

## MISSION D'EXPERTISE POUR LA CURATION ET LA CONCEPTION DE CONTENUS DE FORMATION AUX METIERS DE LA CYBERSECURITE POUR LA PLATEFORME EN LIGNE DU PROJET D-CLIC

| Termes de Référence pour la curation et la conception de contenus de formation en ligne<br>aux métiers de la cybersécurité pour la plateforme en ligne du projet « D-CLIC, formez-vous au<br>numérique avec l'OIF » |                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>Commanditaire</b>                                                                                                                                                                                                | Organisation internationale de la Francophonie (OIF)<br>Direction de la Francophonie économique et numérique (DFEN) |
| <b>Période</b>                                                                                                                                                                                                      | Août – Décembre 2025                                                                                                |

*Remarque : L'utilisation du masculin dans le présent document a pour seul but d'alléger le texte et s'applique sans discrimination de genre.*

### 1. Présentation du commanditaire

L'Organisation internationale de la Francophonie (OIF) est un organisme international de coopération multilatérale fondé en 1970, regroupant actuellement 93 États et gouvernements membres et observateurs partageant l'usage de la langue française. L'OIF est une personne morale de droit international public et possède une personnalité juridique, dont le siège est basé à Paris, France. Elle apporte à ses 93 États et gouvernements un appui dans l'élaboration ou la consolidation de leurs politiques et mène des actions de politique internationale, selon quatre grandes missions :

- Promouvoir la langue française, le plurilinguisme et la diversité culturelle
- Promouvoir la paix, la démocratie et les droits de l'Homme
- Appuyer l'éducation, la formation, l'enseignement supérieur et la recherche
- Développer la coopération économique au service du développement durable.

L'OIF met en œuvre sa coopération multilatérale francophone aux côtés des acteurs de la Charte de la Francophonie.

La nouvelle programmation quadriennale 2024-2027 de l'OIF est structurée suivant trois programmes stratégiques :

- Programme stratégique 1 : La langue française au service des cultures et de l'éducation
- Programme stratégique 2 : La langue française au service de la démocratie et de la gouvernance
- Programme stratégique 3 : La langue française, vecteur de développement durable

### 2. Contexte et justification

Dans le cadre de sa Programmation quadriennale 2024 - 2027, l'Organisation internationale de la Francophonie (OIF) a placé le numérique comme axe stratégique prioritaire pour le soutien aux initiatives des jeunes et des femmes francophones.

Le développement de nouveaux métiers du numérique adaptés à l'expansion des marchés afférents est l'un des corollaires de l'évolution de l'économie numérique, que tous les États et Gouvernements doivent prendre en considération dans la conception et la mise en œuvre de leurs politiques publiques en faveur de l'emploi. La réinvention d'une offre professionnelle adaptée à la transformation numérique de leurs économies devient, dès lors, un défi majeur pour les pouvoirs publics. Tous les pays francophones sont, d'ores et déjà, touchés par ces mutations du marché de l'emploi et l'explosion du secteur numérique.

L'axe d'intervention II de la Stratégie de la Francophonie Numérique (SFN) « ii. Améliorer l'acquisition des compétences numériques, en particulier par les jeunes, les femmes et les personnes en situation de vulnérabilité » traduit la volonté des Etats et Gouvernements membres de l'OIF d'agir dans le sens du renforcement des compétences numériques des populations francophones. C'est pourquoi, en cohérence avec ses missions et les demandes/besoins de ses États et Gouvernements, l'OIF a développé le projet « D-CLIC, formez-vous au numérique avec l'OIF » pour la formation des jeunes de 18 à 35 ans au numérique, notamment à ses métiers stratégiques.

Le projet mis en œuvre depuis 2021 ambitionne principalement :

- D'accompagner le renforcement des compétences numériques des populations francophones, afin de répondre aux évolutions rapides des sociétés, des marchés économiques et du monde du travail, et d'améliorer l'employabilité durable, en particulier pour les populations les plus vulnérables (jeunes, femmes, catégories socioéconomiques éloignées de l'emploi, etc.).
- D'accompagner les acteurs publics, les opérateurs de formation et les acteurs éducatifs dans la conception, la structuration, la mise en œuvre et le suivi-évaluation d'actions de renforcement des capacités et compétences numérique.

Le projet D-CLIC depuis son lancement a permis :

- De former en présentiel plus de 5 500 jeunes aux métiers du numérique dans dix-neuf (19) pays (Bénin, Burkina Faso, Djibouti, Cameroun, Comores, Congo, Congo RD, Côte d'Ivoire, Gabon, Guinée, Haïti, Madagascar, Mali, Mauritanie, Niger, Sénégal, Tchad, Togo et Tunisie) à travers des structures de formation locales (opérateurs de formation). Les formations se sont déroulées en format présentiel et hybride.
- De former en ligne plus de 6 000 jeunes aux métiers du numérique (Développement mobile, Développement web et Marketing numérique). Les formations se sont déroulées entièrement en ligne sur la plateforme de formation du projet D-CLIC. Elles ont été assurées par des tuteurs qualifiés.

Après 4 années de mise en œuvre, le projet a entamé sa phase de passage à l'échelle en 2025 avec une stratégie innovante et hybride pour une meilleure appropriation locale de ses initiatives et un renforcement de l'accompagnement des jeunes formés à l'insertion professionnelle. En complément du dispositif des formations en présentiel, le projet s'appuie sur une plateforme de formation en ligne pour toucher plus de bénéficiaires et de pays. Cette plateforme repose sur des contenus de formation qui pourront être mis à disposition de tout l'écosystème du projet.

Dans cette perspective et pour le renforcement de l'offre déjà disponible sur cette plateforme, l'OIF souhaite développer des contenus de formation **aux métiers de la cybersécurité**.

### 3. Objectifs de la mission

La Direction de la Francophonie économique et numérique (DFEN) de l'OIF recherche l'appui d'un expert capable de l'accompagner dans les objectifs stratégiques et opérationnels suivants :

#### 3.1. Définir des parcours de formation professionnalisants en cybersécurité :

Identifier et structurer deux (2) parcours de formation distincts et pertinents, alignés sur les besoins du marché de l'emploi en cybersécurité dans l'espace francophone, et spécifiquement adaptés au public cible du projet D-CLIC (jeunes de 18 à 35 ans) pour une insertion professionnelle rapide et durable.

#### 3.2. Concevoir et élaborer des contenus pédagogiques innovants :

Produire des contenus de formation professionnelle de haute qualité pour les deux (2) parcours de cybersécurité identifiés, en réalisant une analyse approfondie des cursus existants et des Ressources Éducatives Libres (REL) disponibles en français (sous licences Creative Commons CC BY, CC BY SA v4.0 ou équivalentes). Cette conception inclura également la rédaction des documents de cadrage pédagogique (synopsis, scénarisation détaillée, plans de déroulement et de séquençage des modules, fiches descriptives) et la production de ressources multimédias diversifiées (vidéos, animations, exercices interactifs, travaux pratiques). L'accent sera mis sur une approche par compétences favorisant la pratique, la mise en situation et l'autonomisation des apprenants.

### **3.3. Optimiser l'implémentation et l'interopérabilité des contenus :**

Assurer l'intégration technique des contenus de formation sur la plateforme Moodle du projet D-CLIC, en respectant scrupuleusement les standards d'affichage Moodle et les normes du e-learning (SCORM, LTI, etc.) pour garantir l'accessibilité, l'interopérabilité et la durabilité des ressources. L'utilisation d'outils libres (H5P, etc.) et une approche éco-conçue sont vivement encouragées.

### **3.4. Accompagner la montée en compétence des tuteurs :**

Fournir un soutien et une formation aux tuteurs chargés du suivi des apprenants et de l'animation des formations, en leur fournissant les outils pédagogiques et méthodologiques nécessaires pour un encadrement efficace.

### **3.5. Piloter et évaluer l'expérience de formation :**

Mettre en place un dispositif de suivi et d'évaluation de la phase pilote des formations, afin de mesurer l'atteinte des objectifs d'apprentissage et d'identifier les axes d'amélioration pour une actualisation continue des contenus. Définir une approche et une temporalité de mise à jour des contenus pour assurer leur pertinence à long terme.

### **3.6. Favoriser l'inclusion et l'adaptabilité technologique :**

Veiller à ce que les contenus soient adaptés à des environnements de faible connectivité, aux usages du téléphone mobile, et qu'ils intègrent les innovations technologiques pertinentes, y compris l'Intelligence Artificielle, tout en étant accessibles aux personnes malentendantes et malvoyantes. Les contenus devront être neutres en genre et tenir compte de la diversité culturelle et géographique de l'espace francophone.

## **4. Description des tâches**

L'expert retenu travaillera sous la supervision de l'équipe-projet de la Direction de la Francophonie économique et numérique (DFEN) de l'OIF à Paris et aura pour principales missions :

### **4.1. Ingénierie pédagogique et définition des parcours de formation en Cybersécurité :**

**4.1.1. Analyse approfondie de l'existant et identification des métiers :** Mener une analyse exhaustive des cursus et contenus de formation existants en cybersécurité, spécifiquement ceux disponibles en français et sous licences Creative Commons (CC BY, CC BY SA v4.0 ou apparentées), identifiant les forces, faiblesses et lacunes au regard des besoins du marché de l'emploi dans l'espace francophone. Cette analyse ciblera la définition de deux (2) métiers de la cybersécurité porteurs d'opportunités d'emploi pour le public cible du projet D-CLIC.

**4.1.2. Conception des parcours et référentiels de formation :** Sur la base des résultats de l'analyse, identifier et définir de manière précise deux (2) parcours de formation en cybersécurité. Pour chaque parcours, élaborer un référentiel de formation complet, en privilégiant une Approche par compétences (APC) ou toute autre approche pédagogique active favorisant la pratique, la mise en situation réelle et l'autonomisation des apprenants. Ce référentiel devra inclure, sans s'y limiter : les prérequis détaillés, la durée estimée en jours et en heures (entre 2 et 6 mois maximum par parcours pour une formation courte en ligne), un plan de formation structuré, un séquençage pédagogique détaillé, les programmes de cours, les compétences visées, et les modalités d'évaluation des apprenants.

#### **➤ Critères impératifs pour les référentiels :**

- Rédigés en français et adaptés aux réalités contextuelles et à la diversité culturelle et géographique de l'espace francophone.
- Conçus pour les jeunes de 18 à 35 ans (diplômés en reconversion, non-diplômés, défavorisés, sans emploi), visant une employabilité directe ou le développement de compétences spécifiques en cybersécurité.
- Intégrant des mécanismes d'évaluation clairs des connaissances et compétences acquises.

- Parfaitement adaptés à un apprentissage à distance (e-learning) ou hybride, et favorisant l'auto-apprentissage.
- Éco-conçus et intégrant au maximum des outils libres (ex : H5P pour les activités interactives).
- Neutres et ne reproduisant aucun stéréotype de genre.
- Adaptés à la fois à l'autoformation et à la formation tutorée par des encadrants.
- Intégrant les spécificités de la cybersécurité dans le contexte africain francophone (menaces, cadre légal, infrastructures, etc.).

## **4.2. Rédaction et production des contenus pédagogiques :**

### **4.2.1. Production de contenus originaux et adaptés :**

- Rédiger des contenus de formation originaux, décomposables en plusieurs micromodules/séquences d'apprentissage, répondant aux critères suivants :
  - Rédigés en français et contextualisés aux réalités et à la diversité de l'espace francophone.
  - Directement pertinents pour le profil des jeunes de 18 à 35 ans et orientés vers l'acquisition de compétences opérationnelles pour les métiers visés.
  - Impérativement sous licence Creative Commons CC BY SA – Attribution – Partage dans les mêmes conditions 4.0 International pour favoriser le libre partage et la réutilisation.

### **4.2.2. Intégration de contenus existant (curation) :**

- Pour les contenus existants non produits par l'expert, s'assurer qu'ils sont exclusivement sous licences Creative Commons 4.0 International (CC BY, CC BY SA) ou dans le domaine public, et les intégrer de manière cohérente au cursus, avec des adaptations si nécessaire.

### **4.2.3. Diversification des formats et accessibilité :**

- Développer les contenus sous divers formats multimédias (vidéos, animations graphiques/motion design, éléments de ludification, etc.) ou tout autre support favorisant un apprentissage à distance ou hybride engageant.
- Prendre en compte l'usage prédominant du téléphone mobile en Afrique pour la connexion, les réseaux sociaux numériques et les applications de messagerie.
- Intégrer les innovations technologiques, notamment l'Intelligence Artificielle, pour améliorer l'apprentissage (ex : chatbots pédagogiques, outils d'analyse de progression, etc.).
- Assurer une facile adaptabilité à des solutions numériques utilisables avec un faible niveau de connexion.
- Rendre les contenus accessibles aux personnes malentendantes et malvoyantes (sous-titres, descriptions audio, contrastes, etc.).
- Concevoir spécifiquement les contenus pour des formations tutorées, tout en permettant l'autoformation.

## **4.3. Curation et classification de ressources éducatives libres (REL) :**

### **4.3.1. Constitution d'une base de données de REL :**

- Identifier, classer et curer des ressources éducatives libres (REL) pertinentes et de qualité, disponibles en ligne sur les métiers de la cybersécurité.

### **4.3.2. Respect des licences :**

- S'assurer que ces REL sont exclusivement sous licences Creative Commons 4.0 International (CC BY, CC BY SA ou apparentées) ou tombées dans le domaine public.

## **4.4. Implémentation, accompagnement et suivi :**

**4.4.1. Implémentation technique sur Moodle :** En étroite collaboration avec l'ingénieur de formation en charge de la plateforme Moodle, mettre en ligne les contenus de formation. Effectuer des tests rigoureux, des corrections et organiser un atelier de validation en ligne avec des publics invités pour assurer la qualité et la conformité des contenus.

#### 4.4.2. Formation et accompagnement des tuteurs :

- Concevoir et réaliser des sessions de formation et des documents spécifiques pour les tuteurs afin de les préparer à l'animation et au suivi des apprenants sur les parcours de cybersécurité.

4.4.3. Suivi, évaluation et maintenance des contenus : Assurer le suivi et l'évaluation de la phase pilote de la formation. Rédiger un rapport d'évaluation détaillé. Définir une approche et une temporalité claires pour la mise à jour et l'actualisation régulière des contenus afin de garantir leur pertinence continue face à l'évolution rapide de la cybersécurité.

### 5. Résultats et livrables attendus :

L'expert devra produire les livrables suivants, en veillant à leur qualité, leur conformité aux standards mentionnés et leur adéquation aux objectifs de la mission :

#### 5.1. Livrables d'ingénierie pédagogique et de cadrage :

- Un rapport d'analyse de l'existant et de proposition des deux (2) parcours de formation en cybersécurité, incluant une justification détaillée du choix des métiers ciblés au regard des besoins du marché de l'emploi en Afrique francophone.
- Pour chaque parcours identifié, un référentiel de formation complet et détaillé (incluant prérequis, durée, plan de formation, séquençage pédagogique par compétences, et modalités d'évaluation).
- Des documents de cadrage pédagogique par module/micromodule : synopsis, scénarisation pédagogique détaillée (incluant objectifs spécifiques, activités d'apprentissage, ressources associées, modalités d'évaluation formative et sommative), et fiches descriptives complètes des modules.
- Un plan détaillé d'intégration des outils libres (ex: H5P) et des principes d'éco-conception dans les contenus.

#### 5.2. Contenus de formation produits et curatés :

Deux (2) ensembles complets de contenus pédagogiques de formation professionnelle en cybersécurité, décomposables en micromodules/séquences d'apprentissage, produits selon les référentiels validés. Ces contenus devront inclure :

- Textes de cours, supports de présentation (diaporamas), exercices interactifs, quiz, études de cas, travaux pratiques et projets.
- Ressources multimédias enrichies : scripts et productions de vidéos pédagogiques, animations graphiques (motion design), éléments de ludification, etc., adaptés à l'apprentissage à distance et mobile.
- Scripts d'introduction et de conclusion pour chaque module/séquence.
- Une base de données structurée et classifiée de ressources éducatives libres (REL) pertinentes, libres et ouvertes (réutilisables, reproductibles et modifiables librement), identifiées et curatées dans le domaine de la cybersécurité, avec les licences Creative Commons (CC BY, CC BY SA v4.0 ou apparentées) clairement indiquées pour chaque ressource.

#### 5.3. Livrables techniques et d'accompagnement :

- Les contenus de formation implémentés et testés sur la plateforme Moodle du projet D-CLIC, conformes aux standards d'affichage Moodle et aux normes du e-learning (SCORM, LTI, etc.) pour assurer l'accessibilité, l'interopérabilité et la durabilité des contenus.
- Un rapport de test et de validation technique des contenus sur la plateforme.
- Un atelier de validation en ligne des contenus avec des publics invités.

- Un guide pédagogique et des supports de formation spécifiques à l'attention des tuteurs/encadrants, incluant les méthodes d'animation et de suivi des apprenants.
- Un rapport d'évaluation de la phase pilote de la formation, incluant les retours des apprenants et des tuteurs, et des recommandations d'amélioration.
- Une proposition détaillée d'approche et de temporalité pour l'actualisation et la maintenance régulière des contenus de formation.

#### **5.4. Conditions générales des livrables :**

- Tous les livrables devront être produits en langue française.
- Les exemples et cas pratiques intégrés dans les contenus devront s'inspirer concrètement des environnements et réalités des pays de la Francophonie, notamment africains.
- L'ensemble des contenus originaux produits par l'expert devra être sous licence Creative Commons CC BY SA – Attribution – Partage dans les mêmes conditions 4.0 International.
- Les livrables devront garantir une intégration maximale des outils libres et respecter les principes d'éco-conception.
- Les livrables ne devront pas reproduire de stéréotypes de genre.

### **6. Profil de l'expert :**

L'expert recherché sera un professionnel de haut niveau, idéalement international, combinant une expertise technique pointue et des compétences pédagogiques avérées. Il devra impérativement démontrer les qualifications et expériences suivantes :

#### **6.1. Qualifications académiques et professionnelles :**

- Être titulaire d'un diplôme universitaire supérieur (Bac+5 minimum) dans un domaine pertinent (Informatique, Cybersécurité, Télécommunications, Ingénierie Pédagogique, Sciences de l'Éducation, ou équivalent).
- Posséder des certifications reconnues en cybersécurité (ex : CISSP, CompTIA Security+, CEH, GIAC, ISO 27001, etc.) serait un atout majeur et devra être clairement mentionné dans le CV.
- Avoir des certifications ou formations complémentaires en ingénierie pédagogique, e-learning, ou conception de parcours digitaux est fortement souhaité.

#### **6.2. Expérience professionnelle spécifique :**

- Avoir une expérience avérée d'au moins 7 ans dans la conception, la rédaction et/ou la curation de contenus de formation professionnelle en cybersécurité, notamment pour des publics jeunes et en contexte de formation en ligne.
- Démontrer une expérience significative (au minimum 3 réalisations) dans la conception et le déploiement de curricula de formation professionnelle dans le domaine du numérique, en particulier ceux orientés vers l'employabilité et l'acquisition de compétences techniques concrètes.
- Avoir une expérience prouvée dans la curation de ressources éducatives libres (REL) et la maîtrise de leurs licences (Creative Commons).
- Une expérience en formation de formateurs/tuteurs ou en accompagnement pédagogique est un atout.
- Avoir participé à des projets de formation numérique ou de développement de compétences dans des pays d'Afrique francophone ou des contextes similaires est fortement apprécié et devra être détaillé.

#### **6.3. Compétences techniques et pédagogiques :**

- Maîtrise approfondie des concepts, outils et enjeux actuels de la cybersécurité (analyse de vulnérabilités, gestion des risques, sécurité des systèmes et réseaux, cyberdéfense, cryptographie, forensique numérique, etc.).
- Excellente connaissance de l'Approche par Compétences (APC) et des méthodes pédagogiques actives, innovantes et participatives (apprentissage par projet, résolution de problèmes, gamification).

- Forte capacité à concevoir des contenus adaptés à des publics variés (jeunes diplômés en reconversion, non-diplômés, défavorisés) et à des contraintes techniques (faible bande passante, usage mobile).
- Compétences avérées en écriture scénaristique pédagogique pour le e-learning et production de supports didactiques multimédias.
- Compréhension des enjeux liés à l'Intelligence Artificielle et capacité à l'intégrer, le cas échéant, comme outil pédagogique ou comme sujet d'étude pertinent dans les modules.
- Familiarité avec les plateformes d'apprentissage en ligne (LMS) comme Moodle et les normes SCORM.

#### **6.4. Compétences transversales :**

- Très grandes capacités rédactionnelles en français, avec une aptitude à vulgariser des concepts techniques complexes pour des publics variés.
- Capacités d'animation et de communication efficaces, y compris pour des interactions à distance et via divers canaux multimédias.
- Sens aigu de l'adaptabilité, de la proactivité et de l'autonomie.
- Excellente connaissance des spécificités culturelles et socio-économiques des pays africains francophones.
- Capacité à travailler en étroite collaboration avec une équipe à distance.

#### **7. Calendrier indicatif de la prestation**

La mission sera réalisée entre *août et décembre 2025*. Une réunion de lancement permettra de la préciser. L'expert retenu travaillera en étroite collaboration avec les membres de l'équipe de la DFEN en charge du projet.

La DFEN mettra à la disposition de l'expert toutes les informations et documents disponibles nécessaires à l'accomplissement de la mission.

#### **8. Durée et calendrier indicatif de la prestation**

- Le temps nécessaire au développement des contenus de formation pour deux métiers de cybersécurité est estimé entre 50 et 70 jours (à confirmer par l'expert en fonction de sa compréhension de la demande et de la méthodologie préconisée). À noter que l'Organisation internationale de la Francophonie possède une grille interne de rémunération en fonction de l'expérience des expert(e)s, de la durée et de la complexité de la mission confiée. Les éléments financiers seront donc discutés individuellement pour chaque profil ;
- Sur les plans opérationnel et méthodologique, aucun déplacement n'est à prévoir. L'expert travaillera depuis son lieu de résidence / travail.

#### **9. Constitution du dossier**

- Un curriculum vitae détaillé, démontrant que le candidat possède les qualifications, expériences et aptitudes pertinentes pour la mission, avec la mention d'au moins trois références professionnelles que l'OIF se réserve le droit de contacter ;
- Une liste détaillée des prestations similaires et expériences de missions comparables ;
- Une proposition financière (en jours-homme travaillés) ;
- Une note présentant la compréhension de la mission, la méthodologie proposée et le planning d'exécution (15 pages au maximum).

Le dossier de candidature doit être envoyé au plus tard le 24 août 2025 à 23h59 (heure de Paris) par courrier électronique à l'adresse : [appels.dclic@francophonie.org](mailto:appels.dclic@francophonie.org) avec la référence ci-après en objet : Nom & Prénoms / D-CLIC/02 Cybersécurité.