



MEHARI 2007

Introduzione alla metodologia

MEHARI è un marchio registrato dal CLUSIF

Ringraziamenti

Il CLUSIF ringrazia Jean-Philippe Jouas e Jean-Louis Roule, che hanno scritto questa introduzione alla metodologia MEHARI per la gestione della sicurezza informatica, e ne hanno autorizzato la pubblicazione.

Si ringrazia anche Massimiliano Manzetti e il CLUSIT per aver accettato di occuparsi della traduzione italiana .

1. Introduzione

MEHARI (**ME**todo **H**armonisato de **A**nalisi del **R**ischio) è stato originariamente pensato, e viene costantemente aggiornato, come sostegno per i Responsabili della Sicurezza Informatica nel compito di gestire la sicurezza delle informazioni e dei sistemi informativi.

Questa presentazione è indirizzata principalmente ai professionisti della sicurezza informatica, ma anche agli auditor e ai Risk Manager che condividono, in larga misura, le stesse preoccupazioni.

Lo scopo di questo documento è descrivere l'utilizzo della metodologia MEHARI. La documentazione messa a disposizione contiene anche una descrizione più completa del metodo e dei relativi strumenti, e in particolare:

- una presentazione dei concetti e del funzionamento di MEHARI
- tre guide all'utilizzo, rispettivamente per l'analisi del contesto aziendale, la diagnostica dei servizi di sicurezza e l'analisi del rischio
- dei manuali di riferimento (servizi di sicurezza e scenario dei rischi) e delle basi di conoscenza.

L'obiettivo di MEHARI è mettere a disposizione una gamma di strumenti specificamente progettati per la gestione della sicurezza. Ciò si concretizza in un insieme di azioni che hanno degli obiettivi specifici.

Alcuni esempi sono:

- l'elaborazione e sviluppo dei piani di sicurezza, o di linee guida strategiche;
- la realizzazione di regole e/o policy di sicurezza, che raggrupperemo sotto il nome di "Infrastruttura di riferimento per la sicurezza informatica" ("security reference framework");
- l'effettuazione di valutazioni (assessment) rapide o approfondite dello stato della sicurezza;
- la valutazione e gestione del rischio;
- la gestione della sicurezza nell'ambito dello sviluppo e della gestione di progetti;
- la consapevolezza e formazione sulle tematiche della sicurezza;
- la gestione operativa della sicurezza e le conseguenti azioni di monitoraggio e controllo.

Queste e altre azioni per la gestione della sicurezza, e le loro varianti, non sono esaustive ma, al contrario, ulteriori attività possono essere realizzate contestualmente o successivamente, in funzione di necessità puntuali o permanenti, indipendentemente le une dalle altre o come parte di un progetto integrato.

Inoltre, le medesime azioni di gestione della sicurezza possono essere realizzate in modo differente in base a:

- la maturità e consapevolezza dell'azienda, e del personale dipendente, sulle tematiche della sicurezza informatica;
- il livello di management da coinvolgere nelle decisioni relative alla sicurezza informatica;
- la cultura dell'impresa: gerarchica e tecnocratica (esistono regole e sono applicate) o, al contrario, decentrata e responsabilizzante..

Fatte queste distinzioni, è fondamentale trovare all'interno di un insieme metodologico gli strumenti adatti ad ogni situazione, e che tali strumenti siano coerenti e correlati tra loro di modo che si completino senza duplicazioni di attività e ulteriori carichi di lavoro.

MEHARI propone questo insieme metodologico coerente facendo appello a basi di conoscenze appropriate, capaci di accompagnare i manager dell'azienda, i responsabili della sicurezza e gli altri attori coinvolti nella riduzione del rischio nei loro diversi compiti e attività.

L'obiettivo principale di questa presentazione è descrivere l'utilizzo che è possibile fare di MEHARI. Alla fine di questo documento, viene anche illustrato il posizionamento di MEHARI rispetto alle principali norme internazionali.

2. Utilizzo di MEHARI

MEHARI è, prima di tutto, un metodo di analisi e gestione del rischio..

Ciò vuol dire che MEHARI, e l'insieme delle sue basi di conoscenze, sono costruite per permettere una analisi precisa dei rischi, quando ciò sarà giudicato necessario, senza pertanto imporre l'analisi del rischio come politica di gestione prioritaria.

In effetti la gestione della sicurezza è un processo o una attività che si evolve nel tempo e le decisioni manageriali non sono della stessa natura se l'azienda non ha ancora fatto nulla in tema di sicurezza informatica o se, al contrario, ha già compiuto degli sforzi sostanziali.

Quando si è ai primi passi nell'affrontare il tema della sicurezza informatica, sarà senza dubbio utile fare una valutazione dello stato attuale della misure e policy di sicurezza e poi comparare questa situazione rispetto a best practice o metodologie consolidate per mettere in evidenza il gap da colmare.

Successivamente, fatta questa valutazione e presa la decisione di implementare un'organizzazione per la gestione della sicurezza, delle azioni concrete devono essere pianificate. Queste decisioni, che solitamente saranno organizzate in piani, linee guida, referenze o policy di sicurezza, dovranno essere prese nel quadro di un approccio strutturato. Un tale approccio può essere basato su un'analisi del rischio, o includere dei concetti di rischio, ma tutto ciò non è obbligatorio. Esistono delle altre vie, quali il confronto con una "norma", norma che sia interna, professionale o interprofessionale.

Tuttavia, a questo punto, e senza parlare di una vera analisi del rischio, si pone la questione dell'analisi del contesto aziendale rispetto alle problematiche della sicurezza. Spesso, infatti, quale che sia il modo con cui la decisione di gestire la sicurezza viene presa, il decisore ultimo, colui che dovrà allocare il budget corrispondente, si chiederà "è veramente necessario?". Senza un'analisi preliminare del contesto aziendale (area interessate, minacce, costi-benefici etc.) e senza consenso su questo punto, molti dei progetti di sicurezza vengono abbandonati o respinti.

Spesso successivamente, ma a volte contemporaneamente all'avvio di un progetto di sicurezza informatica, ci si domanda quale sia il livello di rischio al quale è esposta l'azienda (o l'organizzazione), e la questione, precisamente, viene posta in questi termini : "sono stati identificati i rischi ai quali l'organizzazione è esposta e ci si è assicurati che il loro livello sia accettabile?". Questa domanda può, inoltre, essere posta in termini generali o nel quadro limitato d'un nuovo progetto. Bisognerà, allora, utilizzare un metodo di analisi del rischio.

Il principio sul quale è fondato MEHARI è che gli strumenti necessari a qualunque tappa dello sviluppo del sistema di gestione della sicurezza devono essere coerenti, vale a dire che i risultati acquisiti ad uno stadio devono poter essere utilizzati nelle fasi successive.

L'insieme di strumenti e moduli della metodologia MEHARI, concepiti per poter supportare l'analisi del rischio, sono utilizzabili indipendentemente gli uni dagli altri, in tutte le fasi dello sviluppo del sistema di gestione della sicurezza, nell'ambito delle differenti modalità di gestione, e garantiscono la coerenza dell'insieme delle decisioni.

Questi differenti moduli e strumenti, che sono descritti brevemente di seguito, comprendono dei moduli di valutazione della sicurezza, un modulo di analisi del contesto aziendale e un metodo di analisi del rischio con i suoi strumenti associati.

2.1. *La diagnosi della sicurezza*

MEHARI presenta due moduli di valutazione (assessment) della sicurezza :

- Un modulo di diagnosi veloce¹
- Un modulo di diagnosi approfondita

In un caso e nell'altro l'obiettivo è di valutare il livello di sicurezza. In pratica, si valuterà lo stato dei servizi di sicurezza. E' chiaro che l'accuratezza dei risultati dipenderà dal livello di approfondimento dell'analisi.

Il primo modulo è utilizzabile ad un primo approccio per mettere in evidenza le debolezze maggiori. I servizi di sicurezza esaminati sono gli stessi che nella diagnosi approfondita, ma le domande mirano a verificare se la funzione di sicurezza è realizzata, senza controllare se essa presenti delle vulnerabilità. In questo caso, le vulnerabilità messe in evidenza lo sono certamente, i punti di forza eventuali, invece, non possono essere garantiti.

Il modulo di diagnostica approfondita ricerca, in dettaglio, tutte le vulnerabilità possibili di ogni servizio di sicurezza. Costituisce una base di valutazione, può essere il supporto di una analisi del rischio.

La coerenza di questi due moduli permette di partire dal primo e di approfondire, in qualunque momento, quei fattori su cui si ritenga utile avere ulteriori assicurazioni.

Questi moduli di analisi possono essere utilizzati in diversi modi.

2.1.1 L'analisi della sicurezza, elemento dell'analisi del rischio

MEHARI propone un metodo strutturato di analisi del rischio che sarà presentato più avanti.

Diciamo semplicemente, a questo livello, che il modello di rischio prende in considerazione dei fattori di riduzione del rischio, precisamente concretizzati da servizi di sicurezza.

L'analisi approfondita di questi servizi sarà, quindi, al momento dell'analisi del rischio, un elemento importante di assicurazione che i servizi adempiano bene al loro compito, e ciò è essenziale perchè l'analisi del rischio sia credibile.

2.1.2 La pianificazione della sicurezza basata sull'analisi delle vulnerabilità

Un approccio abbastanza comune consiste nel progettare piani d'azione direttamente a partire da un'analisi dello stato della sicurezza.

I processi di gestione della sicurezza per l'analisi dello stato dei servizi di sicurezza è estremamente semplice : si esegue una valutazione e si decide di migliorare tutti i servizi che non hanno un livello di qualità sufficiente.

L'utilizzazione di un'analisi preliminare del contesto aziendale³ è prevista in un apposito modulo, presentato più avanti in questo documento.

Le differenti tappe e i consigli per l'implementazione relativi a queste modalità di gestione sono descritti nella guida di diagnosi dei servizi di sicurezza.

¹ Questo modulo è in corso di sviluppo.

² L'analisi della sicurezza è descritta in dettaglio nella guida che fa parte delle documentazione di MEHARI : Guida all'analisi dello stato dei servizi di sicurezza

³ Nel documento originale viene utilizzato il termine "enjeux", che letteralmente può essere tradotto come "Posta in gioco" e che riassume l'insieme dei beni aziendali, le minacce a cui sono esposti, la probabilità che tali minacce si realizzino e gli eventuali danni connessi (N.d.T)

2.1.3 Il supporto delle basi di conoscenza per realizzare una infrastruttura di riferimento della sicurezza

Il modulo di analisi della sicurezza si appoggia, in pratica, su una base di conoscenza dei servizi di sicurezza (chiamata Manuale di riferimento dei servizi di sicurezza) che descrive, per ogni servizio, la finalità (cosa fa), a cosa serve (contro cosa lotta), i meccanismi e le soluzioni supportate dal servizio e gli elementi da prendere in considerazione per valutare la qualità del servizio..

Questa base di conoscenza, senza dubbio unica nel suo genere, può essere impiegata direttamente per costruire una infrastruttura di riferimento della sicurezza (qualche volta chiamato anche policy di sicurezza) che conterrà e descriverà l'insieme delle regole e delle istruzioni di sicurezza da rispettare nell'impresa o organizzazione.

Questo approccio è frequentemente utilizzato in aziende o organizzazioni con un gran numero di unità operative autonome o di sedi. Si può trattare di imprese multinazionali con numerose filiali ma anche, semplicemente, di medie imprese, o anche piccole, con numerosi agenti o rappresentanti regionali. E' in effetti difficile, in questi casi, moltiplicare le diagnosi o analisi del rischio.

Elaborare le raccomandazioni

I questionari di valutazione, ma soprattutto il manuale di riferimento dei servizi di sicurezza con le spiegazioni che esso contiene, saranno una buona base di lavoro per quei responsabili della sicurezza che decideranno che ciò dovrà essere applicato nell'impresa..

La gestione delle eccezioni

L'attivazione di un insieme di regole, il manuale di riferimento dei servizi di sicurezza, si scontra, sovente, con difficoltà di applicazione locali e si dovrà quindi saper gestire delle eccezioni.

Il fatto di utilizzare una base di conoscenza coerente con degli strumenti e un metodo di analisi del rischio permette in ogni caso di gestire le difficoltà locali trattando le domande di deroga con una analisi del rischio calzata sulla difficoltà messa in evidenza.

2.1.4 Gli ambiti coperti dai moduli di valutazione

Nell'ottica di una analisi del rischio, nel senso dell'identificazione di tutte le situazioni di rischio e della volontà di coprire tutti i rischi inaccettabili, l'ambito coperto da MEHARI non si ferma solo ai sistemi informativi.

I moduli di valutazione coprono, oltre che i sistemi di informazione e comunicazione, l'organizzazione generale, la protezione generale dei siti aziendali, l'ambiente di lavoro degli utilizzatori e gli aspetti regolamentari e giuridici.

2.1.5 Vista d'insieme sui moduli di valutazione

Quello che in sintesi bisogna sapere sui moduli di valutazione è che essi offrono una visione a largo raggio e coerente della sicurezza, utilizzabile con approcci differenti, con una progressiva profondità di analisi che permette di utilizzarli a tutti gli stadi di maturità della sicurezza nell'impresa.

2.2. Analisi del contesto aziendale

Quali che siano gli orientamenti o la politica, in materia di sicurezza, c'è un principio su cui tutti i dirigenti concordano: la giusta proporzione tra i mezzi investiti nella sicurezza e l'importanza dei beni protetti.

Vale a dire che avere una giusta conoscenza del contesto aziendale (beni, loro valore, minacce a cui potrebbero essere esposti, conseguenze...) è fondamentale e che l'analisi di tale contesto merita

⁴ Il manuale di riferimento dei servizi di sicurezza fa parte della base di conoscenza di MEHARI

un alto grado di priorità e un metodo di valutazione rigoroso.

L'oggetto dell'analisi del contesto aziendale è di rispondere a questo duplice interrogativo:

Cosa potrebbe succedere e, nel caso accadesse, quanto sarebbe grave ?

Vale a dire che, nell'ambito della sicurezza, l'analisi del contesto aziendale viene vista nell'ottica delle conseguenze di eventi venuti a perturbare il funzionamento voluto e previsto dell'impresa o organizzazione.

MEHARI propone un modulo di analisi del contesto aziendale, descritto in dettaglio nella guida "Analisi e classificazione del contesto aziendale", che consente di ottenere due tipi di risultati:

- una scala di valore delle minacce (malfunzionamenti)
- una classificazione delle informazioni e delle risorse del sistema informativo

Minacce

L'identificazione delle minacce (malfunzionamenti) nei processi operativi, o degli eventi che potrebbero ridurli, è una modalità operativa che si esercita a partire dalle attività dell'azienda. L'analisi comincia da:

- una descrizione dei possibili tipi di minacce o malfunzionamenti
- una definizione dei parametri che ne influenzano la gravità
- la valutazione delle soglie di criticità di quei parametri che fanno passare la gravità delle minacce da un livello all'altro

Questo insieme di risultati costituisce una scala di valori delle minacce.

Classificazione delle informazioni e delle risorse

Si è soliti parlare, nell'ambito della sicurezza dei sistemi informativi, della classificazione delle informazioni e delle risorse del sistema informativo.

Una tale classificazione consiste nel definire, per ogni tipo di informazione e per ogni risorsa del sistema informativo - e per ognuno dei criteri di classificazione - la disponibilità, l'integrità e la confidenzialità, che sono degli indicatori rappresentativi della gravità di una minaccia a quel criterio per quell'informazione o quella risorsa.

La classificazione delle informazioni e delle risorse è la traduzione, per i sistemi informativi, della scala di valori delle minacce, definita precedentemente, indicando la sensibilità associata alle risorse dei sistemi informativi.

Espressione della sicurezza rispetto al contesto aziendale

La scala dei valori delle minacce e la classificazione sono due maniere distinte di considerare la sicurezza rapportata al contesto aziendale.

La prima è più dettagliata e fornisce più informazioni per i responsabili della sicurezza; la seconda è più globale e più utile alla comunicazione sul grado di sensibilità, con una perdita di precisione.

2.2.1 L'analisi del contesto aziendale, base dell'analisi del rischio

E' chiaro che questo modulo è un elemento chiave dell'analisi del rischio e che senza un consenso sulle conseguenze delle minacce potenziali, qualunque giudizio su un livello di rischio è impossibile.

2.2.2 L'analisi del contesto aziendale, supporto di tutti i piani d'azione strategici

Come indicato nell'introduzione, l'analisi del contesto aziendale è spesso necessario per l'attivazione di qualunque piano di sicurezza. In effetti, quale che sia la strada seguita, ci sarà un

momento in cui si dovrà allocare dei mezzi per porre in atto il piano di azione e immancabilmente la questione sarà posta per ben pianificare un tale investimento.

Le risorse e i fondi destinati alla sicurezza sono, come per le assicurazioni, direttamente proporzionati (in funzione di) all'importanza del rischio e, se non c'è consenso sulle eventuali minacce, è probabile che il budget non sarà reso disponibile.

2.2.3 La classificazione, elemento essenziale di una politica della sicurezza

Abbiamo già menzionato i piani o politiche di sicurezza e le modalità di gestione della sicurezza.

In pratica, le imprese che gestiscono la sicurezza con un insieme di regole sono portate a differenziare dalle regole vere e proprie le azioni da condurre in funzione della sensibilità delle informazioni trattate. Il modo tradizionale per farlo è di far riferimento a una classificazione delle informazioni e delle risorse del sistema informativo.

Il modulo di analisi del contesto aziendale di MEHARI permette quindi di effettuare questa classificazione. .

2.2.4 L'analisi del contesto aziendale, base dei piani di sicurezza

Il processo stesso di analisi del contesto aziendale, per il quale è necessario il contributo dei responsabili operativi, genera spesso un bisogno di azioni immediate..

L'esperienza mostra che quando si incontra un responsabile operativo con un alto livello di responsabilità, qualunque sia la dimensione dell'azienda, e comunque si esprimano quelle che si stimano essere delle minacce gravi, ciò fa nascere un bisogno di sicurezza di cui prima non avevano coscienza di avere e al quali bisogna rispondere rapidamente..

Si possono allora costruire direttamente dei piani d'azione, utilizzando un approccio diretto e veloce basato sulla conciliazione di due aspetti: quello della professione stessa, per i responsabili operativi, e quello delle soluzioni di sicurezza, da parte dei responsabili della sicurezza.

2.3. L'analisi del rischio

L'analisi del rischio è citata da moltissimi testi sulla sicurezza, come se dovesse essere il motore della sicurezza, ma la maggior parte di tali testi poi tacciono sul metodo da utilizzare.

MEHARI propone, da più di 10 anni, un approccio strutturato al rischio⁵ basato su alcuni semplici elementi.

Per mantenersi all'essenziale, una situazione di rischio può essere caratterizzata da diversi fattori:

- Fattori strutturali, che non dipendono dalle misure di sicurezza ma dall'attività dell'impresa, dal suo ambiente e dal contesto nel quale opera.
- Fattori di riduzione del rischio, che sono direttamente funzione delle misure di sicurezza attivate.

MEHARI permette di valutare, qualitativamente e quantitativamente, questi fattori e di arrivare, di conseguenza, a un giudizio sul livello di rischio..

Precisiamo che l'analisi del contesto aziendale sarà presa in considerazione per determinare la gravità massima delle conseguenze di una situazione di rischio, che è tipicamente un fattore strutturale, mentre la valutazione della sicurezza (security assessment) sarà presa in considerazione per valutare i fattori di riduzione del rischio.

⁵ Il dettaglio del modello del rischio è riportato nel documento « Principi e meccanismi di MEHARI » disponibile sul sito del Clusif.

2.3.1 L'analisi del rischio, un ausilio alla pianificazione strategica

L'evidenziazione di fattori di riduzione del rischio, essi stessi funzione delle misure di sicurezza, offre una base metodologica per elaborare un piano di sicurezza o un piano strategico.

Su questa base, MEHARI propone e struttura un percorso che conduce all'elaborazione del piano di sicurezza.

Questo passaggio si appoggia su una base di conoscenza delle situazioni di rischio e su degli automatismi di valutazione dei fattori di riduzione del rischio. Essa è sostenuta da uno strumento software⁶ che scarica l'utilizzatore da tutte le attività di calcolo e permette simulazioni e ottimizzazioni..

In questo utilizzo di MEHARI, l'accento è portato sull'ottimizzazione globale delle misure di sicurezza nell'ottica di una riduzione dei rischi..

2.3.2 L'analisi sistematica delle situazioni di rischio

Sulla stessa base metodologica, un approccio sensibilmente differente consiste nell'identificare tutte le situazioni di rischio potenziale, analizzandone individualmente le più critiche, per poi decidere le azioni da condurre per riportarle ad un livello di rischio accettabile..

MEHARI permette anche questo approccio e la base delle conoscenze è stata sviluppata al fine di rispondere a questo obiettivo..

Da questo punto di vista, MEHARI mette l'accento sull'assicurazione che qualunque situazione di rischio critico è stata presa in considerazione e ben coperta da un adeguato piano d'azione.

2.3.3 L'analisi puntuale del rischio

Gli stessi strumenti possono essere utilizzati puntualmente nel quadro di altre modalità di gestione della sicurezza.

Nei casi che abbiamo analizzato, gestione tramite l'analisi o con un manuale di riferimento della sicurezza, si troveranno sempre dei casi particolari dove le regole stabilite non potranno essere applicate. E' molto utile, in quel caso, potersi valere di una analisi puntuale del rischio per decidere il comportamento da tenere.

2.3.4 L'analisi del rischio legata a nuovi progetti

Il modello e i meccanismi di analisi del rischio possono infine essere utilizzati nell'ambito della gestione di progetti, per analizzarne i rischi e decidere di conseguenza le misure da adottare..

2.4. Vista d'insieme sull'utilizzo di MEHARI

E' chiaro che l'orientamento principale di MEHARI è l'analisi e la riduzione del rischio e che le sue basi di conoscenza, i suoi meccanismi e gli strumenti di supporto sono stati costruiti a questo fine.

E' chiaro anche, nello spirito degli ideatori di questo insieme di metodologie, che il richiamo a un metodo strutturato di analisi e riduzione dei rischi può essere, a seconda dell'impresa:

- un metodo di lavoro permanente, basato su linee guida e strutturato,
- un metodo di lavoro permanente, impiegato contemporaneamente ad altre metodologie di gestione della sicurezza,

⁶ RISICARE realizzato da BUC S.A.

— una modalità operativa occasionale, a complemento di altre metodologie di gestione..

Con questo spirito, quello che MEHARI apporta è un insieme di concetti e strumenti che permettono di ricorrere all'analisi del rischio quando sarà ritenuto utile o necessario.

MEHARI è diffuso liberamente dal Clusif sotto forma di documenti scaricabili. Tra questi, oltre alle basi della conoscenza, si trovano dei manuali che consentono di meglio apprendere i differenti moduli (minacce-rischi-vulnerabilità), al fine di supportare i responsabili della sicurezza informatica. (CISO, Risk Manager, auditors, CIO, ..) nel loro percorso di gestione.

3. MEHARI e gli standard

Spesso, sorge la questione del posizionamento di MEHARI rispetto a delle norme internazionali, e in particolare alle norme ISO 13335, ISO17799⁷ e ISO/IEC 27001⁸.

Non si tratta di paragonare MEHARI e i diversi strumenti metodologici creati attorno alle norme, ma solamente di valutare il posizionamento di MEHARI rispetto alle norme ISO in termini di oggettività e compatibilità.

La norma ISO 13335 contiene un modello di gestione del rischio al quale MEHARI fa riferimento e con il quale MEHARI è totalmente compatibile. MEHARI propone un metodo e degli strumenti analogamente a quanto previsto dalla norma.

Prenderemo dunque in considerazione, qui di seguito, il posizionamento di MEHARI rispetto a ISO 17799 ed a ISO/IEC 27001.

3.1. *Gli obiettivi di ISO 17799, ISO/IEC 27001 e MEHARI*

3.1.1 *Obiettivi della norma ISO 17799:2005*

Questa norma indica che una organizzazione deve identificare le proprie esigenze di sicurezza partendo da tre fonti principali:

- l'analisi dei rischi,
- Le esigenze legali, statutarie, regolamentari o contrattuali,
- l'insieme dei principi, obiettivi ed esigenze relative al trattamento delle informazioni che l'organizzazione ha sviluppato per supportare le proprie attività.

Partendo da qui, i punti di controllo possono essere scelti ed implementati secondo la lista fornita nella parte « codice di pratiche per la gestione della sicurezza dell'informazione » dello standard o provenire da altri insiemi di punti di controllo (§4.2).

Nota : negli « Scope » della versione 17799 :2005 è precisato che lo standard fornisce delle « guidelines and general principles for initiating, implementing, maintaining and improving information security management » che indica che la norma ISO può essere « considerato come un punto di partenza », ma ISO/IEC 27001 indica (§1.2) che tutte le eccezioni devono essere giustificate e che è parallelamente possibile aggiungere altri obiettivi di controllo (allegati A - A.1)

La norma ISO 17799 fornisce quindi una raccolta di linee di riferimento di cui le aziende possono (dovrebbero) tenere conto, precisando che questa raccolta non è esaustiva e che delle misure complementari possono essere necessarie, ma alcuna metodologia è indicata per elaborare il sistema completo di gestione della sicurezza.

Al contrario, qualunque best practice comprende delle introduzioni e dei commenti sugli obiettivi perseguiti, che possono costituire un aiuto apprezzabile.

Nota : La norma ISO indica allo stesso modo nel suo « Scope » che può essere utilizzato « to help build confidence in inter-organizational activities ». Ciò non è stato inserito casualmente e mette in luce un obiettivo essenziale dei promotori dello standard che è la valutazione, vedi certificazione, dal punto di vista della sicurezza delle informazioni dei partner o dei fornitori di

⁷ nella versione ISO/IEC 17799:2005

⁸ nella versione ISO/IEC 27001-2005

servizi.

3.1.2 Obiettivi dell'ISO/IEC 27001

L'obiettivo dell'ISO/IEC 27001 è chiaramente presentato come quello di « *fornire un modello per progettare e gestire un sistema di gestione della sicurezza dell'informazione (ISMS) di una organizzazione* » e « *d'essere utilizzato sia all'interno che da terzi, compresi gli organismi di certificazione* ».

Questo obiettivo di valutazione e certificazione mette fortemente l'accento su degli aspetti di formalizzazione (documentazione e registrazione delle decisioni, dichiarazioni di conformità, applicabilità, registrazioni etc.) e sui controlli (revisioni, audit etc.). A questo titolo, si tratta di un approccio molto orientato alla qualità.

Resta il fatto che, alla fine, il processo di sicurezza presentato implica la realizzazione iniziale di una analisi del rischio alla quale l'azienda o l'organizzazione è esposta, ed una selezione delle misure adeguate per ridurre questo rischio a un livello accettabile (§4.2.1)..

ISO/IEC 27001 indica che un metodo di analisi del rischio deve essere utilizzato, ma esso non fa parte della norma e nessun metodo in particolare viene proposto, se non che deve essere integrato nel processo ricorsivo del modello (PDCA Plan-Do-Check-Act) definito per realizzare l'ISMS.

Peraltro, le raccomandazioni o le « *best practice* » che possono essere selezionate per ridurre i rischi sono allineate a quelle elencate nella norma ISO/IEC 17799:2005, mentre una lista di punti di controllo è fornita in allegato.

La base delle **valutazione del sistema di gestione della sicurezza** secondo la norma ISO/IEC 27001, non è sapere o verificare se le decisioni prese sono pertinenti e se esse riflettano bene le necessità dell'azienda, ma di verificare che, una volta prese queste decisioni, il sistema di gestione è proprio quello che consentirà di avere una certa garanzia che esse siano applicate (nominando un auditor o un certificatore).

3.1.3 Obiettivo di MEHARI

MEHARI si presenta come un insieme coerente di strumenti e metodi di gestione della sicurezza, fondato sull'analisi del rischio. I due aspetti fondamentali di MEHARI, che sono il modello del rischio (qualitativo e quantitativo) e i modelli di gestione della sicurezza basati sull'analisi del rischio, non hanno equivalenti nelle norme l'ISO/IEC 27001 e ISO 17799.

3.1.4 Analisi comparata degli obiettivi di MEHARI e degli standard ISO 17799 e ISO/IEC 27001

Gli obiettivi di MEHARI da un lato e degli standard ISO sopra descritti dall'altro sono radicalmente differenti:

- MEHARI punta a mettere a disposizione degli strumenti e dei metodi per selezionare le misure di sicurezza più adatte per una certa azienda, che non è assolutamente dal punto di vista degli standard ISO.
- I due standard ISO forniscono un insieme di buone pratiche, certamente utili ma non per forza adatte al contesto aziendale, e un mezzo di giudizio della maturità, sul piano della sicurezza dell'informazione, a cura di entità interne o di partner..

Il solo aspetto della metodologia MEHARI che può essere paragonato a ISO 17799 (e all'allegato A della norma ISO/IEC 27001) è **il manuale di riferimento dei servizi di sicurezza** che presenta effettivamente degli elementi dettagliati per essere utilizzati per costruire un sistema di riferimento della sicurezza. Riguardo a questo aspetto, è chiaro che la copertura dei servizi di MEHARI è più vasta

che quella di ISO poiché copre degli aspetti essenziali della sicurezza al di fuori dei sistemi informatici propriamente detti.

3.2. *Compatibilità di questi approcci*

L'approccio di MEHARI è, in realtà, totalmente conciliabile con quello delle norme ISO 17799 perché, sebbene esse non perseguano lo stesso obiettivo, è possibile rappresentare in modo relativamente facile (se questo è necessario) i risultati ottenuti seguendo il processo MEHARI in indicatori ISO 17799.

MEHARI consente di rispondere alle domanda dei due standard di basarsi su un'analisi del rischio per definire le misure da mettere in atto..

3.2.1 *Compatibilità con la norma ISO 17799*

I « controlli » standards o « best practice » dell'ISO sono principalmente delle misure molto generali (organizzative e comportamentali) mentre MEHARI pone prioritariamente l'accento su delle misure tecniche di cui si possa garantire l'efficacia. I risultati, in termini di gestione della sicurezza, saranno radicalmente differenti con i due approcci..

Malgrado questa differenza, esistono, in MEHARI, e in particolare nella versione 2007, delle tabelle di corrispondenza che permettono di fornire dei risultati dei punti di controllo sotto forma di indicatori allineati alla suddivisione della norma ISO 17799:2005; questo può essere utile per coloro che hanno un bisogno particolare di fornire delle prove di conformità a questi standard.

È utile ricordare che i questionari di audit di MEHARI sono progettati e suddivisi al fine di realizzare efficacemente l'analisi delle vulnerabilità da parte dei responsabili delle attività coinvolte e di dedurre la capacità di ridurre il rischio di ciascun servizio di sicurezza.

3.2.2 *Compatibilità con la norma ISO 27001*

È semplice integrare MEHARI nei processi definiti dall'ISO/IEC 27001, principalmente nella fase Plan (§4.2.1), di cui MEHARI copre completamente la descrizione delle attività, permettendo di stabilire le basi dell'ISMS.

Per la fase DO (§4.2.2), che mira a implementare e gestire l'ISMS, MEHARI apporta degli elementi iniziali utili come l'implementazione di piani di trattamento dei rischi, con delle priorità direttamente legate alla classificazione dei rischi e a degli indicatori di stato di avanzamento della realizzazione.

Per la fase CHECK (§4.2.3), MEHARI mette a disposizione gli elementi che permettono di determinare i rischi residui e i miglioramenti introdotti nelle misure di sicurezza. Quindi, tutte le modifiche dell'ambiente (vulnerabilità, minacce, soluzioni e organizzazione) può essere rivalutato agevolmente con degli audit mirati sui risultati dell'audit iniziale realizzato con MEHARI al fine di rivedere i piani di sicurezza in ogni momento.

Per la fase ACT (§4.2.4), MEHARI richiama implicitamente ai controlli e al miglioramento continuo della sicurezza al fine di assicurare la gestione degli obiettivi di riduzione dei rischi. In queste tre fasi MEHARI non è il cuore del processo, ma contribuisce alla loro realizzazione e ad assicurare la loro efficacia.