile del Procedimento comunica i riferimenti dei soggetti abilitati alla verifica dei requisiti al sistema AVCPASS a partire dal giorno successivo alla data di conferma della procedura di affidamento, secondo quanto previsto dal sistema SIMOG. Tali soggetti, se non già iscritti al servizio, riceveranno un messaggio via PEC, all'indirizzo indicato dal Responsabile del Procedimento, con l'invito a completare la fase di registrazione e acquisizione delle credenziali di accesso. Eventuali modifiche dei soggetti abilitati alla verifica sono comunicate dal Responsabile del Procedimento utilizzando le apposite funzionalità previste da AVCPASS.

6. Al fine di garantire che le richieste di verifica dei requisiti interessino unicamente i partecipanti alla specifica procedura, prima di poter accedere alla comprova dei requisiti, il soggetto abilitato alla verifica dei requisiti integra o conferma, utilizzando l'apposita funzionalità di AVCPASS, l'elenco degli operatori economici partecipanti alla procedura di affidamento.

7. Ai fini delle verifiche, il soggetto abilitato avvia tramite AVCPASS la richiesta dei documenti a comprova dei requisiti per gli operatori economici interessati; successivamente l'Autorità avvia presso gli Enti Certificanti le richieste dei documenti definiti nel comma 1 del successivo art. 5.

8. L'Autorità mette a disposizione tempestivamente i documenti a comprova dei requisiti, non appena ricevuti dagli Enti Certificanti.

9. Entro il termine di 60 giorni dalla data dell'aggiudicazione definitiva di ciascuna procedura di affidamento gestita tramite AVCPASS, il Responsabile del Procedimento deve trasferire definitivamente sui propri sistemi, mediante l'apposita funzionalità, i fascicoli di gara e i documenti in essi contenuti.

10. Trascorsi 4 giorni dalla scadenza del termine per l'acquisizione dei documenti,

ove il Responsabile del Procedimento non abbia adempiuto a quanto previsto dal comma 9, l'Autorità procede ad inviare la documentazione via PEC alla stazione appaltante/ente aggiudicatore. Tale invio costituisce consegna ufficiale della documentazione di gara. A partire da questa data la stazione appaltante/ente aggiudicatore acquisisce la piena titolarità dei dati.

11. La conservazione dei documenti è onere di ciascuna stazione appaltante/ente aggiudicatore. L'eventuale richiesta di accesso agli atti è in ogni caso inviata alla stazione appaltante/ente aggiudicatore.

Articolo 5

Documentazione a comprova dei requisiti generali

1. La documentazione e/o i dati a comprova del possesso dei requisiti di carattere generale di cui agli articoli 38 e 39 del Codice, che sono messi a disposizione mediante adeguati sistemi di cooperazione applicativa dagli Enti Certificanti, ai sensi dell'articolo 6-bis, comma 4, del Codice , attraverso il Sistema AVCPASS sono i seguenti:

a) Visura Registro delle Imprese fornita da Unioncamere;

b) Certificato del casellario giudiziale integrale fornito dal Ministero della Giustizia;

c) Anagrafe delle sanzioni amministrative – selettivo ex art. 39 D.P.R. n. 313/2002 dell'impresa, fornita dal Ministero della Giustizia;

d) Certificato di regolarità contributiva di ingegneri, architetti e studi associati, dalla Cassa Nazionale di Previdenza ed Assistenza per gli Ingegneri ed Architetti Liberi Professionisti (Inarcassa);

e) Certificato di regolarità fiscale fornito dall'Agenzia delle Entrate;

f) Documento Unico di Regolarità Contributiva fornito dall'Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro (Inail);

g) Comunicazione Antimafia fornita dal Ministero dell'Interno.

2. Le annotazioni nel casellario informatico dei contratti pubblici, di cui all'art. 7, comma 10, del Codice, sono rese disponibili dall'Autorità nell'ambito del sistema AVCPASS. A tal fine, gli operatori economici possono visualizzare attraverso specifico alert la presenza o meno di annotazione a proprio carico. Le stazioni appaltanti/enti aggiudicatori hanno accesso diretto a tutte le informazioni già fornite attraverso l'apposito servizio accessibile dal portale AVCP.

3. Per quanto non espressamente ricompreso nell'ambito del precedente comma 1, le stazioni appaltanti/enti aggiudicatori provvedono al recupero della documentazione a comprova, secondo le modalità previste dall'art. 40, co. 1, del DPR 445 del 2000.

Articolo 6

Documentazione a comprova dei requisiti di carattere tecnico-organizzativo ed economico-finanziario

1. La documentazione e/o i dati a comprova del possesso dei requisiti di carattere tecnico-organizzativo ed economico-finanziario, che sono acquisiti presso la BDNCP e resi disponibili attraverso il Sistema AVCPASS includono:

a) Documenti e/o dati forniti dagli Enti Certificanti;

b) Documenti resi disponibili direttamente dalla stessa Autorità;

c) Documenti forniti dagli Operatori Economici.

2. La documentazione e/o i dati a comprova dei requisiti di carattere tecnico-organizzativo ed economico-finanziario, di cui al comma 1, lettera a)includono:

a) Bilanci delle società di capitali ove disponibili, forniti da parte di Unioncamere;

b) Certificazioni di sistema di qualità aziendale conforme alle norme europee della serie UNI EN ISO 9000 relative al settore EA28 forniti da Accredia;

c) Fatturato globale e ammortamenti degli operatori economici costituiti in forma d'impresa individuale ovvero società di persone, ove disponibili, forniti da parte dell'Agenzia delle Entrate;

d) Dati relativi alla consistenza e al costo del personale dipendente, forniti da parte dell'Istituto Nazionale per la Previdenza Sociale (INPS).

3. La documentazione a comprova dei requisiti di carattere tecnico-organizzativo ed economico-finanziario, di cui al comma 1, lettera b) include:

a) le Attestazioni SOA;

b) i Certificati Esecuzione Lavori (CEL). Ciascun operatore economico ha la facoltà di richiedere alla stazione appaltante/ente aggiudicatore l'inserimento nell'apposita banca dati CEL dei certificati che dovessero risultare mancanti, secondo quanto prescritto dal Comunicato del Presidente dell'Autorità del 5 ottobre 2010;

c) certificati attestanti l'avvenuta esecuzione di servizi e forniture prestati a favore di amministrazioni o enti pubblici;

d) le ricevute di pagamento del contributo obbligatorio all'Autorità da parte dei soggetti partecipanti.

4. La documentazione a comprova del possesso dei requisiti di carattere tecnico-organizzativo ed economico-finanziario, non inclusi nei commi 2 e 3, è inserita nel sistema dagli operatori economici, conformemente a quanto segnalato dal Responsabile del Procedimento in ordine alle specificità di gara.

Articolo 7

Modalità tecniche per la fornitura dei dati da parti degli Enti Certificanti

1. Ai sensi dell'articolo 6-bis, comma 4, del Codice, i singoli Enti Certificanti che detengono i dati e la documentazione sono tenuti a metterli a disposizione dell'Autorità entro i termini e le modalità definiti tramite apposite convenzioni.

2. I dati e/o i documenti di cui al precedente comma 1 vengono acquisiti dall'Autorità per conto delle stazioni appaltanti/enti aggiudicatori per il solo espletamento delle verifiche in sede di gara.

3. Per le modalità di scambio dati con gli Enti Certificanti vengono adottate le regole tecniche e di sicurezza dello standard SPCoop ed in conformità a quanto stabilito nelle Linee guida per la fruibilità di dati delle pubbliche amministrazioni ai sensi dell'art. 58, comma 2, del D. Lgs. 7 marzo 2005, n. 821 - Codice dell'Amministrazione Digitale- o soluzioni tecnologiche alternative che garantiscono comunque livelli di sicurezza non inferiori a detto standard.

4. In allegato alla presente delibera viene riportata una descrizione di dettaglio dei flussi di dati comunicati all'Autorità dagli Enti Certificanti di cui all'art. 6, comma 1, punto a).

Articolo 8

Protezione dei dati personali e misure di sicurezza

1. L'Autorità tratta i dati acquisiti nell'ambito del sistema AVCPASS per le finalità di cui all'art. 6-bis del decreto legislativo 12 aprile 2006, n. 163 e nel rispetto dei criteri di pertinenza e non eccedenza. L'Autorità agisce in qualità di Titolare autonomo ai sensi dell'art. 28 del D. Lgs. 196/03 e adempie ai relativi obblighi ivi comprese la nomina degli incaricati del trattamento e l'adozione delle misure di sicurezza.

2. La stazione appaltante/ente aggiudicatore, nell'accedere al sistema AVCPASS,

tratta i dati per le finalità cui all'art. 6-bis, comma 3, del Codice e nel rispetto dei criteri di pertinenza e non eccedenza. La stazione appaltante/ente aggiudicatore è Titolare autonomo ai sensi dell'art. 28 del D. Lgs. 196/03 dei trattamenti e adempie ai relativi obblighi, ivi comprese la nomina degli incaricati del trattamento e l'adozione delle misure di sicurezza.

3. L'operatore economico è tenuto a inserire sul sistema AVCPASS esclusivamente la documentazione pertinente alle finalità di cui all'oggetto della seguente delibera. L'operatore economico assume la piena responsabilità della natura e della qualità della documentazione prodotta e solleva l'Autorità da ogni responsabilità relativamente ai dati inseriti ed alla documentazione caricata.

4. Il sistema AVCPASS è stato progettato nel rispetto delle vigenti norme in materia di protezione dei dati personali, compresi gli obblighi di sicurezza di cui all'art. 31 del D. Lgs. 196/03. Sono state disposte, in particolare, le seguenti misure:

a) il sistema garantisce l'identificazione, l'autenticazione e l'autorizzazione dell'utenza secondo i profili assegnati.

b) Il sistema è dotato di una procedura per la verifica delle identità e dei relativi ruoli dichiarati a sistema.

c) L'accesso ai servizi AVCPASS avviene solo a seguito del superamento di una procedura di autenticazione che verifica le credenziali di autenticazione composte dall'identificativo utente e dalla relativa parola chiave e sono adottati idonei criteri di robustezza per la costruzione della password.

d) Le credenziali di autenticazione sono assegnate individualmente ad ogni incaricato e nelle istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata delle credenziali.

e) Il sistema AVCPASS espone i dati ai soggetti autorizzati per il tempo strettamente necessario al trattamento degli stessi nell'ambito delle procedure di cui al comma 1; al termine di dette procedure i dati non sono più residenti sul sistema.

f) Il sistema dispone di misure di sicurezza informatica finalizzate a ridurre al minimo il rischio di violazioni dell'integrità della riservatezza e della disponibilità dei dati trattati. In particolare sono disposte idonee procedure di audit sugli accessi, i cui esiti sono documentati. Tali procedure prevedono attività di audit basate sul monitoraggio statistico degli accessi e su meccanismi di alert che individuino comportamenti anomali o a rischio dal punto di vista della sicurezza informatica.

g) AVCPASS adotta modalità sicure per l'interazione con gli Enti Certificanti; dispone di un sistema di autenticazione degli accessi a fini di sicurezza ed è in grado di fornire su richiesta agli Enti Certificanti evidenza dell'utenza che attraverso il sistema ha generato la singola richiesta di documentazione.

h) È fatto obbligo agli Operatori Economici e alle stazioni appaltanti/enti aggiudicatori di segnalare tempestivamente all'Autorità ogni variazione dei ruoli dei soggetti che sono stati preventivamente autorizzati ad operare secondo i profili dichiarati a sistema, nonché di eventuali utilizzi impropri ed irregolari del sistema.

i) L'operatore economico, la stazione appaltante/ente aggiudicatore si impegnano a comunicare tempestivamente incidenti sulla sicurezza qualora tali incidenti abbiano impatto direttamente o indirettamente sul sistema AVCpass, nonché ogni eventuale esigenza di aggiornamento di stato degli utenti gestiti (nuovi inserimenti, disabilitazioni, cancellazioni).

j) L'Autorità informa l'utenza del corretto utilizzo del sistema.

k) AVCPASS è implementata con protocolli di sicurezza provvedendo ad asseverare l'identità digitale dei server erogatori dei servizi tramite l'utilizzo di certificati digitali emessi da una Certification Authority ufficiale.

l) Le regole di gestione delle credenziali di autenticazione prevedono, in ogni caso, la loro attribuzione univoca a una persona fisica.

m) L'autenticazione deve essere basata su dispositivi o credenziali; queste ultime sono composte dall'identificativo dell'utente e dalla relativa componente riservata (parola d'ordine o password) per la cui costruzione sono adottati idonei criteri di robustezza. Laddove vengano utilizzati dispositivi di autenticazione, deve esserne assicurata la diligente custodia.

n) La password, comunicata direttamente al singolo incaricato separatamente rispetto al codice per l'identificazione, deve essere modificata dallo stesso al primo utilizzo e, successivamente, almeno ogni 90 giorni e le ultime tre password non possono essere riutilizzate.

o) Le password devono rispondere a idonei requisiti di complessità (almeno otto caratteri, uso di caratteri alfanumerici, lettere maiuscole e minuscole, caratteri estesi).

p) Le credenziali sono bloccate a fronte di reiterati tentativi falliti di autenticazione.

q) Nella prima schermata successiva al collegamento con la banca dati, sono visualizzabili le informazioni relative all'ultima sessione effettuata con le

stesse credenziali (indicazione della data, ora e indirizzo di rete da cui è stata effettuata la precedente connessione).

r) Il tempo di conservazione dei dati relativi agli accessi e alle operazioni compiute nel sistema è fissato nei termini di legge.

Articolo 9

Norme transitorie

1. Al fine di consentire agli operatori economici e alle stazioni appaltanti/enti aggiudicatori di adeguarsi gradualmente alle nuove modalità di verifica dei requisiti, l'obbligo di procedere alla verifica stessa attraverso l'utilizzo del sistema AVCPASS decorre secondo le seguenti scadenze temporali:

a) Dal 1° gennaio 2013 per gli appalti di lavori in procedura aperta nel settore ordinario, di importo a base d'asta pari o superiore a € 20.000.000; in via transitoria, fino al 30 giugno 2013, le stazioni appaltanti/enti aggiudicatori per tali appalti possono continuare a verificare il possesso dei requisiti degli operatori economici secondo le previgenti modalità.

b) Dal 1°marzo 2013 per tutti gli appalti di importo a base d'asta pari o superiore a € 40.000,00, con esclusione di quelli svolti attraverso procedure interamente gestite con sistemi telematici, sistemi dinamici di acquisizione o mediante ricorso al mercato elettronico, nonché quelli relativi ai settori speciali; in via transitoria, fino al 30 giugno 2013, le stazioni appaltanti/enti aggiudicatori per tali appalti possono continuare a verificare il possesso dei requisiti degli operatori economici secondo le previgenti modalità.

c) A far data dal 1° luglio 2013 gli appalti di importo a base d'asta pari o superiore a € 40.000,00 di cui ai commi a) e b) entrano in regime di obbligatorietà.

d) Dal 1° ottobre 2013 per gli appalti di importo a base d'asta pari o superiore a € 40.000,00 svolti attraverso procedure interamente gestite con sistemi telematici, sistemi dinamici di acquisizione ed il ricorso al mercato elettronico, nonché per i settori speciali; in via transitoria, fino al 31 dicembre 2013, le stazioni appaltanti/enti aggiudicatori per tali appalti possono continuare a verificare il possesso dei requisiti degli operatori economici secondo le previgenti modalità.

e) A far data dal 1° gennaio 2014 il regime di obbligatorietà è esteso anche agli appalti di cui al comma d).

2. In via transitoria, i certificati attestanti l'avvenuta esecuzione di servizi e forniture prestati a favore di amministrazioni o enti pubblici indicati all'articolo 6, comma 3, lett. c) della presente delibera, sono inseriti nel

sistema dagli operatori economici. In mancanza di detti certificati, gli operatori economici possono inserire nel sistema le fatture relative alla suddetta avvenuta esecuzione indicando, ove disponibile, il CIG del contratto cui si riferiscono, l'oggetto del contratto stesso e il relativo importo, il nominativo del contraente pubblico e la data di stipula del contratto stesso. Resta ferma per la Stazione Appaltante/ente aggiudicatore la facoltà di verificare la veridicità e la autenticità delle attestazioni prodotte dagli operatori economici.

3. In relazione a quanto previsto all'art. 5, comma 1, e all'art. 6, comma 2, in via transitoria, qualora i documenti e i dati non siano messi a disposizione della Banca Dati da parte degli Enti Certificanti, l'Autorità provvede comunque ad inoltrare una apposita richiesta agli Enti Certificanti; tali Enti trasmettono i documenti richiesti dall'Autorità direttamente alle stazioni appaltanti/enti aggiudicatori. La richiesta dell'Autorità agli Enti Certificanti conterrà tutti gli estremi che consentono di ricondurre esplicitamente la richiesta stessa agli obblighi di cui all'art. 6-bis del Codice.

La documentazione di cui agli artt. 6 e 7 della presente delibera e della relativa tabella allegata può essere oggetto di modifica mediante nuova deliberazione. Le parti modificate della delibera sono sottoposte, per i profili di competenza, al parere dell'Autorità Garante per la protezione dei dati personali.

http://www.avcp.it/portal/public/classic/Servizi/Formazione