

*Exposé sur la cybersécurité*

**NOMS DES EXPOSANTS :**

**-NDENGUE FONZE Brindel Ronel**

**-MATANGA ENDALE FRANCE BROOKLYN**

**-SANAMA KING**

**-SONTIA ZIDANE**

**-TAMO LLOYD EVRA**

**PLAN**

INTRODUCTION

* LE POURQUOI ANALYSER LES ENJEUX
* PRINCIPE DE BASE DE MÉHARI
* MODELE DE RISQUE DE MÉHARI
* APPORT DES BASES DE CONNAISSANCES
* LES DIFFERENTES VERSIONS DE MÉHARI
* CAS PRATIQUE DE LA METHODE MEHARI SUR KEYCE

CONCNLUSION

**INTRODUCTION**

La méthode MEHARI (Méthode Harmonisée d'Analyse de Risques) est une approche reconnue et largement utilisée pour évaluer les risques liés à la sécurité de l'information dans les organisations. Développée par le Club de la Sécurité des Systèmes d'Information Français (CLUSIF), elle offre une méthodologie structurée et complète pour identifier, évaluer et gérer les risques de manière efficace.L'objectif principal de la méthode MEHARI est de permettre aux organisations de comprendre les menaces qui pèsent sur leurs actifs informationnels, d'évaluer l'impact potentiel de ces menaces et de mettre en place des mesures de sécurité appropriées pour atténuer les risques identifiés. La méthode MEHARI propose également des outils et des modèles pour faciliter le processus d'analyse des risques, tels que des catalogues de menaces, des fiches d'évaluation des vulnérabilités et des matrices d'évaluation des risques. Ces outils fournissent une structure et une méthodologie claires pour guider les professionnels de la sécurité dans leur travail d'évaluation des risques.C’est donc une méthode qui offre une approche complète et structurée pour analyser les risques de sécurité de l'information. Elle permet aux organisations de mieux comprendre les menaces, les vulnérabilités et les risques associés, et de prendre des mesures proactives pour protéger leurs actifs informationnels. En appliquant cette méthode, les organisations peuvent renforcer leur posture de sécurité et réduire les impacts potentiels des incidents de sécurité.

* **Le pourquoi analyser les enjeux**

**L’analyse des enjeux**

***« Que peut-on redouter et, si cela devait arriver, serait-ce grave »***. C’est ainsi qu’est défini l’analyse des enjeux dans la méthode Mehari.

Il y des éléments importants de reflexion concernant la réponses à apporter à cette question. Les utilisateurs savent bien répondre sur la deuxième   
partie de la question, c’est à dire l’impact du sinistre sur son activité (indisponibilité d’une application, de la totalité du système d’information, perte de confidentialité, … ), mais en revanche ont des difficultés à identifier les origines des sinistres (sauf peut être celles qui sont liées à leur propres collaborateurs).

Cette analyse d’enjeux a donc pour objectifs :

* d’identifier les macro-processus clefs pour l’entreprise
* d’analyser l’impact de scénarios de sinistres et de classer ces impacts
* d’en déduire une classification des actifs essentiels (applications, matériels, équipement mais également ressources humaines).
* **principe de base de MÉHARI**

Le domaine visé par MÉHARI est celui de la sécurité de l’information, englobant les systèmes informatisés mais aussi l’information sous toutes ses formes, numériques, analogiques, écrites, etc.

Dans ce domaine, l’objectif de MÉHARI n’est pas seulement d’identifier les situations de risque et d’en apprécier le niveau, mais de mettre en évidence les mesures permettant de ramener les risques à un niveau acceptable.

Au-delà de la nature des mesures à mettre en œuvre, MÉHARI s’attache en outre à en définir le niveau de qualité et d’efficacité requis.

Enfin, Tous les modules de MÉHARI sont fondés sur un principe de base qui est de ne jamais sous-évaluer un risque et qui se décline de deux manières :

Toujours envisager le pire en termes de conséquences ;

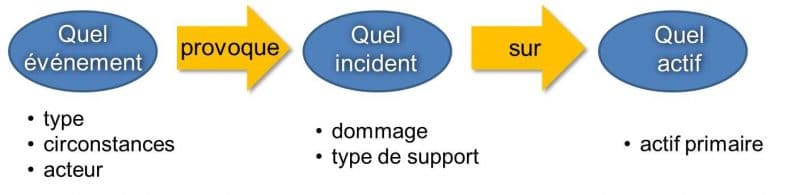
* Ne tenir compte que des effets « contrôlés » des mesures de sécurité.
* **Modèle de risque de MÉHARI**

MÉHARI est basé sur un modèle de risque qui comprend :

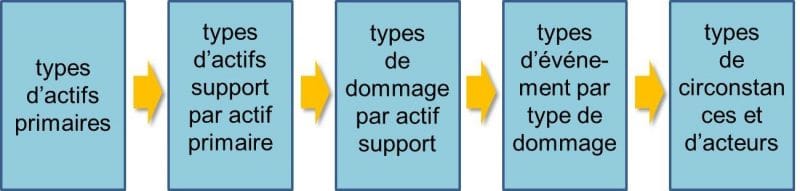
* un aspect « qualitatif » visant à mettre en lumière les différents aspects d’un risque et de sa survenance, afin de mieux comprendre les paramètres qui jouent sur le niveau de gravité du risque ;
* et un aspect « quantitatif » visant à quantifier les divers facteurs de risque et à pondérer les effets cumulés des services de sécurité, afin de pouvoir évaluer les niveaux de risque.

### Le modèle de risque qualitatif

MÉHARI décrit chaque risque comme un scénario qui comprend plusieurs éléments, chaque élément étant décrit et expliqué.



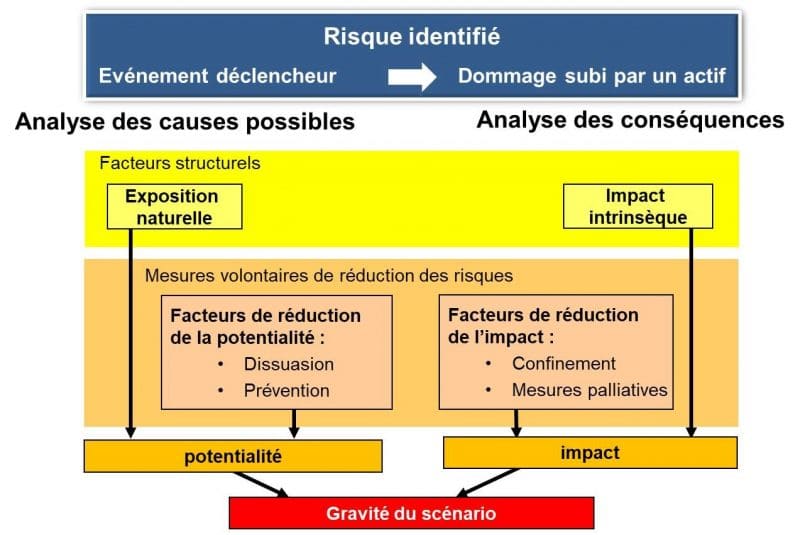
Pour ce faire, MÉHARI définit des typologies qui permettent une standardisation des descriptifs et une exhaustivité dans la recherche des situations de risque.



Sur la base de ces éléments et typologies, MÉHARI décrit quatre modes d’action possibles des mesures visant à réduire des risques :

* La « dissuasion » qui a pour effet de diminuer, par des mesures « dissuasives », la probabilité qu’un acteur décide de mener l’action à l’origine du risque ;
* La « prévention » qui rend plus difficile, donc moins probable, le fait que le déclenchement de l’événement initial conduise effectivement à la réalisation du risque ;
* Le « confinement » qui va limiter l’étendue des dommages directs possibles ;
* La « palliation » qui limite l’étendue des conséquences indirectes des dommages.

Ces modes d’action sont des « Facteurs de réduction de risque ». Le modèle global en résultant est présenté sur le schéma ci-dessous :



### Le modèle de risque quantitatif

La partie « quantitative » du modèle de risque comprend trois aspects essentiels :

* La définition de services de sécurité et l’évaluation quantitative de la qualité de ces services (voir sur ce point la description du module « Diagnostic de l’état des services de sécurité ») ou, pour Méhari-ManagerBC la définition de fonctions de sécurité et l’évaluation quantitative des effets de ces fonctions;
* L’évaluation quantitative, pour chaque scénario de risque, des facteurs de réduction de risque. Chaque scénario décrit dans les bases de connaissances de MÉHARI contient les éléments nécessaires et suffisants à l’évaluation de ces facteurs, en fonction de la qualité des services ou fonctions de sécurité pertinents pour ce scénario ;
* L’évaluation des effets cumulés des facteurs de réduction de risque et, in fine, l’évaluation chiffrée du niveau de gravité de chaque risque. Les bases de connaissances contiennent également les fonctions de calcul et les algorithmes permettant, sur la base des éléments ci-dessus, d’évaluer la gravité de chaque situation de risque.
* Apport des bases de connaissances

La richesse de MÉHARI est basée sur l’utilisation de bases de connaissances.  
Les bases de connaissances de MÉHARI permettent, par une dépersonnalisation et une généralisation des situations de risque, de :

* viser l’exhaustivité des situations de risque analysées ;
* apporter de l’expertise ;
* s’enrichir de l’expérience cumulée ;
* harmoniser et coordonner les plans d’action.

Les bases de connaissances de chaque version de MÉHARI contiennent :

* Des scénarios de risque standards ;
* Des dispositifs de sécurité matérialisés par des « services de sécurité » ou des « fonctions de sécurité » ;
* Des questionnaires d’évaluation de ces services (Méhari-Expert et Méhari- Standard);
* Des mécanismes d’évaluation de l’ensemble des paramètres caractéristiques des risques ;
* Des mécanismes d’aide à la définition de plans et projets de sécurité aptes à réduire les risques ;
* Des outils de pilotage des risques.

MÉHARI comprend trois bases de connaissances :

* [Méhari-E](https://clusif.fr/management_des_risques/les-versions-de-mehari/mehari-expert/)[xpert](https://clusif.fr/services/management-des-risques/les-versions-de-mehari/mehari-expert/) : version destinée aux grandes ou très grandes entreprises et nécessitant une bonne expertise de la méthode ;
* [Méhari-Standard](https://clusif.fr/services/management-des-risques/les-versions-de-mehari/mehari-standard/) : version, destinée aux entreprises moyennes ou grandes, dotée de plus d’outils de pilotage et d’accès plus facile ;
* [Méhari-ManagerBC](https://clusif.fr/services/management-des-risques/les-versions-de-mehari/mehari-manager-bc/) : version destinée aux analyses ciblées d’activités ou de projets.
* LES DIFFERENTES VERSIONS DE MÉHARI
* avec base d’audit des services de sécurité

Les bases de connaissances de [MÉHARI – Expert](https://clusif.fr/services/management-des-risques/les-versions-de-mehari/mehari-expert/) et de [MÉHARI – Standard](https://clusif.fr/services/management-des-risques/les-versions-de-mehari/mehari-standard/) se différencient principalement par le niveau de détail avec lequel sont décrits ou définis :

* Les actifs primaires, répartis entre actifs de service (fonctionnels), actifs de données (nécessaires aux services fonctionnels) et processus de management (les règles et comportements qu’il convient de respecter) ;
* Dans une très faible mesure, les types d’incidents que peuvent subir ces actifs ;
* Les menaces pouvant être à l’origine des incidents que peuvent subir ces actifs ;
* Les services de sécurité pouvant venir réduire ces risques qui doivent être en cohérence avec les types d’actifs et les menaces considérées.

En outre, les aides à l’évaluation des risques et les outils de pilotage de la réduction des risques sont plus ou moins développés selon les bases de connaissances.

Enfin, il existe des différences de correspondances avec les contrôles de la norme ISO 27002, selon les bases de connaissances.

Les différences de conception des bases de connaissances évoquées ci-dessus ont plusieurs types de conséquences.

### La précision de l’identification des risques et leur analyse

En pratique, les différences entre les bases traduisent différentes manières de décrire l’architecture du système (au sens large) de traitement de l’information et l’organisation en charge d’administrer et de piloter ce système :

* Vision plus ou moins globale de l’infrastructure informatique et télécom et des services de sécurité associés ;
* Regroupement plus ou moins fin des catégories d’acteurs et des circonstances de survenance d’un incident.

Cela se traduit par des scénarios de risque plus ou moins détaillés et en nombre plus ou moins grand et, en corollaire, par une vision des risques plus ou moins globale au moment de la prise de décision.

Il est clair cependant que si l’analyse est moins détaillée lors de la prise de décision, elle pourra l’être davantage, et le sera le plus souvent, lors du déploiement et de la mise en place des mesures correctrices.

Ceci étant des architectures complexes seront mieux analysées par une base telle que MÉHARI – Expert.

#### La répartition dans le temps de la charge d’analyse et de planification des actions correctrices

Une autre manière de décrire les différences entre bases est de considérer que cela revient, en grande partie, à répartir différemment dans le temps les charges de travail d’analyse : plus d’analyse avant décision de plans d’action avec les bases plus détaillées, plus d’analyse après décision et avant déploiement avec les bases plus globales.

#### Les outils de pilotage et de management des risques

Les outils de pilotage comprennent deux types d’aides :

* Les présentations de « panorama » de risques ;
* Les outils d’aide à la sélection des mesures nécessaires ;
* Les outils de simulation de l’effet des mesures décidées.

Ces outils sont plus ou moins développés selon les bases et sont décrits dans les paragraphes correspondant à chacune d’elles.

### La correspondance avec les contrôles de l’ISO 27002

Alors que les bases de connaissances contiennent des questionnaires de diagnostic de l’état des services de sécurité, certaines entreprises souhaitent faire un lien entre les réponses à ces questionnaires et la conformité aux bonnes pratiques recommandées par la norme ISO 27002.

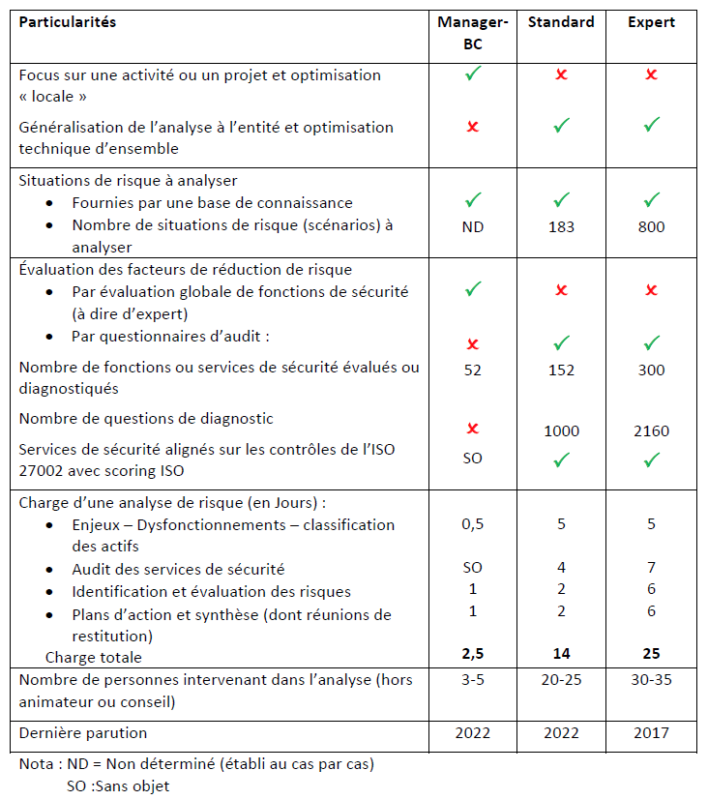
Ce point est abordé de manière différente dans les différentes bases de connaissances et les traitements correspondants sont décrits dans les pages relatives à ces bases.

* Sans base d’audit des services de sécurité

La version actuelle ([MÉHARI – Manager BC](https://clusif.fr/services/management-des-risques/les-versions-de-mehari/mehari-manager/)) est une démarche permettant de s’appuyer sur le modèle de risque de MÉHARI et sur les mêmes éléments de description des risques que Méhari-Standard-2022 pour mener avec des responsables métiers ou des responsables de projets – les « Managers » – une analyse et une réflexion sur les risques auxquels ils sont confrontés et sur les solutions à apporter, en se basant sur une évaluation directe de l’effet des mesures de sécurité sans recourir à un audit précis.

C’est une démarche brève (une journée maximum) et focalisée (un type d’activité ou un projet) qui permet de sensibiliser les responsables et de trouver des solutions « métiers » à des risques spécifiques.

Le tableau ci-dessous offre une comparaison entre les différentes versions de Méhari.



* Description générale de la méthode MEHARI

1. Contexte et périmètre

La première étape de la méthode MEHARI consiste à définir le contexte et le périmètre de l'évaluation des risques. Cela comprend la compréhension des activités, des actifs, des processus et des systèmes d'information concernés.

2. Identification des actifs

Dans cette étape, les actifs du système d'information sont identifiés. Cela peut inclure des informations sensibles, des infrastructures, des applications, des bases de données, des équipements, etc.

3. Identification des menaces

Les menaces potentielles qui pourraient affecter les actifs sont identifiées. Cela peut inclure des attaques informatiques, des catastrophes naturelles, des erreurs humaines, des pannes de matériel, etc.

4. Évaluation des vulnérabilités

Les vulnérabilités du système d'information, c'est-à-dire les faiblesses qui pourraient être exploitées par les menaces, sont évaluées. Cela peut inclure des vulnérabilités logicielles, des erreurs de configuration, des lacunes dans les processus, etc.

5. Estimation des risques

Les risques potentiels sont évalués en prenant en compte la probabilité d'occurrence des menaces et la gravité de leurs impacts sur les actifs. Cela permet de prioriser les risques et de se concentrer sur les plus critiques.

6. Proposition de mesures de sécurité

Des mesures et des contrôles de sécurité appropriés sont proposés pour atténuer les risques identifiés. Cela peut inclure des politiques de sécurité, des procédures, des contrôles techniques, des formations, etc.

7. Plan d'action

Un plan d'action est élaboré pour mettre en œuvre les mesures de sécurité recommandées. Il inclut les responsabilités, les échéances et les ressources nécessaires pour chaque action.

8. Suivi et mise à jour

Une fois les mesures de sécurité mises en place, il est essentiel de surveiller régulièrement l'environnement de sécurité, d'effectuer des audits et de mettre à jour le plan d'action en fonction des évolutions.

* Quelques éléments supplémentaires de la méthode MEHARI

La méthode MEHARI offre une approche structurée pour évaluer les risques et mettre en place des mesures de sécurité appropriées dans un environnement de systèmes d'information. Elle permet aux organisations de mieux comprendre les risques auxquels elles sont confrontées et de prendre des décisions éclairées pour protéger leurs actifs informatiques. Elle est basée sur une approche itérative, c'est-à-dire qu'elle encourage une évaluation continue des risques et une amélioration continue de la sécurité de l'information. Parmi ces elements nous pouvons avoir:

1. Méthode qualitative : MEHARI utilise une approche qualitative pour évaluer les risques. Les risques sont évalués en fonction de leur probabilité d'occurrence et de l'impact potentiel sur les actifs. Les évaluations sont généralement effectuées à l'aide de matrices de risques qui permettent de classer les risques en fonction de leur criticité.

2. Modèle de référence : La méthode MEHARI est basée sur un modèle de référence qui fournit une structuration des différentes étapes de l'évaluation des risques. Ce modèle comprend des catégories de risques, des familles de menaces, des types d'actifs, des vulnérabilités courantes, etc. Il fournit un cadre commun pour l'analyse des risques.

3. Adaptabilité : MEHARI est conçu pour être adapté aux besoins spécifiques de chaque organisation. Il peut être utilisé dans différents contextes, tels que les entreprises, les administrations publiques, les organisations à but non lucratif, etc. Les actifs, les menaces et les vulnérabilités spécifiques à chaque organisation peuvent être pris en compte lors de l'évaluation des risques.

4. Documentation et outils : La méthode MEHARI est accompagnée d'une documentation détaillée qui explique chaque étape du processus d'évaluation des risques. De plus, il existe des outils logiciels disponibles pour faciliter la mise en œuvre de la méthode, notamment pour la collecte des informations, l'analyse des risques et la génération de rapports.

5. Alignement avec les normes de sécurité : MEHARI est conçu pour être en conformité avec les normes de sécurité de l'information, telles que la norme ISO 27001. Il fournit une approche structurée et documentée pour satisfaire aux exigences de sécurité et faciliter les évaluations de conformité.

* Quelques actifs généralement inventoriés

**1. Équipements matériels** :

**- Ordinateurs de bureau** : Ce sont des machines utilisées par les étudiants, les professeurs et le personnel pour effectuer des tâches informatiques. Ils peuvent être équipés de différents composants tels que processeurs, mémoire, disques durs, etc.

**- Ordinateurs portables** : Ces appareils portables permettent aux utilisateurs de travailler de manière flexible et de se déplacer facilement tout en ayant accès aux ressources informatiques nécessaires.

**- Serveurs :** Les serveurs sont des ordinateurs puissants qui fournissent des services et des ressources aux utilisateurs du réseau, tels que le stockage de données, l'hébergement de sites web, les applications réseau, etc.

**- Imprimantes et scanners** : Ces périphériques sont utilisés pour la gestion des documents, l'impression de matériel pédagogique, la numérisation de documents, etc.

**- Routeurs et commutateurs réseau** : Ils permettent de connecter et de gérer les réseaux informatiques au sein de l'université, en acheminant les données entre les différents appareils et en assurant une connectivité fiable.

**- Disques de stockage** : Ils sont utilisés pour stocker des données telles que des fichiers, des documents, des sauvegardes, des images système, etc.

**2. Infrastructures réseau** :

**- Réseau local (LAN) :** Il s'agit du réseau interne de l'université qui relie les différents ordinateurs, serveurs et périphériques au sein d'un même emplacement physique.

**- Réseau étendu (WAN)** : Il représente les connexions à distance qui relient plusieurs sites de l'université, permettant ainsi la communication et le partage de ressources entre eux.

**- Points d'accès Wi-Fi :** Ils fournissent une connectivité sans fil aux utilisateurs, leur permettant d'accéder au réseau et aux services à partir de différents emplacements sur le campus.

**- Pare-feu et dispositifs de sécurité réseau** : Ces dispositifs sont utilisés pour protéger le réseau contre les menaces extérieures en contrôlant le trafic entrant et sortant et en appliquant des politiques de sécurité.

**3. Systèmes d'exploitation et logiciels :**

**- Systèmes d'exploitation :** Ce sont les logiciels de base installés sur les ordinateurs, tels que Windows, macOS, Linux, qui fournissent une interface utilisateur et permettent l'exécution d'autres programmes.

**- Suites bureautiques :** Ces logiciels, tels que Microsoft Office et LibreOffice, comprennent des outils tels que des traitements de texte, des tableurs, des logiciels de présentation, etc., utilisés pour la création et la gestion de documents.

**- Logiciels de programmation et de développement :** Ils sont utilisés par les étudiants et les enseignants pour écrire, tester et déployer des programmes informatiques, tels que des langages de programmation, des environnements de développement intégrés (IDE), des outils de débogage, etc.

**- Logiciels de conception graphique et de modélisation :** Ces outils permettent de créer des graphiques, des images, des modèles 2D/3D, des animations, etc., utilisés dans les domaines de la conception graphique, de l'animation et de la modélisation.

**4. Applications et services :**

**- Système de gestion de l'apprentissage (LMS) :** Il s'agit d'une plateforme logicielle utilisée pour la gestion des cours, la diffusion de contenu pédagogique, les évaluations en ligne, la communication entre les enseignants et les étudiants, etc.

**- Messagerie électronique et services de collaboration :** Ce sont des outils de communication utilisés pour l'échange d'e-mails, la planification de réunions, le partage de documents, la collaboration en ligne, etc.

**- Bases de données** : Elles sont utilisées pour stocker et gérer les données de l'université, telles que les informations des étudiants, les résultats d'examens, les données de recherche, etc.

**- Logiciels de simulation et d'analyse** : Ces outils sont utilisés dans les domaines de l'informatique et de l'IA pour simuler des scénarios, effectuer des analyses de données, réaliser des prédictions et des modélisations, etc.

**- Outils de sécurité de l'information** : Ils comprennent des logiciels antivirus, des pares-feux, des outils de détection d'intrusion, des systèmes de gestion des identités et des accès, etc., qui sont utilisés pour protéger les systèmes et les données contre les menaces de sécurité.

**5. Données et informations** :

**- Bases de données étudiantes** : Elles contiennent des informations sur les étudiants inscrits, y compris leurs données personnelles, leurs programmes d'études, leurs notes, etc.

**- Résultats d'examens et d'évaluations** : Ces données sont utilisées pour enregistrer et gérer les résultats des examens, les évaluations des étudiants, les notes attribuées, etc.

**- Documents de recherche et de projets** : Il s'agit de documents scientifiques, de rapports de recherche, de projets étudiants, etc., qui sont stockés et gérés pour la consultation et la collaboration.

**- Données personnelles des étudiants et du personnel** : Il s'agit d'informations confidentielles telles que les noms, les adresses, les numéros de sécurité sociale, les adresses e-mail, etc., qui doivent être protégées conformément aux réglementations sur la confidentialité des données.

**6. Locaux et installations :**

- Salles de cours et laboratoires informatiques : Ce sont les espaces physiques où les cours d'informatique sont dispensés, équipés d'ordinateurs, de projecteurs, de tableaux blancs interactifs, etc.

- Serveurs de stockage et de sauvegarde : Ils sont utilisés pour stocker les données de l'université de manière sécurisée et effectuer des sauvegardes régulières afin de prévenir la perte de données.

- Salles de serveurs et centres de données : Ce sont des espaces dédiés pour héberger les serveurs, les équipements réseau et les infrastructures informatiques, offrant généralement des conditions de refroidissement et d'alimentation électrique optimales.

- Systèmes de climatisation et d'alimentation électrique : Ils sont essentiels pour maintenir les conditions de fonctionnement optimales des équipements informatiques, notamment en régulant la température et en fournissant une alimentation électrique ininterrompue.

- Systèmes de vidéosurveillance et de sécurité : Ils sont utilisés pour assurer la sécurité des locaux, surveiller les zones sensibles, contrôler l'accès physique, etc.

**7. Actifs humains :**

**- Étudiants, professeurs et personnel administratif** : Ce sont les membres de la communauté universitaire qui interagissent avec les actifs informatiques et utilisent les ressources pour l'apprentissage, l'enseignement et l'administration.

**- Administrateurs système et techniciens informatiques** : Ils sont responsables de la gestion, de la maintenance et du support technique des actifs informatiques, tels que l'installation de logiciels, la résolution de problèmes matériels, la configuration réseau, etc.

**- Responsables de la sécurité de l'information** : Ils veillent à ce que les actifs informatiques et les données sensibles soient protégés contre les menaces de sécurité, en mettant en œuvre des politiques, des contrôles et des mesures de prévention appropriés.

**- Utilisateurs autorisés des systèmes et des applications** : Ce sont les individus autorisés à accéder aux actifs informatiques et à utiliser les systèmes, les applications et les données conformément aux politiques et aux procédures établies.

* CAS PRATIQUE DE LA METHODE MEHARI SUR KEYCE
* ENUMERATTION DES ACTIFS EN GENERALE

**1. Équipements matériels :**

**- Ordinateurs de bureau : Ce sont des machines utilisées par les étudiants, les professeurs et le Ypersonnel pour effectuer des tâches informatiques. Ils peuvent être équipés de différents composants tels que processeurs, mémoire, disques durs, etc.**

**- Ordinateurs portables : Ces appareils portables permettent aux utilisateurs de travailler de manière flexible et de se déplacer facilement tout en ayant accès aux ressources informatiques nécessaires.**

**- Serveurs : Les serveurs sont des ordinateurs puissants qui fournissent des services et des ressources aux utilisateurs du réseau, tels que le stockage de données, l'hébergement de sites web, les applications réseau, etc.**

**- Imprimantes et scanners : Ces périphériques sont utilisés pour la gestion des documents, l'impression de matériel pédagogique, la numérisation de documents, etc.**

**- Routeurs et commutateurs réseau : Ils permettent de connecter et de gérer les réseaux informatiques au sein de l'université, en acheminant les données entre les différents appareils et en assurant une connectivité fiable.**

**- Disques de stockage : Ils sont utilisés pour stocker des données telles que des fichiers, des documents, des sauvegardes, des images système, etc.**

**2. Infrastructures réseau :**

**- Réseau local (LAN) : Il s'agit du réseau interne de l'université qui relie les différents ordinateurs, serveurs et périphériques au sein d'un même emplacement physique.**

**- Réseau étendu (WAN) : Il représente les connexions à distance qui relient plusieurs sites de l'université, permettant ainsi la communication et le partage de ressources entre eux.**

**- Points d'accès Wi-Fi : Ils fournissent une connectivité sans fil aux utilisateurs, leur permettant d'accéder au réseau et aux services à partir de différents emplacements sur le campus.**

**- Pare-feu et dispositifs de sécurité réseau : Ces dispositifs sont utilisés pour protéger le réseau contre les menaces extérieures en contrôlant le trafic entrant et sortant et en appliquant des politiques de sécurité.**

**3. Systèmes d'exploitation et logiciels :**

**- Systèmes d'exploitation :** Ce sont les logiciels de base installés sur les ordinateurs, tels que Windows, macOS, Linux, qui fournissent une interface utilisateur et permettent l'exécution d'autres programmes.

**- Suites bureautiques :** Ces logiciels, tels que Microsoft Office et LibreOffice, comprennent des outils tels que des traitements de texte, des tableurs, des logiciels de présentation, etc., utilisés pour la création et la gestion de documents.

**- Logiciels de programmation et de développement** : Ils sont utilisés par les étudiants et les enseignants pour écrire, tester et déployer des programmes informatiques, tels que des langages de programmation, des environnements de développement intégrés (IDE), des outils de débogage, etc.

**- Logiciels de conception graphique et de modélisation : Ces outils permettent de créer des graphiques, des images, des modèles 2D/3D, des animations, etc., utilisés dans les domaines de la conception graphique, de l'animation et de la modélisation.**

**4. Applications et services :**

**- Système de gestion de l'apprentissage (LMS) : Il s'agit d'une plateforme logicielle utilisée pour la gestion des cours, la diffusion de contenu pédagogique, les évaluations en ligne, la communication entre les enseignants et les étudiants, etc.**

**- Messagerie électronique et services de collaboration :** Ce sont des outils de communication utilisés pour l'échange d'e-mails, la planification de réunions, le partage de documents, la collaboration en ligne, etc.

**- Bases de données :** Elles sont utilisées pour stocker et gérer les données de l'université, telles que les informations des étudiants, les résultats d'examens, les données de recherche, etc.

**- Logiciels de simulation et d'analyse :** Ces outils sont utilisés dans les domaines de l'informatique et de l'IA pour simuler des scénarios, effectuer des analyses de données, réaliser des prédictions et des modélisations, etc.

**- Outils de sécurité de l'information :** Ils comprennent des logiciels antivirus, des pares-feux, des outils de détection d'intrusion, des systèmes de gestion des identités et des accès, etc., qui sont utilisés pour protéger les systèmes et les données contre les menaces de sécurité.

**5. Données et informations :**

**- Bases de données étudiantes** : Elles contiennent des informations sur les étudiants inscrits, y compris leurs données personnelles, leurs programmes d'études, leurs notes, etc.

**- Résultats d'examens et d'évaluations :** Ces données sont utilisées pour enregistrer et gérer les résultats des examens, les évaluations des étudiants, les notes attribuées, etc.

**- Documents de recherche et de projets** : Il s'agit de documents scientifiques, de rapports de recherche, de projets étudiants, etc., qui sont stockés et gérés pour la consultation et la collaboration.

**- Données personnelles des étudiants et du personnel :** Il s'agit d'informations confidentielles telles que les noms, les adresses, les numéros de sécurité sociale, les adresses e-mail, etc., qui doivent être protégées conformément aux réglementations sur la confidentialité des données.

**6. Locaux et installations :**

**- Salles de cours et laboratoires informatiques :** Ce sont les espaces physiques où les cours d'informatique sont dispensés, équipés d'ordinateurs, de projecteurs, de tableaux blancs interactifs, etc.

**- Serveurs de stockage et de sauvegarde** : Ils sont utilisés pour stocker les données de l'université de manière sécurisée et effectuer des sauvegardes régulières afin de prévenir la perte de données.

**- Salles de serveurs et centres de données** : Ce sont des espaces dédiés pour héberger les serveurs, les équipements réseau et les infrastructures informatiques, offrant généralement des conditions de refroidissement et d'alimentation électrique optimales.

**- Systèmes de climatisation et d'alimentation électrique :** Ils sont essentiels pour maintenir les conditions de fonctionnement optimales des équipements informatiques, notamment en régulant la température et en fournissant une alimentation électrique ininterrompue.

**- Systèmes de vidéosurveillance et de sécurité :** Ils sont utilisés pour assurer la sécurité des locaux, surveiller les zones sensibles, contrôler l'accès physique, etc.

**7. Actifs humains :**

**- Étudiants, professeurs et personnel administratif :** Ce sont les membres de la communauté universitaire qui interagissent avec les actifs informatiques et utilisent les ressources pour l'apprentissage, l'enseignement et l'administration.

**- Administrateurs système et techniciens informatiques :** Ils sont responsables de la gestion, de la maintenance et du support technique des actifs informatiques, tels que l'installation de logiciels, la résolution de problèmes matériels, la configuration réseau, etc.

**- Responsables de la sécurité de l'information :** Ils veillent à ce que les actifs informatiques et les données sensibles soient protégés contre les menaces de sécurité, en mettant en œuvre des politiques, des contrôles et des mesures de prévention appropriés.

**- Utilisateurs autorisés des systèmes et des applications :** Ce sont les individus autorisés à accéder aux actifs informatiques et à utiliser les systèmes, les applications et les données conformément aux politiques et aux procédures établies.

* LES VULNERABILITES RENCONTRES EN GENERALE A KEYCE

Dans le cadre de la méthode MEHARI (Méthode Harmonisée d'Analyse de Risques), a KEYCE ,plusieurs vulnérabilités peuvent exister . Parmi les vulnérabilités on peut avoir :

* **Vulnérabilités du réseau** : Cela peut inclure des configurations réseau incorrectes, des pare-feu mal configurés, des vulnérabilités de protocoles réseau, des failles de sécurité dans les équipements réseau, etc. Ces vulnérabilités peuvent permettre des attaques telles que l'interception de données, le déni de service ou l'injection de code malveillant.
* **Vulnérabilités des systèmes d'exploitation** : Les ordinateurs et serveurs utilisés dans une école d'informatique peuvent présenter des vulnérabilités connues, notamment des failles de sécurité dans le système d'exploitation ou les applications installées. Des correctifs et mises à jour régulières doivent être appliqués pour réduire ces vulnérabilités.
* **Vulnérabilités des applications** : Les applications logicielles utilisées dans une école d'informatique peuvent présenter des vulnérabilités de sécurité, telles que des failles de programmation, des erreurs de configuration ou des problèmes d'autorisation. Ces vulnérabilités peuvent permettre des attaques telles que l'injection de code, le vol d'informations sensibles ou la compromission du système.
* **Vulnérabilités liées aux mots de passe** : Les mots de passe faibles, partagés ou non modifiés régulièrement peuvent constituer une vulnérabilité dans une école d'informatique. Cela peut faciliter l'accès non autorisé aux systèmes ou aux données confidentielles.
* **Vulnérabilités physiques** : Les locaux de l'école d'informatique peuvent présenter des vulnérabilités physiques, telles que l'accès non autorisé aux équipements, l'absence de contrôles d'accès appropriés ou la négligence dans la gestion des supports informatiques.
* **Vulnérabilités liées à la sensibilisation à la sécurité :** Une faible sensibilisation à la sécurité informatique parmi le personnel et les étudiants peut conduire à des pratiques négligentes, comme le partage d'informations confidentielles, le téléchargement de logiciels malveillants ou la négligence des procédures de sécurité.
* **Mauvaise gestion des identifiants et des mots de passe :** Les élèves, les professeurs ou les invités peuvent utiliser des mots de passe faibles, les partager avec d'autres personnes ou les stocker de manière non sécurisée, ce qui peut compromettre la sécurité des comptes et des systèmes.
* **Utilisation de logiciels non autorisés ou piratés :** Les élèves, les professeurs ou les invités peuvent installer des logiciels non autorisés ou piratés sur les ordinateurs de l'école, ce qui peut introduire des vulnérabilités et des logiciels malveillants dans le réseau.
* **Pratiques de développement non sécurisées :** Les élèves qui développent des applications peuvent introduire des vulnérabilités de sécurité, telles que des failles d'injection de code ou des erreurs de validation des entrées utilisateur.
* **Partage non autorisé de données confidentielles :** Les élèves, les professeurs ou les invités peuvent partager des informations confidentielles, telles que des mots de passe ou des données sensibles, avec des personnes non autorisées, ce qui compromet la confidentialité des données.
* **Négligence des procédures de sécurité :** Les élèves, les professeurs ou les invités peuvent négliger les procédures de sécurité, comme ne pas verrouiller leurs ordinateurs lorsqu'ils s'absentent, ne pas mettre à jour régulièrement les logiciels ou ne pas sauvegarder leurs données.
* **Utilisation de périphériques de stockage non sécurisés :** L'utilisation de clés USB, de disques durs externes ou d'autres périphériques de stockage sans prendre les mesures appropriées peut introduire des logiciels malveillants ou permettre la fuite de données sensibles.

Il est important de sensibiliser les élèves, les professeurs et les invités à la sécurité de l'information et de mettre en place des politiques et des procédures claires pour prévenir ces vulnérabilités. Cela peut inclure des formations sur la sécurité informatique, des politiques d'utilisation acceptables, des contrôles d'accès appropriés et des processus de gestion des incidents de sécurité. La sensibilisation et l'éducation sont essentielles pour encourager des pratiques sécurisées et minimiser les vulnérabilités créées par les acteurs internes de l'école d'informatique.

* Quelques solutions envisageables pour réduire les vulnérabilité augmenter la sécurité

Une fois que les vulnérabilités spécifiques de KEYCE ont été identifiées, nombreuses mesures de sécurité sont envisagées envisageables pour rendre cette dernière moins vulnérable a savoir :

* Mise en place de pare-feu et de filtrage réseau : Configurer des pare-feu et des systèmes de filtrage réseau appropriés pour contrôler le trafic entrant et sortant, et bloquer les connexions indésirables ou malveillantes.
* **Gestion des correctifs et des mises à jour** : Mettre en place un processus de gestion des correctifs et des mises à jour pour garantir que les systèmes d'exploitation, les applications et les équipements réseau sont régulièrement mis à jour avec les derniers correctifs de sécurité.
* **Sécurisation des mots de passe** : Mettre en œuvre des politiques de sécurité des mots de passe, qui encouragent l'utilisation de mots de passe forts, leur rotation régulière et l'utilisation de méthodes d'authentification à plusieurs facteurs lorsque cela est possible.
* **Sécurisation des applications** : Adopter des pratiques de développement sécurisé pour les applications utilisées dans l'école, en mettant l'accent sur la validation des entrées utilisateur, la prévention des injections de code et l'application de contrôles d'accès appropriés.
* **Sensibilisation à la sécurité :** Organiser des sessions de sensibilisation à la sécurité informatique pour le personnel et les étudiants afin de les informer des meilleures pratiques de sécurité, des risques associés et des mesures de protection à adopter.
* Contrôles d'accès physique : Mettre en place des mesures de contrôle d'accès physique, telles que des cartes d'identité, des systèmes de verrouillage sécurisés et des caméras de surveillance, pour prévenir l'accès non autorisé aux locaux et aux équipements.
* **Sauvegardes régulières des données :** Effectuer des sauvegardes régulières des données critiques de l'école d'informatique et vérifier la validité des sauvegardes pour assurer la disponibilité des données en cas d'incident ou de sinistre.
* **Surveillance du réseau :** Mettre en place des outils de surveillance du réseau pour détecter les activités suspectes, les tentatives d'intrusion ou les comportements anormaux, afin de pouvoir réagir rapidement en cas de problème.

Ces mesures de sécurité ne sont qu'un aperçu des actions possibles pour atténuer les vulnérabilités exitente a KEYCE.

Conclusion

En conclusion, la méthode MEHARI (Méthode Harmonisée d'Analyse de Risques) est une approche solide et largement adoptée pour évaluer les risques de sécurité de l'information dans les organisations. Elle offre une méthodologie structurée et complète qui permet aux professionnels de la sécurité de comprendre les menaces, d'identifier les vulnérabilités et d'estimer les risques associés.Grâce à la méthode MEHARI, les organisations peuvent prendre des décisions éclairées en matière de sécurité de l'information. Elle leur permet d'identifier les actifs critiques à protéger, de comprendre les menaces potentielles qui pourraient les affecter, et d'évaluer les vulnérabilités dans leurs systèmes et processus. En hiérarchisant les risques, elles peuvent se concentrer sur les mesures