**Coutaille BA**

**Ingénieur informaticien et Statisticien**

**Instructeur OACI Système ECCAIRS**

Dakar le 17 Septembre 2025

**RAPPORT DE MISSION**

**-\*-\*-\*-\*-**

**Assistante technique pour la mise à niveau du réseau informatique de l’ANAC**

Du 08 au 17 Avril 2025, nous avons séjourné à l’Agence Nationale de l’Aviation Civile de la Mauritanie pour une mise à niveau de leur plateforme informatique conformément aux standards en matière de système d’information.

L’objectif est pour le Directeur général de l’ANAC de s’inspirer du modèle de l’ANACIM pour bâtir un véritable système d’information sur et performant afin de permettre au personnel de gagner en performance et en productivité.

Notre mission s’est déroulée en trois étapes :

* Existant Système d’information à l’ANAC
* Diagnostic du réseau informatique et recommandations
* Architecture réseau cible
* Mise à niveau des serveurs de l’ANAC
* Projet de digitalisation des inspections.

1. **Existant système d’information à l’ANAC**

L’ANAC dispose de trois sites :

* un premier site qui abrite la Direction générale, la Direction administrative et financière et les conseillers techniques
* un second site qui abrite la Direction sûreté et facilitation et la Direction du transport aérien et ;
* un troisième site regroupant la direction sécurité des vols et la direction de la sécurité et de la navigation aérienne.

Les sites ne sont pas relies en réseau. Chaque site abrite son propre réseau

Le site abritant la Direction générale dispose de deux serveurs et un réseau client-serveur avec un câblage intelligent courant fort et courant faible. L’un des serveurs de la Direction générale abrite les applications SAGE Compta et paie.. Une ligne internet de l’opérateur Telecoms permet au personnel l’ANAC de se connecter à internet.

En termes d’équipements l’ANAC dispose des serveurs ci-dessous :

* Un serveur HP Proliant 350 G6 avec 8Go de RAM, Processeur Intel® Xeon de 2,40GHz et 1To de disque dur
* Un serveur HP Proliant 350 G6 comme serveur de production avec les applications Sage Compta et Paie ;
* Deux armoires 6U installes dans le Datacenter permettent de connecter les utilisateurs et les serveurs.
* Un onduleur 3KVA

1. **Diagnostic du réseau et recommandations**

Le diagnostic du réseau informatique de l’ANAC illustre le manque des services et équipements ci-dessous ;

1. Mise à niveau du Datacenter
2. Ressources humaines
3. Non existence d’une plateforme virtuelle
4. Absence de procédures de gestion de l’architecture informatique
5. Absence d’un système de sauvegarde et restauration non automatisé
6. Absence d’un équipement d’optimisation et de sécurisation du trafic applicatif
7. Absence de plan de reprise d’activités (PRA)
8. Absence de stratégie de cyber sécurité telle recommandée par l’OACI dans le doc 897.
9. **Mise à niveau du Datacenter**

L’ANAC dispose d’un Datacenter avec un onduleur de puissance 3KVA lié à un groupe électrogène et un réseau ondulé pour la protection des tous les équipements connectés au réseau.

La puissance de l’onduleur installé dans la salle serveur est insuffisante pour gérer les serveurs et équipements actifs. Il serait mieux d’acquérir un onduleur de puissance 20KVA pour gérer les serveurs et tous les équipements du réseau installes dans ce site.

Le Datacenter renferme les serveurs de production nécessaires au fonctionnement des activités de l’ANAC. Il est nécessaire de protéger la salle serveur en installant les services ci-dessous :

* Système sécurité incendie
* Système de détection de température, de fumée et d’humidité
* Système de caméra de surveillance
* Système d’accès biométrique

1. **Ressources humaines**

Les nouvelles technologies de l’information et de la communication jouent un rôle prépondérant dans le développement des entreprises notamment dans le domaine de l’aviation civile. Il est nécessaire pour l’ANAC de disposer d’un véritable système d’information avec un personnel suffisant et bien forme. Vu les activités dans la collecte de données, le traitement des demandes, la certification des aéroports et la délivrance de documents (licences du personnel aéronautiques, certificat de navigabilité, permis d’exploitation aérienne et autres) ainsi que les activités administratives et financières, L’ANAC gagnerait à disposer d’un service informatique composé d’au moins trois personnes :

* Un responsable chef du service qui assure la conception et le suivi des projets informatiques des directions opérationnelles ;
* Un cadre chargé de l’administration et la sécurité du réseau informatique et télécommunications ;
* Un cadre chargé de la production et le développement d’applications et de portails informatiques relatifs aux activités de l’ANAC.

Le renforcement des compétences est un volet extrêmement important et ce personnel pourra effectuer les modules ci-dessous :

* Sécurité informatique
* VMware pour la virtualisation ;
* Fortinet pour segmentation, l’optimisation, la sécurité et l’interconnexion des réseaux ;
* Windev, Webdev et DEVOPS pour le développement d’applications informatiques ;
* Gouvernance cybersecurite pour la prévention attaques informatiques

1. **Architecture virtuelle**

L’ANAC dispose de serveurs physiques qui abritent tout le système d’information. Il est important et nécessaire de mettre un place une architecture virtuelle afin d'optimiser les ressources matérielles, permettant d'exécuter plusieurs systèmes d'exploitation sur une seule machine physique, réduisant ainsi les coûts et l'espace, l'isolation et la sécurité grâce à des environnements séparés pour les applications et les tests.

La virtualisation permet de sauvegarder de façon simple les serveurs virtuels et facilite la restauration simple et efficace en cas de sinistre.

1. **Absence de procédures de gestion de l’architecture informatique**

Pour une meilleure gestion de l’infrastructure et de répondre aux standards en terme de système d’information, il est nécessaire d’établir les procédures ci-dessous :

* Procédure de gestion des applications critiques (Sage Compta et Paie, Messagerie et système ECCAIS, système de délivrance des badges )
* Plan reprise d’activité
* Plan de riposte en cas d’attaque

L’absence de ces procédures entraine un pilotage à vue et peut entrainer des conséquences néfastes dans les activités de l’ANAC. La procédure de sauvegarde et restauration automatisée est obligatoire pour une entreprise comme l’ANAC. C’est un élément critique. Il est nécessaire de définir dans un document détaillé la fréquence et la manière de sauvegarder le système d’information notamment les applications critiques.

1. **Absence d’un système de sauvegarde et restauration non automatisée**

Vues les nombreuses attaques et risques et menaces dans le monde, aucune entreprise n’est pas à l’abri et peut être attaquée à tout moment. Il est nécessaire de disposer d’un système de sauvegarde-restauration comme VEEAM et d’effectuer des sauvegardes journalières des applications critiques et de faire des exercices de tests de restauration. Ces applications criques pourront être déployées dans un environnement virtuel, et l’administrateur pourra simplement sauvegarder les machines virtuelles. Il est également nécessaire d’externaliser les sauvegardes en les archivant dans un équipement de compression comme Datadomain ou une baie de stockage.

1. **Absence d’un équipement d’optimisation et de sécurisation du trafic applicatif**

 L’ANAC ne dispose pas de firewall pour le filtrage web et réseau. Compte tenu des nouvelles attaques émergentes, il est important de disposer d’un équipement de filtrage réseau et web et d’un système d’optimisation et de sécurisation du trafic issu des applications critiques. Ce système renseignera à temps réel des menaces et des risques d’attaques sur ces applications métiers.

**g. Automatisation du système de collecte ou de fiche d’intervention**

Il est important pour le service informatique de collecter les différents incidents ou panne survenus dans le réseau (ordinateurs du personnel, problème d’impression, problème d’antivirus, problèmes systèmes etc..) afin d’avoir une cartographie des pannes. Cette collecte automatisée vous permettra de mieux planifier vos besoins en investissement et d’anticiper sur les pannes avec des maintenances préventives programmées. Le système GLPI pourra être déployé a cet effet.

**h. Absence de plan de reprise d’activités**

Les attaques informatiques sont devenues fréquentes, le réseau peut tomber en panne a tout moment et entrainer l’arrêt du système d’information notamment avec des conséquences néfastes dans les activités de l’aviation civile. C’est pour cela qu’il est fortement conseillé de disposer d’un plan de reprise d’activités et d’organiser des séances de test et de simulations d’attaques.

**i. Absence de stratégie de cybersécurité**

Conformément aux recommandations de l’OACI dans la lutte contre les actes d’intervention illicite, l’ANAC devra établir une stratégie de cybersécurité pour prévenir les attaques et réduire les risques liés à la cybercriminalité. Les exploitants pourront s’inspirer de la stratégie de l’ANAC pour établir leur politique de cybersecurite.

Le service informatique devra dans le cadre de la mise en œuvre de la stratégie insister sur la collecte d’incidents et surtout sur la formation et la sensibilisation du personnel à la culture de la cybersécurité.

1. **Architecture réseau cible**

****

La construction d’un nouveau siège pour l’ANAC va regrouper toutes les directions. A cette effet cette architecture centralisée ci-dessous est proposée pour l’infrastructure informatique et télécoms.

Elle est composée d’une partie physique et d’une autre logique:

* La partie physique regroupant la partie énergie (groupe électrogène et onduleur) et la partie informatique (sécurité incendie, système de vidéosurveillance, contrôle d’accès biométrique, système de monitoring de température et détecteur de fumée et d’incendie, serveurs et câblages).
* La sécurité logique composé du pare feu pour le filtrage réseau, filtrage web et filtrage applicatif et logiciel antivirus ;

Elle comprend également une baie de stockage et la restauration de données et un datadomain pour l’archivage ;

L’infrastructure sera entièrement virtualisée avec le système avec VMware et VSphere pour l’optimisation des ressources des serveurs ;

Le premier serveur sera le contrôleur de domaine et peut abriter DHCP, DNS, AD et antivirus, tandis le second serveur abritera toutes les applications de l’ANAC.

1. **Mise à niveau des serveurs de l’ANAC**

Les deux serveurs de l’ANAC tournent sous Windows 2008 et Windows 2019 serveur. L’un abrite le contrôleur de domaine et le système ECCAIRS et l’autre était configuré dans un groupe de travail puisque le service informatique voulait séparer SAGE Compta et le contrôleur de domaine. la distribution d’adresses IP par le contrôleur de domaine créait des conflits et empêchaient les utilisateurs du logiciel SAGE d’accéder à la base de données SAGE via le répertoire partage.

Les corrections nécessaires ont été apportées sur les deux serveurs en désinstallant dans en premier le serveur DHCP sur le contrôleur de domaine et en second en supprimant les services ( AD, DHCP, DNS) sur le second serveur.

Les utilisateurs qui utilisent le logiciel SAGE peuvent être rajoutes via le contrôleur de domaine au répertoire partage SAGE COMPTA.

1. **Mise à jour du Système ECCAIRS**

Le système ECCAIRS a été mis à jour et les corrections nécessaires ont été faites pour l’accès via le web. Les incidents collectés avec l’ancien système ont été convertis en ec5f du système ECCAIRS 5 en installant un outil ECCAIRS Convert. La base de données est opérationnelle et les utilisateurs peuvent y connecter en renseignant les occurrences. Ils peuvent aussi envoyer les occurrences sous format ec5f et l’administrateur pourra les rajouter dans la base de données.

Le système a été aussi déployé sur les ordinateurs des agents concernés notamment ceux chargés de la collecte et du suivi des incidents et accidents.

1. **Projet de digitalisation des inspections**

**COMTEXTE**

La croissance du trafic aérien en Afrique montre des signaux positifs avec une augmentation notable des passagers en 2025 (9,5% selon Ecomnews Afrique), et des projections optimistes d'une croissance annuelle de 3,7 % à 4,1 % pour les vingt prochaines années, visant à doubler le marché d'ici 2043.

Les compagnies aériennes africaines ont enregistré une augmentation de 9,5 % du trafic passagers en 2025, atteignant un taux d'occupation de 74,9 %. En octobre 2024, le trafic passagers avait déjà connu une hausse de 10,4 % sur un an, une performance notable pour le continent.

L'Association du Transport Aérien International (IATA) anticipe que le marché de l'aviation en Afrique plus que doublera d'ici 2043, avec un taux de croissance annuel moyen estimé entre 3,7 % et 4,1 %.

Cette croissance du trafic aérien en Afrique explique le développement et la création de compagnies aériennes nationales (Ethiopian Airlines, Royal Air Maroc, South Africa Airlines, Mauritania Airlines, Kenya Airways, Air Sénégal International, Asky, Air Cote D’Ivoire etc.…). L’augmentation du trafic entraine aussi des défis relatif à la supervision de la sécurité et de la sureté par les autorités d’aviation civile à travers les aspects relatifs aux inspections sureté, SAFA, SANA et aérodromes, à la délivrance de certificat de navigabilité, de permis d’exploitation aérienne, de licences du personnel aéronautiques, des opérations aériennes en vol et au sol, de l’immatriculation et de l’inspection des aéronefs, de la surveillance et de l’homologation ou de la certification des aéroport et sociétés de sureté aéroportuaires.

**Présentation de SGI**

**Conformément aux recommandations de l’OACI dans les questions de protocole EC7** et vu le développement des nouvelles technologies de l’information et de la communication à travers même les compagnies aériennes et les exigences des passagers, la digitalisation de ces procédures citées en dessus nécessitent une plateforme informatique moderne, efficace et efficiente qui pourra augmenter la performance et la productivité des autorités d’aviation civile.

Le système de gestion des inspections sureté, sureté, SAFA, SANA, RAMP et aérodromes est conçu pour répondre à ce défi de dématérialisation des processus de supervision de la sureté et de la sécurité.

La mise en place de ce dispositif informatique permettra non seulement d’accélérer le traitement des inspections mais aussi de disposer d’un système d’information exhaustif, performant, cohérent et adapté à ses propres besoins. Cette plateforme qui sera connectée à un outil de reporting et d’aide à la prise de décision, s’inscrit dans le processus d’accompagnement et de renforcement des capacités du personnel des autorités aéroportuaires.

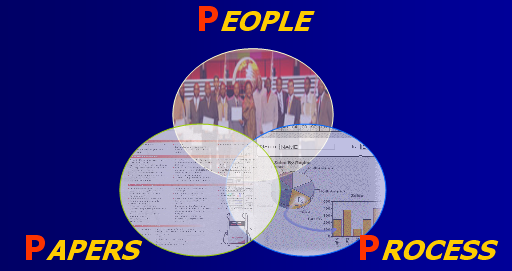
Le système facilite la reporting et le suivi des constatations et des recommandations et l’édition de rapport d’inspection a temps réel. Il renferme un outil d’aide à la décision qui est compose d’un puissant tableau de bord relatif aux inspections par type, par domaine, par entité inspectée ainsi que le suivi des recommandations et l’historique des inspections.

**Objectifs de SGI**

Le but visé à travers ce système c’est de mettre en place une plateforme intégrée Progiciel de gestion intégré (PGI ou ERP en anglais) afin de faciliter le traitement des inspections relatives aux différentes activités techniques des autorités d’aviation civile. Cette plateforme permet d’enregistrer et de traiter les inspections avec des accès sécurisés.

La plateforme est  un programme très ergonomique et simple d’utilisation. Il informe en temps réel sur l’état d’avancement et de suivi des inspections, leur niveau de traitement ainsi que leur localisation.

Elle est **conçue** et élaborée en conformité au principe des **3P’s**. **(People ; Papers ; Process)** c’est à dire la gestion interactive entre les acteurs, les documents et les procédures.

****

Cette plateforme électronique permet aux différents utilisateurs travaillant en réseau, d’accéder, de consulter, d’interroger, d’extraire, de partager et de diffuser des données et informations.

La mise en œuvre de l’application inclut absolument :

* Assurer la fiabilité et la cohérence des données ;
* Garantir la gestion efficace et efficiente des informations ;
* Implémenter la technologie fullweb dans un environnement sécurisé - accès distant ;
* assurer l’accès à l’information en temps réel ;
* Mettre en place une ergonomie favorisant une appropriation et une exploitation optimale de l’application par les utilisateurs ;
* Assurer la maintenance qui comprend la sauvegarde régulière des données du système ;
* Assurer la pérennité du dispositif.

**Modules et fonctionnalités de SGI**

Plus spécifiquement, la plateforme electronique comprend les modules ci-après :

* **Suivi des inspections Sureté,**
* **Suivi des inspections RAMP, SANA, SAFA,**
* **Suivi des inspections Aérodromes. ;**

Le système englobe les principales fonctionnalités :

* L’accès distant ;
* La prise en compte du circuit de traitement et de validation des inspections (workflow) ;
* Le système de reporting ;
* La génération automatique de tableaux de bord pour aider à la prise de décisions ;
* L’implémentation d’un système d’alerte sous forme d’email ;
* L’enregistrement rapide et la mise à disposition des informations en temps réel pour permettre un gain de temps précieux ;
* La diffusion et le partage sécurisés des données ;
* Le traitement pour automatiser et simplifier au maximum les tâches administratives :
  + *Gestion des diligences*
  + *Gestion du niveau de sensibilité et de confidentialité*
  + *Gestion de la traçabilité*
* La recherche pour garantir l’accès rapide et pertinent à l’information et accélérer les prises de décision ;
* La gestion des délais de traitements des dossiers ;
* Assurer la formation des utilisateurs ;
* Gestion des profils des utilisateurs ;
* Gestion discriminante de l’accès à l’information.

Durant la mission, nous avons rencontré le Directeur Sureté et Facilitation, le Coordinateur de la mise en œuvre de la Sureté a l’Aéroport de Nouakchott et le responsable informatiques et avons présenté le système de gestion des inspections Sureté de l’ANACIM.

La DSF et le Coordonnateur de la mise en œuvre de la Sureté ont vivement apprécié le système de gestion des inspections et souhaite la conception d’un tel système personnalise et adapte à leur plateforme pour faire le suivi des constations et des recommandations lors de la Contrôle Qualité.

Ils ont par ailleurs exprimé le souhait de prendre toutes les questions de protocoles de l’OACI dans le domaine EC7 afin de faciliter les audits avec l’OACI. Ils sont demande aussi d’ajouter une fenêtre qui fera une analyse suscinte annuelle des inspections effectuées avec les recommandations et les plans d’action des entités inspectées. Cette analyse permettra de générer le planning de l’année suivante qui prendra en compte les écarts non fermes.

Le DSF a aussi exprimé le souhait d’avoir un système de gestion des formations pour les inspecteurs et le personnel d’inspection filtrage.

Le Coordonnateur de la Mise en œuvre de la Sureté a aussi exprimé le souhait de disposer d’un système de gestion des inspections sureté pour mieux mettre en œuvre les mesures de sureté et suivre les recommandations de l’ANAC.

**Module Suivi des inspections Sureté**

Ce module prend le suivi des mesures sureté conformément aux questions de protocoles de l’OACI. Il renferme toutes les domaines d’inspection :

**VII. Recommandations**

* Acquérir et installer un onduleur de puissance 20KVA pour renforcer la protection des serveurs et équipements actifs du réseau informatique ;
* Acquérir un système automatisé de sauvegarde et de restauration des données et effectuer des sauvegardes journalières incrémentielles et des sauvegardes hebdomadaires complètes;
* Acquérir une baie de stockage ou équipement de sauvegarde des données ;
* Mettre à niveau la salle serveur en installant :
  + - Système sécurité incendie
    - Système de détection de température, de fumée et d’humidité
    - Système de caméra de surveillance
    - Système d’accès biométrique
* Recruter un technicien en informatique pour la sécurité et l’administration du réseau et un développeur pour la productions d’applications informatiques dans le domaine aéronautique
* Élaborer un projet de stratégie de cybersecurite au niveau du secteur aéroportuaire ;
* Finaliser et implémenter le système de gestion des inspections en validant les différentes étapes de la conception et de la réalisation.

**IV. Conclusion**

La mission a permis de diagnostiquer en profondeur le réseau informatique et apporter les corrections nécessaires pour une meilleure exploitation du système d’information. Le système ECCAIRS est mis à jour et est devenu opérationnel et peut aussi être déployer sur le serveur de production. Des soucis sur les anciens navigateurs ont été constatés. Ces problèmes dus au système d’exploitation qui abrite le système ECCAIRS, pourront être résolus en déplaçant le système ECCAIRS vers le serveur de Production.

Les observations, remarques et recommandations sur le système de gestion des inspections sureté seront prises en compte dans les meilleurs délais et le système pourra être présenter à nouveau à tout le personnel de la DSF. Cette présentation et prise en main du système pourra se faire en début Novembre 2025 sur 5 jours avec un manuel d’utilisation et des inspections sur site avec des tablettes.

Nous sommes également disponible à accompagner la DSF pour la conception et la réalisation d’un système de gestion de la formation pour les inspecteurs et le personnel d’inspection filtrage.