Plan du cours

Titre	Cycle de vie, principes et bonnes pratiques pour l'élaboration et la mise en œuvre d'une stratégie nationale de cybersécurité
Modalité de la formation	Apprentissage en ligne et Exercice sur table
Dates	16 Janvier-31 Décembre 2023
Durée	Formation en ligne de 4 h Cours virtuel de 2 h *(uniquement pour les équipes nationales/régionales sur demande)*
Date limite d'inscription	22 Décembre 2023
Frais d'inscription	Gratuit
Description	La cybersécurité représente un défi complexe qui englobe plusieurs aspects différents, liés à la gouvernance, à la politique, à l'exploitation, à la technique et au juridique. La présente formation permet d'acquérir des connaissances générales pour aborder, organiser et hiérarchiser nombre de ces domaines selon des modèles, des cadres et d'autres références existants et bien établis. La présente formation porte sur des éléments permettant d'assurer la protection des aspects civils du cyberespace et, en tant que tel, couvre les principes généraux et les bonnes pratiques à prendre en compte lors de l'élaboration, du déploiement et de la gestion d'une stratégie nationale de cybersécurité. À cette fin, elle établit une distinction claire entre la "procédure", qui sera adoptée par les pays durant le cycle de vie d'une stratégie nationale de cybersécurité (lancement, inventaire et analyse, production, mise en œuvre, examens), et le "contenu", à savoir le texte qui figurera effectivement dans un document de stratégie nationale de cybersécurité. La présente formation ne couvre pas certains cas spécifiques tels que le développement de cybercapacités défensives ou offensives par les forces de défense militaire ou les services de renseignement d'un pays. La présente formation donne également une vue d'ensemble des principales composantes que les pays devront prendre en compte pour se préparer en termes de cybersécurité, en soulignant les aspects critiques que les gouvernements sont appelés à prendre en considération lorsqu'ils établissent leur stratégie nationale et leur plan de mise en œuvre. Enfin, la présente formation offre aux décideurs un aperçu global et de haut niveau des approches et applications existantes et renvoie à des ressources supplémentaires et complémentaires pouvant donner des informations sur des actions particulières menées au niveau national en matière de cybersécurité.

Code de la formation	23OS100128AFR-F

1. OBJECTIFS D'APPRENTISSAGE

L'objectif de cette formation est de donner aux dirigeants et aux décideurs nationaux les connaissances nécessaires pour développer une réflexion stratégique en matière de cybersécurité au niveau national. Cette formation permettra aux utilisateurs d'atteindre les objectifs d'apprentissage suivants:

- Se familiariser avec les principaux concepts et les principales définitions dans le domaine de la cybersécurité et acquérir des bases solides sur le fonctionnement de la cybersécurité au niveau national.
- Se familiariser avec le guide pour l'élaboration d'une stratégie nationale de cybersécurité.
- Connaître les cinq phases du cycle de vie d'une stratégie nationale de cybersécurité (lancement; inventaires et analyse; production; mise en œuvre; suivi et évaluation).
- Connaître les principes transversaux à prendre en considération pour élaborer une stratégie nationale de cybersécurité prospective et globale.
- Se familiariser avec les bonnes pratiques pertinentes en matière de cybersécurité et avec les manières possibles de les appliquer dans le contexte national.

2. RESULTATS ATTENDUS

À l'issue de la formation, les utilisateurs seront capables:

- de comprendre les principaux concepts et les principales définitions dans le domaine de la cybersécurité ainsi que le fonctionnement de la cybersécurité au niveau national;
- d'utiliser efficacement le guide pour l'élaboration d'une stratégie nationale de cybersécurité;
- de comprendre les cinq phases du cycle de vie d'une stratégie nationale de cybersécurité (lancement; inventaires et analyse; production; mise en œuvre; suivi et évaluation) et les manières possibles de les mettre en œuvre dans le contexte national;
- de comprendre les principes transversaux à prendre en considération pour élaborer une stratégie nationale de cybersécurité prospective et globale;
- de comprendre les bonnes pratiques pertinentes en matière de cybersécurité et les manières possibles de les appliquer dans le contexte national.

3. PUBLIC CIBLE

La présente formation est avant tout destinée aux décideurs chargés de l'élaboration d'une stratégie nationale de cybersécurité. Elle cible en second lieu toutes les autres parties prenantes des secteurs public et privé impliquées dans le développement et la mise en œuvre d'une stratégie, par exemple les fonctionnaires compétents, les autorités de réglementation, les forces de police, les fournisseurs de TIC, les opérateurs d'infrastructures essentielles, la société civile, les universités et les instituts de recherche. Cette formation pourrait également être utile aux différents acteurs de la communauté internationale du développement, qui fournissent une assistance en matière de cybersécurité.

4. CONDITIONS D'ENTREE

Aucune qualification ou expérience particulière n'est nécessaire pour suivre ce cours. Les utilisateurs sont invités à faire leur demande d'inscription sur la plate-forme de l'académie de l'UIT. L'équipe de l'UIT travaillant sur la cybersécurité traitera les demandes et confirmera la participation. Les décideurs chargés de l'élaboration d'une stratégie nationale de cybersécurité sont prioritaires.

5. CONTENU DU COURS

La formation est composée de quatre modules de cyberapprentissage et d'une mise en situation en ligne, reposant sur le guide pour l'élaboration d'une stratégie nationale de cybersécurité. Le contenu portera sur les sujets suivants:

- Module 0 Introduction: Ce module présente aux participants les principaux concepts et les principales définitions dans le domaine de la cybersécurité et leur permet d'acquérir des bases solides sur le fonctionnement de la cybersécurité au niveau national.
- Module 1: Ce module donne une vue d'ensemble des différentes phases de l'élaboration d'une stratégie, à savoir:
  - Lancement
  - Inventaires et analyse
  - Production de la stratégie nationale de cybersécurité
  - Mise en œuvre
  - Suivi et évaluation.
- Module 2: Ce module présente les principes transversaux qui aident à élaborer une stratégie nationale de cybersécurité prospective et globale, à savoir:
  - Vision
  - Approche globale
  - Approche inclusive
  - Prospérité économique et sociale
  - Droits humains fondamentaux
  - Gestion des risques et résilience
  - Instruments politiques
  - Encadrement, rôles et attribution des ressources
  - Environnement de confiance.
- Module 3: Ce module présente un ensemble d'éléments de bonnes pratiques susceptibles de rendre la stratégie globale et efficace, tout en permettant une adaptation au contexte national. Ces éléments de bonne pratique sont regroupés en des domaines d'intervention distincts comme suit:
  - Gouvernance
  - Gestion des risques de cybersécurité au niveau national
  - Préparation et résilience
  - Services d'infrastructures critiques et services essentiels
  - Renforcement des capacités et sensibilisation
  - Législation et réglementation
  - Coopération internationale.

- Mise en situation *(organisée pour les équipes nationales/régionales ayant formulé une demande)* : Les mises en situation virtuelles sont des séances de discussion lors desquelles les utilisateurs se réunissent dans une salle de classe virtuelle et ont la possibilité de tester les connaissances acquises dans le cadre d'exercices pratiques et de discussions dirigées. Ces mises en situation porteront sur le contenu de la formation ainsi que sur l'expérience pratique et les bonnes pratiques que les participants souhaiteront présenter.

6. AGENDA DU COURS

Session	Sujet	Exercices et interactions
Questionnaire initial	Notions de base relatives à la cybersécurité	À son propre rythme. S'il obtient la note minimale requise (24 bonnes réponses sur 30), l'utilisateur passe directement au Module 1. S'il n'obtient pas la note minimale, l'utilisateur devra suivre le Module 0 et réussir le test.
Module 0 + Questionnaire	Notions de base relatives à la cybersécurité	À son propre rythme (1 h). Il est obligatoire de suivre le module et de répondre correctement au questionnaire pour passer à l'activité suivante. S'il ne répond pas correctement au questionnaire (au moins 60% de bonnes réponses), l'utilisateur devra à nouveau suivre le module et répondre au questionnaire.
Module 1 + Questionnaire	Cycle de vie d'une stratégie nationale de cybersécurité	À son propre rythme (1 h). Il est obligatoire de suivre le module et de répondre correctement au questionnaire (au moins 60% de bonnes réponses), pour passer à l'activité suivante. S'il ne répond pas correctement au questionnaire, l'utilisateur devra à nouveau suivre le module et répondre au questionnaire.
Module 2 + Questionnaire	Principes pour l'élaboration d'une stratégie nationale de cybersécurité	À son propre rythme (1 h). Il est obligatoire de suivre le module et de répondre correctement au questionnaire (au moins 60% de bonnes réponses), pour passer à l'activité suivante. S'il ne répond pas correctement au questionnaire, l'utilisateur devra à nouveau suivre le module et répondre au questionnaire.
Module 3 + Questionnaire	Bonnes pratiques relatives à la stratégie nationale de cybersécurité	À son propre rythme (1 h). Il est obligatoire de suivre le module et de répondre correctement au questionnaire (au moins 60% de bonnes réponses), pour compléter la formation et recevoir le certificat de réussite. S'il ne répond pas correctement au questionnaire, l'utilisateur devra à nouveau suivre le module et répondre au questionnaire.
Exercice pratique *(uniquement pour les utilisateurs inscrits à la mise en situation virtuelle)*	Cycle de vie, principes et bonnes pratiques concernant la stratégie nationale de cybersécurité	À son propre rythme (hors ligne). L'exercice pratique est une activité préparatoire destinée uniquement aux utilisateurs inscrits à la mise en situation virtuelle. Lors de son inscription pour la mise en situation, l'utilisateur recevra un exercice pratique. Il devra rendre l'exercice fini au moins 5 jours avant la mise en situation. L'utilisateur doit obligatoirement rendre l'exercice dans les délais pour pouvoir participer à la mise en situation.
Mise en situation virtuelle *(la mise en situation virtuelle est organisée pour les équipes nationales/régionales sur demande)*	Cycle de vie, principes et bonnes pratiques concernant la stratégie nationale de cybersécurité	Classe virtuelle (2 h). Les classes virtuelles sont organisées pour les équipes nationales/régionales en ayant formulé la demande. Après avoir suivi les modules de cyberapprentissage, l'utilisateur dispose d'un délai d'un an pour s'inscrire à une mise en situation virtuelle. L'UIT organisera des sessions de mise en situation à intervalle régulier et les utilisateurs pourront choisir la date qu'il souhaite. Il

		est obligatoire de participer à la mise en situation pour valider la formation et recevoir l'attestation correspondante.

7. MODE D'ANIMATION PEDAGOGIQUE

La formation sera dispensée entièrement en ligne et associera différentes approches didactiques :

- **4 modules de cyberapprentissage à suivre à son propre rythme**: Les modules 0, 1, 2 et 3 sont des cours numériques à suivre à son propre rythme présentés sous la forme de diapositives associées à des informations et des supports pédagogiques (vidéo, audio et images). Ces modules font appel à la ludification avec des questionnaires, des simulations, des éléments à déplacer, etc. Ces modules sont à suivre à son propre rythme, ce qui laisse la possibilité aux utilisateurs de s'organiser de manière autonome pour suivre le cours et achever le module.
- **4 questionnaires numériques**: Chaque module comprend un questionnaire numérique de 30 questions au maximum permettant aux utilisateurs de tester leurs connaissances et leurs progrès. Les questionnaires comprennent différents types de questions (oui/non, questions à choix multiples, arborescences, éléments à déplacer, etc.).
- **1 exercice pratique** *(uniquement pour les utilisateurs inscrits à la mise en situation virtuelle)* : Une fois les modules de cyberapprentissage terminés, les participants inscrits à la mise en situation virtuelle, recevront un exercice pratique à faire de manière autonome et hors ligne. Cet exercice est composé d'un ensemble de questions théoriques et pratiques ouvertes portant sur le cycle de vie, les principes et les domaines d'intervention à prendre en compte pour élaborer une stratégie nationale de cybersécurité. Il n'y pas de réponses justes ou fausses à ces questions qui sont conçues pour: a) renforcer la planification stratégique; b) encourager l'esprit critique; c) sensibiliser au contexte national en matière de cybersécurité; d) encourager la résolution des problèmes; e) permettre de partager les enseignements tirés. Les participants devront rendre l'exercice fini au moins cinq jours avant la mise en situation en ligne.
- **1 mise en situation** : *Les mises en situation sont organisées pour les équipes nationales/régionales sur demande*. Les mises en situation virtuelles sont des séances de discussion lors desquelles les utilisateurs se réunissent dans une salle de classe virtuelle et ont la possibilité de tester les connaissances acquises dans le cadre d'un débat dirigé avec le groupe complet. Afin que les bénéfices soient maximums sur le plan de la formation, les mises en situation sont encadrées par des coordonnateurs de l'UIT qui seront présents pour contrôler le rythme et le déroulement de la mise en situation. Ces coordonnateurs encourageront également le débat et dégageront des discussions les sujets pertinents, les difficultés, les enseignements tirés, les solutions et les points à améliorer. Les discussions en ligne comprendront également des éléments interactifs et ludiques (sondage, tableaux blancs, etc.). La mise en situation se déroulera en ligne via la plate-forme Zoom.

8. EVALUATION ET NOTATION

Pour valider la formation, tous les participants devront réussir les éléments suivants:

- Questionnaire initial: La formation débutera avec un questionnaire initial comprenant jusqu'à 30 questions pour évaluer les connaissances des participants et leur compréhension de ce que sont la cybersécurité et une stratégie nationale de cybersécurité. S'il obtient la note minimale requise (60% de bonnes réponses), le participant passera directement au module 1. En revanche, un

participant n'ayant pas obtenu la note minimale requise devra à nouveau suivre le module 0 et répondre correctement à un questionnaire pour passer au module suivant.

- Questionnaires de fin de module: À la fin de chaque module, un questionnaire d'évaluation comprenant jusqu'à 30 questions permet d'évaluer les acquis des utilisateurs. Il est indispensable d'obtenir une note minimale à ce questionnaire (au moins 60% de bonnes réponses) pour passer au module suivant. Les utilisateurs n'obtenant pas cette note minimale devront à nouveau suivre le module et passer le test. Seuls les participants ayant réussi tous les questionnaires avec une note au dessus de 60% se verront attribuer le certificat de l'ITU.
- Exercice pratique: Uniquement les participants inscrits à la mise en situation virtuelle devront rendre l'exercice achevé au moins 5 jours avant la mise en situation virtuelle. Cet exercice n'est pas noté, mais le participant doit le finir et le soumettre dans les délais pour prendre part à la mise en situation.
- Mise en situation virtuelle: Les mises en situation virtuelle sont organisées pour les équipes nationales/régionales sur demande. Bien qu'il n'y ait pas d'évaluation lors de cette phase, il est attendu des participants qu'ils prennent activement part aux discussions et aux activités lors de la mise en situation (ludification, sondages, tableaux blancs, etc.).

9. COORDINATION DU COURS

Coordinateur du cours :	**Coordinateur UIT:**
Nom: Email :	Nom: Serge Zongo Email : serge.zongo@itu.int