MEHARI 2010

Introduzione alla metodologia

Ottobre 2010

Gruppo di lavoro metodi

Per domande e commenti uso:

http://mehari.info/

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador, 75009 Paris (France)

Tel.: +33 1 53 25 08 80 – Fax: +33 1 53 25 08 88
e-mail: clusif@clusif.asso.fr Web: http://www.clusif.asso.fr

Ringraziamenti

Il CLUSIF ringrazia le persone che hanno reso possibile la realizzazione di questo documento, e in particolare :

Jean-Philippe	Jouas	Responsabile dell'Espace Méthodes Responsabile del « Groupe de Travail Principes, Mécanismes et Bases de connaissances de Méhari »
Jean-Louis	Roule	Responsabile del « Groupe de Travail Documentation de Méhari »
Dominique	Buc	BUC S.A.
Olivier	Corbier	Docapost
Martine	Gagné	HydroQuébec
Moïse	Hazzan	Ministère des Services Gouvernementaux du Québec
Gérard	Molines	Molines Consultants
Chantale	Pineault	AGRM
Luc	Poulin	CRIM
Pierre	Sasseville	Ministère des Services Gouvernementaux du Québec
Claude	Taillon	Ministère de l'Éducation, du Loisir et du Sport du Québec
Marc	Touboul	BULL SA

Si ringrazia anche **Massimiliano Manzetti, membro del Comitato Direttivo Clusit**, per aver curato la traduzione italiana.

1. Introduzione

La metodologia Méhari (**Mé**thode **h**armonisée d'**a**nalyse des **ri**sques) è stata pensata, e viene costantemente aggiornata, per supportare i Responsabili della Sicurezza Informatica nel compito di gestione e governo della 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 Méhari. La documentazione messa a disposizione dal Clusif contiene anche una descrizione più completa del metodo e dei relativi strumenti, e in particolare:

- una presentazione dei principi fondamentali e delle specifiche funzionali di Méhari
- delle 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)
- delle basi di conoscenza.

L'obiettivo primario di Méhari è mettere a disposizione un metodo di analisi[1] e di gestione del rischio e, più specificamente per l'ambito della sicurezza informatica, una metodologia conforme alla norma ISO/IEC 27005:2008, completa degli strumenti e metodi richiesti per la sua messa in atto[2].

A questo obiettivo primario se ne aggiungono due complementari:

- permettere una analisi diretta e personalizzata delle situazioni di rischio presentate tramite scenari di rischio
- fornire una gamma completa di strumenti adatti alla gestione della sicurezza a breve, medio e lungo termine, quale che sia la maturità dell'organizzazione in tema di sicurezza e quali che siano le azioni considerate.

Tenuto conto di questi obiettivi, Méhari propone un 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.

Alla fine di questo documento viene illustrato il posizionamento di Méhari rispetto allea norma ISO/IEC 27000.

[1] Valutazioen del rischio secondo la ISO/IEC 27005
[2] Vedi documento « *Méhari 2010 – Principes fondamentaux et spécifications fonctionnelles* »

2. Utilizzo di Méhari

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

Infatti, tenendo conto del secondo obiettivo sopracitato, Méhari, e l'insieme delle sue basi di conoscenze, sono costruite per permettere una analisi precisa delle situazioni di rischio, quando ciò sarà giudicato necessario, tramite scenari di rischio.

In effetti la gestione della sicurezza è un processo o una attività che si evolve nel tempo e le azioni corrispondenti 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 un determinato modello di "riferimento" per mettere in evidenza il gap da colmare.

Successivamente, fatta questa valutazione e presa la decisione di mettere in piedi i cambiamenti necessari 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, così come richiede la norma ISO/IEC 27001 che tratta dei Sistemi di Gestione della Sicurezza delle Informazioni[3]. Va considerato, però, che oggi esistono altre vie, come ad esempio allinearsi a uno standard di riferimento, indipendentemente dal fatto che sia interno, 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 (aree 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 di un nuovo progetto. Bisognerà, allora, utilizzare un metodo di analisi del rischio.

Il principio sul quale è fondato Méhari 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 in una determinata fase devono poter essere utilizzati nelle fasi successive.

L'insieme di strumenti e moduli della metodologia Méhari, concepiti per poter supportare una analisi diretta e personalizzata 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, costituiscono un metodo di analisi del rischio con degli strumenti associati, dei moduli di analisi delle minacce ed un modulo di diagnostica dello stato della sicurezza. .

[I] in inglese « Information Security Management System » o ISMS ; in francese « Systèmes de Gestion de la Sécurité de l'Information » o SMSI

2.1 L'analisi (o valutazione) del rischio

L'analisi del rischio è citata da moltissimi testi sulla sicurezza, e specialmente nella norma ISO/IEC 27000, come se dovesse essere la base per evidenziare le necessità della sicurezza, ma la maggior parte di tali testi poi tacciono sul metodo da utilizzare.

Méhari propone, da più di 15 anni, un approccio strutturato al rischio[4] 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.

Precisiamo che l'analisi delle minacce è necessaria 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) è necessaria per valutare i fattori di riduzione del rischio.

Méhari permette di valutare, qualitativamente e quantitativamente, questi fattori e di arrivare, di conseguenza, a un giudizio sul livello di rischio. Méhari utilizza strumenti (criteri di valutazione, metodi di calcolo etc.) e basi di conoscenza (in particolare per la diagnostica della sicurezza) che si rivelano complemento indispensabile al completamento del quadro minimo proposto dalla norma ISO 27005.

2.1.1 L'analisi sistematica delle situazioni di rischio

Per rispondere alle domande " A quali rischi l'organizzazione è esposta? E questi rischi sono accettabili?" un approccio strutturato 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..

Méhari permette di realizzare questo approccio e la base delle conoscenza è stata sviluppata al fine di rispondere a questo obiettivo. Da questo punto di vista, Méhari 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.

Questo passaggio si appoggia su una base di conoscenza delle situazioni di rischio e su dei meccanismi di valutazione dei fattori caratterizzanti ciascun rischio, permettendo di valutarne il livello. La metodologia fornisce, inoltre, un aiuto per definire i piani di intervento appropriati.

Il processo di valutazione del rischio può essere supportato:

- Sia da un insieme di funzioni della base di conoscenza (Microsoft Excel) che permettono di integrare i diversi moduli di Méhari (in particolare, classificazione dei rischi attivi risultanti dall'analisi delle minacce e diagnostica di sicurezza). Queste funzioni permettono di valutare il livello di rischio attuale e di proporre delle misure aggiuntive per ridurre la gravità dello scenario.
- Sia per una utility software (come RISICARE)[5] che offre una assistenza più evoluta e più completa permettendo simulazioni, visualizzazioni e ottimizzazioni.

[4] Il dettaglio del modello del rischio è riportato nel documento « Principes fondamentaux et spécifications fonctionnelles de MEHARI »

[5] RISICARE realizzato da BUC S.A.

2.1.2 L'analisi puntuale del rischio

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

In effetti, nell'ambito di metodiche di governo della sicurezza per le quali la gestione del rischio non è la base principale, così come la gestione tramite l'analisi o con un manuale di riferimento della sicurezza, si troveranno spesso dei casi particolari dove le regole stabilite non potranno essere applicate. E' molto utile, in questi casi, potersi avvalere di una analisi puntuale del rischio per decidere il comportamento da tenere.

2.1.3 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..

2.2 La diagnostica della sicurezza

La metodologia integrata dei questionari di diagnosi approfondita delle misure di sicurezza[6] effettivamente attive permette di valutare il livello di qualità dei meccanismi e soluzioni attivate per ridurre il rischio

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

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 perché l'analisi del rischio sia credibile e affidabile.

Uno dei punti di forza di Méhari come metodo di analisi e gestione dei rischi è certamente che sia l'analisi del livello di rischio attuale, sia la previsione del rischio futuro si appoggiano su una valida diagnostica della qualità delle misure di sicurezza attualmente in esssere o decise.

2.2.2 La pianificazione della sicurezza basata sull'analisi delle vulnerabilità

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

I processi di governo 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.

I questionari di diagnostica di Méhari possono essere utilizzati a questo scopo.

L'utilizzazione di un'analisi preliminare del contesto aziendale[7] è allora raccomandata, come prevista in un apposito modulo, presentato più avanti in questo documento. L'analisi del contesto aziendale permetterà di fissare gli obiettivi di qualità dei servizi di sicurezza, e ciò selezionando solo i servizi pertinenti alla valutazione nel quadro della dignostica.

[6] Le misure sono raggruppate per sottoservizi, essi stessi raggruppati in servizi e poi in domini di sicurezza

[7] 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)

2.2.3 Le basi di conoscenza come supporto alla realizzazione di uno standard 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 uno standard ("referentiel") della 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 lo standard

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 applicazioni 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.

2.2.4 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 Méhari 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.

2.2.5 Vista d'insieme sui moduli di diagnostica

Quello che in sintesi bisogna sapere sui questionari di diagnostica 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.

2.3 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 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.

Méhari 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 (ed eventualmente per altri criteri come la traciabilità o il valore probatorio), 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.

2.3.1 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.

Un altro punto di forza di Méhari è quello di presentare un metodo rigoroso per valutare il contesto aziendale e classificare gli asset, senza affidarsi al "sentire" degli utilizzatori e fornendo

output oggettivi e razionali.

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

L'analisi del contesto aziendale è spesso necessaria 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.

2.3.3 La classificazione, elemento essenziale di una politica della sicurezza

Abbiamo già menzionato i piani o politiche di sicurezza e le modalità di governo 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 degli asset del sistema informativo.

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

2.3.4 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.

2.4 Vista d'insieme sull'utilizzo di Méhari

E' chiaro che l'orientamento principale di Méhari 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,
- una modalità operativa occasionale, a complemento di altre metodologie di gestione..

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

Méhari è diffuso dal Clusif sotto forma di documenti scaricabili contenente le basi delle conoscenza e dei manuali che consentono di meglio apprendere i differenti moduli (minacce-rischi-vulnerabilità), al fine di supportare i responsabili della sicurezza informatica. (RSSI, Risk Manager, auditors, DSI, ..) nell'adempimento delle loro responsabilità.

3. Méhari e le norme ISO/IEC 27000

Spesso, sorge la questione del posizionamento di Méhari rispetto a delle norme internazionali, e in particolare alle norme ISO/IEC 27000[8].

Si tratta di valutare il posizionamento di Méhari in confronto a queste norme, in termini di oggettività e compatibilità, in particolare, per quanto riguarda le ISO/IEC 27001, 27002 et 27005.

3.1 Gli obiettivi di ISO/IEC 27001, 27002, 27005 e di Méhari

3.1.1 Obiettivi della norma ISO 27002:2005

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 trattamenti delle informazione 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 27002 :2005 è precisato che lo standard fornisce delle « guidelines and general principles for initiating, implementing, maintaining and improving information security management », il che indica che la norma ISO può essere « considerata 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 27002 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 governo 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-organizatinal activities »*. Ciò non è stato inserito casualmente e mette in

[8] In particolare ISO/IEC 27001:2005, 27002:2005 et 27005:2008

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 servizi.

3.1.2 Obiettivi dell'ISO/IEC 27001:2005

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 nell'ambito del 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 allineati a quelle elencate nella norma ISO/IEC 27002:2005, 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 governo è proprio quello che consentirà di avere una certa garanzia che esse siano applicate (nominando un auditor o un certificatore).

3.1.3 Obiettivo dell'ISO/IEC 27005:2008

Gli obiettivi di questa norma non riguardano la implementazione di un metodo completo di gestione del rischio, ma ne fissano un quadro minimo e imposto dalle esigenze tanto per il processo da seguire, quanto per l'identificazione di minacce e vulnerabilità che permette di stimare i rischi e di valutarne il livello, per poi poter scegliere come trattarli e quali piani ed elementi (tra cui misure di sicurezza e indicatori) saranno utilizzati per migliorare la situazione.

Non si tratta, dunque, di un insieme metodologico completo ed autosufficiente –vi è comunque precisato che la scelta di una metodologia deve essere fatta- ma di un inquadramento che permette di evitare la scelta di metodologie troppo semplicistiche e/o troppo lontane rispetto alla nozione di gestione del rischio voluta dalla norma.

3.1.4 Obiettivo di Méhari

Méhari si presenta come un insieme coerente, completo e autosufficiente di strumenti e metodi di gestione e governo della sicurezza, fondato su una analisi precisa del rischio. Gli aspetti fondamentali di Méhari, che sono il modello del rischio (qualitativo e quantitativo), la presa in considerazione, in questo modello, di una valutazione quantitativa dell'efficacia dei servizi di sicurezza attivati o progettati, la possibilità di valutare e simulare gli effetti delle misure individuate sui livelli di rischio residui, sono dei complementi indispensabili all'utilizzo delle norme ISO 27000 e, in particolare, dell'ISO/IEC 27005.

3.1.5 Analisi comparata degli obiettivi di Méhari e degli standard ISO 27002 e ISO/IEC 27001

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

- Méhari punta a mettere a disposizione degli strumenti e dei metodi per selezionare le misure di sicurezza più adatte, tecnicamente ed economicamente, per una certa azienda, che non è assolutamente il 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..

In ambito Méhari il **"***Manuel de référence des services de sécurité***"** presenta degli elementi dettagliati per essere utilizzati per costruire un sistema di riferimento della sicurezza tale da essere comparato alla norma ISO/IEC 27002. Riguardo a questo aspetto, è chiaro che la copertura dei servizi di Méhari 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 MÉHARI è, in realtà, totalmente conciliabile con quello delle norme ISO 27002 perchè, sebbene esse non perseguano lo stesso obiettivo, è possibile rappresentare in modo relativamente facile (se questo è necessario) i risultati ottenuti seguendo il processo MÉHARI in indicatori ISO 27002.

Méhari consente di rispondere alle domanda dei due standard (ISO 27001 e 27002) di basarsi su un'analisi del rischio per definire le misure da mettere in atto..

3.2.1 Compatibilità con la norma ISO/IEC 27002 :2005

I « controlli » standards o « best practice » dell'ISO sono principalmente delle misure molto generali (organizzative e comportamentali) mentre Méhari, integrando queste misure, pone prioritariamente l'accento su delle misure di cui si possa garantire l'efficacia per ridurre le vulnerabilità

Malgrado questa differenza, esistono, in Méhari delle tabelle di corrispondenza che permettono di fornire dei risultati sotto forma di indicatori allineati alla suddivisione della norma ISO 27002:2005; 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 Méhari 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 Méhari nei processi PDCA (Plan Do Check Act) definiti dall'ISO/IEC 27001, principalmente nella fase Plan (§4.2.1), di cui Méhari 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, Méhari 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), Méhari mette a disposizione gli elementi che permettono di determinare i rischi residui e i miglioramenti introdotti nelle misure di sicurezza. D'altronde, tutte le modifiche dell'ambiente (vulnerabilità, minacce, soluzioni e organizzazione) possono essere rivalutate agevolmente con degli audit mirati sui risultati dell'audit iniziale realizzato con Méhari al fine di rivedere i piani di sicurezza in ogni momento.

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

3.2.3 Compatibilità con la norma ISO/IEC 27005:2008

Il quadro fissato dalla norma ISO si applica strettamente al modo con cui Méhari permette di gestire il rischio, in particolare per :

- Il processo di analisi, di valutzione e di trattamento del rischio (ripreso dall'ISO 13335).
- L'identificazione degli asset primari (o primordiali) e di supporto nonché i livelli di classificazione (o valorizzazione) correlati, a seguito dell'analisi del contesto aziendale.
- L'identificazione delle minacce e la determinazione del loro livello (esposizione naturale) per cui Méhari è più precisa nella desrizione degli scenari di rischio.
- L'identificazione e la valorizzazione dell'efficacia delle misure di sicurezza esistenti, destinate a ridurre le vulnerabilità correlate.
- La considerazione di questi elementi per indicare il livello di gravità degli scenari di rischio su una scala a 4 livelli.
- La selettività nella scelta delle misure di sicurezza da integrare nel piano di riduzione dei rischi.

Inoltre, la metodologia Méhari non solo si integra facilmente in un percorso di ISMS come quello descritto dalla ISO 27001, ma soddisfa anche interamente le esigenze dettate dalla ISO 27005 per una tale metodologia.

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11, rue de Mogador
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.asso.fr

Scarica le produzioni CLUSIF:

www.clusif.asso.fr