|  |  |
| --- | --- |
| **Point de l'ordre du jour: PL 2** | **Révision 1 du  Document C23/93-F** |
| **14 juillet 2023** |
| **Original: anglais** |
|  |  |
| Contribution du Brésil (République fédérative du) | |
| ÉLABORATION DU PROGRAMME MONDIAL CYBERSÉCURITÉ (GCA) | |
| **Objet**  Le présent document vise à donner des orientations pour assurer la mise en œuvre de la grande orientation C5 du SMSI (Instaurer la confiance et la sécurité dans l'utilisation des TIC).  **Suite à donner par le Conseil**  Le Conseil est invité à **adopter** le projet de décision figurant en annexe.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **Références**  [Résolution 130](https://www.itu.int/en/council/Documents/basic-texts-2023/RES-130-F.pdf) (Rév. Bucarest, 2022) de la Conférence de plénipotentiaires – Renforcement du rôle de l'UIT dans l'instauration de la confiance et de la sécurité dans l'utilisation des technologies de l'information et de la communication.  Recommandation 3 du Groupe de travail de la plénière de la PP-22 (point 1.8 de l'ordre du jour – [Document PP‑22/206](https://www.itu.int/md/S22-PP-C-0206/en)): Programme mondial cybersécurité.  [Résolution 1332](https://www.itu.int/md/S19-CL-C-0137/en) du Conseil (C11, dernière mod. C19) – Rôle de l'UIT dans la mise en œuvre des résultats du SMSI et du Programme de développement durable à l'horizon 2030. | |

Contexte

**Informations et considérations générales concernant la révision 1: la présente révision 1 de la contribution du Brésil est le fruit d'ajustements et de modifications apportés sur la base des contributions informelles que le Brésil a reçues de différents États Membres depuis la publication du Document C23/93-F. Elle s'inscrit dans le cadre d'un effort visant à parvenir à un consensus.**

Le Brésil a soumis à la Conférence de plénipotentiaires de 2022 de l'UIT (PP-22) une contribution visant à modifier la Résolution 130 relative au renforcement du rôle de l'UIT dans l'instauration de la confiance et de la sécurité dans l'utilisation des technologies de l'information et de la communication, qui comporte une disposition particulière consistant à inviter les Membres (États Membres, Membres de Secteur et Associés) à prendre part au processus d'actualisation du cadre qu'offre le Programme mondial cybersécurité (GCA) ([Document PP-22/79(Add.1)](https://www.itu.int/md/S22-PP-C-0079/en)).

Au cours des travaux de la Conférence, il est apparu clairement que toute initiative relative au programme GCA était source de désaccord entre les membres. Plusieurs heures et plusieurs séries de discussions ont été consacrées à ce sujet, et le Brésil a toujours défendu sa position concernant la nécessité d'élaborer un document de base faisant consensus et établissant le programme GCA en tant que moyen de faire progresser les initiatives de l'UIT liées à la cybersécurité. Cette position n'était pas uniquement celle du Brésil, mais elle était partagée par de nombreux autres pays. Le Brésil reconnaît toutefois que plusieurs États Membres ont exprimé leur opposition.

La décision prise par la PP-22 a été d'approuver la recommandation ci-après du Groupe de travail de la plénière (point 1.8 du [Document PP-22/206](https://www.itu.int/md/S22-PP-C-0206/en)):

RECOMMANDATION 3: Programme mondial cybersécurité (GCA)

Le Groupe de travail de la plénière recommande que la Conférence de plénipotentiaires invite le Conseil à examiner les propositions des États Membres concernant le Programme mondial cybersécurité (GCA), son utilisation actuelle et sa possible évolution future. ([Document PP-22/188(Rév.1)](https://www.itu.int/md/S22-PP-C-0188/en))

Compte tenu de la discussion qui a été menée à la PP-22 et des échanges supplémentaires tenus entre les délégués, le Brésil a proposé d'inscrire à l'ordre du jour de la présente session du Conseil de l'UIT un point relatif à la cybersécurité dans le cadre de la Résolution 130 (Rév. Bucarest, 2022).

De cette manière, le Brésil entend réaffirmer l'importance de poursuivre et de faire progresser ces discussions qui peuvent être très profitables, en particulier pour les pays en développement.

Le Brésil prend note et se félicite de la contribution soumise à la 30ème réunion du Groupe consultatif pour le développement des télécommunications (GCDT) par le Danemark, la France, l'Allemagne, la Lituanie, les Pays-Bas, la Pologne, le Portugal, la Roumanie, l'Espagne, la Suède et le Royaume-Uni sur la mise en œuvre des Résolutions de l'UIT à l'appui de la cybersécurité: proposition d'exercice de cartographie. Le Brésil souscrit à la proposition du GCDT et estime qu'il s'agit d'une solution importante pour améliorer la transparence et l'efficacité des initiatives de l'UIT-D liées à la cybersécurité. Néanmoins, il est également important de souligner que cette proposition ne remet pas en cause le développement du programme GCA au niveau du Conseil. Le Brésil considère qu'il s'agit d'une initiative complémentaire qui contribuera au processus d'élaboration éventuel du programme GCA.

Concept

Compte tenu de ce qui précède, le Brésil souhaite présenter sa proposition concernant l'élaboration future du programme GCA, en réaffirmant que celle-ci est primordiale pour les travaux de l'UIT sur la cybersécurité, dans la mesure où le programme GCA constitue le cadre qui sert de base méthodologique pour l'Indice mondial de cybersécurité (GCI).

Le questionnaire concernant la cinquième édition de l'Indice mondial de cybersécurité (GCIv5) comprend 84 questions réparties selon 19 indicateurs se rapportant aux cinq piliers du programme GCA (cadre juridique, mesures techniques, mesures organisationnelles, mesures de renforcement des capacités et mesures de coopération). Les travaux concernant la cinquième édition de l'Indice GCI sont en cours et le questionnaire associé a été examiné par le Groupe de travail par correspondance dirigé par le Brésil à la fin de 2022 (ce groupe a été créé dans le cadre de la Question 3/2 de l'UIT-D – Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité).

Les questions relatives à l'Indice GCI ne font pas publiquement l'objet d'un désaccord, ce qui témoigne d'un consensus sur la nécessité d'adopter ces mesures spécifiques concernant les cinq piliers, afin de relever le défi que représente la cybersécurité, même si les mesures concernent un domaine qui ne relève pas du mandat de l'UIT (la cybercriminalité par exemple). Aucun État Membre ne s'est jamais opposé publiquement à l'inclusion de questions sur la cybercriminalité dans le questionnaire, compte tenu du rôle et du mandat de l'UIT.

Dans la mesure où le questionnaire relatif au programme GCA représente une liste de mesures qui doivent être mises en œuvre dans le cadre de chacun des cinq piliers (indépendamment du mandat de l'UIT) et étant donné que les membres n'ont exprimé aucune opposition concernant le contenu de chaque pilier, il semble naturel d'utiliser cette structure pour élaborer le cadre du programme GCA.

Dans ce contexte, le Brésil propose d'élaborer le cadre du programme GCA, en conservant les cinq piliers et en utilisant le questionnaire comme document de base pour ces travaux. De plus, outre la description du contenu de chaque pilier, sur la base des questions figurant dans le questionnaire, chaque thème devrait contenir une explication concernant le mandat de l'UIT sur la question et les activités/initiatives à cet égard. Si une mesure ne relève pas du mandat de l'UIT, il convient également d'indiquer les organisations/initiatives qui peuvent apporter un appui aux membres sur ce point spécifique.

Ces efforts permettront non seulement aux membres d'avoir une idée plus générale des capacités et des mesures à mettre en place, mais ils pourront aussi mieux cerner le mandat de l'UIT et identifier facilement les autres organisations susceptibles de les aider et de leur fournir des ressources dans différents domaines. Toutes ces informations sont regroupées au sein d'un document de synthèse cohérent.

Par conséquent, le Brésil invite les Membres du Conseil de l'UIT à examiner le présent document et son annexe comme un point de départ pour les discussions sur l'élaboration future du programme GCA.

**Annexe: 1**

ANNEXE

PROJET de nouvelle DÉCISION [...]

Sources d'information visant à aider les États Membres à renforcer leurs capacités en matière de cybersécurité et de cyberrésilience

Le Conseil de l'UIT,

considérant

*a)* La Résolution 130 (Rév. Bucarest, 2022) relative au renforcement du rôle de l'UIT dans l'instauration de la confiance et de la sécurité dans l'utilisation des technologies de l'information et de la communication;

*b)* la Résolution 45 (Rév. Kigali, 2022) de la Conférence mondiale de développement des télécommunications (CMDT) relative aux mécanismes propres à améliorer la coopération en matière de cybersécurité, y compris la lutte contre le spam;

*c)* la Résolution 50 (Rév. Genève, 2022) de l'Assemblée mondiale de normalisation des télécommunications (AMNT) relative à la cybersécurité;

*d)* la Recommandation 3 du Groupe de travail de la plénière de la Conférence de plénipotentiaires de 2022, par laquelle le Conseil est invité à examiner les propositions des États Membres concernant le Programme mondial cybersécurité (GCA), son utilisation actuelle et sa possible évolution future,

rappelant

*a)* que la cybersécurité est un élément fondamental de la sécurisation des infrastructures de télécommunication/TIC;

*b)* que le renforcement de la confiance et de la sécurité dans l'utilisation des TIC joue un rôle essentiel pour tirer parti des possibilités immenses qu'offrent les technologies numériques;

*c)* que pour améliorer la connectivité numérique, des efforts supplémentaires sont nécessaires afin de renforcer les capacités de sensibilisation concernant la cybersécurité et la cyberrésilience, ainsi que pour réduire les fractures numériques,

décide de charger le Secrétaire général, en étroite coopération avec les Directeurs des trois Bureaux

1 de mettre en place des sources d'information destinées aux États Membres comprenant notamment, dans le cadre de chaque pilier du Programme mondial cybersécurité:

a) des exemples de bonnes pratiques;

b) des sources répertoriant les conseils, l'assistance et les orientations fournis par l'UIT et d'autres organisations pertinentes afin de permettre aux pays de renforcer leurs capacités en matière de cybersécurité et de cyberrésilience;

c) des renseignements sur les programmes de renforcement des capacités proposés par l'UIT et d'autres organisations compétentes;

2 de tenir et de mettre à jour ces sources, afin de tenir compte des défis qui se font jour, des faits nouveaux et des nouvelles activités connexes de l'UIT, ainsi que des nouvelles activités menées par d'autres organisations susceptibles d'aider les membres à renforcer leurs capacités en matière de cybersécurité et de cyberrésilience.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_