

## **MAGERIT: una metodologia europea per l'analisi e la gestione dei rischi legati alle informazioni**

Articolo pubblicato su "ICT Security" n. 59, Ottobre 2007

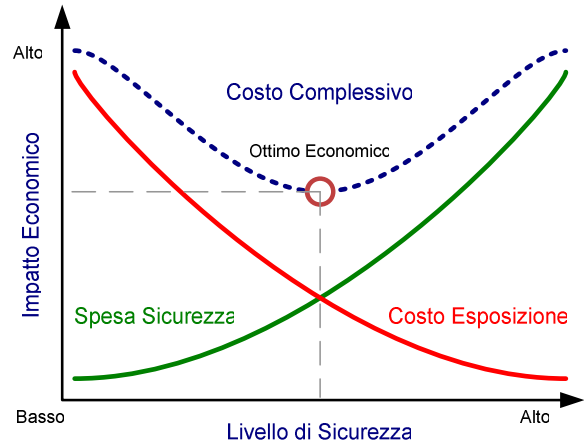
### **Introduzione**

MAGERIT (Metodologia di Analisi e Gestione dei Rischi per l'Information Technology) è una metodologia sviluppata in Spagna per il Ministero della Pubblica Amministrazione nazionale a partire dal 1997 da due enti di tutto rispetto: il Centro Nazionale di Intelligence e il Centro Crittografico Nazionale. Nel 2005 è stata pubblicata la sua seconda versione, di natura aperta come la prima ma affinata nella struttura e nell'impostazione, la quale mette a frutto otto anni di applicazione sia nel settore pubblico che in quello privato. La metodologia è liberamente disponibile in spagnolo, inglese e, più recentemente, in italiano.

Gli obiettivi che Magerit si prefigge coincidono con quelli tradizionali per l'attività di Information Security Risk Management, ovvero fondamentalmente:

1. identificare e quantificare i rischi a cui l'organizzazione in esame è soggetta
2. guidare gli investimenti per la sicurezza volti a ridurre tali rischi ad un livello accettabile

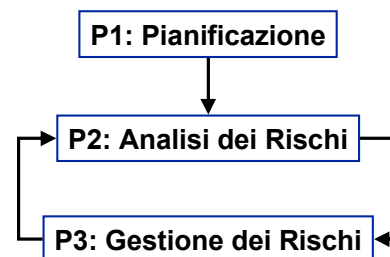
In particolare, lo scopo del secondo punto è di individuare e realizzare un livello di sicurezza accettabile applicando una logica di costi-benefici. Il grafo successivo esemplifica visivamente questo aspetto, sottolineando l'obiettivo di raggiungere la massima efficacia negli investimenti per la sicurezza. Il *costo dell'esposizione* rappresenta la spesa (derivante da fermi macchina, avarie e più generalmente incidenti) che si stima di affrontare, ovvero il rischio economico, che sommata agli investimenti per la sicurezza dà il *costo complessivo*.



### **Metodologia**

Il processo di Analisi e Gestione dei Rischi (o Trattamento dei Rischi secondo alcuni riferimenti) è formato da un'insieme di attività che richiedono preparazione organizzativa, tecnica e comunicativa. La sua conduzione, specie in realtà medio-grandi, deve essere assegnata ad un team (interno o esterno) di persone preparate professionalmente e dotate di strumenti ed autorizzazioni appropriate. Dato che in essa sono coinvolte pesantemente attività di stima di eventi futuri (*minacce*) e di valutazione degli scenari derivanti (*impatti*), risulta molto difficile avere dei risultati assolutamente precisi. Tale obiettivo diventa ancora più difficile se non si seguono delle metodologie ben definite ma soprattutto collaudate e consolidate, in virtù delle quali è possibile anche paragonare i risultati ottenuti per realtà simili o per la stessa realtà in tempi diversi.

La metodologia Magerit si articola in tre processi principali:



Come si può vedere dallo schema, P2 e P3 sono processi ciclici. Questo perché il Risk

Management deve essere un'attività continua nel tempo e all'analisi di realtà che cambiano corrispondono contromisure di gestione per garantirne la perdurante sicurezza.

Si procederà ora ad una rapida illustrazione dei processi (P) e delle relative attività (A) centrali di Magerit.

**P1: Pianificazione**

L'obiettivo principale di questo processo è stabilire una traccia generale di riferimento valida per tutto il progetto. Le attività codificate al suo interno sono:

- A1.1: Studio dell'opportunità
- A1.2: Determinazione dell'ambito del progetto
- A1.3: Pianificazione del progetto
- A1.4: Lancio del progetto

**P2: Analisi dei Rischi**

Questo processo costituisce il cuore di Magerit e la sua corretta applicazione condiziona validità ed utilità di tutto il progetto. L'identificazione e la stima degli asset e delle possibili minacce che li

interessano rappresentano un compito complesso che comprende:

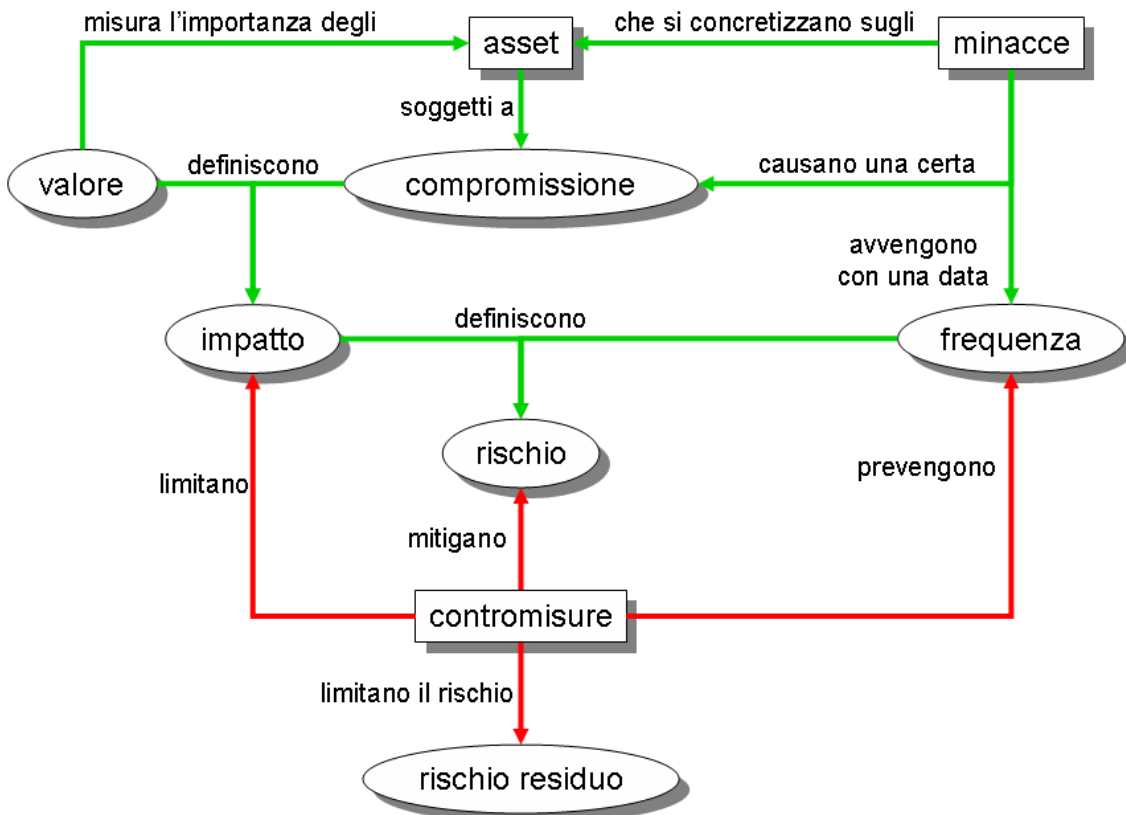
- A2.1: Caratterizzazione degli asset
- A2.2: Caratterizzazione delle minacce
- A2.3: Caratterizzazione delle contromisure
- A2.4: Stima dello stato di rischio

**P3: Gestione de Rischi**

Sono qui trattati gli impatti e i rischi identificati nel processo precedente. Per affrontare i rischi considerati inaccettabili si elabora un piano di sicurezza che corregga la situazione attuale. Tale piano ordina ed organizza nel tempo le azioni destinate a portare lo stato di rischio ad un livello accettabile ed approvato dalla direzione. Questo processo si sviluppa attraverso le seguenti attività e compiti:

- A3.1: Presa di decisioni
- A3.2: Piano di sicurezza
- A3.3: Esecuzione del piano

Per avere meglio l'idea di come si struttura il processo di Analisi e Gestione dei Rischi seguendo Magerit e di quali sono le sue



caratteristiche più innovative, si considerino P2 e P3 nello schema riassuntivo a lato.

P2 ha inizio creando un modello degli asset (in alto nella figura), definendone il tipo, organizzandoli in livelli e collegandoli attraverso relazioni di dipendenza. Quindi si passa alla loro valorizzazione, che può essere qualitativa (basso, medio, alto) o quantitativa (in Euro). La valorizzazione può essere effettuata per ogni dimensione di sicurezza rilevante (e.g. disponibilità, riservatezza, integrità, autenticità ...). A questo punto, seguendo le frecce nella figura, si individuano le minacce applicabili e le si associa una frequenza di accadimento atteso, in base allo storico del sistema in esame o dell'ubicazione, e una compromissione in percentuale. Questa rappresenta il livello di danno rispetto al valore dell'asset che il concretizzarsi della minaccia può causare.

Fatto questo si possono calcolare gli impatti, ovvero i danni potenziali derivanti da una minaccia e infine i rischi, ovvero gli impatti bilanciati dalla frequenza stimata per ogni minaccia. Questo chiude il processo di Analisi dei Rischi (P2).

La Gestione dei Rischi (P3) introduce la valutazione delle contromisure, ovvero il loro effetto di riduzione della frequenza e/o della compromissione rispetto a una o più minacce, proporzionalmente al livello di efficacia di cui si è dato credito alla contromisura in questione.

Si ottengono quindi gli impatti e i rischi residui, calcolabili secondo un metodo cumulativo e un metodo riflesso. La differenza fra questi metodi tra loro complementari è strettamente connessa con il concetto di dipendenze tra asset.

Quest'ultima permette la propagazione del valore degli asset e delle minacce a cui sono soggetti, in modo da rendere più verosimile l'analisi e la modellizzazione di sistemi complessi, anche laddove dotati di numerose interconnessioni.

La metodologia è illustrata in tre "libri" la cui versione completa in spagnolo e inglese si trova sul sito originale:

<http://www.csi.map.es/csi/pg5m20.htm>

oppure il solo libro della metodologia (per ora!) sul mirror ufficiale italiano

<http://www.sgsi.net>.

Il suo impiego può essere inquadrato in una serie di norme, leggi o regolamenti, a partire dai Sistemi di Gestione per la Sicurezza delle Informazioni (ISO/IEC 27001, ex BS 7799 e ISO 17799), ed è coerente con la norma in fase finale di sviluppo ISO/IEC 27005 sull'Information Security Risk Management e ancora:

- D.lgs.196/2003 Testo unico sulla Privacy, Allegato B punto 19.3
- International Convergence of Capital Measurement and Capital Standards (Basilea 2), part 2 sect. V
- Bollettino di Vigilanza della Banca d'Italia Luglio 2004, parte 2 punto 3.1

Vale la pena di sottolineare che anche l'analisi di impatto, universalmente riconosciuta come necessaria per la continuità operativa, è assimilabile ad un processo di gestione dei rischi legati alla sicurezza delle informazioni se i servizi in questione sono basati su sistemi informativi o se, più semplicemente, si considerano i processi in base al flusso di informazioni. In entrambi i casi la gestione dei rischi è focalizzata su tutte le minacce e le vulnerabilità che possono andare a causare un impatto sulla disponibilità degli asset.

Magerit è attualmente molto utilizzata in Spagna, sia da utenti istituzionali come il Ministero delle Pubbliche Amministrazioni, della Difesa, dell'Agricoltura e dalla Zecca sia da utenti privati tra cui diverse aziende di consulenza. Impiegata anche dalla NATO, si sta diffondendo in Francia e Ungheria, mentre in Italia sta venendo testata, tra le altre, da un'importante Banca e da una software house certificata ISO/IEC 27001.

Stanno inoltre partendo nel nostro paese i primi corsi rivolti al suo impiego pratico.

## **PILAR (già EAR)**

PILAR, acronimo di "Procedura Informatico-Logica per l'Analisi dei Rischi" è uno strumento di supporto sviluppato dietro specifica del Centro Nazionale di Intelligence spagnolo per supportare l'analisi dei rischi di sistemi informativi seguendo la metodologia Magerit. Fino a metà del 2007 la release destinata al mercato privato era

denominata "EAR" mentre quella rivolta alle istituzioni era nota come "PILAR", ma si è recentemente deciso di uniformare la denominazione del prodotto.

Questo software di supporto è scritto in linguaggio Java ed è un'applicazione standalone, adatta ad un impiego semplice ed economico, sia per ambienti Windows-based che Unix-based.

I file di analisi sono di dimensioni ridotte (nell'ordine dei 50Kb) e protetti dall'uso non autorizzato. Le analisi supportate da PILAR sono quattro, ovvero:

- Analisi dei Rischi quantitativa
- Analisi dei Rischi qualitativa
- Analisi d'Impatto (BIA) qualitativa
- Analisi d'Impatto (BIA) quantitativa

I progetti sono impostati prevedendo la possibilità di realizzare scenari di simulazione di tipo "what if".

L'impiego pratico di PILAR è facilitato da funzioni di assistenza all'analista di notevole efficacia (quali i set predefiniti di minacce valorizzate e di contromisure), generando una reportistica varia, in formato sia testuale che grafico. Include infine supporto nativo della norma ISO/IEC 27002 (ex 17799), del d.lgs 196/2003 e di altri schemi.

Una demo in italiano del prodotto, di natura commerciale a differenza della metodologia, è scaricabile dal sito <http://www.sgsi.net>.

## Confronto con altre metodologie

Il sito web di ENISA, l'agenzia europea per la sicurezza delle reti e delle informazioni, riporta un interessante catalogo delle più diffuse metodologie di gestione dei rischi e dei relativi strumenti accessibile alla seguente pagina:

[http://www.enisa.europa.eu/rmra/rm\\_home.htm](http://www.enisa.europa.eu/rmra/rm_home.htm)

Magerit e PILAR sono in essa censiti e quindi confrontabili a piacimento, cosa che verrà di seguito schematizzata prendendo in considerazione le due metodologie più diffuse nel vecchio continente: la proprietaria e solida CRAMM e l'open-source EBIOS.

### CRAMM

Vantaggi rispetto a Magerit:

- maggiore base di utenza
- più lunga presenza sul mercato

Svantaggi rispetto a Magerit:

- non localizzato in lingua italiana
- compliance verso meno norme internazionali
- non integrabile con altri strumenti
- maggiore specializzazione richiesta per l'impiego

### EBIOS

Vantaggi rispetto a Magerit:

- disponibilità di tool di supporto open

Svantaggi rispetto a Magerit:

- non localizzato in lingua italiana
- minore supporto disponibile per gli utenti

Andando poi a considerare anche i relativi strumenti di supporto, il cui impiego si rende necessario per esaminare realtà estese e strutturate, si evidenziano altri aspetti la cui valutazione lasciamo però al lettore, non essendo questo lo scopo del presente articolo.

## Conclusioni

La diffusione di metodologie e strumenti per la gestione dei rischi legati alla sicurezza delle informazioni attinenti a linee guida e norme internazionali è di primaria importanza per portare questo processo dall'essere un'arte oscura, appannaggio di pochi "guru", a seguire un approccio di impronta più scientifica e sempre verificabile.

La soggettività, che per forza di cose è coinvolta sia al fine di raggiungere dei risultati sia per prendere delle decisioni, difficilmente potrà mai essere eliminata. Tuttavia un suo ridimensionamento e inquadramento all'interno di metodi collaudati non può che contribuire molto alla precisione dei risultati ottenuti.

*Fabio Guasconi,  
Consulente indipendente per la Sicurezza  
delle Informazioni*

tel. +39.329.46.56.930

[fabio.guasconi@sgsi.net](mailto:fabio.guasconi@sgsi.net)

[www.sgsi.net](http://www.sgsi.net)