La norma UNI 11697:2017 e la figura del DPO

Lo scorso dicembre – dopo lunghe discussioni – è stata pubblicata la norma UNI 11697:2017 "Attività professionali non regolamentate – Profili professionali relativi al trattamento e alla protezione dei dati personali – Requisiti di conoscenza, abilità e competenza", inerente la definizione dei requisiti relativi all'attività professionale dei soggetti operanti nell'ambito del trattamento e della protezione dei dati personali (compreso il DPO), da questi esercitata a diversi livelli organizzativi (pubblico o privato).

L'UNI dichiara che "*La norma definisce i profili professionali relativi al trattamento e alla protezione dei dati personali coerentemente con le definizioni fornite dall'EQF e utilizzando gli strumenti messi a disposizione dalla UNI 11621-1 Attività professionali non regolamentate – Profili professionali per l'ICT – Parte 1: Metodologia per la costruzione di profili professionali basati sul sistema e-CF*".

La norma, anche dopo la sua uscita, è stata fonte di animate discussioni fra gli esperti del settore e, soprattutto, è stata vivacemente contestata da chi ritiene che non esponga in modo chiaro e preciso i requisiti professionali delle figure in oggetto oppure definisca delle figure professionali favorevoli a certi profili piuttosto che altri.

Le figure professionali delineate dalla norma UNI sono le seguenti:

1. **Data Protection Officer** (DPO), figura di supporto al titolare o responsabile del trattamento nell'applicazione e per l'osservanza del Regolamento (UE) 2016/679, in conformità all' art. 37 (Designazione del Responsabile della protezione dei dati), art. 38 (Posizione del Responsabile della protezione dei dati) e art. 39 (Compiti del Responsabile della protezione dei dati).
2. **Manager Privacy**, figura che assiste il titolare nelle attività di coordinamento di tutti i soggetti che – nell'organizzazione – sono coinvolti nel trattamento di dati personali (responsabili, incaricati, amministratori di sistema, ecc.), garantendo il rispetto delle norme in materia di privacy e il mantenimento di un adeguato livello di protezione dei dati personali.
3. **Specialista Privacy**, figura di supporto appositamente formato (è richiesta una formazione minima di 24 ore), che collabora con il Manager Privacy e cura la corretta attuazione del trattamento dei dati personali all'interno dell'organizzazione, svolgendo le attività operative che, di volta in volta, si rendono necessarie durante tutto il ciclo di vita di un trattamento di dati personali.

4. **Valutatore Privacy**, figura dotata di una apposita formazione (minima di 40 ore) che si caratterizza per la sua terzietà sia nei confronti del Manager che dello Specialista Privacy; egli esercita una attività di monitoraggio (audit) andando ad esaminare periodicamente il trattamento dei dati personali e valutando il rispetto delle normative di settore emanate.

Concentriamoci sulla figura del DPO o RPD. La norma definisce una **descrizione sintetica** del profilo, una **missione**, dei **risultati attesi**, dei **compiti principali**, delle **competenze,** delle **abilità e delle conoscenze.**

Per ognuna delle competenze assegnate seguenti è definito un livello di competenza:

- Pianificazione di Prodotto o di Servizio
- Sviluppo della Strategia per la Sicurezza Informatica
- Gestione del Contratto
- Sviluppo del Personale
- Gestione del Rischio
- Gestione delle Relazioni
- Gestione della Sicurezza dell'Informazione
- Governante dei sistemi informativi

Tra le **Abilità** (Skill) stabilite che deve possedere il DPO si segnalano:

- Contribuire alla strategia per il trattamento e per la protezione dei dati personali
- Capacità di analisi
- Capacità organizzative
- Pianificazione e programmazione
- Saper analizzare gli asset critici dell'azienda ed identificare debolezze e vulnerabilità riguardo ad intrusioni o attacchi
- Saper anticipare i cambiamenti richiesti alla strategia aziendale dell'information security e formulare nuovi piani
- Saper applicare gli standard, le best practice e i requisiti legali più rilevanti all'information security
- Garantire che la proprietà intellettuale (IPR) e le norme della privacy siano rispettate
- egoziare termini e condizioni del contratto
- Preparare i template per pubblicazioni condivise
- Progettare e documentare i processi dell'analisi e della gestione del rischio
- Essere in grado di seguire e controllare l'uso effettivo degli standard documentativi aziendali

Invece tra le **Conoscenze** (Knowledge) possedute dal DPO vi sono:

- I principi di privacy e protezione dei dati by design e by default I diritti degli interessati previsti da leggi e regolamenti vigenti Le responsabilità

connesse al trattamento dei dati personali
- Norme di legge italiane ed europee in materia di trattamento e di protezione dei dati personali
- Norme di legge in materia di trasferimento di dati personali all'estero e circolazione dei dati personali extra UE
- Le metodologie di valutazione d'impatto sulla protezione dei dati e PIA
- Le norme tecniche ISO/IEC per la gestione dei dati personali
- Le tecniche crittografiche
- Le tecniche di anonimizzazione
- Le tecniche di pseudonimizzazione
- Sistemi e tecniche di monitoraggio e "reporting"
- Gli strumenti di controllo della versione per la produzione di documentazione
- I rischi critici per la gestione della sicurezza
- I tipici KPI (key performance indicators)
- Il ritorno dell'investimento comparato all'annullamento del rischio
- la computer forensics (analisi criminologica di sistemi informativi)
- La politica di gestione della sicurezza nelle aziende e delle sue implicazioni con gli impegni verso i clienti, i fornitori e i sub-contraenti
- Le best practice (metodologie) e gli standard nella analisi del rischio
- Le best practice e gli standard nella gestione della sicurezza delle informazioni
- Le norme legali applicabili ai contratti
- Le nuove tecnologie emergenti (per esempio sistemi distribuiti, modelli di virtualizzazione, sistemi di mobilità, data sets)
- Le possibili minacce alla sicurezza
- Le problematiche legate alla dimensione dei data sets (per esempio big data)
- Le problematiche relative ai dati non strutturati (per esempio data analytics)
- Le tecniche di attacco informatico e le contromisure per evitarli

Fra le competenze richieste determinate dalla norma emergono profili afferenti a:

- Consulenti direzione
- Consulenti ed esperti di sistemi di gestione della sicurezza delle informazioni (famiglia delle norme ISO 27000)
- Auditor di sistemi di gestione
- Esperti di Risk Management
- Consulenti/esperti sulle normative attinenti alla privacy ed alla protezione dei dati personali (leggi, normative, disposizioni del Garante, ecc.)

Inoltre sono richieste conoscenze legali sulla contrattualistica, competenze sulla sicurezza informatica (tecniche di attacco, crittografia, ecc.) e sui sistemi informatici e relativi database.

Pur con le dovute precisazioni relative al fatto che il candidato DPO dovrà ricoprire un ruolo le cui caratteristiche dipendono fortemente dall'organizzazione in cui dovrà andare a operare, è evidente che prevalgono le competenze gestionali/manageriali e quelle relative alla sicurezza delle informazioni, piuttosto che quelle legali. Per quanto possa essere contestata, la norma chiaramente individua soggetti più vicini all'ingegnere dell'informazione che all'esperto legale come possibile DPO/RPD. Sicuramente le competenze legali eventualmente mancanti a un profilo molto vicino all'ingegnere dell'informazione sono più facilmente colmabili, anche attraverso consulenze specifiche, rispetto ad altre situazioni in cui il potenziale DPO si trova a dover colmare il gap di competenza relativo ai sistemi di gestione della sicurezza delle informazione, al risk management, alle basi di dati e magari anche alla *cybersecurity*.

Sicuramenteci sono in giro illustri avvocati esperti di *info security* e *data protection*, magari anche consulenti ed auditor ISO 27001, ma tutti coloro che si propongono per il ruolo di DPO con competenze essenzialmente giurisprudenziali saranno adatti a ricoprire il ruolo di DPO?

Naturalmente queste considerazioni valgono se si pensa di affidare il ruolo di DPO ad un'unica figura, con l'eventuale supporto di un team di esperti nelle varie discipline.

Chiaramente ogni organizzazione o ente pubblico che vorrà selezionare il proprio DPO potrà decidere come meglio crede in base ai compiti e le caratteristiche identificate per il DPO dal Regolamento UE 679/2016, ma la norma UNI 11697, volontaria, dice questo.

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 (564 download) (compreso l'allegato con le FAQ)
- Linee Guida Valutazione-Impatto WP 248 (300 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.

La sicurezza delle informazioni in caso di calamità naturali e non naturali

In caso di catastrofi e calamità naturali quali terremoti, alluvioni, inondazioni, incendi, eruzioni vulcaniche, uragani oppure atti terroristici, uno dei danni collaterali dopo la perdita di vite umane e i danni materiali ad edifici ed infrastrutture, occorre considerare il blocco dei sistemi informativi che può rallentare notevolmente la ripresa delle normali attività.

Le metodologie da impiegare per prevenire e mitigar i danni che possono compromettere la ripresa delle attività dopo un evento catastrofico riguardano la tematica della business continuity (continuità operativa).

Nell'intervento presentato lo scorso 17/11 al Convegno EVENTI SISMICI: PREVENZIONE, PROTEZIONE, SICUREZZA, EMERGENZA, le cui slide sonono scaricabili in questa pagina, si sono presentate tutte le attività da porre in essere per controllare tali situazioni indesiderate, in particolare sono stati trattati i seguenti argomenti:

- business continuitymanagement
- normative ISO 22301, ISO 2001/27002 e ISO 27031 per la gestione della business continuity, con particolare riferimento ai sistemi informatici
- gestione dei rischi per la continuità operativa
- disaster recovery
- obiettivi ed indicatori di business continuity
- business continuity plan (piano di continuità operativa).

La sicurezza dei dati in caso di terremoto (214 download)

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.

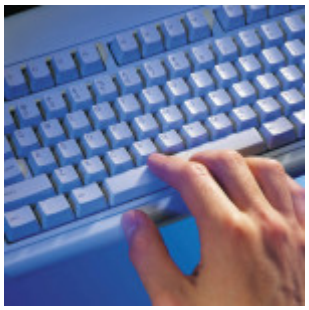
L'indeterminatezza di alcune regole potrà essere colmata da disposizioni specifiche dei singoli Stati membri e/o da linee guida di settori specifici che potranno agevolare l'interpretazione della legge.

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.

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*.

Business Continuity Plan, questo sconosciuto

Il BCP (*Business Continuity Plan*) o **Piano di Continuità Operativa** è un documento richiesto alle **organizzazioni certificate ISO 27001** (*Sistema di gestione per la sicurezza delle informazioni* – Requisiti) al controllo A.17.1 "Continuità della sicurezza delle informazioni", ma anche – e soprattutto – dalla norma specifica UNI EN ISO 22301:2014 – *Sicurezza della società – Sistemi di gestione della continuità operativa – Requisiti*, che abbiamo trattato in un precedente articolo.

Gli eventi delle ultime settimane, ma anche degli ultimi anni, hanno mostrato quanto scarsa sia l'adozione di questo strumento nel nostro Paese. Molti sono, infatti, gli esempi di situazioni critiche – essenzialmente causate da disastri naturali – che non sono state fronteggiate nel modo corretto e che hanno portato a costi sociali elevatissimi che si sono scaricati inevitabilmente sulla collettività:

- Il terremoto dell'Aquila e dell'Emilia;
- Le alluvioni in Liguria ed in Toscana;
- Le interruzioni di energia elettrica protrattesi nel tempo a Cortina qualche Natale fa e, più recentemente, in Emilia dopo una forte nevicata;
- Le forti nevicate verificatesi in Emilia-Romagna nel 2012.

In tutte queste situazioni di emergenza, oltre ai danni materiali ed alle perdite di vite umane, si sono verificate disfunzioni e ritardi nella **ripresa dell'operatività ordinaria**. Il vantaggio di avere predisposto un buon piano di continuità operativo è proprio questo: ipotizzando una situazione di crisi si cerca di **limitare i danni** e di **tornare all'operatività normale nel più breve tempo possibile**.

Tornando ad aspetti più tecnici, mentre la **ISO 27001** tratta la continuità operativa in termini di sicurezza delle informazioni, ovvero di garantire il ritorno alla piena disponibilità delle informazioni senza perdite significative delle stesse, la **ISO 22301** amplia il raggio di azione del *business continuity plan*, comprendendo la gestione delle discontinuità di un servizio, non necessariamente legato alla disponibilità di informazioni su supporto cartaceo o elettronico (anche se oggi ben poche attività possono farne a meno). Alcuni esempi possono chiarire meglio il concetto:

- La gestione di un ospedale a fronte di grandi epidemie che riducono anche la disponibilità di risorse umane sufficienti ad affrontare l'emergenza;
- Un servizio di trasporto di persone o beni in caso di calamità naturali;
- Un servizio di pronto intervento di manutenzione in caso di calamità naturali che impediscono al personale di recarsi al lavoro;
- Un servizio di ristorazione collettiva in caso di calamità naturali o epidemie influenzali che impediscono al personale di recarsi al lavoro;
- E così via.

Si ricorda che la **continuità operativa** è l'insieme di attività volte a minimizzare gli effetti distruttivi, o comunque dannosi, di un evento che ha colpito un'organizzazione o parte di essa, garantendo la continuità delle attività in generale.

La sfera di interesse della continuità operativa va oltre il solo ambito informatico, interessando l'intera funzionalità di un'organizzazione (Azienda, Ente

Pubblico, ecc.) ed è, pertanto, assimilabile all'espressione "*business continuity*".

La continuità operativa comprende sia gli aspetti strettamente organizzativi, logistici e comunicativi che permettono la prosecuzione delle funzionalità di un'organizzazione, sia la continuità tecnologica, che riguarda l'infrastruttura informatica e telecomunicativa (ICT) ed è nota come "*disaster recovery*" (DR). Pertanto, le soluzioni per garantire la continuità dei servizi non considerano soltanto le componenti tecnologiche utilizzate, ma anche tutte le altre risorse (personale, impianti, infrastrutture, ecc.).

Le analisi, valutazioni e scelte di trattamento del rischio richieste dalla gestione della continuità operativa sono le seguenti:

- Identificazione dei rischi;
- Analisi e valutazione dei rischi;
- Analisi delle conseguenze di disastri, malfunzionamenti, interruzioni di servizi (*Business Impact Analysis*);
- Realizzazione di piani (controlli) affinché i processi di business siano riattivati entro il tempo richiesto.

Le analisi valutano per ogni *asset* (o gruppo di *asset*) critico il tempo che tale *asset* può rimanere indisponibile con danno basso o nullo. I piani (*Business Continuity Plan*) devono essere mantenuti costantemente aggiornati per essere efficaci al momento del bisogno.

Per meglio comprendere la predisposizione di un BCP occorre introdurre alcune definizioni basilari:

- **Mission Critical Activity** (MCA): attività critica o di supporto al business relativamente ai servizi o prodotti offerti dall'organizzazione (internamente o esternamente), incluse le sue correlazioni con altri processi e *single points of failure*, che permettono all'organizzazione di raggiungere i suoi obiettivi di business considerando le stagionalità e/o tempi di rilascio critici
- **Business Impact Analysis** (BIA): analisi gestionale attraverso la quale un'organizzazione valuta quantitativamente (per esempio finanziariamente, *Service Level Agreement*, SLA) e qualitativamente (per esempio reputazione, leggi, regolamenti) gli impatti e le perdite che possono risultare se l'organizzazione subisce un grave incidente, e il minimo livello di risorse necessarie per il ripristino.
- **Maximum Tollerance DownTime** (MTDT): massimo intervallo di tempo ammissibile di interruzione del servizio (*quante ore posso permettermi di non erogare il servizio ai clienti?*).
- **Maximum Tollerance Data Loss** (MTDL): massima perdita di dati tollerata (*quanti dati posso permettermi di perdere?*).
- **RTO** (*Recovery Time Objective*): periodo di tempo entro il quale devono essere ripristinati un minimo livello di servizio, i sistemi di supporto e le

funzionalità principali dopo un'interruzione dei servizi. Normalmente è il lasso di tempo entro il quale cui le MCA devono essere ripristinate.
- **RPO** (Recovery Point Objective): istante (punto) nel tempo al quale i dati sono coerenti e possono essere ripristinati.
- **MBCO** (*Minimum Business Continuity Objective*): livello di servizio minimo accettabile dall'organizzazione per raggiungere i propri obiettivi di business durante una rottura.

Il processo di gestione della continuità operativa deve prendere in esame tutti i processi e le attività aziendali e classificarli in funzione della loro criticità nel modo seguente:

1. Attività critiche per il business (MCA's);
2. Attività importanti;
3. Attività secondarie.

Per le **attività critiche** vengono stabiliti degli **obiettivi di continuità operativa** in termini di MTDT, MTDL, RTO, RPO, MBCO e stabiliti dei **piani di continuità operativa**, che comprendono le contromisure messe in campo per garantire gli obiettivi.

Per la pianificazione delle attività di continuità operativa è necessario valutare preliminarmente gli impatti degli eventi che possono causare interruzioni dei processi di business, predisponendo una BIA.

A seguito della **valutazione dei rischi di interruzione del servizio** erogato ai clienti devono essere predisposti, attuati e periodicamente verificati uno o più **Piani di Continuità Operativa** (*Business Continuity Plan*) aventi lo scopo di mantenere o ripristinare il funzionamento dei processi critici ed assicurare la disponibilità delle informazioni necessarie a garantire un **livello di servizio accettabile**, a fronte del verificarsi dei rischi di interruzioni o malfunzionamenti precedentemente identificati e valutati.

Dunque se pensiamo ad un servizio di pubblica utilità (servizi ospedalieri, trasporto pubblico, mense scolastiche, servizi di pulizia e raccolta rifiuti, ecc.) occorre definire due livelli:

- Un primo livello che identifica il ripristino di un servizio minimo dopo l'interruzione;
- Un secondo livello che sancisce la ripresa dell'attività ordinaria.

Per ogni livello devono essere stabiliti i tempi entro i quali vengono raggiunti e che possono costituire SLA contrattuali.

È bene comprendere che i BCP devono prefigurare uno **scenario di crisi** ben definito, al verificarsi del quale si vuole reagire in modo adeguato. Chiaramente non tutti

gli scenari possibili possono essere gestiti nei BCP, ma solo quelli **più probabili e di impatto più grave**, sulla base della valutazione dei rischi preliminarmente svolta.

I contenuti dei BCP potrebbero essere i seguenti:

1. Scopo e campo di applicazione
2. Obiettivi
3. Requisiti di business continuity (RPO, RTO,…)
4. Identificazione dei processi critici (MCA's)
5. *Business Impact Analysis*
6. Piano di *Disaster Recovery*
7. Piano di Continuità Operativa, contenente:

   - Rilevazione dell'incidente (metodi e procedure): dichiarazione del disastro o incidente, valutazione del danno, attivazione del piano):
   - Risposta all'incidente (attività, tempi, responsabilità, procedure);
   - Ripristino dell'operatività (attività, tempi, responsabilità, procedure di azione e continuità);
   - Risorse (personale e competenze, tecnologie, infrastruttura, software, dati, siti alternativi, centri di emergenza o crisi);
   - Fornitori (Lista dei fornitori di *recovery*, dettagli dei contratti, procedure di attivazione);
   - Organizzazione e Responsabilità;
   - Documentazione;
   - Comunicazioni (contatti, soggetti da informare, messaggi);

8. Test del BCP (prove, tempi, responsabilità)
9. Manutenzione del BCP

Si precisa che i BCP possono far riferimento ad altri documenti (ad es. Piani di *Disaster Recovery*), aggiornati autonomamente. In ogni caso deve essere sempre possibile risalire alla configurazione attuale del BCP, ovvero alle revisioni vigenti dei documenti esterni richiamati nel Piano di Continuità Operativa. Tale configurazione e la relativa rintracciabilità dei documenti relativi al BCP deve essere disponibile sia in formato elettronico, sia su supporto cartaceo, con gestione di copie di riserva del BCP disponibili in locali/siti/ubicazioni alternative, al fine di essere sempre disponibili in caso di verificarsi dell'evento che ha generato l'interruzione dei processi critici.

Si rammenta che per la Pubblica Amministrazione la continuità operativa ed i relativi Piani di Business Continuity sono previsti dall'Art. 50 bis del Codice per l'Amministrazione Digitale; essa, pertanto, deve essere gestita dagli responsabili degli Enti Pubblici in modo adeguato, con riferimento agli standard internazionali sulla materia.

[Download non trovato]

La certificazione SSAE 16 per i servizi in outsourcing

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

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

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

Per le aziende soggette a tale standard la **Sezione 404 del Sarbanes-Oxley Act (SOX)** richiede che i fornitori di servizi in outsourcing siano provvisti di una particolare certificazione, il **Report SSAE 16**, per **garantire che controlli e processi interni siano appropriati alla gestione delle informazioni dei propri clienti**.

La crescente richiesta di **servizi in outsourcing** pone, quindi, l'esigenza da parte delle organizzazioni che forniscono servizi in outsourcing delle tipologie sopra elencate (payroll, contabilità, gestione documentale, …) di fornire ai propri

clienti e ad altri soggetti un rapporto di revisione completo sui sistemi di controllo e sui processi, al fine di assicurare che i servizi erogati alla clientela siano sicuri e conformi a uno standard riconosciuto.

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

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

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

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

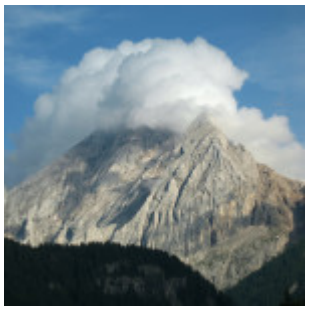
Sebbene questo schema SSAE 16 ricalchi per alcuni elementi la certificazione ISO 9001 e la certificazione ISO 27001, esso presenta una valenza particolare in determinati settori e costituisce il logico completamente in un percorso di miglioramento e di qualificazione dell'organizzazione di servizi nei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

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

- Servizi di gestione paghe del personale
- Acquisizione dati e documenti in formato digitale

- Conservazione sostitutiva
- Servizi contabili e fiscali
- Servizi di assistenza e sviluppo software.

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



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

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

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

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

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

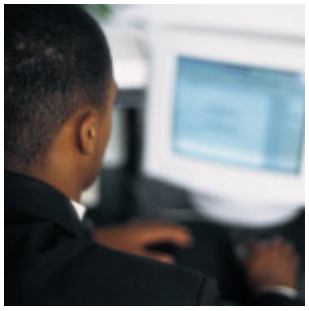
In una logica di *Risk Assessment*, naturalmente, ogni impresa fa storia a se; bisogna conoscere quali dati vorrebbe mettere sul cloud, qual è il livello di riservatezz**a** che tali dati devono avere, se si tratta di dati sensibili, quali **procedure di backup** sono implementate, di che tipo di **connessione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

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

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

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

Infine la **privacy**, ovvero la **protezione dei dati personali** con la relativa legge italiana (D.Lgs 196/2003) ed il **nuovo Regolamento Europeo** che sarà emanato probabilmente il prossimo anno. In questo ambito un Parere della Commissione Europea del 2012 ha per il momento fugato molti dubbi sulle garanzie legali che un'impresa dovrebbe richiedere al proprio fornitore di servizi cloud per essere tranquilla di non incorrere in pesanti problemi legali.



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

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

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

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

Oggi esistono molti sistemi per garantirsi un futuro tranquillo con i dati nel *cloud*, ad esempio seguendo i principi ed i metodi indicati dalle **norme della famiglia ISO 27000** (ISO 27001 che riporta i requisiti di un **sistema di gestione della sicurezza delle informazioni** certificabile, ISO 27002 che riporta le *best practices*, ovvero i controlli che possono essere messi in atto, ISO 27005 che è la linea guida per il *risk assessment*, …) includendovi i requisiti cogenti per la

privacy in vigore in Italia ed in Europa. Se il problema di mantenere una certa continuità operativa costituisce un fattore critico si può adottare la metodologia esposta nella ISO 22301 ed in altri standard e linee guida sull'argomento.

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

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

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

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

Una metodologia di valutazione dei rischi per la sicurezza delle informazioni

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

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

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

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

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

1) Identificazione dei rischi

2) Analisi e ponderazione dei rischi

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

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

5) Accettazione dei rischi residui.

Le attività suddette vengono descritte nel **Rapporto di valutazione dei rischi** (*Risk*

assessment report).

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

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

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

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

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

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

Impatto = Valore Asset x Gravità Minaccia x Gravità Vulnerabilità.

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

a) La valutazione della probabilità che si verifichino i singoli rischi identificati nella fase precedente. La probabilità di accadimento di un rischio avviene considerando gli **incidenti** verificatisi in passato e statistiche eventualmente disponibili. L'assegnazione di una livello di probabilità attraverso una scala qualitativa avviene secondo il seguente schema:

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

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

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

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

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

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

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

I controlli vengono ritenuti applicabili o non applicabili, se applicabili possono essere attuati in modo completo o parziale. L'applicazione dei controlli può infatti

essere ritenuta conveniente solo su alcuni processi/attività, in funzione della diversa esposizione al rischio che possiedono le varie attività svolte dall'organizzazione.

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

Il piano di trattamento dei rischi riporta le seguenti informazioni:

1) Elenco dei rischi da trattare;

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

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

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

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

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

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

Gli asset possono essere delle seguenti tipologie:

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

3. *Risorse Umane*: dipendenti, collaboratori esterni e consulenti.

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

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

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

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

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

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

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