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.

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 (136 download) (compreso l'allegato con le FAQ)
- Linee Guida Valutazione-Impatto WP 248 (185 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.

Opportunità per le imprese con il Piano Industria 4.0

In questi mesi si sente parlare molto delle agevolazioni fiscali per le imprese relative al Piano Industry 4.0, promosso già dal Governo Renzi in autunno 2016. Cerchiamo, in questo articolo, di capire meglio quali sono le reali opportunità per le imprese ed i vincoli che la Legge pone per usufruire degli incentivi, anche per capire in quali situazioni conviene realmente investire in questa direzione, al fine di non trovarsi brutte sorprese ad investimenti effettuati.

Il focus del Piano Industria 4.0 è il **settore manifatturiero**, esso punta alla **digitalizzazione** delle imprese produttrici, anche se non sono completamente escluse le aziende di servizi. Il fine del Governo è quello di **incrementare gli investimenti nelle imprese**, che al momento latitano e vedono il nostro Paese indietro rispetto al

resto d’Europa. La carenza di investimenti è molto probabilmente la principale causa della crescita bassa (in termini di “zero virgola”…) dell’Industria del nostro Paese, soprattutto se paragonata agli altri Paesi industrializzati dell’Europa.

Perché Industria 4.0? La prima rivoluzione industriale è avvenuta alla fine del 18° secolo con l’introduzione di potenza vapore per il funzionamento degli stabilimenti produttivi, la seconda rivoluzione industriale si colloca all’inizio del 20° secolo con l’introduzione dell’elettricità, dei prodotti chimici e del petrolio; la terza rivoluzione industriale è iniziata all’inizio degli anni ’70 con l’utilizzo dell’elettronica e dell’IT per automatizzare ulteriormente la produzione (robot industriali e computer). Ora, invece, nella quarta rivoluzione industriale, il concetto fondamentale è la **connessione con un sistema di raccolta e gestione dei dati**, collegamento a internet, IoT o Internet delle Cose (utilizzo di macchine intelligenti, interconnesse e collegate ad internet) ed altro ancora.

L’elemento caratterizzante del piano di incentivazione, dunque, è la connessione, fra diversi dispositivi (macchina-elaboratore, macchina-macchina, macchina-internet, macchina-dispositivo mobile, ecc.).

Le **tecnologie coinvolte** nel piano Industry 4.0 sono le seguenti:

1. *Advanced Manufacturing Solutions* (Robot collaborativi interconnessi e rapidamente programmabili).
2. *Additive manufacturing* (Stampanti in 3D connesse a software di sviluppo digitali).
3. *Augmented Reality* (Realtà aumentata a supporto dei processi produttivi).
4. *Simulation* (Simulazione tra macchine interconnesse per ottimizzare i processi).
5. *Horizontal/Vertical Integration* (Integrazione informazioni lungo la catena del valore dal fornitore al consumatore).
6. *Industrial Internet* (Comunicazione multidirezionale tra processi produttivi e prodotti)
7. *Cloud* (Gestione di elevate quantità di dati su sistemi aperti).
8. *Cyber- security* (Sicurezza durante le operazioni in rete e su sistemi aperti).
9. *Big Data and Analytics* (Analisi di un’ampia base dati per ottimizzare prodotti e processi produttivi).

Evidentemente l’elenco è disomogeneo, ma in ogni caso indica alle imprese quali sono le tecnologie abilitanti per usufruire delle agevolazioni.

Fra le voci più significative vi è l’integrazione orizzontale e verticale.

L’**integrazione verticale** va dall’acquisizione di dati a livello produttivo, attraverso sensori, all’elaborazione dati tramite software gestionali: è l’integrazione che parte dal MES (*Manufacturing Execution System*) al sistema di Controllo di Gestione.

Sono diverse le soluzioni di **integrazione orizzontale**, ad esempio possono passare attraverso la connessione con il fornitore per migliorare la *supply chain* comprendendo soluzioni per la collaborazione, il *planning*, l’*order management*, il *tracking* per la logistica, il *data analytics* e molto altro ancora.

Nel piano Industria 4.0 le **principali incognite** per le imprese possono essere così riepilogate:

- il rapporto costi/benefici dell’intervento;
- la mancanza di competenze digitali interne;
- la portata degli investimenti, che comunque rappresentano un costo che, ricordiamolo, viene finanziato solo se l’impresa è in utile;
- la carenza di standard digitali;
- l’incertezza sulla sicurezza dei dati (ad esempio nel caso della connessione attraverso *Internet of Things* e il *Cloud Computing*).

Su quest’ultimo punto il Piano Industria 4.0 ha pensato di introdurre il capitolo della Sicurezza delle Informazioni, anche relativamente ai dati gestiti in ambito IoT.

Per capire meglio il significato e la portata di tali incognite occorre precisare che – per chi ancora non lo sapesse – le agevolazioni sono costituite dall’**iper-ammortamento** (250% del valore del bene) e dal **super-ammortamento** (140% del valore del bene), che si applicano, nel primo caso, ai beni materiali acquistati, nel secondo anche ai beni immateriali.

L’elenco dei beni materiali e immateriali a cui è applicabile il super e iper ammortamento è stato ufficialmente pubblicato dal Ministero dello Sviluppo Economico (MISE) ed è scaricabile in allegato al presente articolo insieme alle **linee guida del MISE** stesso per l’applicazione delle agevolazioni.

Occorre precisare che per rientrare nel Piano Industria 4.0 ed usufruire degli incentivi occorre **acquisire almeno un bene materiale rientrante nell’elenco**, ovvero acquisire strumentazione atta a trasformare un’apparecchiatura/macchina preesistente in un “bene Industria 4.0” (caso del *revamping* di macchinari). In altre parole per poter usufruire del super ammortamento per l’acquisto di un bene immateriale, ad

esempio un software, rientrante nelle categorie previste dalla Legge, occorre che **il soggetto beneficiario del finanziamento acquisti anche un bene materiale**; non è richiesto il collegamento fra bene materiale e beni immateriali acquistati per usufruire dell'agevolazione! Ad esempio, al limite un'impresa potrebbe acquistare un sistema di sensori per acquisire dati da una macchina produttiva (ad esempio temperature da un forno) ed applicare il super ammortamento all'acquisto di un sistema MES o *big data analytics* che non trattano i dati rilevati dalla macchina 4.0.

Tra i vincoli per poter usufruire dell'agevolazione vi è che l'investimento deve avvenire entro il 31/12/2017, con almeno un ordine ed un anticipo del 20% pagato entro il 31/12/2017 e con consegna del bene entro 30/06/2018. La **perizia giurata** di un ingegnere iscritto all'Albo o di un perito industriale è necessaria per investimenti superiori a 500.000 € per il singolo bene, negli altri casi è sufficiente una autodichiarazione del Legale Rappresentante dell'impresa.

È evidente che il fattore tempo gioca un ruolo fondamentale nella decisione ed effettuazione di investimenti che, soprattutto nel caso di PMI, normalmente richiedono una valutazione abbastanza lunga ed incerta. Visto poi che la Legge non è di chiarissima interpretazione (si attende in questo mese una Circolare interpretativa dell'Agenzia delle Entrate su molti aspetti ambigui), alcune imprese rischiano di effettuare investimenti che poi non risulteranno ammissibili, magari trascinati dalle indicazioni di venditori di macchine e apparecchiature. Al proposito va ricordato che l'autodichiarazione del Legale Rappresentante ha risvolti penali in caso di non ammissibilità del bene; dunque esiste la concreta possibilità che molte aziende **richiedano comunque la perizia giurata di un ingegnere abilitato** per garantire il vertice aziendale contro brutte sorprese (costo non iper-ammortizzabile e dichiarazione mendace). Buona prassi sarebbe rivolgersi, prima di effettuare l'investimento, ad un consulente che possa indirizzare l'azienda ed il management non competente nelle tecnologie da acquisire e verso investimenti che, non solo siano ammissibili agli incentivi Industria 4.0, ma che **risultino realmente utili per l'azienda** nel medio-lungo periodo.

Fra i principali fattori inibitori nell'adottare le tecnologie incluse nel piano Industria 4.0 vi è sicuramente la scarsa cultura digitale delle PMI italiane e una mancanza di *leadership digitale* del management della PMI stessa.

Tra i processi che potrebbero trarre maggior vantaggio dall'implementazione di misure Industry 4.0 spiccano sicuramente le tematiche di **pianificazione, schedulazione e controllo avanzamento della produzione** e lo **sviluppo del prodotto/industrializzazione**.

Il Piano Industria 4.0 è un percorso di trasformazione, non solo tecnologico, ma anche organizzativo e gestionale. Il fine dell'impresa deve essere l'incremento del valore per il cliente, anche attraverso il miglioramento dell'efficienza aziendale, la fornitura di soluzioni innovative, la proposta di servizi innovativi e

migliorativi rispetto allo standard.

Per iniziare un progetto di Industria 4.0 è importante effettuare una valutazione iniziale finalizzata all'obiettivo Industry 4.0 per capire **di cosa l'azienda realmente bisogno**, quali sono gli elementi di possibile **miglioramento** e le **opportunità** da poter cogliere, ma anche dei rischi connessi agli investimenti.

Si ribadisce che i benefici per beni materiali e immateriali devono essere connessi attraverso il soggetto beneficiario, non direttamente fra gli *asset* fisici e immateriali, ma chiaramente un piano Industry 4.0 coerente dovrà prendere in considerazione l'interconnessione fra gli uni e gli altri, solo così facendo si otterrà il massimo nel miglioramento dell'efficienza dei processi aziendali.

Si ricorda che il software deve essere incluso nell'allegato B per poter rientrare nell'incentivo, mentre per i software c.d. "*embedded*" prevale il riferimento al bene iper-ammortizzabile nel quale è contenuto. Tale bene deve appartenere ai beni dell'allegato A alla Legge.

Infine non è ancora chiaro quali costi accessori (consulenza finalizzata all'utilizzo del bene) siano iper e super ammortizzabili, al proposito si attende la Circolare di chiarimento dell'Agenzia delle Entrate.

Linea Guida MISE Industria 4.0 (72 download)

Beni ammissibili Piano Industria 4.0 (70 download)

Articolo 1 commi da 8 a 13 della legge 11 dicembre 2016 n 232 - Proroga con modificazioni della disciplina del c.d. super ammortamento e introduzione del c.d. iper ammortamento (58 download)

RPO e RTO: come progettare il disaster recovery

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

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

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

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

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

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

Supponiamo che una piccola organizzazione che opera nel settore dei servizi, denominata ALFA srl, decida di effettuare un **backup incrementale** dei propri dati con frequenza giornaliera su un NAS interno, mantenendo le ultime 7 versioni dei dati e che poi, per cautelarsi a fronte di eventuali catastrofi naturali che potrebbero rendere inutilizzabile il sistema informatico aziendale e tutti i backup salvati su NAS, effettui anche un **backup completo** su nastri DAT con cadenza settimanale. I nastri magnetici dell'ultimo backup settimanale sono conservati a casa del titolare, a 20 km di distanza dalla sede dell'azienda, il quale quando si porta via il backup restituisce quello della settimana precedente.

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

Occorre distinguere fra diversi tipi di problemi (disastro):

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

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

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

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

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

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

una infrastruttura tecnologica in *cloud*.

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

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 (145 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.

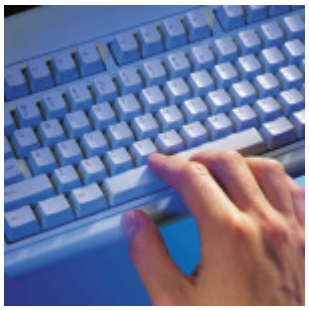
L'indeterminatezza di alcune regole potrà essere colmata da disposizioni specifiche dei singoli Stati membri e/o da linee guida di settori specifici che potranno agevolare l'interpretazione della legge.

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*.

La nuova edizione della norma ISO 27002 (prima parte)

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

Struttura della norma

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

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

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

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

La descrizione dei controlli sono strutturate come segue:

- Controllo: definisce nello specifico il controllo funzionale alla soddisfazione dell'obiettivo di controllo.
- Guida attuativa: fornisce informazioni più dettagliate per supportare l'attuazione del controllo. La guida può risultare completamente attinente o sufficiente a tutte le situazioni oppure potrebbe non soddisfare i requisiti specifici di controllo dell'organizzazione.
- Altre informazioni: fornisce informazioni aggiuntive che potrebbe essere necessario considerare, per esempio considerazioni legali e riferimenti ad altre norme. Nel caso non vi siano informazioni aggiuntive da considerare questa parte non è riportata nel testo.

Elenco dei controlli

I punti di controllo definiti dalla norma sono i seguenti:

5 POLITICHE PER LA SICUREZZA DELLE INFORMAZIONI

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

6 Organizzazione della sicurezza delle informazioni

In questa sezione sono definiti le seguenti categorie principali:

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

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

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

7 Sicurezza delle risorse umane

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

- **Prima dell'impiego (7.1)**: in due controlli vengono esposte tutte le cautele da intraprendere al momento dell'assunzione di una persona o dell'incarico ad un collaboratore esterno, non solo accordi di riservatezza e clausole contrattuali sul futuro rapporto lavorativo, ma anche – per quanto reso possibile dalla legislazione applicabile – un'accurata indagine conoscitiva sul passato,

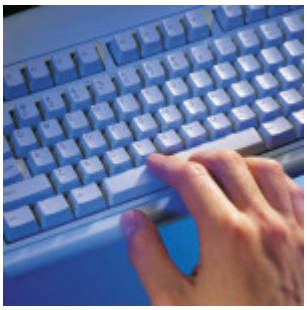
lavorativo e non, del futuro dipendente/collaboratore.
- **Durante l'impiego (7.2)**: nel corso della normale attività lavorativa viene data enfasi all'applicazione delle procedure stabilite e le responsabilità della Direzione nell'applicazione delle stesse, alla formazione-addestramento e sensibilizzazione del personale ed al ricorso ad eventuali processi disciplinari. Dunque regole da rispettare, ma anche motivazione ed incentivazione del personale, oltre che sanzioni a chi infrange le regole.
- **Cessazione e variazione del rapporto di lavoro (7.3)**: vengono presi in esame tutti gli aspetti e le attività da svolgere quando si chiude un rapporto di lavoro o avviene un'assegnazione ad altro incarico, come ad esempio il prolungamento della validità degli accordi di riservatezza, i passaggi di consegne e la comunicazione all'altro personale interessato della cessazione del rapporto di lavoro.

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

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

8 Gestione degli asset

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



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

trasporto, ecc.).

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

9 Controllo degli accessi

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

- **Requisiti di business per il controllo degli accessi (9.1)**: occorre definire una politica di controllo degli accessi basata sull'accesso alle sole informazioni necessarie per svolgere il proprio lavoro (come impone anche la normativa sulla privacy in vigore in Italia) e regolamentare l'accesso alle reti (soprattutto evitare l'uso incontrollato delle reti wi-fi senza autenticazione utente).
- **Gestione degli accessi degli utenti (9.2)**: è necessario regolamentare il processo di registrazione (tramite credenziali di autenticazione univoche) e de-registrazione degli utenti, la fornitura delle credenziali di accesso (*provisioning*), la gestione degli accessi privilegiati (ad es. quelli in qualità di "amministratore di sistema", cfr. apposita disposizione del Garante della Privacy), la gestione delle informazioni segrete per l'autenticazione (password, smartcard, ecc.), il riesame periodico dei diritti di accesso, la rimozione degli stessi al termine del rapporto (o la revisione in caso di cambio mansioni).
- **Responsabilità dell'utente (9.3)**: è importante regolamentare ed istruire il personale sull'uso della password.
- **Controllo degli accessi ai sistemi e alle applicazioni (9.4)**: è opportuno limitare l'accesso alle informazioni, predisporre procedure di log-on sicure, procedure di gestione delle password, limitare l'impiego di programmi di utilità privilegiati, limitare gli accessi al codice sorgente dei programmi.

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

accesso,…) spesso non vengono implementate.

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

10 Crittografia

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

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

11 Sicurezza fisica e ambientale

La sezione comprende due categorie:

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

possibile accedere ad informazioni riservate ed occorre definire politiche di "scrivania pulita" per prevenire la visione di informazioni riservate da parte di personale non autorizzato.

fine I parte ….continua…

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);

1. Test del BCP (prove, tempi, responsabilità)
2. 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]