Chi è il DPO?

Chi è realmente il Responsabile della protezione dei dati (RPD) o Data Protection Officer (DPO), figura prevista dal Regolamento UE 679/2016 (GDPR)?

Forse sarebbe meglio rispondere anche ad altre domande:

- Cosa fa il DPO?
- Quali requisiti deve possedere?
- A chi serve il DPO?

Il Garante italiano per la Protezione dei Dati Personali e le **Linee-guida del WP243**, sviluppate dall'apposito Gruppo di Lavoro Articolo 29 a livello europeo, ci vengono in aiuto, ma non bastano a disperdere il polverone che si sta facendo da ogni parte attorno a questa figura.

Si legge da varie fonti di "Corsi specialistici per DPO", "Esami per qualifiche da DPO", "migliaia di posti di lavoro come DPO" e così via. È tutto al vero?

Vediamo anzitutto **quali sono i requisiti di un DPO** o RPD che dir si voglia.

Il Responsabile della Protezione dei Dati (RPD o DPO), nominato dal titolare del trattamento o dal responsabile del trattamento, dovrà:

1. Possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze.
2. Adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse. In linea di principio, ciò significa che il RPD non può essere un soggetto che decide sulle finalità o sugli strumenti del trattamento di dati personali.
3. Operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio (RPD/DPO esterno).

Il titolare o il responsabile del trattamento dovranno mettere a disposizione del Responsabile della Protezione dei Dati le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

Leggendo queste righe si evince che non possono esistere corsi per DPO che qualifichino per questo ruolo, né elenchi o albi. Ovviamente tutti i "corsi per DPO" possono essere più o meno validi per svolgere questa mansione in futuro, ma non forniscono la "patente" per farlo.

Le competenze del DPO (insieme di livello di istruzione, conoscenze, capacità/abilità ed esperienza…) devono svariare fra **competenze legali**, **informatiche** ed **organizzativo-gestionali**. Naturalmente il RPD deve conoscere bene il Regolamento UE 679/2016, ma anche il D.Lgs 196/2003 che costituisce tuttora la normativa sulla privacy italiana da oltre 13 anni ed i vari provvedimenti del Garante italiano su videosorveglianza, Amministratori di Sistema, ecc..

Quali saranno le competenze prevalenti? Fino a che livello un DPO deve sapere di sicurezza informatica?

Sicuramente sono più importanti competenze di base consolidate a 360° negli ambiti legale, informatico e gestionale, piuttosto che essere esperti di una materia e non conoscere nulla delle altre. Infatti il DPO non dovrà configurare un firewall (attività che potrà delegare a tecnici sistemisti), ma dovrà sapere cos'è e conoscere i suoi principi di funzionamento.

Per capire quali competenze precise dovrà possedere il DPO occorre comprendere che il DPO è **un ruolo** da ricoprire in una determinata organizzazione, dunque sarà importante che il DPO conosca discretamente i processi gestionali dell'organizzazione in cui dovrà operare ed in funzione del tipo di organizzazione dovrà possedere requisiti minimi differenti. Per esempio il DPO di un Ospedale o di una organizzazione della Sanità Privata non dovrà necessariamente avere le stesse competenze del DPO di un Comune, di un Ufficio Giudiziario o di una Società che sviluppa software per la profilazione di utenti. Quindi ad ognuno il suo DPO.

Infine sottolineiamo il fatto che il DPO deve essere indipendente dalle altre funzioni aziendali e dipendere solo dal titolare del trattamento, dunque in molte organizzazioni difficilmente una figura interna possiede questi requisiti.

Quindi, **quali sono i compiti del DPO**?

Il Responsabile della Protezione dei Dati dovrà, in particolare:

- **sorvegliare** l'osservanza del Regolamento, **valutando i rischi** di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
- **collaborare** con il titolare/responsabile, laddove necessario, nel condurre una **valutazione di impatto** sulla protezione dei dati (DPIA);
- **informare** e **sensibilizzare** il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal Regolamento e da altre disposizioni in materia di protezione dei dati;
- **cooperare** con il Garante e fungere da **punto di contatto** per il Garante su ogni questione connessa al trattamento;
- **supportare** il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un **registro delle attività di trattamento**.

Esaminando i suddetti punti emerge un ruolo un po' da **consulente** e un po' da **auditor**, ma con contorni non ben definiti. In base al tipo di organizzazione il DPO o RPD che dir si voglia dovrà svolgere compiti più o meno estesi, potrà essere supportato da un *team* di altre persone, interne o esterne all'organizzazione, che potranno essere specialisti in ambito informatico, legale o altro a seconda del settore di appartenenza. Ad esempio in una organizzazione sanitaria il DPO potrebbe essere supportato da esperti nel settore sanitario, ad esempio medici.

Anche un DPO esterno potrebbe assumere l'incarico avvalendosi di un *team* di collaboratori, anche per far fronte alle numerose richieste da parte degli interessati che potrebbero porre quesiti sulle modalità di trattamento dei propri dati personali.

Inoltre è da sottolineare il fatto che il DPO deve disporre anche di **autonomia** e **risorse sufficienti** a svolgere in modo efficace i compiti cui è chiamato ed è il titolare (o responsabile) del trattamento che ha l'onere di garantire ciò.

In definitiva il perimetro dei compiti del DPO andrebbe definito bene di caso in caso in apposito contratto o delega del titolare.

Si osserva che il GDPR impone al titolare o al responsabile del trattamento di pubblicare i dati di contatto del DPO e di comunicare i dati di contatto del DPO alle pertinenti autorità di controllo; dunque è un incarico ufficiale e pubblico, affinché tutti gli interessati al trattamento di dati personali effettuato dall'organizzazione possano contattare il DPO per richiedere informazioni sul trattamento dei dati che li riguardano.

Da ultimo, ma non di minore importanza: i DPO **non rispondono personalmente in caso di inosservanza del GDPR**, ma tale responsabilità ricade sempre e solo sul titolare o sul responsabile del trattamento.

Vediamo, infine, **in quali casi è previsto il DPO**, ovvero quando una organizzazione è obbligata a nominare un DPO.

Dovranno designare obbligatoriamente un RPD:

1. amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;
2. tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
3. tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Anche per i casi in cui il regolamento non impone in modo specifico la designazione di un RPD, è comunque possibile una nomina su base volontaria. Ma questa frase non farà effetto su quelle Società che pensano di nominare un DPO solo se strettamente obbligatorio per legge.

Si precisa che un gruppo di imprese o soggetti pubblici possono nominare un unico RPD.

Dunque un consulente esterno qualificato potrebbe assumere il ruolo di DPO, per così dire, in *outsourcing*, per diverse organizzazioni.

Gli esempi forniti nella Linea-guida del GdL Articolo 29 su chi effettivamente dovrà nominare un DPO in ambito privato forniscono qualche indicazione, ma non dirimono tutti i dubbi. Soprattutto il concetto di "larga scala" è molto dibattuto: preso atto che un medico di famiglia non tratta dati particolari (sanitari in questo caso) su *larga scala*, salendo sul gradino superiore di questa scala virtuale, quale soggetto, avente comunque un organico ridotto, tratta dati particolari su larga scala: un poliambulatorio privato, una clinica/ospedale privati, un Amministratore di Condominio, un fornitore di servizi di ristorazione collettiva?

Speriamo che non siano le sentenze a definire meglio la normativa che, qui come in altre parti, lascia ampio spazio all'interpretazione.

Da quanto esposto emerge una similitudine fra la figura del DPO – che deve proteggere i dati personali dell'individuo – e l'RSPP (Responsabile del Servizio Prevenzione e Protezione per la Sicurezza e Salute del Lavoro, secondo il D.Lgs 81/2009 e s.m.i.) – che deve garantire la sicurezza nei luoghi di lavoro -, con un distinguo, però: l'RSPP è responsabile anche legalmente in caso di incidente, mentre il DPO non è responsabile in caso di violazione dei dati personali.

Il GDPR per la privacy nella sanità privata

Mancano ormai solo 8 mesi all'attuazione del nuovo Regolamento UE 679/2016 sulla Protezione dei Dati Personali (o *General Data Protection Rule*, GDPR), pubblicato nel maggio 2016, che diverrà pienamente attuativo il 25 maggio 2018. Esso apporta importanti novità alla Legge sulla Privacy italiana attualmente in vigore, il D. Lgs 196/2003 e s.m.i., ed impone un diverso modo per affrontare la privacy nelle organizzazioni che trattano dati sanitari, i quali costituiscono una particolare categoria di "dati sensibili" (ora definiti "dati particolari" dal GDPR).

In questo articolo ci occuperemo delle regole per la privacy dei dati sanitari secondo il GDPR, ma non di ciò che attiene alla Sanità Pubblica, quali Ospedali, ASL, ambulatori pubblici, ecc., i quali dovranno sottostare alle medesime regole, ma con adempimenti leggermente diversi (ad es. la figura del DPO o *Data Protection Officer* è obbligatoria sempre) e con l'identificazione del titolare del trattamento che investe un'entità della Pubblica Amministrazione. Da un certo punto di vista lo Stato ha mezzi adeguati per affrontare, speriamo nel modo corretto, l'adeguamento al GDPR.

Invece, per quanto riguarda la Sanità Privata, le cose sono un po' diverse ed a volte l'organizzazione interna non contempla competenze e tecnologie adeguate per far fronte al nuovo Regolamento 679/2016. Parliamo di organizzazioni di piccole e medie dimensioni, che vanno dalle Farmacie ai Poliambulatori di analisi diagnostiche, alle Cliniche e Case di Cura Private.

Alcuni adempimenti nelle organizzazioni private che si occupano di servizi sanitari sono da interpretare, in quanto la norma europea non fornisce indicazioni così precise su alcuni aspetti, ma pone l'accento sulla "responsabilizzazione" del titolare del trattamento, ovvero sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento, cioè misure tecniche ed organizzative adeguate.

Ci troviamo così di fronte ad un problema di competenze: il titolare del trattamento di queste organizzazioni della Sanità Privata è la società stessa che gestisce la struttura (a volte il singolo professionista), quindi tutte le responsabilità

ricadono, di fatto, sul legale rappresentante della stessa, il quale normalmente si occupa di tutt'altro (medico, farmacista o manager amministrativo) e non sa quali misure adottare per tutelarsi, non solo dalle possibili sanzioni (fino al 4% del fatturato annuo), ma anche da eventuali richieste di risarcimento danni di pazienti che non sentissero adeguatamente tutelata la propria privacy.

Gli elementi da considerare nella gestione della privacy in una organizzazione sanitaria privata sono diversi: la gestione dei documenti su supporto cartaceo o analogo (es. lastre di esami diagnostici), la gestione dei documenti su supporto digitale, la gestione delle informazioni elaborate dai sistemi informatici, la gestione delle informazioni trasmesse verbalmente…

Coloro che hanno gestito la privacy in passato con l'aiuto di un avvocato – che gli ha preparato lettere di nomina incaricati, informative e consensi – e di una società di consulenza informatica – che gli ha gestito la sicurezza dei dati (antivirus, backup, ecc.) – dovranno modificare il proprio approccio in quanto la nuova privacy del GDPR richiede un approccio più sistemico ed orientato alla valutazione dei rischi.

I principi introdotti dal GDPR – in particolare il principio di liceità del trattamento, di integrità e di riservatezza, di limitazione delle finalità… – devono essere recepiti interpretandoli nel modo corretto, declinandoli nella propria realtà; non esistono più regole ben definite (password di almeno 8 caratteri, antivirus aggiornati con una certa frequenza, ecc.).

I passi fondamentali che un'organizzazione sanitaria privata dovrebbe affrontare per adeguarsi al GDPR sono i seguenti:

- Analisi dei processi dell'organizzazione;
- Mappatura dei trattamenti di dati personali;
- Identificazione di ruoli e responsabilità per il trattamento;
- Predisposizione del Registro dei trattamenti di dati personali;
- Valutazione dei rischi sui trattamenti di dati;
- Valutazione di impatto per quei trattamenti che lo richiedono;
- Definizione delle misure organizzative per la protezione dei dati personali;
- Definizione delle misure tecniche per la protezione dei dati personali;
- Predisposizione delle procedure per il trattamento dei dati e loro documentazione.

In questo percorso si incontrano alcuni elementi particolarmente significativi, la cui gestione richiede molta attenzione ed una corretta interpretazione del Regolamento 679/2016:

- La formulazione dell'**informativa** e dei **consensi** al trattamento da parte degli interessati;
- La progettazione, implementazione e gestione della **sicurezza delle informazioni**

(non solo informatica);
- Gestione degli **applicativi informatici** e dei rapporti con i relativi fornitori;
- Rapporti con i **responsabili del trattamento esterni**;
- Eventuale **nomina del DPO** o RPD (Responsabile del Trattamento dei Dati);
- Modalità di effettuazione della **valutazione dei rischi** e necessità del c.d. *Data Impact Assessment* (DIA).

Vediamo di chiarire un paio di punti relativamente alle organizzazioni sanitarie private.

La nomina del DPO (RPD) è obbligatoria:

1. se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
2. se le attività principali del titolare o del responsabile consistono in **trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala**;
3. se le attività principali del titolare o del responsabile consistono nel **trattamento su larga scala di categorie particolari di dati** o di dati personali relativi a condanne penali e reati.

Se è evidente che non siamo nel caso (a), probabilmente nemmeno nel caso (b), occorre riflettere bene sul caso (c).

I dati sanitari ricadono senz'altro nelle particolari categorie di dati definite dal GDPR e resta solo da capire cosa significa "su larga scala". Le interpretazioni ufficiali (Regolamento e Linea Guida sui RPD del GdL Articolo 29) ci indicano che i pazienti trattati da un singolo medico di famiglia non rientrano nel concetto di "larga scala". Analogamente si potrebbe pensare per una Farmacia o un piccolo ambulatorio privato, ma salendo di dimensione nelle organizzazioni è evidente che questa condizione trova applicazione.

Altra questione è quella relativa alla necessità di istituire un **Registro dei Trattamenti**: qui l'obbligo si ha per organizzazioni con più di 250 addetti oppure in presenza di rischio per diritti e libertà degli interessati per trattamenti non occasionali di dati sensibili o giudiziari. In questo caso le nostre organizzazioni della sanità privata ricadono quasi tutte nell'obbligo di trattamento, fermo restando che è comunque opportuno, per il principio di responsabilizzazione (*accountability*) del titolare del trattamento, creare e gestire tale Registro.

Esiste, infine, la possibilità, per i titolari del trattamento che vorranno garantirsi maggiormente dai rischi inerenti la privacy, di ottenere la certificazione del proprio processo di gestione di dati sanitari (per ora solo lo Schema di Certificazione ISDP©10003:2015 di INVEO, accreditato da ACCREDIA).

Come sta la privacy ad un anno dall'attuazione del GDPR?

Il Regolamento (Ue) 2016/679, noto anche come **RGPD** (Regolamento Generale sulla Protezione dei Dati) o **GDPR** (*General Data Protection Regulation*), troverà piena attuazione esattamente fra un anno da oggi, il **25 maggio 2018**, ovvero al termine del periodo di transizione.

A seguito dell'interessante seminario svoltosi venerdì 19 maggio 2017 presso l'Ordine degli Ingegneri di Bologna sulle **possibili forme di certificazione in ambito Privacy**, è utile fare qualche riflessione sull'attuazione di questa nuova normativa nelle organizzazioni del nostro Paese.

Attualmente esistono alcuni documenti ufficiali che permettono di comprendere meglio come declinare i requisiti del GDPR nella propria organizzazione, tra i quali:

- Linee Guida all'applicazione del RGPD del Garante Privacy italiano
- Linee guida sui responsabili della protezione dei dati (RPD) WP 243 (272 download) (compreso l'allegato con le FAQ)
- Linee Guida Valutazione-Impatto WP 248 (260 download) .

Al momento, però, le indicazioni fornite non sono in grado di fugare tutti i dubbi sull'applicazione del GDPR, anzi!

Il GDPR dà spazio a integrazioni dei requisiti in esso riportati per regolamentare situazioni specifiche per tipo di dati trattati e particolari legislazioni nazionali, sarà compito del Garante Italiano definire eventuali disposizioni integrative che avranno valore di Legge.

Esaminando i concetti principali del GDPR, quali **responsabilizzazione** (*accountability*) del titolare e del responsabile del trattamento, ***privacy by design***, ***privacy by default***, **valutazione di impatto**, **valutazione dei rischi** e "misure di sicurezza adeguate", è facile individuare molti punti di debolezza di numerose organizzazioni italiane che, per mentalità, non sono abituate ad affrontare il problema della protezione dei dati personali con metodo e come una reale priorità. Per molti vertici aziendali la privacy è "solo una scocciatura" e il nuovo Regolamento un "ennesimo obbligo cui toccherà adeguarsi", ma non tanto prima della

scadenza. Come se bastasse fare quattro documenti per risolvere il problema per sempre (o per lo meno fino al prossimo cambiamento normativo)!.

Purtroppo questo "approccio" per essere conformi al GDPR deve cambiare, perché è una norma di stampo anglosassone (tipo "*common law*", a dispetto della Brexit) che richiede una **forte responsabilizzazione di coloro che ricopriranno il ruolo di titolari** (rappresentanti legali per le società) **e responsabili del trattamento**.

L'affidamento all'esterno di dati personali, anche solo per adempimenti legislativi, come la preparazione delle buste paga demandate allo Studio di Consulenza del Lavoro, devono richiedere un'attenta analisi del contratto con il soggetto esterno e verifica che esso soddisfi tutti i requisiti in termini di misure di sicurezza per la protezione dei dati.

Certamente per le PMI che trattano solo dati personali di dipendenti e collaboratori, oltre a nominativi di referenti di clienti e fornitori, l'adeguamento al GDP non sarà di particolare impatto, ma basta demandare all'esterno ad un servizio via web come la gestione del personale oppure avere un sito internet di *e-commerce* che raccoglie dati di utenti per rendere la gestione un pochino più complessa.

Viceversa le **organizzazioni che trattano dati particolari** (i.e. sensibili), soprattutto se poco strutturate e se gestiscono tali dati insieme a fornitori di servizi mediante internet, dovranno cambiare il loro atteggiamento sulla privacy e valutare attentamente i rischi che corrono. Soprattutto non credano che basti far scrivere un DPS o "riesumare" quello precedentemente redatto prima che il Governo lo abolisse: la carta (o i documenti digitali) non bastano, occorre la consapevolezza e la sostanza di applicazione di regole comportamentali, misure di sicurezza fisica e logica (sistemi informatici) ritenute adeguate (da chi?) e instaurare con fornitori e partner rapporti contrattuali che prendano in considerazione anche il trattamento dei dati personali e la loro tutela.

Recenti eventi come i *ransomware* del tipo *Wannacry* potrebbero far piangere veramente i titolari di trattamenti di dati sanitari, il cui valore per gli hacker potrebbe essere ben superiore dei 300 dollari in Bitcoin. Il ricatto potrebbe essere non del tipo "se rivuoi i tuoi dati paga", ma "se non vuoi che divulghi su internet i tuoi dati paga il riscatto"!. Ci sono stati già casi analoghi legati a ricatti a proprietari di diritti di serie TV americane molto più innocui.

Relativamente al ruolo del DPO, l'obbligo di nomina imposto dal Regolamento ricade in modo certo solo su Enti Pubblici, mentre le Organizzazioni che controllano in modo regolare e sistematico dati personali di interessati su larga scala e quelle che trattano dati particolari (traducibili con i dati sensibili del vecchio Codice Privacy, D.Lgs 196/2003) su larga scala o trattano dati relativi a condanne penali e reati non sono facilmente determinabili. Cosa significa "su larga scala"? Le indicazioni fornite hanno permesso di stabilire che un medico di base della Sanità

Italiana non tratta dati sanitari su larga scala, ma come considerare strutture superiori come Farmacie, Ambulatori medici Privati, Cliniche Private? Gli Studi Legali devono nominare un DPO?

Sicuramente le **competenze del DPO** dovrebbero comprendere competenze **legali** (conoscenza di normative e leggi applicabili alla materia ed ai dati trattati dall'organizzazione titolare del trattamento), competenze **informatiche** (non necessariamente particolarmente approfondite, per esse può rivolgersi a tecnici specializzati come sistemisti ed esperti di sicurezza informatica) e **gestionali-organizzative**.

Relativamente alle forme di **certificazione sulla privacy** che, beninteso, non esimono i titolari ed i responsabili del trattamento da essere passibili delle sanzioni previste dal Regolamento e dal Garante Privacy Italiano in caso di infrazioni, occorre distinguere fra diversi tipi di certificazione:

- Certificazione di prodotto o servizio, accreditata secondo ISO 17065, come ad es. lo schema ISDP 10003:2015 – *Criteri e regole di controllo per la Certificazione dei processi per la tutela delle persone fisiche con riguardo al trattamento dei dati personali – Reg. EU 679/2016*.
- Certificazione delle figure Professionali della Data Protection (DPO, "Auditor Privacy", "Privacy Officer" e "Consulente Privacy").
- Certificazione delle Aziende del *Data Protection Management System* in conformità al Codice di Condotta DPMS 44001:2016© ed al Reg. (UE) 679/2016.
- Certificazione del sistema di gestione della sicurezza delle informazioni secondo la ISO 27001:2013.

Premesso che la certificazione accreditata secondo il Regolamento UE 679/2016, così come esposta dall'articolo 43 dello stesso RGPD, trova attualmente riscontri solo in standard e certificazioni afferenti allo schema di accreditamento ISO 17065 (certificazioni di prodotto o servizio), emergono le seguenti considerazioni:

- Non si è ancora affermato un sistema di gestione della privacy riconosciuto che, sulla base della struttura HLS delle norme sui sistemi di gestione (ISO 9001, ISO 27001, ecc.), consenta di gestire la protezione dei dati con un approccio sistemico, basato sui processi e concetti come il *risk based thinking* e l'attuazione di azioni finalizzate ad affrontare i potenziali rischi sul trattamento di dati personali.
- Il ruolo del *Data Processor Officer* (DPO o RPD), come è definito dal Regolamento, non corrisponde ad una figura professionale specifica avente determinati requisiti di competenza (istruzione scolastica e post scolastica, conoscenze normative e tecniche, esperienza nell'ambito privacy, partecipazione a corsi di formazione, superamento di esami o abilitazioni). Il DPO è piuttosto "un ruolo" che potrebbe richiedere competenze differenti a seconda della realtà in cui opera e della criticità della protezione dei dati personali nell'organizzazione stessa.

- Tutti gli schemi e gli standard sopra indicati permettono di ridurre il rischio che il titolare del trattamento e gli eventuali responsabili incorrano in infrazioni nel trattamento di dati personali e, quindi, rischino infrazioni anche pesanti e/o gravi danni di immagine.

Per concludere, secondo il *risk based thinking*, quali rischi corrono le aziende che non sono adeguate al GDPR?

La probabilità di essere sanzionati a seguito di ispezioni del Nucleo Privacy della GdF è estremamente bassa, un po' più alta per organizzazioni che trattano dati particolarmente critici (la valutazione è fatta in base al numero delle ispezioni avvenute negli ultimi anni).

La probabilità di incorrere in sanzioni o in risarcimento danni a causa di istanze di interessati che si sentono danneggiati nella loro privacy oppure in caso di incidenti di dominio pubblico è un po' più alta.

L'impatto delle conseguenze nel caso si verifichino suddetti eventi negativi dipende dal tipo di organizzazione e dai dati trattati, può essere significativo o devastante a seconda dei casi.

Leggi anche l'articolo Impatti del Regolamento Privacy sullo sviluppo software.

Impatti del Regolamento Privacy sullo sviluppo software

Il Nuovo Regolamento Europeo sulla Privacy (GDPR), emanato lo scorso maggio ed in vigore entro fine maggio 2018, pone nuove questioni relativamente all'impiego di programmi software per l'elaborazione di dati personali, in particolare se si tratta anche di dati c.d. "sensibili" secondo la vecchia definizione del D. Lgs 196/2003.

Infatti il nuovo Regolamento Europeo sulla privacy ("Regolamento UE 2016/679 del Parlamento europeo") impone alle organizzazioni che intendono effettuare trattamenti di dati personali di "progettare" il sistema in modo tale che sia conforme fin da subito (**Privacy by design**) alle regole della privacy, spostando la responsabilità del corretto trattamento tramite strumenti informatici idonei sul titolare e sul

responsabile del trattamento, quando identificato.

Nella pratica una organizzazione, prima di impiegare un applicativo software per trattare dati personali dovrà verificare che esso sia conforme ai requisiti stabiliti dal Regolamento UE 679/2016, ovvero che presenti caratteristiche di sicurezza adeguate per mantenere protetti i dati personali, compresa l'eventuale pseudonomizzazione dei dati personali, quando necessaria, e la cifratura dei dati stessi.

Il Regolamento parla anche di "certificazione" della privacy, che può riferirsi ad un singolo o ad un insieme di trattamenti effettuati da un programma software, oppure da tutti i trattamenti effettuati da una organizzazione. In quest'ultimo caso siamo molto vicini alla certificazione del sistema di gestione ISO 27001, anche se in realtà il GDPR intende qualcosa di differente. Al proposito è stato approvato da ACCREDIA lo schema proprietario ISDP©10003:2015 (conformità alle norme vigenti EU in tema di trattamenti dei dati personali)che conente di certificare un prodotto, processo o servizio relativamente alla gestione dei dati personali, quindi anche un applicativo software che tratta dati personali.

Lo schema di certificazione ISDP 10003:2015 risponde ai requisiti di cui agli art. 42 e 43 del Regolamento 679/2016 ed è applicabile a tutte le tipologie di organizzazioni soggette alle norme vigenti in tema di tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati. Lo schema di certificazione specifica ai "Titolari" e "Responsabili" del trattamento, soggetti ai vincoli normativi vigenti nel territorio dell'EU, i requisiti necessari per la corretta valutazione della conformità alle norme stesse.

Per maggiori informazioni su questo schema di certificazione si veda la pagina del sito Inveo
http://www.in-veo.com/servizi/certificazioni-inveo/isdp-10003-2015-data-protection.

Ricordiamo anche che all'art 25, coma 2 il Regolamento sancisce che:

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Rappresenta **la c.d. Privacy by default**: devono essere trattati "per default" solo i dati necessari a perseguire le finalità del trattamento posto in essere dal responsabile dello stesso, ovvero non devono essere trattati dati in eccesso senza che una persona fisica autorizzata lo consenta.

La certificazione introdotta all'Art. 42 può servire a dimostrare l'adozione di misure tecniche ed organizzative adeguate.

L'impatto di queste regole sugli **applicativi software** utilizzati per trattare anche dati personali è notevole: una organizzazione di qualsiasi dimensione che adotta un sistema informatico gestionale che tratta dati personali non in modo conforme al Regolamento UE 679/2016 di fatto rischia di essere sanzionata perché non ha adottato misure di sicurezza adeguate. Le responsabilità ricadono, in questo caso, sul titolare del trattamento e sul responsabile del trattamento, ove presente.

Dunque prima di adottare un nuovo software che gestisce archivi contenenti dati personali (a maggior ragione se vengono gestiti dati sanitari o altri dati c.d. "sensibili") titolari e responsabili del trattamento devono valutarne la **conformità alla normativa sulla privacy** e questo può essere al di fuori delle competenze di chi decide l'acquisto di un applicativo software (responsabili EDP, Direttori Generali, ecc.), soprattutto nelle piccole e medie imprese o nelle strutture sanitarie di modeste dimensioni (es. Cliniche ed ambulatori privati).

La casistica di software che ricadono in questa sfera è vastissima, si va dai comuni ERP che trattano anche dati del personale, ai software per la gestione delle paghe, ai programmi per la gestione delle *fidelity card*, ai software impiegati in strutture sanitarie o quelli utilizzati dagli studi legali.

Oggi molti applicativi, magari obsoleti, non permettono di implementare misure di sicurezza adeguate (password di lunghezza adeguata, password di complessità minima variate periodicamente, password trasmesse via internet con connessioni crittografate, gestione utenti, raccolta di dati minimi indispensabili, gestione dei consensi, procedure di backup, ecc.) e in futuro il loro impiego diverrà non conforme alla normativa sulla privacy, ovvero non saranno più commercializzabili.

Da un lato i progettisti e gli sviluppatori di applicativi software dovranno considerare fra i requisiti di progetto anche quelli relativi alla normativa privacy, dall'altro le organizzazioni che adotteranno applicativi software (o che già li stanno utilizzando) saranno responsabili della loro eventuale non conformità al Regolamento Privacy. Sicuramente una certificazione di tali applicativi o un assessment indipendente potrà sollevare il titolare del trattameto dalle rsponsabilità (cfr. principio dell'*accountability)* connesse all'adozione di un software che non tratta i dati in conformità al GDPR.

Nuovo Regolamento UE sulla Privacy: cosa cambia per le imprese?

Lo scorso 4 maggio è stato pubblicato sulla gazzetta ufficiale della Comunità Europea il "**Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE** (regolamento generale sulla protezione dei dati)" e dopo 20 giorni dalla sua pubblicazione è divenuto legge europea, pertanto a partire dal 25 maggio 2016 decorrono i due anni di transitorio per l'applicazione del nuovo Regolamento.

Nella pagina Documenti di questo sito è possibile scaricare il testo ufficiale (ora anche per gli utenti non registrati).

Il Garante per la Protezione dei dati personali ha pubblicato un'apposita guida (http://194.242.234.211/documents/10160/5184810/Guida+al+nuovo+Regolamento+europeo+in+materia+di+protezione+dati).

Rispetto al precedente articolo pubblicato su questo sito il 27/04/2016, basato sulla traduzione della proposta di Regolamento approvata dal Parlamento Europeo a dicembre 2015, di cui il presente articolo costituisce un aggiornamento, si rilevano alcune differenze nella traduzione del testo originale inglese in lingua italiana, rispetto all'attuale Codice privacy D.Lgs 196/2003:

- Viene mantenuto il "Titolare del trattamento" (*Data Controller*);
- Viene mantenuto il "Responsabile del Trattamento" (*Data processor*);
- Viene abolito l'Incaricato del trattamento.

Il nuovo Regolamento introdurrà una legislazione in materia di protezione dati uniforme e valida in tutta Europa, affrontando temi innovativi – come il diritto all'oblio e alla portabilità dei dati – e stabilendo anche criteri che da una parte responsabilizzano maggiormente imprese ed enti rispetto alla protezione dei dati personali e, dall'altra, introducono notevoli semplificazioni e sgravi dagli adempimenti per chi rispetta le regole. Il Regolamento UE 679/2016, però, non sarà l'unica fonte legislativa per regolamentare la protezione dei dati personali, infatti le Autorità dei singoli Stati Membri – e quindi il Garante della Privacy per l'Italia – potranno integrare i contenuti del Regolamento dettagliando meglio alcuni aspetti che al momento appaiono poco chiari, introdurre linee guida generali e di settore, regolamentare aspetti particolari, ecc.

A tal proposito occorre ricordare che, con l'uscita del Regolamento 679 non vengono aboliti i provvedimenti del nostro Garante su Videosorveglianza, Amministratori di Sistema, fidelity card, biometria, tracciamento flussi bancari, ecc. Tali provvedimenti probabilmente verranno modificati e/o integrati dal Garante Privacy per aggiornarli ed eventualmente adeguarli alle prescrizioni del Regolamento Europeo 679.

Il Garante Privacy italiano potrà inoltre integrare il Regolamento UE 679 per disciplinare il trattamento di dati personali effettuato per adempiere obblighi di legge italiana e in particolari ambiti, ad esempio quello dei dati sanitari, oppure per definire in modo più dettagliato gli obblighi per le PMI (ovvero per le organizzazioni che occupano meno di 250 dipendenti, per le quali il regolamento 679 ha stabilito delle semplificazioni).

Ma quali sono le principali novità per le imprese nella gestione della privacy a fronte del Regolamento UE?

L'aspetto più significativo è sicuramente il cambio di approccio rispetto al Codice Privacy attualmente in vigore in Italia, ed in particolare all'Allegato B, ovvero al Disciplinare Tecnico delle Misure Minime di Sicurezza. Il nuovo Regolamento Europeo sulla privacy, infatti, non definisce requisiti specificati in termini precisi, come avviene per l'attuale normativa italiana sulla privacy, ma sposta la responsabilità di definire le misure di sicurezza idonee a garantire la privacy dei dati personali trattati sul titolare o responsabile del trattamento, dopo un'attenta analisi dei rischi.

Dunque non ci sono più misure minime, ma solo misure di sicurezza adeguate, progettate dal titolare o responsabile del trattamento dopo aver effettuato l'analisi dei rischi che incombono sui dati personali che si intende trattare. Sottolineiamo quest'ultimo aspetto: le misure di prevenzione vanno poste in atto prima di iniziare il trattamento.

Poiché a livello nazionale la legislazione italiana ed il Garante per la Protezione dei Dati Personali hanno seguito il percorso europeo, a partire dalla Direttiva Europea 46/95, a livello di principi sulla privacy non ci sono differenze significative tra normativa italiana e Regolamento Europeo. Infatti, alcune regole già imposte dal Codice Privacy e dalle successive disposizioni del Garante restano valide, anche se con contorni un po' meno definiti da criteri oggettivi. In sostanza:

- Viene regolamentato solo il trattamento di dati personali di persone fisiche (non giuridiche) per scopi diversi dall'uso personale.
- Resta una distinzione fra trattamento di dati personali comuni e trattamento di dati c.d. sensibili, anche se la definizione del D.lgs 196/2003 non viene utilizzata nel Regolamento UE 679, lasciando però la possibilità agli Stati membri di stabilire una disciplina particolare in merito.

- Restano gli obblighi di informare l'interessato sull'uso che verrà fatto dei suoi dati personali.
- Restano gli obblighi di ottenere il consenso per i trattamenti non necessari o per i trattamenti di particolari tipi di dati, ad esempio quelli idonei a rivelare lo stato di salute delle persone, le origini razziali, le idee religiose, ecc.

Tra gli elementi che cambiano vi sono sicuramente:

- La denominazione ed i ruoli degli attori: il titolare del trattamento rimane tale, **il responsabile del trattamento è ora responsabile in solido con il titolare per i danni derivanti da un trattamento non corretto**, l'incaricato rimane il soggetto che fisicamente tratta i dati, ma tale ruolo non è delegabile, se non attraverso uno specifico accordo contrattuale. Il responsabile può individuare un proprio rappresentante.
- I dati personali trattati devono essere protetti con misure organizzative e tecniche adeguate a garantirne la riservatezza e l'integrità.
- I diritti dell'interessato sono più ampi e maggiormente tutelati.
- Il responsabile del trattamento deve mettere in atto **misure tecniche ed organizzative** tali da consentirgli di dimostrare che tratta i dati personali in conformità al Regolamento. Tali misure devono seguire lo stato dell'arte e devono derivare dall'analisi dei rischi che incombono sui dati, secondo relativa gravità e probabilità.
- **Privacy by default**: devono essere trattati "per default" solo i dati necessari a perseguire le finalità del trattamento posto in essere dal responsabile dello stesso, ovvero non devono essere trattati dati in eccesso senza che una persona fisica autorizzata lo consenta.
- **Privacy by design**: ogni nuovo trattamento di dati personali dovrà essere progettato in modo da garantire la sicurezza richiesta in base ai rischi a cui è sottoposto prima di essere implementato. Anche i sistemi informatici dovranno essere progettati secondo tale principio.
- Possono esserci più responsabili per un medesimo trattamento che risulteranno, pertanto, corresponsabili di eventuali trattamenti non conformi, ma dovranno stabilire congiuntamente le rispettive responsabilità.
- Le imprese **con sede al di fuori dell'Unione Europea**, che trattano dati personali di interessati residenti nella UE dovranno eleggere una propria organizzazione o entità all'interno della UE che sarà responsabile di tali trattamenti.
- Devono essere mantenuti **registri dei trattamenti** di dati effettuati con le informazioni pertinenti e le relative responsabilità. Tali registri non sono obbligatori per organizzazioni con meno di 250 dipendenti salvo che non trattino dati sensibili (secondo la definizione del Codice della Privacy attualmente in vigore) o giudiziari. Tale discriminante potrà essere meglio specificata da appositi provvedimenti del nostro Garante.
- Il responsabile del trattamento deve notificare all'autorità competente – e, in casi gravi, anche all'interessato – ogni **violazione dei dati** (*data breach*) trattati entro 72 ore dall'evento.

- Quando un trattamento presenta dei rischi elevati per i dati personali degli interessati (i casi specifici dovranno essere esplicitati dall'Autorità Garante), il responsabile del trattamento deve effettuare una **valutazione di impatto preventiva**, prima di iniziare il trattamento.
- Viene introdotta la **certificazione** del sistema di gestione della privacy (le cui modalità dovranno essere meglio definite tramite gli Organismi di Accreditamento Europei, ACCREDIA per l'Italia)..
- È richiesta la designazione di un **Responsabile della Protezione dei Dati** (*Data Protection Officer*) nelle Aziende Pubbliche e nelle organizzazioni che trattano dati sensibili o giudiziari su larga scala oppure che la tipologia di dati trattati e la loro finalità richieda il controllo degli incaricati al trattamento su larga scala.

Proprio quest'ultimo punto, variato rispetto alle precedenti versioni del Regolamento, farà molto discutere, poiché non stabilisce criteri precisi ed oggettivi (cosa significa "su larga scala"?) per l'adozione di tale figura professionale, di competenze adeguate a garantire una corretta applicazione della normativa sulla privacy. Il Responsabile per la Protezione dei Dati dovrà essere correttamente informato dal Responsabile del Trattamento su tutte le attività che riguardano la privacy e dovrà disporre di risorse adeguate per svolgere il proprio compito e mantenere le sue competenze adeguate al ruolo che ricopre. Egli dovrà inoltre essere indipendente dalle altre funzioni dell'organizzazione e riferire solamente all'alta direzione.

La sicurezza dei dati – in termini di riservatezza, integrità e disponibilità – deve essere garantita in funzione del rischio che corrono i dati stessi, dei costi delle misure di sicurezza e dello stato dell'arte della tecnologia. Pertanto le password di almeno 8 caratteri variate almeno trimestralmente, l'antivirus aggiornato, il firewall e l'aggiornamento del sistema operativo potrebbero essere misure adeguate per determinati trattamenti, ma non per altri, oppure in determinate organizzazioni, ma non in altre, in ogni caso lo potrebbero essere oggi, ma non domani quando il progresso tecnologico (anche degli hacker e di coloro che minacciano i nostri dati) potrebbe renderle insufficienti.

Lasciando per il momento stare gli impatti che il nuovo Regolamento UE sulla privacy potrà avere per i colossi del web, quali Facebook, Google, ecc., è opportuno osservare che per le piccole e medie imprese italiane dovrà cambiare l'approccio

alla privacy, soprattutto per quelle organizzazioni che trattano dati sensibili o giudiziari. Occorrerà un cambio di mentalità: non serve più un po' di carte (informative, consensi, lettere di incarico, …) ed alcune misure minime di sicurezza specifiche (password, antivirus,…) per garantire il rispetto della legge. Poiché molti imprenditori vedono la privacy solo come un disturbo da gestire soltanto per non incorrere in sanzioni e, quindi, come una pratica da sbrigare nel modo più indolore possibile, ecco che il passaggio al nuovo Regolamento – che dovrà avvenire nei prossimi due anni – non sarò proprio una passeggiata.

Le responsabilità in capo al responsabile del trattamento (ex titolare del trattamento) sono maggiori e comunque più impegnative da gestire, soprattutto laddove il trattamento di dati venga delegato a fornitori (es. consulenti del lavoro, consulenti fiscali e legali, strutture esterne, ecc.) che dovranno inevitabilmente essere tenuti sotto controllo.

Non è che taluni principi fossero assenti dalla normativa italiana del 2003, ma – complice la crisi e le semplificazioni adottate da precedenti governi, soprattutto l'abolizione del DPS – hanno un po' sminuito l'importanza della privacy in azienda, anche perché – si sa come siamo fatti noi italiani – senza sanzioni esemplari non ci preoccupiamo di nulla… e sono stati molto rare le sanzioni comminate alle aziende, anche perché i controlli sono stati molto poco frequenti.

Paradossalmente ha spaventato di più la disposizione sui *cookie* perché la sua mancata applicazione è di fatto pubblica, mentre altre regole di fatto trascurate rimangono tra le muar delle organizzazioni di ogni dimensione.

L'indeterminatezza di alcune regole potrà essere colmata da disposizioni specifiche dei singoli Stati membri e/o da linee guida di settori specifici che potranno agevolare l'interpretazione della legge.

Ora la privacy sarà meno materia per avvocati – se non per la stesura di contratti che regolamentano i rapporti fra clienti e fornitori anche in materia di trattamento dati personali – e più materia per **esperti della sicurezza delle informazioni**. Infatti l'approccio del nuovo Regolamento Europeo sulla Privacy si avvicina, *mutatis mutandis*, a quello della norma UNI EN ISO/IEC ISO 27001 e della linea guida UNI EN ISO/IEC 27002.

L'adozione del nuovo Regolamento UE sarà, pertanto, più impegnativa per piccole organizzazioni che trattano molti dati c.d. sensibili o giudiziari, quali organizzazioni private nel campo della sanità (cliniche ed ambulatori privati, farmacie, …), studi di consulenza del lavoro, infortunistiche, studi legali, studi di consulenza fiscale, ecc., piuttosto che per aziende che trattano come unici dati sensibili i dati relativi ai propri dipendenti. Anzi saranno proprio queste ultime che dovranno pretendere da società e studi di consulenza esterna adeguate garanzie

per il trattamento dei dati di cui sono responsabili.

Il “cookie” non è un biscotto

In questi giorni entra in vigore un provvedimento del Garante Privacy (si veda http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3118884) relativo alla necessità di informare gli utenti di ogni sito web il cui proprietario risiede in Italia – ed a raccogliere il relativo consenso in determinati casi – dell’utilizzo dei c.d. cookies da parte del sito stesso.

Il termine per l’adeguamento dei siti web è un anno dalla pubblicazione in Gazzetta Ufficiale del suddetto provvedimento, avvenuta il 03/06/2014.

Si ricorda che l’uso dei cookie rientra tra i trattamenti soggetti all’obbligo di notificazione al Garante ai sensi dell’art. 37, comma 1, lett. d), del Codice, laddove lo stesso sia finalizzato a “*definire il profilo o la personalità dell’interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l’utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti*“, ma da tale obbligo sono esclusi – sulla base di quanto previsto dal provvedimento del Garante del 31 marzo 2004, che ha inserito espressamente, tra i trattamenti esonerati dal suindicato obbligo – quelli “*relativi all’utilizzo di marcatori elettronici o di dispositivi analoghi installati, oppure memorizzati temporaneamente, e non persistenti, presso l’apparecchiatura terminale di un utente, consistenti nella sola trasmissione di identificativi di sessione in conformità alla disciplina applicabile, all’esclusivo fine di agevolare l’accesso ai contenuti di un sito Internet*“.

Da ciò, pertanto, emerge che, mentre i **cookie di profilazione**, i quali hanno caratteristiche di permanenza nel tempo, **sono soggetti all’obbligo di notificazione**, i cookie che invece hanno finalità diverse e che rientrano nella categoria dei **cookie tecnici**, ai quali sono assimilabili anche i ***cookie analytics***, **non debbono essere notificati al Garante**.

Resta però l’obbligo di **informativa breve**, tramite *banner* nella *home page* del sito e

in altre pagine, oltre che di **informativa estesa** facilmente reperibile nel sito stesso, anche tramite apposito link nel banner suddetto, relativamente all'uso dei cookie fatto dal sito web stesso.

Il mancato rispetto di tale provvedimento può comportare una sanzione da 6.000 a 36.000 euro e questo sta spaventando molto le organizzazioni che dispongono di un sito web, anche se con l'utilizzo di cookie minimale, spesso solo per raccogliere statistiche aggregate sulla consultazione del proprio sito. Questo non tanto perché è l'unico elemento di apparente non conformità al Codice della Privacy in molte organizzazioni, se non altro perché è un provvedimento recente, ma perché – a differenza di altri requisiti privacy per i quali sono previsti meccanismi sanzionatori equivalenti – in questo caso i tecnici dell'Ufficio del Garante Privacy possono verificare la presenza e la correttezza dell'informativa via internet, stando comodamente seduti alle loro scrivanie.

Dunque le imprese, **buona parte delle quali presentano altri aspetti di non conformità alla privacy**, non temono la poco probabile (viste anche le statistiche delle ispezioni effettuate nell'ultimo anno) ispezione del Nucleo Privacy della Guardia di Finanza, ma la più agevole verifica a campione sul proprio sito internet, disponibile pubblicamente e teoricamente soggetto anche a segnalazioni al Garante da parte di terzi senza troppa fatica.

In realtà i c.d. cookie di profilazione ("*I cookie di profilazione sono volti a creare profili relativi all'utente e vengono utilizzati al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dallo stesso nell'ambito della navigazione in rete*") sono quelli più insidiosi, sui quali il Garante richiede azioni di maggior tutela da parte dei gestori dei siti web (obbligo di informativa con consenso, notifica, ecc.), ma solo pochi siti ne fanno realmente uso.

Il problema, però, sta nella gestione inappropriata della privacy da parte di molte PMI, che non hanno il pieno controllo dei loro siti web (solo sito pubblicitario, vengono raccolte statistiche sulla consultazione, viene realizzato un servizio di e-commerce?).

Si tenga presente che è facile trovare risorse nel web (ad es. http://www.whois.com/whois/) in grado di scoprire a chi appartiene un determinato dominio, con tanto di ragione sociale o nome e cognome di una persona fisica. Così molti legittimi proprietari hanno demandato a società esterne la gestione del proprio sito, in alcuni casi abbandonandolo al suo destino, dimenticando, però, che ne restano responsabili di fronte alla legge.

Dunque non sapere "cosa fa il proprio sito web" è un rischio non trascurabile e può comportare responsabilità legali, oltre al fatto che è uno strumento di comunicazione e di marketing importantissimo che spesso andrebbe gestito meglio.

Maggiori informazioni su questi cookie, per evitare che diventino biscotti

indigesti, si possono trovare in questo video
https://www.youtube.com/watch?v=Mut-YXSExnw&feature=youtu.be

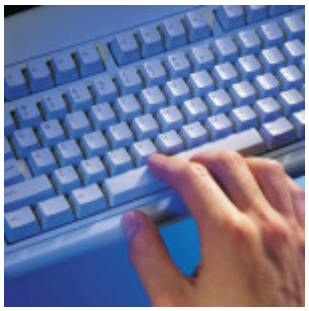
Ed a questi link

http://www.garanteprivacy.it/cookie

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3167231

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2142939

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 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 sì 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

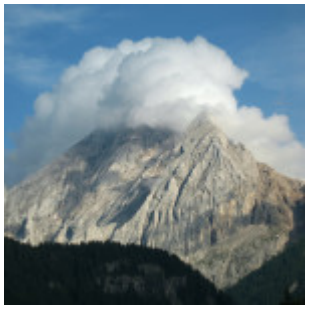
dell'evento.

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

---

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.

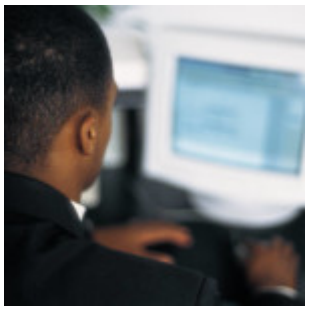
In linea generale parlare di dati poco sicuri nel *cloud* perché si teme che qualcuno possa "guardarci dentro" non ha molto senso: a parte che bisognerebbe valutare quale livello di sicurezza ci si aspetta per ogni tipo di dato (si veda il precedente articolo sulla valutazione dei rischi per la sicurezza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

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**.