MODELLO DI ORGANIZZAZIONE DELLE AZIENDE DI TLC, PER RISPONDERE ALLE RICHIESTE DELL'AUTORITÀ GIUDIZIARIA

di Giovanni Nazzaro

Tutte le grandi aziende private hanno un'organizzazione tale da consentire di affidare un preciso compito ad una ben assegnata funzione aziendale. Il modello adottato da queste aziende non solo risponde ad un preciso obbligo di normativa[1], che nella pratica è necessario per prevenire predeterminati reati e per applicare la giusta contromisura, ma risponde alle due esigenze di efficienza nella risposta e di proattività verso i Clienti, i quali possono essere interni all'azienda, nel qual caso saranno rappresentati da un'altra funzione aziendale, oppure esterni.
Il concetto di Cliente interno ed esterno all'azienda è funzionale alla struttura dei processi aziendali: una volta definito l'oggetto sociale si definiscono i processi aziendali che portano ad ottenere tale risultato. **Ogni processo aziendale ha un *input* ed un *output*, costituito da risorse trasformate da ogni singola attività che compone il processo stesso**. Un volta elencati i processi primari (verso Clienti esterni) e processi secondari (verso Clienti interni), applicando il principio di separazione dei ruoli, distinguendo tra ruoli di tipo direzionale, gestionale e operativo si arriva alla definizione dell'organizzazione.

Per le aziende di telecomunicazioni il Cliente primario è l'utilizzatore del servizio offerto, chiamato abbonato. Non meno importante di quest'ultimo ci sono altri Clienti primari, nell'eccezione di interlocutore esterno, non interessati propriamente alla fruizione del servizio di telecomunicazioni ma all'ottenimento di specifiche conferme nell'applicazione delle norme e delle leggi. Uno di questi è l'Autorità Giudiziaria; benché la terminologia possa sembrare forte, l'Autorità Giudiziaria (AG) è di fatto è un Cliente primario per un'azienda di telecomunicazioni, nell'eccezione ovvia di interlocutore esterno, perché le sue richieste devono essere trasformate in *input* per i processi aziendali sopra menzionati.

Cercando di definire il contesto di riferimento, tra l'altro facilmente desumibile confrontando le strutture d'azienda esposte sui propri siti *web* da diverse aziende di telecomunicazioni italiane e straniere, **l'organizzazione tipo prevede una suddivisione in almeno le seguenti funzioni d'azienda: Marketing, Affari istituzionali e Legali, Amministrazione/Finanza e Controllo, Security, Technology, Risorse Umane**. Tralasciando l'importanza di ognuna di queste, rivolgiamo la nostra attenzione alla funzione di Security, a cui spetterebbe la gestione della sicurezza e l'assunzione di responsabilità sotto tale profilo, la prevenzione dei rischi non di tipo competitivo, il contrasto di iniziative aggressive e la definizione delle azioni necessarie al ripristino dei servizi danneggiati. **All'interno della funzione di Security o della funzione Affari Legali dovrebbe essere allocata la funzione d'azienda (di seguito Funzione) che gestisce le richieste dell'AG**, che in termini pratici possono consistere nell'attivazione delle intercettazione dei servizi di telecomunicazione, la fornitura dei tabulati delle comunicazioni effettuate nel passato, l'identificazione degli abbonati, ecc. La specificità della richiesta dipende dai servizi offerti dall'azienda come ad esempio quelli di telefonia fissa o mobile, di accesso alla rete Internet, di *email* oppure di *hosting* di domini *web*.

Un primo aspetto fondamentale per la costituzione del gruppo di risorse umane che dovranno comporre tale funzione è **l'individuazione di soggetti che abbiamo competenze non solo su leggi e norme vigenti nel paese in cui opera l'azienda, ma anche tecniche**. Generalmente le richieste dell'AG vengono evase mediante accesso a sistemi informativi che operativamente eseguono quanto richiesto. Tuttavia possono essere frequenti richieste che richiedono un'analisi più approfondita e quindi, superata la fase di verifica dell'autenticità e validità della richiesta dell'AG, poi questa deve essere opportunamente e tecnicamente tradotta per i riferimenti interni all'azienda a cui le informazioni di tipo giudiziario non possono essere trasmesse. Occorre infatti considerare che un altro requisito che concorre alla necessità di avere una tale funzione nelle aziende di telecomunicazioni è quella di predeterminare le risorse umane che tratteranno i dati classificati giudiziari[2]. Per quanto attiene invece la numerosità, abbiamo esempi di funzioni aziendali[3] costituite da circa una decina di risorse, in alcuni casi si arriva anche al centinaio in funzione anche della grandezza dell'azienda.

Generalmente si potrebbe ritenere che le attività descritte, di esecuzione delle richieste tramite sistemi informativi opportunamente predisposti e, in casi alternativi, di analisi tecnico-legali effettuate in ausilio con altre funzioni d'azienda, costituisca la parte predominante del lavoro svolto da tale gruppo. Sotto tale profilo la Funzione che risponde per conto dell'azienda alle richieste dell'AG potrebbe apparire una sorta di *front end* o *front office*, oppure una zona di confine interna all'azienda che, in funzione della specificità della richiesta, sappia tradurre opportunamente la domanda in un *input* per il processo aziendale di riferimento. Dal punto di vista quantitativo questa interpretazione potrebbe corrispondere al vero, considerando ad esempio i numeri dichiarati dagli operatori USA in termini di richieste ricevute delle Autorità competenti[4]. **Dal punto di vista qualitativo, l'attività più importante è invece costituita dal presidio di tale Funzione sui tavoli interni all'azienda in cui sono concepiti i nuovi servizi di telecomunicazioni**, affinché possano essere fornite alle altre funzioni d'azienda le indicazioni necessarie perché la catena di produzione di tali servizi contenga già quelle funzionalità che servono a soddisfare le richieste dell'AG.

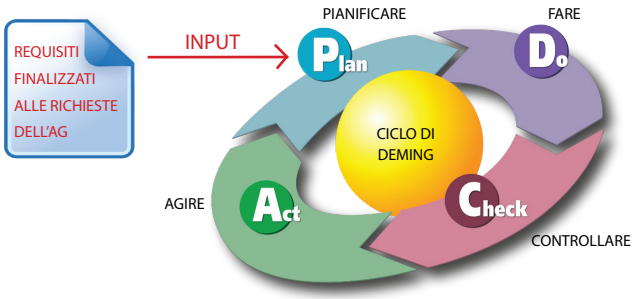
Il momento in cui intervenire per definire ed inserire le predette funzionalità nel contesto di produzione dei servizi costituisce un aspetto fondamentale. **L'intervento deve essere fatto a priori per due ragioni**. Supponendo che i sistemi che erogano un certo servizio siano stati già prodotti ed il servizio sia già commercializzabile ai Clienti finali, un intervento postumo per inserire determinate funzionalità, ad esempio quelle di intercettazione o di tracciamento delle comunicazioni richieste dall'AG, per l'Azienda rappresenterebbe un onere economicamente più impegnativo rispetto al caso in cui tali sistemi siano stati già disegnati e prodotti con incorporate le funzionalità a supporto delle richieste dell'AG (che sono dette quindi *embedded*). In tale ipotesi, inoltre, si violerebbe il principio, spesso formalizzato in specifiche leggi nazionali, secondo cui **se un servizio è reso pubblico allora occorre dare all'AG la possibilità di supervisionare le comunicazioni sin dal momento in cui avviene la prima comunicazione di quel genere**. Sotto questo profilo costituisce un requisito di legge per l'Azienda.

Allora vediamo come si potrebbe concretizzare il presidio di tale Funzione sui tavoli interni all'Azienda, per consentire di rispettare le ragioni sopra esposte. In qualunque ambito produttivo, un progetto prima di essere realizzato viene pesato mediante il classico rapporto dei Costi/Benefici. Sintetizzando gli aspetti principali della sua realizzazione, ai fini del nostro ragionamento possiamo affermare che anche per i servizi di telecomunicazioni esiste un'analisi preventiva di tale genere a cui partecipano inizialmente le funzioni di Marketing e quelle di Technology, quest'ultima è quella che generalmente rappresenta i Costi di realizzazione nei quali rientrano anche i costi necessari alla securizzazione[5] del servizio che può essere presidiata dal processo per il *Risk Management*[6]. Una volta approvato il progetto si passa alla definizione delle clausole del contratto che potrà essere rivolto al *partner* tecnologico piuttosto che all'utilizzatore finale, coinvolgendo altre funzioni d'Azienda.

La figura in alto mostra l'attività eseguita dalla funzione di gestione delle richieste dell'AG, effettuata trasversalmente al ciclo di produzione del Servizio che è composto dalle seguenti fasi:

1. ***Concecpt/Analysis***, nel quale il Servizio è inizialmente abbozzato e analizzato dalla funzione di Marketing e il contributo della Funzione è dato dalla rappresentazione dei requisiti generali per l'implementazione delle funzionalità sollecitate dall'AG e dalla definizione delle clausole contrattuali a copertura di quest'ultime;
2. ***Project***, nel quale il Servizio è progettato e sono concordati i dettagli implementativi;
3. ***Design***, nel quale il Servizio è realizzato e non è direttamente richiesto alcun contributo alla Funzione;
4. ***Testing***, nel quale si collauda il servizio e le funzionalità a copertura di quanto potrebbe richiedere l'AG;
5. ***Release***, nel quale il Servizio è rilasciato e commercializzabile.

La fase in cui sono raccolti i requisiti generali per le funzionalità che l'AG potrebbe richiedere per uno specifico Servizio, nella loro forma di dettaglio tecnico d'implementazione, **dovrebbero essere raccolti e formalizzati verso il processo aziendale di *Risk Management*** che, in accordo all'impostazione della norma ISO 27001, prevede tra i controlli per la certificazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) appunto la *compliance* ai requisiti di legge[8], ma anche il rispetto delle clausole contrattuali. La figura seguente mostra l'interazione tra il contributo della Funzione ed il ciclo di Deming che definisce il processo di controllo e miglioramento continuo del SGSI.



Tra le due ultime fasi del processo d'industrializzazione del Servizio, a valle dell'esito positivo della fase di *testing*, tale Funzione dovrebbe produrre un documento a carattere confidenziale, da destinare all'AG, in cui è descritto il Servizio e quali novità introduce rispetto alla situazione contingente. Tale comunicazione risulta non necessaria qualora il Servizio non produca alcun elemento di novità sia nelle modalità di richiesta sia nelle informazioni ricevute dall'AG. ©

NOTE

1. D.Lgs 231/01 - Responsabilità amministrativa delle società e modelli di organizzazione, gestione e controllo
2. In Italia la classificazione, la definizione ed il trattamento dei dati giudiziari sono contenuti nel Dlgs. 196/2003.
3. Cfr. "I LISTINI DEGLI OPERATORI MOBILI AMERICANI PER LE RICHIESTE DELLE FORZE DELL'ORDINE" di G. Nazzaro su "Sicurezza e Giustizia" n. III/MMXII pagg.39-41
4. Vedi nota 2.
5. È questa la traduzione italiana ormai convenzionalmente accettata del termine inglese securitization. È frequente anche la versione "sicurizzazione".
6. Il "risk management", letteralmente "gestione del rischio", è il processo mediante il quale si misura o si stima il rischio e successivamente si sviluppano delle strategie per governarlo. In generale tale processo condivide l'impostazione dello standard ISO/IEC 27001:2005.
7. Cfr. COBIT Control Objective PO9.6 - Maintenance and Monitoring of a Risk Action Plan is contained within Process Assess and Manage IT Risks.
8. ISO/IEC 27001:2005 - Controls and Objectives - A.15.1 Compliance with legal requirements
9. Cfr. http://it.wikipedia.org/wiki/Ciclo_di_Deming ◊