

REPUBLIQUE DE GUINEE

*Travail-Justice-Solidarité*



**UNIVERSITE GAMAL ABDEL NASSER DE CONAKRY**

-----

**CENTRE INFORMATIQUE  
(NTIC)**

Projet de Fin d'Etude

**Spécialité : NTIC (Nouvelle Technologie de l'Information et de la Communication)**

**Entreprise : ENTACIG (Espace Numérique de Technologie et d'Alerte du Centre Informatique de Gamal)**

Présenté Par :

1/ BERETE Moussa

2/ SAGNO Beko

Licence III (NTIC)

Licence III (NTIC)

# BIENVENUE SUR ENTACIG

Le nom d'ENTACIG viennent de deux étudiants du centre informatique de l'**Université Gamal Adbel Nasser de Conakry (UGANC)** **MOUSSA BERETE** **et BEKO SAGNO**, la création de ce nom a été dévoiler le 01 novembre 2024. Dans le contexte de la réalisation d'un projet système de détection et d'alerte précoce utilisant des réseaux de capteurs distribués et l'IA.

Pourquoi ce nom ENTACIG ?

Le nom **ENTACIG** est un acronyme reflétant les valeurs et les missions clés de l'entreprise. La signification de chaque mot et son importance dans le contexte du projet

### **E - Espace**

L'acronyme commence par "Espace" pour signifier que le système ENTACIG couvre un large domaine d'application, notamment dans un campus de **Gamal**, où il veille à la sécurité de l'espace physique et numérique.

*Importance* : Cela souligne l'objectif de surveiller et de protéger l'espace du campus dans son ensemble, en offrant un environnement sécurisé pour les étudiants, le personnel, et les visiteurs.

### **N - Numérique**

"Numérique" représente l'utilisation de technologies modernes, de capteurs IoT (Internet of Things) et de solutions digitales pour la surveillance et l'analyse des données.

*Importance* : Ce mot reflète le recours aux outils numériques avancés et à l'intelligence artificielle pour rendre la sécurité plus intelligente et proactive. Cela marque l'innovation et l'adaptabilité du système aux technologies de pointe.

## **T - Technologie**

"Technologie" fait référence aux dispositifs techniques, aux algorithmes de détection, et aux infrastructures réseau nécessaires pour mettre en œuvre une surveillance automatisée.

*Importance* : La technologie est le pilier fondamental du projet. Grâce aux technologies de capteurs et à l'IA, ENTACIG peut surveiller, analyser et alerter de manière automatique et rapide, garantissant une protection constante.

## **A - Alerte**

"Alerte" souligne la capacité de l'entreprise à détecter et signaler les dangers potentiels en temps réel.

*Importance* : L'alerte rapide est essentielle pour éviter les incidents graves. Cela permet aux utilisateurs de réagir immédiatement face à un danger, qu'il s'agisse d'un incendie, d'une intrusion, ou d'autres événements potentiellement risqués.

## **C - Centre**

"Centre" fait référence au campus ou à l'institution de **Gamal** qui constitue le point central de surveillance et de protection du système.

*Importance* : Cela indique que l'approche de sécurité d'ENTACIG est centralisée et globale, ce qui renforce la coordination et l'efficacité dans la détection et la gestion des incidents.

## **I - Informatique**

"Informatique" représente les systèmes, logiciels et outils numériques mis en œuvre pour collecter, analyser et gérer les données en temps réel.

*Importance* : L'informatique est indispensable pour le traitement des données, l'IA, et l'intégration des capteurs. Elle garantit que le système ENTACIG reste performant, automatisé, et intelligent dans la gestion des alertes.

## **G - Gamal**

"Gamal" se réfère ici à l'université ou au campus spécifique (par exemple, **Université Gamal Abdel Nasser de Conakry**) sur lequel le système sera initialement mis en place.

*Importance :* En identifiant une institution particulière, ENTACIG se personnalise pour répondre aux besoins uniques de cet établissement. Cela démontre également l'adaptabilité du projet à d'autres campus universitaires qui pourraient adopter ce modèle de sécurité.

## **Importance Globale d'ENTACIG**

L'acronyme **ENTACIG** représente une vision holistique de la sécurité et de l'alerte précoce dans un environnement universitaire, combinant technologie de pointe, protection des espaces, et réactivité. Ce projet vise à établir un modèle de sécurité moderne et intelligent, adaptable à différents campus, avec une approche proactive pour garantir un environnement sûr et résilient.

Le nom complet d'**ENTACIG** qui est :  
**Espace Numérique de Technologie d'Alerte du Centre Informatique de Gamal**

# Pourquoi l'entreprise ENTACIG ?

Espace Numérique de Technologie d'Alerte du Centre Informatique de Gamal



# Problématique liée au concept a notre entreprise

Quels sont les problèmes sociaux et/ou environnementaux que nous allons essayer de résoudre ?

Qu'est-ce que notre business va améliorer ?

Dans 5 ans, qu'est-ce que notre entreprise d'ENTACIG changera dans la société ?

Quel sera l'impact ?

# La présentation de l'entreprise de l'ENTACIG

## INTRODUCTION

Dans un monde où la sécurité et la réactivité aux incidents sont de plus en plus primordiales, les établissements universitaires, en particulier les campus, nécessitent des systèmes de protection avancés et efficaces. ENTACIG, un projet innovant et multidimensionnel, vise à répondre à ces besoins en intégrant l'intelligence artificielle et les réseaux de capteurs distribués pour créer un système de détection et d'alerte précoce.

Conçu pour les espaces universitaires comme le campus Gamal Abdel Nasser de Conakry (UGANC), ENTACIG utilise la puissance des technologies numériques et informatiques pour surveiller en temps réel, analyser les situations à risque, et notifier instantanément les parties concernées. Grâce à cette approche, ENTACIG contribue non seulement à renforcer la sécurité des personnes et des biens, mais aussi à instaurer une culture de vigilance proactive, faisant de la sécurité une composante intégrée de la vie universitaire.

<b>9) Partenaires</b> <b>Les partenaires potentiels pourraient inclure :</b> <b>Partenaire :DAO (Direction Assistée des Ordinateurs)</b> <b>Sponsors :</b> CENTRE INFORMATIQUE <b>Partenaires technologiques et assistances :</b> LAGUIPRESS. <b>Fournisseurs :</b> Les fabricants de capteurs et de matériel informatique. <b>Menerga</b>	<b>8) Activités clé</b> Les activités principales incluent la R&D pour l’optimisation des capteurs et de l’IA, la gestion de projets pour les installations sur site, le support client, et l’amélioration continue de la solution.	<b>2) Offre de valeur</b> <b>Concept du projet :</b> <b>ENTACIG</b> propose une solution de détection et d’alerte précoce reposant sur des réseaux de capteurs intelligents et de l’intelligence artificielle, capable d’identifier des situations anormales ou à risque en temps réel et de notifier instantanément les parties concernées. La solution est personnalisable pour s’adapter aux spécificités de chaque établissement.	<b>5) Relation client</b> <b>ENTACIG</b> souhaite entretenir une relation de partenariat de long terme avec ses clients, axée sur la confiance et la sécurité. La relation serait proactive, incluant un support technique et une assistance à la demande pour assurer une réactivité maximale.	<b>3) Cibles</b> <b>Bénéficiaires :</b> Les étudiants, le personnel, les enseignants et les visiteurs du campus bénéficieront de cet impact social direct en évoluant dans un environnement plus sûr. <b>Clients :</b> Les universités, les centres de recherche, et autres établissements éducatifs sont les clients susceptibles de financer cette solution pour assurer la sécurité de leurs espaces. <b>Intéressés à acheter :</b> Les administrations universitaires, les responsables de sécurité, et potentiellement les associations étudiantes qui souhaitent améliorer la sécurité du campus. <b>Bénéficiaires directs :</b> Les bénéficiaires directs incluent les personnes présentes sur le campus, mais également les autorités en charge de la sécurité qui bénéficieront de données en temps réel.
	<b>7) Ressources</b> <b>Financières :</b> Besoin d’investissements initiaux pour le développement des capteurs et l’infrastructure logicielle. <b>Humaines :</b> Une équipe composée de développeurs spécialisés en IA et IoT, de techniciens pour la mise en place et la maintenance, ainsi que de commerciaux. <b>Logistique :</b> Besoin d’un système logistique pour distribuer les capteurs, installer et maintenir les dispositifs. <b>Propriété intellectuelle :</b> Brevets sur les algorithmes d’IA utilisés pour la détection et l’alerte, ainsi que la propriété des données recueillies pour des analyses d'amélioration.		<b>4) Canaux de distribution</b> Le produit serait livré principalement sous forme de service, incluant l’installation des capteurs, le déploiement de l’IA, et la formation des utilisateurs. Cela peut se faire par vente directe, en partenariat avec des intégrateurs technologiques, ou par le biais de contrats de maintenance.	
<b>10) Coûts</b> Les principaux coûts incluent : Développement et maintenance du système logiciel. Achat et installation des capteurs et infrastructure réseau. Support technique et maintenance des installations. Marketing et commercialisation pour la promotion de la solution auprès des établissements éducatifs. <b>Total = DevMaint + AchInstCap + SupTechMaint + MarkCom = SomTotal</b>			<b>6) Revenus</b> Les revenus proviendront des ventes du produit sous forme de solution complète, avec des frais d’installation initiaux et des contrats de maintenance mensuels ou annuels. D’autres revenus pourraient être générés par l’offre de services supplémentaires, comme des mises à jour du système et des formations périodiques.	
1) Bénéfices sociaux et environnementaux Problèmes résolus : Le projet ENTACIG vise à améliorer la sécurité et le bien-être au sein d’un campus universitaire. Les capteurs permettront de détecter des anomalies ou des menaces (incidents de sécurité, incendies, ou risques environnementaux) en temps réel, offrant ainsi une alerte précoce. Ce système réduit les risques de blessures, de pertes matérielles et améliore la réactivité des équipes d’urgence. Améliorations : Dans 5 ans, ENTACIG aura contribué à créer un environnement de campus plus sûr et résilient. Ce système permettra de prévenir des incidents graves et de sensibiliser la communauté à des pratiques de sécurité renforcées. Impact : L’impact attendu est une baisse des accidents et des pertes liées aux risques environnementaux. De plus, cela développera une culture de sécurité proactive dans les campus universitaires et incitera les autres établissements à adopter des solutions similaires.				

# CAHIER DE CHARGE

## **1. Contexte et Objectif du Projet**

L'objectif est de créer un système intelligent de détection et d'alerte précoce pour le campus universitaire afin de surveiller l'environnement en temps réel, identifier les anomalies (mouvements suspects, incendies, fuites de gaz, etc.), et alerter rapidement les autorités ou les responsables de la sécurité du campus. Le système s'appuie sur un réseau de capteurs distribués et sur des algorithmes d'intelligence artificielle pour l'analyse des données recueillies.

### **1.1 Contexte**

Le campus est vaste et inclut des zones critiques telles que les résidences étudiantes, laboratoires, salles de classe, et zones de stationnement, qui nécessitent une surveillance constante pour garantir la sécurité. Le projet vise à minimiser les risques potentiels en identifiant les menaces avant qu'elles ne se manifestent.

# 1.2 Objectif

- Détection automatique et en temps réel des menaces (incendies, mouvements inhabituels, fuites de gaz, bruits anormaux, etc.).
- Alerte précoce et notification immédiate aux responsables du campus via SMS, e-mail ou notification mobile.
- Interface de visualisation des événements en temps réel via un tableau de bord accessible depuis des PC et smartphones.

# 2. Périmètre du Projet

## 2.1 Fonctionnalités principales

- Détection de mouvement : Surveillance des zones sensibles pour détecter les mouvements non autorisés.
- Détection d'incendies : Identification précoce des fumées et des hausses anormales de température.
- Détection de gaz : Détection de fuites de gaz potentiellement dangereuses dans les laboratoires.
- Analyse des sons : Surveillance des bruits excessifs ou anormaux pouvant signaler des incidents.
- Surveillance par caméra : Utilisation de caméras pour capturer et analyser des vidéos via des algorithmes de vision par ordinateur.
- Alertes et notifications : Envoi d'alertes en temps réel aux responsables via SMS, e-mail, ou notifications push sur mobile.
- Hologramme : pour afficher les images détecté dans l'air

## 2.2 Interfaces utilisateur

- Tableau de bord web : Visualisation des événements détectés, accès aux caméras en direct, gestion des capteurs, consultation des historiques.
- Application mobile: Réception des notifications d'alertes et accès au système depuis les smartphones.

## **2.3 Capteurs utilisés**

- Capteurs de mouvement (PIR).
- Capteurs de température.
- Capteurs de fumée et gaz (MQ-2)
- Capteurs sonores.
- Caméras de surveillance.
- Hologramme

# 3. Contraintes techniques

## 3.1 Langages et technologies

- Frontend (interface utilisateur):
  - React.js pour le développement du tableau de bord et de l'interface web.
  - React Native pour le développement de l'application mobile (facultatif).
- Backend (serveur) :
  - Node.js pour la gestion des API et la collecte des données des capteurs.
  - Python pour l'analyse de données et l'implémentation d'algorithmes IA.
- Base de données :
  - MongoDB ou PostgreSQL pour stocker les données collectées par les capteurs.
- Capteurs et dispositifs IoT :
  - ESP32/ESP8266, Raspberry Pi, ou Arduino pour la collecte de données et la communication avec les capteurs.

## 3.2 IA et traitement des données

- Algorithmes d'intelligence artificielle :  
Utilisation de modèles de machine learning (comme TensorFlow ou Scikit-learn) pour analyser les données des capteurs et détecter les anomalies.
- Traitement en temps réel : Les données doivent être traitées rapidement pour déclencher des alertes immédiates en cas d'anomalie.



# 4. Exigences fonctionnelles

## 4.1 Collecte et traitement des données

- Collecte des données : Les capteurs doivent pouvoir collecter des données en temps réel (mouvements, températures, fumées, gaz, sons, images).
- Analyse et détection des anomalies : Implémenter des modèles de détection d'anomalies pour analyser les données collectées.
- Stockage des données : Utiliser une base de données pour stocker les événements détectés ainsi que les journaux des capteurs.

## 4.2 Système de notification

- Envoi d'alertes immédiates par SMS, e-mail ou notification push aux responsables lorsqu'une menace est détectée.
- Notifications différenciées selon la gravité de la menace (alertes critiques ou simples avertissements).

## **4.3 Interface utilisateur**

- Tableau de bord web pour visualiser les capteurs, les alertes, les flux de caméras, et accéder aux historiques.
- Interface mobile pour que les responsables puissent recevoir des notifications et consulter les événements à distance.

# 5. Exigences non fonctionnelles

## 5.1 Performance

- Les capteurs doivent envoyer les données en temps réel.
- Le système d'alerte doit réagir instantanément à la détection d'une menace.

## 5.2 Sécurité

- Sécurisation des communications entre les capteurs et le serveur via des protocoles sécurisés (SSL/TLS).
- Gestion des accès utilisateurs pour le tableau de bord (authentification avec OAuth2 ou JWT).

## 5.3 Fiabilité

- Les capteurs doivent fonctionner en continu avec une alimentation ininterrompue (solutions de batterie ou panneaux solaires).
- Tolérance aux pannes pour garantir que le système reste fonctionnel même si un capteur tombe en panne.

# 6. Contraintes de délais et de budget

## 6.1 Délais

- Le projet doit être réalisé en deux mois. Un planning sera établi avec les étapes clés, comprenant :
  - **Phase de conception (2 semaines)** : Définition des spécifications, conception des interfaces, architecture des capteurs.
  - **Phase de développement (4 semaines)** : Développement du frontend, backend, et configuration des capteurs.
  - **Phase de test (2 semaines)** : Tests unitaires, tests d'intégration, et validation des fonctionnalités du système.

## 6.2 Budget

### Le budget devra inclure :

- Coût des capteurs (mouvement, température, fumée, gaz, caméras).
- Coût des microcontrôleurs (ESP32, Raspberry Pi, Arduino).
- Coût des serveurs ou services cloud.
- Coût des licences logicielles (si applicable).
- Coût de développement logiciel (temps des développeurs).

## 7. Livrables attendus

- **Rapport de conception** : Documentation complète sur l'architecture du système.
- **Système de détection fonctionnel** : Système opérationnel avec les capteurs déployés.
- **Application web et mobile**: Tableau de bord et notifications pour les responsables du campus.
- **Documentation technique**: Guide de déploiement, documentation du code, et manuel utilisateur.

## 8. Équipe de réalisation

- **Chef de projet** : Responsable de la gestion des délais et du suivi du projet.
- **Développeurs frontend** : Pour le développement du tableau de bord et de l'application mobile.
- **Développeurs backend** : Pour la mise en place des API, gestion des données, et intégration avec les capteurs.
- **Expert IoT** : Pour la configuration des capteurs et la gestion des microcontrôleurs.
- **Data scientist** : Pour l'implémentation des algorithmes IA et l'analyse des données.

Ce cahier des charges servira de base à la réalisation du projet en définissant clairement les objectifs, les fonctionnalités, les contraintes techniques et les livrables attendus dans le délai imparti.

# CONCLUSION

ENTACIG se positionne comme une solution de pointe, en harmonie avec les besoins de sécurité actuels des campus universitaires. En fusionnant la technologie de détection, l'analyse prédictive et la réactivité, ce projet a le potentiel de transformer la gestion de la sécurité sur les campus.

Non seulement ENTACIG protège les individus et les infrastructures, mais il crée également un environnement où l'innovation est mise au service du bien-être collectif. En offrant un modèle de sécurité intelligent et adaptable, ENTACIG ouvre la voie à une vision moderne de la protection universitaire, où chaque incident potentiel peut être anticipé, et chaque risque, réduit.

FIN