

## DPS e Basilea II Incombenze per ogni azienda

Quanti problemi hanno dato alla vostra azienda le tanto discusse direttive **BASILEA II e il DPS più volte rinviato?**

Alcuni analisti, tra il serio ed il faceto, paragonano il carico di lavoro derivante dalle incombenze relative a questi temi recentemente cadute fra capo e collo degli IT manager con gli aggiornamenti dovuti a suo tempo per il passaggio all'Euro o per il famoso "millenium bug".

Il DPS (Documento Programmatico della Sicurezza) richiede una serie di interventi ai fini di garantire i requisiti minimi aziendali in materia di sicurezza dei dati e protezione della privacy.

*Le direttive BASILEA 2, che sono essenzialmente orientate alla gestione dei rischi operativi e le relative raccomandazioni da parte della Banca d'Italia sono da tempo una fonte di grattacapi anche per le nostre aziende.*

Un dossier Microsoft è dedicato proprio a BASILEA II e ricorda che nel 2007 erano oltre cinque milioni le imprese italiane che, adeguandosi a quella normativa, dovevano predisporre, oltre a tante altre cose, anche un piano che avesse garantito una efficiente procedura di **Disaster Recovery**, peraltro richiesta anche dal DPS (Documento Programmatico della Sicurezza) e dalla certificazione standard ISO 17799 che a sua volta rientra negli standard richiesti per i sistemi informatici.

Vale la pena notare che tutte queste sigle hanno un denominatore comune: richiedono all'IT Manager una grande attenzione al problema della **Business Continuity** e alla prevenzione da eventi straordinari (disaster recovery). Alzi la mano chi almeno una volta, magari nel proprio ufficio, non ha visto svanire di colpo lavori, programmi, documenti vari e quant'altro. Ci sono aziende che hanno subito danni colossali e molte hanno rasentato il fallimento per aver trascurato questi temi.

In genere un precedente disastro, in informatica come per ogni altra cosa, spinge o meglio costringe a premunirsi per il futuro ed a valutare il rischio che corre l'azienda (**risk assessment**).

Per l'Azienda, mantenere costante la propria operatività, la Business Continuità, deve essere un dovere soprattutto in questo periodo di lavoro che scarseggia e con clienti sempre più esigenti.

Parlando con gli IT Manager emerge che non è certo la distrazione e la noncuranza il motivo principale per il quale non si predispongono un piano di Disaster Recovery blindato, ma i costi che non sono mai lievi per la piccola impresa, per cui è necessario trovare un buon compromesso.

E sono appunto i costi che preoccupano chi dovrà omologarsi a BASILEA 2.

**Vediamo come fare una valutazione dei rischi (risk assessment) per un progetto di questo tipo.**

Il modo migliore per giustificare la spesa di business continuity è capire esattamente quanto l'azienda perde durante un blocco dei sistemi, la cosiddetta **business impact analysis**, e confrontarlo con l'investimento necessario a evitare questa perdita.

Le formule possibili possono essere abbastanza semplici.

Calcolata ad esempio la durata media di un blocco dei sistemi, la si moltiplica per il costo orario che l'azienda deve sopportare in casi simili.

Tale costo non deve comprendere solo il salario dei dipendenti che non possono lavorare proprio a causa del blocco, ma anche il fatturato perso e le eventuali penalità per contratti o accordi non rispettati.

***Insomma nella malaugurata ipotesi di un disastro l'investimento per garantire la propria continuità operativa si rivela sempre ben speso (nome in codice di tutto questo ROSI: Return of Security Investment).***

### **DPS: opportunità per il miglioramento**

Il punto è semplice: ogni Paese industriale deve la sua sopravvivenza a una molteplicità di "sistemi nervosi digitali" che a loro volta controllano o fanno funzionare i gangli vitali del sistema (energia, trasporti, banche, informazione, sanità). Se queste reti sofisticate saltano, perché strutturalmente insicure o mal protette, si possono verificare eventi negativi a catena (come il black-out elettrico del 28 settembre 2003) con conseguenze anche piuttosto gravi.

Si pensi a sistemi come quelli degli aeroporti, delle torri di controllo, dei radiofari; alle linee ferroviarie ad alta velocità sincronizzate da sofisticati sistemi di segnalazione. **L'intera sicurezza di un Paese è oggi legata alla robustezza, a prova di disastro, dei sistemi digitali di comunicazione, sia tra esseri umani sia tra dispositivi e macchine, sia dentro il loro software.**

Tuttavia l'attenzione collettiva è quasi sempre rivolta solo a ciò che è indispensabile, al minimo, come se la sicurezza fosse ingombrante, una imposizione e non un mezzo per tutelare il patrimonio informativo dell'impresa. Non tutelando i dati da accessi indesiderati, mantenendoli integri, esatti, disponibili quando richiesti, l'azienda si espone a diversi rischi; **è principalmente la mancanza di copie di sicurezza a provocare danni irreversibili quando si è vittima di un attacco.** Anche i documenti Word possono contenere tracce imbarazzanti delle revisioni precedenti e che l'indirizzo e-mail del mittente è falsificabile con estrema facilità, quindi diffondere una "catena di Sant'Antonio" dal posto di lavoro a propria insaputa diventa un danno di immagine per l'azienda ma anche una potenziale responsabilità nei confronti della legislazione vigente in materia di tutela dei dati personali e del loro trattamento.

**Alle imprese che fanno largo uso di dispositivi mobili, laddove è proprio necessario portare "fuori" dall'azienda i dati sensibili, è consigliabile di utilizzare sistemi per cifrarli e renderli inutilizzabili a chi ne venisse in possesso in maniera illegale o accidentale.** La sicurezza influenza, quindi, la qualità dei processi aziendali e i servizi erogati e incide anche sulla sua immagine e sulla sua reputazione. È perciò un tratto distintivo della cultura organizzativa di ogni impresa. Inoltre, la soddisfazione dei bisogni di sicurezza e riservatezza condiziona la fiducia dei consumatori che è alla base della propensione ad accettare le innovazioni.

**La linea generale è quella di proteggersi da Internet, come se tutti i mali venissero dalla grande rete mondiale,** in verità, da diversi studi, emerge che la maggior parte degli attacchi o dei ricatti connessi a furto di dati, provengono dall'interno dell'organizzazione che ne è vittima. Un impiegato corrotto, magari da una azienda concorrente, può distruggere o sottrarre dati strategici, arrecando un danno irrimediabile, o sottoponendo l'azienda a ricatto economico. Questo purtroppo è inevitabile, chi conosce il sistema, sa come funzione, come abbatterlo, come indebolirlo. **Un buon consulente per la sicurezza è comunque in grado di indicare ai responsabili dell'azienda le "best practices" adeguate per ovviare anche a questi pericoli, difficilmente arginabili dall'antivirus di turno a 100 euro**

tutto compreso o dalla scatola magica quasi munita di intelligenza autonoma che comunemente si ritiene sia il firewall.

Sul fronte sicurezza è altrettanto importante anche possedere un piano per il **disaster recovery**, cioè le procedure da adottare nel caso di perdita parziale o totale di dati o compromissione del sistema informativo (esteso anche a quello che apparentemente non è un computer, come appunto telefonia VoIP o sistemi di telecontrollo). Da una ricerca internazionale condotta da Dynamic Markets emerge poco più del 10% dei manager intervistati ammette di essere coinvolto nel processo di sviluppo delle strategie di disaster recovery e che sono circa l'85% le aziende che hanno subito, nel corso dell'ultimo anno, un fermo imprevisto ai sistemi informativi.

*La ricerca mostra che nonostante il numero delle aziende che sviluppano piani di disaster recovery cresca di anno in anno, la mancanza di manutenzione programmata è una carenza allarmante: il 57% revisiona i piani di disaster recovery solo con cadenza annuale o meno, mentre un allarmante 6% non esegue mai alcuna revisione.*

In Italia, principalmente per mancanza di tempo e di fondi, e in misura inferiore perché un collaudo provoca potenziali disagi per i dipendenti, le procedure di tutela dei sistemi informativi non vengono tenute nella dovuta considerazione. Alcune aziende si dichiarano impegnate in progetti di analisi per mettere in sicurezza i sistemi informativi, altre non prendono in considerazione nemmeno semplici applicativi che permettono di proteggere i dati sui computer portatili o effettuare la copia periodica dei dati. Nonostante il ruolo chiave che la protezione dei dati riveste per il business di qualsiasi azienda, le decisioni relative ai piani di disaster recovery, di Documento Programmatico sulla Sicurezza, e in generale di sicurezza informatica, sono ancora oggi, nell'85% delle realtà italiane, esclusivo appannaggio dei responsabili IT. I vertici aziendali non risultano essere coinvolti (interessati) in queste scelte.

**L'opportunità di miglioramento è quindi l'obbligo, per molte imprese che trattano dati personali, di predisporre ogni anno un documento programmatico sulla sicurezza, basato sull'analisi dei rischi che incombono sui dati, sull'individuazione delle contromisure da adottare per ridurli al minimo e, per chi è tenuto, sul fatto di riferire o di avere compilato o aggiornato il documento, nella relazione accompagnatoria del bilancio di esercizio.**

### **Vediamo Il Documento programmatico della Sicurezza:**

Il Dlgs. 196/2003 (anche noto come Codice sulla Privacy) è entrato in vigore il 01/01/2004. Raccoglie in un Testo Unico le precedenti Leggi, Decreti e Codici Deontologici in tema di Privacy. Le Aziende che trattino dati personali, di fatto tutte le Aziende, devono trattare tali dati in conformità al Codice stesso.

**Per essere conformi, le aziende devono agire su tre fronti:**

1. pianificare misure organizzative, amministrative e tecniche di sicurezza attraverso un documento formale conosciuto come Documento Programmatico sulla Sicurezza;
2. **adeguarsi alle misure tecniche minime di sicurezza** definite nell'allegato B del Dlgs. 196/2003;
3. dare informativa trasparente e completa (se e quando dovuta) dei trattamenti dei dati personali ai relativi interessati.

Trattare dati personali in non-conformità con la Legge, espone l'azienda sul piano civile e penale con sanzioni amministrative **fino a 90.000 Euro** (fatti comunque salvi i risarcimenti eventualmente dovuti in sede civile) e può esporre i suoi dirigenti ed il suo Legale Rappresentante a sanzioni penali fino a **tre** anni di detenzione.

Il primo e più significativo passo verso la conformità è la stesura del “Documento Programmatico sulla Sicurezza” -- un documento che descrive i trattamenti di dati personali trattati in Azienda, l'organizzazione di sicurezza dell'Azienda e analizza i rischi che incombono sui dati personali. Si tratta di un'analisi strutturata dei dati personali trattati in Azienda, dell'organizzazione della sicurezza dei dati e delle misure in essere e da pianificare per mettere e mantenere in sicurezza i dati. Da questo documento derivano tutte le altre azioni richieste dal Dlgs.196/2003: misure minime, informative, lettere d'incarico al personale preposto ai trattamenti.

**I dati personali** sono quelli che identificano una persona FISICA o GIURIDICA. Pertanto tutte le Aziende trattano dati personali, anche solo per il fatto di gestire un archivio cartaceo od informatico dei Clienti/utenti o altri archivi che contengano i dati identificativi di persone o aziende (fascicoli del personale, elenco negozi, albo delle associazioni, ruoli tributari ...).

**I dati personali sensibili** sono quelli che indicano o “sono idonei” a rivelare, fra gli altri, dati personali quali le idee religiose, politiche e filosofiche, lo stato di salute o la vita sessuale, l'origine razziale ed etnica. La questione non è ovvia. Solo un'analisi attenta dei trattamenti effettuati nella VS Ditta può rilevare se trattiamo o meno “dati sensibili”, che dovranno essere trattati con maggiore cautela rispetto ai dati personali non sensibili. Infatti, anche dati apparentemente innocui possono rivelarsi “idonei” a fornire dati personali sensibili. Per esempio: la foto degli stranieri sul permesso di soggiorno (quando non sia già sufficiente il nome!), permette di capire l'origine razziale.

**L'art. 34, comma 1 del D. Lgs 196/2003 obbliga il Titolare del trattamento di dati personali effettuato con strumenti elettronici alla tenuta di un Documento aggiornato in materia di sicurezza dei dati, oltre che ad adottare una serie di misure “minime” di sicurezza.**

Il Documento Programmatico sulla Sicurezza (DPS) va riveduto ogni anno entro il 31 Marzo e della sua adozione o revisione **il Titolare riferisce nella relazione accompagnatoria del bilancio d'esercizio.**

Pur esplicitando il Codice l'obbligo di adottare il DPS solo in presenza di trattamenti effettuati con strumenti elettronici, **il Disciplinare Tecnico in materia di misure di sicurezza (Allegato B al D.Lgs 196/2003) richiede che tra i contenuti del DPS (art. 19) vi siano non solo informazioni che riguardano le procedure di tipo “informatico” sui trattamenti effettuati ma anche una serie di informazioni riconducibili alla struttura dell'ente (ambiente fisico e responsabilità dei soggetti), alla formazione rivolta al personale, alle garanzie in caso di trattamenti di dati affidati all'esterno della struttura.**

**Nel Documento allegato non sono quindi presenti alcuni contenuti espressamente previsti dall'art. 19 del Disciplinare Tecnico (Allegato B al D. Lgs 196/2003).**

Ritengo doveroso segnalare che tale Documento costituisce pertanto solo parte del DPS, così come previsto dalla legge.

**A completamento del DPS dovrebbe infatti essere previsto:**

- un censimento dei trattamenti di dati sensibili e giudiziari effettuati presso la VS Ditta;
- una rilevazione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- la previsione degli interventi formativi degli incaricati del trattamento;
- la descrizione dei criteri da adottare per i trattamenti di dati affidati all'esterno (pertanto preceduta da un'analisi dei soggetti esterni preposti al trattamento di dati della Vs. Ditta)
- Un'analisi delle condizioni fisiche degli ambienti e delle attrezzature (arredi) contenenti dati riferiti a trattamenti effettuati senza l'ausilio di strumenti elettronici, ricordando che non esistono solo banche dati automatizzate ma anche solo cartacee (archivio corrente e storico, faldoni, pratiche esclusivamente cartacee).

*Servizi di Consulenza per la Sicurezza e la Privacy - GFC*