

CONVEGNO CEPAS
Security: Un valore per l'impresa
Roma – Hotel dei Congressi – 22 Ottobre 2004

EVOLUZIONE DELLA SECURITY

BREVE STORIA ED EVOLUZIONE DELLA FUNZIONE DI SECURITY.

La security aziendale si è sviluppata nell'Europa occidentale in un medesimo contesto internazionale anche se in ambienti nazionali differenziati per cultura, caratteristiche socio-economiche ed istituzionali.

I principali **fattori ambientali** che per i temi di Security hanno giocato un ruolo di determinante influenza sull'impresa sono stati e sono:

- **l'ambito politico**, determinato dalle strategie di Governo e dalla natura degli impulsi esistenti all'interno della collettività nazionale;
- **l'ambito amministrativo**, generato dalla natura e dalla forza dei vincoli posti dallo Stato e dalla sua amministrazione;
- **l'ambito internazionale**, determinato dallo stato delle relazioni internazionali sia politiche che economiche;
- **l'ambito economico**, creato dalla situazione congiunturale nazionale ed internazionale;
- **l'ambito sociale**, determinato dalla struttura delle relazioni tra le forze sociali;
- **l'ambito tecnologico**, nelle sue evoluzioni produttive soprattutto nel settore dell'informatica e della telematica;
- **l'ambito della sicurezza pubblica**, inteso sia come risultato dell'azione delle forze di polizia che come percezione di sicurezza o incertezza generale;
- **l'ambito culturale**, cioè il tradizionale approccio della collettività verso i problemi collettivi, in particolare quello della sicurezza.

Lo studio dei suaccennati fattori, nel loro complesso, ha come risultato la creazione degli scenari di riferimento che determinano le politiche di security.

Sono cinque, a mio parere, i periodi che contraddistinguono le vicende della security aziendale in Italia.

1

1945 – 1968

In questo primo periodo che parte dal dopoguerra e termina con il così-detto “autunno caldo” si verificano avvenimenti di carattere internazionale e nazionale che determinano la nascita di un embrione di security che si svilupperà progressivamente sino a raggiungere la forma attuale.

Successivamente alla ratifica del Patto Atlantico da parte dell’Italia, il 29.08.1955 viene diramata la normativa per la tutela del segreto industriale per le imprese a carattere strategico, sulla base della qualità/quantità della loro produzione.

Nello stesso anno vengono costituiti nell’ambito dell’Arma dei Carabinieri i “Nuclei Industriali” con il compito istituzionale di controllare l’applicazione della normativa relativa al segreto industriale. Per la prima volta imprese private, in periodo di pace, impiegano proprio personale appositamente addestrato ed un Responsabile della Sicurezza nell’applicazione di una normativa che valorizza l’informazione tecnologica e ne determina la segretezza in relazione al suo peculiare valore strategico.

Sempre in questo periodo si verifica il più importante flusso immigratorio interno soprattutto dal Sud verso il Nord ma anche dal Nord-Est verso il triangolo industriale del Nord-Ovest. Sulla scorta di questo fenomeno si assiste ad un crescente sviluppo della criminalità che coinvolge anche l’impresa con nuovi rischi di security.

A queste problematiche ed in seguito ad un impetuoso sviluppo economico che prese il nome di “miracolo italiano” si aggiungono forti tensioni sociali che sfociano, nel 1968, nella contestazione giovanile e, nel 1969, nel così detto “Autunno caldo”.

Con l’Autunno caldo ha inizio una lunga fase che si protrarrà per oltre un decennio nel corso del quale, come vedremo, prende definitivamente corpo la funzione di security.

1969 – 1981

Nel corso di questo decennio si verificano fatti straordinari che determinano il definitivo decollo della funzione di security nelle aziende italiane. Attraverso fasi successive si passa dalla rivolta studentesca all’autunno caldo con forti tensioni

sindacali ed infine ai così detti anni di piombo connotati da una forte recrudescenza del terrorismo e dal consolidarsi delle attività della criminalità organizzata. E' questo il periodo che io ho scherzosamente battezzato del "Deserto dei Tartari" o della "Guerra di trincea" per caratterizzare quella fase della security aziendale in cui l'obiettivo principale era quello di difendersi dalle offese esterne barricandosi nel perimetro del proprio insediamento e cercando di relegare all'esterno le insidie e quindi i rischi, soprattutto quelli puri.

Conseguenza di questo atteggiamento sono le misure che l'azienda adotta per proteggersi. Sono soprattutto le misure di sicurezza fisica quelle che per prima vengono realizzate, in concomitanza con il controllo degli accessi e con la realizzazione delle procedure operative necessarie per regolamentare e disciplinare con molta più rigidità rispetto al passato i servizi interni di sorveglianza e di controllo.

E nella quasi totalità delle grandi aziende appare il security manager, in una veste molto diversa da quella attuale, soprattutto in termini di competenze e finalità operative. Gli obiettivi di contrasto al terrorismo ed all'azione della criminalità organizzata, che in questa fase si manifesta nella esecuzione di centinaia di sequestri di persona, fa sì che il compito primario del security manager sia quello di tutelare l'incolumità delle risorse umane, soprattutto del top management.

Con queste finalità i contatti con le altre funzioni aziendali sono scarsi e siamo ancora lontani dal totale coinvolgimento che attualmente permea la funzione.

Ma, come vedremo nelle fasi successive, la nostra è la funzione aziendale più sensibile all'evolversi degli scenari entro cui svolge le proprie competenze dovendo essere sempre in grado di operare con rapidità trasformazioni ed adattamenti per essere in grado di contrastare i nuovi rischi che minacciano l'impresa.

Questa fase si conclude con l'esaurirsi dei fenomeni del terrorismo e dei sequestri di persona e con l'inizio di un lungo periodo di trasformazioni che sfocia in una società post-industriale con problematiche assolutamente diverse da quelle sin qui esaminate.

1982 – 1990

Innovazioni tecnologiche importanti coinvolgono ogni settore cambiando in modo sostanziale non solo il lavoro manuale attraverso l'automazione, ma anche quello intellettuale mediante l'impiego dei sistemi informatici.

Questi sono gli anni connotati dal fenomeno delle grandi ristrutturazioni aziendali e dal sorpasso del settore dei servizi sul settore industriale.

Queste trasformazioni sono favorite da un lungo ciclo economico favorevole nel corso del quale si delineano tutta una nuova serie di rischi che minacciano ogni settore dell'azienda. Quest'ultima, proprio perché protagonista dell'evolversi della società e dell'economia, si trova a dover affrontare problematiche di competitività in un contesto del tutto diverso rispetto al passato, anche recente.

La security deve operare anch'essa una profonda trasformazione per concorrere ad assicurare la competitività delle aziende attraverso il coinvolgimento della propria attività in ogni settore dell'impresa.

Il venir meno delle criticità degli anni settanta facilita questo cambiamento imposto dai nuovi scenari e fanno sì che questa nuova funzione aziendale prenda coscienza di se stessa dotandosi dei mezzi necessari per far fronte alle nuove esigenze.

I nuovi rischi, in questa fase, sono connessi alle grandi trasformazioni che le aziende affrontano per essere sempre più competitive. Assistiamo a fenomeni nuovi quali il "white collar crime" ed il "tampering" assieme a vecchi quali il sabotaggio della produzione o del prodotto, come sempre quando si è in clima di forti tensioni sociali ed economiche.

La necessità di adeguare la funzione di security ai nuovi compiti determina il nascere di iniziative culturali e associative tali da supportare gli sforzi di adeguamento alle nuove realtà che interessano le aziende.

E' alla fine di questa fase ed in funzione di queste esigenze che sorgono l'A.I.P.S.A., Associazione Italiana Professionisti della Security Aziendale, e, contestualmente, SPACE, Centro Europeo per gli Studi sulla Protezione Aziendale, presso l'Università Bocconi di Milano.

Si prende coscienza che le problematiche di security, sino ad ora affrontate soprattutto in chiave emergenziale, dovranno essere sistemizzate, regolamentate e risolte sviluppando piani e politiche operative che ogni azienda dovrà predisporre per mantenere ed accrescere la propria capacità competitiva.

1991 – 2001

Ha inizio una nuova fase determinata dalla caduta dei blocchi contrapposti e dal conseguente insorgere di un nuovo fenomeno che coinvolge ogni settore della vita sociale, politica ed economica: la globalizzazione.

In particolare, la globalizzazione dell'economia determina tutta una serie di nuovi rischi che la funzione di security dovrà contrastare per assicurare la competitività delle proprie aziende minacciate mai come ora anche da agenti esterni che ne compromettono l'integrità e l'incolumità.

Le nuove frontiere della security, come in precedenza, non possono prescindere dagli scenari entro cui è maturato il cambiamento. La caduta dei grandi blocchi ha avuto come corollario l'apertura delle frontiere, i grandi flussi emigratori, l'aumento della concorrenza internazionale non più arginata da dazi e barriere doganali, la continua evoluzione tecnologica e, per quanto ci riguarda da vicino, un faticoso travaglio politico, sociale ed economico.

La necessità di sistemizzare la funzione di security porta all'emanazione, nel 1995, della norma UNI 10459 che per la prima volta nella storia stabilisce i requisiti dei Professionisti della Security Aziendale dando anche la definizione di security aziendale intesa come *"Lo studio e l'attuazione delle strategie, delle*

politiche e dei piani operativi volti a prevenire, fronteggiare e superare eventi in prevalenza di natura dolosa e/o colposa che possono colpire le risorse materiali, immateriali organizzative e umane di cui l'azienda dispone o di cui necessita per garantirsi un'adeguata capacità concorrenziale nel breve, nel medio e nel lungo termine."

Vedremo successivamente, nel dettaglio, la struttura di questa norma che ha dato una svolta decisiva alla sistemizzazione della funzione, definendone confini e competenze.

Nella fase che stiamo esaminando ed in conseguenza dell'emanazione della norma UNI 10459 nasce anche l'esigenza di certificare il possesso dei requisiti indicati nella norma stessa al fine di garantire la professionalità dei security manager, in armonia con i processi di qualità aziendali. Alla fine del 1998 nasce la figura del professionista certificato, attraverso un'attenta valutazione, per titoli ed esami, dell'effettivo possesso dei requisiti previsti dalla norma UNI.

Nel frattempo gli scenari degli anni '90 si modificano velocemente. Gli effetti di una globalizzazione sempre più spinta determinano nuovi fenomeni e fermenti sociali. La competizione si trasforma in **ipercompetizione** ed assistiamo alla progressiva digitalizzazione dell'economia con nuovi rischi sempre più difficili da governare e contrastare.

A questo si aggiunge il fenomeno della così detta "Era multipolare" in cui il potere politico centrale si indebolisce e perde il ruolo di governo e regolamentazione dell'economia. Gli Stati sono sempre più interdipendenti tra loro e contemporaneamente in competizione.

Tutto ciò determina nelle imprese complessità, incertezza ma anche maggiori opportunità per quelle che si attrezzano a competere nella nuova realtà.

In questa fase assistiamo ad una competizione economica di volta in volta definita **globale, totale, offensiva** (Dalle definizioni di Jean e Luttwack). Anche la funzione di security, di conseguenza, si adatta alla nuova contingenza abbandonando il tradizionale atteggiamento "difensivo" per assumere un ruolo più idoneo a contrastare i nuovi rischi e le conseguenti minacce. Prende così corpo quella che viene definita **business security** intesa come *"attività volta ad individuare, analizzare e gestire le minacce e gli illeciti in grado di ledere i fattori chiave del successo, della capacità competitiva e di generazione del valore dell'impresa"*.

Questa definizione, che non contrasta affatto con quella precedente della norma UNI ed anzi la rafforza, ha però il pregio di indirizzare ed orientare l'attività di security anche alla creazione del valore inserendola nei processi aziendali e rendendola dinamica e proattiva rispetto all'evoluzione delle minacce e delle risorse critiche adottando linguaggio e strumenti manageriali comuni alle altre funzioni aziendali.

Tutto ciò ha posto la security in stretta integrazione con gli obiettivi strategici, le strategie ed il processo di pianificazione aziendale in coerenza con i fattori ambientali di riferimento e con uno spiccato orientamento al mercato.

11 settembre 2001 – 2004: gli scenari in essere.

La tragedia delle Twin Towers ha radicalmente mutato la fisionomia di questa nostra epoca e l'ha calata in una nuova era densa di incognite e di pericoli: o perlomeno ci ha resi tutti consci che rischi sino a ieri solo ipotizzabili possono realmente tradursi in eventi che non esito a definire catastrofici.

Siamo nell'era della globalizzazione. Se questo sia o meno un fenomeno perverso da contrastare o da esaltare sono cose che, dal punto di vista professionale, non ci riguardano. Il fenomeno esiste, è irreversibile ed è frutto di una concatenazione di eventi e di una incessante evoluzione tecnologica.

In questo contesto la security dovrà essere preparata ad affrontare e risolvere una serie di nuovi rischi ed anche a gestire con prontezza e professionalità le inevitabili emergenze che potranno insorgere in conseguenza dell'instabilità e della fluidità in cui viviamo.

Questo comporta che in azienda il ruolo del security manager sia ben definito e soprattutto maggiormente supportato e legittimato dal top-management.

La business security, infatti, richiede che la security sia, come abbiamo già visto, sempre più un'attività interfunzionale di supporto a tutti i processi aziendali al fine di mantenere sul mercato la competitività dell'azienda.

Il fenomeno più appariscente che caratterizza questa nuova fase è quello del terrorismo. Questo fenomeno interagisce con un altro, quello della globalizzazione, di cui può considerarsi un'appendice parassitaria.

Sfrutta infatti, per la sua diffusione e per le sue azioni, le indubbie facilitazioni che la globalizzazione assicura in tema di economia, comunicazioni, trasporti, informatizzazione, ecc.

E' così in grado di penetrare agevolmente nel cuore dei più sofisticati e apparentemente protetti centri di potere causando o essendo in grado di causare eventi di portata devastante.

Inevitabilmente il sistema si protegge o cerca di proteggersi determinando una situazione nuova che io definisco di **vischiosità**.

E' lo stesso fenomeno che nel mondo vegetale si verifica quando molte specie di piante si difendono dagli insetti secernendo delle sostanze resinose.

Ora è indubbio che in epoca di globalizzazione e di ipercompetitività questa nuova situazione costituisce una variabile inattesa che potrebbe compromettere anche seriamente la capacità concorrenziale di una azienda, specie se opera in campo multinazionale.

I rallentamenti causati dal rischio terrorismo e, più recentemente da guerre che anche se locali in ambiente globalizzato non lo sono più, interessano in modo particolare ogni settore dell'economia, della finanza, della produzione, della distribuzione, del commercio e cioè di tutti quei comparti che viceversa hanno

avuto dalla globalizzazione un enorme impulso ed una vistosa accelerazione dei processi evolutivi.

Le conseguenze di questi rallentamenti sono quelle che determinano la vischiosità del sistema.

In particolare le cause che ostacoleranno e condizioneranno l'attività delle imprese sono le seguenti:

- l'intensificazione dei controlli al traffico delle persone e delle merci;
- la vigilanza sempre più serrata dei flussi finanziari per evitare che inconsapevolmente alimentino organizzazioni terroristiche;
- la limitazione della diffusione dei prodotti ad alta tecnologia;
- la limitazione ed il controllo degli spazi aerei;
- il controllo materiale del traffico navale in varie zone del pianeta.

Queste ed altre misure fanno sì che le operazioni soprattutto di carattere economico, che sino all'undici settembre si svolgevano con la massima tranquillità, sono ora e lo saranno ancora di più in futuro sottoposte ad una serie di rallentamenti e di condizionamenti che inevitabilmente si tradurranno in perdita o diminuzione di capacità competitiva da parte di molte aziende.

In questo contesto il ruolo della security sarà sempre più strategico in relazione ai compiti che le saranno assegnati per il mantenimento della capacità concorrenziale dell'impresa per cui o entro cui opera.

Sarà infatti anche suo il compito sempre più impegnativo e delicato di analizzare e gestire tutte le cause che determinano la vischiosità e quindi il rallentamento delle attività per mezzo delle quali l'impresa in cui opera realizza la propria mission.

Questa attività dovrà sfociare in una attenta analisi dei rischi non disgiunta dalla gestione delle emergenze e metterà le aziende in grado di evitare le varie "impasse" in cui potrà incorrere il proprio apparato produttivo.

Va da sé che nell'attuale contingenza l'attività principale del security manager sarà quella di intelligence nelle sue varie accezioni e specialità.

Progettare la business-security del futuro significherà soprattutto creare le condizioni perché la propria azienda possa superare ogni genere di difficoltà che l'attuale emergenza internazionale sta determinando.

Queste condizioni si realizzeranno partendo da un attento e scrupoloso esame degli scenari entro cui si svolge l'attività dell'impresa per arrivare a tutta una serie di misure e contromisure che abbiano come fine l'attenuazione o addirittura l'eliminazione della vischiosità che in questo momento ne riduce la capacità

LA GESTIONE DEI NUOVI RISCHI

L'evoluzione dell'ambiente e degli scenari incidono profondamente sui comportamenti delle aziende che hanno come fine ed obiettivo la sopravvivenza e lo sviluppo. Questo ha determinato nuovi scenari competitivi che corrispondono a

nuove scelte strategiche che portano con se nuove opportunità ma anche nuove minacce.

Il nuovo scenario di riferimento, come abbiamo visto nel primo capitolo, è connotato da quattro variabili che sono la **globalizzazione**, l'**ipercompetizione**, la **digitalizzazione dell'economia** e l'**era multipolare**.

La **globalizzazione** è un sistema di mercato che opera senza riferimento ai confini nazionali e si è sviluppato essenzialmente grazie allo sviluppo ed alla diffusione delle nuove tecnologie, alla riduzione delle barriere istituzionali ed allo sviluppo dei mezzi di comunicazione. Tutto ciò si è estrinsecato in una contrazione delle dimensioni spazio-temporali, nella maggiore possibilità di trasferimento di risorse e beni ed anche nella omogeneizzazione della domanda.

L'**ipercompetizione** consiste in un maggiore confronto competitivo fra le imprese in cui le regole della concorrenza vengono costantemente messe in discussione. La sovversione dello status-quo è la chiave per insidiare le posizioni di dominio dei concorrenti rivali con la costante ricerca di nuove opportunità per conseguire vantaggi anche solo su base temporanea. La conseguenza più evidente dell'ipercompetizione è la **criticità del fattore tempo**.

La **digitalizzazione dell'economia** è un fenomeno sempre meno elitario ed in crescita esponenziale perché più di 400 milioni di persone in tutto il mondo hanno accesso ad internet e si prevede che alla fine del 2005 siano più di un miliardo. Nel 1998 Internet ha generato più di 301 miliardi di \$ di fatturato creando più di 1.200.000 posti di lavoro (fonte: Dipartimento del Commercio degli Stati Uniti) e l'economia della rete cresce ad un tasso del 174,5% (fonte: University of Texas). Sempre nel 1998 le aziende americane hanno realizzato più di \$ 43 mld di fatturato b2b on-line ed entro il 2003 un volume di \$ 1.300 mld, pari al 9,4% del fatturato complessivo degli scambi corporate (fonte: The Forrester Report novembre 1998). In Italia più di 14,5 milioni di persone dispongono di un collegamento a Internet (fonte: Il Sole 24 ore del 22.01.01).

L'**era multipolare**, infine, ha determinato una nuova dimensione che si è concretizzata in uno "status" non più dominato esclusivamente dal potere politico ma anche dalla conoscenza e dal capitalismo intellettuale. Gli Stati stanno progressivamente perdendo il tradizionale ruolo di regolamentazione centralizzata dell'economia e si trovano in una situazione di interdipendenza reciproca ma contemporaneamente, di competizione. (L'esempio più vicino a noi è dato dagli Stati componenti l'Unione Europea).

Quali sono le conseguenze e come reagiscono le imprese a questi nuovi scenari?

L'aspetto che maggiormente risalta è quello di una maggiore **complessità** del sistema economico. Ciò determina confini meno netti tra segmenti di mercato, tempi più brevi di difendibilità dei vantaggi competitivi, "confini" dell'impresa meno definiti e maggiore criticità degli intangibles asset rispetto a quelli materiali.

Altra conseguenza è quella dell'**incertezza** che si manifesta con l'instabilità dei vantaggi competitivi legati a fattori di localizzazione, con la volatilità dei mercati finanziari (specie dei titoli tecnologici) con la crisi del sistema creditizio (vedi recenti vicende legate al mercato dei bond), con la riduzione della vita media dei prodotti (non importa quanto sia buono il tuo prodotto: sei solo a 18 mesi dal fallimento "N. Myhrvold, vicepresidente Microsoft") ed infine con l'instabilità socio-politica determinata soprattutto da episodi destabilizzanti di terrorismo.

Agli aspetti negativi si contrappongono maggiori **opportunità** quali l'espansione su nuovi mercati, la riduzione dei tempi di progettazione e di sviluppo dei prodotti ed anche una maggiore circolazione dei capitali (con conseguente maggiore possibilità di finanziarsi sui mercati borsistici).

L'ipercompetizione d'altro canto genera anche una riduzione dei costi mediante la riduzione dei livelli gerarchici (e quindi dei controlli), deleghe sempre più ampie con accorpamento delle responsabilità ed impiego sempre più impegnativo della "business & competitive intelligence".

In questo contesto la risposta delle imprese è stata in un certo senso obbligata per cui ne sono derivate scelte maggiormente rischiose come quella di operare in ambienti e mercati instabili e turbolenti. Altra conseguenza è stata quella di assumere dimensioni e organizzazione più snelle e di ricorrere maggiormente all'outsourcing, al lavoro interinale, al telelavoro ed al decentramento strutturale con elevati investimenti in intangibles assets (tutela marchio, ricerca e sviluppo, informazioni commerciali, brevetti, ecc) ed in nuove tecnologie.

I maggiori investimenti in intangibles assets hanno avuto tuttavia conseguenze positive che si sono tradotte in maggiori proventi da prodotti e servizi, migliore reputazione e immagine, accesso agevolato alle tecnologie di altri, riduzione del contenzioso, blocco dei competitors attualmente sul mercato e barriere nei confronti di coloro che si accingono ad entrarvi ed infine maggiore fedeltà dei propri clienti.

Altra conseguenza del regime di ipercompetizione si è concretizzata in un sistema informativo sempre più complesso ed in una crescente dipendenza dalle risorse umane chiave con tutti i rischi che ne conseguono.

Il risultato è stato il passaggio da un sistema aziendale accentrato alla così detta azienda aperta che utilizza sempre maggiormente le risorse esterne quali

l'outsourcing, i consulenti, i fornitori, i clienti, i distributori, gli enti pubblici, le aziende collegate, i partners, le banche, gli enti finanziari, i telelavoratori, ecc.

Altro fenomeno che si è registrato è quello di una maggiore conflittualità sia all'esterno che all'interno dell'azienda ove i dipendenti agiscono con minore senso di appartenenza, maggiore spirito opportunistico e minore motivazione creando di fatto un deterioramento del clima organizzativo.

Conseguenza della maggiore conflittualità è il manifestarsi di maggiori rischi fra cui la sottrazione da parte di aziende concorrenti di dipendenti chiave con rilascio consapevole e non di informazioni riservate e di know how. Si verificano altresì nuove tipologie di frodi, sempre maggiori casi di computer crimes ed utilizzo non autorizzato di marchi e brevetti.

Tutti gli attacchi alle aziende hanno però un fine comune: danneggiare il suo business. La risposta a questo stato di cose è che le aziende non possono più limitarsi, come sino al recente passato, a tutelare il proprio patrimonio ma anche e soprattutto il proprio business. Questo è **il nuovo impegno della security**, come ho già sottolineato nella prima parte di questa relazione, e consiste, lo ripeto, in una "attività volta ad individuare, analizzare e gestire le minacce e gli illeciti in grado di ledere i fattori chiave del successo, della capacità competitiva e di generazione del valore dell'impresa".

La business security avrà pertanto come prioritarie finalità quella di essere orientata alla creazione del valore dell'azienda, alla responsabilizzazione del management, dovrà essere inserita nei processi aziendali ed essere orientata alla soluzione delle problematiche che dovessero insorgervi, dovrà essere dinamica rispetto all'evoluzione delle minacce e delle risorse critiche e dovrà infine adottare linguaggio e strumenti manageriali comuni alle altre funzioni aziendali.

Per realizzare i propri scopi la business security dovrà agire in stretta integrazione con gli obiettivi strategici, le strategie ed il processo di pianificazione aziendale con particolare orientamento al mercato di riferimento e coerentemente agli obiettivi ed ai valori di fondo dell'azienda. Tutto ciò applicando le tecniche collaudate di analisi e gestione del rischio che prevedono in primis l'analisi strategica del contesto competitivo ed a seguire l'analisi organizzativa dei fattori critici di successo, l'individuazione delle minacce e delle vulnerabilità, la valutazione dei rischi, la definizione delle alternative strategiche di gestione del rischio, la definizione delle contromisure ed il monitoraggio e aggiornamento continuo ai fini dell'apprendimento.

Il tutto si concretizzerà nella realizzazione del piano di security che consisterà nella progettazione globale delle misure di sicurezza necessarie con il fine di

ridurre le vulnerabilità individuate nella fase di analisi dei rischi mediante un approccio che dovrà essere necessariamente sistemico e dinamico.