AVIS DE SOLLICITATION A MANIFESTATION D'INTERET
N°021/ASMI/MINPOSTEL/PATNUC/UGP/MC2/SFM/2025 POUR LA SELECTION D'UN CONSULTANT EN VUE DE LA FORMATION SUR LA SECURITE INFORMATIQUE AUX AGENCES GOUVERNEMENTALES.

DATE : 12 NOV 2025

FINANCEMENT : IDA 69870-CM

1. CONTEXTE ET JUSTIFICATION

1.1. Contexte

Le Gouvernement du Cameroun a bénéficié d'un prêt de la Banque mondiale d'un montant de 100 millions USD pour mettre en œuvre le Projet d'Accélération de la Transformation Numérique au Cameroun (PATNUC). Le PATNUC est placé sous la tutelle du MINPOSTEL et a pour objectif d'accroître l'inclusion numérique et l'utilisation de solutions agricoles numériques par des petits exploitants agricoles acteurs des chaînes de valeur agricoles cibles. Ainsi, le PATNUC incarne l'approche de la transformation numérique, ciblant un secteur hautement stratégique pour le Cameroun tout en proposant de réformer le cadre règlementaire du secteur des Technologies de l'Information et de la Communication (TIC). Ce projet, avec son investissement dans la connectivité et les compétences numériques, soutient des interventions qui tirent parti des innovations numériques pour stimuler la croissance agricole, afin de contribuer en fin de compte à l'amélioration de la qualité des moyens de subsistance en milieu rural.

Le PATNUC est structuré autour de 4 composantes : (i) Stratégie, politique publique et réglementation numérique pour l'inclusion et la transformation numérique ; (ii) connectivité et inclusion numériques ; (iii) facilitation de l'implémentation des solutions numériques basées sur les données dans le secteur agricole ; et (iv) gestion du projet et l'engagement citoyen. Ainsi, le gouvernement à travers la SND30, ambitionne d'enclencher véritablement la transformation structurelle de l'économie camerounaise. La transformation digitale passera forcément par un renforcement de capacité des principaux acteurs du numérique dans l'écosystème camerounais. Dans la composante 1 du projet, il a été ciblé certaines institutions actrices du secteur du numérique dont la performance nécessite une mise à jour et l'acquisition de nouvelles connaissances dans le secteur du numérique.

1.2. Justificatif de la mission

Dans l'optique d'améliorer ses performances, d'optimiser ses processus et réduire les interactions humaines qui sont souvent source de corruption, le gouvernement de la République du Cameroun, sous l'impulsion éclairée du Président de la République, a entamé un vaste programme de transformation digitale de l'Administration camerounaise.

Cependant bien que l'adoption des TIC soit bénéfique, elle charrie néanmoins des risques importants liés aux attaques informatiques.

C'est fort de cela qu'à travers la loi N°2010/012 sur la cybersécurité et la cybercriminalité, l'ANTIC a été chargée entre autres d'assurer la sécurité des infrastructures cybernétiques des Structures publiques et privées à travers notamment la veille sécuritaire et les audits de sécurité.

Les audits de sécurité des Administrations publiques réalisés sur la base de la norme ISO 27001 ont révélé plus de 3420 vulnérabilités sur les plans organisationnel, physique et technique. Une analyse des causes racines de ces vulnérabilités laisse transparaître que le manque de compétences techniques sur la cybersécurité des personnels des départements informatique des Administrations et le déficit de sensibilisation des agents de l'Etat sur les règles hygiène numérique constituent les principales causes de la prolifération des menaces cybernétiques au sein des Structures publiques.

C'est dans ce sens que le PATNUC dans ses activités prévoit le financement des formations en sécurité informatique à l'endroit desdites Administrations autour d'un programme qui repose sur trois (03) grands axes à savoir : la gouvernance de la cybersécurité, la sécurité applicative et la sécurité des systèmes et réseaux.

Le présent document vise donc à proposer les termes de référence d'un projet visant à renforcer les capacités opérationnelles des personnels techniques des départements informatiques des administrations parapubliques (agences du gouvernement, établissement publiques administratifs) sur la cybersécurité.

2. OBJECTIFS DE LA MISSION

Les présents TDR visent à permettre au personnel technique des administrations parapubliques d'acquérir des compétences pratiques leur permettant d'assurer au quotidien la sécurité des systèmes d'information de leurs Administrations respectives. De manière spécifique, il s'agira de :

- Proposer un cursus de formations pratiques basé sur des programmes certifiants dans le domaine de **la gouvernance de la cybersécurité**. A l'issue de ces formations les apprenants devront être capable d'élaborer et piloter des stratégies et procédures basés sur des référentiels techniques élaborés par l'ANTIC et ancrés sur des normes internationales ;
- Proposer une plateforme en ligne de sensibilisation des personnels non informaticien de des agences gouvernementales retenues sur les règles de bonnes pratiques sécuritaires ou d'hygiène numérique. Ladite plateforme devra présenter une excellente ergonomie avec des contenus digestes afin de faciliter leur appropriation par les apprenants. Cette plateforme pourrait s'inspirer de la certification CSCU (Certified Secure Computer User) et pour le suivi des formations certifiante en ligne ;
- Développer une méthodologie pédagogique axée sur la pratique et la simulation de scénarios réels d'attaques et d'incidents, afin de préparer concrètement le personnel des Administrations à répondre efficacement aux cybermenaces ;
- Mettre en place un calendrier de formation qui minimise l'impact sur les opérations courantes des Administrations, tout en assurant une formation complète de l'ensemble du personnel concerné ;
- Assurer une organisation logistique sans faille pour permettre aux personnels des Administrations de se concentrer pleinement sur leur apprentissage et leur développement de compétences ;
- Mettre en œuvre une évaluation rigoureuse des compétences acquises, permettant de mesurer l'impact de la formation ;
- Proposer des recommandations pour des formations complémentaires, assurant une mise à niveau continue des compétences des apprenants face à l'évolution constante des menaces ;
- Doter les apprenants de supports de formation, facilitant l'application des connaissances acquises dans leurs tâches quotidiennes de protection du cyberspace national ;
- Rendre compte en atelier des résultats de la formation aux différentes administrations parties prenantes ;
- Atteindre un pourcentage de personnels certifiés élevé et touchant toutes les administrations ;
- Atteindre un pourcentage élevé d'administration disposant d'un plan de réponse aux incidents (IRP) et d'un registre des risques approuvé ;

- Former cents (100) personnels des départements IT des Administrations publiques afin de leur capacité sur l'élaboration et le pilotage des stratégies et procédures basés sur des référentiels techniques élaborés par l'ANTIC et ancrés sur des normes internationales ;
- Veiller que la présence par participants et par modules soit supérieure ou égale a 90% (preuves : feuilles d'émargement et journaux de connexion aux labs) ;
- Veiller au suivi efficace afin d'atteindre le taux de réussite minimale acceptable de 70% dans les 120 jours suivant chaque session (preuves : certificats / e-mails des organismes, Complétion des laboratoires ≥ 85 % preuves : rapports plateforme, Satisfaction ≥ 4/5 preuves : questionnaires agrégés) ;
- Animer 03 ateliers pour la formation en présentiel des personnels, 01 atelier de sensibilisation des personnels des Administrations publiques et 01 atelier de restitution des travaux et de validation du rapport final et (runbooks, preuves : PV signés + documents).

3. PORTEE DE LA MISSION

Il sera question de capaciter en présentiel 100 (cent) personnels, provenant des administrations parapubliques et un nombre maximal en ligne. La mission devra en outre intégrer une approche inclusive, en tenant compte des genres, des niveaux de responsabilité et de la diversité des agences gouvernementales bénéficiaires, **Une réunion de cadrage** permettra de s'assurer de la bonne compréhension commune de la mission et donnera les orientations pour une définition de la méthodologie par le consultant.

4. RESULTATS ATTENDUS

Au terme de ces formations, les résultats attendus sont les suivants :

- Un cursus de formations pratiques basé sur des programmes certifiants dans le domaine de **la gouvernance de la cybersécurité.** A l'issue de ces formations les apprenants devront être capable d'élaborer et piloter des stratégies et procédures basés sur des référentiels techniques élaborés par l'ANTIC et ancrés sur des normes internationales est proposé ;
- Un cursus de formations pratiques basé sur des programmes certifiants dans le domaine de **la sécurité des plateformes applicatives.** A l'issue de ces formations, les apprenants devront être capable d'assurer la sécurité des applications informatiques durant tout leur cycle de vie de la conception jusqu'à l'exploitation est proposé ;
- Une plateforme en ligne de sensibilisation des personnels non informaticien de toutes les agences gouvernementales sur les règles de bonnes pratiques sécuritaires ou d'hygiène numérique. Ladite plateforme devra présenter une excellente ergonomie avec des contenus digestes afin de faciliter leur appropriation par les apprenants. Cette plateforme pourrait s'inspirer de la certification CSCU (Certified Secure Computer User) est disponible ;
- Une méthodologie pédagogique axée sur la pratique et la simulation de scénarios réels d'attaques et d'incidents, afin de préparer concrètement le personnel des Administrations à répondre efficacement aux cybermenaces est développé ;
- Un calendrier de formation qui minimise l'impact sur les opérations courantes des Administrations, tout en assurant une formation complète de l'ensemble du personnel concerné est élaboré ;
- Une organisation logistique sans faille pour permettre aux personnels des Administrations de se concentrer pleinement sur leur apprentissage et leur développement de compétences est assurée ;
- Mettre en œuvre une évaluation rigoureuse des compétences acquises, permettant de mesurer l'impact de la formation ;

➢ Proposer des recommandations pour des formations complémentaires, assurant une mise à niveau continue des compétences des apprenants face à l'évolution constante des menaces ;

➢ Les apprenants sont dotés de supports de formation, facilitant l'application des connaissances acquises dans leurs tâches quotidiennes de protection du cyberspace national ;

➢ 100 personnels des départements IT des Administrations publiques capable d'élaborer et piloter des stratégies et procédures basés sur des référentiels techniques élaborés par l'ANTIC et ancrés sur des normes internationales ;

➢ Le taux présence par participants et par modules d'au moins 90% est atteint ;

➢ Un taux de réussite d'au moins de 70% dans les 120 jours suivant chaque session (preuves : certificats / e-mails des organismes, Complétion des laboratoires ≥ 85 % preuves : rapports plateforme, Satisfaction ≥ 4/5 preuves : questionnaires agrégés) est acquis ;

➢ Trois (03) ateliers pour la formation en présentiel des personnels, 01 atelier de sensibilisation des personnels des Administrations publiques et 01 atelier de restitution des travaux et de validation du rapport final et (runbooks, preuves : PV signés + documents) sont organisés ;

➢ Un atelier de restitution de la mission est organisé.

5. DUREE DE LA MISSION

La formation est prévue pour une durée douze (12) mois et se fera en deux étapes : en présentiel et en ligne.

6. PROFIL DU CONSULTANT

Le consultant sélectionné sera soit un Cabinet ou un groupement de cabinets ayant une expertise dans la Cybersécurité et la cybercriminalité.

Il devra :

➢ Disposer du personnel qualifié possédant de certifications ou équivalents dans les différents modules de formation, ainsi que les ressources matérielles, logicielles et logistiques nécessaires ;

➢ Posséder des connaissances et avoir au moins une (01) référence dans la formation en cybersécurité ou des cursus académique de master en cybersécurité en Afrique.

Le consultant devra également justifier d'une expérience sur les référentiels du FIRST.

7. METHODE DE SELECTION

Il est porté à l'attention des Consultants que les Cabinets ou Groupement de Cabinets/Bureau d'études seront sélectionnés selon la Méthode « **Sélection Fondée sur la Qualité et le Coût » (SFQC) telle que décrite dans le Règlement de Passation des Marchés pour les Emprunteurs sollicitant le Financement de Projets d'Investissement (FPI) de la Banque Mondiale, édition de Septembre 2025**. La langue de travail est le français et l'anglais. Il est également porté à l'attention des Consultants que les dispositions relatives aux règles de la Banque Mondiale en matière de conflit d'intérêts sont applicables.

8. CONTENU DES MANIFESTATIONS À ADRESSER AU PATNUC

Le Coordonnateur National du Projet d'Accélération de la Transformation Numérique au Cameroun (PATNUC) invite, en vue d'élaborer la liste restreinte, les consultants admissibles à manifester leur intérêt à fournir les services décrits ci-dessus. Les cabinets/groupement de cabinets intéressés doivent fournir les informations indiquant qu'ils sont qualifiés pour exécuter les services. Cette manifestation rédigée en français ou en anglais devra contenir :

- Une lettre de manifestation d'intérêt datée et signée ;

- La justification du statut juridique du consultant ;
- Les pièces justificatives du cabinet (copies des marchés similaires ou contrat, attestation de services fait, d'autres références du cabinet) permettant la vérification du profil du consultant tel que présenté ci-dessus.

9. CONTACT ET INFORMATIONS SUPPLÉMENTAIRES

Les dossiers doivent parvenir au plus tard 28 NOV 2025 à **16 heures :**

- Soit par courriel à : procurement@patnuc.cm avec copie à elsiddik22@gmail.com; janerosine@yahoo.fr L'offre doit être incluse dans un fichier unique avec le nom qui respecte la nomenclature suivante : {CONSULTANT}_{NumASMI}_{DATESOUMISSION].pdf Ex (Ex : CANON_ASMI000_10112025.pdf) ;
- Soit déposés sous pli fermé en cinq (05) exemplaires (un original et quatre copies) à l'Unité de gestion du Projet, à la nouvelle route Bastos, derrière Tradex, bâtiment Ancien SNV. Tél. : +237 222 232 628. (Coordonnées géographiques : 3.88433, 11.51239) portant la mention :

« AVIS DE SOLLICITATION A MANIFESTATION D'INTERET N°021 /ASMI/MINPOSTEL/PATNUC/UGP/MC2/SPM/2025 POUR LA SELECTION D'UN CONSULTANT EN VUE DE LA FORMATION SUR LA SECURITE INFORMATIQUE AUX AGENCES GOUVERNEMENTALES ».

Les termes de références de cette mission peuvent être retirés physique au niveau de l'Unité de Gestion du PATNUC, pendant les jours ouvrables entre 10h et 16h. Ils peuvent également être retirés en version numérique en adressant la demande par mail à l'adresse elsiddik22@gmail.com avec copie à procurement@patnuc.cm.

Yaoundé le, 12 NOV 2025

Le Coordonnateur National du PATNUC

Dr MEGUH Windfred FUAYE KENJI

Ampliations:
- PATNUC;
- ARMP;
- SOPECAM;
- ARCHIVES;
- AFFICHAGE.

CALL FOR EXPRESSIONS OF INTEREST No. 021/AMI/MINPOSTEL/PATNUC/UGP/MC2/SPM/2025 FOR THE SELECTION OF A CONSULTANT TO PROVIDE TRAINING ON IT SECURITY TO GOVERNMENT AGENCIES.

DATE: 12 NOV 2025

FUNDING : IDA 69870-CM

1. CONTEXT AND JUSTIFICATION

1.1. Context

The Government of Cameroon has received a loan of USD 100 million from the World Bank to implement the Project for the Acceleration of Digital Transformation in Cameroon (PATNUC). PATNUC is overseen by MINPOSTEL and aims to increase digital inclusion and the use of digital agricultural solutions by smallholder farmers involved in targeted agricultural value chains. PATNUC thus embodies the digital transformation approach, targeting a highly strategic sector for Cameroon while proposing to reform the regulatory framework for the Information and Communication Technology (ICT) sector. This project, with its investment in connectivity and digital skills, supports interventions that leverage digital innovations to stimulate agricultural growth, ultimately contributing to improved livelihoods in rural areas.

PATNUC is structured around four components: (i) Strategy, public policy and digital regulation for digital inclusion and transformation; (ii) digital connectivity and inclusion; (iii) facilitating the implementation of data-driven digital solutions in the agricultural sector; and (iv) project management and citizen engagement. Through SND30, the government aims to truly kick-start the structural transformation of Cameroon's economy. Digital transformation will necessarily involve capacity building for the main digital players in the Cameroonian ecosystem. Component 1 of the project targets certain institutions active in the digital sector whose performance requires updating and the acquisition of new knowledge in the digital sector.

1.2. Justification of the mission

With a view to improving its performance, optimizing its processes and reducing human interaction, which is often a source of corruption, the Government of the Republic of Cameroon, under the enlightened leadership of the President of the Republic, has embarked on a vast program of digital transformation of the Cameroonian administration.

However, although the adoption of ICT is beneficial, it nevertheless carries significant risks related to cyber-attacks. It is with this in mind that, through Law No. 2010/012 on cybersecurity and cybercrime, ANTIC has been tasked, among other things, with ensuring the security of the cyber infrastructure of public and private structures, in particular through security monitoring and security audits.

Security audits of public administrations carried out on the basis of the ISO 27001 standard revealed more than 3,420 vulnerabilities at the organizational, physical and technical levels. An analysis of the root causes of these vulnerabilities shows that the lack of technical skills in cybersecurity among IT department staff in government departments and the lack of awareness among civil servants of digital hygiene rules are the main causes of the proliferation of cyber threats within public structures.

It is in this context that PATNUC plans to fund IT security training for these administrations within the framework of a program based on three main areas: cybersecurity governance, application security, and system and network security.
The purpose of this document is therefore to propose the terms of reference for a project aimed at building the operational capacities of technical staff in the IT departments of parastatal administrations (government agencies, public administrative institutions) in the area of cybersecurity.

2. OBJECTIVES OF THE MISSION

These TORS aim to enable technical staff in semi-public administrations to acquire practical skills enabling them to ensure the day-to-day security of their respective administrations' information systems.

Specifically, this will involve:

- Offer a practical training program based on certification programs in the field of cybersecurity governance. At the end of these training courses, learners should be able to develop and implement strategies and procedures based on technical standards developed by ANTIC and anchored in international standards.
- Offer an online platform to raise awareness among non-IT staff in selected government agencies about best practices in security and digital hygiene. This platform should be highly user-friendly with easily digestible content to facilitate learning. This platform could be based on the CSCU (Certified Secure Computer User) certification and for the monitoring of online certification training;
- Develop a teaching methodology focused on practice and the simulation of real attack and incident scenarios, in order to prepare government staff to respond effectively to cyber threats;
- Establish a training schedule that minimizes the impact on the day-to-day operations of government departments, while ensuring comprehensive training for all relevant staff.
- Ensure seamless logistical organization to enable government staff to focus fully on their learning and skills development.
- Mettre en œuvre une évaluation rigoureuse des compétences acquises, permettant de mesurer l'impact de la formation ;
- Propose recommendations for additional training, ensuring that learners' skills are continuously updated in line with constantly evolving threats;
- Provide learners with training materials, facilitating the application of the knowledge acquired in their daily tasks of protecting the national cyberspace;
- Report the results of the training to the various stakeholder administrations in a workshop;
- Achieve a high percentage of certified personnel across all administrations;
- Achieve a high percentage of administrations with an incident response plan (IRP) and an approved risk register;
- one hundred (100) staff from the IT departments of public administrations to develop and implement strategies and procedures based on technical standards developed by ANTIC and anchored in international standards;
- Ensure that attendance per participant and per module is greater than or equal to 90% (evidence: attendance sheets and lab connection logs);

- Ensure effective follow-up in order to achieve the minimum acceptable success rate of 70% within 120 days of each session (evidence: certificates/emails from organizations, completion of laboratories ≥ 85% evidence: platform reports, satisfaction ≥ 4/5 evidence: aggregated questionnaires);

- Lead three workshops for face-to-face staff training, one workshop to raise awareness among public administration staff, and one workshop to present the work and validate the final report (runbooks, evidence: signed minutes + documents).

3. SCOPE OF MISSION

The aim is to provide face-to-face training for 100 (one hundred) staff members from semi-public administrations and a maximum number of staff members online. The mission must also adopt an inclusive approach, taking into account gender, levels of responsibility and the diversity of the beneficiary government agencies. A scoping meeting will ensure that there is a common understanding of the mission and will provide guidance for the consultant to define the methodology.

4. EXPECTED RESULTS

At the end of these training courses, the expected outcomes are as follows:

- A practical training program based on certification programs **in the field of cybersecurity governance.** At the end of these courses, learners should be able to develop and implement strategies and procedures based on technical standards developed by ANTIC and anchored in international standards.
- A practical training course based on certification programs in the **field of application platform security.** At the end of these courses, learners should be able to ensure the security of IT applications throughout their life cycle, from design to operation.
- An online platform to raise awareness among non-IT staff in all government agencies about best practices in security and digital hygiene. This platform should be highly user-friendly with easily digestible content to facilitate learning. This platform could be modelled on the CSCU (Certified Secure Computer User) certification.
- A teaching methodology focused on practical training and simulation of real-life attack and incident scenarios is developed to prepare government staff to respond effectively to cyber threats.
- A training schedule is drawn up that minimizes the impact on day-to-day government operations while ensuring that all relevant staff receive comprehensive training.
- Flawless logistical organization is ensured to allow government personnel to focus fully on their learning and skills development.
- Implement a rigorous assessment of the skills acquired, enabling the impact of the training to be measured.
- Propose recommendations for additional training, ensuring that learners' skills are continuously updated in line with constantly evolving threats;
- Learners are provided with training materials, facilitating the application of the knowledge acquired in their daily tasks of protecting the national cyberspace;
- 100 staff members from the IT departments of public administrations capable of developing and implementing strategies and procedures based on technical standards developed by ANTIC and anchored in international standards;
  - An attendance rate of at least 90% per participant and per module is achieved;

- A success rate of at least 70% within 120 days of each session (evidence: certificates/emails from organizations, completion of laboratories ≥ 85% evidence: platform reports, satisfaction ≥ 4/5 evidence: aggregated questionnaires) is achieved;
- Three (03) workshops for face-to-face staff training, one (01) awareness-raising workshop for public administration staff and one (01) workshop to present the work and validate the final report and runbooks (evidence: signed minutes + documents) are organized;
- A workshop to present the mission is organized.

5. DURATION OF THE MISSION

The training program is scheduled to last for twelve (12) months and will be delivered in two stages: face-to-face and online.

6. CONSULTANT'S PROFILE

The selected consultant will be either a firm or a group of firms with expertise in cybersecurity and cybercrime.

They will be required to :

- Have qualified staff with certifications or equivalent qualifications in the various training modules, as well as the necessary material, software and logistical resources;
- Have knowledge and at least one (01) reference in cybersecurity training or academic master's programs in cybersecurity in Africa.

The consultant must also demonstrate experience with FIRST standards.

7. METHOD OF SELECTION

Consultants are advised that firms or groups of firms/consulting firms will be selected using the **'Quality and Cost-Based Selection' method " (QFBC) as described in the Procurement Regulations for Borrowers Seeking Investment Project Financing (IPF) from the World Bank, September 2025 edition.** The working languages are French and English. Consultants are also advised that the World Bank's rules on conflicts of interest apply.

8. CONTENT OF BIDS TO BE SUBMITTED AT PATNUC

The National Coordinator of the Project for the Acceleration of Digital Transformation in Cameroon (PATNUC) invites eligible consultants to express their interest in providing the services described above, with a view to drawing up a shortlist. Interested firms/consortia must provide information demonstrating that they are qualified to perform the services. This expression of interest, written in French or English, must contain:

- A dated and signed letter of expression of interest;
- Proof of the consultant's legal status;
- Supporting documents for the firm (copies of similar contracts or agreements, certificates of services rendered, other references for the firm) enabling verification of the consultant's profile as presented above.

9. CONTACT AND ADDITIONAL INFORMATION

Applications must be received by 4 p.m. on the 28 NOV 2025 at the latest:

- Either by email to: procurement@patnuc.cm with a copy to elsiddik22@gmail.com; janerosine@yahoo.fr . The bid must be included in a single file with a name that complies with the following nomenclature: {CONSULTANT}_{NumASMI}_{DATESOUMISSION].pdf Ex (e.g. CANON_ASMI000_10112025.pdf);

- Or submitted in a sealed envelope in five (05) copies (one original and four copies) to the Project Implementation Unit, at the Nouvelle Route Bastos road, behind Tradex, former SNV building.

Tel.: +237 222 232 628. (Geographical coordinates: 3.88433, 11.51239) marked as:

« CALL FOR EXPRESSIONS OF INTEREST No. 021 /ASMI/MINPOSTEL/PATNUC/UGP/MC2/SPM/2025 FOR THE SELECTION OF A CONSULTANT TO PROVIDE TRAINING ON IT SECURITY TO GOVERNMENT AGENCIES.».

The terms of reference for this mission can be obtained in hard copy from the PATNUC Management Unit on working days between 10 a.m. and 4 p.m. They can also be obtained in digital format by sending a request by email to elsiddik22@gmail.com with a copy to procurement@patnuc.cm

Yaoundé the, 12 NOV 2025

The National Coordinator of PATNUC

Dr. MBOH Windfred FUAYE KENJI

Ampliations:
- PATNUC;
- ARMP;
- SOPECAM;
- ARCHIVES;
- NOTICE BOARD.