IV Workshop dei docenti e ricercatori di Organizzazione Aziendale - Paper

I PROCESSI DECISIONALI PER LA GESTIONE DEL RISCHIO INFORMATIVO NELLE AZIENDE ITALIANE

Autori

Roberto Palmieri – **roberto.palmieri@uni-bocconi.it**

Matteo Marzotto – **matteo.marzotto@sdabocconi.it**

Università Commerciale Luigi Bocconi

Istituto di Organizzazione e Sistemi Informativi

Milano

1. INTRODUZIONE

Il valore della conoscenza maturata in contesti aziendali e i processi decisionali posti in essere per assicurare la sua protezione rappresentano il focus di questo articolo. L'obiettivo è quello di mostrare come le modalità di generazione e diffusione della conoscenza impongano un ripensamento dei processi di Information Security, al fine di considerarne gli aspetti organizzativi, oltre a quelli tecnologici tradizionalmente trattati dall'informatica. A tale scopo, dopo un breve cenno alle teorie sulla creazione e diffusione della conoscenza, ci si avvarrà di un modello per la pianificazione dei sistemi informativi orientati alla sicurezza per interpretare i risultati di una ricerca empirica effettuata su un campione di aziende italiane.

2. IL VALORE DELLA CONOSCENZA

"Immaginate che la vostra azienda sia improvvisamente colpita da un disastro che cancelli tutta la conoscenza presente al suo interno dai supporti su cui è memorizzata, incluse le menti degli impiegati. La differenza tra il valore di mercato dell'azienda prima e dopo il disastro, rappresenta il valore del capitale intellettuale dell'azienda".

Nonostante il suo approccio decisamente catastrofista e provocatorio, con questa affermazione Touraj Nasseri (Nasseri, 1996) ha il merito di mettere bene in evidenza il valore economico che il capitale intellettuale riveste all'interno dell'azienda moderna. Per capitale intellettuale, si intende qui la combinazione tra capitale umano e conoscenza esplicita. Il capitale umano è costituito dal talento individuale e dalla conoscenza accumulata dai singoli componenti dell'organizzazione durante la propria educazione, la formazione professionale e l'esperienza; la conoscenza esplicita è invece rappresentata dalla conoscenza documentata sottoforma di ricerche, resoconti, libri articoli, manoscritti, brevetti o software. La conoscenza esplicita, vale a dire quella che può essere considerata come asset non volatile dell'azienda, è quindi costituita da quella

parte della conoscenza individuale che viene in qualche modo formalizzata e resa disponibile a tutti i componenti dell'organizzazione che ne sono interessati. L'interazione e l'integrazione tra le due componenti del capitale intellettuale dell'azienda, il capitale umano e la conoscenza esplicita, rappresentano un aspetto essenziale da perseguire per la massimizzazione del profitto e il raggiungimento del successo competitivo. Anche le risorse fisiche, che costituiscono il capitale materiale delle aziende, infatti, devono molto del loro valore al capitale intellettuale, che ne determina le modalità di acquisizione, destinazione e impiego. In molti casi, la reale competitività di un'azienda, non si evince tanto dalle sue registrazioni contabili, o dagli altalenanti andamenti delle quotazioni di borsa, quanto dalla valutazione del capitale intellettuale (Strassmann, 1999). Per più del 90% delle aziende questo capitale è superiore rispetto a quello finanziario (il cosiddetto "book value"), mostrato dai bilanci redatti con le tecniche di contabilità tradizionale. Le tecniche contabili tradizionali del valore, del resto, faticano a misurare il valore della conoscenza, in quanto essa risiede principalmente nel comportamento delle persone[i]. Negli ultimi anni il filone di studi sul Knowledge Management ha reso più diffusa la consapevolezza dell'importanza di valutare puntualmente il capitale intellettuale distribuito in azienda, e questa maggiore tensione rispetto agli elementi più intangibili dell'asset aziendale è entrata a far parte delle priorità di manager, analisti finanziari, azionisti e portatori di interessi più in generale[ii]. Giusto per fornire un esempio dell'entità del fenomeno cui si fa riferimento, si riporta in tabella 2.1 il risultato di un progetto di misurazione del capitale intellettuale presso la società farmaceutica statunitense Abbott Laboratories (Strassmann, 1999).

Tabella 2.1 Valutazione del capitale intellettuale presso la società farmaceutica "Abott Laboratories" – Fonte: (Strassmann, 1999)

Abbott Labs: The Value of Knowledge

(in thousands)	Net Income	Financial Capital	Interest Rate	Knowledge Capital
1991	$1,088,745	$3,202,987	9.54%	$8,209,434
1992	$1,239,057	$3,347,641	5.16%	$20,665,092
1993	$1,399,126	$3,674,929	4.72%	$25,967,571
1994	$1,516,683	$4,049,400	4.69%	$28,289,257
1995	$1,688,700	$4,396,847	4.68%	$31,686,486
1996	$1,882,033	$4,820,182	4.12%	$40,860,231
1997	$2,094,462	$4,998,677	4.95%	$37,313,687
1998	$2,333,231	$5,713,661	5.16%	$39,503,994

Da tale tabella risulta evidente come il capitale intellettuale possa in alcuni casi superare di gran lunga il capitale finanziario misurato con le tradizionali tecniche contabili. Questo importante cambiamento di paradigma nella definizione del valore aziendale, ha aperto la strada a un nuovo modo di considerare la sicurezza dei sistemi informativi. In particolare, la prospettiva si è spostata dalla protezione fisica dei supporti informatici sui quali è stoccata l'informazione, al concetto più ampio e articolato di tutela della conoscenza e del patrimonio intellettuale aziendale. Questa nuova concezione di Information Security, senz'altro ispirata dal succitato orientamento alla valorizzazione degli elementi intangibili del patrimonio aziendale, è frutto della consapevolezza che difficilmente il danno derivante da un incidente riguardante i sistemi informativi è riconducibile a cause esclusivamente di natura tecnologica. In realtà, realizzare un sistema di Information Security significa gestire una combinazione tra il rischio indotto dalla tecnologia e quello derivante dal comportamento delle persone. La vera sfida di chi è responsabile dell'Information Security aziendale, dunque, è quella di definire in che modo proteggere la ricchezza incorporata nella conoscenza. La scelta, la predisposizione e l'implementazione delle misure di sicurezza non possono quindi

prescindere dalla valutazione del capitale intellettuale e dall'attenta analisi dei processi mediante i quali la conoscenza stessa viene generata, esplicitata e diffusa. A tal proposito risulta utile richiamare, anche se brevemente, il concetto di "diffusione della conoscenza", che aiuterà nel seguito a descrivere come i nuovi paradigmi legati alla conoscenza impongano l'adozione di una prospettiva organizzativa nella definizione del processo decisionale inerente l'Information Security. Prendere in considerazione questo genere di dinamiche, oltre a rendere più efficaci le misure di sicurezza poste in essere, contribuisce inoltre a spiegare e rendere giustificabili i crescenti budget dedicati all'Information Security.

2.1. Diffusione della conoscenza e valore

Il concetto di *personal knowledge*, e quello strettamente correlato di conoscenza tacita, sono stati proposti per la prima volta nel campo della filosofia della scienza da Polany (Polany 1967), che pone la sua attenzione sull'evidenza che "noi conosciamo più di quello che possiamo esprimere". Il significato di questa affermazione è che esiste un livello della conoscenza umana che non può essere sempre e immediatamente resa con le parole. In quest'ottica, le conoscenze accumulate in un sistema cognitivo, anche se inespresse, costituiscono uno schema implicito che orienta le decisioni degli individui. L'incidenza della conoscenza tacita sui comportamenti individuali all'interno delle organizzazioni, è rintracciabile anche nella teoria evolutiva dell'impresa. In tale filone, Winter (Winter 1987) concentra la propria attenzione sul concetto di conoscenza come asset aziendale, analizzando in modo originale rispetto alla tradizione gli stretti rapporti tra dimensioni economiche e cognitive riconducibili all'organizzazione. Quest'ottica ben si adatta alle risorse legate alla conoscenza (competenze, abilità, know-how, capacità), tutte difficilmente definibili in termini di proprietà. Alle conoscenze e alle risorse informative ad esse collegate vengono quindi attribuite delle qualità in base alle

diverse possibilità di trasferimento, da una totale impossibilità (conoscenze completamente tacite) fino a una totale trasferibilità (conoscenze codificate). Per identificare gli elementi mediante i quali si rende possibile la creazione di valore tramite la diffusione della conoscenza, è possibile fare riferimento ad Hall (Hall 1992) il quale, su una base concettuale simile a quella di Winter, indica quattro differenziali di capacità sulla base dei quali l'azienda può aspirare alla costituzione di un vantaggio competitivo sui concorrenti:

- il differenziale *funzionale*: determinato dal saper fare, dalle conoscenze acquisite, dall'abilità ed dalle esperienze delle persone, ossia dei fattori che consentono all'azienda di raggiungere e mantenere la propria posizione competitiva nei confronti dei concorrenti;
- il differenziale *culturale,* legato ad atteggiamenti, abitudini, credenze e valori aziendali. Si tratta, ad esempio, dell'orientamento alla qualità del lavoro svolto, o della proattività rispetto agli stimoli esterni;
- il differenziale *posizionale*, effetto di azioni passate che cha hanno prodotto posizioni di forza in grado di innalzare barriere all'ingresso nei confronti dei potenziali concorrenti;
- il differenziale *di regolazione*, infine, che consiste dalla detenzione legalmente riconosciuta di diritti di proprietà intellettuale, contratti, brevetti, ecc.

I primi due di questi differenziali sono strettamente legati alle competenze e alle capacità individuali e, sono quindi decisamente dipendenti dagli individui (o, in altre parole, legati alla dimensione del saper fare), mentre gli altri due sono legati alla natura del business (e alla dimensione dell'avere)

A differenza delle risorse materiali, che tendono a deteriorarsi con il passare del tempo, la conoscenza e il "saper fare" (e in generale le risorse immateriali) si rafforzano quando vengono applicate e condivise, arricchendosi mediante l'effetto network generato dalla

comunicazione. Per sfruttare queste dinamiche virtuose, tuttavia, è necessario che le organizzazioni promuovano la diffusione continua della conoscenza al proprio interno e provvedano a difendere opportunamente il patrimonio intellettuale così generato. I processi che consentono il passaggio dalla dimensione tacita a quella esplicita e viceversa devono, in altre parole, essere continuamente presidiati dal management (ivi compreso chi detiene la responsabilità dell'Information Security). A questo proposito è interessante analizzare il modello dinamico della creazione della conoscenza proposto da Nonaka e Tacheuchi (Nonaka, Takeuchi, 1997), secondo i quali "la conoscenza umana si crea e si diffonde attraverso l'interazione sociale fra conoscenza tacita ed esplicita", cui danno il nome di "conversione della conoscenza". Sempre i due autori distinguono quattro modalità di conversione della conoscenza (Figura 2.1):

- la *socializzazione* (da conoscenza tacita a conoscenza tacita);
- l'*esteriorizzazione* (da conoscenza tacita a conoscenza esplicita);
- la *combinazione* (da conoscenza esplicita a conoscenza esplicita), che è un processo di sistematizzazione di concetti in un sistema di conoscenza;
- l'*interiorizzazione* (da conoscenza esplicita a conoscenza tacita).

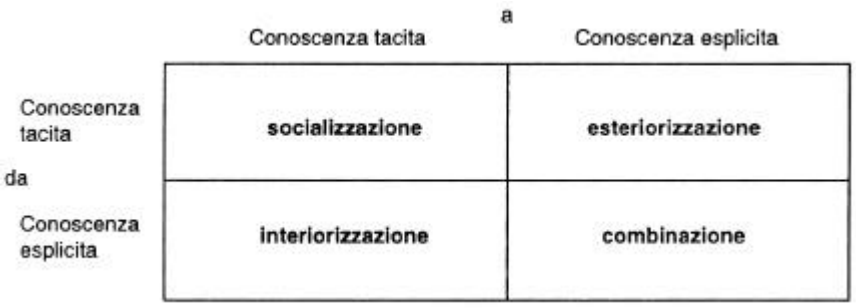

Figura 2.1: Le quattro modalità di conversione della conoscenza secondo Nonaka e Tacheuchi – Fonte: (Nonaka, Takeuchi, 1997)

Nonaka e Tacheuchi affermano poi che nell'impresa che crea conoscenza questi quattro processi si intersecano in una sorta di "spirale della conoscenza" (Figura 2.2), considerata la vera fonte di vantaggi competitivi duraturi, in quanto la conoscenza si incorpora rapidamente in nuove tecnologie e prodotti.

Figura 2.2: La spirale della conoscenza di Nonaka e Tacheuchi – Fonte: (Nonaka, Takeuchi, 1997)

"Il processo di creazione di conoscenza organizzativa parte dalla condivisione di conoscenza tacita , che si identifica grosso modo con la modalità della socializzazione, e che consiste nella diffusione all'interno dell'organizzazione del patrimonio inesplorato di conoscenza degli individui. Nella seconda fase, la conoscenza tacita condivisa viene convertita in conoscenza esplicita sotto forma di un nuovo concetto, attraverso un processo analogo a quello di esteriorizzazione. Il concetto creato viene giustificato nella terza fase, nella quale l'organizzazione decide se esso è veramente degno di essere perseguito. Una volta giustificati, nella quarta fase i concetti vengono convertiti in archetipi, che possono prendere forma di un prototipo nel caso di sviluppo di prodotti "hard" o di uno schema operativo nel caso di innovazioni "soft", un nuovo valore di corporate, un sistema di gestione innovativo, una rinnovata struttura organizzativa" (Nonaka, Takeuchi, 1997).

2.2. La nuova prospettiva della gestione del rischio informativo

Il breve escursus nella teoria della generazione e diffusione della conoscenza consente di rimarcare come l'oggetto dell'Information Security, vale a dire la protezione del patrimonio intellettuale dell'organizzazione, non si possa limitare alla difesa dei mezzi tecnici impiegati per la raccolta, l'elaborazione e la comunicazione dell'informazione. Al contrario, nell'accezione più ampia del termine, governare l'Information Security significa espletare un processo continuo che molto ha a che fare con la gestione manageriale, configurandosi come un complesso di decisioni da assumere in condizioni di razionalità limitata in un contesto dinamico e incerto. Così come la generazione e la diffusione della conoscenza è un processo complesso non solo dal punto di vista dei supporti tecnologici, ma anche, e soprattutto, dal punto di vista organizzativo, così la gestione del rischio informativo connesso a tale patrimonio intellettuale si configura come un processo prima di tutto di gestione organizzativa, all'interno del quale la componente tecnologica rappresenta solo una delle possibili prospettive di osservazione. In questo senso è possibile affermare che la sicurezza informativa dovrebbe fare parte integrante dei processi produttivi aziendali, costituendo elemento di qualità discriminante nell'ambito sia dei processi, sia del prodotto finale generato da tali processi. Questa visione, del resto, è confermata dall'evoluzione delle procedure per la certificazione di qualità dei processi produttivi aziendali, che considerano con sempre maggior determinazione il sistema informativo come uno strumento essenziale di produzione e la sicurezza cablata al loro interno come prerequisito essenziale di conformità agli standard. E non a caso il riferimento normativo utilizzato come benchmark per la definizione degli standard di qualità sono i BS7799 (BSI-DISC Committee, 1999) - recepiti dall'ISO con lo standard ISO17799 - che, a differenza dei precedenti standard TCSEC, ITSEC e degli stessi Common Criteria (CC), fanno riferimento esplicito alla gestione di processi organizzativi, piuttosto che alla

classificazione dei sistemi di trattamento automatizzato dell'informazione secondo criteri di valutazione della robustezza tecnica dei sistemi stessi.

A questa differente visione dell'attività di Information Security, corrisponde la necessità di definire all'interno dell'azienda un modello quanto più possibile strutturato e trasversale per la gestione del rischio informativo. Evidentemente, se è vero quanto argomentato fin qui, l'approccio da adottare dovrà necessariamente essere quanto più possibile idoneo a trattare in modo integrato obiettivi strategici aziendali di alto livello, scelte inerenti la pianificazione dei sistemi informativi e decisioni riguardanti la sicurezza informativa. A tale scopo viene presentato il "modello di sintesi per la pianificazione dei sistemi informativi orientati alla sicurezza", frutto della rielaborazione degli studi inerenti la pianificazione dei sistemi informativi (Palmieri, 1994), unita all'esame delle best practices derivanti dall'applicazione dei modelli di sicurezza in contesti aziendali reali.

3. UN MODELLO DI SINTESI PER LA PIANIFICAZIONE DI SISTEMI INFORMATIVI ORIENTATI ALLA SICUREZZA

Provvedere alla sicurezza del patrimonio informativo aziendale significa innanzi tutto definire in modo preciso cosa proteggere, vale a dire definire per ogni categoria di dati le funzioni di sicurezza ritenute indispensabili e i requisiti in termini di robustezza dei meccanismi necessari per ottenere i livelli di Riservatezza, Integrità e Disponibilità che si intendono raggiungere. Questa fase preliminare è perciò direttamente legata al processo di classificazione dei dati. L'Orange Book, ITSEC e i Common Criteria sono totalmente basati sul concetto di livello di sicurezza, prevedendo che ad ogni TOE (Target Of Evaluation) venga assegnato un livello di sicurezza desiderato in base al quale definire funzioni di sicurezza e robustezza dei meccanismi. Gli stessi documenti

BS 7799 (British Standard) e NIST 800-18 (National Institute of Standards and Technology), che come si è ricordato presentano un approccio più legato ai processi che alle tecnologie, prevedono comunque come attività preliminare e propedeutica alla pianificazione della sicurezza la formalizzazione di una precisa Security Policy, recante indicazioni relative agli obiettivi della gestione della sicurezza, ai livelli di assurance ritenuti soddisfacenti per ogni categoria di dati e alle specifiche funzioni di sicurezza indispensabili per ottenerli. Questo approccio, come esplicitamente sottolineato all'interno del documento NIST 800-18, ben si adatta al concetto di sicurezza come investimento teso al perseguimento della qualità all'interno dei processi aziendali. Come qualsiasi altro investimento, quello per la sicurezza dei sistemi informativi deve essere attentamente valutato in termini sia monetari che strategici, in modo tale da assicurare che il costo del controllo non ecceda il valore dei benefici attesi. Ciò significa che la sicurezza dovrebbe risultare appropriata e proporzionata al valore del bene protetto e alla gravità, probabilità ed estensione dei potenziali attacchi. I requisiti in termini di sicurezza sono quindi variabili in relazione alle risorse da difendere e alla specifica architettura del sistema informativo. Se è vero che, in generale, l'investimento in misure di sicurezza comporta la riduzione della frequenza e della gravità delle perdite correlate alla sicurezza dei sistemi informativi, infatti, è pur vero che tali benefici impongono il sostenimento di costi sia diretti che indiretti. I costi diretti includono il costo opportunità delle persone, l'acquisto, l'installazione e la gestione delle misure di sicurezza. I costi indiretti concernono invece tutta la serie di ripercussioni, spesso difficilmente quantificabili, riconducibili all'implementazione delle misure di sicurezza, come la possibile perdita di efficienza del sistema, gli impatti negativi sul morale dei dipendenti o, più semplicemente, la necessità di allestire corsi di aggiornamento per il personale. In molti casi, questi costi addizionali eccedono il costo iniziale del controllo. La scelta e l'implementazione delle misure di sicurezza sono dunque diretta

conseguenza della criticità e del valore delle risorse da proteggere, nonché del rischio cui esse sono sottoposte e dalle specifiche caratteristiche dell'organizzazione, della sua struttura e della configurazione del suo sistema informativo. Risulta inoltre essenziale che la perimetrazione dell'ambito da proteggere venga effettuata con chiarezza e tempestività, prima della progettazione delle misure di sicurezza vere e proprie. Il perimetro dello scenario da analizzare riguarda generalmente l'intera azienda; in alcuni casi, tuttavia, è possibile che lo scenario di intervento venga ristretto alle risorse informative di maggiore rilevanza o che, cosa sempre più frequente con la diffusione dei sistemi informatici interconnessi, la linea di sicurezza venga definita non esclusivamente secondo criteri logistici, ma anche in base a criteri di natura logica, vale a dire rispetto a una determinata procedura, o a un particolare insieme di procedure. La definizione dello scenario deve contenere altresì un'analisi degli elementi a valenza giuridica, normativa, statutaria e ambientale che condizionano la correttezza e la legittimità del sistema di protezione dei dati che si ha intenzione di progettare.

È infine utile considerare l'importanza che riveste l'attività di controllo. Le misure di sicurezza, fisiche, logiche o organizzative che siano, non sono in grado di garantire l'immunità assoluta da attacchi potenzialmente dannosi. In questa situazione le misure di sicurezza rappresentano un indispensabile deterrente, in grado di restringere il numero dei potenziali agenti dannosi e di rallentarne l'azione, ma nulla possono in mancanza di un'adeguata capacità di reazione dell'organizzazione, che si basa, oltre che su un'attività di controllo continuo, sulla competenza dei responsabili della sicurezza (primo intervento e intervento specializzato), sulla formazione degli utenti e sulla pianificazione di procedure organizzative adeguate ad arginare l'incidente. Prevenzione e capacità di reazione sono dunque i due elementi interconnessi e necessari per far fronte alle minacce nei confronti del sistema informativo provenienti tanto dall'interno, quanto dall'esterno dell'organizzazione. Incrociando l’orizzonte temporale (preventive o

di ripristino) con la natura delle misure di sicurezza (fisiche, logiche, organizzative), è possibile identificare una tassonomia, pur non esaustiva, comunque utile per tracciare un quadro di riferimento ed effettuare alcune considerazioni in merito alle misure stesse (figura 3.1).

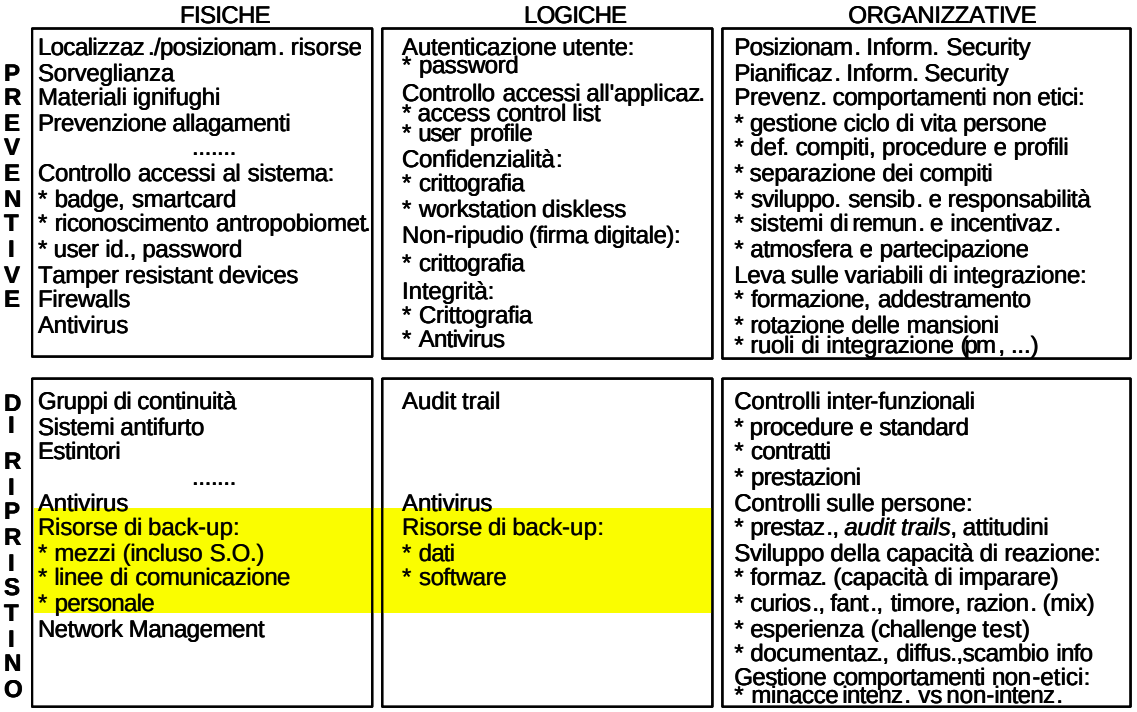

Figura 3.1: Un quadro di riferimento per le misure di information security

Preme qui richiamare all'attenzione due concetti evidenziati dallo schema proposto. Si tratta dei concetti di integrazione (apprezzabile leggendo lo schema orizzontalmente) e di equilibrio (evidenziato, invece, dalla lettura verticale) delle misure di sicurezza:

- per *integrazione* si intende la necessità di provvedere all'implementazione delle misure secondo un approccio che non trascuri nessuno degli elementi costituenti il sistema informativo. Come è possibile notare analizzando le misure presentate nello schema, una corretta politica della sicurezza dovrebbe prevedere la predisposizione di misure concernenti persone (misure organizzative e misure

fisiche per la protezione dei siti), dati (misure di back-up, misure logiche per il controllo degli accessi alle basi di dati e per il mantenimento della Disponibilità, Riservatezza e Integrità dei dati), procedure (misure organizzative, misure logiche per il controllo degli accessi alle applicazioni, antivirus) e mezzi tecnici (misure fisiche di protezione dei siti e di difesa dai furti). L'importanza di un approccio di questo genere è ravvisabile nel principio secondo il quale il livello di sicurezza di un sistema si attesta sul livello che caratterizza il suo elemento più debole. Il rispetto di questo principio si traduce praticamente nella necessità di predisporre le misure di sicurezza in modo tale da non generare uno squilibrio tra le tre tipologie di misure individuate: fisiche, logiche e organizzative. In caso contrario, anche le misure di sicurezza più all'avanguardia, perdono gran parte della propria efficacia. A tal proposito sia sufficiente riflettere sulla effettiva utilità della definizione di un insieme di procedure dettagliate per la protezione del patrimonio informativo, se non si provvede contestualmente a definire un sistema di controllo organizzativo che induca gli utenti a rispettarle. Oppure, solo a titolo di ulteriore esempio, si pensi all'efficacia di un sofisticato sistema di controllo degli accessi, in assenza di una politica che determini i privilegi di accesso ai dati di ciascuna categoria di utenti;

- con il termine *equilibrio*, si intende la necessità di predisporre un mix bilanciato tra misure preventive e misure di ripristino. La transizione verso sistemi informativi caratterizzati da crescenti livelli di complessità e da architetture basate sull'informatica distribuita e sulle reti di elaboratori, ha da tempo convinto i responsabili dell'information security ad abbandonare il concetto di "sicurezza totale". Ciò significa che nessun meccanismo di sicurezza è attualmente in grado di ridurre a zero il rischio di incidente informatico, rendendo indispensabile la predisposizione da parte dell'azienda di misure adatte

alla gestione dell'emergenza. D'altra parte, la capacità di risposta dell'azienda agli attacchi che minacciano il proprio patrimonio informativo è strettamente legata all'efficacia dei meccanismi di sicurezza preventiva.

3.1. Il modello di pianificazione della sicurezza

L'esperienza ha dimostrato che esistono alcuni fattori critici che determinano il successo di un piano di sicurezza informativa (BS 7799-1, 1999):

- la definizione di una Security Policy, di obiettivi e di attività che riflettano gli obiettivi fissati dalle strategie e dalle politiche di alto livello;
- un approccio all'implementazione della sicurezza che sia integrato nella cultura dell'organizzazione;
- un supporto visibile e un impegno diretto da parte del management;
- una buona comprensione dei requisiti di sicurezza e un efficace processo di analisi e di gestione del rischio;
- un'efficace sensibilizzazione di manger e dipendenti ai temi inerenti la sicurezza, che prevede la comunicazione delle linee guida e degli standard fissati dalla politica di sicurezza e appropriate attività di formazione e addestramento;
- la predisposizione di un sitema completo e bilanciato che consenta di misurare le prestazioni in termini di sicurezza e fornisca un adeguato *feedback* per il loro miglioramento.

Il modello proposto per la pianificazione dell'Information Security (figura 3.2), è stato ideato a partire da questi requisiti fondamentali. Si procederà dunque presentando i concetti di Information Security Policy e di analisi del rischio, per poi procedere con la presentazione del piano di sicurezza informativa e dell'attività di controllo e reporting degli incidenti.

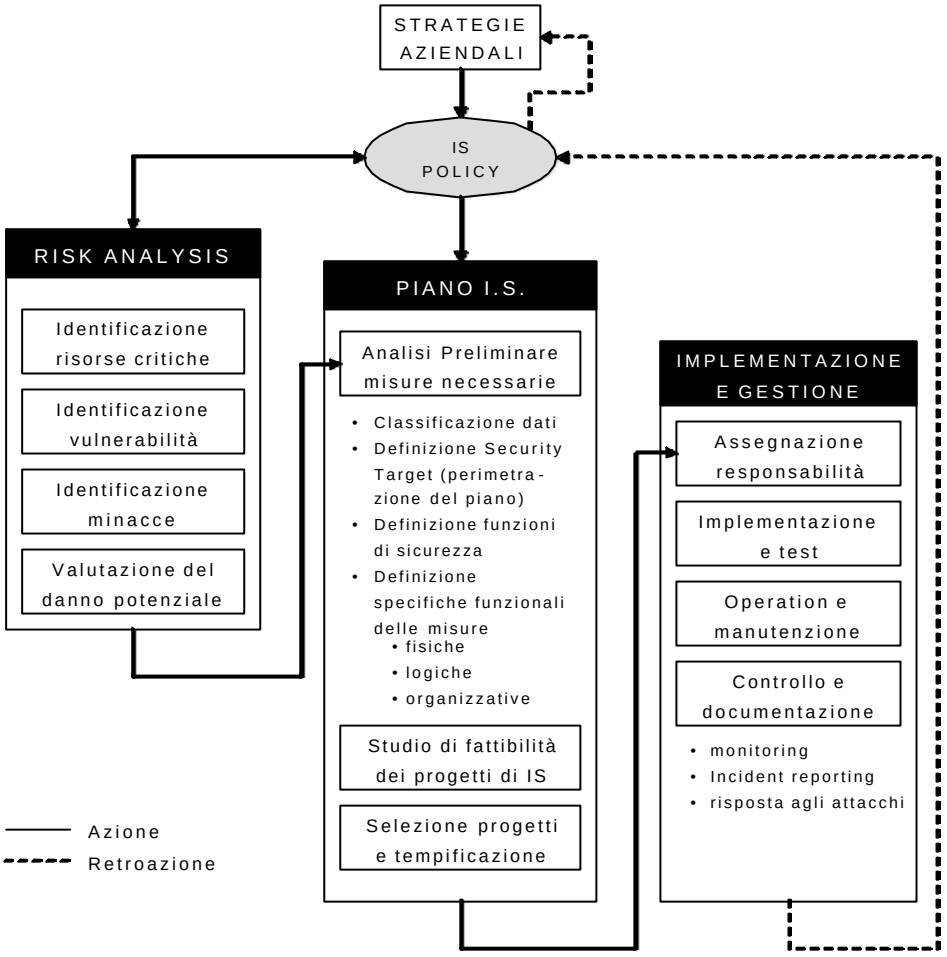

Figura 3.2: Modello di pianificazione dell'information security basato sul ciclo di vita dei sistemi informativi

3.1.1. La politica di sicurezza informativa

L'input principale del processo di pianificazione della sicurezza è rappresentato, nel modello proposto, dalle strategie e dalle politiche definite dall'alta direzione in fase di pianificazione strategica. Le politiche e le strategie di alto livello, che esprimono gli obiettivi di lungo periodo dell'impresa e lo stile manageriale scelto per perseguirli, sono infatti la base sulla quale definire le politiche di sicurezza informativa (Information Security Policies). Mediante la definizione delle politiche di sicurezza, il management, in collaborazione con i responsabili della sicurezza, esprime i principi e gli standard che serviranno come riferimento nelle fasi di definizione del piano di sicurezza. In particolare, l'Information Security Policy dovrebbe essere approvata dal management,

pubblicata e comunicata in modo appropriato a tutti i dipendenti. Dovrebbe inoltre provare l'impegno del management e tracciare le linee guida dell'approccio dell'organizzazione all'Information Security. I seguenti aspetti dovrebbero essere sempre considerati all'interno della politica di sicurezza informativa:

- gli obiettivi di Information Security, che devono essere definiti in relazione alle caratteristiche dell'organizzazione, alla sua collocazione geografica, al suo patrimonio materiale e immateriale;
- l'impegno del management a supportare gli obiettivi (da cui dipende direttamente la legittimazione e l'autorità dei responsabili della sicurezza e dei sistemi di controllo e sanzione da loro posti in essere);
- la definizione non ambigua dei requisiti e degli standard minimi di sicurezza;
- le responsabilità del management e del personale;
- la definizione delle procedure di incident reporting.

All'interno dell'azienda dovrebbe essere creato un responsabile della politica della sicurezza, che si occupi di mantenerla aggiornata in base a un processo di revisione ben definito. Tale processo dovrebbe verificare che una revisione venga effettuata ogniqualvolta avvenga un cambiamento significativo delle basi su cui è stata effettuata l'analisi del rischio (per esempio incidenti al sistema informativo di notevole entità, la nascita di nuove vulnerabilità in virtù del cambiamento ambientale, oppure un significativo cambiamento organizzativo o dell'infrastruttura tecnologica dell'azienda). In particolare, dovrebbe essere mantenuto un controllo continuo su tre aspetti fondamentali:

- l'efficacia della politica di sicurezza, valutata in base alla natura, al numero e all'entità degli incidenti informativi registrati;
- i costi e l'impatto del controllo sull'efficienza delle attività operative;

- gli effetti sull'efficacia della politica di sicurezza dovuti all'evoluzione tecnologica.

3.1.2. L'analisi del rischio

L'analisi del rischio, vale a dire il processo di interpretazione e di valutazione del rischio, rappresenta il secondo principale input della pianificazione della sicurezza informativa. A seconda della politica di sicurezza prescelta, l'attività di risk analysis può essere caratterizzata da livelli superiori o inferiori di dettaglio e può essere svolta ad intervalli più o meno regolari. Analogamente alla politica di sicurezza, tuttavia, il processo di analisi del rischio dovrebbe avere all'interno dell'azienda un responsabile, cui è demandato il compito di provvedere alla reiterazione dell'analisi, se non secondo una cadenza periodica, almeno in conseguenza di sensibili cambiamenti dell'ambiente circostante, o dell'azienda stessa. In generale l'attività di Risk Analysis dovrebbe essere il risultato della collaborazione di tutte le unità organizzative, in modo da coinvolgere gli esperti appartenenti alle diverse aree funzionali. In realtà, spesso tale attività è prerogativa della funzione Security (o, in sua assenza, di quella Sistemi Informativi) che provvede a raccogliere le valutazioni dei differenti responsabili funzionali.

La valutazione del rischio si compone fondamentalmente delle seguenti attività[iii]:

- censimento delle risorse del sistema informativo;
- definizione dell'esposizione al rischio per ciascuna risorsa;
- valutazione dell'esistenza e dell'efficacia dei controlli;
- identificazione e quantificazione del rischio
- definizione delle tipologie delle misure di protezione.

3.1.3. Il piano di sicurezza

La fase di stesura del piano di sicurezza prevede una serie di attività finalizzate a tradurre i principi generali contenuti all'interno della politica di sicurezza in progetti operativi che serviranno come input alla successiva fase di definizione delle specifiche tecniche e di implementazione dei meccanismi di sicurezza ritenuti indispensabili per attuare tali principi. Il piano di sicurezza dovrebbe espletare le seguenti attività:

- *identificazione degli elementi da proteggere.* Il primo passo da compiere è individuare quali elementi del sistema informativo sono soggetti a un rischio eccessivo rispetto al loro livello di criticità. Tali elementi sono tipicamente dati memorizzati all'interno del sistema che si vuole proteggere, servizi erogati agli utenti del sistema stesso, mezzi tecnici o persone. Un approccio possibile per individuare gli obiettivi del piano di sicurezza è quello di partire dalla classificazione dei dati che, oltre a dare un quadro complessivo delle risorse informative da proteggere, assegna loro un livello di criticità e valuta le conseguenze di un eventuale attacco. La "mappa" delle risorse informative critiche, e il suo confronto con i risultati dell'analisi del rischio, consente di individuare le aree di vulnerabilità non compatibili con i requisiti e gli standard minimi di sicurezza definiti dalla Information Security Policy. Gli obiettivi del piano di sicurezza saranno dunque le architetture informatiche, le procedure e le persone che trattano le risorse informative così individuate. L'individuazione degli obiettivi consente di restringere il piano di sicurezza ai soli elementi che necessitano di un intervento; questo procedimento viene abitualmente denominato "perimetrazione" del piano di sicurezza;
- *identificazione delle minacce a cui gli elementi definiti in (1) sono sottoposti.* Per ognuno degli elementi definiti al punto 1, è necessario articolare l'analisi del rischio in modo da individuare le possibili minacce cui può essere sottoposto.

Ad esempio se può essere oggetto di modifiche ad opera di persone non autorizzate, se può essere oggetto di attacchi finalizzati all'interruzione del servizio, ecc.;

- *analisi dei rischi specifici*. Con gli elementi definiti nei passi precedenti è possibile procedere ad un'analisi dei rischi specifica per i singoli obiettivi individuati. Definite per ogni elemento del punto 1 le relative minacce a cui può essere sottoposto, è necessario stabilire, in accordo con i principi della politica di sicurezza, la soglia sopra la quale il rischio viene giudicato non conforme;
- *Definizone delle funzioni di sicurezza*. Al termine del punto 3 si è già in possesso di informazioni precise riguardo agli elementi da proteggere e alle fonti di rischio che li minacciano. A questo punto è necessario procedere alla definizione delle funzioni di sicurezza specifiche per ciascun elemento, al fine di diminuire il rischio complessivo a livelli accettabili. L'output di questa fase è rappresentato da una serie di indicazioni di massima che verranno approfondite nella fase successiva;
- *studio di fattibilità tecnica ed economica*. Una volta definite le funzioni di sicurezza che gli obiettivi del piano devono garantire, è possibile effettuare una analisi della fattibilità tecnica delle soluzioni di massima formulate in precedenza. Se un progetto viene giudicato tecnicamente fattibile, viene sottoposto ad un'analisi di fattibilità economica, in cui i costi economici e organizzativi riconducibili al controllo vengono confrontati con i benefici attesi. Se il risultato dell'analisi è considerato soddisfacente il progetto viene inserito nel portafoglio progetti;
- *selezione e tempificazione dei progetti di Information Security*. In questa fase, i progetti che sono stati giudicati fattibili, vengono ordinati secondo il loro livello di criticità, e selezionati in base alle risorse disponibili. Ai progetti selezionati

vengono allocate le risorse necessarie e viene definito un programma delle attività che devono essere svolte, al fine di poter esercitare un controllo efficace sul loro corretto sviluppo.

3.1.4. Implementazione e controllo

In questa fase avviene l'implementazione vera e propria delle misure di sicurezza, durante la quale si portano a termine le specifiche attuative dei progetti vagliati dall'attività di selezione, si definiscono nel dettaglio le misure necessarie ad ottenere le funzioni di sicurezza ritenute indispensabili, e si procede all'acquisizione e l'installazione dei dispositivi, oltre che alla definizione dettagliata e alla documentazione delle procedure organizzative. Alla fase di implementazione segue quella di test, in cui si verifica che le misure poste in essere a difesa del sistema funzionino correttamente. L'implementazione e la verifica dei meccanismi di sicurezza spesso implicano l'impiego di competenze sovrapposte tra la funzione Sistemi Informativi e quella di Sicurezza. Per questo motivo, considerare nettamente separati i due processi (il processo di sviluppo dei sistemi informativi e quello di implementazione dei meccanismi di sicurezza) appare una forzatura che può risultare utile esclusivamente a fini espositivi. Del resto, la sovrapposizione tra le competenze di sicurezza e quelle tecniche di ICT, costituisce una delle ragioni a sostegno di un approccio congiunto ai due problemi. In questa fase avviene anche la definizione delle procedure organizzative e delle regole comportamentali con cui si dà attuazione pratica ai principi concernenti il controllo e l'*incident reporting* espressi all'interno della politica di sicurezza. Ciò significa definire le responsabilità degli utenti del sistema in caso di incidente, le procedure secondo le quali chi viene a conoscenza di un incidente deve comunicarlo (quando, a chi, fornendo quali indicazioni) ed eventualmente intervenire, i sistemi sanzionatori e di incentivazione tesi ad accrescere la sensibilità dei dipendenti ai temi della sicurezza.

Una gestione efficace delle risorse umane passa per una chiara definizione delle mansioni, delle procedure e delle responsabilità, nonché dalla predisposizione di un efficace sistema di controllo. Altre tematiche che devono essere affrontate riguardo alla risposta in caso di incidente sono: la definizione delle procedure di primo intervento, le modalità di coordinamento tra responsabili del primo intervento e specialisti della sicurezza, il coordinamento tra diverse unità interconnesse ma disperse geograficamente, la valutazione dell'opportunità di riportare o meno l'accaduto all'autorità giudiziaria, la priorità da assegnare ai servizi in fase di ripristino. La capacità di reazione, oltre che dalla predisposizione di adeguate procedure, è funzione della formazione dei dipendenti e degli specialisti, dalla loro attitudine al controllo (a propria volta conseguenza di un adeguato mix tra curiosità, fantasia, diffidenza e razionalità) e dalla documentazione, la diffusione e lo scambio di informazioni all'interno dell'organizzazione.

L’attività di monitoring del sistema avviene mediante controlli periodici a livello fisico (sorveglianza dei locali, controllo degli accessi, verifica dell’efficienza dei sistemi antifurto, manutenzione dei sistemi antincendio, ecc.), logico (impiego di appositi software di *intrusion detection* che gestiscono allarmi automatici in caso di accesso non consentito al sistema, audit trails, ossia controllo dei log che tengono traccia delle attività degli utenti connessi al sistema, ecc.), e organizzativo (controllo del rispetto delle procedure, erogazione di sanzioni nei confronti dei trasgressori, attività di intelligence e antifrode, ecc.). L'attività di check-up (valutazione del sistema di sicurezza nel suo complesso), infine, risponde alla necessità, comune a qualsiasi progetto o investimento, di confrontare i risultati raggiunti con quelli fissati inizialmente come obiettivo: l'analisi degli scostamenti da tali obiettivi consente, infatti, di valutare in modo razionale il successo del progetto/investimento e di predisporre le eventuali modifiche necessarie a correggere gli errori commessi.

3.2. Un modello di sintesi

Esistono alcuni evidenti punti di contatto tra la pianificazione dei sistemi informativi e quella del sistema di Information Security. In primo luogo è evidente notare come i sistemi informativi siano l'oggetto dell'Information Security. Questo legame consente di individuare con una certa facilità l'azione di vincolo che l'architettura del sistema informativo esercita nei confronti della sicurezza. Ciò significa che, compito specifico della pianificazione dell'Information Security è quello di prendere atto della configurazione del sistema informativo e predisporre tutte le misure necessarie a renderlo compatibile con le funzioni di sicurezza definite dalla strategia aziendale in fase di definizione della politica di sicurezza. Spesso meno evidente risulta però il legame inverso, cioè quello che vincola l'attività di sviluppo dei sistemi informativi alle considerazioni in merito alla sicurezza del patrimonio informativo aziendale. Trascurare questo secondo vincolo significa non considerare nella valutazione dei progetti riguardanti i sistemi informativi le implicazioni di tipo economico, tecnico e organizzativo riconducibili all'ambito della sicurezza informativa.

Il secondo importante punto di contatto tra i due processi è rappresentato dal loro comune obiettivo. Sia il processo di pianificazione dei sistemi informativi che quello della sicurezza hanno come fine il miglior utilizzo del patrimonio informativo aziendale. In entrambi i casi, perciò, l'analisi dei flussi informativi e la classificazione dei dati in funzione della loro rilevanza strategica rappresentano fasi fondamentali.

La terza affinità tra pianificazione dei sistemi informativi e pianificazione dell'Information Security è rappresentata dal comune requisito di aderenza alle linee guida fissate in fase di pianificazione strategica di alto livello. Ciò significa che per un'impresa né la predisposizione dei sistemi informativi, né la gestione del rischio informativo rappresentano attività fini a sé stesse, bensì mezzi per perseguire i propri obiettivi. D’altra parte in entrambi i casi esiste anche la possibilità che, da semplici

strumenti che devono allinearsi alla strategie aziendali, sistemi informativi e sicurezza informativa si trasformino in fattori critici di successo o persino in fonti di vantaggio competitivo. Sistemi informativi efficaci e "ragionevolmente sicuri" sono infatti la base per l'utilizzo della conoscenza a scopi strategici, mediante la sua esplicitazione e condivisione all'interno delle organizzazioni.

La comunanza di obiettivi dovrebbe far riflettere sul fatto che le due attività di pianificazione in questione non dovrebbero essere gestite come due processi rigidamente separati e antitetici (poiché, secondo quest'ottica, i costi della sicurezza costituirebbero risorse sottratte allo sviluppo dei sistemi informativi). Un approccio contestuale e integrato alle due tematiche dovrebbe consentire di giungere più rapidamente, tramite la negoziazione degli obiettivi, a una gestione della conoscenza rispondente alle esigenze aziendali.

Date queste premesse, nel prossimo paragrafo si cercherà di sintetizzare i vantaggi derivanti dalla pianificazione congiunta dei sistemi informativi e della sicurezza ad essi connessa.

3.3. L'importanza di un approccio integrato

Dalle considerazioni svolte fino ad ora è possibile dedurre che, sebbene un piano della sicurezza informatica possa teoricamente essere sviluppato in qualsiasi fase del ciclo di vita del sistema informativo, l'approccio più raccomandabile è certamente quello di predisporre il piano contestualmente al processo di pianificazione dei sistemi informativi. La sicurezza, infatti, come tutti gli altri aspetti riguardanti il sistema informativo, è più facilmente gestibile se programmata lungo tutto il ciclo di vita del sistema. Secondo un consolidato principio largamente condiviso all'interno della comunità degli esperti di informatica (NIST, 1998), aggiungere una funzionalità in un sistema dopo che è stato progettato costerebbe dieci volte di più rispetto ad includere

tale funzionalità direttamente in fase di progettazione. La principale ragione che induce a implementare le funzioni di sicurezza durante la fase di pianificazione del sistema, dunque, è che farlo in un secondo tempo risulta più difficile, e questa maggiore difficoltà generalmente si riflette anche in un incremento dei costi. Implementare le funzioni di sicurezza quando il sistema è già operativo, inoltre, tende ad aumentare i disagi riscontrati durante il normale svolgimento delle attività per le quali il sistema è stato realizzato. Oltre che risultare meno efficiente dal punto di vista delle risorse impiegate, implementare nuove funzioni di sicurezza in seguito a una violazione del sistema, ad un incidente, o all'individuazione di una falla nel sistema di sicurezza, spesso risulta anche meno efficace rispetto a un approccio che preveda l'incorporazione delle funzioni di sicurezza direttamente in fase di progettazione del sistema. Un approccio alla sicurezza saltuario e basato sulla pura reazione agli eventi dannosi, infatti, risulta antitetico rispetto ai principi di integrità e di equilibrio che caratterizzano l'attività di predisposizione delle misure di sicurezza.

Come accennato in precedenza, infine, l'inclusione delle funzioni di sicurezza all'interno della pianificazione dei sistemi informativi consente di valutare in modo più accurato i progetti nella fase dello studio di fattibilità. La considerazione degli aspetti tecnici, economici e organizzativi riconducibili all'ambito della sicurezza informativa all'interno del processo di valutazione dei progetti è infatti indispensabile per ottenere delle stime realmente attendibili sulla convenienza dei progetti.

3.4. Il modello di pianificazione dei sistemi orientati alla sicurezza

Nel precedente paragrafo si sono analizzati i vantaggi derivanti da una gestione integrata lungo tutto il ciclo di vita del sistema informativo delle problematiche connesse alla realizzazione del sistema e alla predisposizione delle relative misure di sicurezza. Si presenterà ora un modello di sintesi che consenta di rappresentare in modo

congiunto le attività che caratteristiche dei due processi di pianificazione, nonché le relazioni che le legano. A tale scopo si procederà presentando la rappresentazione grafica del modello (Figura 3.3), cui seguirà una descrizione delle principali caratteristiche.

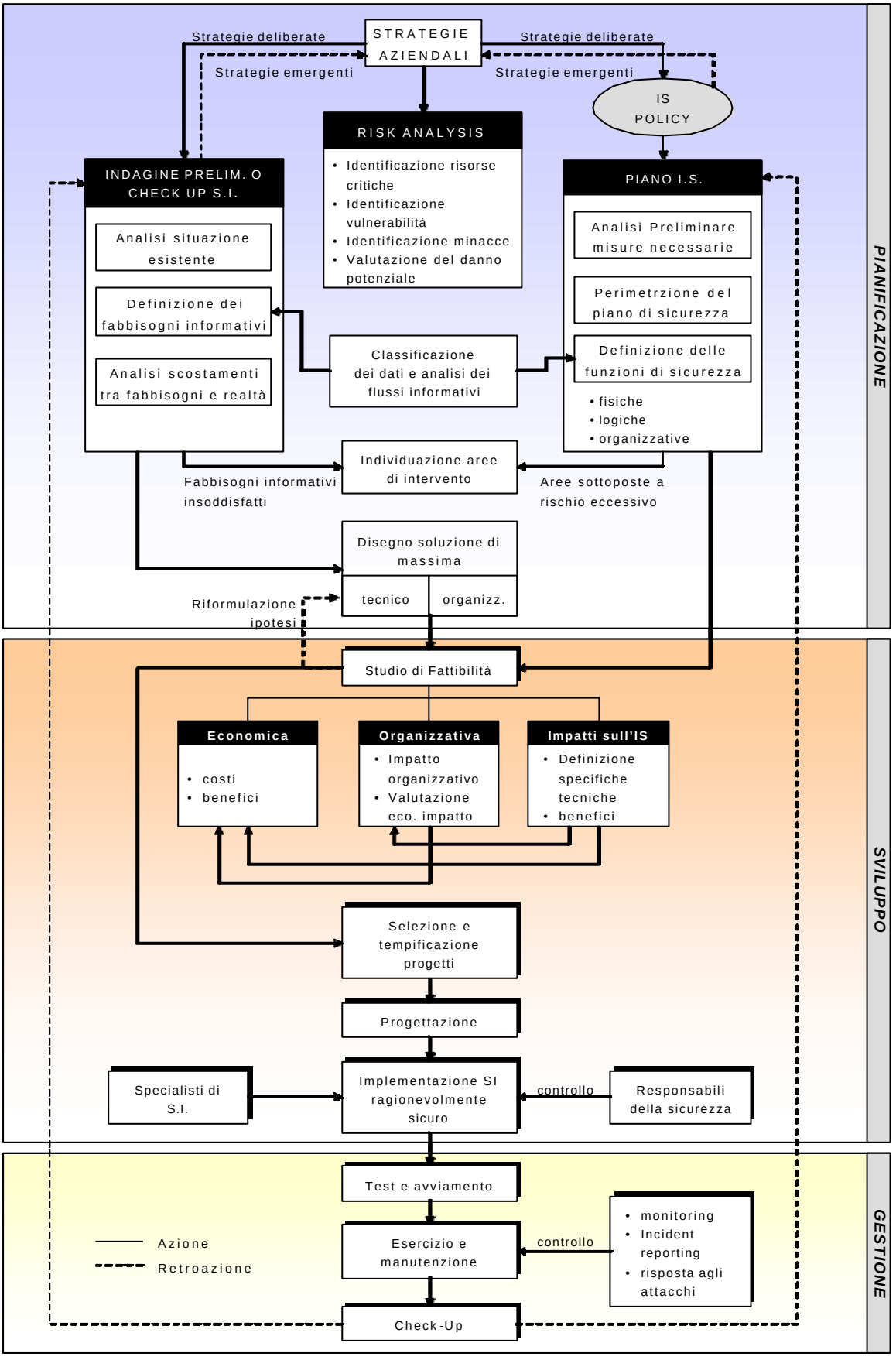

Figura 3.3: Un modello di sintesi per la pianificazione di sistemi informativi orientati alla sicurezza

Sia l'attività di pianificazione dei sistemi informativi che quella di pianificazione dell'Information Security vengono attivate dalle linee guida fissate dalle strategie aziendali di alto livello. La prima fase del processo è prevalentemente destinata all'analisi della situazione attuale, all'identificazione delle esigenze generate dalla necessità di allineamento strategico e alla definizione delle aree di intervento, che avviene mediante il confronto tra la situazione attuale e quella giudicata auspicabile. In questa prima fase esistono delle attività caratteristiche che distinguono i due processi: mentre quello di sviluppo dei sistemi informativi deve principalmente occuparsi di rilevare i fabbisogni informativi insoddisfatti degli utenti del sistema, il processo di Information Security deve provvedere a definire le funzioni di sicurezza, vale a dire i requisiti in termini di sicurezza che il sistema deve soddisfare. Pur nella loro diversità, tuttavia, le attività svolte all'interno dei due processi presentano alcuni importanti punti di contatto. In primo luogo entrambi i processi, oltre al compito di allineamento alle strategie competitive di alto livello, svolgono in comune la funzione di proposizione delle strategie emergenti. Ciò significa che combinazioni innovative tra configurazione dei sistemi informativi e sicurezza informativa possono dare luogo a strategie originali in grado di generare vantaggio competitivo e, di conseguenza, valore per l'impresa. Esiste inoltre una forte corrispondenza di obiettivi e di metodi sia tra la definizione dei fabbisogni informativi e quella delle funzioni di sicurezza, sia tra l'attività di analisi degli scostamenti tra situazione reale e quella desiderata e l'analisi del rischio. Sia l'individuazione dei fabbisogni informativi insoddisfatti che la definizione delle funzioni di sicurezza si basano sulla meticolosa analisi del patrimonio informativo e dei flussi informativi che caratterizzano i processi aziendali. In entrambi i casi il metodo utilizzato per raggiungere l'obiettivo è basato sulla collaborazione degli utenti appartenenti a tutte le unità organizzative e ad ogni livello gerarchico. Sia nel caso dell'analisi dei fabbisogni informativi che in quello della definizione delle funzioni di sicurezza, si

procede all'interrogazione degli utenti tramite interviste e/o questionari. Nel primo caso si cerca di tracciare un quadro sufficientemente dettagliato dei flussi informativi al fine di rintracciare eventuali lacune nelle informazioni fornite agli utenti, mentre nel secondo l'attività è rivolta a valutare la criticità delle risorse a loro disposizione.

Anche tra l'attività di analisi degli scostamenti tra situazione reale del sistema informativo e situazione desiderata e l'attività di analisi del rischio esistono legami forti. In effetti, il livello di rischio informativo che caratterizza l'impresa in un dato instante, dipende in gran parte dalla configurazione del suo sistema informativo in quel momento. Ipotizzare un livello di rischio inferiore, significa di fatto intervenire sulla configurazione del sistema informativo, così come, in senso inverso, ipotizzare variazioni sostanziali dell'assetto del sistema implica un impatto inevitabile sulla sicurezza. Proprio come due elementi facenti parte del medesimo sistema, configurazione del sistema informativo e sicurezza informativa si trovano in uno stato di equilibrio che viene turbato ogniqualvolta si interviene su uno dei due elementi. Questa forte interdipendenza rende auspicabile, pur nel rispetto delle rispettive competenze e autonomie, un'attività congiunta e coordinata tra la funzione sistemi informativi e quella di Information Security, finalizzata all'individuazione delle aree di intervento, così da evitare che i due processi, gestiti in modo completamente autonomo, finiscano per giungere a soluzioni tra loro incompatibili. Questa comunanza di intenti dovrebbe rispondere sia alla necessità di omogeneità tra strategie e politiche di alto livello e struttura aziendale, sia all'opportunità di porre in essere strategie emergenti innovative e sostenibili dall'organizzazione.

Ma il vero elemento unificante di questa fase è rappresentato dall'attività di classificazione dei dati e di analisi dei flussi informativi. Si tratta di un passaggio obbligato per la definizione delle funzioni di sicurezza, per la rappresentazione del sistema informativo attuale e per il disegno del sistema nella sua nuova configurazione.

Questa attività rappresenta senza dubbio uno dei passaggi chiave da cui dipende la qualità di tutto il processo di pianificazione e, senza dubbio, costituisce uno dei motivi principali per cui risulta vantaggioso un approccio integrato alla pianificazione dei sistemi informativi e della sicurezza ad essi relativa. Analizzare e classificare dati e flussi informativi, infatti, costituisce un'attività molto lunga e laboriosa che impegna, oltre al team di lavoro, anche la maggior parte degli utenti del sistema.

Una volta definiti gli ambiti di intervento, risulta indispensabile tradurre le linee guida fornite dalle strategie aziendali in soluzioni di massima, a cui devono essere associati dei progetti. Lo scopo di questa fase è quella di definire gli obiettivi dei singoli progetti e le specifiche funzionali delle soluzioni ad essi associati. È a questo punto che l'interazione tra processo di sviluppo dei sistemi informativi e processo di definizione delle misure di sicurezza si fa più serrato. In questa fase il livello di dettaglio con cui vengono definite le soluzioni è ancora piuttosto scarso (le specifiche tecniche verranno definite solo in fase di progettazione), per cui i progetti sono ancora caratterizzati da un notevole grado di incertezza. In questa situazione diventa difficile coordinare lo sviluppo del sistema con le esigenze in termini di sicurezza, in quanto non conoscendo ancora l'architettura che caratterizzerà il nuovo sistema, risulta troppo ampio il ventaglio di alternative da considerare nella fase di definizione della soluzione di massima per quanto riguarda le misure di sicurezza. Un modo di uscire da questa *empasse*, può essere quello di reiterare più volte il processo di definizione delle specifiche funzionali del sistema informativo e delle misure di sicurezza, in modo tale da raggiungere, per approssimazioni successive, una soluzione di massima che presenti un compromesso ritenuto soddisfacente tra architettura (e prestazioni) del sistema ed esigenze attinenti il dominio della sicurezza.

Una seconda soluzione, scelta nel modello presentato, è quella di dare priorità alla definizione delle soluzioni di massima per ciò che concerne i sistemi informativi e, fino

a quel punto, affidare alla funzione Security un ruolo prevalentemente di controllo. In questo caso i fabbisogni informativi riacquistano un'indiscutibile centralità all'interno del processo di pianificazione. L'analisi dei fabbisogni informativi insoddisfatti, condotta come descritto in precedenza in parallelo rispetto all'individuazione delle aree critiche per la sicurezza, dà il via al processo di pianificazione del nuovo sistema, che giunge fino al disegno della soluzione di massima. A questo punto, nel corso dello studio di fattibilità, vengono valutati insieme agli aspetti economici e organizzativi, anche quelli relativi alla sicurezza. In particolare viene considerata la possibilità tecnica di mantenere il rischio relativo al nuovo progetto al di sotto degli standard fissati dalla politica di sicurezza, la sostenibilità degli impatti organizzativi provocati dall'implementazione delle misure di sicurezza necessarie e i costi diretti e indiretti riconducibili al controllo. Questa attività di valutazione dovrebbe garantire la soddisfazione di tutti i vincoli: economici, funzionali e di sicurezza.

Successivamente i progetti vengono selezionati secondo la loro convenienza, ordinati in base alla loro priorità e, infine, vengono allocate le risorse ritenute necessarie per portare a termine ciascun progetto. A questo punto il processo diventa di fatto unico, in quanto esiste una forte sovrapposizione di competenze tra funzione sistemi informativi e funzione Security durante le fasi di sviluppo del sistema. In particolare, nella fase di implementazione dei meccanismi di sicurezza esiste una forte prevalenza di competenza specialistiche appartenenti alla funzione sistemi informativi, mentre si accentua il ruolo di controllo svolto dai responsabili della sicurezza.

4. ANALISI RISULTATI DELLA RICERCA EMPIRICA

In questo paragrafo vengono presentati i risultati di due ricerche empiriche effettuate a distanza di un anno l'una dall'altra, mediante le quali si è indagato l'approccio delle aziende italiane nei confronti dei temi inerenti la sicurezza informativa trattati in questo

lavoro. Le indagini sono state condotte su un campione di 400 aziende italiane composto rispettando la distribuzione dimensionale, territoriale e settoriale risultante dall'ultimo censimento ISTAT, con uno sbarramento ai 15.000.000 € di fatturato per le aziende non appartenenti alla PA. Il target del questionario sottoposto al campione è stato individuato in prima istanza nel responsabile Sistemi Informativi, al quale è stato chiesto di coinvolgere nella compilazione anche l'eventuale responsabile della Security, o chiunque all'interno o all'esterno (es. consulenti) dell'azienda fosse in grado di allargare il punto di osservazione della ricerca. I risultati vengono presentati in macrosezioni, corrispondenti agli argomenti salienti analizzati nella presentazione del modello.

4.1. Percezione dell'Information Security

Dai risultati raccolti, è possibile affermare che i rispondenti attribuiscono al tema dell'Information Security un'importanza piuttosto elevata per il proprio business nella prima ricerca, ma decrescente nella seconda (7,67 su 10 nel 2002 contro il 6,55 nel 2003). Si nota inoltre come tra i tre obiettivi principali dell'Information Security (Disponibilità, Integrità e Riservatezza), la Disponibilità sia quella ritenuta più critica in entrambi gli anni.

Rispetto alle attività comprese nella definizione di una strategia di Sicurezza dei Sistemi Informativi, è interessante notare come, nella maggior parte dei casi, esista una certa corrispondenza tra le fasi individuate dal modello proposto e la prassi aziendali (Figura 4.1). Questo avviene in particolare per le fasi più concettuali del processo di definizione della strategia di sicurezza (Classificazione delle risorse e definizione degli obiettivi e delle funzioni di sicurezza che si intendono realizzare), mentre le attività più operative del processo (definizione delle misure, delle specifiche tecniche e scelta dei prodotti di

sicurezza sul mercato) sono considerati aspetti meno critici e non vengono inseriti tra le attività da presidiare necessariamente all'interno.

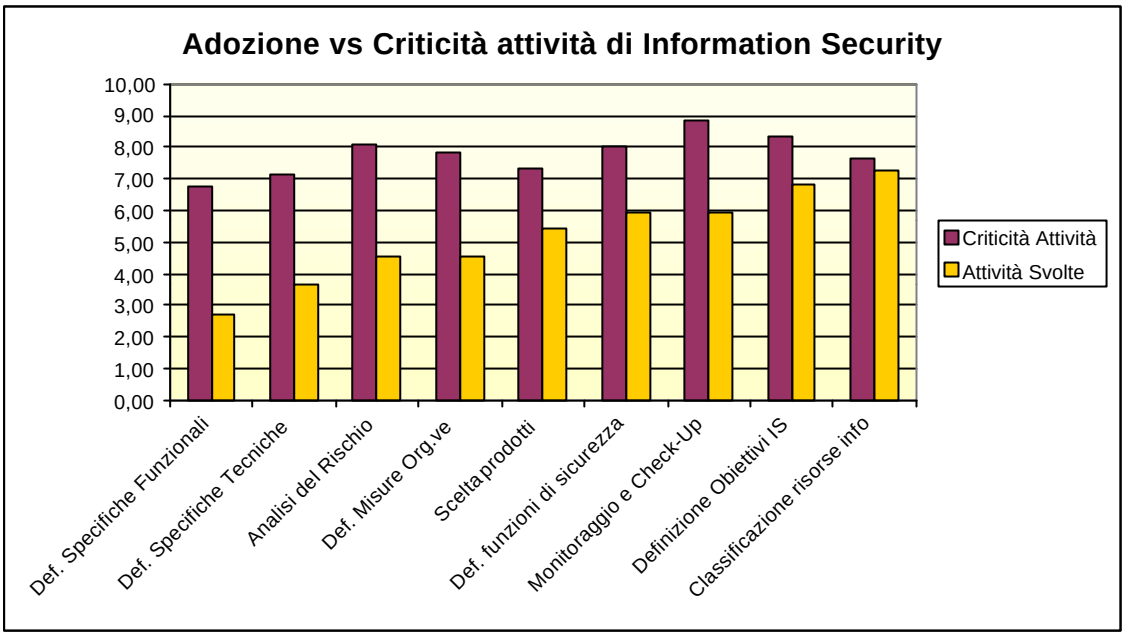

Figura 4.1: Attività di Information Security svolte dalle aziende rispondenti e loro giudizio di criticità (i dati relativi alle attività svolte sono su base 100)

Un caso a parte è rappresentato dall'attività di Analisi del Rischio. Questa attività è sicuramente da inserire tra quelle concettualmente fondamentali per una efficace definizione delle strategie di Information Security, in quanto trait d'union tra la classificazione delle risorse (dove l'analisi del rischio è parte del processo di valutazione dell'informazione) e la definizione degli obiettivi (che non possono prescindere dai profili di rischio stilati per ogni risorsa).

Nonostante la sua centralità nel processo di valutazione, l'analisi del rischio viene effettuata solo dal 45% dei rispondenti. L'incongruenza è spiegata dall'analisi delle criticità associate a ciascuna attività. Alla scarsa percentuale di rispondenti che dichiarano di effettuare l'attività di analisi del rischio, corrisponde un giudizio di criticità tra i più alti (superiore ad 8/10). Questo lascia intendere che, pur essendo ben

chiara la criticità dell'attività, esistono verosimilmente dei fattori inibitori che ne impediscono l'effettuazione. In questo senso è plausibile ipotizzare che lo sforzo necessario alla classificazione l'informazione presente in azienda e la soggettività di giudizio che caratterizza le più diffuse metodologie di Risk Analisys, rappresentino limiti significativi all'effettiva valutazione del rischio informativo.

Un discorso analogo potrebbe essere fatto anche per quanto riguarda la definizione delle specifiche funzionali e tecniche delle misure di sicurezza. Anche per queste due attività, infatti, esiste un differenziale piuttosto alto tra criticità percepita e percentuale di rispondenti che effettuano tali attività. In questi due casi, tuttavia, sembra piuttosto plausibile ipotizzare che le attività di definizione delle specifiche, pur ritenute critiche, non vengano necessariamente svolte internamente, ma ci si avvalga per esse di competenze reperite all'esterno dell'azienda, in grado di monitorare con più costanza la rapida evoluzione del mercato (consulenti esterni, piuttosto che direttamente i fornitori di tecnologie). L'attenzione nei confronti della Sicurezza Informativa, e la propensione a gestirla conformemente a processi e a strategie strutturati, è infine provata dalla percentuale di rispondenti che affermano di possedere una propria Information Security Policy (pari a ben l'82% del campione nel primo anno e al 78% nel secondo), anche se in più del 50% dei casi tale policy non risulta formalizzata e solo nel 5% dei casi è previsto un programma di comunicazione aziendale ad hoc (Figura 4.2).

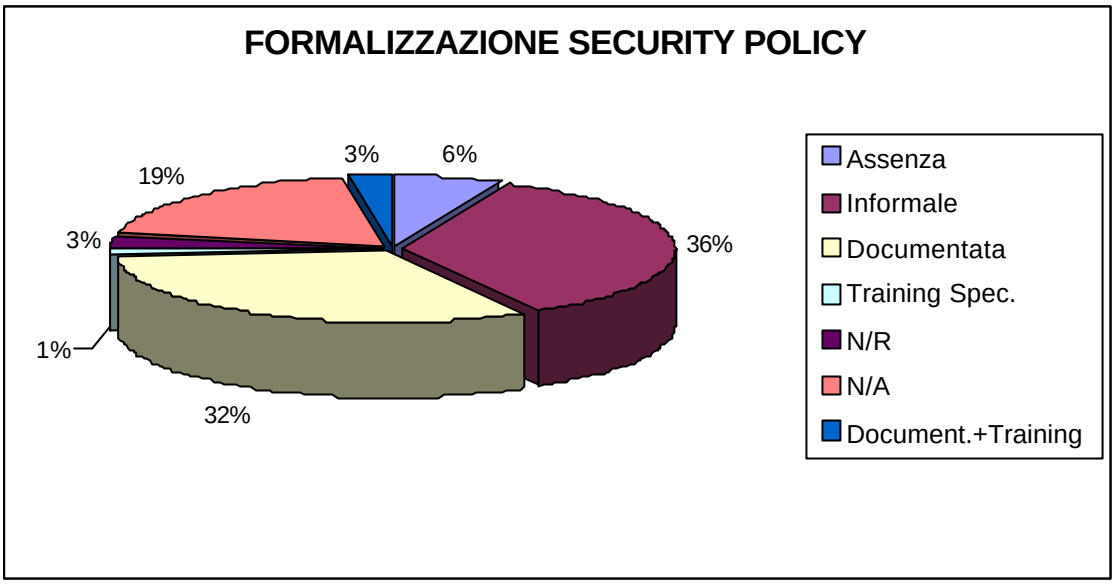

Figura 4.2: Livello di formalizzazione della Security Policy

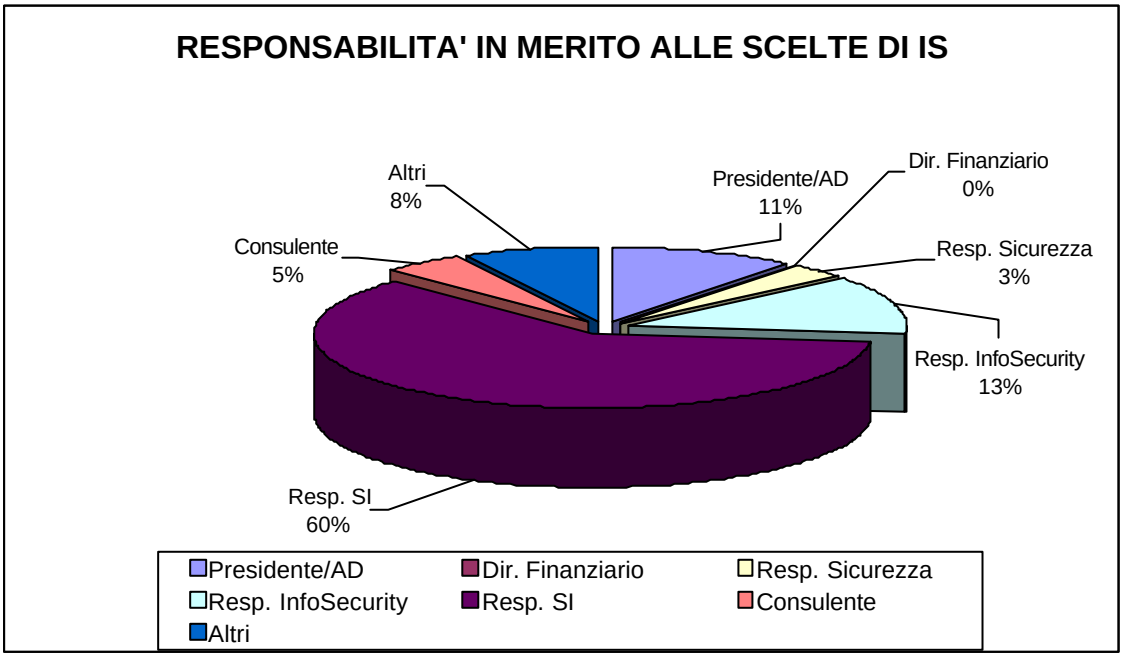

Figura 4.2: Responsabilità in merito alle scelte di Information Security

4.2. Struttura organizzativa

Se i dati relativi alla percezione dimostrano una certa aderenza delle aziende rispondenti al modello proposto, l'analisi della struttura organizzativa adibita alla gestione del rischio informativo dimostra ancora una certa difficoltà da parte delle aziende

rispondenti a darsi un assetto compatibile con le considerazioni effettuate in merito alla pianificazione congiunta dei sistemi informativi e della sicurezza. In particolare, l'elemento che più risalta è una non chiara commistione tra le decisioni inerenti gli investimenti in ICT e le scelte in ambito di information security. Oltre a rilevare che solo un'azienda su quattro possiede una funzione dedicata alla gestione del rischio informativo, affidandosi negli altri casi prevalentemente alla funzione sistemi informativi e in qualche caso (10%) ricorrendo esclusivamente a consulenti esterni, dall'analisi empirica si evince che, laddove una funzione dedicata esiste, nel 55% dei casi essa riporta alla direzione dei sistemi informativi, in chiaro disaccordo con le necessità di controllo reciproco presentata nel modello. Questa commistione di ruoli, del resto, si deduce anche dalla distribuzione delle responsabilità: anche tra le aziende che dispongono di una funzione dedicata alla gestione dell'information security, le scelte di carattere strategico inerenti la sicurezza vengono prevalentemente riservate ai responsabili sistemi informativi (60% dei casi, contro il 13% in cui vengono lasciate ai Responsabili Sicurezza), che delegano, invece, le scelte inerenti la spesa (5% contro il 44%), figura 4.3.

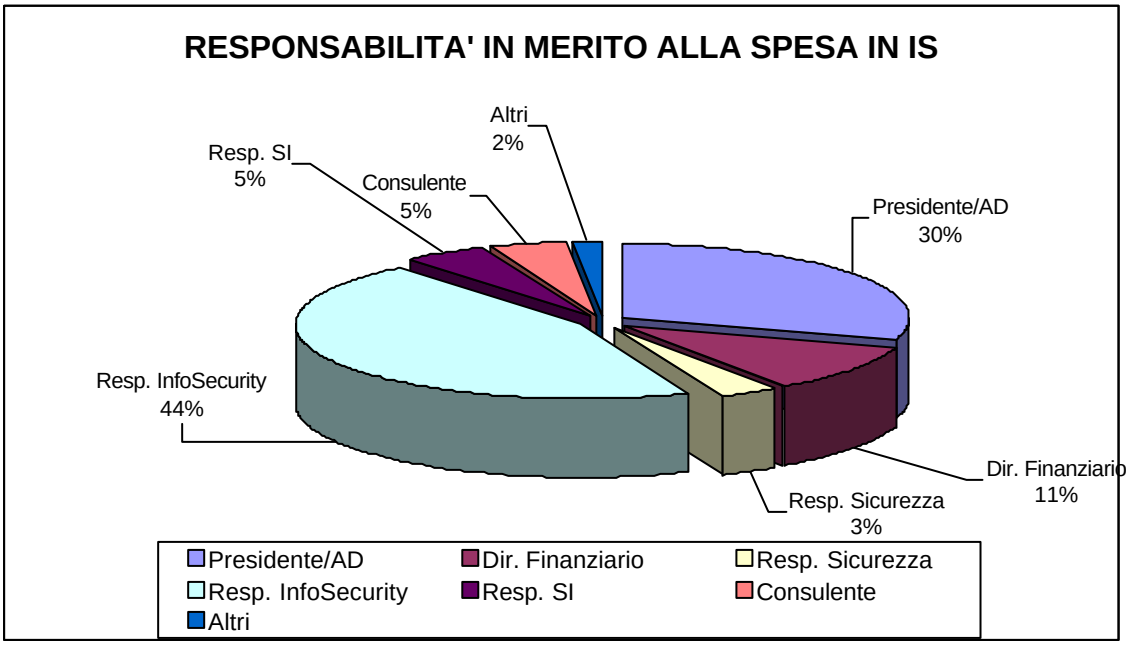

Figura 4.3: Responsabilità in merito alla spesa in Information Security

Questa distribuzione delle responsabilità lascia pensare ad un ruolo ancora marginale dell'Information Seurity nelle strategie aziendali, in cui la sicurezza è vista come vincolo allo sviluppo dei sistemi informativi.

4.3. Vulnerabilità

Analizzando la percezione delle aziende rispetto alla vulnerabilità del proprio sistema di sicurezza, si evince che, nonostante la volontà diffusa di formulare una politica di sicurezza, la valutazione media della capacità del sistema di raggiungere gli obiettivi prefissati è piuttosto scarsa (6,5). I vincoli alla protezione efficace delle risorse informative, e questo non sorprende visto quanto affermato fin qui, sono solo in minima parte ascrivibili a cause di natura tecnologica (dinamismo delle minacce 6%, dinamismo della tecnologia 11%). Tolta l'insufficienza di risorse a disposizione, le ragioni principali dell'inadeguatezza sono ravvisabili in cause di natura prettamente organizzativa (nell'ordine: scarso supporto della direzione, mancanza di competenze, mancanza di formazione e assenza di politiche adeguate). Le difficoltà di carattere organizzativo si ravvisano anche analizzando le procedure di controllo dei sistemi di sicurezza (variabile prevalentemente organizzativa che tecnologica); tra le aziende che affermano di aver subito almeno un incidente nel corso dello scorso anno, meno del 50% è stata in grado di porre in atto misure preventive. Di per sé questo non sarebbe un dato preoccupante, visto che il principio di equilibrio delle misure di sicurezza contempla anche la necessità di misure in grado di rispondere all'incidente dopo il suo manifestarsi. Il problema si ravvisa nel fatto che le aziende intervistate ritengono nell'88% dei casi più efficaci le misure di sicurezza preventive, e nel 92% dei casi ritengono il loro sviluppo un'attività prioritaria per il prossimo anno. Sempre in relazione alle misure di information security, risulta difficile, se non facendo riferimento ancora una volta alla percezione parziale del problema da parte delle aziende,

individuare una spiegazione alla scarsa priorità attribuita da parte delle aziende rispondenti allo sviluppo futuro delle misure organizzative.

5. CONCLUSIONI

In conclusione, a fronte della rilevanza del rischio informativo nelle aziende moderne e della sua notevole componente organizzativa, considerate altresì le esigenze di strutturazione del processo decisionale interente alle politiche e alle scelte di Information Security e la necessità di raccordo di tale processo con la pianificazione dei sistemi informativi, la situazione che emerge dall'analisi empirica effettuata mostra quanto segue:

- vi è un'enfasi insufficiente riguardo alla criticità attribuita alla gestione dell'Information Security in azienda;
- le aziende non mostrano particolari preoccupazioni rispetto al possibile verificarsi di incidenti riguardanti il proprio capitale intellettuale (il 64% degli intervistati ritiene poco probabile che si verifichi almeno un incidente nel corso del prossimo anno);
- i sistemi di sicurezza risultano ancora piuttosto carenti, soprattutto per quanto concerne le misure organizzative;
- non emerge un modello prevalente riguardo all'attribuzione delle responsabilità inerenti la sicurezza delle informazioni nell'ambito dell'organizzazione.

In definitiva, da un'analisi comparata dei risultati ottenuti nel 2002 e nel 2003, si ricava la sensazione che le aziende si siano avvicinate al problema della sicurezza con un approccio prevalentemente tecnologico. Verosimilmente, l'adeguamento formale alle recenti norme di legge vigenti in materia di sicurezza dell'informazioni ha favorito la predisposizione di misure tecniche di information security che sembrano aver dato alle aziende un certo senso di invulnerabilità. Infine, nonostante i rispondenti dichiarino di

svolgere buona parte delle attività previste dal modello proposto, risulta tuttavia poco evidente un approccio alla sicurezza formalizzato e coerente con le attuali esigenze di gestione della conoscenza in chiave strategica.

6. RIFERIMENTI BIBLIOGRAFICI

1. BSI-DISC Committee, 1999, *Information Security Management. Part 2: specification for information security management systems, BS 7799-1:1999*, British Standard
2. Carducci G., 1999, *La tutela dei dati aziendali,* Angeli, Milano
3. Gilardoni A., 1992, *La protezione aziendale*, EGEA, Milano
4. Guatri L., Eccles R.G., (a cura di), 2000, *Informazione e valore*, EGEA, Milano
5. Hall R., The Strategic Analysis of Intangibile Resources, in *Strategic Management Journal*, n. 13, 1992
6. Itami H., *Mobilizing Invisible Assets*, 1997, ed. it. *Le risorse invisibili*, Petrini, Torino, 1988
7. Martella G., Cremonesi C., 1990, *I crimini informatici*, Mondatori Informatica, Milano
8. Misani N., 1994, *Introduzione al risk management*, EGEA, Milano
9. Nasseri T., 1996, "Knowledge Leverage: The Ultimate Advantage", *in* ***www.brint.com*** *(The Premier Business Technology Knowledge Portal and Global Community Network for E-Business, Information, Technology, and Knowledge Management tm)*
10. National Institute of Standards and Technology Systems [NIST], 1998, *Guide for developing security plans for information technology systems*, NIST 800-18

11. Nonaka I., Takeuchi H., 1997, *The knowledge creating company*, Guerini e Associati, Milano

12. Palmieri R., 1994, Pianificazione dei Sistemi Informativi, in Camussone P.F. (a cura di), *Enciclopedia dell'Impresa*, Vol. 4, UTET, Torino

13. Polany M., 1967, *The Tacit Dimension*, Anchor Books, Garden City, 1967

14. Strassmann P.A., 1999, "Calculating Knowledge Capital", in *Knowledge Management*, ottobre 1999

NOTE

i Per una trattazione relativa alla problematica degli intangibles nella valorizzazione contabile e nell'informativa aziendale, si veda anche (Guatri, 2000)

ii Alla crucialità di conoscenze e competenze per l'acquisizione di vantaggi competitivi si richiama l'importante filone di analisi riguardante la valorizzazione delle risorse invisibili o intangibili. Nella definizione più classica (Itami, 1997) le risorse invisibili (invisibile asset) fanno parte della più ampia categoria delle risorse aziendali nella quale vanno comprese persone, beni, capitali e informazioni di cui un'azienda può disporre per raggiungere i propri obiettivi a breve e a lungo termine. Fondamentali tra queste risorse sono le informazioni, articolate in tre tipologie essenziali: le informazioni ambientali (verso l'azienda), le informazioni aziendali (verso l'esterno) e quelle interne (che sono incorporate nella cultura aziendale).

iii Per una trattazione completa al riguardo, si veda anche (Martella, 1990), (Misani, 1994) e (Gilardoni, 1992)