RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPERIEURE
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DE BLIDA 1 – SAAD DAHLAB

FACULTE DES SCIENCES

Département d'Informatique

Mémoire présenté par :

Mlles. DAHAK Lynda et SBA Ouarda

Pour l'obtention du diplôme de Master

Domaine : Mathématique et Informatique

Filière : Informatique

Spécialité : Sécurité des Systèmes d'Information

Sujet :

Conception et implémentation d'un monitoring dans le cadre de la mise en place d'un plan de reprise d'activité au niveau de la CNAS

Soutenu le : 14/07/2021, devant le jury composé de :

M.FERFERA Sofiane	Université de Blida 1	Président
Mme. LAHIANI Nesrine	Université de Blida 1	Examinatrice
Mme. BOUSTIA Narhimene	Université de Blida 1	Promotrice
M.KOUADRIA Nadir	La CNAS	Encadreur

Organisme d'accueil :

Caisse Nationale des Assurances Sociales des Travailleurs Salariés (CNAS)

Année universitaire : 2020/2021

Résumé

La sécurité informatique est devenue une réelle préoccupation des dirigeants et responsables IT d'entreprise car ces dernières années les menaces se sont multipliées.

Dans notre projet, on a fait d'abord une analyse profonde des risques qui menace le système d'informations de la « CNAS » basé sur la méthode MEHARI pour pouvoir mettre en place les solutions qui permettent de se débarrasser ou de diminuer le risque qui peut provoquer une perte des données sensibles.

Après l'étape de l'analyse, on a mis en place un « Plan de reprise d'activité » qui permet à l'organisation de s'assurer qu'en cas de sinistre, d'incendie ou accident, le système d'information de l'entreprise puisse redémarrer rapidement ses activités à l'aide de différentes stratégies de reprise, tout en limitant les pertes de données.

Après toute cette étude nous avons pu proposer une application web « Monitoring » dont le but est de surveiller, rapporter et alerter les fonctionnements normaux et anormaux du système de l'organisation, chaque évènement exécuté par cette application produit un fichier log qui liste toutes les actions faites par un utilisateur d'une manière chronologique. Ils sont utiles pour comprendre la source de l'erreur lorsqu'elle se produit.

Mots clés : Plan de reprise d'activités, Gestion de risques, MEHARI, Monitoring, Log.

Abstract

The computer security has become a real concern of the leaders and IT managers of company because these last years the threats have multiplied.

In our project we first made a deep analysis of risk that threatens the information system of the "CNAS" based on the MEHARI method to be able to put our solutions that allows to getrid of or reduce the risk that can cause a loss of sensitive data.

After the stage of the analysis it was the creation of “Disaster Recovery Plan” which allows the organization to make sure that in the event of disaster, fire or accident, the information system of the company can restart its activities quickly using various strategies of resumption,while limiting the losses of data.

After all this study we were able to propose a web application "Monitoring" which consists ofmonitoring, reporting and alerting the normal and abnormal functioning of the system of the organization, each event executed by this application produces a log file listing all actions made by a user in a chronological way. They are useful to understand the source of the error when it occurs.

Keywords: Disaster recovery plan, Risk management, MEHARI, Monitoring, Log.

ملخص

أصبح أمن تكنولوجيا المعلومات مصدر قلق حقيقي للمدراء والمسؤولين التنفيذيين لتكنولوجيا المعلومات في المؤسسات حيث تضاعفت التهديدات في السنوات الأخيرة.

في مشروعنا،اجرينا اولا تحليلا عميقا عن المخاطر التي تهدد نظام المعلومات الخاص بالمؤسسة استنادا إلى طريقة مهاري حتى نتمكن من حلولنا التي تجعل من الممكن التخلص أو التقليل من المخاطر التي قد تؤدي إلى فقدان البيانات الحساسة.

بعد مرحلة التحليل،تم تنفيذ "خطة استعادة الأعمال"التي تسمح للمؤسسة بضمان أنه في حالة وقوع كارثة أو حريق أو حادث،يمكن لنظام معلومات الشركة إعادة تشغيل أنشطته بسرعة باستخدام استراتيجيات استرداد مختلفة،مع تقييد فقدان البيانات.

بعد كل هذه الدراسة،تمكنا من تقديم تطبيق ويب "للمراقبة"والذي يتكون من مراقبة وإبلاغ وتنبيه العمليات العادية والغير العادية لنظام المؤسسة،ينتج عن كل حدث يتم تنفيذه بواسطة هذا التطبيق ملف تسجيل يسرد جميع الإجراءات التي قام بها المستخدم بطريقة زمنية وهي مفيدة لفهم مصدر الخطأ عند حدوثه.

الكلمات المفتاحية : خطة التعافي من الكوارث،إدارة المخاطر،مهاري، المراقبة،السجل.

Dédicaces

Ce travail est dédié

A mes chers parents ma source de volonté, leur prière, encouragement,

Sacrifices, aides, et soutenir …m'ont vraiment aidé pour que je puisse

Continuer mon parcours, que Dieu le tout Puissant vous préserve, vous accord

la santé et le plus haut de paradis Incha'Allah.

A Mes sœurs et Mes frères

A Ma binôme Lynda qui m'a soutenu et encouragé toute au long de ce travail.

A mes chers amis Islem, Hind, Amira et Imane

A tous ceux qui m'ont aidé et encouragé

A tous mes collègues

Ouarda

Dédicaces

A mes chers parents.

Que nulle dédicace ne peut exprimer mes sincères sentiments.

Pour leur grand sacrifice, leur patience, leur tendresse et leur soutien.

A mes chers frères Younes, Karim et Mustapha.

Pour leur amour et leur encouragement tout au long de mon parcours universitaire.

A mes chères amies Lamiss, Manel, Abir et Hanane.

Qui m'ont toujours soutenu, et à qui je souhaite plus de succès.

A mon cher binôme Ouarda.

Pour son encouragement et sa sympathie

Je dédie ce travail à tous ceux qui ont permis la réalisation de ce projet.

Lynda

Remerciement

Nous remercions en premier lieu le bon Dieu le tout puissant qui nous à donner le courage, la volonté et la patience pour accomplir ce travail.

Tout d'abord nous adressons spécialement à remercier **M.KOUADRIA Nadir** notre encadrant pour tous ses conseils et le temps précieux qu'il a bien voulu nous consacrer et sans qui ce travail n'aurait jamais vu le jour.

Nous tenons aussi à remercier notre chef d’option et promotrice Mme **BOUSTIA Narhimene** pour tous ses conseils et directives tout au long de notre parcours.

Nous remercions toute l’équipe CNAS pour leur hospitalité et leur aide.

On remercie aussi tous ceux qui ont contribué de prés ou de loin pour accomplir notre travail de fin d'étude.

Table des matières

Liste des figures

Liste des tableaux

Liste des acronymes

- **CNAS :** Caisse Nationale des Assurés Sociaux.
- **DMSI :** Direction de la Modernisation et des Systèmes d'Information.
- **PSI :** Plan de Secours Informatique.
- **PRA :** Plan de Reprise d'Activité.
- **PCA :** Plan de Continuité d'Activité.
- **SI :** Système d'Information.
- **RTO :**Recovery Time Objective.
- **RPO :**Recovery Point Objective.
- **EBIOS :** Expression des Besoins et Identification des Objectifs de Sécurité.
- **MEHARI :** Méthode Harmonisée d'Analyse des Risques.
- **CLUSIF :** Club de la Sécurité de l'Information Français.
- **ANSSI :** Agence Nationale de la Sécurité des Systèmes d'Information.
- **WAF :** Web Application Firewall.
- **IPS :** Système de prévention d'intrusion.
- **IDS :** Système de détection d'intrusion.
- **VPN :** Réseau privé virtuel.
- **UML :** Unified Modeling Language.
- **ICMP :** Internet Control Message Protocol.
- **HTTP :** Hypertext Transfer Protocol.
- **DNS :** Domain Name System.
- **CNAME :** Canonical NAME.
- **CRUD:** Create Read Update Delete.

Glossaire

Terme	Définition
Intrusion	Accès non autorisé à un système informatique ou à un réseau, obtenu en contournant ou en désamorçant les dispositifs de sécurité en place.
Fournisseur de connexion	Entreprise ou personne dont l'activité est d'offrir un accès à des services de communication au public en ligne, autrement dit à l'internet
Authentification	Procédure qui permet à un système informatique de vérifier l'identité d'une personne ou un ordinateur.
Risque	Le risque est la prise en compte par une personne de la possibilité de la réalisation d'un évènement contraire à ses attentes ou à son intérêt.
Risque informatique	Le risque informatique correspond au risque de perte résultant d'une organisation inadéquate, d'un défaut de fonctionnement, ou d'une insuffisante sécurité du système d'information, entendu comme l'ensemble des équipements systèmes et réseaux et des moyens humains destinés au traitement de l'information de l'institution
Attaque	n'importe quelle action qui compromet la sécurité des informations.
Cyberattaque	Une cyberattaque ou attaque informatique est une action volontaire et malveillante menée au moyen d'un réseau informatique visant à causer un dommage aux informations et aux personnes qui les traitent
Menace	Description de l'ensemble des éléments conduisant à l'occurrence du risque incluant l'événement déclencheur et son caractère volontaire ou accidentel, l'acteur déclenchant cet événement et les circonstances dans lesquelles survient cet événement.
vulnérabilité	Faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser. Remarques : Une vulnérabilité peut être utilisée par un code d'exploitation et conduire à une intrusion dans le système
Sinistre	Événement grave d'origine naturelle ou humaine, accidentelle ou intentionnelle, occasionnant des pertes et des dommages importants aux systèmes informatiques d'une organisation ou d'un individu.
Actif	Tout élément du système d'information, qu'il s'agisse de l'information proprement dite, quelle que soit sa forme, ou de tout ce qui peut être nécessaire pour la communiquer, la traiter ou la stocker.

actif primaire	les fonctions essentielles de l'unité ainsi que les informations nécessaires à l'accomplissement de la mission.
actif secondaire	représentent l'ensemble des matériels, logiciels, les locaux, les personnels qui supportent et manipulent les informations à sécuriser.
Incident	Manifestation concrète de l'occurrence du risque, sous forme d'une atteinte à la disponibilité, à l'intégrité ou à la confidentialité de données ou de services.
Impact	Conséquence, pour l'organisme concerné, de l'occurrence du risque considéré.
Probabilité	Probabilité de l'occurrence du risque considéré, dans le contexte l'organisme concerné
Scénario de risque	Description de l'ensemble des caractéristiques d'un risque, incluant l'actif concerné, la vulnérabilité intrinsèque de cet actif mise en cause et la menace conduisant à l'occurrence du risque.
Les contres mesures	Mesure destinée à s'opposer à une action, à un événement ou à les prévenir.
Antivirus	Logiciel permettant d'identifier, neutraliser et éliminer toute intrusion de logiciels malveillants tel que les virus informatiques.
Contrôle d'accès	Moyen de surveillance et de protection consistant à limiter aux seules personnes autorisées les accès aux comptes de l'entité, aux documents comptables, aux systèmes, aux données en mémoire, aux ressources, aux actifs, etc.
Service de sécurité	Description d'une fonction de sécurité répondant à un besoin.
Faille	Vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.
Malveillance	Tout programme développé dans le but de nuire à ou au moyen d'un système informatique ou d'un réseau
Pare-feu (firewall)	Un pare-feu, est un outil permettant de protéger un ordinateur connecté à un réseau ou à l'internet. Il protège d'attaques externes (filtrage entrant) et souvent de connexions illégitimes à destination de l'extérieur (filtrage sortant) initialisées par des programmes ou des personnes

Introduction Générale

1 Contexte de travail

De nos jours, la sécurité informatique est devenue un problème majeur qui préoccupe les organisations et les entreprises à cause des incidents de sécurité de leurs systèmes d'information. Ces incidents de sécurité qui représentent tout événement ne faisant pas partie des opérations standards et pouvant provoquer une interruption de service ou altérer sa qualité, sont de plus en plus nombreux et multiformes. De plus, aucune organisation ne peut affirmer maîtriser à 100% son système d'information et encore moins sa sécurité.

2 Problématique

Pour toute entreprise, le système d'information est considéré comme un élément central du fonctionnement d'une organisation. Il permet de créer, collecter, stocker et traiter les données.

La perte de données peut mettre en danger l'ensemble de l'entreprise, pour conserver ses données le plus longtemps possible et poursuivre les activités critiques qui permettent à l'organisation de fonctionner correctement, la CNAS fait un basculement vers un site secondaire en cas d'interruption. Cela a comme risques :

- Possibilité que le site secondaire tombe lui-même en panne ou qu'il induise une panne dans un autre sous-système.
- Plus grande complexité de gestion.
- La copie des données augmentera le trafic réseau.
- La gestion du processus de déplacement des systèmes et des ressources nécessitent du temps et des frais très généreux.

Pour répondre à cette problématique, on a opté pour la réalisation d'un plan de reprise d'activité qui assure la reprise des activités le plus tôt possible pour éviter des pertes importantes en termes d'opportunités commerciales et de chiffre d'affaires, qui peuvent parfois être fatales pour l'entreprise. Aussi le développement d'une solution qui permettre de réaliser la surveillance (Monitoring).

3 Objectif

Ce travail compte répondre à trois objectifs principaux qui sont:

- La mise en place d'un plan de reprise d'activité
- La conception d'une solution qui offre un service de surveillance.
- Réalisation d'une application réalisant la surveillance et le contrôle distant.

4 Organisation du mémoire

Dans le premier chapitre nous allons définit ce qu'est un plan de reprise d'activité et d'expliquer son importance.

Dans le deuxième chapitre, Nous commençons ce chapitre par la présentation de l'organisme d'accueil ensuite nous allons détailler le plan de reprise d'activité afin de prévenir les catastrophes et planifier la reprise après sinistre. En vue d'éliminer les risques, nous adopterons la méthode de gestion des risques MEHARI.

Le troisième chapitre est dédié à la modélisation du système de Monitoring.

La mise en œuvre de ce système est décrite dans le quatrième chapitre.

Ce mémoire se terminera par une conclusion générale, dans laquelle nous repositionnerons par rapport aux objectifs initiaux de la recherche. Enfin, nous discuterons les perspectives de travail.

Chapitre I : Etat de l'art

Introduction

Les catastrophes sur l'infrastructure du système d'information se présentent non seulement sur les événements catastrophiques naturel, mais également d'incidents tels que panne matérielle, cyber attaque, et erreur humaine. Les entreprises et organisation peuvent remettre en route leur système d'information lorsque un tel risque survenant en créant des plans de reprise d'activité qui détaillent les actions à entreprendre et les processus à suivre en cas de sinistre afin de reprendre les fonctions essentielles rapidement et sans perte des activités.

1 Plan de reprise d'activité

La reprise après sinistre traite de l'impact immédiat d'un événement et implique les processus, les politiques et les procédures nécessaires à la reprise des opérations et à la poursuite des fonctions essentielles d'une organisation après un sinistre. [1]

Dans l'espace informatique, la reprise après sinistre se concentre sur les systèmes informatiques qui contribuent à soutenir les fonctions essentielles de l'entreprise. Le terme continuité des activités est souvent associé à la reprise après sinistre, mais les deux termes ne sont pas totalement interchangeables. La reprise après sinistre fait partie de la continuité des activités, qui se concentre davantage sur le maintien de tous les aspects de l'entreprise en dépit du sinistre. Les systèmes informatiques étant aujourd'hui si essentiels au succès de l'entreprise, la reprise après sinistre est un pilier essentiel du processus de continuité des activités. [2]

2 Plan de continuité d'activité

Le plan de continuité des activités (PCA) est une méthodologie utilisée pour créer et valider un plan permettant de maintenir la continuité des activités avant, pendant et après des catastrophes et des événements perturbateurs.

Le PCA concerne la gestion des éléments opérationnels qui permettent à une entreprise de fonctionner normalement afin de générer des revenus. Il s'agit souvent d'un concept utilisé pour évaluer les différentes stratégies technologiques. [3]

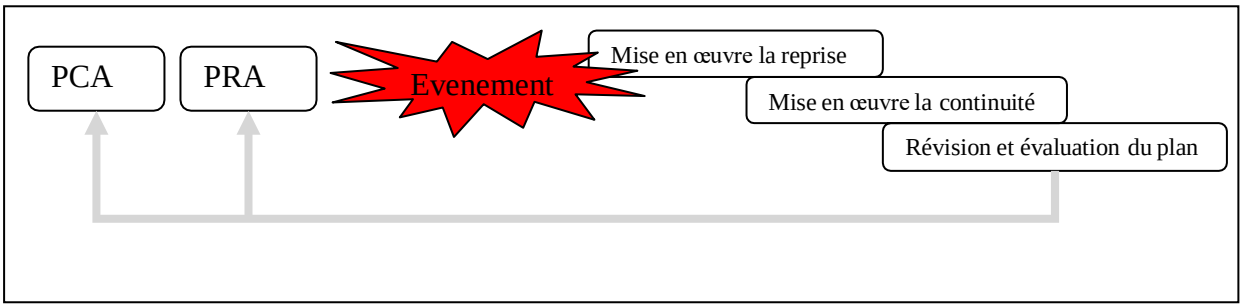

Figure 1 : Cycle de continuité des activités et de reprise après sinistre [3]

3 Comparaison entre le PRA et PCA

Le tableau ci-dessous présente une comparaison entre le PCA et le PRA.

Acronyme	Intitulé	Périmètre	Objectifs	Responsable	Principaux acteurs
PRA	Plan de Reprise d'Activité	Le SI	Reprendre l'activité du SI après une interruption. En général, la reprise s'effectue sur unsite distant. Se limite aux interruptions majeures avec des effets à long terme	Le directeur du SI ou le responsable d'exploitation	La cellule de crise Les équipes informatiques Les équipes d'intervention et lesutilisateurs
PCA	Plan de continuité d'activité	L'entreprise	Assurer la résilience de l'entreprise en : minimisant l'impact d'un sinistre majeur sur l'activité de l'entreprise assurant le fonctionnement des activités critiques pendant la crise permettant un retour maitrisé à la situation nominale.	Le responsable de PCA	Cellule de crise Direction générale DirectionSI équipes Directions métiers Equipes d'intervention définies Direction communication DRH Autoritécivile

Tableau 1: Tableau comparatif [4]

4 Le contenu d'un PRA

Chaque PRA doit être ajusté en fonction de l'entreprise et de ses caractéristiques, il n'y a pas de modèle idéal. En dernière analyse, le plus important est de tout prévoir et d'avoir une vue d'ensemble aussi complète que possible afin de mieux maîtriser l'imprévu.

De manière générale, le plan de reprise d'activité devrait inclure:

1. L'identification des activités critique qui doivent absolument se poursuivre.
2. L'identification de tous les risques.
3. Les Différentes solutions de maintenance.
4. Appliquer des procédures selon différentes situations.
5. Les ressources nécessaires à la continuité des activités (ressources humaines, matières premières, équipements, sous-traitants, etc.).
6. Les périodes de récupération à respecter. [5]

5 Les objectifs visés par le PRA

- Réduire les temps d'arrêt pour les activités en cours.
- Former et éduquer tous les employés.
- Minimisez les dommages matériels.
- Prendre des mesures pour sauvegarder les données.
- Protégez l'infrastructure informatique. [6]

6 Le périmètre de PRA

Chaque site important possède son propre plan. Afin de faciliter la lecture des données d'un site, seules les données ayant des relations importantes avec le site sinistré seront retenues.

Le périmètre doit d'abord provenir d'une analyse du l'environnement ainsi que des champs géographique et organisationnel pris en compte. Il doit fournir une liste de tous les éléments permettant de définir le champ d'action à l'intérieur et à l'extérieur de l'entreprise, notamment les paramètres de réponse :

- La durée maximale d'interruption admissible.
- Les événements pouvant de déclencher le plan de reprise.
- Le comité de crise.
- Les partenaires métier.
- Les sites de secours.
- Les sites d'archivage et de sauvegardes.
- Les autorités locales.

7 Le processus de PRA

Lors de l'élaboration d'un plan de reprise d'activité, on doit suivre ces étapes organisées :

7.1 Identification et évaluation de risque

Identifier et répertorier les incidents graves qui peuvent affecter le fonctionnement normal de l'organisation.

7.2 Evaluation les ressources et les activités critique

Si les ressources sont limitées, il faut les utiliser de manière efficace pour mettre en place un plan efficace de reprise après sinistre. Classification par ordre les activités critiques. Pour ce faire, on doit définir les données suivantes :

- **RTO :**
  Il s'agit du temps d'arrêt maximal que l'entreprise peut supporter avant que les choses ne deviennent vraiment mauvaises. Ce temps d'interruption est calculé entre le moment où la ressource informatique n'est plus en fonctionnement et où l'activité reprend normalement
- **RPO :**
  Elle correspond à la durée maximale de perte de données autorisée par l'entreprise. Par exemple, une activité limitée à une sauvegarde complète de la base de données par jour a un RPO de 24 heures. Pour certaines entreprises qui effectuent des sauvegardes plus régulières, cela peut être considérablement réduit. [5]

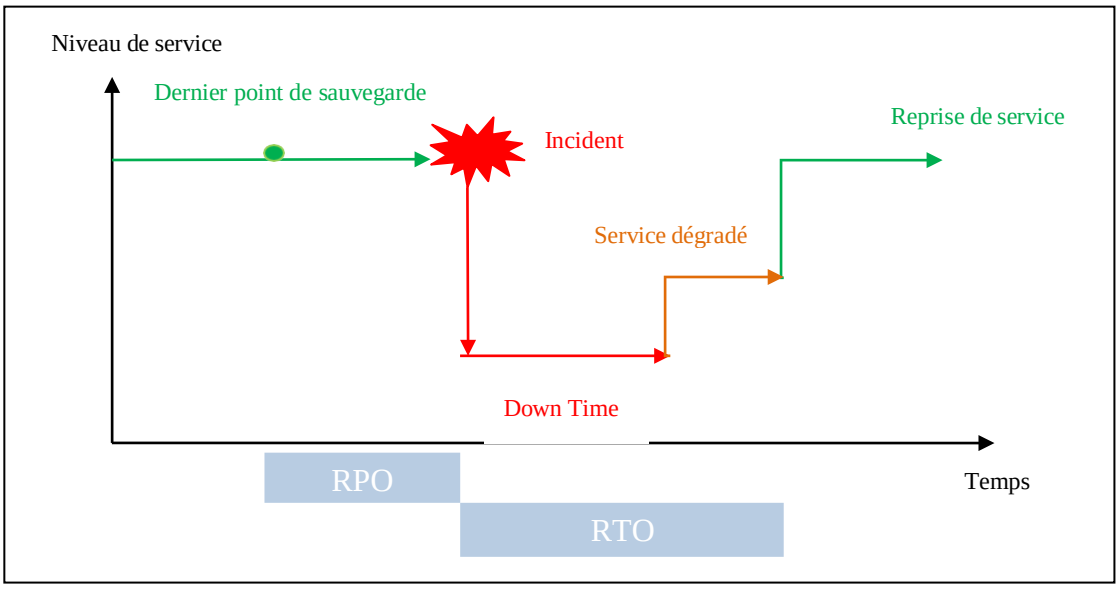

Figure 2 : Les indicateurs RTO et RPO [5]

7.3 Définition de la stratégie de reprise d'activité

Après avoir identifié et évalué les activités critiques, il est temps de définir les mesures de sécurité qui peuvent réduire la possibilité d'incidents pouvant perturber les services fournis par le SI à la ligne d'activité. Il existe deux types de mesures :

7.3.1 Les mesures préventives

- La redondance des donnés et des équipements
- La sauvegarde en ligne :

Il existe deux types de sauvegardes: [7]

a. Sauvegarde à chaud :

La sauvegarde à chaud permet de sauvegarder la base de données sans cette dernière soit arrêtée. S'appuie sur une recopié des données du site de production vers le site de secours.

b. Sauvegarde à froid :

Sauvegarde à froid lorsque la base de données soit arrêtée. S'appuie sur une recopié des données du site de production vers le site de secours.

- L'utilisation de sites de secours.

7.3.2 Les mesures curatives

- L'utilisation de site secondaire.
- La restauration ou la reprise des données.
- Le redémarrage des applications.
- Le redémarrage des machines. [5]

7.4 Classification par ordre de priorité les ressources matérielles

Après avoir déterminé les activités critiques essentielles, il faut mettre en correspondance ces activités avec les composants technologiques qui rendent ces activités possibles. Ces informations sont utiles pour identifier les composants critiques de l'environnement technologique et pour hiérarchiser chaque composant en conséquence.

7.5 Documentation du plan

Le plan de reprise après sinistre doit être documenté selon des étapesséquentielles permettant à l'organisation de revenir à l'état normal.

La documentation d'un plan de reprise peut être structurée en 4 niveaux quisont :

- Les documents de communication sur le PRA :
  Ne doit pas être négligée. Elle permettre aux responsables d'avoir une bonne vue d'ensemble des solutions prévues et de leurs conditions générales de mise en œuvre.
- Les documents de mise en œuvre du PRA :
  Ce document constitue le cœur du PRA. Il est destiné aux personnes ayant la responsabilité des différents dispositifs du plan.
- Les documents de gestion du PRA :
  C'est une documentation complémentaire destinée aux responsables du plan et des dispositifs associés.
- Les documents de contrôle du PRA. [7]

7.6 Test du plan

Afin d'en garantir l'efficacité du plan il faut effectuer des tests réguliers sur le plan de reprise après sinistre. Les tests doivent être effectués sur l'ensemble du processus du plan. Une technique de test utile consiste à élaborer un scénario de test basé sur une situation de catastrophe. Une fois les tests terminés, il faut examiner les résultats avec les membres de l'équipe afin de déterminer les améliorations possibles et mettre à jour le plan en conséquence. [1]

7.7 Mettre à jour le plan de reprise

Pour que le plan de reprise après sinistre soit efficace, il faut le tenir à jour et l'appliquer à la technologie et aux processus commerciaux actuels. Les changements apportés au plan doivent être communiqués à tout le personnel concerné par ces changements. [1]

8 Avantages d'un plan de reprise d'activité

- **L'amélioration des processus d'entreprise :** Les processus opérationnels étant soumis à une telle analyse et à un tel examen.
- **Une technologie améliorée :** Souvent, vous devez améliorer les systèmes informatiques pour soutenir les objectifs de récupération que vous développez dans le plan de reprise après sinistre.
- **Moins de perturbations :** Grâce à l'amélioration de la technologie, les systèmes informatiques ont tendance à être plus stables.
- **Des services de meilleure qualité :** Grâce à l'amélioration des processus et des technologies, vous améliorez les services.
- **Avantages concurrentiels :** Un PRA permet également à une entreprise de revendiquer une plus grande disponibilité et fiabilité des services. [8]

9 La gestion des risques

La gestion des risques est la mise en œuvre de toutes les mesures organisationnelles et techniques visant à réduire sa probabilité d'occurrence ou à réduire sa gravité.

Nous présentons par la suite trois méthodes d'appréciations des risques :

9.1 EBIOS

La méthode EBIOS (Expression des besoins et identification des objectifs de sécurité) a été créée conjointement par l'Agence Nationale de Sécurité du Système d'Information (ANSSI) et le Club EBIOS, elle permet d'apprécier et de traiter les risques. Elle fournit également tous les éléments nécessaires à la communication au sein de l'organisation et de ses partenaires et à la vérification du traitement des risques. Par conséquent, il constitue un outil complet de gestion des risques. [10]

La nouvelle méthode d'analyse de risque EBIOS RM se distingue par une approche qui réalise une synthèse entre conformité et scénarios. Elle se fonde sur un socle de sécurité solide, construit grâce à une approche par conformité. La démarche par scénarios vient solliciter ce socle face à des menaces particulièrement ciblées ou sophistiquées, qui prennent en compte l'écosystème métier et technique dans lequel l'organisation ciblée évolue. [11]

9.2 OCTAVE

OCTAVE est une méthode d'évaluation et de planification stratégique de la sécurité basée sur les risques développée en 1999 à l'université Carnegie Mellon (CMU), pour le ministère de la défense des Etats-Unis. Elle est autodirigée, ce qui signifie qu'une organisation doit gérer le processus d'évaluation et prendre les décisions relatives à la protection des informations. Une équipe interdisciplinaire, appelée équipe d'analyse, dirige l'évaluation. Elle contient les phases suivantes :

- Phase1, Établir des profils de menaces basés sur les actifs.
- Phase2, Identifier les vulnérabilités de l'infrastructure.
- Phase3, Développer une stratégie et des plans de sécurité. [12]

9.3 MEHARI

MEHARI est une méthode de gestion des risques créée par le CLUSIF, un club de sécurité informatique français. Son objectif n'est pas seulement d'identifier la situation de risque et d'évaluer son niveau, mais aussi de mettre l'accent sur les mesures visant à réduire le risque à un niveau acceptable. [13]

Dans notre travail, nous nous sommes particulièrement intéressées à cette méthode d'appréciations des risques. Notre choix s'est fait par rapport au choix de l'organisme d'accueil. A cet effet, plus de détails sur cette méthode seront élaboré par la suite.

MEHARI a été conçue et est en constant développement pour aider les RSSI dans leur tâche de gestion et de pilotage de la sécurité de l'information et des systèmes d'information. L'objectif premier de MEHARI est de fournir une méthode d'analyse et de gestion des risques et, plus particulièrement pour le domaine de la sécurité de l'information, une méthode conforme aux exigences de la norme ISO/IEC 27005, avec l'ensemble des outils et moyens requis pour sa mise en œuvre. [14]

9.3.1 Objectifs de MEHARI

- Identifier tous les risques encourus par l'entreprise.
- Quantifier le niveau de chaque risque.
- Pour chaque risque jugé inacceptable, prendre des mesures pour assurer Ce risque est réduit à un niveau acceptable.
- Mettre en place une surveillance permanente des risques et des niveaux comme outil de gestion.
- S'assurer que chaque risque est correctement géré et que la décision a été acceptée, réduite, évitée ou transférée. [15]

9.3.2 Démarche de MEHARI

La méthode MEHARI propose une démarche qui se fait en 3 étapes. Le schéma ci-dessous présente ces étapes.

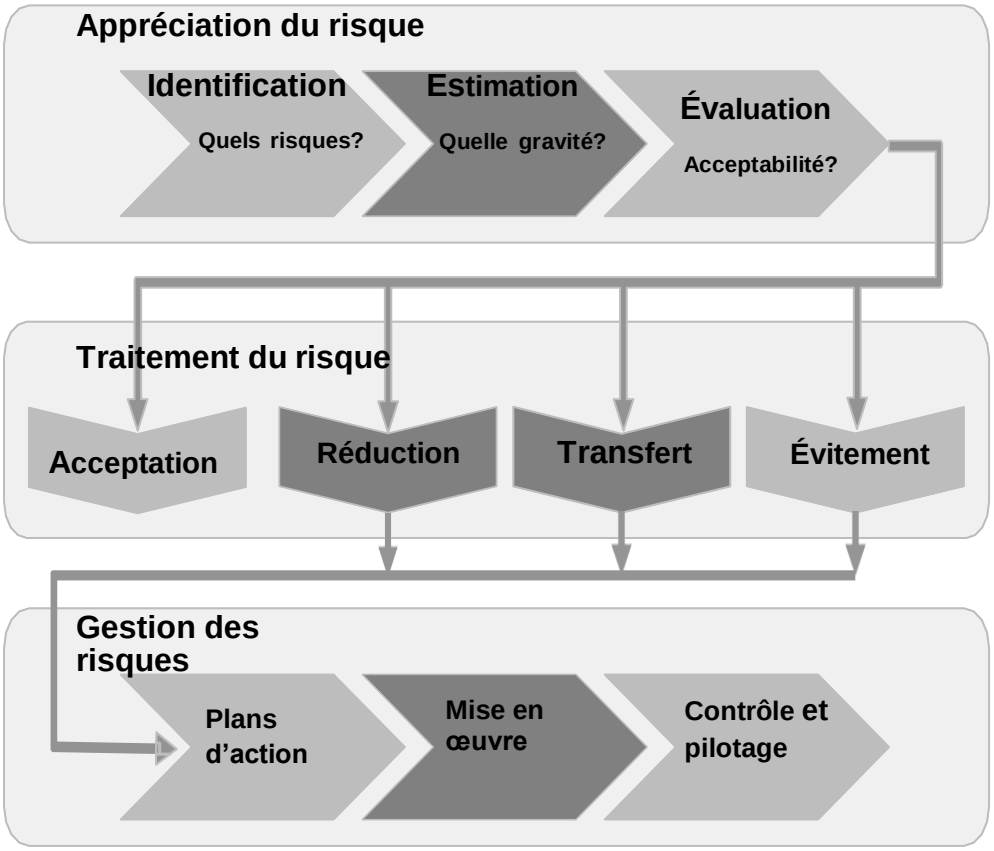

Figure 3 : Etapes pour la réalisation de MEHARI [15]

- **Appréciation du risque**: L'appréciation des risques comprend la détermination de tous les risques encourus par l'entreprise ou l'organisation avec le plus de détails possible, l'estimation de leur gravité séparément et l'évaluation de l'acceptabilité de chaque risque. Par conséquent, chaque étape qui constitue ce processus doit être réalisée conformément à cette exigence, afin qu'un jugement précis.
- **Traitement du risque** : Une fois que les risques sont déterminés, répertoriés et évalués, c'est-à-dire une fois que chaque risque est jugé acceptable ou non, il comprend une variété d'options possibles. Par conséquent, nous présenterons successivement quatre options principales de traitement des risques, qui sont les suivantes:
  - L'acceptation du risque,
  - La réduction du risque,
  - Le transfert du risque,
  - L'évitement du risque.

- **Gestion des risques**: La gestion des risques englobe tous les processus. Une fois les décisions prises en matière de gestion des risques, ces processus permettront de mettre en œuvre ces décisions, de surveiller leurs effets et d'apporter des améliorations si nécessaire.

9.3.3 Mise en service des bases de connaissances de MEHARI

La richesse de MEHARI repose sur l'utilisation d'une base de connaissances personnalisable et généralisable par statut de risque: Le but est de se concentrer sur les détails de la situation de risque analysée, d'apporter de l'expertise, d'enrichir l'expérience accumulée et coordination des plans d'action. [16]

MEHARI comprend trois bases de connaissances :

- **Méhari-Expert :** s'adresse plus particulièrement à des architectures comprenant plusieurs sites et des organisations décentralisées avec pluralité d'acteurs.
- **Méhari-Standard :** s'adresse plus particulièrement à des architectures moyennes comprenant un seul site et une organisation des systèmes d'information centralisée (DSI).
- **Méhari-pro :** s'adresse plus particulièrement à des petites ou très petites entreprises.

Elle comprend également un module sans base de connaissances : **Méhari-Manager**, est particulièrement destiné à des managers ou décideurs qui souhaitent procéder à une analyse de risques plus particulièrement ciblée sur certains points d'intérêt.

Les bases de connaissances de MEHARI sont disponibles en téléchargement gratuit sur le site de CLUSIF Clusif au format Microsoft Excel.

Conclusion

Dans ce chapitre, nous avons présenté les concepts généreux sur le plan de reprise d'activité dans une organisation et aussi son élaboration et les différentes méthodes d'analyse de risque. Dans le prochain chapitre, nous présenterons le plan de reprise d'activité pour la CNAS.

Chapitre II : Plan de Reprise d'Activité de l'Organisme d'accueil

Introduction

En cas de catastrophe, il n'y a presque pas de temps pour réagir. Plus il faut de temps pour restaurer les systèmes critiques, plus la perte potentielle est importante. Il est extrêmement important d'être prêt à agir immédiatement. Par conséquent, la première étape de la reprise après sinistre est la planification et la prévention. Ce chapitre traite de la sécurité des systèmes, afin d'éviter les sinistres, et de la planification de la reprise après sinistre.

1 Présentation de l'organisme d'accueil

La CNAS est considérée comme l'établissement pivot du système de sécurité sociale en Algérie, dans la mesure où elle protège une très large population contre la quasi-totalité des risques de la vie (maladie, maternité, accidents du travail, maladies professionnelles, invalidité et décès).

La CNAS est un organisme de sécurité sociale érigé en EPGS conformément au décret exécutif 92-07 du 04 Janvier 1992 portant statut juridique des caisses de sécurité sociale et organisation administrative et financière de la sécurité sociale et a pour mission de :

Figure 4 : Les missions de la CNAS

1.1 L'organigramme de la CNAS

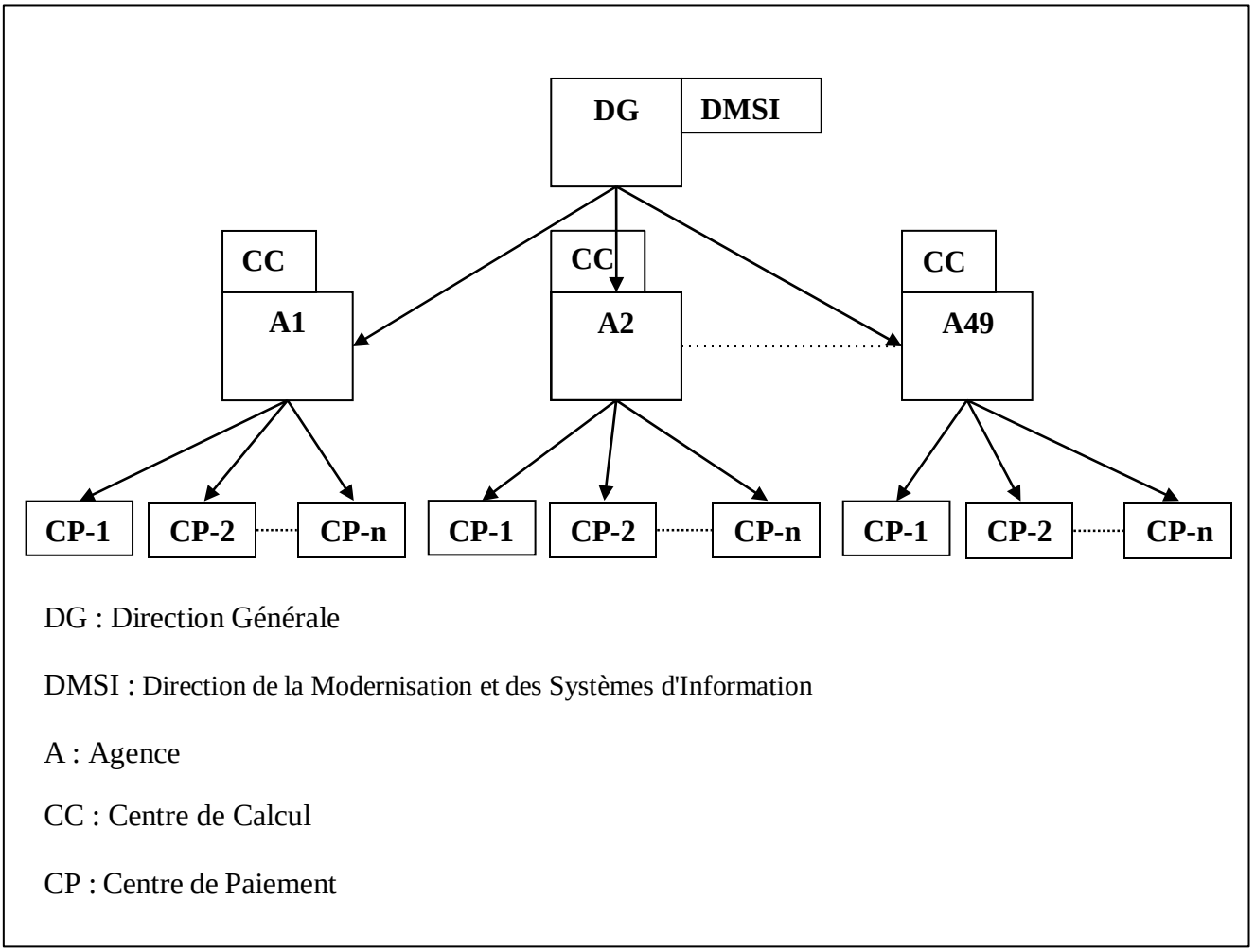

Figure 5 : l'organigramme de la CNAS [17]

La Direction Générale
La Direction Générale se situe à Ben-Aknoun, son rôle est de gérer toutes les informations provenant des directions centrales à travers les wilayas vers Alger. Elle est représentée par des agences locales auxquelles sont rattachées plusieurs structures.

La Direction de la Modernisation et des Systèmes d'Information
Elle est rattachée à la direction générale. Son rôle est d'établir les différents programmes utilisés dans les structures de la CNAS et d'assurer la maintenance.

Les Agences :
L'agence de wilaya de la CNAS est chargée, sous l'autorité du directeur, outre son rôle, d'organiser, de coordonner et de contrôler les activités des centres de paiement des communes et des antennes d'entreprise ou d'administration.

Centre de calcul :
Le centre de calcul est chargé du traitement et de la saisie des données, ainsi que de l'édition, de l'enregistrement, des allocations familiales, de la comptabilité, du transfert des assurés, etc.

Le centre de calcul fait partie de l'agence, et chaque agence a un centre de calcul sauf les Wilayas peu peuplées, son travail est effectué par d'autres centres de données.

1.2 Les structures de la CNAS

- Une direction générale.
- 49 Agences de wilaya (dont 2 à Alger).
- 826 structures de paiement (dont 356 centres de paiement, 401 antennes de paiement, 69 correspondances locales).
- 4 cliniques spécialisées (chirurgie cardiaque infantile, orthopédie et rééducation ORL, dentaire).
- 4 centres régionaux.
- 35 centres de diagnostic et de soins.
- 55 officines pharmaceutiques.
- 30 crèches et jardins d'enfant.
- Une imprimerie à Constantine.
- Un centre familial à caractère social à Ben Aknoun. [18]

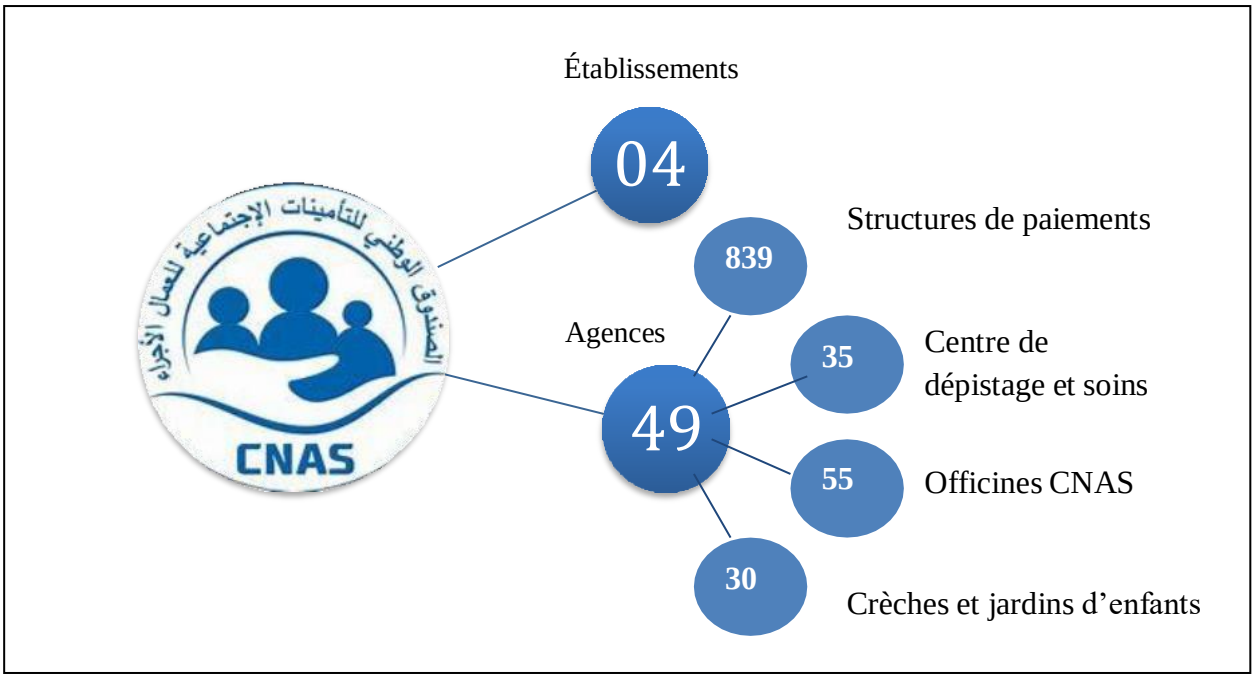

Figure 6 :Les structures de la CNAS

1.3 L'organigramme de la DMSI

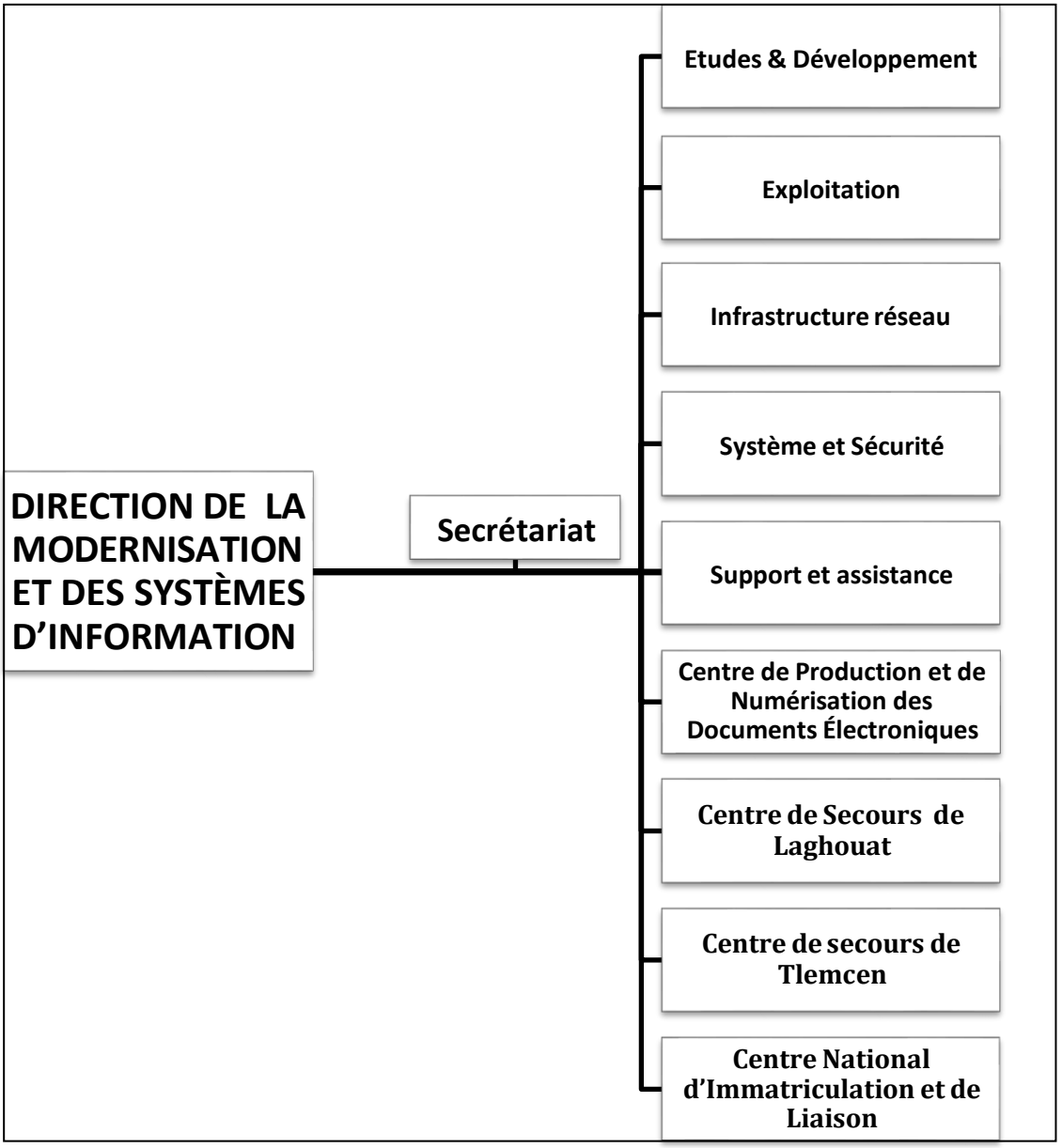

Figure 7 : L'organigramme de la DMSI [17]

Site central de Laghouat : construit en 2007 pour être le site de secours du site central d'Alger

•Héberge la totalité et réplique des données et solution liée au système d'information de la CNAS

•Inclut la seconde zone de production des cartes CHIFA d'une capacité de production de 500 Cartes/Jour.

Site central de Tlemcen : construit en 2017 pour être le site Backup du site central d'Alger

•Héberge les Backups des données et solutions liées au système d'information de la CNAS. [17]

1.4 Le flux informationnel

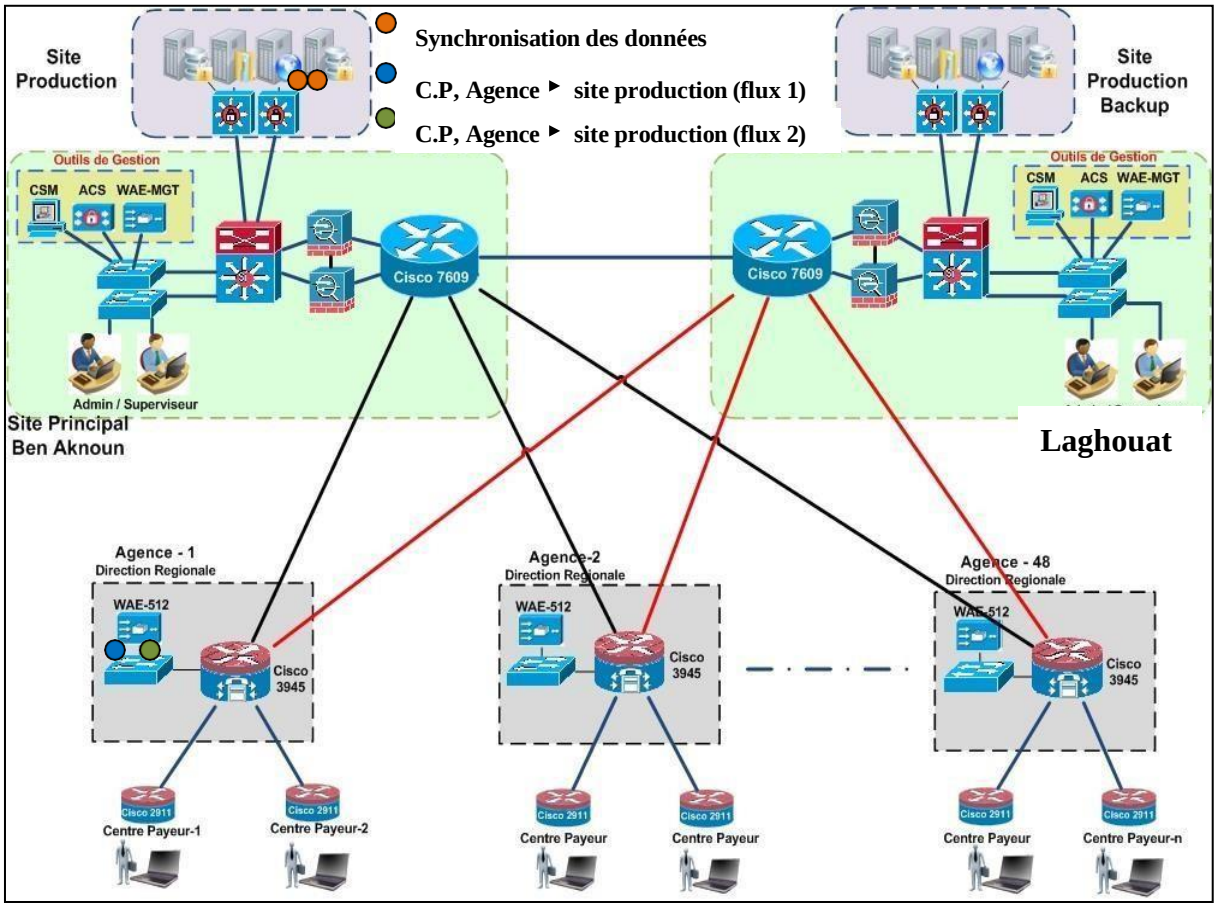

Figure 8 :Le schéma de flux informationnel

2 Identification des actifs

Actifs	Vulnérabilités	Menaces
Actifs primaires		
Informationnels		
site web: www.cnas.com	Faille dans les langages de développement du serveur Web	Prise de contrôle du site web, attaque par déni de service
Messages électroniques	La réception et l'intégrité des messages non contrôlés	Faux message
Document d'utilisation	Intégrité et version de documentation non contrôlé	Modification malveillante, le pharmacien non à jour
Processus		
Processus d'exploitation de l'application de la carte CHIFA	Manque de comptabilité des logiciels, pas de planification des notifications pour les nouvelles versions de l'application	Difficulté d'installation
Mise à jour de la liste noire qui contient des cartes CHIFA perdues, des assurés suspendus etc.	Infection du fichier de MSJ	Echec de la MAJ
Mise à jour de la liste des assurés hors CHIFA		L'assuré suspendu de bénéficiassions des médicaments
Mise jour de la liste nomenclature des médicaments		L'assuré suspendu de bénéficiassions des médicaments
Actifs secondaires		
Personnel		
Propriétaire de la pharmacie	Manque de formation	Faible utilisation de l'application

Agent CNAS	Manque de formation et de communication	Perte de partenaire
Matériel		
Ordinateur	Manque de performance	Perte de temps dans la réalisation des taches
Carte CHIFA	Pas de mécanisme de contrôle	Utilisation frauduleuse de la carte CHIFA
Logiciels		
CHIFA OFFICINE	Non mis à niveau de l'application, Dysfonctionnement de logiciel	Retard de service
CHIFA-WEB	Faille dans les langages de développement du serveur Web	Attaque XSS, SQL injection
Client VPN	Mal configuration de règles de routage dans le client VPN	Corruption de données, Eavesdropping
Système d'exploitation	Faille de système	Exploitation d'une vulnérabilité connue
Réseaux		
Modem	Absence ou indisponibilité de service du fournisseur de connexion	Pas de connexion à l'internet

Tableau 2: Identification des actifs

3 Paramètres d'évaluation des risques

3.1 L'impact

MEHARI distingue 4 niveaux d'impact

- **Niveau 4: vital** à ce niveau le dysfonctionnement redouté et extrêmement grave et met en danger l'existence même ou la survie de l'entité ou l'une de ses activités majeurs.
- **Niveau 3: Très grave** il s'agit de dysfonctionnement très grave au niveau de l'entité, sans que son avenir ne soit compromis.
- **Niveau 2: Important** il s'agit là de dysfonctionnement ayant un impact notable au niveau des opérations de l'entité, de ses résultats ou de son

image, mais restant globalement supportables.

- **Niveau 1: Non significatif** a ce niveau les dommages encourus n'ont pratiquement pas de conséquences sur les résultats de l'entité ni sur son image. **[19]**

Echelle d'évaluation de l'impact

Qualification du besoin en			Niveau	
confidentialité	Intégrité	Disponibilité	Signification	Valeur
Informations pouvant être publiques	Pas de validation nécessaire	Aucune	Non significatif	1
Accès autorisé à l'ensemble	Peut être partiellement intègre	Arrêt de travail court	Important	2
Accès autorisé à l'ensemble de l'équipe	Doit être intègre	Arrêt de travail long	Très grave	3
Accès autorisé à un membre unique de l'équipe	Doit être parfaitement intègre	Aucun arrêt tolérable	Vital	4

Tableau 3: Echelle de l'impact

- **Niveau 4: Très probable**, il est raisonnable de penser que le scénario se produira très certainement et vraisemblablement à court terme.

- **Niveau 3: Probable**, il s'agit là des scénarios dont il est raisonnable de penser qu'ils pourraient bien se produire, à plus ou moins court terme. L'espoir que l'événement ne survienne pas insensé mais dénote un certain optimisme. La survenance de l'évènement déçoit, mais ne surprend pas.

- **Niveau 2: Improbable**, il s'agit là de scénarios dont il est raisonnable de penser qu'ils ne surviendront pas. L'expérience passée montre souvent d'ailleurs qu'ils ne sont pas survenus. Ils demeurent néanmoins possible et ne sont pas complètement invraisemblables.

- **Niveau 1: Très improbable** à ce niveau l'occurrence du scénario est tout à fait improbable. De tels scénarios ne sont pas strictement impossibles car il existe toujours une probabilité, même infime, pour que cela se produise. **[19]**

3.2 La gravité

La gravité de la situation de risque résulte à la fois de sa probabilité et de son impact. Il ne s'agit pas, cependant, d'une opération mathématique entre ces deux valeurs mais d'un jugement sur le caractère acceptable ou non de la situation.

- **Risque insupportables**, qui devrait faire l'objet de mesures d'urgence, en dehors de tout cycle budgétaire.
- **Risque inadmissibles**, qui devrait être réduits ou éliminés à une Echéance à déterminer, donc à prendre en compte dans une planification.
- **Risques tolérés. [19]**

		Probabilité			
		Très improbable	**Improbable**	**Probable**	**Très probable**
Impact	**Vital**	Toléré	Inadmissible	Insupportable	Insupportable
	Très grave	Toléré	Inadmissible	Inadmissible	Insupportable
	Important	Toléré	Toléré	Toléré	Inadmissible
	Insignifiant	Toléré	Toléré	Toléré	Toléré

Tableau 4: Matrice de gravité [19]

4 Les types de Risque

On distingue trois types de risque :

4.1 Le risque toléré

On ne prévoie pas de mesure spécifique pour ce type de risque. On considère :

- Que son impact est insignifiant sur les continuités des activités dela direction.
- Ou que sa probabilité est trop faible pour qu'on s'en inquiète.

4.2 Le risque inadmissible

Les risques qui devraient être réduits ou éliminés à une échéance à déterminer, Donc on prévoit des mesures.

4.3 Le risque insupportable

Le niveau de risque le plus élevé, il devrait faire l'objet de mesure d'urgence en dehors de tout cycle budgétaire.

5 La gestion des risques

5.1 Appréciation des risques

Les risques encourus sont de différentes natures, et peuvent s'étaler sur un très grand éventail (humains, naturels, financière, Politiques, technologiques ...), mais le déclanchement du PRA se repose sur les risques qu'on a illustré comme suit :

Type du risque	Risque	Impact	Probabilité	Niveau de gravité
Absence ou indisponibilité accidentelle de service	Absence de service: électricité	3	4	Insupportable
	Instabilité dans le courant électrique du Datacenter	3	2	Inadmissible
	Absence de maintenance système ou applicative	3	2	Inadmissible
	absence de service: climatisation	3	2	Inadmissible
	Absence de fournisseur de connexion	3	3	Inadmissible
	Absence de service: locaux(Datacenter)	4	1	Toléré
Erreur de matérielle ou de comportement personnel	Erreur de saisie ou de frappe	3	4	Insupportable
	Perte de données DATA	4	2	Inadmissible
Malveillance menée par voie logique ou fonctionnelle	Cyberattaque interne	4	3	Insupportable
	Cyberattaque externe	3	4	Insupportable
	Accès non autorisé aux fichiers système	4	2	Inadmissible
Malveillance mené par voie physique	Vol physique	3	3	Inadmissible
	Vandalisme	4	1	Toléré
	Terrorisme	4	1	Toléré
Catastrophe naturelle et Accident grave d'environnement	séisme	4	3	Insupportable
	Incendie	4	2	Inadmissible
	Pollution	4	2	Inadmissible
	foudroiement	4	2	Inadmissible
	Inondation	4	1	Toléré
Incident dû à l'environnement	Surcharge électrique	3	2	Inadmissible
Panne hardware	Panne des équipements de sécurité	3	2	Inadmissible
	Panne d'équipement informatique et télécom	2	3	Toléré
Incident logique ou fonctionnel	Incident d'exploitation	2	2	Toléré
	Bug dans un logiciel	2	2	Toléré
	virus	2	3	Toléré
Absence de personnel	Absence accidentelle de personnel	1	3	Toléré
	Conflit social avec grève	2	2	Toléré
panne software	Défaillance de	4	2	Inadmissible

	l'application métier			
	Défaillance de l'application support	3	2	Inadmissible
	L'inactivité des logiciels de contrôle de cyberattaque	4	2	Inadmissible
Panne réseau	Coupure réseau	4	3	Insupportable
	Saturation réseau	4	3	Insupportable

Tableau 5: Les scénarios des risques

5.2 Réponse et mesure à prendre

Le travail jusqu'à présent a permis d'identifier et d'évaluer, l'objectif maintenant est de déterminer des réponses et plans d'action pour mitiger les risques. Cette section doit être consulté et appliqué dans le cas du déclenchement du **PRA.**

La hiérarchisation des risques est réalisée selon leur niveau de gravité décroissant. Elle permet de préciser les risques à prendre en compte ainsi que leurs priorités de prise en compte.

Type du risque	**Risque**	**Mesure de sécurité existante**	**Mesure de sécurité à mettre en place**
Absence ou indisponibilité accidentelle de service	Absence de service: électricité	-Groupe électrogène seconde source électrique	
	Absence de service: locaux (DATA center)	-Site de secours	
	absence de service: climatisation	-Redondance des équipements	-Analyse de la capacité -Tests et maintenance réguliers
	Absence de fournisseur de connexion	-Service supervision - Contacter les fournisseurs de connexion pour régler le problème	
	Absence de maintenance système ou applicative	-Brigades 7/7 -Permanence de la maintenance des applications critiques	
Erreur de matérielle ou de comportement	Perte de donnés DATA	-Sauvegarde et redondance des bases de données	
	Erreur de saisie	-Contrôle permanant sur les données	-Détection des

personnel	ou de frappe		tentatives de modification
Malveillance menée par voie logique ou fonctionnelle	Cyberattaque interne	Utilisation de : -Fichiers journaux (LOG) -WAF\Firewall\VPN \IPS	-Contrôle d'accès RBAC - IDS
	Cyberattaque externe	Utilisation de : -Fichiers journaux (LOG) -WAF\Firewall\VPN\IPS Isoler les programmes et processus à tester afin d'analyser leur comportement	-Contrôle d'accès RBAC - IDS
	Accès non-autorisé aux fichiers système		-Un contrôle d'accès RBAC
Malveillance mené par voie physique	Terrorisme	-Contrôle d'accès physique	
	Vandalisme	-Surveillance des locaux (télésurveillance) et des intervenants externes (ménage)	
	Vol physique	-Utilisation des empreintes -mettre des règles de protection	Utilisation des: -Accès par mot de passe -Carte à puce
Catastrophe naturelle et Accident grave d'environnement	foudroiement		Protection contre la foudre : -paratonnerre, -protection contre les surtensions
	Incendie	-Détecteur de fume	
	Inondation	-Détecteur d'humidité	
	séisme		-Construire des bâtiments parasismiques
Incident dû à l'environnement	Surcharge électrique		-Qualité et sécurité de la fourniture électrique : redondance,

			onduleur, maintenance et vérification des équipements -Sécurité des équipements de servitude : remplacement rapide
Crise sanitaire	Pandémie		-Déclenchement de PCA
Accident matériel	Panne d'équipement informatique et télécom	-Redondance des équipements -Basculement automatique sur la liaison de secours	-Un outil de supervision de réseau
	Perte du réseau de communication IP		
Incident logique ou fonctionnel	Incident d'exploitation	-Tests réguliers	
	Bug dans un logiciel		-contrôle de la mise en production -contrôle de la conformité des configurations -Sécurité des processus de développement applicatifs (tests de non-régressions, stress-tests
	virus	-Protection antivirus	
Absence de personnel	Absence accidentelle de personnel	-Gestion du personnel et des partenaires stratégiques -travail en équipe	
	Conflit social avec grève	-Gestion des ressources humaines	
panne software	Défaillance de l'application métier	- Correction de code -Test d'intégrité -Redéploiement	
	Défaillance de l'application support	- Correction de code -Test d'intégrité -Redéploiement -Mise à jour	

	L'inactivité des logiciels de contrôle de cyberattaque	-Activation immédiate	
Panne réseau	Coupure réseau	-Basculement sur le site de secours	-Outil de supervision
	Saturation réseau	- Détection des pertes -Augmentation de débit	-Outil de supervision

Tableau 6: Les contres mesures

Pour assurer sa pérennité, l'entreprise doit comprendre la menace de perturbation de ses activités. L'analyse des risques lui permettra de quantifier l'évaluation des pertes et la probabilité des sinistres. Ainsi, avec une meilleure compréhension de l'étendue des risques qui se présentent, l'entreprise sera en mesure de rechercher des options pour réduire son impact. Ce n'est qu'ainsi qu'il pourra décider des actions à entreprendre pour maîtriser le risque.

6 Les ressources matérielles

6.1 Equipement de stockage

- **Baie de stockage :**

Une Baie de stockage est un composant informatique serveur dédié uniquement au stockage de données, il est caractérisé par une grande capacité de stockage et une politique de protection de données bien défini, de tell composant ce trouve uniquement dans les zones centrales.

Ci-dessous le tableau des Baie de stockage des différentes zones centrales

Zone	Référence	Capacité utilisable
Alger	DELL X	7 To
	DELL X	13 To
	DELL X	52 To
Laghouat	DELL X	27 To
Tlemcen	DELL X	27 To

Tableau 7: Baie de stockage

6.2 Equipement de communication (Réseau)

- **Routeur :**

Un routeur est un équipement réseau informatique assurant le routage des paquets de données.

Le tableau Ci-dessous présente les routeurs niveau nationale :

Référence	Nombre
A	2
B	1
C	19
D	18
E	96
F	269
G	15
H	423

Tableau 8: Les routeurs

- **Switch :**

Un Switch permet aux équipements de traitement d'un réseau de communiquer entre eux.

Le tableau Ci-dessous présente les Switch de niveau nationale :

Référence	Nombre
Cisco A	1407
Cisco B	64
Cisco C	2
Cisco D	8
Cisco E	3
Cisco F	2
Cisco G	3

Tableau 9: Les switch

- **IP-Phone :**

Un équipement utilisant des technologies de voix sur IP pour passer et transmettre des appels téléphoniques sur un réseau IP. Le parc de téléphone IP est de l'ordre de 3750 répartie sur l'ensemble des structures.

6.3 Equipement de traitement

- **Les serveurs**:

Considérés comme étant la puissance de calcul centrale du système d'information. Les sites centraux sont dotés d'une capacité de calcul adapté au besoin de l'organisme.

Le tableau suivant présente la liste des Serveurs Centraux

Zone	Référence	Nombre	Capacité unitaire	Capacité total
Alger	DELL	18	83 GHz	1494 Ghz
	DELL	34	56 GHz	1802 Ghz
Laghouat	DELL	16	83 GHz	1328 Ghz
	DELL	10	56 GHz	560 Ghz
Tlemcen	DELL	6	83 GHz	498 Ghz
	DELL	20	56 GHz	1120 Ghz

Tableau 10: Les serveurs

- **Les Terminaux** : estimé à plus de 1000 Pc.

6.4 Equipement de sécurité

Il existe deux types d'équipement de sécurité

- Les équipements de sécurité de zone (tel que les système anti incendie, anti inondation...)
- Les équipements de sécurité de cyberattaque (Firewall, WAF, IPS)
    - Entre Le site central et Internet
    - Entre Les structures internes

6.5 Les applications

Type	Application	description
Métier	SIGAS	Système de gestion des assurés sociaux (Gestion des risques)
	SIGCM	Système de gestion du contrôle médicale
	SIGMA	Système de gestion de recouvrement
	AF/RENTE	Allocation familiale et rente
	TELEDECLARATION	Système de déclaration des cotisations en ligne
	EL HANNA	Service en ligne destiné aux assurés
	PAIE	Gestion de la paie et de la carrière
	PASSERELLE DOF	Logiciel de régularisation des comptes comptable
	INSPECTION	Logiciel pour la gestion de l'inspection générale
	CELLULE D'ECOUTE	Logiciel de gestion de la cellule d'écoute

Support	Stockage et archive	Outil de sauvegarde et restauration des données
	Supervision	Outil de surveillance d'équipementet réseau
	Sécurité	Outil de prévention contre les cyberattaque
	Audit	Outil d'évaluation des normes
	Communication	Téléphone IP, messagerie…

Tableau 11: Les applications

7 Les activités critiques :

Quels sont les données, applications, logiciels et autres éléments qui faut absolument retrouver au plus rapide en cas d'incident majeur ? Pour répondre à cette question, on a répertoriés Les activités clés de la direction et leurs stratégies de sauvegarde et back-up adaptées ci-dessous :

Département / Centre	Activité (service) critique	Emplacement de l'activité (serveur, matériel)	RTO	Stratégie de sauvegarde/back up	Nom et emplacement de la sauvegarde
Réseau	Routage	Routeurs / Data Center	10 Min	Annuel et lors des modifications de configuration	Disque externe + DVD (responsable réseau) DVD (coffre DI)
	Switching	Switch / DataCenter	10 Min	Annuel et lors des modifications de la config	Disque externe + DVD (responsable réseau) DVD (coffre DI)
	Communication IP	Call Manager / DataCenter	10 Min	Annuel et Mensuel	Disque externe + DVD (responsable réseau) DVD (coffre DI)

	Sécurité	ASA + StoneSoft / DataCenter	10 Min	Annuel et lors des modifications de la config	Disque externe + DVD (responsable réseau) DVD (coffre DI)
Centre Personnalisation de carte CHIFA	Base de données (CMS, CNAS, SITE, NUM)		10 Min	-Réplication temps réel -Restauration Robot de sauvegarde	
	KMS (Key Manager system)		10 Min	-Redondance des Serveurs -restauration des sauvegardes des clés cryptographiques	
	Autorité de certification PKI		10 Min	Réplication temps réel -restauration des sauvegardes des clés cryptographiques	
	Vérification des Factures Electroniques		15 MIN	-Redondance des Serveurs -restauration des sauvegardes des clés cryptographiques	
	Machines de productions		10 Min	-Redondance des Machines	
	Robot de Sauvegarde		10 Min	-Redondance site Backup Laghouat	

Centre National D'immatriculation et de Liaison	Sauvegarde	Data center	10 Min	Support magnétique	Sigma/Data centre
Exploitation	Base de données Assurances sociales (ASS)	Serveur X	10 Min	Sauvegarde quotidienne à chaud	Bande de sauvegarde
		Data Center Central (DMSI)		Sauvegarde mensuelle à froid	Baie de stockage Archive du Data Center Principal
		-Stockage : Baie de stockage Principale		Réplication hebdomadaire vers le site de secours de Laghouat	Baie de stockage du site de secours de Laghouat
	Base de données du recouvrement (SIGMA)	Serveur X	10 Min	Sauvegarde quotidienne à chaud	Bande de sauvegarde
		Data Center Central (DMSI)		Sauvegarde mensuelle à froid	Baie de stockage Archive du Data Center Principal
		-Stockage : Baie de stockage Principale		Réplication quotidienne vers le site de secours de Laghouat	Baie de stockage du site de secours de Laghouat
	Base de données des allocations familiales et les Rentes d'ATMP	Serveur X	15 Min	Sauvegarde quotidienne à chaud	Bande de sauvegarde
		Data Center Central (DMSI)		Sauvegarde mensuelle à froid	Baie de stockage Archive du Data Center Principal

		-Stockage : Baie de stockage Principale		Réplication quotidienne vers le site de secours de Laghouat	Baie de stockage du site de secours de Laghouat
	Base de données des Professionnels de Santé	Virtual machine sur le Serveur X	10 Min	Sauvegarde quotidienne à froid	Bande De sauvegarde
		Data Center Central (DMSI)			
		-Stockage : Baie de stockage Principale		Réplication quotidienne vers le site de secours de Laghouat	Baie de stockage du site de secours de Laghouat
	Base de données Elhanaa	Virtual machine sur le Serveur X	10 Min	Sauvegarde quotidienne à froid	Bande De sauvegarde
		Data Center Central (DMSI)			
		-Stockage : Baie de stockage Principale		Réplication quotidienne vers le site de secours de Laghouat	Baie de stockage du site de secours de Laghouat
	Base de données ERP	Serveur X	15 Min	Sauvegarde quotidienne à froid	Bande De sauvegarde
		Data Center Central (DMSI)			

		-Stockage : Baie de stockage Principale		Réplication quotidienne vers le site de secours de Laghouat	Baie de stockage du site de secours de Laghouat
	FTP Fiche Médicale Electronique	Serveur X	15 Min	Réplication en temps réel	Baie de stockage du site de secours de Laghouat
		Data Center Central (DMSI)			
		-Stockage : Baie de stockage Principale			

Tableau 12: les activités critiques de la CNAS

8 Liste des contacts d'urgence :

domaine de responsabilité	Nom/Prénom	fonction	numéro IP phone	numéro mobile	adresse mail
Directeur du recouvrement des opérations	Agent X	Directeur Informatique	X	X	X
Responsable de la reprise des opérations et équipes	Agent X	Responsable SSI	X	X	X
Équipe de rétablissement des installations	Agent X	Technicien supérieur	X	X	X
	Agent X	Administrateur Réseau	X	X	X
Équipe de récupération du réseau	Agent X	Responsable d'infrastructure réseau	X	X	X
	Agent X	Administrateur réseau	X	X	X

Équipe de récupération de la plate-forme	Agent X	Responsable l'exploitation	X	X	X
	Agent X	Développeur	X	X	X
Équipe d'évaluation et de récupération des dommages	Agent X	Administrateur BD	X	X	X
	Agent X	Consultant technique	X	X	X
Équipe de sécurité physique	Agent X	Agent de sécurité	X	X	X
	Agent X	Agent de sécurité	X	X	X
Équipes de communication	Agent X	Ingénieur réseau	X	X	X
	Agent X	Responsable support	X	X	X
Équipes d'installation du matériel	Agent X	Technicien	X	X	X
	Agent X	Ingénieur réseau	X	X	X
Équipes chargées des opérations informatiques	Agent X	Responsable des opérations informatique	X	X	X
	Agent X	Administrateur réseau	X	X	X
	Agent X	Ingénieur système	X	X	X
Équipes techniques informatiques	Agent X	Responsable technique	X	X	X
	Agent X	technicien	X	X	X
Équipes administratives	Agent X	Assistante	X	X	X

Tableau 13: Liste des contacts d'urgence

9 Les responsabilités

Domaine de responsabilité	**Responsabilité dans le PRA**	
	Avant le sinistre	**Après le sinistre**
Directeur du recouvrement des opérations	- Approuver le PRA final et les procédures. - Maintenir le PPA et les procédures.	- Déclarer l'occurrence d'une catastrophe - Définir la mise en œuvre de la stratégie si plusieurs stratégies existent. - Gérer et surveiller l'ensemble du processus de récupération.
Responsable des équipes et de la reprise des opérations	- Développer, maintenir et mettre à jour le PRA. - Attribuer des parties du PRA aux différentes équipes de rétablissement. - Coordonner les tests du PRA. - Former les membres de l'équipe de rétablissement à la mise en œuvre du plan	- La déclaration de sinistre à tous les chefs d'équipe de rétablissement. - Déterminer le degré d'interruption de service dû à la catastrophe. - coordonner et résumer les rapports de dommages de toutes les équipes. - Informer le directeur de l'organisation de la gravité de la catastrophe. - Organiser des réunions d'information avec les équipes de rétablissement.
Équipe de rétablissement des installations	- Préparer le site alternatif avec du matériel et des fournitures. - Création d'un plan et d'une procédure de récupération pour le site de secours.	- Réparation et reconstruction du site primaire.
Équipe de récupération du réseau	- Installer les équipements de réseau sur le site de secours.	- Fournir des connexions réseau sur le site alternatif. - Rétablissement des connexions réseau sur le site principal.
Équipe de récupération de la	- Test de vulnérabilité	- Installation d'équipements matériels.

plate-forme		- Restauration de données et de systèmes à partir de sauvegardes à distance
Équipe d'évaluation et de récupération des dommages	- Comprendre les rôles et les responsabilités - Former les employés pour qu'ils soient bien préparés en cas d'urgence. - Participer aux tests du PRA.	- Détermination des dommages. - Tenir un registre du matériel et des équipements réparables. - Estimation du temps de récupération en fonction de l'évaluation des dommages.
Équipe de sécurité physique	- Comprendre les rôles et les responsabilités - Former les employés. - Se familiariser avec liste de contact d'urgence. - Tenir à jour la liste des membres autorisés à pénétrer dans le site du sinistre et le site de secondaire	- Évaluation des dommages sur le site de la catastrophe. - Bloquer l'accès illégal au centre des données. - Organiser la sécurité pour le transport des fichiers, des rapports et des équipements.
Équipes de communication	- Comprendre les rôles et les responsabilités - Former les employés. - Participer aux tests du PRA. - Mettre en place et maintenir l'équipement de communication sur le site de secours.	- Récupérer la configuration de communication à partir des unités de stockage hors site. - Planifier, coordonner et installer l'équipement de communication sur le site de secours
Équipes d'installation du matériel	- Maintenir la configuration actuelle du système et du réseau local dans un stockage hors site.	- Vérifier les besoins en matériel sur le site de secours. - Inspecter l'espace physique requis sur le site de secours. - Coordonner le transport des équipements réparables vers le site de secours. - Planifier et installer le matériel sur le site de secours.

Équipes chargées des opérations informatiques	- Comprendre les rôles et les responsabilités - Assurer des sauvegardes complètes selon le calendrier prévu. - Assurer que les sauvegardes sont envoyées à l'emplacement distant.	- Envoi et réception de conteneurs de stockage hors site. - S'assurer que les bandes de sauvegarde sont envoyées au stockage hors site. - Maintenir une méthode de signature d'entrée/sortie pour toutes les ressources sur le site de secours. - Vérifier la sécurité du site de secours et de son réseau local. - coordonner le transfert des systèmes, des ressources et des personnes vers le site de secours.
Équipes techniques informatiques	- Comprendre les rôles et les responsabilités en matière de reprise après sinistre. - Former les employés. - Participer aux tests du PRA	- Restauration des ressources du système à partir du support de sauvegarde. - Effectuer des sauvegardes sur le site distant. - Tester et vérifier les systèmes d'exploitation. - Modification de la configuration du réseau local pour se connecter à la configuration de l'autre site.
Équipes administratives	- Comprendre les rôles et les responsabilités en matière de reprise après sinistre. - Former les employés. - Assurer la disponibilité adéquate de fonds d'urgence. - Évaluer les communications alternatives nécessaires si les services téléphoniques ne sont plus disponibles.	- Tenir un registre de tous les achats en cours et des livraisons prévues. - Traiter les demandes de paiement pour toutes les factures liées à la procédure de recouvrement. - Fournir des moyens de communication - Effectuer des tâches administratives et de gestion provisoires selon les besoins des équipes de reprise après sinistre.

Tableau 14: Les responsabilités des équipes

10 Déclenchement du PRA

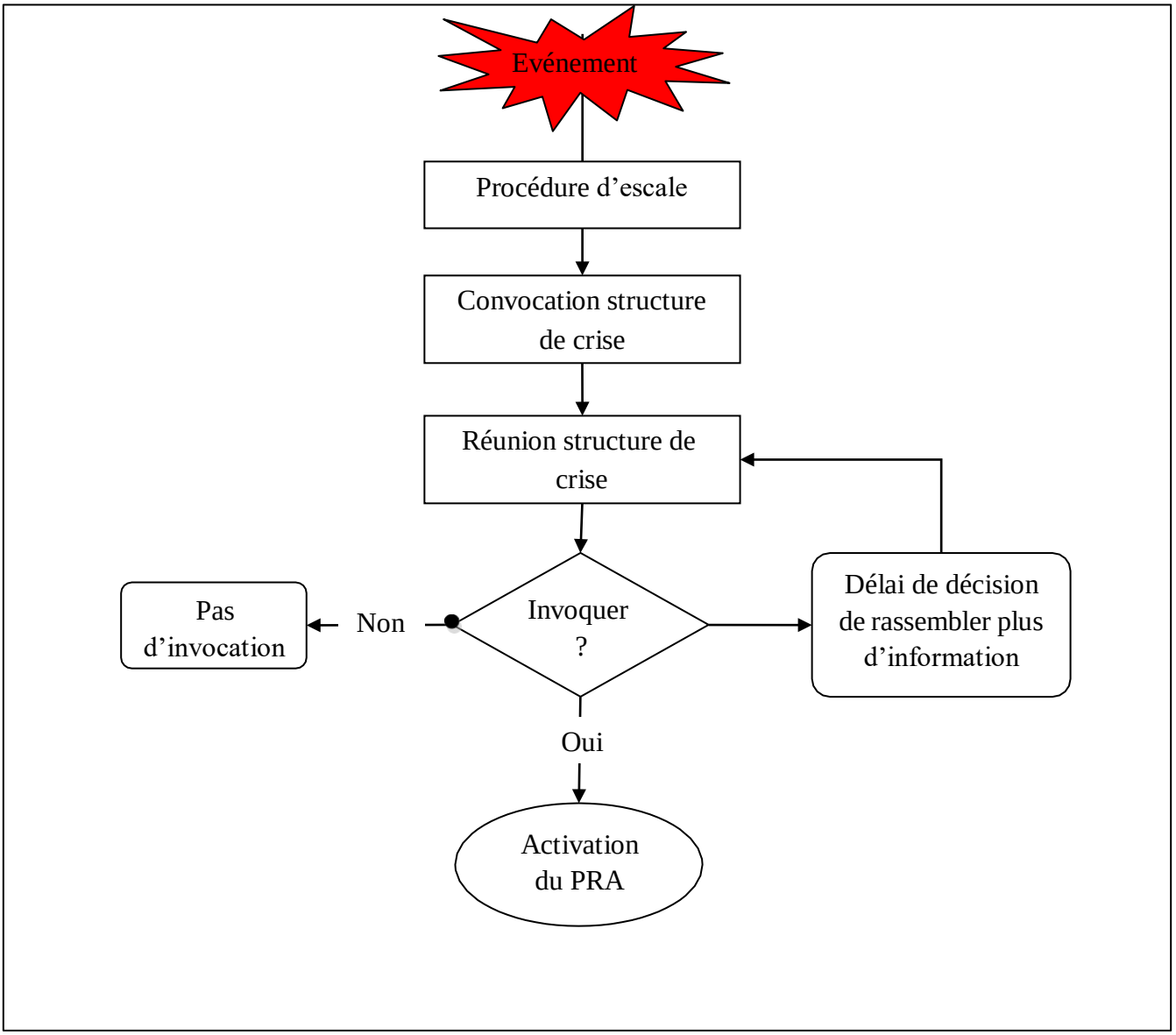

Figure 9 : Déclenchement du PRA [7]

Procédure d'escale désigne la procédure à suivre pour informer un superviseur ou un opérateur plus spécialisé.

La structure de la crise se compose d'un comité de crise et d'une cellule de coordination.

Le comité de crise est composé de directeur général, le responsable du PRA et les directeurs des sous directions (infrastructure réseau, systèmes et sécurité, étude et développement, exploitation, support et assistante). Le comité de crise prend la

décision principale, notamment, il juge de l'opportunité de déclencher certaines composantes du PRA en fonction du contexte.

La cellule de coordination est composée du responsable PRA et du personnel chargé de la coordination des opérations informatiques.

Conclusion

Dans ce chapitre, on a appliqué le plan de reprise d'activité sur l'organisme d'accueil en utilisant la méthode de gestion de risque MEHARI. Dans le prochain chapitre, nous allons automatiser le Monitoring pour le plan de reprise d'activité.

Chapitre III : Conception

Introduction

Pour l'étude conceptuelle de notre projet, nous avons opté pour le Processus Unifié qui est basé sur le langage de modélisation UML comme processus de développement.

Dans ce chapitre nous présenterons les besoins de système et les différents diagrammes.

1 Les diagrammes

1.1 Les diagrammes de cas d'utilisation

Fournit une vue d'ensemble de la fonctionnalité du système ou des processus opérationnels du point de vue de l'utilisateur. La façon dont un utilisateur "utilise" le système est le point de départ pour créer un diagramme de cas d'utilisation. [21]

1.2 Les diagrammes de séquences

Modélise les interactions entre les objets en fonction de leurs lignes de temps. Les objets peuvent être spécifiquement représentés sur ces diagrammes, mais ils peuvent aussi être des objets anonymes appartenant à une classe. La séquence d'exécution des messages entre objets au moment de l'exécution est bien modélisée par ces diagrammes, d'où leur nom. [21]

1.3 Le diagramme de classe

Représente les classes, leurs définitions et leurs relations. Les classes et les entités de l'espace problème sont également des entités techniques détaillées dans l'espace des solutions. Les attributs et les opérations qui définissent les classes sont incluses dans ce diagramme de classes. Les relations dans un diagramme de classes illustrent comment les classes interagissent, collaborent, et héritent d'autres classes. Les classes peuvent également représenter des tables relationnelles, des interfaces utilisateur et des contrôleurs. [21]

1.4 Le diagramme de navigation

Représente le modèle de navigation de notre application qui donne une vision générale sur le design d'application et une illustration de la navigation entre ses différentes interfaces.

2 Capture des besoins

Dans cette première partie, nous allons détailler et analyser les différents besoins fonctionnels et non fonctionnels.

2.1 Besoin fonctionnels

Le système à réaliser doit répondre aux besoins suivants :

2.1.1 Inscription :

Chaque utilisateur doit s'inscrire avant de s'authentifier dans l'application pour avoir un accès sécurisé à un compte protégé par un mot de passe.

2.1.2 Authentifier :

Pour accéder aux différents pages de l'application il faut s'authentifier d'abord.

2.1.3 Gérer les groupes de check :

Représente un regroupement de vérification connexe avec lequel on peut opérer conjointement.

- ✓ Titre: Pour identifier le groupe de check.

2.1.4 Contrôle :

Représente une vérification ou un point de surveillance sur un service distant.

- ✓ Titre : Titre pour identifier le check.
- ✓ Description : Informations supplémentaires sous forme textuelle sur le check.
- ✓ Fréquence de la vérification: Fréquence temporelle de la vérification, exprimée en minutes.
- ✓ Notifier par mail : Indique si les changements dans le statut du check doivent être notifiés par mail.

2.1.5 Check Ping :

Représente une vérification via des paquets ICMP.

- ✓ Identifiant de la machine à laquelle est envoyé le Ping.

2.1.6 Check Port :

Représente une vérification d'un port s'il est ouvert ou non sur un serveur distant.

- ✓ Identifiant de la machine à vérifier.
- ✓ Port cible : Port distant sur la machine à vérifier.

2.1.7 Check DNS :

Représente une vérification d'enregistrement DNS sur un domaine.

- ✓ Domaine sur lequel effectuer la vérification DNS.

- ✓ Type d'enregistrement **:** Type d'enregistrement DNS à vérifier. Il peut s'agir de A, AAAA, CNAME, MX et TXT.

2.1.8 Check http :

Représente une vérification via des requêtes HTTP sur un hôte distant.

- ✓ URL cible à vérifier.
- ✓ Code d'état : Code que la requête doit renvoyer à l'URL indiquée.

2.1.9 Registre de vérification:

Représente le résultat de l'exécution d'une vérification à un instant donné.

- ✓ La date et l'heure d'obtention de cet enregistrement.
- ✓ Statut : c'est le résultat du lancement de la vérification, l'état peut être Up, ce qu'il dit que l'objectif fonctionne; Down, ce qui indique que la cible ne fonctionne pas correctement ; et Error, qui indique qu'il y a eu un problème de lancement de la vérification.
- ✓ Le temps de réponse : (uniquement pour les contrôles de type Ping) indique le temps de réponse moyenne obtenue au lancement du contrôle.

2.1.10 Vérifier l'état :

Représente un changement dans l'état d'un check, détecté après analyse d'un enregistrement de check.

- ✓ Date de début : La date et l'heure auxquelles le check est entré dans cet état.
- ✓ Date de fin : La date et l'heure auxquelles le check est sorti de cet état.
- ✓ Statut : Définition du statut du check. Le statut peut être Up, ce qui indique que l'objectif fonctionne ; Down, ce qui indique que l'objectif ne fonctionne pas correctement; et Error, qui indique qu'il y a eu un problème de lancement de la vérification.

2.2 Besoins non fonctionnels

Les besoins non fonctionnels sont les besoins qui spécifient les propriétés du système.
Ce sont les besoins en matière de performance, de type de matériel ou de type de conception.
Ils peuvent aussi concerner les contraintes d'implémentation (langage de programmation, type SGBD, de système d'exploitation, etc.).

2.2.1 Simplicité :

Les interfaces doivent être simples, lisibles et faciles à utiliser.

2.2.2 Fiabilité et rapidité :

Notre système doit garantir la rapidité et la fiabilité de la recherche des informations, ainsi qu'une gestion optimale des ressources.

2.2.3 Facilité :

Facilité de manipulation de l'application.

2.2.4 Convivialité :

Interface conviviale et ergonomique (navigation simple au niveau des interfaces).

3 Modélisation de l'interface

Dans cette section nous présenterons les diagrammes de notre interface

3.1 Diagramme de cas d'utilisation

3.1.1 Les acteurs

Ils sont les entités externes qui interagissent avec le système.

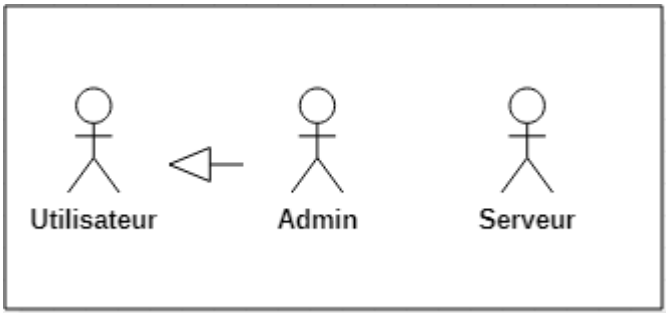

Figure 10 : Les acteurs

Acteur	Description
Utilisateur	Utilisateur externe du système, qui peut créer un compte ou s'être connecté.
Admin	L'administrateur est représenté par tout utilisateur utilisant la console d'administration de l'application.
Serveur	Le moteur de l'application, qui supervise périodiquement les services.

Tableau 15: La description des acteurs

3.1.2 Diagramme de cas d'utilisation général

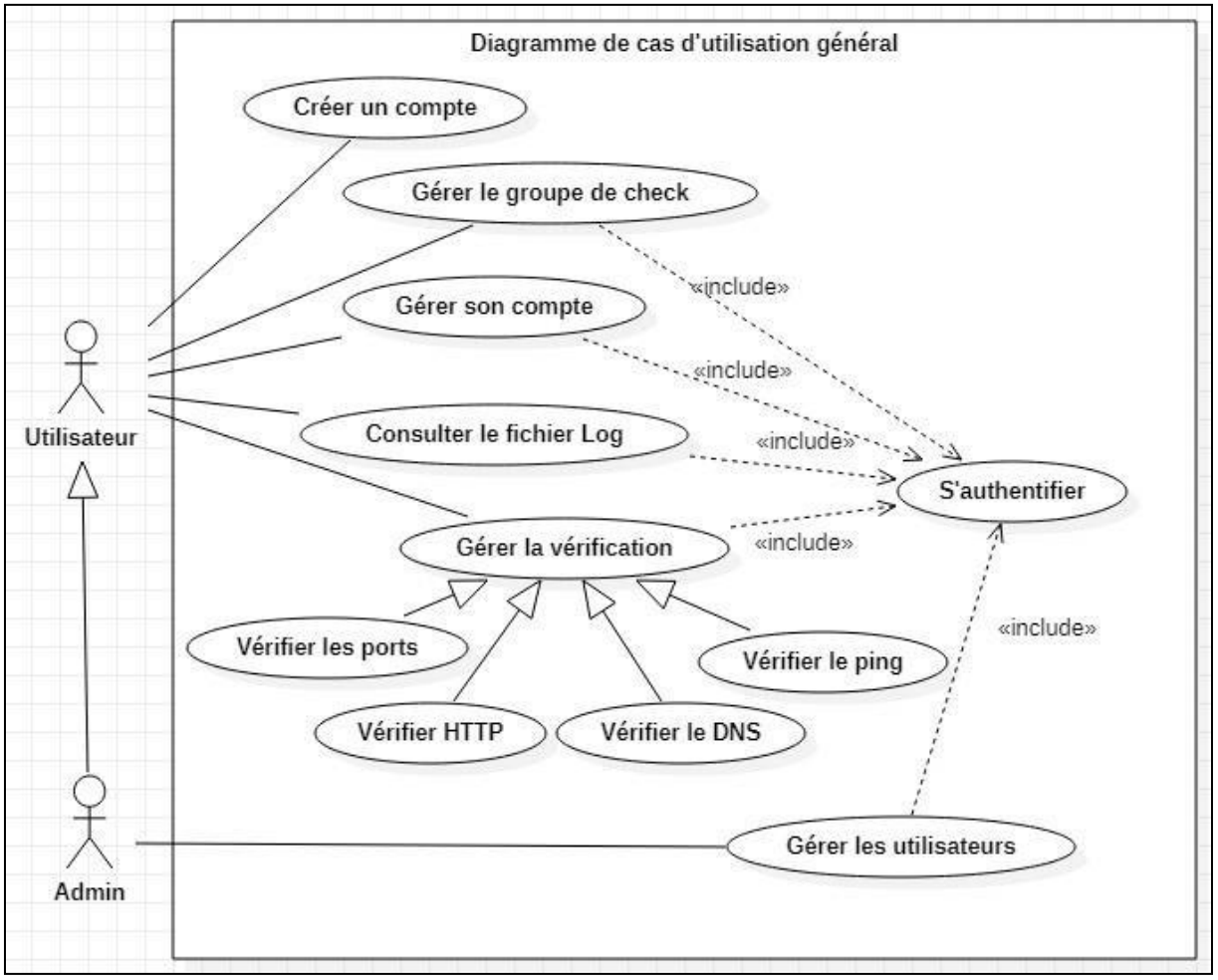

Figure 11 : Cas d'utilisation « général»

Cas d'Utilisation	Détails
Créer un compte	**Acteur :** Utilisateur.
	Description : Un utilisateur décide de créer un compte pour accéder à l'application.
	Scénario nominal : **1.** un utilisateur décide de s'enregistrer dans le système et accède au panneau d'enregistrement. **2.** L'utilisateur saisit son nom d'utilisateur, son adresse électronique et son mot de passe. **3.** Le système vérifie que les données saisies sont correctes. Le système ouvre une session pour l'utilisateur.
	Scénario alternatif : **3.1)** Certaines des données saisies sont incomplètes ou incorrectes. Le système informe l'utilisateur de l'erreur.

	3.2) Le nom d'utilisateur ou l'adresse électronique a déjà été utilisé par un autre utilisateur. Le système informe l'utilisateur de l'erreur.
Modification d'un groupe de check	**Acteurs :** Utilisateur.
	Description : L'internaute qui possède déjà un compte veut faire login dans l'application.
	Scénarios nominal : **1.** Un utilisateur décide de se connecter au système. **2.** L'utilisateur accède au panneau de connexion et entre son nom d'utilisateur et le mot de passe. **3.** Le système vérifie que les données saisies sont correctes. L'utilisateur se connecte à l'application.
	Scénarios alternatif : **2.1)** Certaines des données saisies ne sont pas au bon format ou non rempli. Le système informe l'utilisateur de l'erreur. **2.2)** Les données saisies ne correspondent à aucun utilisateur enregistré. Le système informe l'utilisateur de l'erreur.

Tableau 16: Description textuelle de cas d'utilisation général

3.1.3 Gérer groupe de check

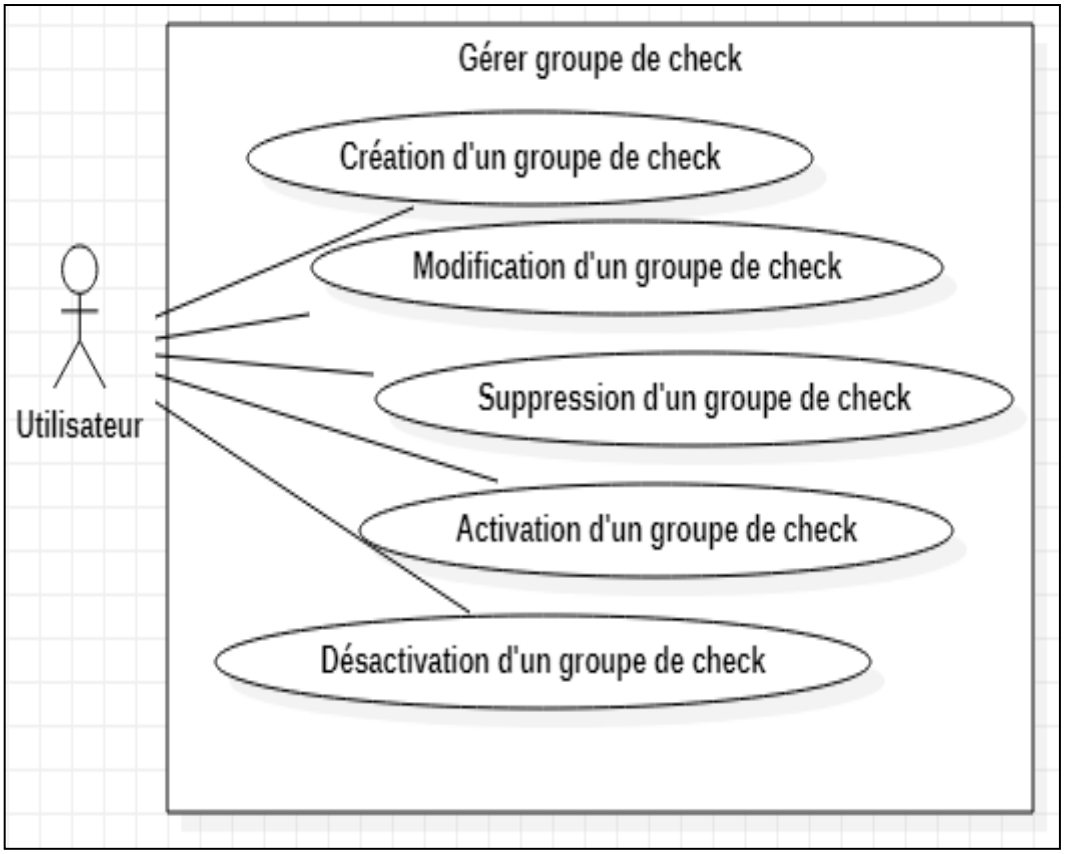

Figure 12 : Cas d'utilisation « Gérer groupe de check »

Cas d'Utilisation	Détails
Création d'un groupe de check	**Acteur :** Utilisateur.
	Description : Un utilisateur décide de créer un groupe de check.
	Scénario nominal : 1. L'utilisateur clique sur le bouton « add groupe ». 2. Le système affiche le formulaire pour ajouter un nouveau groupe. 3. L'utilisateur tape le titre de groupe. 4. Le système valide le titre. 5. Le système crée le nouveau groupe.
	Scénario alternatif : **4.1)** Le titre saisi est vide ou existe déjà. Le système informe le utilisateur de l'erreur.
Modification d'un groupe de check	**Acteurs :** Utilisateur.
	Description : Un utilisateur décide de modifier un groupe de check
	Scénarios nominal : **1.** L'utilisateur clique sur le bouton « Actions » puis « Edit »dans le groupe qu'il veut modifier. **2.** Le système affiche le formulaire pour modifier le groupe. **3.** L'utilisateur modifie le titre du groupe ensuite clique sur le bouton « Edit group ». **4.** Le système valide le titre saisi. **5.** Le système met à jour les données du groupe
	Scénarios alternatif : **4.1)** le titre est vide ou existe déjà. Le système informe l'utilisateur de l'erreur.
Suppression d'un groupe de check	**Acteur :** Utilisateur.
	Description : Un utilisateur décide de supprimer un groupe de check.
	Scénarios nominal : 1. L'utilisateur décide de supprimer un groupe. 2. L'utilisateur appuie sur le bouton « Actions » puis « Delete ». 3. Le système affiche le formulaire de confirmation de suppression. 4. L'utilisateur confirme la suppression. 5. Le système supprime les vérifications du groupe. 6. Le système supprime le groupe.
	Scénarios alternatif : **3.1)** Si l'utilisateur ne confirme pas la suppression. Le système revient à l'écran d'accueil.
Activation	**Acteur :** Utilisateur

d'un groupe de check	**Description :** Un utilisateur décide d'activer un groupe de check.
	Scénarios nominal : **1.** L'utilisateur appuie sur le bouton « Enable all checks ». **2.** Le système active toute les vérifications du ce groupe de check. **3.** Le système informe l'utilisateur que toutes les vérifications ont été activées.
Désactivation d'un groupe de check	**Acteur :** Utilisateur
	Description : L'utilisateur décide de désactiver un groupe de check.
	Scénarios nominal : **4.** L'utilisateur appuie sur le bouton « Disable all checks ». **5.** Le système désactive toute les vérifications du ce groupe de check. **6.** Le système informe l'utilisateur que toutes les vérifications ont été désactivées.

Tableau 17: Description textuelle de gérer groupe de check

3.1.4 Gérer les vérifications

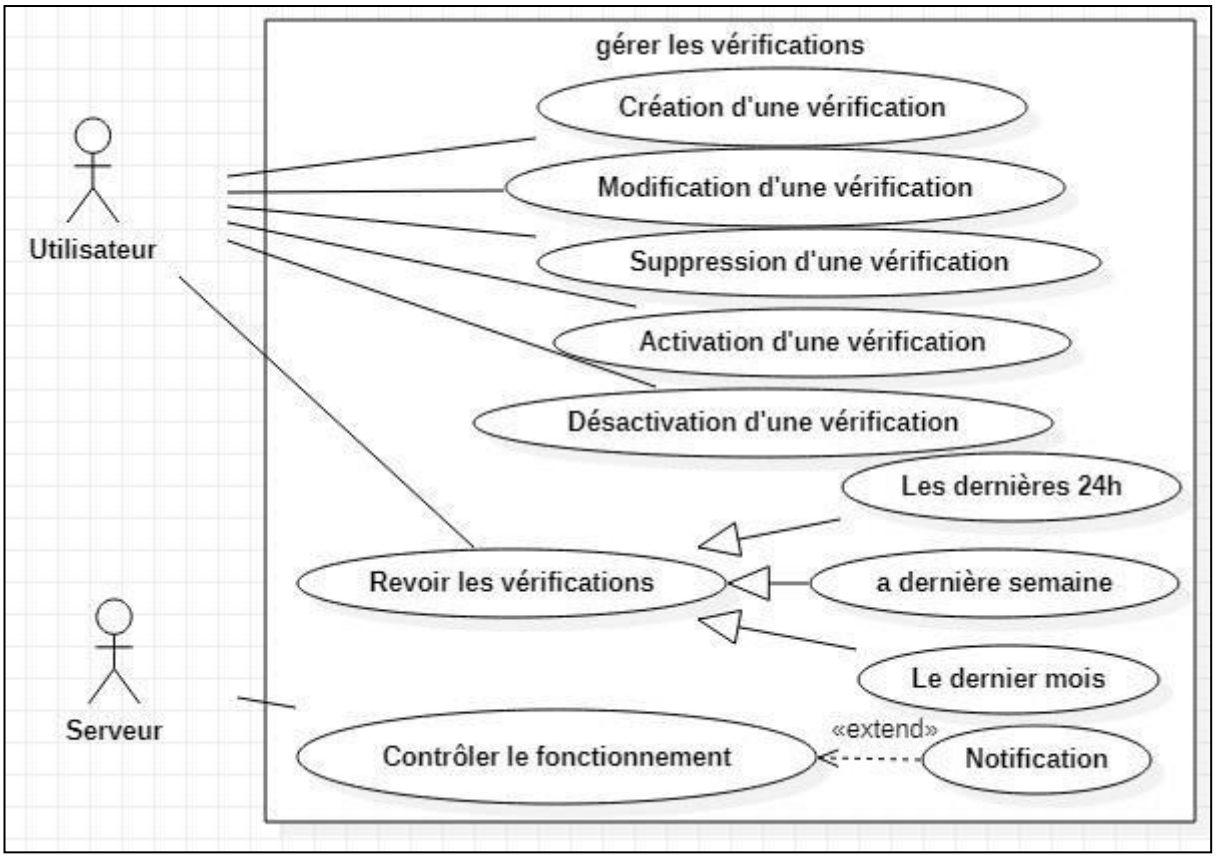

Figure 13 : Cas d'utilisation « Gérer les vérifications »

Cas d'Utilisation	**Détails**
Création d'une vérification	**Acteur :** Utilisateur.
	Description : Un utilisateur décide de créer une vérification au sein d'un groupe.
	Scénario nominal : 1. L'utilisateur clique sur le bouton "Add check" d'un groupe. 2. Le système affiche le formulaire pour choisir le type de vérification. 3. L'utilisateur choisit le type de vérification à ajouter. 4. Le système affiche le formulaire avec les champs correspondant au type de contrôle choisi. 5. L'utilisateur saisit les détails de la vérification et transmet le formulaire. 6. Le système reçoit et vérifie que les données sont correctes. 7. Le système enregistre la nouvelle vérification.
	Scénario alternatif : **5.1)** Si quelques données saisies ne sont pas correctes. Le système informe l'utilisateur de l'erreur et affiche à nouveau le formulaire.
Modification d'une vérification	**Acteurs :** Utilisateur.
	Description : Un utilisateur décide de modifier une vérification au sein d'un groupe.
	Scénarios nominal : **1.** L'utilisateur clique sur le bouton "Edit" d'un groupe. **2.** Le système affiche le formulaire pour modifier la vérification. **3.** L'utilisateur modifier les champs de la vérification ensuite clique sur le bouton « Update check ». **4.** Le système enregistre les modifications et affiche le tableau de bord après les modifications.
	Scénarios alternatif : **3.1)** l'utilisateur clique sur le bouton « Go back ». le système revient au tableau de bord.
Suppression d'une vérification	**Acteur :** Utilisateur.
	Description : Un utilisateur décide de supprimer une vérification précédemment créé
	Scénarios nominal : **1.** L'utilisateur décide de supprimer une vérification dans un groupe. **2.** L'utilisateur appuie sur le bouton « Delete ». **3.** Le système affiche le formulaire de confirmation de suppression. **4.** L'utilisateur confirme la suppression. **5.** Le système supprime la vérification.

	Scénarios alternatif : 3.2) Si l'utilisateur ne confirme pas la suppression. Lesystème revient à l'écran d'accueil.
Activation d'une vérification	**Acteur :** Utilisateur
	Description : Un utilisateur décide d'activer une vérification.
	Scénarios nominal : **1.** L'utilisateur appuie sur le bouton « Enable ». **2.** Le système active la vérification.
Contrôler le fonctionnement	**Acteur :** Serveur
	Description : Le serveur doit lancer un contrôle périodique.
	Scénarios nominal : **1.** Le serveur demande les vérifications actives. **2.** Le système renvoie les vérifications actives. **3.** Le serveur choisit une vérification active. **4.** Le serveur exécute la vérification. **5.** Le système renvoie le résultat du contrôle. **6.** Le serveur vérifie le résultat de la vérification, l'enregistre dans la base de données et, s'il diffère de l'état précédent de la vérification, déclenche la notification de l'état de la vérification.
	Scénarios alternatif : **2.1)** S'il n'y a pas de vérification active. Le système renvoie une liste vide.
Notification	**Acteur** : Serveur
	Description : Le serveur détecte un changement d'état et déclenche une notification.
	Scénarios nominal : **1.** Le serveur détecte un changement d'état d'une vérification. **2.** Le serveur vérifie le champ « Notify_mail »de lavérification. **3.** Le serveur déclenche une notification par mail. **4.** Le système envoie la notification à l'utilisateur qui possède la vérification.
	Scénarios alternatif : **2.1)** L'option « Notify_mail » n'est pas active pour la vérification. Le serveur n'envoie pas la notification.

Tableau 18: Description textuelle de gérer les vérifications

3.2 Diagramme de séquence

3.2.1 Inscription :

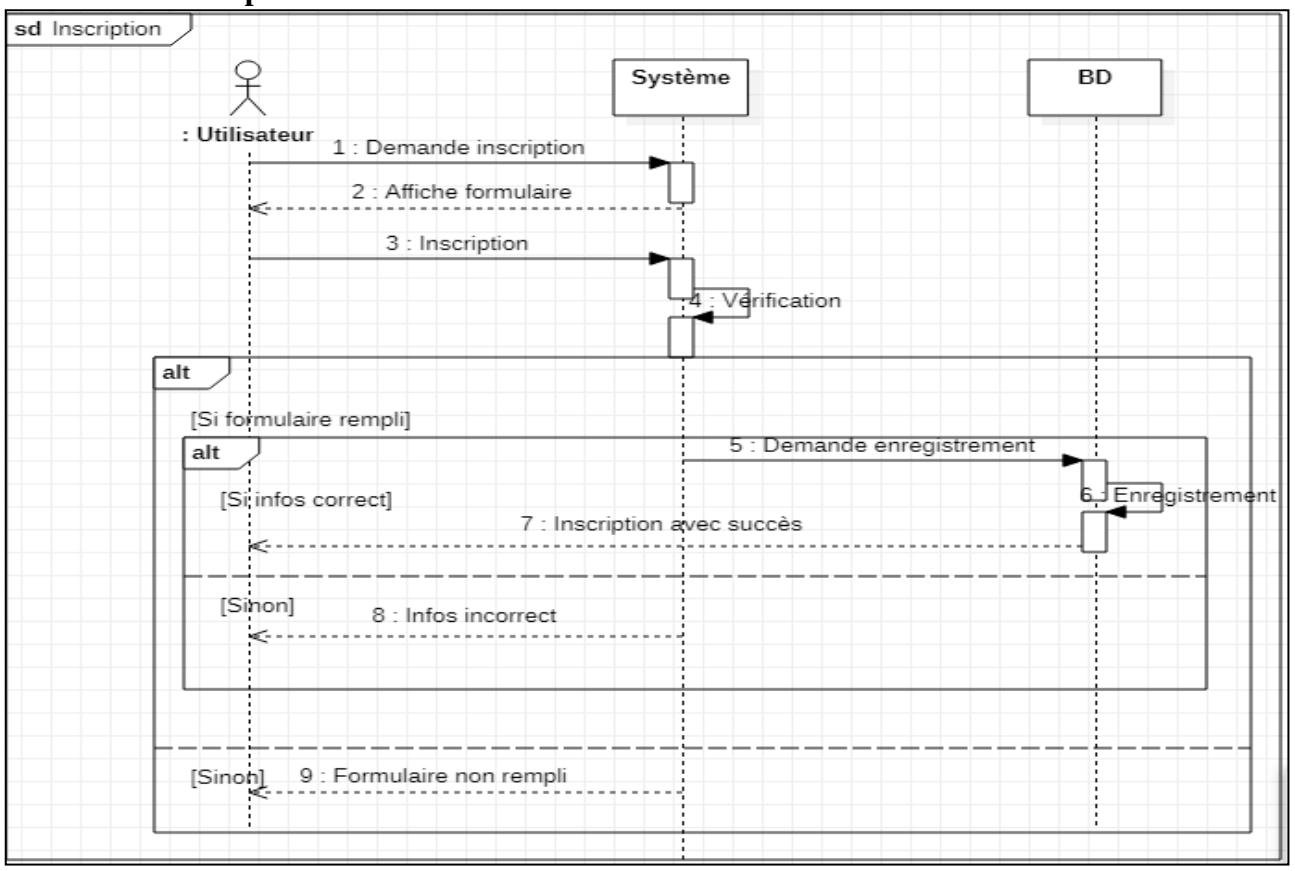

Figure 14 : Diagramme de séquence « inscription »

Acteur	Utilisateur
Description	utilisateur non connecté s'inscrit dans l'application pour pouvoir la gérer.
Scénario nominal	**1.** Un utilisateur décide de s'inscrire dans le système et d'accéder au formulaire d'inscription. **2.** L'utilisateur saisit son nom d'utilisateur, son adresse e-mail et mot de passe. **3.** Le système vérifie que les données saisies sont correctes. **4.** Le système enregistre l'utilisateur.
Scénario alternatif	**2.1)** Certaines des données saisies sont incomplètes ouincorrectes. Le système informel'utilisateur de l'erreur. **2.2)** Le nom d'utilisateur ou l'adresse e-mail a déjà été utilisé par un autre utilisateur précédemment. Le système informe l'utilisateur de l'erreur

Tableau 19: Description textuelle d'inscription

3.2.2 Authentification

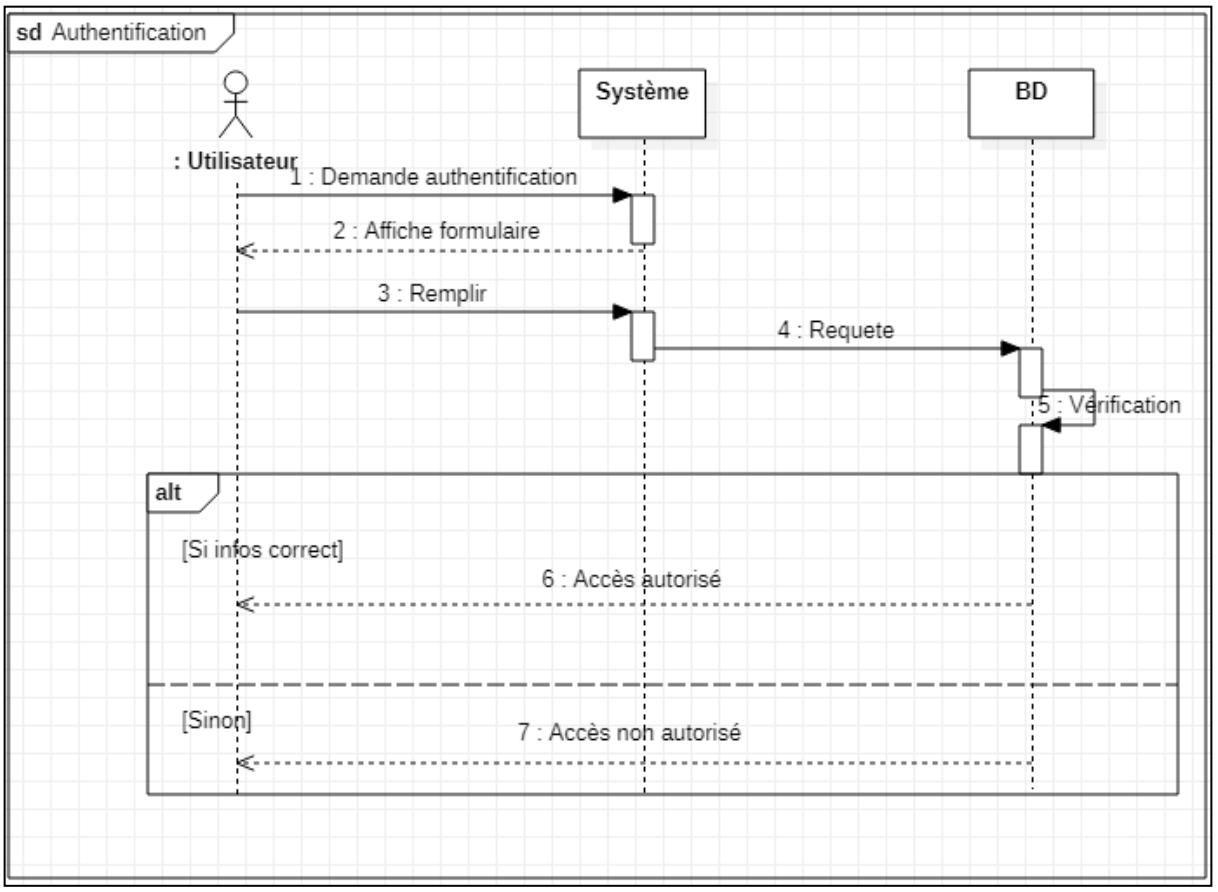

Figure 15 : Diagramme de séquence « inscription »

3.2.3 Modification de profil

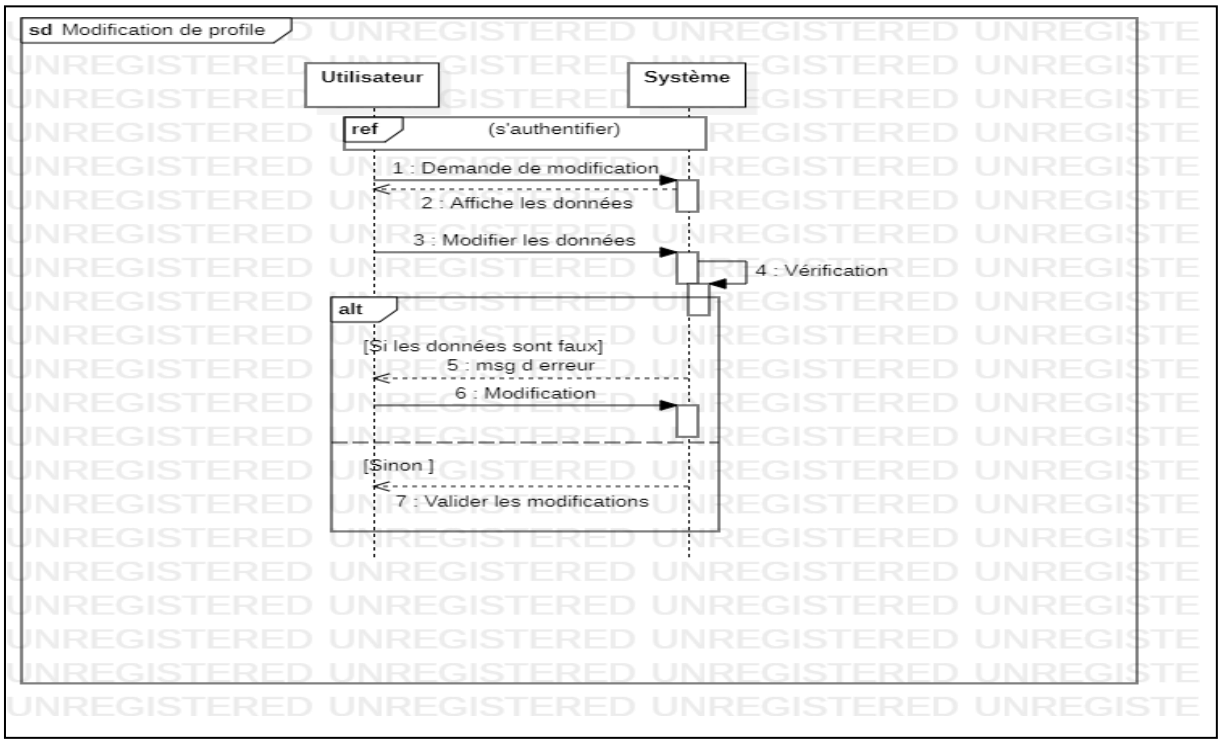

Figure 16 :Diagramme de séquence « modification de profil »

Acteur	Utilisateur
Description	Un utilisateur connecté décide de modifier certaines de ses données personnelles.
Scénario nominal	**1.** L'utilisateur accède à son profil d'utilisateur via le lien your profil. **2.** Le système affiche les données actuelles. **3.** L'utilisateur modifier les données qu'il souhaite et soumet le formulaire. **4.** Le système vérifie les nouvelles données et enregistre les modifications.
Scénario alternatif	**4.1)** Certaines des nouvelles données ne sont pas valides. Le système signale l'erreur à l'utilisateur

Tableau 20: Description textuelle de modification de profil

3.2.4 La création d'un groupe de check

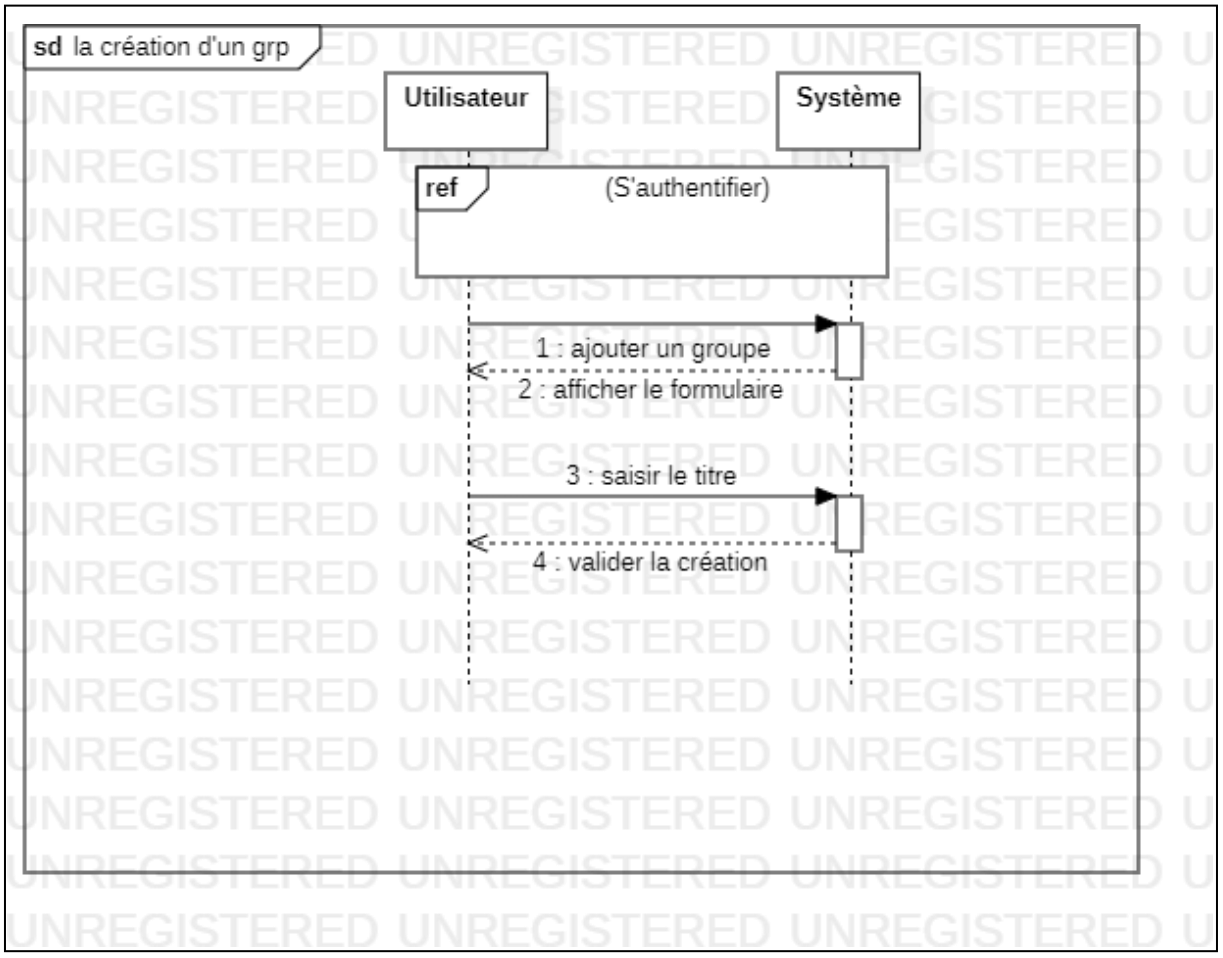

Figure 17 : Diagramme de séquence « création de groupe »

3.3 Diagramme de classe

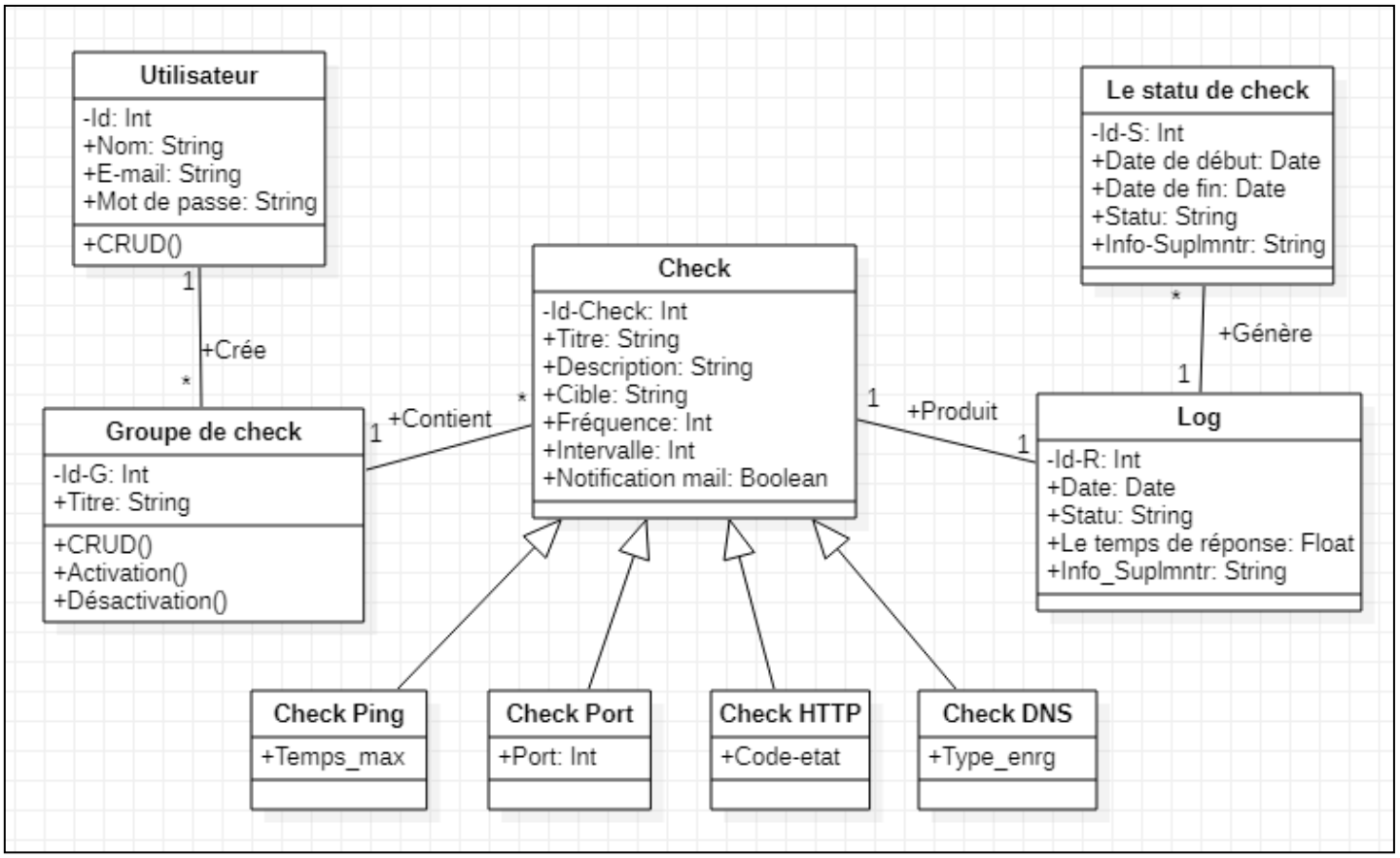

Figure 18 :Diagramme de classe

3.4 Diagramme de navigation

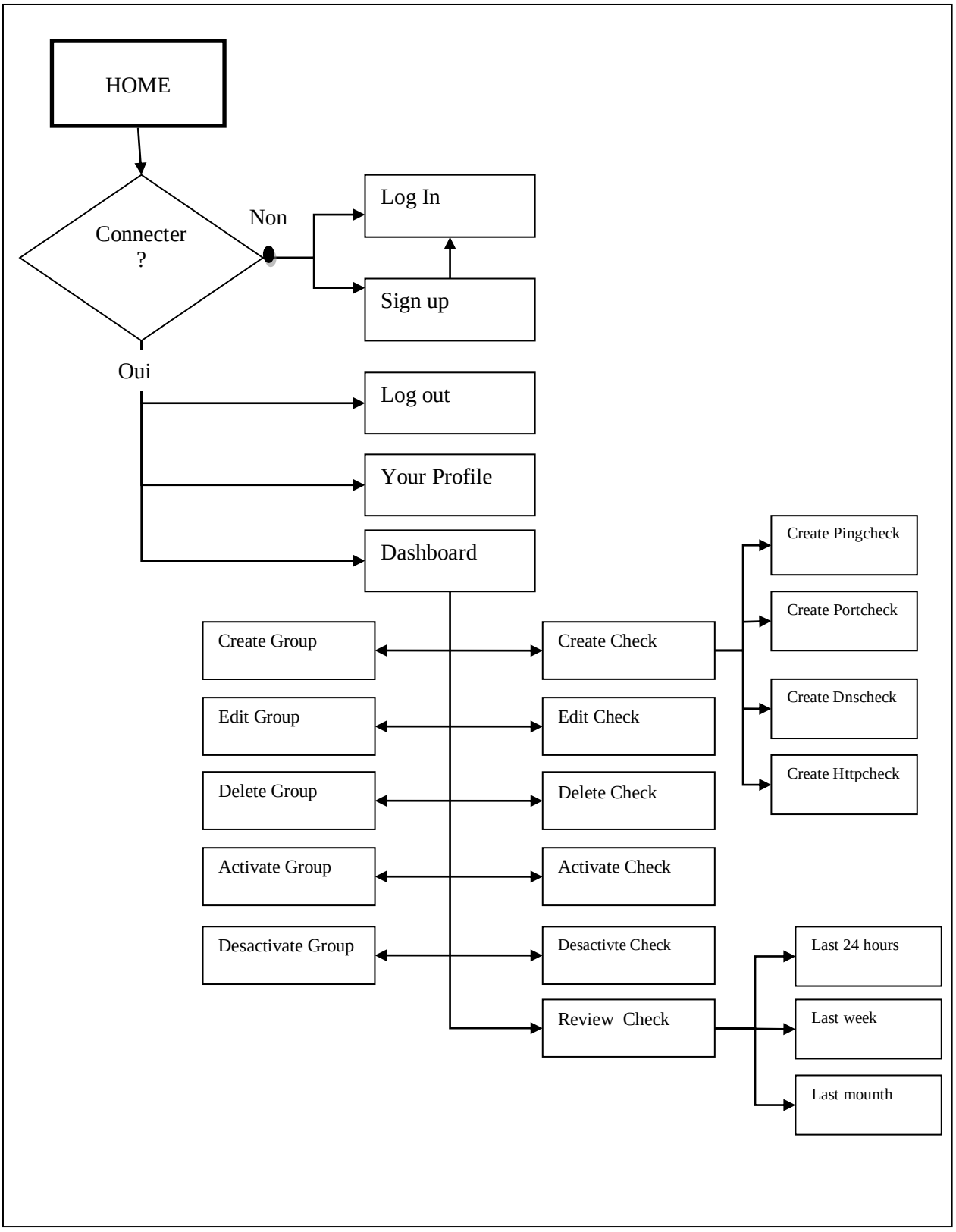

Figure 19 : Diagramme de navigation

Conclusion :

Dans ce chapitre on a présenté le coté conceptuel de notre application, et les différents besoins fonctionnelles de l'organisation, avec plusieurs diagrammes qui explique sa structure pour faciliter la réalisation de l'application.

Dans le chapitre suivant, nous présenterons la mise en œuvre de notre application.

Chapitre IV : Mise en Place la Solution

Introduction

Après tout ce qui a été dit dans les chapitres précédents, et toutes les notions théoriques présentées, passons maintenant à l'étape d'implémentation et réalisation de notre travail.

Dans ce chapitre nous parlerons d'environnement de travail, du langage et outils de développement utilisés.

1 Environnement de travail

L'environnement de travail est constitué par deux parties : matériel et logiciel.

1.1 Environnement matériel

Notre environnement matériel est caractérisé par :

Processeur	Intel(R) Core(TM) i7-3612QM CPU @ 2.10GHz 2.10 GHz
Mémoire RAM	8,00 GO
Système d'exploitation	Linux

Tableau 21: Les caractéristiques techniques d'environnement matériel

1.2 Environnement logiciel

Notre environnement logiciel est constitué par :

1.2.1 Logiciel utilisé

- **StarUML**

  StarUML est un outil de modélisation de logiciels open source qui prennent en charge le cadre UML (Unified Modeling Language) pour la modélisation de systèmes et de logiciels. Il est basé sur UML version 1.4, fournit 11 types de diagrammes différents et accepte la notation UML 2.0. Il prend activement en charge l'approche MDA (Model Driven Architecture) en prenant en charge le concept de fichiers de configuration UML et en permettant la génération de code pour plusieurs langues. [23]

Langage de modélisation

- **UML :**

  Abréviation de Unified Modeling Language (langage de modélisation unifié), est un langage de modélisation standardisé composé d'un ensemble intégré de diagrammes, développé pour aider les développeurs de systèmes et de logiciels à spécifier, visualiser, construire et documenter les artefacts des systèmes

logiciels, ainsi que pour la modélisation d'entreprise et d'autres systèmes non logiciels. L'UML représente un ensemble de bonnes pratiques d'ingénierie qui ont fait leurs preuves dans la modélisation de systèmes importants et complexes. L'UML est une partie très importante du développement de logiciels orientés objet et du processus de développement logiciel. L'UML utilise principalement des notations graphiques pour exprimer la conception de projets logiciels. [24]

1.2.2 Framework

- **Django :**
  Est un Framework web Python de haut niveau qui permet le développement rapide et une conception propre et pragmatique. Conçu par des développeurs expérimentés, Django se charge d'une grande partie des taches liées au développement Web, ce qui vous permet de vous concentrer sur l'écriture de votre application sans avoir à réinventer la roue. [25]

1.2.3 Langages de développement

- **Python :**
  Python est un langage de programmation interprété, orienté objet, de haut niveau et doté d'une sémantique dynamique. Ses structures de données intégrées de haut niveau, combinées au typage dynamique et à la liaison dynamique, le rendent très attrayant pour le développement rapide d'applications. La syntaxe simple et facile à apprendre de Python privilégie la lisibilité et réduit donc le coût de la maintenance des programmes. [26]
- **SQLite :**
  C'est une bibliothèque écrite en C qui implémente un moteur de base de données SQL transactionnel autonome, sans serveur, sans configuration. Le code de SQLite est dans le domaine public et est donc libre d'utilisation à toutes fins, commerciales ou privées. SQLite est la base de données la plus largement déployée dans le monde, avec plus d'applications que nous ne pouvons en compter, y compris plusieurs projets de haut niveau. [27]
  La décision a été prise d'utiliser SQLite car il s'agit de l'option par défaut utilisée par Django. De plus les données sont stockées dans un fichier, on peut donc déplacer le système d'un serveur à un autre.
- **JavaScript :**
  JavaScript est un langage de programmation qui permet d'implémenter des mécanismes complexes sur des pages Web. Lorsque la page Web affiche non seulement du contenu statique,

elle affiche également du contenu mis à jour, des cartes interactives, des animations 2D/3D et des menus vidéo défilants à l'heure définie. [26]

1.2.4 Environnement de développement

- **Pycharm :**
  Est un environnement de développement le plus populaire pour Python, et il est doté d'excellentes fonctionnalités telles que la complétion et l'inspection du code, un débogueur avancé, et la prise en charge de la programmation web et de Framework tels que Django et Flask. [28]

1.2.5 Bibliothèques :

- **jQuery** :
  C'est une bibliothèque JavaScript rapide, petite et riche en fonctionnalités. Cela simplifie considérablement la navigation et la manipulation de documents HTML, la gestion des événements, l'animation et Ajax avec une API facile à utiliser qui fonctionne sur une multitude de navigateurs. [29]
- **South :**
  C'est une bibliothèque de migrations de bases de données intelligentes pour le Framework Web Django. Il est indépendant des bases de données et compatible DVCS, ainsi que de nombreuses autres fonctionnalités. [30]

1.2.6 Les outils :

- **Virtualenv :**

  C'est un outil pour créer des environnements Python isolés. Il crée un environnement qui a ses propres répertoires d'installation, qui ne partage pas de bibliothèques avec d'autres environnements virtualenv (et n'accède éventuellement pas non plus aux bibliothèques installées globalement). [31]

- **Supervisor** :
  C'est un système client/serveur qui permet à ses utilisateurs de surveiller et de contrôler un certain nombre de processus sur des systèmes d'exploitation de type UNIX. [32]
- **RabbitMQ** :
  Est une solution de messagerie orientée message, ou solution Middleware orienté message (MOM). Le middleware est un logiciel tiers utilisé pour créer un réseau d'échange d'informations entre les applications. La technologie d'échange d'informations utilisée par RabbitMQ est l'échange de messages. Le terme MQ

(Message Queuing) qui apparaît dans RabbitMQ met l'accent sur cette technologie et les principales caractéristiques du produit. Il représente la connexion d'applications par le biais de messages routés grâce à un broker. On peut comparer le broker à La Poste, c'est-à-dire qu'il reçoit un message d'une application et le délivre à une autre.

RabbitMQ propose :

- Un broker, appelé aussi serveur de messagerie.
- Des API client, permettant de communiquer avec le broker. [33]

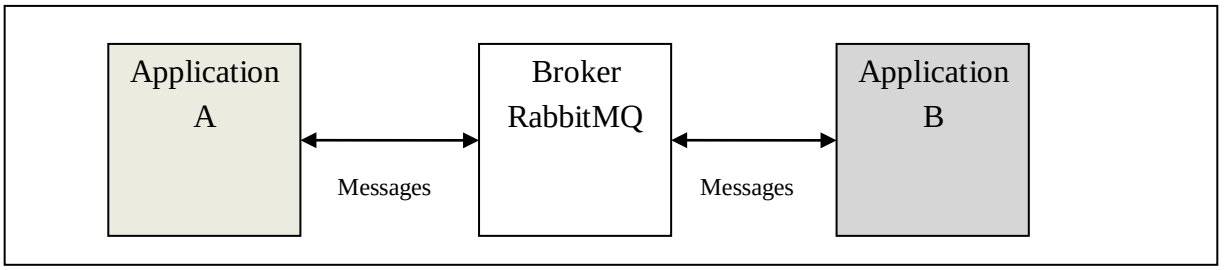

Figure 20 : La connexion d'application grâce à un Broker

- **Celery** :

  C'est un système distribué simple, flexible et fiable pour traiter de grandes quantités de messages, tout en fournissant aux opérations les outils nécessaires pour maintenir un tel système.

  Il s'agit d'une file d'attente de tâches axée sur le traitement en temps réel, tout en prenant en charge la planification des tâches. [34]

2 Sécurité de l'application

2.1 Fichier LOG :

La journalisation (logging en anglais) est une façon de suivre les événements qui ont lieu durant le fonctionnement d'un logiciel. Le développeur du logiciel ajoute des appels à l'outil de journalisation dans son code pour indiquer que certains événements ont eu lieu. Un événement est décrit par un message descriptif, qui peut éventuellement contenir des données variables (c'est-à-dire qui peuvent être différentes pour chaque occurrence de l'événement). Un événement a aussi une importance que le développeur lui attribue ; cette importance peut aussi être appelée niveau ou sévérité. [36]

Niveau	Quand il est utilisé
DEBUG	Information détaillée, intéressante seulement lorsqu'on diagnostique un problème.
INFO	Confirmation que tout fonctionne comme prévu.
ERROR	Du fait d'un problème plus sérieux, le logiciel n'a pas été capable de réaliser une tâche.

Tableau 22: Les niveaux de log

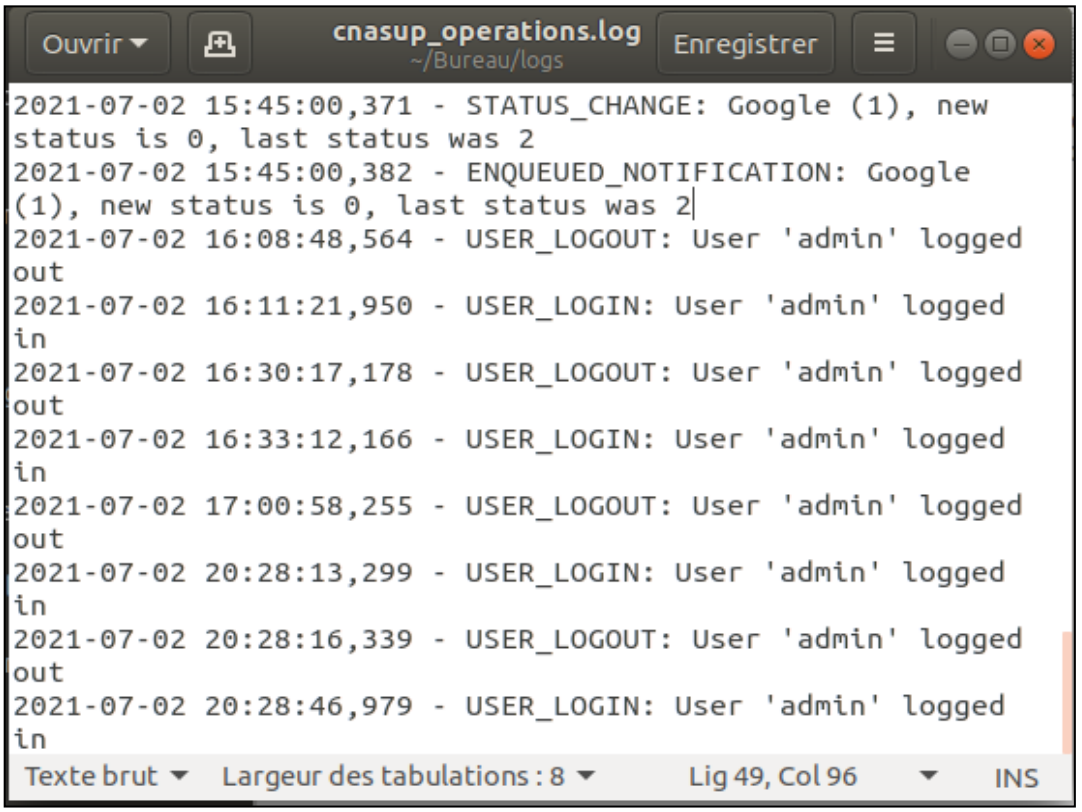

Figure 21 : Aperçu de fichier LOG de notre application

2.2 Sha-256 :

Le Sha-256 est une fonction de l'algorithme Sha-2 c'est un algorithme de "hashage" crée par la NSA pour répondre au problème de sécurité posé par le Sha-1. L'algorithme accepte en entrée un message de longueur maximum 2^64 bits et produit un hash. Ce dernier propose un bon équilibre entre espace de stockage en ligne et sécurité. Comme les autres fonctions cryptographiques de sa famille, Sha-256 est unilatéral et on ne peut retrouver le message originel avec le seul hash sha256. Il faut donc comparer ce hash sha256 à une base de données. Le Sha-256 est une bonne solution pour stocker des mots de passe, sa sécurité est bien plus importante que le Md5 ou le Sha-1. [37]

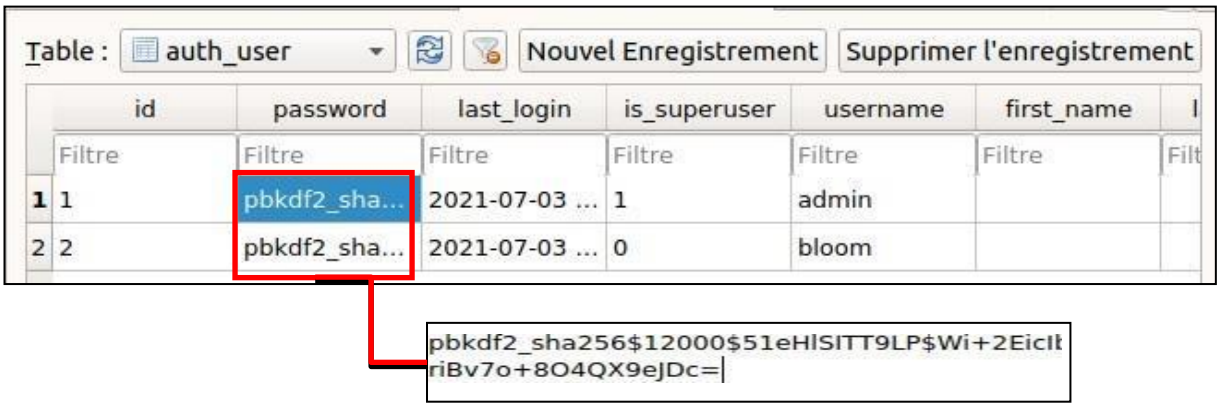

Figure 22 : Représentation des mots de passe cryptés dans notre base de données

3 Présentation de l'application

CnasUp s'agit d'une application web, sur laquelle les utilisateurs ont la possibilité de donner des contrôles élevés de divers types : envoi de pings, contrôle de port, contrôle de DNS et de Http. Ces contrôles sont exécutés par le système périodiquement et générer des notifications lorsque ils détectent les pannes, ces notifications sont envoyées par e-mail. Les utilisateurs ont la possibilité de voir les fichiers journaux obtenues lors d'un déroulement d'une tache précis.

3.1 Home

Si l'utilisateur n'est pas connecté, les options de navigation disponibles sont :

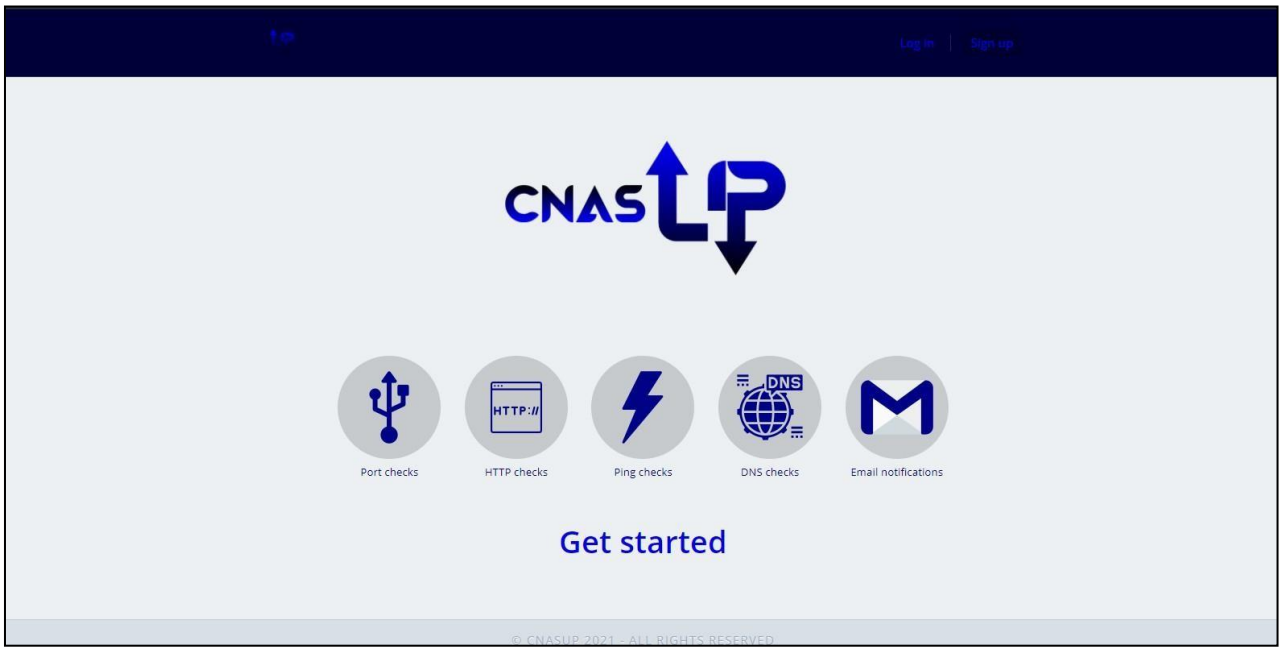

Figure 23 :Interface d'accueil

3.2 Inscription

Si l'utilisateur n'a pas de compte il doit s'inscrire pour y accéder

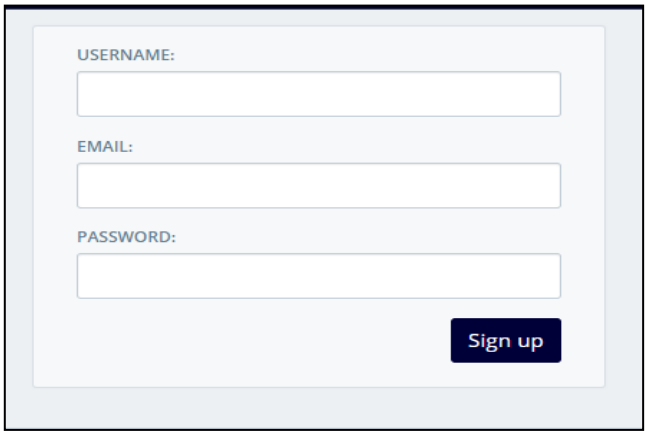

Figure 24 : Interface d'inscription

3.3 Connexion

Cette interface représente un formulaire dans lequel l'utilisateur doit saisir son nom d'utilisateur et son mot de passe, puis appuyez sur le bouton Log in, si les données saisies sont correct, le système se connectera et redirigera l'utilisateur vers la liste de contrôle ; sinon, le formulaire réapparaîtra avec les erreurs qui ont été produit.

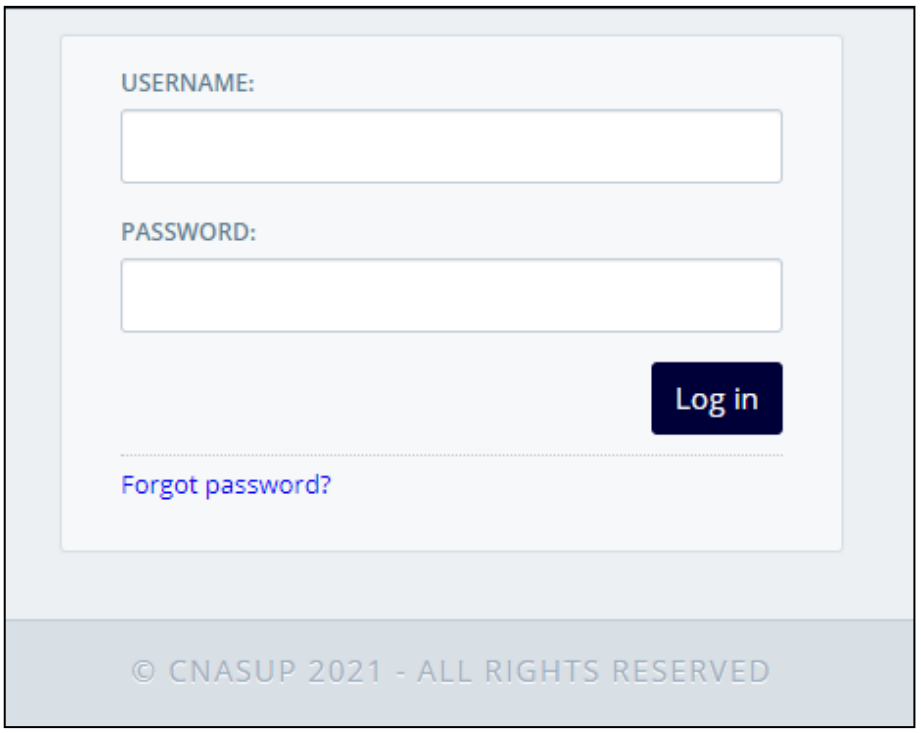

Figure 25 :Interface de connexion

3.4 Interface de récupération de mot de passe

Si l'utilisateur oublie son mot de passe il peut le récupérer après avoir rempli ce formulaire, si l'e-mail saisi est correct, le système enverra un e-mail.

Figure 26 : Interface de récupération de mot de passe

3.5 Tableau de bord

Cet écran montre les groupes de vérifications qui sont enregistré par un utilisateur, ainsi que les vérifications qui appartiennent à chaque groupe de check. Depuis cet écran on peut faire un grand nombre d'opérations :

- Appuyez sur le bouton Add group pour afficher l'écran de création de groupe.
- Lorsque vous cliquez sur le bouton Actions il est possible de :
  Ajouter un contrôle
  Modifier le nom de groupe
  Désactiver ou activer tous les vérifications de groupe
  Supprimer le groupe

Chacun des vérifications de chaque groupe contient le titre, la description, un graphe de son statut au cours des dernières 24 heures.

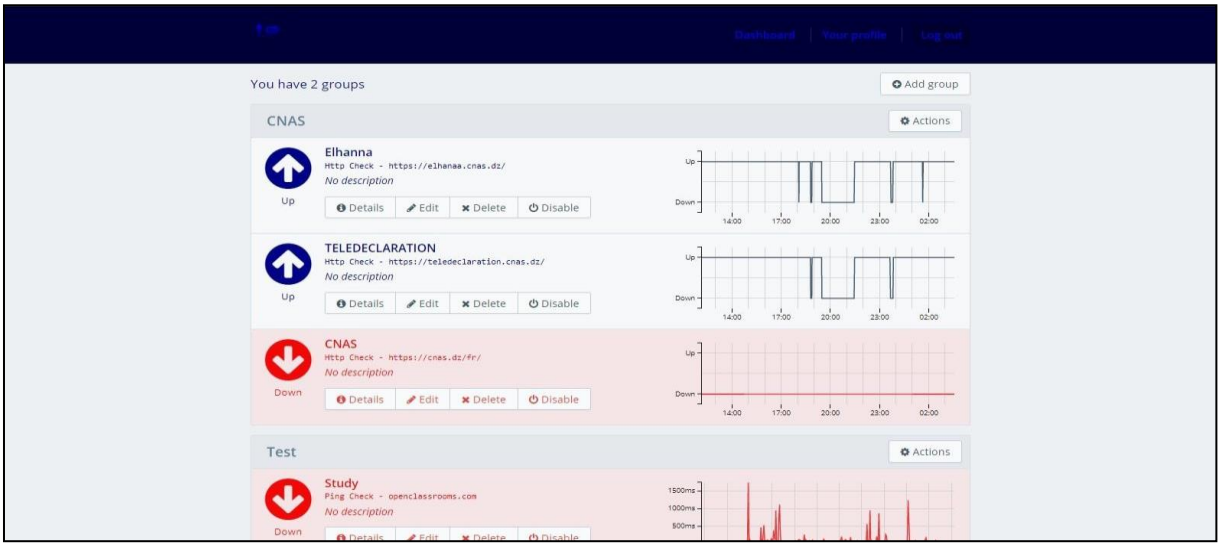

Figure 27 :Tableau de bord

3.6 Détails :

Cette interface permis de modifier ou supprimer ou désactiver un contrôle ainsi que d'afficher des informations et des événements qui se sont produits à différents intervalles de temps.

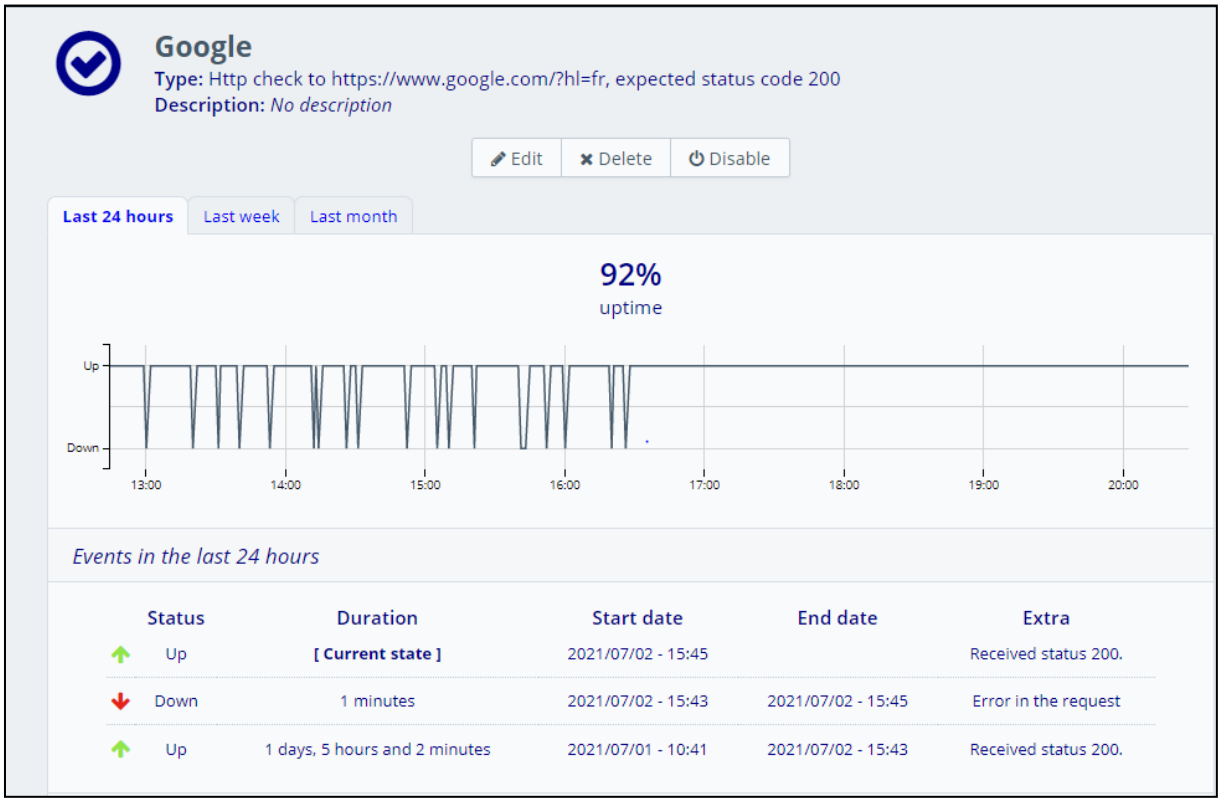

Figure 28 : Interface de détails d'un contrôle

3.7 Création de groupe de contrôle :

Cette interface représente la création d'un groupe de contrôle.

Figure 29 : Interface de création d'un groupe de contrôle

3.8 Liste de contrôle :

Cette liste est pour ajouter un type de vérification.

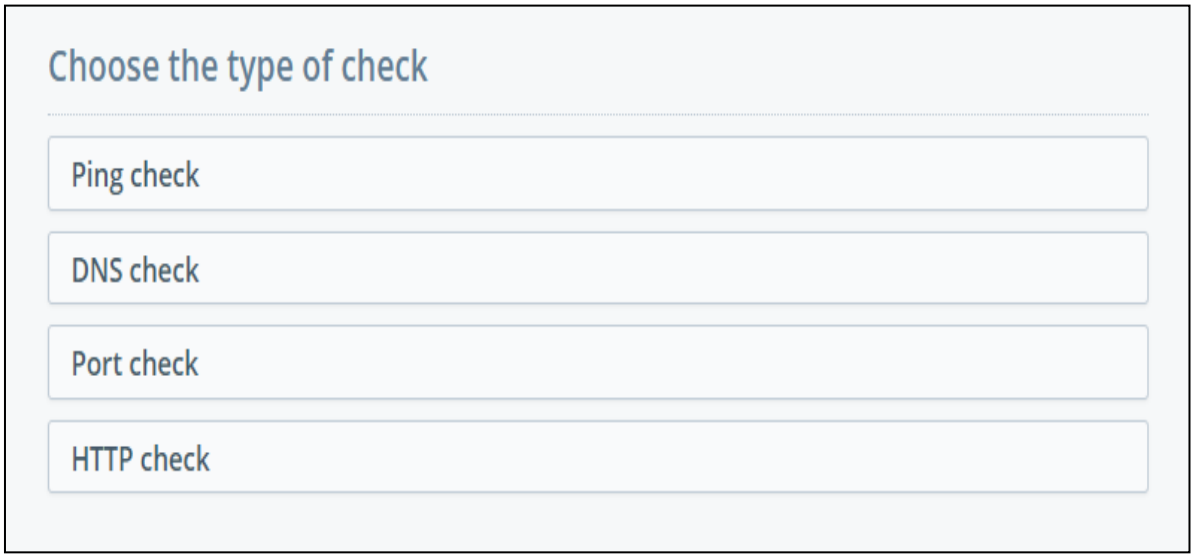

Figure 30 : Liste de type de contrôle

3.9 Profil utilisateur :

A partir de cet écran l'utilisateur peut modifier ses données : nom d'utilisateur, e-mail et si vous souhaitez recevoir un rapport quotidien sur l'état de vos vérifications.

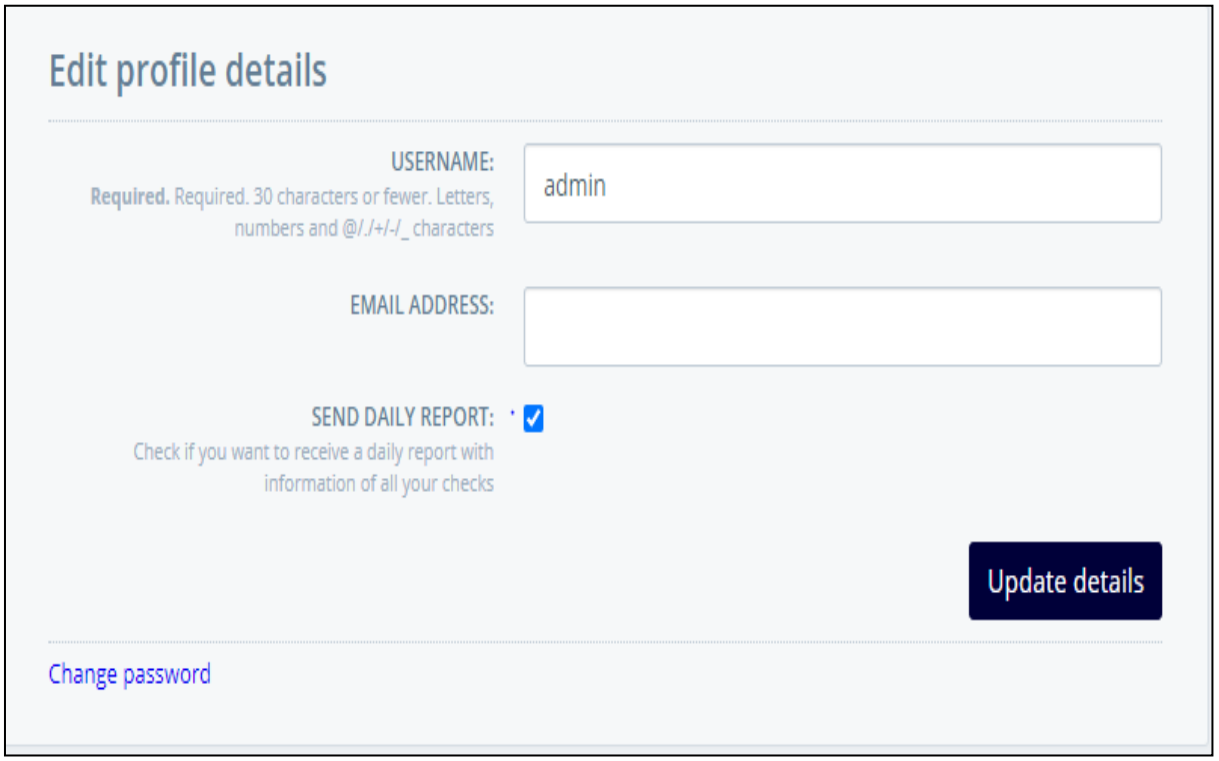

Figure 31 : Interface de la modification de profil

3.10 Notification par email :

Un rapport qui vous permet de connaitre l'état de vos groupes de vérifications.

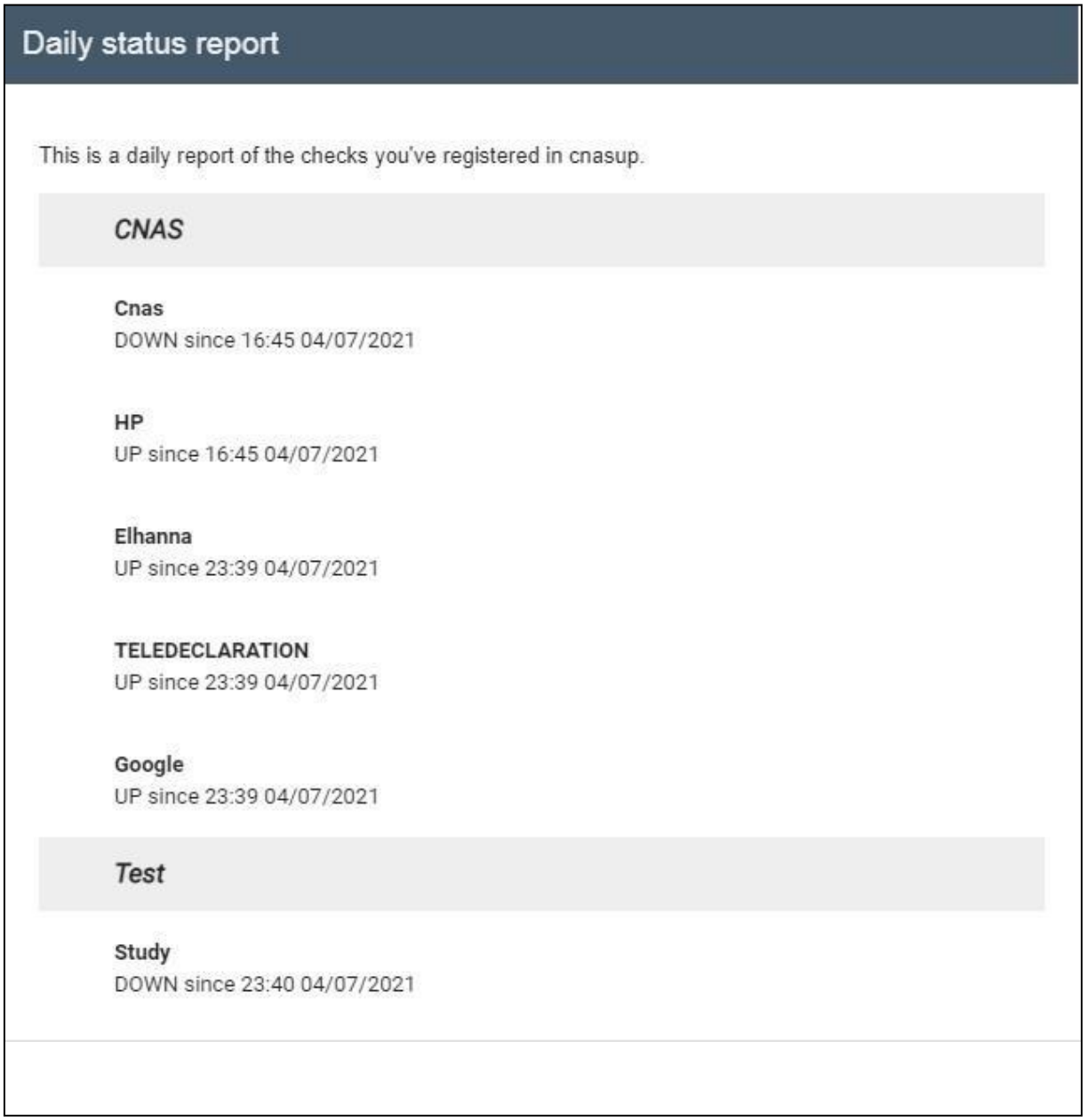

Figure 32 :Notification par mail

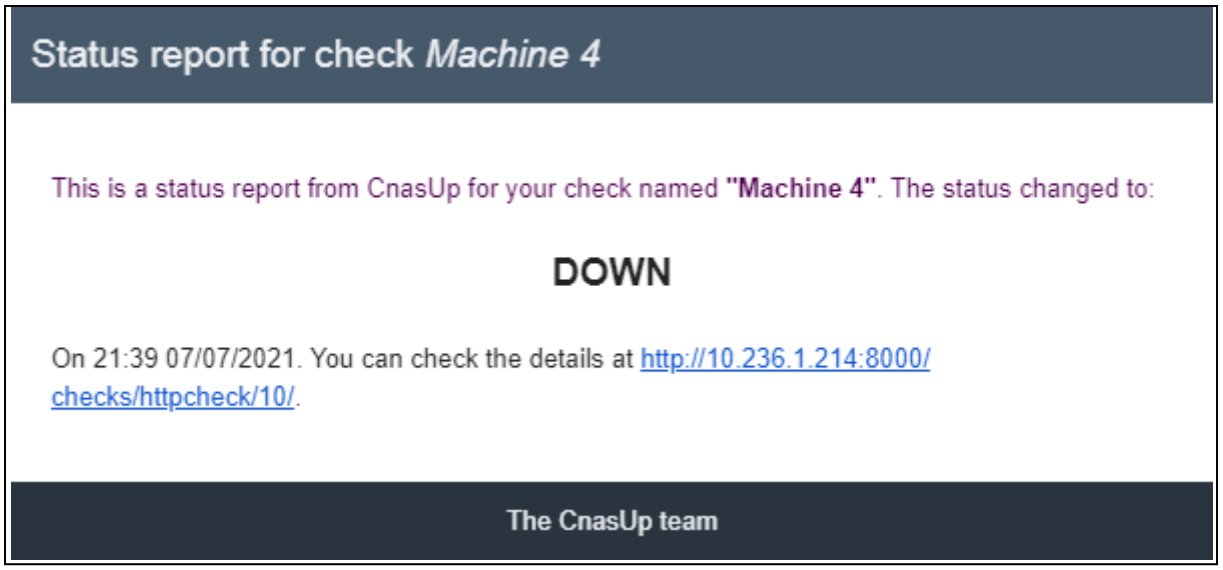

Figure 33 : Notification par mail détaillé

Conclusion

Dans ce chapitre nous avons présenté notre application avec ces différents fonctionnements et ces différentes interfaces, ainsi les outils utilisés pour la réaliser.

Conclusion Générale

N'importe quelle entreprise peut être confrontée à une catastrophe informatique, qui peut entrainer des conséquences grave comme la perte de données ou dégradation de la réputation de l'entreprise. A ce contexte, il nous a semblé important d'élaborer un plan de reprise d'activité afin de pouvoir prévenir le risque.

Dans ce travail, nous avons commencé par définir le plan de reprise d'activité, son objectif et son contenu. Nous avons aussi présenté les méthodes d'analyse de risque qui permettent d'évaluer et d'identifier les risques liés à la sécurisation de l'information au sein de l'entreprise. Ensuite nous avons implémenté le PRA de l'organisme d'accueil « CNAS ». Nous avons identifié et évaluer les risques en utilisant la méthode MEHARI, défini les activités critiques de l'entreprise et proposer les mesures. A la fin nous avons développé une solution de surveillance de services à distance. Pour la réalisation de cette phase nous avons d'abord fait une étude fonctionnelle pour fixer les différents services que le monitoring doit accomplir puis générer un diagramme de classe en utilisant l'UML.

Ce travail nous a permis d'avoir une idée sur les procédures de la réalisation des logiciels et de concevoir une bonne maitrise de langage Python et le Framework Django. Aussi, ce stage nous a permet de découvrir le monde du travail et d'appliquer nos connaissances acquises lors de notre formation à de vrai problématique d'entreprise.

Perspectives :

Notre travail sera enrichie par :

- L'ajout d'une application mobile qui reçoit des notifications avec informations sur les résultats des contrôles enregistrés dans le système pour faciliter la surveillance à distance.

Bibliographie

[1] E. Council, Disaster Recovery, Cengage Learning, 2010.

[2] S. Keith, «how to prepare a buiseness continuity plan,» 23 january 2017.

[3] S. Susan et R. Chris, Business Continuity and Disaster Recovery Planning fot IT Professionals Second Edition, Syngress, 2013.

[4] M. BENNACER, plan de continuité d'activité et système d'information 2e édition vers l'entreprise résiliente, Dunod, 2010.

[5] J. Montérémal, «Plan de reprise d'activité,» 03 mars 2021.

[6] Abdelmajid, «Plan de reprise d'activité PRA,» 29 Mars 2019. [En ligne]. Available: https://blog.advancia-itsystem.com/plan-de-reprise-d-activite-pra/. [Accès le 20 avril 2021].

[7] V. LUC et F. TETE, L'OBSERVATOIRE des Directeurs d'infrastructures et de production, CRIP, 2011.

[8] CLUSIF, «Plan de Continuité d'Activité --- Stratégie et Solitions de Secours du SI,» CLUSIF, 2003.

[9] G. Peter, CISA et CISSP, IT Disaster Recovery Planning, For Dummies, 2007.

[10] DCSSI, «Expression des Besoins et Identification des Objectifs de Sécurité,» 2010.

[11] ANSSI, «ALERTES,» 2018. [En ligne]. Available: http://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/. [Accès le 11 avril 2021].

[12] A. Christopher, D. Audrey, S. James et W. Carol, «Introduction to the OCTAVE Approach,» carnegie mellon university, 2003.

[13] «clusiq,» clusif, 2018. [En ligne]. Available: http://www.clusiq.ca/mehari/.

[14] CLUSIF, «MEHARI présentation générale,» CLUSIF, 2017.

[15] CLUSIF, «MEHARI principes fondamentaux et spécifications fonctionnelles,» CLUSIF, 11, rue Magador, 75009 PARIS, 2017.

[16] CLUSIF, «services,» [En ligne]. Available: https://clusif.fr/services/management-des-

risques/les-fondamentaux-de-mehari/. [Accès le 02 Avril 2021].

[17] SECRETARIAT GENERAL DU GOUVERNEMENT, «JOURNAL OFFICIEL DE LA REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE,» Les Vergers, Bir-Mourad Raïs, BP 376 ALGER-GARE, 2019.

[18] L. CNAS, «présentation de la CNAS,» juillet 2018. [En ligne]. Available: https://cnas.dz/fr/presentation-de-la-cnas/. [Accès le 11 avril 2021].

[19] CLUSIF, «Mehari Manager,» CLUSIF, 2013.

[20] U. Bhuvan, Software Engineering with UML, Auerbach, 2020.

[21] F. Martinig, «StarUML - Open Source UML Tool,» [En ligne]. Available: http://www.methodsandtools.com/tools/staruml.php. [Accès le 02 juillet 2021].

[22] «what is uml,» [En ligne]. Available: https://www.visual-paradigm.com/guide/uml-unified-modeling-language/what-is-uml/. [Accès le 15 juin 2021].

[23] «Django The web framework for perfectionists with deadlines,» [En ligne]. Available: https://www.djangoproject.com/. [Accès le 22 juin 2021].

[24] «What is Python? Executive Summary,» [En ligne]. Available: https://www.python.org/doc/essays/blurb/. [Accès le 15 mai 2021].

[25] «About SQLite,» [En ligne]. Available: https://www.sqlite.org/. [Accès le 03 juillet 2021].

[26] «Qu'est ce que le JavaScript ?,» [En ligne]. Available: https://developer.mozilla.org/. [Accès le 01 juin 2021].

[27] P. Kroger, Modern Python Development With Pycharm.

[28] «What is jQuery?,» [En ligne]. Available: https://jquery.com/. [Accès le 02 juin 2021].

[29] «South: Migration for Django,» [En ligne]. Available: https://pypi.org/. [Accès le 29 juin 2021].

[30] «Virualenv,» [En ligne]. Available: https://virtualenv.pypa.io/en/latest/. [Accès le 26 mai 2021].

[31] «Supervisor: A Process Control System,» [En ligne]. Available: http://supervisord.org/. [Accès le 01 juin 2021].

[32] «RabbitMQ - Solution Message-Oriented Middleware,» [En ligne]. Available: http://igm.univ-mlv.fr/.

[33] «Celery - Distributed Task Queue,» [En ligne]. Available: https://docs.celeryproject.org/en/stable/. [Accès le 15 juin 2021].

[34] «Tutoriel sur la journalisation,» [En ligne]. Available: https://docs.python.org/fr/. [Accès le 01 juin 2021].

[35] «Sha256() Encrypt & Decrypt,» [En ligne]. Available: https://md5decrypt.net/Sha256/. [Accès le 29 juin 2021].