

Il modello metodologico del Sistema di Misurazione e Valutazione della sicurezza aziendale (MVS)

>> Il Sistema MVS permette di misurare e valutare la sicurezza aziendale (nell'accezione di Security) nei tre domini in cui essa si articola (logico, fisico e organizzativo) mediante: l'elaborazione di un quadro generale sull'infrastruttura di governo della sicurezza attraverso le attività di controllo e di registrazione dello stato di avanzamento dei programmi di protezione aziendali; l'individuazione dei punti deboli di una organizzazione aziendale e la definizione di opportune azioni correttive sotto forma di perimetri di intervento su cui effettuare l'analisi del rischio; l'indicazione delle linee di tendenza e degli esiti prevedibili in assenza di azioni correttive.

L'aspetto innovativo del Sistema MVS è quello di aver dato una risposta all'interrogativo se sia possibile misurare e valutare la sicurezza aziendale al punto che a giugno 2009 è stata depositata in Italia la domanda di brevetto per invenzione industriale.

Peraltro, tra dicembre dello stesso anno e il gennaio del 2011 la metodologia ha vinto due premi innovazione in Finmeccanica.

L'apparente immediatezza semantica del concetto di sicurezza ha generato e continua a generare una indeterminatezza diffusa tale da consentire un utilizzo talvolta improprio, non di rado sfociato in abuso, in una cornice di generale superficialità e sostanziale approssimazione.

A ciò si aggiunge, inoltre, il frequente ricorso a sistemi e soluzioni che privilegiano per lo più il momento qualitativo rispetto a quello quantitativo. Un numero sempre maggiore di addetti ai lavori rigetta la più elementare nozione di costo appellandosi al termine di investimento senza, tuttavia, argomentare adeguatamente tale proposizione.

Ciò che viene proposto è un approccio di analisi del tutto singolare e un metodo originale ed inedito che, traendo ispirazione dai principi della strategia militare e dell'Intelligence, consentono – come già accennato – di delineare un quadro generale circa l'infrastruttura di governo della sicu-

Cristhian Re,

*Finmeccanica Security Governance
e Corporate Security*

rezza, definire le opportune azioni correttive, indicare le linee di tendenza e gli esiti prevedibili in assenza delle azioni suggerite.

LA METODOLOGIA

La metodologia si articola in quattro fasi:

- A. definizione dello scenario (Base di Conoscenza);
- B. compilazione del questionario;
- C. elaborazioni statistiche;
- D. azioni correttive (perimetri di intervento).

A. Definizione dello scenario (Base di Conoscenza)

La Base di Conoscenza è uno speciale database – all’interno del quale possono essere fatti confluire fonti, letteratura attinente alla materia, manualistica, articoli, ecc. – per la gestione della conoscenza di cui facilita la raccolta, la codificazione, la strutturazione, l’organizzazione, la condivisione e la diffusione.

L’aspetto più rilevante di una base di conoscenza è il tipo di dati e informazioni in essa contenuti – diversi a seconda del settore di business in cui opera l’azienda e del contesto cui si fa riferimento – che contribuiscono alla creazione di un sostrato comune.

Un database sensibile al variare della conoscenza, aggiornato e sottoposto a revisione continua, tale da configurarsi come vera e propria spina dorsale lungo la quale corrono i nervi motori del sistema.

Nell’ambito del dominio organizzativo vengono recepite specifiche disposizioni in materia derivanti internamente da: direttive, procedure, istruzioni operative, ecc., ed esternamente da: leggi, regolamenti, standard e convenzioni internazionali, best practice, ecc. Tali disposizioni, che prevedono da parte dell’azienda attività da porre in essere, vengono convertite in controlli puntuali tesi a verificarne l’attuazione (equiparabili a contromisure). L’asset che si vuole proteggere è l’azienda nella sua globalità.

Pertanto, la mancata attuazione di uno o più controlli, aggregati in classi, costituisce una inadempienza che si traduce, in termini di sicurezza, in un vulnus con riflessi sull’intera azienda. Nei domini fisico e logico, invece, si raccolgono quelle soluzioni tecnologiche offerte dal mercato, suggerite da normative varie, imposte dall’azienda, ecc. Tali soluzioni, traducibili anch’esse in contromisure da installare sui componenti, sono aggregate, secondo il criterio dell’omogeneità, in classi

DOMINIO ORGANIZZATIVO

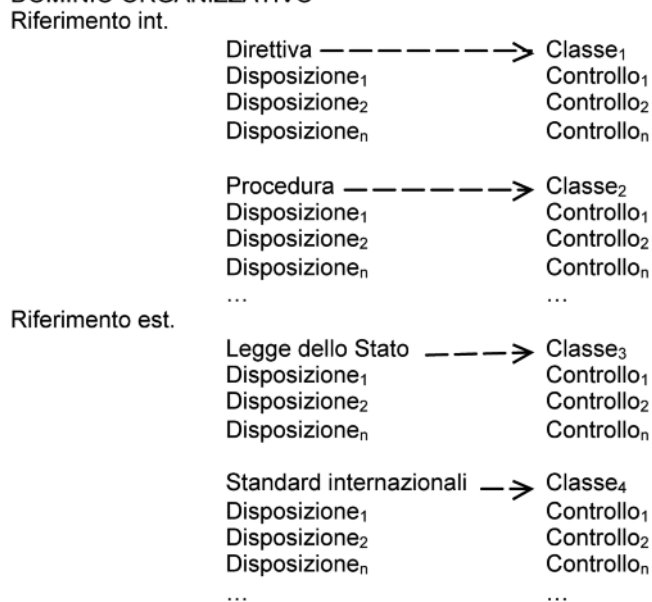


Figura 1

cui viene assegnato un peso specifico sulla base del tasso di intercambiabilità e indispensabilità. Il diagramma sottostante illustra il processo di astrazione appena descritto che dalla base di conoscenza si traduce in un questionario di rilevazione: il questionario di rilevazione, infatti, rappresenta lo strumento veicolante che consente il passaggio dal piano teorico a quello pratico. Esso non solo raccoglie e traduce le istanze ricevute attraverso il già citato processo di astrazione, trasformazione e codificazione, ma rileva altresì i livelli di copertura relativi alle classi di contromisure e ai componenti. Dall’intersezione delle due grandezze oggetto di analisi, componenti e contromisure, ha origine una matrice caratterizzata da pertinenze tecnologiche che

DOMINIO FISICO/LOGICO

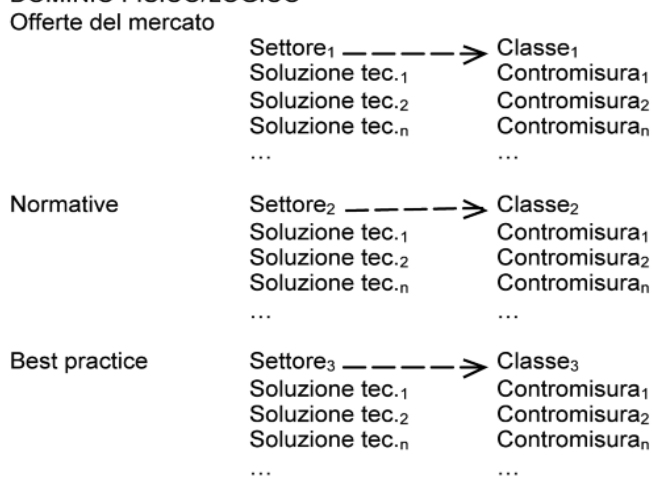


Figura 2

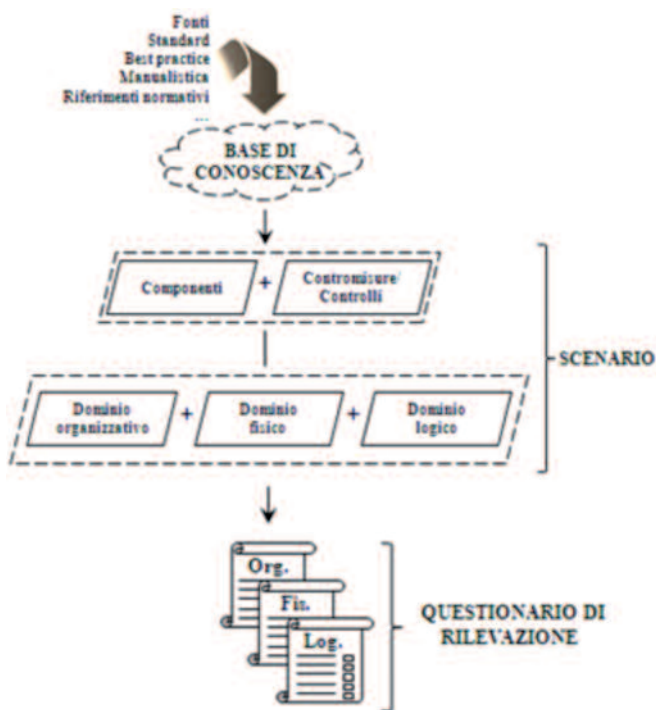


Figura 3

esplicitano l'attinenza di una soluzione tecnologica in relazione a un asset da proteggere. Ancor più chiaramente, la pertinenza tecnologica esprime il legame che intercorre tra la contromisura e il componente.

Le contromisure/controlli, tra loro omogenei o affini per finalità di impiego, sono aggregati in classi, cioè in famiglie, più note in letteratura come funzionalità di sicurezza.

Ciascuna contromisura/controllo, inoltre, assolve a una specifica "funzione", cioè è utilizzata per un preciso scopo. L'insieme delle contromisure pertinenti (cioè applicabili) a un particolare componente determina la pertinenza tecnologica (PT). In ogni classe agisce un fattore di ridondanza ($Fr \leq PT$), vera e propria bilancia del sistema. Esso è il rapporto tra la PF e PT () e indica il tasso di rilevanza delle contromisure definendo, così, la pertinenza funzionale (PF).

Un Fr prossimo o pari a 1 segnala la sostanziale obbligatorietà e indispensabilità di tutte le contromisure contenute all'interno della classe. Di contro, quanto più il valore è lontano da 1 tanto maggiore sarà il grado di "vicarianza", cioè di complementarità e intercambiabilità delle contromisure.

B. Compilazione del questionario

Il compilatore indicherà la presenza (o l'eventuale

assenza) delle contromisure e dei controlli praticati mediante l'assegnazione di un valore (convenzionalmente compreso tra 0 e 1 laddove "tecnologicamente pertinenti") sulla base di due criteri valutativi:

- robustezza/adequatezza ("R");
- efficienza/applicazione ("E").

"R" nei domini fisico e logico è rappresentato dalla robustezza, cioè dal livello di tecnologia della misura di protezione installata che connota il grado di resistenza a un potenziale attacco. Nel dominio organizzativo, invece, è rappresentato dall'adequatezza, cioè dal livello di idoneità e congruità del controllo da porre in essere.

"R" viene espresso per mezzo di un valore che fa riferimento ad una scala di graduazione costituita da tre gradini: basso, medio e alto. I valori 0 e 1 rappresentano i due estremi, rispettivamente: assenza della contromisura ovvero inadeguatezza del controllo e massimo grado di robustezza/adequatezza. Possiamo convenzionalmente associare alla variante basso il valore 0,33 e alla variante medio lo 0,67.

"E" nei domini fisico e logico è rappresentato dall'efficienza, cioè dalla qualità della contromisura di essere davvero funzionante e capace di produrre l'effetto cui essa è destinata. Nel dominio organizzativo, invece, dall'applicazione, cioè dalla reale ed effettiva messa in atto del controllo.

"E" viene espresso per mezzo di un valore che fa riferimento, come per "R", ad una scala di graduazione costituita da tre scalini: poco soddisfacente, discreto e perfetto. I valori 0 e 1 rappresentano gli antipodi, rispettivamente: totale mancanza di efficienza della

		R ↑		
		Alto	Medio	Basso
VALORE	Alto	0,33	0,67	1
	Medio	0,22	0,44	0,67
	Basso	0,11	0,22	0,33
		0	E →	
		Poco soddisfacente	Discreto	Perfetto
		VALORE		

Figura 4

contromisura ovvero controllo non applicato e il perfetto stato di efficienza/applicazione. Anche in questo caso, possiamo associare alla variante poco soddisfacente il valore 0,33 e alla variante discreto lo 0,67.

Pertanto, il valore indicante la presenza della contromisura/controllo (V_{CM}) è funzione di "R" ed "E" secondo la relazione:

$$V_{CM} = f(R, E)$$

C. Elaborazioni statistiche

In questa fase avviene il complesso processo di elaborazione degli indici di copertura.

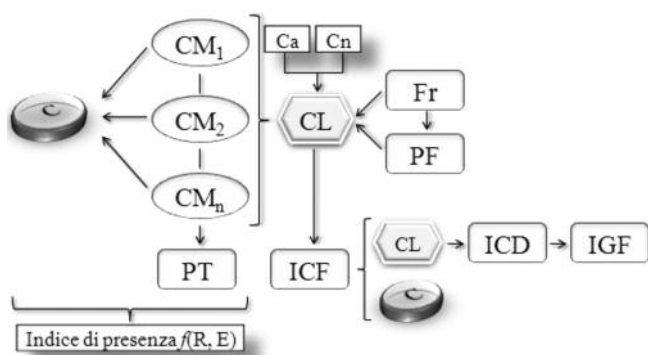


Figura 5

La grafica vettoriale mostra due forze catalizzatrici, componente (C) e classe di contromisure (CL). Sul componente insistono n contromisure (CM) – aggregate in classi ed espresse in funzione dei due criteri valutativi: robustezza/adequatezza (R) e efficienza/applicazione (E) – la somma delle quali determina una pertinenza tecnologica (PT) al cui interno non è raro si verifichi una "vicarianza" (intercambiabilità, complementarità tra contromisure) rappresentata mediante uno specifico fattore di ridondanza (Fr).

Sulla classe, invece, agiscono tre distinti elementi:

- il già citato Fr che, depurando PT, definisce una pertinenza funzionale (PF);
- il coefficiente di abbattimento (Ca) che, in assenza di contromisure ritenute imprescindibili all'intero della propria classe, interviene durante la fase di calcolo dell'indice di copertura funzionale (ICF) correggendone il valore;
- il coefficiente di normalizzazione (Cn) che, qualora vi

fosse una sola contromisura tecnologicamente pertinente all'interno della classe in relazione a un dato componente, modifica il valore di Fr. Gli ICF così elaborati afferiscono sostanzialmente a due entità:

- i singoli componenti e insiemi di componenti;
- le classi di contromisure. Questi ultimi, ulteriormente aggregati ed elaborati, originano indici di copertura per i tre domini di sicurezza (ICD) che a loro volta generano un indice di copertura globale funzionale (IGF) riferito alla Azienda nella sua interezza.

Calcolati gli indici di copertura sarà compito dell'analista di sicurezza quello di rendere intelligibili per il decisore i dati prodotti. Utilizzando una tabella metrica in base alla quale si fissa convenzionalmente al 60% lo spartiacque tra ciò che costituisce una situazione critica (cioè di non copertura) da ciò che, invece, non lo è, si avrà quanto segue:

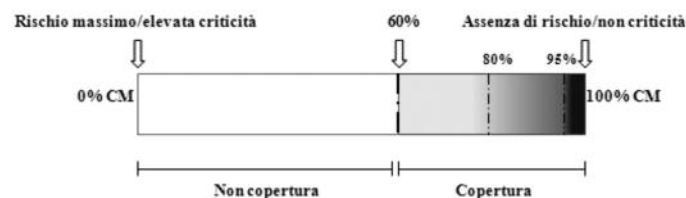


Figura 6

Alla prima linea di demarcazione ne seguono altre che indicano ulteriori soglie di progressiva adeguatezza all'interno di quella che si reputa essere un'area di copertura (ad esempio 80% e 95%).



Figura 7

Le percentuali risultanti per i tre domini di sicurezza saranno confrontati con i valori di soglia appartenenti

alla tavola sottostante e, in funzione della loro collocazione, sarà possibile formulare un sintetico giudizio sul profilo di sicurezza complessivo aziendale:

SOGGIE	DOMINIO 1	DOMINIO 2	DOMINIO 3	PROFILO DI SICUREZZA
	≤60%	≤60%	≤60%	Inadeguato
	≤60%	≤60%	≥60%	Inadeguato
	≤60%	≥60%	≥60%	Inadeguato
	≥60%≤80%	≥60%≤80%	≥60%≤80%	In fase di graduale adeguamento
	≥60%≤80%	≥60%≤80%	≥80%	In fase di graduale adeguamento
	≥60%≤80%	≥80%	≥80%	In fase di graduale adeguamento
	≥80%≤95%	≥80%≤95%	≥80%≤95%	Prossimo all'adeguamento
	≥80%≤95%	≥80%≤95%	≥95%	Prossimo all'adeguamento
	≥80%≤95%	≥95%	≥95%	Prossimo all'adeguamento
≥95%	≥95%	≥95%	Adeguato	

Figura 8

D. Azioni correttive (perimetri di intervento)

Quest'ultima fase si differenzia dalle tre precedenti poiché meno organica in ragione della bivalenza delle sue finalità. Infatti, essa oltre a chiudere il ciclo della rilevazione, apre nel contempo all'attività di analisi del rischio grazie all'oggettiva individuazione di aree di scopertura (veri e propri punti deboli) ordinate e gerarchizzate in perimetri di intervento. La classificazione dei componenti – che costituiranno i futuri perimetri di intervento – avviene utilizzando la tavola di seguito riprodotta che si presenta come una matrice i cui elementi sono in un piano cartesiano. In ascisse è riportata una scala finalizzata ad esprimere il posizionamento dei componenti in relazione alla loro prossimità alla missione aziendale. I suoi valori indicano non solo la collocazione nel contesto aziendale ma anche il peso che rivestono:

CONTRIBUZIONE AL SUCCESSO/COMPETITIVITÀ DELL'AZIENDA	Determinante	5	10	15	20	25
	Rilevante	4	8	12	16	20
	Influente	3	6	9	12	15
	Poco influente	2	4	6	8	10
	Marginale	1	2	3	4	5
		Struttura generale	Struttura di controllo	Supporto alla gestione	Supporto alla missione	Missione d'impresa
POSIZIONAMENTO RISPETTO ALLA MISSIONE AZIENDALE						

Figura 9

In ordinate è espressa un'analoga scala, crescente verso l'alto, finalizzata alla classificazione del componente mediante la valutazione del contributo al successo/competitività raggiunta dall'azienda, in termini di: marginale, poco influente, rilevante o determinante. La determinazione della criticità si realizza stabilendo per ciascun componente prima il posizionamento rispetto alla missione e, successivamente, il contributo al successo/competitività raggiunta dall'azienda. Il valore del componente (Vc) risulta funzione dei valori del parametro1 (posizionamento rispetto alla missione aziendale – Pm) e del parametro2 (contribuzione al successo/competitività dell'azienda – Cs) secondo la relazione:

$$Vc = Pm * Cs$$

Una volta censiti e classificati, i componenti saranno poi aggregati secondo i più disparati criteri (funzionalità, rilevanza, finalità, contromisure installabili, ecc.) in modo da costituire degli insiemi omogenei. Se si accostassero i diagrammi di flusso relativi al Sistema MVS e all'analisi del rischio si noterebbero due sezioni (in tratteggio) che evidenziano contiguità metodologiche.

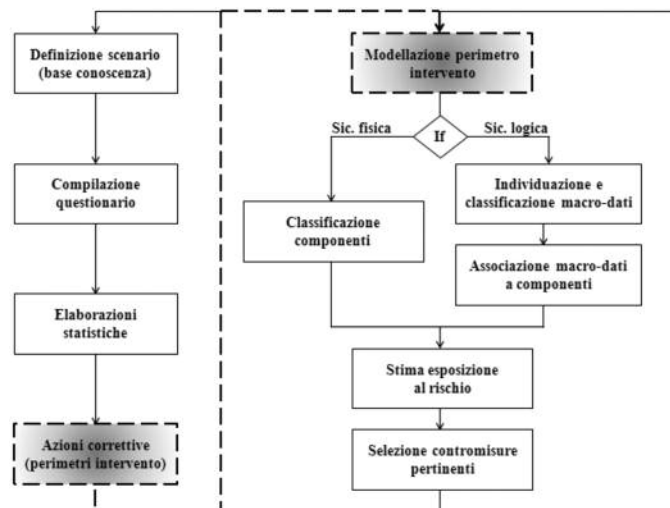


Figura 10

In un processo di analisi del rischio la modellazione di un perimetro di intervento costituisce l'attività decisamente più complessa e più onerosa in termini di risorse, energie, tempo. Stabilire quali elementi siano da includere e quali altri, invece, siano da escludere da

un eventuale perimetro, delimitandone esattamente i confini, non è cosa facile né immediata. Se si raffigurasse l'analisi del rischio come una scala a quattro gradini, il sistema collocherebbe l'analista di sicurezza direttamente sul secondo scalino con evidenti vantaggi non solo di natura economica.

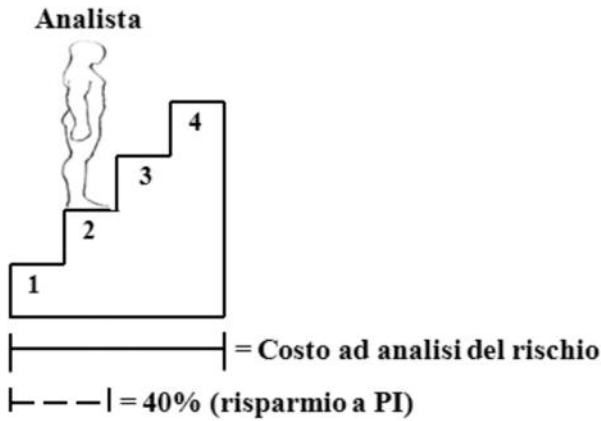


Figura 11

L'individuazione di un perimetro di intervento proveniente dall'interno della società e non dall'esterno (ad esempio con il contributo di società terze) permette una migliore aderenza alle specifiche esigenze interne aziendali, una maggiore tutela delle informazioni sensibili (incalcolabile il danno in caso di perdita o sottrazione) e una più proficua ottimizzazione delle risorse.

Nel dominio della sicurezza fisica quanto descritto non necessita di ulteriore spiegazione; ogni insieme costituisce un perimetro su cui poter effettuare un'analisi del rischio. Sarà compito dell'analista escludere, eventualmente, quei componenti caratterizzati da un alto livello di copertura, da bassa criticità o da ridotta significatività.

Per quanto riguarda, invece, l'ambito logico, è noto che è il componente a ereditare la classe di criticità del macrodato e non viceversa. Tuttavia, si può affermare che il rapporto tra componenti e macrodati è 1:n, cioè su un componente di natura logica (ad esempio: server, lap top, workstation, ecc.) potrebbero risiedere indifferentemente in tutte le tipologie di macrodati (come quelli del personale dipendente, di marketing, commerciali, finanziari, tecnici, ecc.).

Pertanto, definiti aprioristicamente dei perimetri standard verso cui orientarsi, l'analista di sicurezza interverrà successivamente per associare il macrodato al componente, come raffigurato nello schema:

CONCLUSIONI

I margini consentiti all'esposizione hanno suggerito di adottare rigidi criteri di selezione degli argomenti (tra la molteplicità di quelli offerti correlati, peraltro, anche ad altri temi).

Ne è derivato, dunque, un approccio orientato a privilegiare la sintesi e a ricercare una visione di insieme il più possibile idonea a rappresentare il quadro generale, spesso sacrificando dettagli non trascurabili come formule, grafici, tavole, algoritmi, ecc. a vantaggio, invece, di diagrammi e figure.

Il modello metodologico, connotato da un complesso gioco di pesi e contrappesi – qui solo sommariamente accennato si snoda lungo le pagine del volume *La Misura della Sicurezza. Sistema per la misurazione e la valutazione della sicurezza aziendale*, cui si rimanda per gli opportuni approfondimenti.

Si è certi, tuttavia, di aver fornito quegli elementi utili per rispondere in maniera affermativa al quesito iniziale da cui è partiti, cioè se la sicurezza, alla stregua di altre grandezze, sia una realmente misurabile.

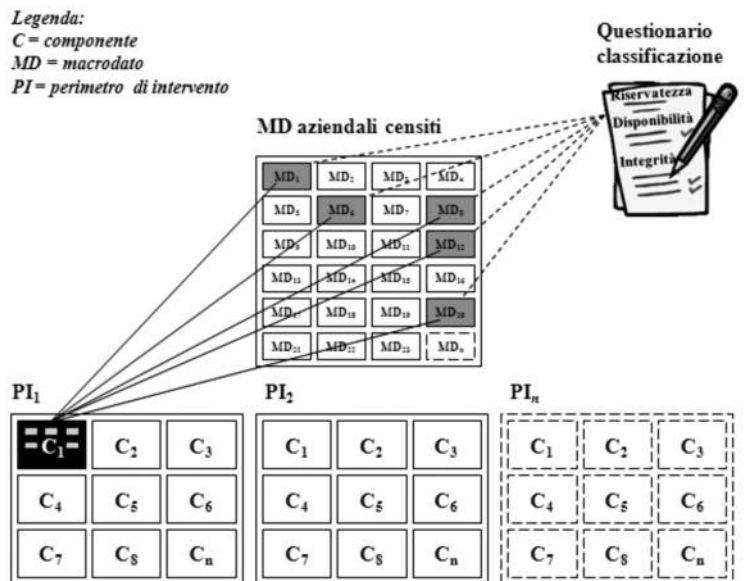


Figura 12