MEHARI 2010

Introducción

Julio 2010

Comisión de Métodos

Plantea tus dudas y comentarios en el foro:
www.mehari.info

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11, rue de Mogador, 75009 PARIS

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

AGRADECIMIENTOS

El CLUSIF quiere agradecer especialmente a Jean-Philippe Jouas por su colaboración, así como a los miembros de la Comisión de Métodos que han participado en la realización de este documento:

El CLUSIF quiere agradecer igualmente a Hugo Llanos (LKS, S. Coop., www.lks.es) que ha realizado la traducción del presente documento al español.

Jean-Philippe	Jouas	Responsable de la Comisión de Métodos
		Responsable del grupo de trabajo Principios, Mecanismos & Base de Conocimientos para MEHARI
Jean-Louis	Roule	Responsable del grupo de trabajo de documentación de 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 INTRODUCCIÓN

La metodología MEHARI se diseño inicialmente, y se actualiza continuamente, para ayudar a los CISO (Chief Information Security Officers) en la gestión de las actividades de la seguridad de la información.
Esta introducción está principalmente dirigida a éstos, pero también está concebida para auditores, CIO o gestores de riesgos que comparten ampliamente los mismos o similares retos.

El espíritu de este documento es describir como se aplica MEHARI. Existen otros documentos disponibles en el CLUSIF, donde se describe con mayor detalle la metodología y las herramientas asociadas, concretamente:

- *MEHARI: Conceptos y especificaciones funcionales,*
- *Guías MEHARI: para*
    - *Análisis y clasificación de amenazas,*
    - *Evaluación de servicios de seguridad y*
    - *Análisis de riesgos,*
- *MEHARI Manual de referencia de servicios de seguridad,*
- MEHARI base de datos de conocimientos.

El primer objetivo de MEHARI es proporcionar un método para la evaluación y gestión de riesgos, concretamente en el dominio de la seguridad de la información, conforme a los requerimientos de la ISO/IEC 27005 :2008, proporcionando el conjunto de herramientas y elementos necesarios para su implementación.[1]

Otros objetivos adicionales son:

- Permitir un análisis directo e individual de situaciones de riesgos descritas en los escenarios,
- Proporcionar un completo conjunto de herramientas específicamente diseñadas para la gestión de la seguridad a corto, medio y largo plazo, adaptables a diferentes niveles de madurez y tipos de acciones consideradas.

De hecho, MEHARI proporciona una metodología consistente, con unas bases de datos de conocimiento adecuadas, para ayudar a los CISO, responsables generales y de seguridad, u otras personas implicadas en la reducción del riesgo, en sus diferentes tareas y actividades.
La relación de MEHARI con el estándar ISO/IEC 27000 se describe al final de este documento.

[1] Las herramientas y medios asociados, proporcionados por MEHARI de acuerdo a l estándar, se encuentran descritos y justificados en: *MEHARI: Conceptos y especificaciones funcionales.*

2 USOS DE MEHARI

MEHARI es, por encima de todo, un método para la evaluación y gestión del riesgo.

En la práctica, esto significa que MEHARI y sus bases de datos de conocimientos relacionadas han sido diseñadas para un análisis preciso de situaciones de riesgo descritas a través de escenarios.

En la práctica diaria, la gestión de la seguridad es una función o actividad que evoluciona con el tiempo. Las acciones correctivas son diferentes en función de si la organización no ha llevado a cabo nada en el dominio, o –por el contrario- ha invertido tiempo y esfuerzo en el mismo.
Durante los primeros pasos en materia de seguridad, es sin duda recomendable realizar un balance de las medidas de seguridad y políticas existentes en la organización, y comparar éstas con las mejores prácticas, para determinar los pasos a seguir.

Tras evaluar la situación y tomar la decisión de implantar la seguridad en la organización, se tienen que decidir actividades concretas. Tales decisiones, que habitualmente se agrupan en planes, reglas corporativas, políticas o un marco de referencia de seguridad, se pueden componer utilizando un enfoque estructurado. Este enfoque puede basarse en un análisis de riesgos, tal y como se requiere por la ISO/IEC 27001 como parte de un SGSI (Sistema de Gestión de la Seguridad de la Información). Existen otros medios, como la comparación, bien interna bien externa, profesional o interprofesional.

En este punto, es cierto que sin mencionar específicamente el análisis de riesgos, debe abordarse la cuestión de los objetivos involucrados en la seguridad. A menudo, a pesar de que la decisión ya se ha tomado, la persona que toma la decisión final en la asignación de presupuesto no dudará en realizar la pregunta "¿es realmente necesario?". Muchos proyectos de seguridad se abandonan o aplazan debido a una falta de una evaluación preliminar -y de un acuerdo general- sobre lo que está en juego.

A menudo más tarde, pero en ocasiones directamente desde el comienzo de un enfoque de seguridad, se cuestiona el riesgo real que la organización o la empresa sufre. Habitualmente se formula en términos similares a lo siguiente: "¿Se han identificado todos los riesgos a los que se puede encontrar expuesta la organización, y hay una garantía de que dichos niveles de riesgo son aceptables?". Esta cuestión puede presentarse a nivel corporativo o en referencia a un proyecto concreto. Es necesaria una metodología que incluya un análisis de riesgos.

MEHARI se fundamenta en el principio de que las herramientas requeridas en cada fase del desarrollo de la seguridad deben ser consistentes. Por ello, tiene que entenderse que cualquier resultado obtenido en una fase debe poder ser reutilizado por otras herramientas o en otro lugar de la organización.

Las diferentes herramientas y módulos de la metodología MEHARI, diseñados para acompañar un análisis de riegos directo e individual, se pueden utilizar de forma separada unas de otras en cualquier etapa del desarrollo de la seguridad, utilizando diferentes enfoques de gestión y garantizando la consistencia de las decisiones resultantes.

Todas estas herramientas y módulos –someramente descritos debajo- componen un método coherente de evaluación de riesgos con las herramientas y módulos de soporte requeridas para el análisis de los objetivos y auditoría de la calidad de las medidas de seguridad, etc.

2.1 Análisis o evaluación de riesgos

El análisis de riesgos se menciona en prácticamente todas las publicaciones relativas a seguridad, como la fuerza tractora para determinar los requerimientos de seguridad, y esto se afirma nuevamente en los estándares ISO/IEC. Sin embargo, la mayoría de estas publicaciones no discuten los métodos que pueden ser utilizados.

Durante más de 15 años, MEHARI ha proporcionado un enfoque estructurado para la evaluación del riesgo, basándose en unos pocos simples principios.

Una situación de riesgo se puede caracterizar por diferentes factores:

- Factores estructurales (u organizacionales), los cuales no dependen de medidas de seguridad, sino de la actividad principal de la organización, su entorno y su contexto.
- Factores de reducción del riesgo, que son una función directa de las medidas de seguridad implementadas.

De hecho, el análisis de la seguridad es necesario para determinar el nivel máximo de gravedad como consecuencia de una situación de riesgo. Esto es típicamente un factor estructural, mientras que la evaluación de la seguridad se utilizará para evaluar los factores de reducción del riesgo.

MEHARI permite la evaluación cualitativa y cuantitativa de esos factores, y colabora en la evaluación de los niveles de riesgo como consecuencia de ello. MEHARI integra herramientas (como criterios de evaluación, fórmulas, etc.) y bases de datos de conocimiento (en particular para el diagnóstico de las medidas de seguridad), que son un complemento esencial al marco mínimo propuesto por la ISO/IEC 27005.

2.1.1 Análisis sistemático de situaciones de riesgo

Con el fin de contestar a la pregunta "¿Cuáles son los riesgos sobre la Organización y si son aceptables o no?", es necesario un enfoque estructurado que permita identificar todas las situaciones potenciales de riesgo, con el fin de analizar individualmente las más críticas y poder identificar las acciones para reducir el riesgo a niveles aceptables.

El enfoque proporcionado por MEHARI se basa en una base de datos de conocimientos y en procedimientos automatizados para la evaluación de los factores que caracterizan cada uno de los riesgos, y que permite evaluar su nivel. Además, el método proporciona asistencia para la selección de los planes de tratamiento adecuados.

Con el fin de evaluar el riesgo, se proponen dos opciones principales:

- Utilizar una serie de funciones de la base de datos de conocimiento (para Microsoft Office o Open Office) que permiten integrar los resultados de los módulos de MEHARI (p.e.: clasificación de activos en base al análisis de objetivos, diagnósticos de seguridad). Desde estas funciones es posible evaluar el nivel actual de riesgo y proponer medidas adicionales para la reducción del mismo.
- Emplear una aplicación software (como RISICARE[2]) que proporciona una interfaz más completa que permite simulaciones, visualizaciones y más optimizaciones.

2.1.2 Análisis espontáneo de las situaciones de riesgo

Se puede utilizar el mismo conjunto de herramientas en cualquier momento en otros enfoques de la gestión de la seguridad.

[2] De BUC S.A.

En algunos modelos de gobernanza de la seguridad, donde la gestión de riesgos no es el principal objetivo y donde la seguridad se gestiona a través de auditorías o marcos de referencia de seguridad, habrá casos específicos en los que las reglas no puedan ser aplicadas. En estos casos se puede utilizar el análisis de riesgos espontáneo para decidir cómo proceder de la forma más correcta.

2.1.3 Análisis de riesgos en nuevos proyectos

El modelo de análisis de riesgos y mecanismos se puede utilizar en la gestión de proyectos, con el fin de planificar el riesgo y decidir qué medidas deben implementarse como resultado del mismo.

2.2 Evaluaciones de seguridad

MEHARI integra cuestionarios de controles de seguridad, lo que permite evaluar el nivel de calidad de los mecanismos y soluciones encaminadas a la reducción del riesgo[3].

2.2.1 Revisión de vulnerabilidades, un elemento del análisis de riesgos

MEHARI proporciona un modelo de riesgos estructurado que considera los "factores de reducción del riesgo" en forma de servicios de seguridad.

El resultado de la evaluación de la vulnerabilidad será, por lo tanto, una entrada fundamental para el análisis de riesgos, con el fin de garantizar que los servicios de seguridad cumplen realmente su cometido – un punto esencial para la credibilidad y fiabilidad del análisis de riesgos.

Una Fortaleza esencial de MEHARI es su capacidad de evaluar el nivel de riesgo actual así como los nivel(es) futuro(s) en base a una base de datos experta de conocimientos para evaluar el nivel de la calidad de las medidas de seguridad.

2.2.2 Planes de seguridad basados en la revisión de vulnerabilidades

Un posible enfoque es la confección de planes de seguridad como resultado directo de la evaluación del estado de los servicios de seguridad.

El proceso de gestión de la seguridad siguiendo este enfoque es muy sencillo: ejecutar una evaluación y decidir mejorar todos aquellos servicios que no tienen un suficiente nivel de calidad.

Los cuestionarios de diagnostico de MEHARI se pueden utilizar para este tipo de enfoque.

Se debe planificar igualmente un análisis preliminar de los riesgos del negocio con el fin de proporcionar un vínculo con este módulo de MEHARI. El análisis de objetivos permite determinar los niveles de calidad requeridos para los servicios de seguridad relevantes y, consecuentemente, ignorar el resto como parte del análisis.

[3] Los controles, o medidas, de seguridad se agrupan en subservicios, después en servicios y finalmente en dominios de seguridad.

2.2.3 Apoyo de las bases de datos de conocimiento en la creación de un marco de referencia de seguridad

Las bases de datos de conocimiento de MEHARI se pueden utilizar directamente para crear un marco de referencia de seguridad (o políticas de seguridad) que contendrá, y describirá, el conjunto de reglas e instrucciones de seguridad que debe seguir la empresa u organización.

Este enfoque se utiliza frecuentemente en organizaciones o empresas con un alto número de unidades operacionales o localizaciones independientes. Es el caso de las grandes compañías multinacionales con un alto número de subsidiarias, pero se puede aplicar fácilmente a compañías de tamaño medio con un alto número de delegaciones o agencias regionales. En estos casos, la realización de numerosas evaluaciones o análisis de riesgos resulta complicado.

Construyendo el marco de referencia de seguridad

Los cuestionarios de evaluación de MEHARI son una buena base de trabajo para los responsables de seguridad para decidir lo que debe ser aplicado en la organización.

Gestionando las excepciones desde las reglas

La creación de un conjunto de reglas, a través de un marco de referencia de seguridad, se enfrenta a menudo a dificultades en la implementación local, por lo que se deben gestionar exenciones y excepciones a las reglas.

Utilizando una base de datos de conocimiento coherente, con un conjunto consistente de herramientas y de metodología analítica, permite gestionar las divergencias locales. Las peticiones de excepciones se pueden cubrir a través de un análisis de riesgos específico para la dificultad identificada.

2.2.4 Dominios cubiertos por el modulo de evaluación de vulnerabilidades

Desde un punto de vista de análisis de riesgos, en base a la identificación de todas las situaciones de riesgo y con el deseo de cubrir todos aquellos riesgos inaceptables, MEHARI no se limita simplemente al dominio IT.

El modulo de evaluación cubre, además de los sistemas de información, el conjunto de la organización, así como la protección del sitio en general, así como el entorno de trabajo y aspectos legales y regulatorios.

2.2.5 Descripción general del modulo de evaluación

El único punto a tener en cuenta sobre el módulo de evaluación de vulnerabilidades es que proporciona una visión amplia y coherente de la seguridad. Esto puede utilizarse en una gran variedad de enfoques, evolucionando en profundidad y granularidad del análisis, y se puede utilizar en todas las etapas de madurez en la concienciación y organización de la seguridad en la organización.

2.3 Análisis de amenazas

Seguridad es proteger los activos. Sea cual sea la orientación de la política de seguridad, hay un principio en el que coinciden todos los responsables: debe existir un equilibrio entre las inversiones de seguridad por un lado y en la importancia de los principales retos empresariales por el otro.

Esto significa que la comprensión de las amenazas al negocio es fundamental, y que el análisis del contexto de seguridad merece un nivel prioritario y un método estricto y riguroso de evaluación.

El fin del análisis de las amenazas de seguridad es responder a la siguiente doble pregunta:

"¿Qué puede suceder, y si sucede, puede ser serio?"

Esto demuestra que, en el Área de la Seguridad, las amenazas se consideran como consecuencias de eventos que interrumpen las operaciones previstas de una empresa u organización.

MEHARI proporciona un modulo de análisis de amenazas, descrito en *MEHARI: Análisis y clasificación de amenazas,* que proporciona dos tipos de resultados:

- Una escala de valores de malfuncionamiento
- Una clasificación de la información y de los activos TI

La escala de valores de malfuncionamiento

La identificación de malfuncionamientos o eventos potenciales es un proceso que comienza con las propias actividades de la empresa, y consiste en la identificación de posibles malfuncionamientos en sus procesos operacionales. Esto resultará en:

- La descripción de los posibles tipos de malfuncionamientos.
- La definición de parámetros que influyen en cada malfuncionamiento.
- Una evaluación de los umbrales críticos de dichos parámetros que cambian el nivel de gravedad del malfuncionamiento.

Este conjunto de resultados constituye la escala de valores de malfuncionamiento.

Clasificación de la información y de los activos

En la seguridad de los sistemas TI es habitual hablar de la clasificación de la información y de la clasificación de los activos TI.

Esta clasificación consiste en la definición, para cada tipo de información y para cada activo TI, y para cada criterio de clasificación (habitualmente: Disponibilidad, Integridad y Confidencialidad, aunque pueden utilizarse otros criterios, como Auditabilidad), de los indicadores representativos de la gravedad del criterio sobre el que impacta o de la pérdida de la información o activo.

La clasificación de la información y de los activos para los Sistemas de Información, es la escala de valores de malfuncionamiento definida anteriormente traducido a indicadores de sensibilidad asociados con los activos TI.

Definiendo amenazas de seguridad

La escala de valores de malfuncionamiento y la clasificación de la información y activos son dos formas distintas de expresar las amenazas de seguridad.

El primero es más detallado y proporciona más información a los CISO. El segundo es más generalista y resulta más útil para las campañas de sensibilización e información, pero es menos granular.

2.3.1 Analizando las amenazas, la base para un análisis de riesgos

Sin duda alguna, este modulo es la clave en un análisis de riesgos. Sin un acuerdo común sobre las consecuencias de potenciales malfuncionamientos no es posible ningún juicio sobre los niveles de riesgo.

MEHARI presenta un método riguroso para la evaluación de las amenazas y para la clasificación de los activos, que proporcionan datos objetivos y racionales.

2.3.2 El análisis de las amenazas de seguridad: la piedra angular de cualquier plan estratégico de acción

Obviamente se requiere el análisis de amenazas para la puesta en marcha de cualquier tipo de plan de seguridad. Efectivamente, sin importar el enfoque utilizado, en algún punto se determinarán los medios necesarios para la implantación de los planes de acción, e inevitablemente, se requerirá la justificación de dichas inversiones.

Los medios y fondos que se destinarán a la seguridad son, como las pólizas de seguros, directamente proporcionales al riesgo. Si no hay un acuerdo común sobre el potencial malfuncionamiento, es raro que se llegue a asignar presupuesto.

2.3.3 Clasificación: un elemento esencial para las políticas de seguridad

Ya se han mencionado anteriormente en este documento los marcos de referencia, las políticas y los enfoques de gestión de la seguridad asociados.

En la práctica, las empresas que gestionan la seguridad a través de un conjunto de reglas se encuentran obligadas a diferenciar entre las propias reglas y entre las acciones que se tienen que implementar en función de la sensibilidad de la información procesada. Esto es común a la hora de referirse a la clasificación de la información y de los activos TI.

El modulo de análisis de amenazas de seguridad de MEHARI proporciona los medios necesarios para realizar esta clasificación.

2.3.4 Análisis de las amenazas de seguridad: fundamento de la planificación de la seguridad

El propio proceso de análisis de las amenazas de seguridad que obviamente requieren de la contribución de los responsables operacionales, conlleva habitualmente la necesidad de acciones inmediatas.

La experiencia demuestra que cuando se entrevista a los altos niveles de gestión operativa sobre su punto de vista y estimación de malfuncionamientos importantes, con independencia del tamaño de la organización, conduce a necesidades de seguridad que no se habían considerado previamente y que requieren de una rápida respuesta.

Los planes de acción se pueden confeccionar directamente a través de un enfoque ligero y directo basado en la combinación de dos tipos de experiencias: la de la propia actividad profesional, proporcionada por la gestión operativa, y la de las soluciones de seguridad, proporcionada por expertos en este ámbito.

2.4 Introducción general de la utilización de MEHARI

La principal orientación de MEHARI es la evaluación y reducción de riesgos. Sus bases de datos de conocimiento, mecanismos y herramientas se han creado con ese objetivo.

Asimismo, en la mente de los diseñadores del conjunto de la metodología, la necesidad de un método estructurado para el análisis y reducción de riesgos puede ser, en función de la organización:

- Un método permanente de trabajo – la línea base para un grupo especializado,
- Un método de trabajo utilizado en paralelo junto a otras prácticas de gestión de la seguridad,
- Un método de trabajo utilizado de forma ocasional para complementar otras prácticas regulares.

Con esto en mente, MEHARI proporciona un conjunto de enfoques y herramientas que permiten realizar un análisis de riesgos cuando es necesario.

La metodología MEHARI, que comprende las bases de datos de conocimiento, los manuales y las guías que describen los diferentes módulos (amenazas, riesgos, vulnerabilidades), se encuentra disponible para ayudar a las personas implicadas en la gestión de la seguridad (CISO, responsables de riesgos, auditores, CIO,…), en sus diferentes tareas y actividades.

3 MEHARI Y LOS ESTÁNDARES ISO/IEC 27000

Una pregunta frecuente es como se alinea MEHARI con los estándares internacionales, en particular con la serie ISO/IEC 27000.

El objetivo de este apartado es explicar cómo encaja MEHARI con los estándares ISO 27001, 27002 y 27005, en términos de compatibilidad y objetivos.

3.1 Objetivos de la ISO/IEC 27001, 27002, 27005 y MEHARI, respectivamente

3.1.1 Objetivos del estándar ISO/IEC 27002:2005

Este estándar estipula que una organización debe identificar sus requerimientos de seguridad utilizando para ello tres fuentes principales:

- El análisis de riesgos,
- Requerimientos legales, estatutarios, regulatorios o contractuales,
- El conjunto de principios, objetivos y requerimientos que aplican al procesamiento de la información que la organización ha desarrollado para soportar sus operaciones.

Utilizando esto como base, hay que identificar e implementar los puntos de control, de acuerdo a la lista proporcionada en la sección del estándar "Código de buenas prácticas para la gestión de la seguridad de la información" u otros conjuntos de puntos de control (§4.2).

Observación: en el alcance de la 27002:2005 se estipula que el estándar proporciona "directrices y principios generales para la puesta en marcha, implementación, mantenimiento y mejora de la gestión de la seguridad de la información", lo que significa que el estándar ISO debe entenderse como un punto de partida. Sin embargo, la ISO/IEC 27001 estipula (§1.2) que cualquier exclusión debe justificarse y que es susceptible de añadir nuevos puntos de control (Apéndice A – A.1)

El estándar ISO 27002 proporciona un recopilatorio de directrices que pueden utilizarse por cualquier organización. Se señala, en cualquier caso, que la lista no es exhaustiva y que se pueden emplear otras medidas complementarias. Sin embargo, no se recomienda ninguna metodología para la creación de un sistema completo de gestión de la seguridad.

Por otro lado, cada apartado de la guía de buenas prácticas incluye introducciones y comentarios sobre los objetivos perseguidos, que resulta de una buena ayuda.

Observación: el estándar ISO estipula asimismo en su alcance, que puede ser utilizado para "ayudar en la implementación de la confidencialidad en las actividades inter-organizacionales". Esto no está incluido por casualidad, y pone de relieve un aspecto esencial que los patrocinadores del estándar promueven, que es la evaluación (incluso la certificación), desde un punto de vista de la seguridad de la información, de partners y proveedores.

3.1.2 Objetivos de la ISO/IEC 27001:2005

El principal objetivo de la ISO/IEC 27001 es "proporcionar un modelo para implementar y administrar un **sistema de gestión de la seguridad de la información (SGSI)**" y para "ser utilizado internamente o por terceras partes, incluyendo las entidades de certificación".

Los objetivos de la evaluación y certificación ponen especial hincapié en los aspectos formales (documentación y registro de decisiones, declaración de aplicabilidad, registros, etc.) y los controles (revisiones, auditorías, etc.).

Está claro que la base de un enfoque de seguridad implica que tienen que llevarse a cabo análisis de riesgos para determinar a cuales se encuentra expuesta la organización, y para seleccionar las medidas adecuadas para la reducción del riesgo a un nivel aceptable (apartado 4.2.1).

La ISO/IEC 27001 determina que se debe utilizar una metodología de análisis de riesgos, pero ésta no forma parte del estándar, y tampoco se propone ningún método específico, aparte de su integración en el PDCA (Plan, Do, Check, Act), proceso recursivo del modelo tal y como se encuentra definido en la creación del SGSI.

Asimismo, las recomendaciones o *buenas prácticas* que se pueden emplear en la reducción del riesgo se encuentran "alineadas con aquellas listadas en la ISO/IEC 27002:2005", mientras que se proporciona una lista de puntos de control asociados en los apéndices.

De acuerdo a la ISO/IEC 27001, la base de la **evaluación del sistema de gestión de seguridad** no es tanto el conocimiento o la verificación de que las decisiones que se han tomado son apropiadas y adecuadas a las necesidades de la organización, sino más bien para verificar que una vez que se han tomado las decisiones, el sistema de gestión permite que un auditor o certificador pueda estar seguro de que las decisiones se encuentran realmente implantadas.

3.1.3 Objetivos de la ISO/IEC 27005:2008

Los objetivos de este estándar no son la constitución de un método de gestión de riesgos, sino más bien fijar un marco mínimo de trabajo y describir los requerimientos para el proceso de evaluación de riesgos en si mismo, para la identificación de las amenazas y vulnerabilidades que permiten estimar el riesgo, su nivel, y estar entonces en situación para seleccionar un modo de tratamiento así como los planes y medidas adecuados destinados a evaluar y mejorar la situación.

La norma establece que se debe seleccionar un método de análisis de riesgos de acuerdo a estos requisitos, con el fin de evitar el uso de métodos inconsistentes o simplistas, coincidiendo con la intención de los editores de la norma.

3.1.4 Objetivos de MEHARI

MEHARI es un conjunto de herramientas y funcionalidades metodológicas para la gestión de la seguridad y de las medidas asociadas, basado en un análisis de riesgos preciso. Los aspectos fundamentales de MEHARI son:

- Su modelo de riesgos (cualitativo y cuantitativo),
- el examen de la eficacia de las medidas de seguridad en vigor o previstas,
- la capacidad para evaluar y simular los niveles de riesgo derivados de medidas adicionales,

complementos obligatorios a los requerimientos de la norma ISO/IEC 27000 y particularmente de la ISO/IEC 27005.

3.1.5 Comparativa entre los objetivos de MEHARI y las normas ISO/IEC 27001 y 27002

Los objetivos de MEHARI y de las normas ISO mencionadas son radicalmente diferentes.

- Mehari tiene como objetivo proporcionar herramientas y métodos que se pueden utilizar para seleccionar las medidas de seguridad más adecuadas para una organización, y para evaluar los riesgos residuales una vez que estas medidas están implementadas. Este no es el objetivo primordial declarado en las normas ISO.
- Las normas ISO proporcionan un conjunto de mejores prácticas, que sin duda son muy útiles, pero no necesariamente apropiadas para lo que está en juego en la organización, y son útiles para cubrir los aspectos de madurez en seguridad, planificación de la seguridad de la información, independiente de las unidades internas y partners.

El **manual de referencia de servicios de seguridad** de MEHARI proporciona elementos detallados que se pueden utilizar para construir un marco de referencia de seguridad comparable a la ISO/IEC 27002. En este punto, está claro que la cobertura de MEHARI es más amplia que la ISO, y que cubre aspectos esenciales de seguridad más allá de los sistemas de información.

3.2 Compatibilidad entre enfoques

El enfoque de MEHARI es totalmente complementario a la ISO 27002, ya que si bien no tienen los mismos objetivos declarados, es relativamente sencillo para representar los resultados del análisis de MEHARI en términos de indicadores de la ISO 27002.

MEHARI responde a las necesidades, expresadas en las normas ISO 27001 y 27002, para un análisis de riesgos que permita definir las medidas que deben ser implementadas.

3.2.1 Compatibilidad con la norma ISO/IEC 27002:2005

Los puntos de control de la norma o las *mejores prácticas* de la ISO son generalistas, situacionales o medidas organizativas, mientras que MEHARI, de forma adicional, hace hincapié en la necesidad de medidas cuya eficiencia pueda ser garantizada.

A pesar de estas diferencias, la revisión de vulnerabilidades de MEHARI proporciona tablas de correspondencia para alinear indicadores con el desglose utilizado en la norma ISO 27001:2005, utilizable por aquellos que necesitan demostrar el cumplimiento con dicha norma.
Vale la pena mencionar que los cuestionarios de auditoría de MEHARI se han diseñado y constituido con el fin de permitir a los responsables operacionales realizar revisiones de vulnerabilidades de forma eficiente y deducir la capacidad de cada servicio de seguridad para la reducción de dichos riesgos.

3.2.2 Compatibilidad con la norma ISO/IEC 27001

MEHARI se puede integrar de forma sencilla en el proceso PDCA (Plan – Do – Check – Act) tal y como se encuentra formulado por la ISO/IEC 27001, principalmente en la fase 'PLAN' (§4.2.1). MEHARI cubre completamente la descripción de las tareas que permiten la creación de las bases del SGSI.

Para la fase 'DO' (§4.2.2), cuyo objetivo es implementar y administrar el SGSI, MEHARI proporciona elementos útiles de partida, como la construcción de planes para la gestión del riesgo, con priorización directamente relacionada a la clasificación de los riesgos y las medidas de progreso durante su uso.

Para la fase 'CHECK' (§4.2.3), MEHARI proporciona elementos que permiten la evaluación del riesgo residual, y las mejoras efectuadas sobre las medidas de seguridad. Además, cualquier cambio en el entorno (los riesgos, amenazas, soluciones y organización) pueden ser fácilmente reevaluados por auditorias concretas que utilicen los resultados de la auditoría inicial sobre MEHARI. De esta forma, los panes de seguridad se pueden revisar y evolucionar a lo largo del tiempo.
Para la fase 'ACT' (§4.2.4), implícitamente MEHARI emplea controles y una mejora continua de la seguridad, asegurando de esta forma que se alcanzan los objetivos de reducción del riesgo. En estas tres fases, si bien MEHARI no se encuentra en el corazón de los procesos, contribuye en gran medida a su puesta en marcha y a asegurar su eficiencia.

3.2.3 Compatibilidad con el estándar ISO/IEC 27005:2008

El marco de trabajo expuesto en este nuevo estándar es totalmente aplicable en la forma en la que MEHARI permite la gestión de riesgos, por ejemplo:

- Los procesos del análisis, evaluación y tratamiento de riesgos (extraídos de la ISO 13335),
- La identificación de los activos principales y los de soporte, así como la clasificación en niveles aparejada a los mismos, tras el análisis de amenazas,
- La identificación de amenazas incluyendo su nivel (exposición natural), para el que MEHARI es muy preciso en la descripción de los escenarios de riesgo,
- La identificación y cuantificación de la eficiencia de las medidas de seguridad (o controles) en la reducción de vulnerabilidades,
- La combinación de estos elementos para la evaluación del nivel de severidad de los escenarios de riesgos,
- La habilidad de seleccionar directamente las medidas de seguridad requeridas para los planes de reducción de riesgos.

Por lo tanto, MEHARI no sólo se integra fácilmente en un SGSI, tal y como se solicita por la ISO 27001, sino que cumple con los requerimientos de la ISO 27005 para un método de gestión de riesgos.