Programme des Nations Unies pour le développement

IC NOTICE N°036/2021/PNUD-BFA

Recrutement d'un Consultant Régional pour la fourniture de services de formation en cybercriminalité.

Date : 23 aout 2021
Agence : UNODC
Pays : Burkina Faso
Durée de réalisation : 22 jours ouvrés
Lieu d'affectation : Ouagadougou

Votre soumission devra être déposée à l'adresse suivante :
Par email : offres.burkina@undp.org

Au plus tard : **7 septembre 2021 à 12 heures**

Les propositions, adressées à l'Operations Manager, doivent être envoyées à l'adresse e-mail ci-dessus indiquée, avec la mention « **IC NOTICE N°033-2021/PNUD -BFA : Recrutement d'un Consultant Régional pour la fourniture de services de formation en cybercriminalité.**
Les termes de références sont disponibles sur le site du PNUD Burkina à l'adresse : http://www.bf.undp.org/content/burkina_faso/fr/home/operations/procurement.html

La proposition technique devra comprendre : **Une brève présentation de l'approche méthodologique et de l'organisation de la mission envisagée, une note de compréhension des TDRs, un curriculum vitae incluant au moins deux (02) références avec les adresses Emails.**
La proposition financière devra être élaboré suivant le format fourni en annexe.
Les demandes de clarifications devront être transmises uniquement par écrit à l'adresse suivante : procurement.burkina@undp.org

Contexte et Justification

La pandémie de la COVID-19 a favorisé l'augmentation considérable de la cybercriminalité qui est en pleine expansion. La fraude en ligne, l'extorsion de fonds et les abus sexuels d'enfants en ligne ciblent des individus, alors que les rançongiciels, compromettent essentiellement les systèmes, y compris ceux des hôpitaux. Alors que les gouvernements continuent d'être la cible de logiciels malveillants, la propagation croissante de la désinformation et des informations erronées continuera à semer la confusion dans l'esprit du public et à saper la réponse scientifique. Le télétravail a augmenté le nombre de victimes potentielles de la cybercriminalité. Les personnes prennent de plus grands risques en ligne à la maison, exposant ainsi par inadvertance le système informatique des entreprises aux cybercriminels. L'hameçonnage continue de permettre aux criminels et aux autres spécialistes, un accès malveillant à des systèmes critiques.

Qualification :

Formation	Un diplôme universitaire supérieur en Informatique, en application de la loi ou dans un domaine connexe est requis.

Expérience professionnelle :	• Une expérience préalable de 5 ans dans le domaine de la formation ou l'enseignement de la lutte contre la cybercriminalité ou dans la gestion des preuves numériques est requise. • Un minimum de 10 ans d'expérience professionnelle en informatique plus précisément en investigation numériques et en criminalistique est exigée. • Une connaissance approfondie de toutes les questions de justice pénale et de cybercriminalité, notamment en gestion des preuves numériques est requise. • Une expérience professionnelle dans le domaine de la cybercriminalité est un avantage. • Une expérience antérieure de travail en Afrique occidentale ou centrale ou dans d'autres pays en développement est un avantage.

Evaluation

L'évaluation des Propositions Techniques et Financières se déroule en deux étapes. L'évaluation des propositions techniques est achevée avant l'ouverture et la comparaison des propositions financières.

a. *Les propositions techniques*

La sélection sera faite sur la base des critères notés sur 100 comme suit :

Critères de sélection	Grille de notation
Niveau académique	20 points
Compréhension des TdR, méthodologie et chronogramme	30 points
Expérience professionnelle générale	25 points
Expérience dans le domaine de la formation	25 points
Total	100 points

b. *Les propositions financières*

La proposition financière est évaluée selon la formule suivante :

Note financière A = [(Offre financière la moins disante) /Offre financière de A] x 30

Seuls les consultants ayant obtenu une note technique d'au moins 70 points/100, verront leurs offres financières ouvertes. Cette note technique sera pondérée à 70% et la note financière pondérée à 30%.

Le/la Consultant (e) fait sa proposition financière suivant le Tableau des coûts. Il doit proposer un montant forfaitaire et présenter dans le Tableau des coûts la ventilation de ce montant forfaitaire. Le/la Consultant (e) avec le cumul de notes (Technique pondérée + Financière) le plus élevé sera retenu pour la consultation.

Durée du contrat

La durée totale de la consultation est de **22 jours ouvrés**

NB : Les candidatures féminines sont fortement encouragées.

Laouali Sanou
Operations Manager a.i

Signature : Date :

Immeuble des Nations Unies, Koulouba 01 BP 575 Ouagadougou 01 – Tél : (226) 25.49.06.00 – Email : registry.bf@undp.org - Burkina Faso -

TERMES DE REFERENCE

I. Job Information	
Title	Consultant Régional pour la fourniture de services de formation en cybercriminalité
Number of Position :	01
Level of Position :	Regional
Nature of the consultancy (Support / Substance) :	Substance
Type of Contract and Grade:	Contrat retainer
Duty Station or home-based:	Home-based
Working days	22 jours ouvrés
Duration:	1er Novembre 2021 – 31 Décembre 2021
Estimated starting date:	1er Novembre 2021
Fee range:	D

II. Contexte and Objectif
La pandémie de la COVID-19 a favorisé l'augmentation considérable de la cybercriminalité qui est en pleine expansion. La fraude en ligne, l'extorsion de fonds et les abus sexuels d'enfants en ligne ciblent des individus, alors que les rançongiciels, compromettent essentiellement les systèmes, y compris ceux des hôpitaux. Alors que les gouvernements

Immeuble des Nations Unies, Koulouba 01 BP 575 Ouagadougou 01 – Tél : (226) 25.49.06.00 – Email : registry.bf@undp.org - Burkina Faso -

continuent d'être la cible de logiciels malveillants, la propagation croissante de la désinformation et des informations erronées continuera à semer la confusion dans l'esprit du public et à saper la réponse scientifique.

Le télétravail a augmenté le nombre de victimes potentielles de la cybercriminalité. Les personnes prennent de plus grands risques en ligne à la maison, exposant ainsi par inadvertance le système informatique des entreprises aux cybercriminels. L'hameçonnage continue de permettre aux criminels et aux autres spécialistes, un accès malveillant à des systèmes critiques.

Le nombre d'agents des forces de l'ordre spécialisés dans la lutte contre la cybercriminalité est réduit pendant la majeure partie de l'année 2020. Cela entraîne une augmentation de la cybercriminalité à court terme et une difficulté pour les victimes à obtenir réparation. Cela favorise également l'augmentation de toutes autres sortes de crimes connexes (trafic de drogues, d'armes et de personnes, crimes de la faune, criminalité maritime, etc.), facilités par l'augmentation considérable du nombre de personnes connectées à Internet, aussi bien celles qui sont familières à son utilisation que celles qui ne le sont pas. En plus, étant donné que tout le monde possède désormais des appareils électroniques qui peuvent contenir beaucoup de preuves permettant d'innocenter ou de condamner des prévenus.

Par l'intermédiaire de son Bureau régional pour l'Afrique de l'Ouest et du Centre (ROSEN), basé au Sénégal, et de ses bureaux nationaux basés dans la région, l'ONUDC aide les gouvernements nationaux d'Afrique de l'Ouest et du Centre à lutter efficacement contre la criminalité transnationale organisée. Pour ce faire, il renforce les capacités institutionnelles et humaines des agents d'application de la loi, améliore les cadres juridiques et politiques, renforce la collecte de données et la recherche, et crée des mécanismes de coordination régionale. L'ONUDC a développé divers outils d'assistance technique qui visent à aider les États à mettre en œuvre les instruments juridiques internationaux. Cela comprend des ateliers de formation, du mentorat, des manuels de formation spécialement conçus pour les acteurs de l'application de la loi et les officiers de justice, des lois modèles et des systèmes de collecte de données.

Avec l'augmentation considérable des cybercrimes, Il devient urgent de renforcer les capacités d'enquête sur la cybercriminalité des services d'application de la loi d'Afrique de l'Ouest. Des techniques telles que la criminalistique numérique permettent d'analyser de nombreux types de dispositifs et d'extraire des preuves numériques qui peuvent être utilisées pour soutenir des systèmes de justice pénale équitables et transparents

Toutefois, une connaissance minimale des enquêtes sur la cybercriminalité est primordiale pour commencer à améliorer véritablement les compétences des agents d'application de la loi de première ligne afin qu'ils sachent quelles peuvent être les sources possibles de preuves numériques sur une scène de crime ou pendant les enquêtes et qu'ils sachent comment les préserver pour que les spécialistes de la criminalistique numérique puissent les recueillir.

La consultation portera sur la formation des services d'application de la loi du Burkina Faso dans les domaines suivants :

Immeuble des Nations Unies, Koulouba 01 BP 575 Ouagadougou 01 – Tél : (226) 25.49.06.00 – Email : registry.bf@undp.org - Burkina Faso -

1. **Enquêtes de cybercriminalité**: Connaître les outils, procédures et techniques permettant de mener une enquête de cybercriminalité, depuis la scène de crime ou la plainte jusqu'à la présentation des preuves devant le juge.
2. **Mise en place du laboratoires de criminalistique numérique du Burkina Faso**: Connaissance des procédures opérationnelles de gestion d'un laboratoire numérique, maitrise des différents logiciels et équipements du laboratoire. Respect de la chaîne de conservation des preuves numériques et présentation de preuves numériques valables devant le juge.
3. **Formation de formateurs** : Former les agents les plus qualifiés des laboratoires numériques ou des membres des unités de lutte contre la cybercriminalité afin qu'ils puissent former leurs collègues et les nouveaux personnels qui rejoignent l'unité ou le laboratoire.
4. **Encadrement du personnel de laboratoire de criminalistique numérique :** Accompagner le staff du laboratoire dans la recherche de preuves numériques selon les méthodes appliquées dans les formations.

Le consultant fera également :

1. Des recommandations sur l'évolution du laboratoire dans les années à venir (capacité, logiciels, équipements, etc.)
2. Un rapport pour chaque formation effectuée indiquant le déroulement de la formation, le niveau de connaissance des apprenants avant et après la formation, et des suggestions pour un plan de formation

Pour obtenir les résultats attendus, le consultant travaillera en étroite collaboration avec l'équipe de projet de l'ONUDC basée à Dakar, au Sénégal. Il/Elle sera en liaison avec le coordonnateur de projet cybercriminalité pendant tout le processus pour s'assurer que les objectifs de la formation sont atteints

Les tâches pourront être effectuées à distance, avec des déplacements dans les pays d'Afrique de l'Ouest quand c'est possible et dans les autres pays participant à la mise en œuvre du Programme mondial de lutte contre la Cybercriminalité.

III. Fonctions and Responsabilités

Le consultant travaillera sous la supervision directe du Coordonnateur de Projet (Cybercriminalité) du Bureau régional de l'ONUDC pour l'Afrique de l'Ouest et du Centre (ROSEN).

Dans le cadre de cette mission, le consultant devra fournir les résultats suivants :

A. Organiser et conduire une formation avancée en présentiel sur la collecte, la recherche, la préservation et la présentation de preuves numériques en utilisant les logiciels et équipements disponibles (et à venir) du laboratoire.

- Dispenser une formation sur la criminalistique et la recherche de preuves numériques.

Immeuble des Nations Unies, Koulouba 01 BP 575 Ouagadougou 01 – Tél : (226) 25.49.06.00 – Email : registry.bf@undp.org - Burkina Faso -

- Rapports pendant et après la formation : préparer un rapport de formation, des tests de connaissance avant et après la formation, des rapports d'activité préliminaires et finaux de la formation à partager avec le coordonnateur de projet (Cybercriminalité).

B. Organiser et conduire une formation de formateurs sur la recherche de preuves numériques, la criminalistique numérique ou tout autre activité en rapport avec le bon fonctionnement d'un laboratoire de criminalistique numérique.

- Dispenser une formation de formateurs sur la criminalistique numérique aux agents les plus qualifiés des laboratoires numériques ou des membres des unités de lutte contre la cybercriminalité afin qu'ils puissent former leurs collègues et les nouveaux personnels qui rejoignent l'unité ou le laboratoire.

C. Encadrer et servir de mentor au personnel de laboratoire de criminalistique numérique.

- Accompagner le staff du laboratoire dans leurs activités quotidiennes (investigations, recherche de preuves numériques) pour les aider à appliquer les procédures opérationnelles, utiliser les logiciels et les équipements à leur disposition pour résoudre des cas réels.

IV. Détails des livrables et Chronologie

Les paiements seront effectués après chaque formation, sous réserve de l'achèvement satisfaisant des activités de renforcement des capacités et / ou de la présentation de rapports de mission en fonction des résultats suivants :

Livrable	Résultats	Nombre de jours	À accomplir avant le (date)
A	Organiser et conduire une formation avancée en présentiel sur la collecte, la recherche, la préservation et la présentation de preuves numériques en utilisant les logiciels et équipements disponibles (et à venir) du laboratoire	6 jours = 4 jours de formation + 1 jours de préparation + 1 jour d'édition des rapports	22 Novembre 2021
B	Organiser et conduire une formation de formateurs sur la recherche de preuves numériques, la criminalistique numérique ou tout autre activité en rapport avec le bon fonctionnement d'un laboratoire de criminalistique numérique.	6 jours = 4 jours de formation + 1 jours de préparation + 1 jour d'édition des rapports	10 December 2021
C	Accompagner le staff du laboratoire dans leurs activités quotidiennes (investigations, recherche de preuves numériques) pour les aider à appliquer les procédures opérationnelles, utiliser les logiciels et les équipements à leur disposition pour résoudre des cas réels	10 jours ouvrables	31 Décembre 2021

Immeuble des Nations Unies, Koulouba 01 BP 575 Ouagadougou 01 – Tél : (226) 25.49.06.00 – Email : registry.bf@undp.org - Burkina Faso -

V. Compétences recherchées

Les candidats devront manifester leur engagement envers les missions de l'ONUDC, faire preuve de sensibilité et d'adaptabilité aux différences de culture, de sexe, de religion, de race, de nationalité et d'âge.

Leur profil devra refléter les compétences suivantes :

Professionnalisme : Expertise de fond dans l'approche de programmation régionale et intégrée de l'ONUDC. Connaissance des domaines de fond avec de très bonnes compétences en matière de recherche et d'analyse. Être capable d'identifier et de contribuer à la résolution de problèmes/questions. Être fier de son travail et de ses réalisations ; faire preuve de compétence professionnelle et de maîtrise du sujet ; être consciencieux et efficace dans le respect des engagements, des délais et des résultats ; être motivé par des préoccupations professionnelles plutôt que personnelles ; fait preuve de persévérance face à des problèmes ou des défis difficiles ; reste calme dans les situations de stress.

Travail d'équipe : Bonnes compétences interpersonnelles et capacité à établir et à maintenir des partenariats et des relations de travail efficaces dans un environnement multiculturel, avec sensibilité et respect de la diversité, y compris l'équilibre entre les sexes.

Communication : Capacité à écrire de manière claire et concise et à communiquer efficacement à l'oral.

VI. Qualifications/Expertise sought

Formation	Un diplôme universitaire supérieur en Informatique, en application de la loi ou dans un domaine connexe est requis.

Immeuble des Nations Unies, Koulouba 01 BP 575 Ouagadougou 01 – Tél : (226) 25.49.06.00 – Email : registry.bf@undp.org - Burkina Faso -

Expérience professionnelle :	• Une expérience préalable de 5 ans dans le domaine de la formation ou l'enseignement de la lutte contre la cybercriminalité ou dans la gestion des preuves numériques est requise. • Un minimum de 10 ans d'expérience professionnelle en informatique plus précisément en investigation numériques et en criminalistique est exigée. • Une connaissance approfondie de toutes les questions de justice pénale et de cybercriminalité, notamment en gestion des preuves numériques est requise. • Une expérience professionnelle dans le domaine de la cybercriminalité est un avantage. • Une expérience antérieure de travail en Afrique occidentale ou centrale ou dans d'autres pays en développement est un avantage.
Langues requises :	Les langues de travail du Secrétariat des Nations Unies sont l'anglais et le français. Pour ce poste, une parfaite maîtrise du français est exigée. La maîtrise de l'anglais est un avantage.

VII. Indicators to evaluate the consultant's performance

Toutes les délivrables doivent satisfaire les standards du coordonnateur de projet cybercriminalité de l'ONUDC à Dakar, Sénégal, selon les critères suivants :

- Qualité des résultats soumis
- Compétence technique
- Respect des délais de livraison

VIII. Payment Milestones

Les paiements seront effectués après l'achèvement et/ou la présentation satisfaisante des produits/livrables .

Veuillez noter que le dernier paiement doit coïncider avec la fin du contrat et doit être identique aux phases de paiement dans la demande d'engagement du consultant/IC.

Immeuble des Nations Unies, Koulouba 01 BP 575 Ouagadougou 01 – Tél : (226) 25.49.06.00 – Email : registry.bf@undp.org - Burkina Faso -