# MEHARI 2010

**Resumo**

Abril 2010

Grupo de métodos de trabalho

Por favor publique suas perguntas e comentários no fórum:
http://mehari.info/

**CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS**

11 rue de Mogador – 75009 Paris (France)
Tél : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88
clusif@clusif.asso.fr – www.clusif.asso.fr

# RECONHECIMENTOS

A CLUSIF gostaria de agradecer em especial ao Consultor e Conselheiro de Segurança da Informação Leandro Malaquias pela tradução ao português, e aos membros da comissão de métodos que participaram na realização deste documento:

| | | |
|---|---|---|
| Jean-Philippe | Jouas | Responsável pela comissão de Métodos<br><br>Responsável pelos Princípios do Grupo de Trabalho, Mecanismos e Base de Conhecimento do MEHARI |
| Jean-Louis | Roule | Responsável pela documentação do Grupo de Trabalho MEHARI |
| 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 |

# CONTENTS

1. Introdução ..... 5

2. Funcionalidades do Mehari ..... 6

2.1. Análise ou Avaliação de Risco ..... 7

2.1.1 Análise Espontânea de Situações de Risco ..... 8

2.1.2 Análise de Risco em novos projetos ..... 8

2.2. Avaliações de Segurança ..... 8

2.2.1 Revisão da vulnerabilidade, um elemento da análise de risco ..... 8

2.2.2 Planos de Segurança baseados na revisão da vulnerabilidade ..... 8

2.2.3 O apoio prestado pelas bases de conhecimento na criação de um framework de segurança ..... 9

2.2.4 DomíniosDominios cobertos pelo modulo de avaliação de vulnerabilidade ..... 9

2.2.5 Visão geral do módulo de avaliação ..... 9

2.2.6 Analisando os desafios ..... 10

2.2.7 Analisando os desafios: a base para uma análise de risco ..... 11

2.2.8 A análise de desafios de segurança: o pilar de qualquer planejamento de ações estratégicas ..... 11

2.2.9 Classificação: um elemento essencial para política de segurança ..... 11

2.2.10 Análise de desafios de segurança: a base para o planejamento de segurança ..... 12

2.3. Visão geral da utilização do Mehari ..... 12

3. Mehari e a norma ISO/IEC 27000 ..... 13

3.1. Os respectivos objetivosobjectivos da ISO / IEC 27001, 27002, 27005 e Mehari ..... 13

3.1.1 Objetivos da norma ISO/IEC 27002:2005 ..... 13

3.1.2 Objetivos da ISO/IEC 27001:2005 ..... 14

3.1.3 Objetivos da ISO/IEC 27005:2008 ..... 14

3.1.4 Objetivos da Mehari ..... 14

3.1.5 Comparação das metas do Mehari e as normas ISO / IEC 27001 e 27002 ..... 15

3.2. Compatibilidade entre as abordagens ..... 15

3.2.1 Compatibilidade com a norma ISO/IEC 27002:2005 ..... 15

3.2.2 Compatibilidade com a norma ISO/IEC 27001 ..... 16

3.2.3 Compatibilidade com a norma ISO/IEC 27005:2008 ..... 16

# 1. INTRODUÇÃO

A metodologia MEHARI foi originalmente desenvolvida e é constantemente atualizada para auxiliar os *Chief Information Security Officers* **(CISOs)** na gestão das atividades de segurança da informação.

Este resumo foca principalmente neles mas também destina-se a auditors, CIOs ou gestores de risco que compartilham desafios similares.

O principal objetivo deste document é descrever como o MEHARI pode ser utilizado. Uma descrição mais detalhada da metodologia e ferramentas associadas está disponível em outras publicações do Clusif, algumas em particular são:

- MEHARI: Conceitos e Funcionalidades específicas,
- Guias MEHARI para:
    - Análise limitações e classificação;
    - Evolução dos serviços de segurança e
    - Análise de risco,
- Manual de Referência MEHARI para serviços de segurança,
- MEHARI Base de Conhecimento MEHARI.

O primeiro objetivo da MEHARI é oferecer um método de avaliação e gestão de risco, especificamente no domínio da segurança da informação, em conformidade com os requisitos da ISO/IEC 27005:2008 e provendo um conjunto de ferramentas e elementos necessários para a implementação[1].

Outros objetivos são:

Permitir análise direta e individual de situações de risco descritas por cenários,

Proporcionar um conjunto completo de ferramentas especialmente projetadas para a gestão de segurança de curta, media e longa duração, adaptáveis a vários níveis de maturidade e tipos de ações consideradas.

Na verdade MEHARI oferece uma metodologia consistente, com uma base de conhecimento apropriada para auxiliar *Chief Information Security Officers* **(CISOs)**, diretores gerais, gestores de segurança ou pessoas comprometidas com a redução do risco, em suas diferentes funções e ações.

A relação do Mehari com a norma ISO/IEC 27001 está descrita no final do documento.

[1] Os meios associados e ferramentas fornecidas pelo MEHARI em complemento a norma, estão descritos e justificados no MEHARI: Conceitos e Funcionalidades específicas

# 2. FUNCIONALIDADES DO MEHARI

MEHARI é acima de tudo um método para avaliação e gestão de risco

***Na pratica, isso significa que MEHARI e sua base de conhecimento associada foram projetadas para uma analise precisa de situações de risco descrita por cenários.***

No dia a dia, gestão de segurança é uma função ou atividade que evolui com o tempo. Ações corretivas são diferentes, dependem se a organização não tiver feito nada neste domínio ou, ao contrário, tenha feito um investimento substancial em tempo e esforço. Dar os primeiros passos em segurança, é, sem dúvida, aconselhável que se faça um balanço do estado das medidas e políticas de segurança existentes na organização, e compará-las com as melhores práticas, para identificar as lacunas que devem ser preenchidas.

Após esta avaliação da situação e da decisão de implementar uma segurança organizacional, ações concretas deverão ser tomadas. Tais decisões, as quais normalmente são agrupadas em planos, regras corporativas, politicas ou um framework de referência de segurança, devem ser feitas utilizando uma abordagem estruturada. Esta abordagem pode ser baseada em análise de risco, conforme exigido pela ISO/IEC 27001 como parte de um SGSI (Sistema de Gestão em Segurança da Informação). Existem outros meios, tais como *benchmarking*, seja ele interno, terceirizado ou inter empresas.

Nessa fase, é verdade que, sem mencionar especificamente a análise de risco, a questão dos desafios envolvidos na segurança deve ser tratados. Inevitavelmente, qualquer que seja a decisão tomada, a pessoa responsável por alocar o orçamento apropriado, sem dúvida irá perguntar "isso é realmente necessário?". Devido à falta de uma avaliação preliminar dos desafios envolvidos e do acordo geral, muitos projetos de segurança são abandonados ou adiados.

Normalmente tardia, mas às vezes desde o início de uma abordagem de segurança, o risco real que uma organização ou empresa corre é questionada. Isto é frequentemente formulado em termos semelhantes a estes: "Foram identificados todos os riscos que possam expor a organização, e há alguma garantia os níveis mapeados são aceitáveis?". Esta pergunta poderia ser facilmente feitas no âmbito corporativo, ou em referência a um projeto específico. Uma metodologia que inclua análise de risco é necessária.

MEHARI se baseia no princípio que as ferramentas necessárias em cada fase do desenvolvimento da segurança devem ser consistentes. Por isso, deve-se entender que qualquer resultado gerado num estágio deve ser reutilizável por outras ferramentas mais tarde ou em outra parte da organização.

**As várias ferramentas e módulos do conjunto de metodologia MEHARI, projetados para acompanhar análises de risco direta e individual, podem ser utilizados separadamente uns dos outros em qualquer fase do desenvolvimento de segurança, utilizando abordagens de gestão diferentes e garantindo a coerência das decisões resultantes.**

Todas estas ferramentas e módulos, resumidos abaixo, compõem um método de avaliação consistente do risco com as ferramenta e módulos de apoio necessários para analisar os desafios e auditando a qualidade das medidas de segurança, etc.

## 2.1. Análise ou Avaliação de Risco

A análise de risco é mencionada em quase todas as publicações relacionadas a segurança, como sendo a força motriz para expressar os requisitos de segurança e também mencionado nas normas ISO/IEC. No entanto, a maioria falha em discutir quais métodos devem ser utilizados.

Por mais de 15 anos, MEHARI oferece uma abordagem estruturada para avaliar risco[2], com base em alguns princípios simples.

Uma situação de risco pode ser caracterizada por diversos fatores:

- Fatores estruturais (ou organizacionais) que não dependem de medidas de segurança mas da atividade principal da organização, seu ambiente e seu contexto.
- Fatores de redução de risco que são uma consequência direta das medidas de segurança já implementadas.

Na realidade, a análise dos desafios da segurança é necessária para determinar o nível de gravidade máximo das consequências de uma situação de risco. Isso é um fator tipicamente estrutural, enquanto a avaliação da segurança será utilizada para estimar os fatores de redução de risco.

O MEHARI permite estimativas tanto qualitativa como quantitativa desses fatores, e auxilia na estimativa dos níveis de risco como resultado. Ao fazê-lo, MEHARI integra ferramentas (como critérios de avaliação, fórmulas, etc) e bases de conhecimento (particularmente para o diagnóstico de medidas de segurança), que são complementos essenciais para o quadro mínimo proposto pela ISO / IEC 27005.

Análise Sistemática das Situações de Risco

A fim de responder à pergunta «Quais são os riscos de uma organização e são eles aceitáveis ou não?», uma abordagem estruturada é necessária para identificar todas as potenciais situações de risco, para analisar os mais críticos individualmente e em seguida, identificar ações para reduzir o risco a um nível aceitável.

A abordagem proposta pelo MEHARI é baseado numa base de conhecimentos de situações de risco e procedimentos automatizados para avaliar fatores que caracterizam cada risco e que permitem avaliar seus níveis. Além disso, o método provê suporte na seleção de planos de tratamento adequado.

A fim de avaliar o risco, duas opções principais são propostas:

- Usar um conjunto de funções da base de conhecimento (para o Microsoft Excel ou Open Office) que permite a integração dos resultados dos módulos Mehari (por exemplo, classificação de ativos da análise de desafios, o diagnóstico de segurança). A partir dessas funções, é possível avaliar o nível atual de risco e propor medidas para a redução do risco.
- Ou uma aplicação (como RISICARE3) que fornece uma interface mais completa para o usuário e que permite simulações, visualizações e otimizações adicionais.

---

2 *Uma descrição detalhada do modelo de risco disponível no MEHARI: Especificações de Princípios Fundamentais e Funcionais*

3 BUC S.A

### 2.1.1 Análise Espontânea de Situações de Risco

O mesmo conjunto de ferramentas podem ser utilizadas a qualquer momento em outras abordagens de gestão de segurança.

Em algumas abordagens para conduzir a segurança, onde a gestão de risco não é o principal objetivo e a segurança é gerida através de auditorias ou de algum framework de referência, haverá frequentemente casos específicos em que as regras não podem ser aplicadas. Análise de risco espontânea pode ser usada para decidir a melhor forma de proceder.

### 2.1.2 Análise de Risco em novos projetos

O modelo e mecanismos de análise de risco podem ser utilizados na gestão de projetos; para planejar contra o risco e decidir quais medidas devem ser adotadas.

## 2.2. Avaliações de Segurança

MEHARI integra através de meticulosos questionários de diagnóstico dos controles de segurança implementados, permitindo avaliar o nível de qualidade dos mecanismos e soluções que visam reduzir o risco[4]

### 2.2.1 Revisão da vulnerabilidade, um elemento da análise de risco

MEHARI fornece um modelo estruturado de risco que leva em consideração "fatores de redução de risco", no formato de serviços de segurança.

A análise de vulnerabilidade resultante será um contributo importante para a análise de risco assegurar que os serviços de segurança realmente cumprem seu papel - um ponto essencial para a credibilidade e confiabilidade da análise de risco.

Um dos pontos fortes do MEHARI, é sua capacidade de avaliar o nível atual do risco, como também os seus níveis futuros baseando-se numa especializada base de conhecimentos para avaliar o nível de qualidade das medidas de segurança, seja operacional ou decidido.

### 2.2.2 Planos de Segurança baseados na revisão da vulnerabilidade

Uma abordagem possível é criar planos de ação como resultado direto da avaliação da situação dos serviços de segurança.

O processo de gestão de segurança que segue esta abordagem é extremamente simples: faça uma avaliação e decida por melhorar todos os serviços que não têm um nível de qualidade satisfatório.

Os questionários de diagnóstico MEHARI podem ser utilizados nesta abordagem.

Uma análise preliminar dos desafios do negócio também deve ser planejada, fornecendo assim uma ligação a este módulo de MEHARI. A análise de desafios permite apontar requisitos de níveis de qualidade para os serviços de segurança relevantes e, consequentemente ignorar os outros como parte da avaliação.

---

[4] Controles de segurança ou medições estão agrupadas em sub-serviços, então serviços estarão finalmente no domínio da segurança

### 2.2.3 O apoio prestado pelas bases de conhecimento na criação de um framework de segurança

A incomparável base de conhecimento do Mehari pode ser usada diretamente para criar um framework de referência de segurança (ou políticas de segurança) que irá conter e descrever o conjunto de regras que definem a segurança e orientações que a empresa ou organização deverá seguir.

Esta abordagem é frequentemente utilizada em organizações ou empresas com unidades operacionais ou sítios independentes. Este normalmente seria o caso típico de grandes empresas multinacionais com filiais, mas também pode facilmente ser aplicado a empresas de médio porte com gerências regionais ou agências. Nesses casos, torna-se mais difícil realizar diversas avaliações ou análises de risco.

***Construindo a framework de referência de segurança***

Questionários de avaliação MEHARI são uma boa base de trabalho para os gestores de segurança para decidirem o que deve ser aplicado nas suas organizações.

***Gerindo excessões às regras***

A criação de um conjunto de regras, através de um framework de referência de em segurança, geralmente esbarra em dificuldades locais de implementação, portanto isenções e exceções devem ser geridas.

O uso de uma base de conhecimento coerente com um conjunto consistente de ferramentas e metodologia analítica, permite gerir as divergências locais. Os pedidos de exceções podem ser cobertos por uma análise de risco específica focada na dificuldade identificada.

### 2.2.4 Domínios cobertos pelo modulo de avaliação de vulnerabilidade

Do ponto de vista da análise de risco, em termos relativos à identificação todas as situações de risco e o desejo de cobrir todos os riscos inaceitáveis, Mehari não se restringe apenas ao domínio de TI.
O módulo de avaliação abrange, além do sistema de informação, toda a organização e da proteção do sítio em geral, bem como o ambiente de trabalho e os aspectos legais e regulamentares.

### 2.2.5 Visão geral do módulo de avaliação

A única coisa que se deve ter em mente sobre o módulo de avaliação de vulnerabilidade é que ele proporciona uma visão ampla e consistente da segurança. Isso pode ser utilizado em diversas abordagens, evolutiva na profundidade e de alta granularidade na análise, e pode ser utilizada em todas as fases de maturidade da sensibilização sobre a segurança organizacional da empresa.

### 2.2.6 Analisando os desafios

Segurança significa proteger ativos. Seja qual for a orientação da política de segurança, há um princípio no qual todos os gestores concordam: deve haver um equilíbrio justo entre os investimentos em segurança e a importância dos relevantes desafios do negócio.

Isto significa que uma compreensão adequada dos desafios do negócio é fundamental, e que a análise dos desafios de segurança merece um nível de prioridade elevado e um método rigoroso e estruturado de avaliação.

O objetivo de uma análise de desafios de segurança é para responder a pergunta dupla:

***"O que poderia acontecer? E se acontecer, seria grave?"***

Isso mostra que em segurança, desafios são vistos como consequências de eventos que perturbam as operações pretendidas de uma empresa ou organização. Mehari oferece um módulo de análise de desafios, descrito em Mehari: análise e classificação dos desafios, que produzem dois tipos de resultados:

- Uma escala de valores de falhas
- Uma classificação das informação e dos ativos de TI.

***A escala de valores de falhas***

Identificação de falhas ou eventos em potencial é um processo que começa com as atividades da empresa e consiste em identificar possíveis falhas em seus processos operacionais. Isso irá resultar em:

- Descrição dos possíveis tipos de falha
- Definição dos parâmetros que influenciam na gravidade de cada falha
- Avaliação dos limites críticos dos parâmetros que alteram o nível de gravidade das falhas

Este conjunto de resultados constituem a escala de valores de falhas

***Classificação das informações e ativos***

Em sistemas de segurança de TI, é comum falar sobre a classificação das informações e a classificação dos ativos de TI.

Tal classificação consiste em definir para cada tipo de informação, para cada ativo de TI, e para cada critério de classificação (classicamente: Disponibilidade, Integridade e Confidencialidade embora outros critérios possam ser utilizados, tais como a rastreabilidade), indicadores representativos da gravidade do critério sendo afetados ou perdidos desta informação ou ativo.

A classificação das informações e ativos, para sistemas de informação, é a escala de valores de falhas definida anteriormente e traduzida em indicadores de sensibilidade associadas com os ativos de TI.

***Expressando desafios da segurança***

A escala de valores de falhas e a classificação de informações e ativos são duas formas distintas de expressar os desafios de segurança.

A primeira é mais detalhada e fornece mais informações para os Chief Information Security Officers **CISOs**. A segunda é mais abrangente e mais útil para campanhas de sensibilização e comunicação, mas é menos detalhada.

### 2.2.7 Analisando os desafios: a base para uma análise de risco

Claramente, este módulo é fundamental na análise de risco. Sem um acordo comum sobre as consequências das possíveis falhas, nenhum julgamento dos níveis de risco será possível.

Mehari apresenta um método rigoroso para a avaliação dos desafios e a classificação de ativos, o qual fornece resultados objetivos e racionais.

### 2.2.8 A análise de desafios de segurança: o pilar de qualquer planejamento de ações estratégicas

Obviamente, analisar os desafios é necessário para a implementação de qualquer plano de segurança. Efetivamente, seja qual for a abordagem utilizada, em algum momento, recursos terão que ser alocados para implementar o plano de ação e, inevitavelmente, a justificativa para tal investimento será questionado.

Os meios e recursos que serão alocados para a segurança são como apólices de seguro, em proporção direta ao risco. Se não houver um acordo comum sobre as possíveis falhas, então é muito improvável que qualquer orçamentos seja alocado.

### 2.2.9 Classificação: um elemento essencial para política de segurança

O framework de referência de segurança, políticas de segurança, e a abordagem associados à gestão de segurança já foram mencionados neste documento.

Na prática, empresas que gerem a segurança através de um conjunto de regras são obrigadas a diferenciar nas próprias regras entre as ações a serem executadas como uma função sobre a sensibilidade da informação sendo processada. É habitual referir-se a classificação das informações e ativos de sistemas de TI.

O módulo de análise de desafios de segurança do MEHARI fornece os meios para realizar esta classificação.

### 2.2.10 Análise de desafios de segurança: a base para o planejamento de segurança

O próprio processo de análise desafios de segurança, que obviamente requer a contribuição dos gestores operacionais, muitas vezes leva a uma ação imediata.

A experiência mostra que, quando a alta gestão operacional é entrevistada, independentemente do tamanho da organização, e eles puderam explicar sua visão e estimativa de falhas graves, isto acaba levando a uma necessidade de segurança que não havia sido considerada anteriormente e que respostas rápidas são requeridas.

Planos de ação podem ser criados diretamente, utilizando uma abordagem leve e focada baseada na combinação de duas expertises: a dos próprios profissionais que dominam o negócio, proporcionada pela gestão operacional, e a das soluções de segurança, fornecida pelos consultores especialistas.

## 2.3. Visão geral da utilização do MEHARI

Claramente, a orientação principal do MEHARI é a avaliação e redução de riscos. Suas bases de conhecimento, mecanismos e ferramentas foram criadas com este propósito primordial em mente.

Além disso, na mente dos criadores do conjunto de metodologias, a necessidade de um método estruturado para análise de risco e redução é possível, desde que a organização tenha:

- Um método de trabalho permanente - diretrizes para um grupo especializado,
- Um método de trabalho utilizado em paralelo com outras práticas de gestão de segurança,
- Um método de trabalho utilizado ocasionalmente como complemento às práticas regulares.

Com isto em mente, MEHARI oferece um conjunto de abordagens e ferramentas que permitem a análise de risco a serem realizadas quando necessário.

A metodologia MEHARI, compreendendo as bases de conhecimento, os manuais e guias que descrevem os diferentes módulos (desafios, riscos, vulnerabilidades), está presente e é disponibilizada para auxiliar pessoas envolvidas na gestão da segurança (CISOs, gestores de risco, auditores, CIOs, ..), em suas diferentes tarefas e ações.

# 3. MEHARI E A NORMA ISO/IEC 27000

Uma pergunta frequente é: qual é a compatibilidade do MEHARI com normas internacionais - em particular a série de normas ISO / IEC 27000?

A intenção aqui é explicar como Mehari se adéqua as normas ISO 27001, 27002 e 27005, em relação à compatibilidade e objetivos.

## 3.1. Os respectivos objetivos da ISO / IEC 27001, 27002, 27005 e MEHARI

### 3.1.1 Objetivos da norma ISO/IEC 27002:2005

Este padrão determina que uma organização deve identificar seus requisitos de segurança utilizando três formas principais:

- Análise de Risco,
- Requisitos legais, estatutários, regulamentares ou contratuais,
- Conjunto de princípios, objetivos e requisitos aplicados ao processamento da informação que a organização desenvolveu para suportar suas operações.

Utilizando isto como base, pontos de controle podem ser escolhidos e implementados utilizando a lista fornecida na seção "código de boas práticas para a gestão de segurança da informação" da norma, ou de qualquer outro conjunto de pontos de controle (§4.2).

*NB: no âmbito da 27002: 2005, estipula-se que a norma ofereça "diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão da segurança da informação", o que significa que a norma ISO pode ser vista como um ponto de partida. No entanto, a ISO / IEC 27001 estipula (§ 1.2) que qualquer exclusão deve ser justificada e que é aceitável adicionar pontos de controle (Apêndice A - A.1).*

A norma ISO 27002 oferece uma compilação de diretrizes, que uma organização pode utilizar. De toda a forma, é observado que a lista não é exaustiva, e que medidas complementares podem ser necessárias. No entanto, nenhuma metodologia é recomendada para a criação de um sistema completo de gestão de segurança.

Por outro lado, cada parte do guia de boas práticas inclui introduções e comentários sobre os objetivos as metas pretendidas, o que pode ser uma ajuda muito útil.

*NB: A norma ISO também estipula em seu escopo que pode ser utilizada para "auxiliar na construção a estabelecer confiança nas atividades inter organizacionais". Isso não está incluído por acaso, e traz à tona um aspecto essencial que os defensores da norma promovem, que é a avaliação (até certificação), a partir de um ponto de vista de segurança da informação, dos parceiros e fornecedores.*

### 3.1.2 Objetivos da ISO/IEC 27001:2005

O objetivo claro da ISO / IEC 27001 é a de "fornecer um modelo para criar e administrar um sistema de gestão de segurança de informações corporativo (SGSI)" e ser "utilizado tanto internamente quanto por terceiros, incluindo autoridades certificadoras".

A avaliação e objetivos para a certificação colocam grande ênfase nos aspectos formais (documentação e registro de decisões, declaração de aplicabilidade, registros, etc) e controle (revisões, auditorias, etc.)

Está claro que a base de uma abordagem de segurança implica que uma análise de risco seja realizada, para avaliar os riscos aos quais a organização pode estar exposta, e para selecionar as medidas adequadas para reduzir os riscos a um nível aceitável (parágrafo 4.2.1) .

A ISO / IEC 27001 estabelece que um método de análise de risco deve ser utilizado, mas isto não faz parte da norma e nenhum método específico é proposto, além da integração dos processos recursivos do PDCA (Plan, Do, Check, Act) do modelo tal como definido para a criação do SGSI.

Além disso, as recomendações ou melhores práticas que poderão ser utilizadas para reduzir o risco estão "alinhadas com aqueles descritos na ISO / IEC 27002:2005", enquanto uma lista associada de pontos de controle é fornecido nos apêndices.

De acordo com a ISO / IEC 27001, a base para a **avaliação de um sistema de gestão de segurança** não é tanto o conhecimento ou verificar se as decisões que foram tomadas são adequadas e adaptadas às necessidades da organização, mas, uma vez que as decisões tenham sido tomadas, verificar se o sistema de gestão encontra-se definido de tal forma que um auditor ou entidade certificadora possa ter a certeza que as decisões foram realmente implementadas.

### 3.1.3 Objetivos da ISO/IEC 27005:2008

Os objetivos desta norma não constituem um método de gestão de risco, mas sim para fixar um framework mínimo e descrever requisitos, tanto para o processo de avaliação de risco em si, quanto para a identificação das ameaças e vulnerabilidades, permitindo estimar os riscos, seu nível e depois estar em posição para selecionar o modo de tratamento e os planos associados e medições destinadas a avaliação e melhorarias da situação.

A norma diz que um método de avaliação de risco deve ser selecionado de acordo com esses requisitos, a fim de evitar o uso de métodos inconsistentes ou simplistas, em comparação com a intenção dos editores da norma.

### 3.1.4 Objetivos da MEHARI

MEHARI é um conjunto de ferramentas e recursos metodológicos consistentes para a gestão de segurança e medidas associadas, baseado em uma análise precisa dos riscos. Os aspectos fundamentais da MEHARI são complementos obrigatórios aos requisitos da ISO / IEC 27000 e em particular as normas da ISO / IEC 27005.

A seguir:

Modelo de risco (qualitativo e quantitativo);

Eficacia das medidas de segurança em vigor ou planejadas; e

Capacidade de avaliar e simular os níveis de risco residual resultantes de medidas adicionais.

### 3.1.5 Comparação das metas do Mehari e as normas ISO / IEC 27001 e 27002

Os objetivos do Mehari e das normas ISO acima são radicalmente diferentes.

- Mehari visa proporcionar ferramentas e métodos que possam ser utilizados para escolher as medições de segurança mais apropriadas para uma determinada organização e para avaliar os riscos residuais uma vez que essas medições estejam operando. Este não é o objetivo principal declarado em nenhuma das normas ISO.
- As normas ISO proporcionam um conjunto de melhores práticas, que são certamente muito úteis, para cobrir os aspectos de maturidade em segurança, planejamento de segurança da informação, unidades internas independente e parceiros, mas não necessariamente apropriadas para o que se tem em foco nas organizações.

O **manual de referência de serviços de segurança** da MEHARI efetivamente provê elementos detalhados os quais podem ser utilizados para construir um framework de segurança e pode ser comparado com a ISO / IEC 27002. Neste caso, fica claro que a abrangência da MEHARI é maior do que da ISO, e inclui aspectos essenciais de segurança que vão além daqueles encontrados nos sistemas de informação.

## 3.2. Compatibilidade entre as abordagens

A abordagem MEHARI é totalmente conciliável com a ISO 27002 porque, apesar de não terem os mesmo objetivo, é relativamente fácil representar resultados de uma análise MEHARI em termos de indicadores ISO 27002.

MEHARI responde às necessidades, expressadas em ambos padrões ISO 27001 e 27002, para uma análise de risco definir as medições que devem ser implementadas.

### 3.2.1 Compatibilidade com a norma ISO/IEC 27002:2005

Os pontos de controle da norma ou melhores práticas da ISO são principalmente generalizadas por medições comportamentais ou organizacionais, enquanto MEHARI em adição a deles, salienta a necessidade de medidas cuja eficiência pode ser garantida.

Apesar destas diferenças, a revisão de vulnerabilidade MEHARI proporciona tabelas de correspondência para exibir indicadores alinhados com a desagregação utilizada na ISO 27002:2005, úteis àqueles que necessitam provar a sua conformidade com a norma.

Vale a pena mencionar que os questionários de auditoria MEHARI foram elaborados e constituídos de modo a permitir que gestores operacionais executem revisões de vulnerabilidade e deduzam a capacidade de cada serviço de segurança para reduzir esses riscos.

### 3.2.2 Compatibilidade com a norma ISO/IEC 27001

Mehari pode ser facilmente integrado aos processos do PDCA (Plan - Do - Check - Act) como mencionado pela ISO / IEC 27001, nomeadamente a fase de 'PLANEJAMENTO' (§ 4.2.1). Mehari cobre toda a descrição das tarefas que permitem a criação das bases ISMS.

Para a fase de "EXECUÇÃO" (§ 4.2.2), que visa implementar e administrar o ISMS, Mehari proporciona elementos iniciais úteis, tais como a construção de planos de gestão de riscos, com a priorização diretamente ligada a classificação de risco. e também as medições de progresso durante a sua utilização.

Para a fase de 'VERIFICAÇÃO' (§ 4.2.3), Mehari proporciona elementos que permitem a avaliação de riscos residuais, e melhorias feitas nas medições de segurança. Além disso,

quaisquer alterações ao ambiente (desafios, ameaças, soluções e organização) podem ser facilmente reavaliadas por auditorias direcionadas, que utilizem os resultados da auditoria Mehari inicial. Dessa forma os planos de segurança podem ser revisados e evoluírem com o tempo.

Para a fase de 'AÇÃO' (§ 4.2.4), Mehari chama implicitamente os controles e melhoria contínua de segurança, garantindo assim que as metas de redução de risco sejam atingidas. Nestas três fases, enquanto Mehari não estiver no centro dos processos, contribui muito para a execução delas e garante sua eficácia.

### 3.2.3 Compatibilidade com a norma ISO/IEC 27005:2008

O framework estabelecido por esta nova norma é plenamente aplicável à maneira que a Mehari permite gerir os riscos, por exemplo:

- Processos de análise de risco, avaliação e tratamento (retirados a partir da ISO 13335),
- Identificação dos bens primários e de apoio como também os níveis de classificação que lhes são inerentes, após uma análise de desafios,
- Identificação de ameaças incluindo seus níveis (exposição natural), para o qual Mehari é mais precisa para a descrição dos cenários de risco,
- Identificação e quantificação da eficácia das medições de segurança (ou controles) na redução das vulnerabilidades,
- Combinação destes elementos para a avaliação do nível de gravidade dos cenários de risco, em uma escala com 4 níveis.
- Capacidade de selecionar diretamente as medições de segurança necessárias para os planos de redução de riscos.

Portanto, Mehari não apenas integra-se facilmente aos processos de ISMS , como difundidos pela ISO 27001, mas atende completamente aos requisitos da norma ISO 27005 para o método de gestão de risco.


L'ESPRIT DE L'ÉCHANGE

# CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11, rue de Mogador
75009 Paris (France)
✆ +33 1 53 25 08 80
clusif@clusif.asso.fr

*Baixar publicações CLUSIF pelo site:*

www.clusif.asso.fr