2020

White paper series
**Édition 9**

# _ ÉDUCATION A LA _
# CYBERSÉCURITÉ

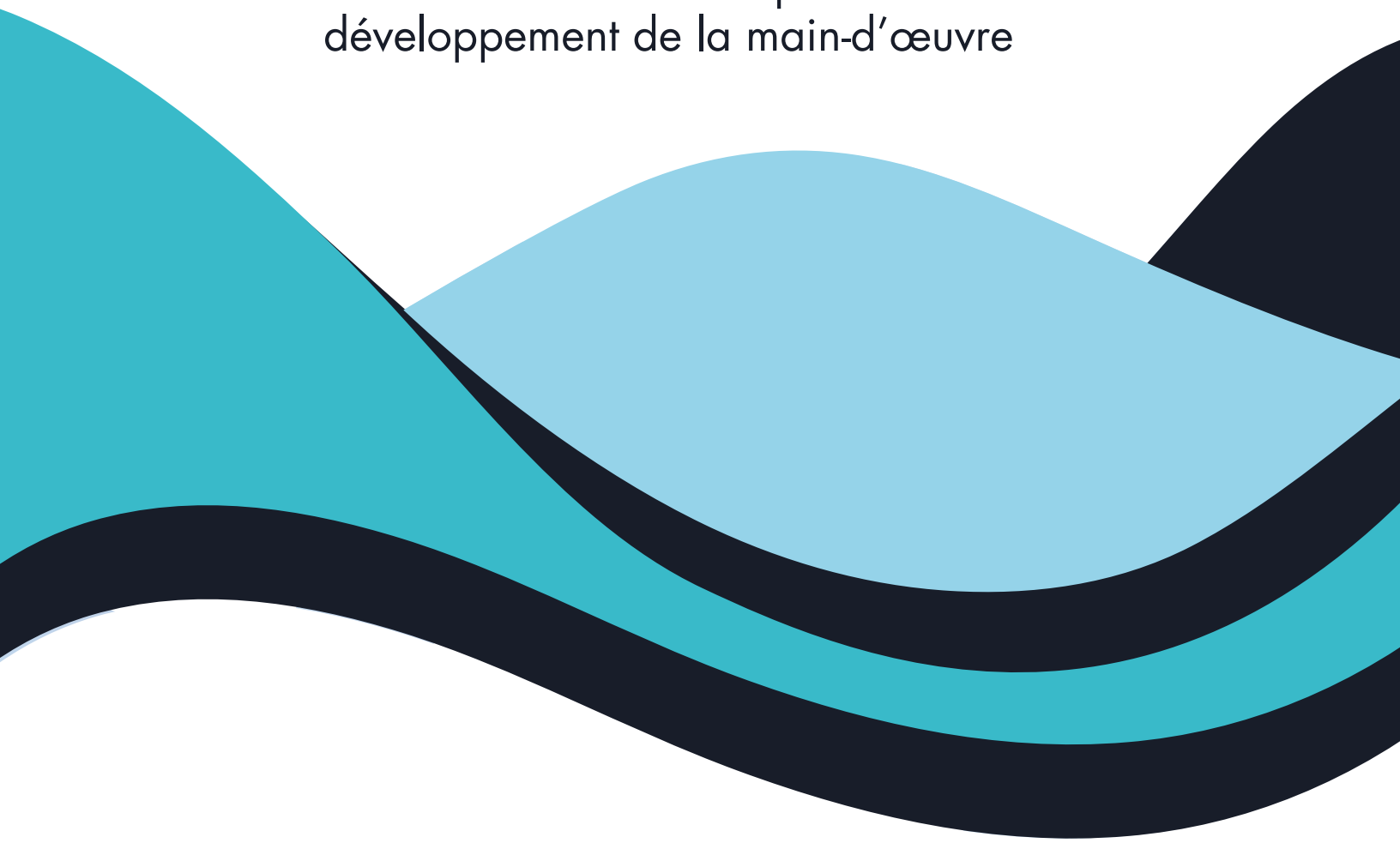
## Planifier l'avenir par le développement de la main-d'œuvre

OEA | Plus de droits pour plus de personnes

aws

# _ ÉDUCATION A LA _
# CYBERSÉCURITÉ

## Planifier l'avenir par le développement de la main-d'œuvre



Préparé et publié par le Programme de cybersécurité du Comité interaméricain contre le terrorisme (cybersecurity@oas.org).

# CRÉDITS


**Luis Almagro**
Secrétaire général
de Organisation des États
Américains (OEA)

**Équipe technique de l'OEA**
Farah Diva Urrutia
Alison August Treppel
Belisario Contreras
Kerry-Ann Barrett
Gabriela Montes de Oca Fehr
Babara Marchiori de Assis
Rolando Ramirez

**Équipe technique de AWS**
Abby Daniell
Melanie Kaplan
Jordana Siegel


_ ÉDUCATION A LA _
**CYBERSÉCURITÉ**
Planifier l'avenir par le
développement de la main-d'œuvre

# TABLE DES MATIÈRES

# _ ÉDUCATION A LA _
# **CYBERSÉCURITÉ**

Planifier l'avenir par le
développement de la main-d'œuvre

# Quel est l'objectif du présent document?

Face à l'accroissement du nombre d'activités nuisibles dans le cyberespace, il est nécessaire de compter sur une main-d'œuvre qualifiée en matière de cybersécurité. Les compétences que la main-d'œuvre doit maîtriser incluent l'habileté à concevoir et opérer de façon optimale des applications et des systèmes qui permettent d'identifier et de répondre aux cybermenaces, ainsi que d'élaborer des politiques publiques efficaces pour les contrecarrer. On ne pourra relever les défis de main-d'œuvre en matière de cybersécurité qu'en encourageant des cheminements professionnels centrés sur la cybersécurité. Le fossé entre le nombre disponible de professionnels spécialisés en cybersécurité et la demande de personnel qualifié sur le sujet exige une action immédiate pour former les praticiens actuels tout en mettant en œuvre des politiques qui outillent la prochaine génération de professionnels de la cybersécurité. À défaut d'adopter des politiques qui améliorent les compétences de leur main-d'œuvre en matière de cybersécurité, les pays ne peuvent tirer pleinement avantage de l'économie numérique. Le présent document aborde les étapes à suivre pour élaborer un Plan d'action en éducation à la cybersécurité (PAEC) qui inclue des mécanismes permettant d'intégrer l'éducation à la cybersécurité au développement de politiques et aux parcours académiques, et ainsi faire face à la pénurie de main-d'œuvre qualifiée en cybersécurité en Amérique latine et dans les Caraïbes. Il s'agit aussi d'une boîte à outils qui présente des initiatives et des moyens, au niveau national, pour susciter l'intérêt à faire carrière dans le domaine de la cybersécurité.

# _ ÉDUCATION A LA _
# **CYBERSÉCURITÉ**

Planifier l'avenir par le
développement de la main-d'œuvre

# Pourquoi l'éducation à la cybersécurité est-elle importante en Amérique latine?

La « Quatrième Révolution industrielle » a pour moteur la croissante inter-connectivité du monde (Schwab, 2016, p. 3). L'Amérique latine a été prompte à adopter des services numériques, favorisés par l'informatique en nuage, les appareils mobiles et les réseaux à larges bandes passantes, conduisant à une transformation en profondeur des gouvernements et des entreprises, entre autres par l'incorporation de la gestion des données dans le processus décisionnel des décideurs politiques, favorisant des décisions intégrées et efficaces. Malgré l'adoption en Amérique latine de ces technologies, le nouveau panorama a aussi transformé la nature de la criminalité et ses façons de faire. En Amérique latine et dans les Caraïbes, le coût de la cybercriminalité était estimé en 2017 entre 15 et 30 milliards de dollars US, autrement dit entre 0,28% et 0,57% du PIB de la région (Lewis, 2018, p. 7). Les pays de la région sont non seulement la cible d'attaques en ligne mais en sont aussi activement la source (Lewis, 2018, p. 20). L'augmentation des cyber-risques exige des entreprises et des gouvernements d'implanter la cybersécurité à même leurs processus, leur acquisition de technologies, et leur sélection de personnel.

En dépit de ces menaces, on observe toujours une pénurie mondiale d'experts en cybersécurité, évaluant le manque de main-d'œuvre à quelque 4,07 millions de personnes. Seulement en Amérique latine, le déficit de main-d'œuvre spécialisée en cybersécurité s'élève à environ 600 000 personnes ((ISC)², 2019, p. 8). Ce chiffre constitue une hausse significative par rapport à 2018 alors qu'on estimait la pénurie à environ 136 000 professionnels. ((ISC)², 2018, p. 4). La demande de professionnels de la cybersécurité est forte tant au sein des moyennes que des grandes entreprises, ce qui exige la formation d'une main-d'œuvre capable de concevoir, bâtir et opérer les nouvelles technologies, principalement à un niveau technique (World Economic Forum ¬– WEF, 2015, p. 20).

# _ ÉDUCATION A LA _
# **CYBERSÉCURITÉ**

Planifier l'avenir par le
développement de la main-d'œuvre

# L'éducation à la cybersécurité

En Amérique latine et dans les Caraïbes, le fossé entre la demande de main-d'œuvre qualifiée en cybersécurité et l'offre disponible a augmenté, en particulier au niveau des moyennes entreprises ((ISC)2, 2019). Selon le rapport 2019 de (ISC)2, « les professionnels de la cybersécurité détiendront vraisemblablement un diplôme universitaire, et un peu plus du tiers d'entre eux un diplôme de niveau maîtrise ou de doctorat/post-doctorat. Tandis que la majorité dans le domaine acquerront leur diplôme en informatique et sciences de l'information (40%), plusieurs obtiendront un diplôme dans un domaine non centré sur les TIC, comme le génie (19%) et la science économique (10%). » Concernant la région plus spécifiquement, le rapport indique que les organisations auront tendance à cibler leur recrutement au sein des institutions d'enseignement et des entreprises de sécurité. Il est clair que le début de carrière d'une vaste majorité de professionnels de la cybersécurité n'aura pas été en cybersécurité, plusieurs suivant d'abord un autre cheminement, souvent dans des domaines n'ayant pas à voir avec les TIC. Les décideurs politiques doivent adopter une approche nationale d'éducation à la cybersécurité de façon à créer une pépinière de professionnels de la cybersécurité, et penser stratégiquement à la meilleure façon de positionner l'éducation à la cybersécurité au sein de la politique nationale en matière de cybersécurité.

## Le pilier éducatif

De nombreux outils ont été créés afin d'aider à évaluer le niveau de compétence d'un pays donné en matière de cybersécurité. Le Cybersecurity Capacity Maturity Model for Nations (CMM) et l'Indice mondial de cybersécurité en sont deux exemples. Ces instruments soulignent l'incidence de l'éducation à la cybersécurité sur la compétence d'une nation en matière de cybersécurité et considèrent que l'éducation à la cybersécurité devrait être un pilier central de toute stratégie nationale.

Le CMM, créé par le Global Cyber Security Capacity Centre (GCSCC),[1] est un système de mesure qui évalue la situation au niveau national de la compétence d'un pays donné en matière de cybersécurité. Le CMM inclut un champ d'analyse consacré à l'Éducation, la formation et les habiletés en cybersécurité qui met en évidence que l'éducation à la cybersécurité constitue un pilier central dont doivent tenir compte les décideurs politiques au moment d'évaluer les compétences en cybersécurité, en se penchant sur la capacité, la qualité et la mise en œuvre de l'offre éducative et de formation à divers groupes, y inclus les représentants gouvernementaux, le secteur privé, et la population dans son ensemble (Cybersecurity Capacity Portal, 2020). Ce champ d'analyse comprend à son tour trois composantes centrales : 1) la conscientisation des citoyens et citoyennes, 2) le programme éducatif, et 3) le programme de formation professionnelle. Tandis que la première rubrique porte sur l'existence de campagnes de conscientisation du public en général, la seconde fait référence aux programmes accrédités au niveau universitaire, aux initiatives de recherche et développement (R&D) et à un parcours académique national en cybersécurité.

1. https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0

Quant à la troisième rubrique, elle souligne l'importance des programmes de certification et de formation en cybersécurité qui assurent un développement des compétences sur le long terme.

De façon similaire, l'Indice mondial de cybersécurité 2018 (CGI), créé par l'Union internationale des télécommunications (UIT),[2] souligne l'importance de conjuguer les différentes approches, techniques et instruments, afin de réduire le fossé éducationnel en cybersécurité. Comme le CMM, le CGI utilise des indicateurs semblables au niveau du pilier de la «Génération des compétences», ce qui inclut «les campagnes de conscientisation du public, le programme de certification et d'accréditation des professionnels de la cybersécurité; les programmes de formation professionnelle en cybersécurité, les programmes d'enseignement et les parcours académiques en cybersécurité; l'investissement dans les programmes de R&D en cybersécurité, les mesures incitatives, et l'industrie locale de la cybersécurité» (ITU, 2019, p. 8). Les deux modèles insistent aussi sur l'importance des programmes d'éducation, du fait qu'ils peuvent avoir une incidence sur le changement social et la croissance économique.

Les modèles et indices d'évaluation de la maturité en matière de cybersécurité démontrent que l'éducation doit aussi occuper une place prépondérante au sein de la stratégie nationale de cybersécurité des pays. En Amérique latine, les gouvernements de l'Argentine, du Brésil, du Chili, de la Colombie, du Costa Rica, de la République dominicaine, du Guatemala, du Mexique, du Panama et du Paraguay, ont tous publié ou mis à jour leurs stratégies nationales de cybersécurité. Ces stratégies englobent un programme de perfectionnement des compétences et des lignes d'action visant le renforcement de l'éducation à la cybersécurité au niveau national. Par exemple, les deux premiers objectifs de la stratégie nationale de l'Argentine s'intéressent à la conscientisation et à l'éducation à la cybersécurité.[3] Quatre des sept objectifs de la Politique nationale de sécurité de l'information du Brésil fait référence à la R&D, à la génération des compétences de la main-d'œuvre, au développement des habiletés, et à une culture de sécurité de l'information.[4] De façon analogue, les programmes nationaux de cybersécurité du Chili[5] et de la Colombie[6] ont une portée qui considère l'éducation comme un élément essentiel pour améliorer la maturité en cybersécurité, et ils identifient aussi des actions spécifiques à mettre en œuvre, en spécifiant un calendrier et les acteurs responsables de mener à bien les différentes phases. Les Plans d'action en éducation à la cybersécurité permettent de consolider et orienter les politiques de cybersécurité afin de remédier aux problèmes de la main-d'œuvre individuelle et aux lacunes des systèmes d'enseignement.

Au moment de compléter le présent document, la COVID-19 s'est transformée en pandémie mondiale, bouleversant le monde de l'éducation aux quatre coins du globe. Les ministères et départements de l'éducation, aux niveaux fédéral, étatique et provincial, ont agi rapidement pour placer leur contenu académique sur le nuage et assurer que des millions d'étudiants et d'enseignants puissent avoir un accès ininterrompu aux outils d'apprentissage à distance. Les universités publiques et privées, les collèges et les écoles, de la 1ère à la 12è année, ont emboîté le pas. L'enseignement à distance est devenu une réalité prédominante et dans la foulée, il en va de même de la nécessité de tenir compte des enjeux de cybersécurité quant à la connectivité qui permet l'apprentissage. Des exercices de formation en ligne et des moyens pour soutenir les enseignants et les étudiants en matière d'éducation à la cybersécurité sont devenus encore plus prioritaires dans ce processus d'adaptation aux méthodes d'enseignement virtuelles.

**2.** https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

**3.** Argentina (2019). Estrategia Nacional de Ciberseguridad. Disponible à l'adresse internet http://www.enre.gov.ar/web/bibliotd.nsf/203df3042bad9c40032578f6004ed613/1e2bd1ba24f72e9b03258408003abee3/$FILE/anexo%201.pdf.

**4.** Brazil (2018). Política Nacional de Segurança da Informação. Retrieved from http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2018/Decreto/D9637.htm.

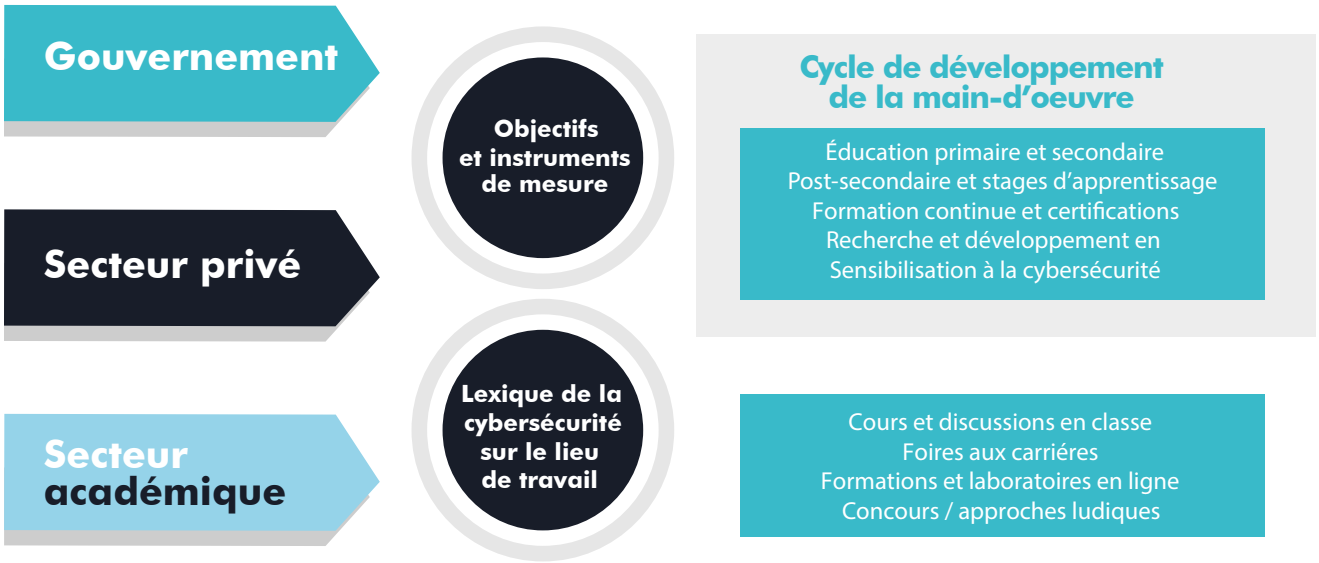
# Bâtir un Plan d'action en éducation à la cybersécurité

Le Plan d'action en éducation à la cybersécurité (CEAP selon l'acronyme anglais) est un modèle de référence pour les décideurs politiques, permettant d'élaborer des politiques publiques efficaces qui consolident leurs stratégies nationales en matière de cybersécurité et de développer une main-d'œuvre qualifiée en cybersécurité.

Le diagramme suivant montre comment un CEAP s'articule aux objectifs généraux de la stratégie nationale de cybersécurité en tant que ligne d'action spécifique concernant le pilier de l'éducation.

## Stratégie nationale de cybersécurité

### Plan d'action en éducation à la cybersécurité



L'élaboration d'un CEAP devrait se pencher sur:

1. L'identification des objectifs généraux.
2. L'inclusion des parties intéressées au CEAP.
3. L'identification des objectifs spécifiques et des instruments de mesure.
4. L'élaboration d'un plan de mise en œuvre du CEAP.
5. L'identification des ressources nécessaires à la mise en œuvre du CEAP.

L'initiative nationale d'éducation à la cybersécurité (NICE selon l'acronyme anglais),[5] que mène l'Institut national de standards et de technologie (NIST selon l'acronyme anglais) aux États-Unis, constitue un exemple d'initiative politique dont peuvent s'inspirer les décideurs politiques pour développer un CEAP. NICE fonctionne grâce à un partenariat entre le gouvernement, le secteur privé et la société civile pour faire face à la pénurie de main-d'œuvre, et vise à accroître la capacité du pays à relever les défis actuels et futurs en matière de cybersécurité. Tenant compte de la nature multidisciplinaire de la cybersécurité et des recommandations émises par les parties intéressées du secteur académique, du secteur privé et du gouvernement, le cadre de référence de NICE définit clairement les rôles et les fonctions des parties intéressées au sein de la stratégie d'amélioration des compétences en cybersécurité aux États-Unis (NIST, 2017, pp. 1-2). En date du mois d'août 2020, le NIST poursuit ses consultations publiques sur la mise à jour du cadre de référence NICE et prévoit rendre publique une version bonifiée en novembre 2020.[6]

Par l'entremise du cadre de référence NICE, le NIST offre aux décideurs politiques des exemples de l'importance de moduler les activités de cybersécurité en fonction de chaque phase du cycle de développement de la main-d'œuvre. Le cadre peut être utilisé comme guide de référence pour les organisations qui souhaitent développer des programmes d'enseignement et de formation en cybersécurité, et peut être adapté par chaque pays. NICE est le seul cadre de référence existant au niveau mondial qui cherche à standardiser les rôles requis au sein de la main-d'œuvre en cybersécurité, incluant tant les rôles techniques que non techniques. Des pays comme l'Australie, Singapour et le Japon, ont utilisé NICE comme base pour la création de leur propre cadre de référence et les ont divulgués largement au sein des secteurs public, privé et académique. À ce jour, aucun pays d'Amérique latine et des Caraïbes n'a formellement adopté un programme inspiré de NICE.

Les sections suivantes décrivent les cinq étapes cruciales pour l'élaboration d'un CEAP selon le cadre de référence NICE. La première section, intitulée ***L'identification des objectifs généraux***, présente les objectifs précis qu'il faut établir pour définir les résultats à long terme du plan d'action. La seconde section, intitulée ***L'inclusion des parties intéressées au Plan d'action en éducation à la cybersécurité***, décrit l'importance d'identifier adéquatement les acteurs qui prendront part à la conception et à la mise en œuvre du plan d'action. La troisième section, intitulée ***L'identification des objectifs spécifiques et des instruments de mesure***, souligne l'importance de sélectionner des objectifs qui sont mesurables et applicables au contexte où se déploiera le plan d'action. La quatrième section, intitulée ***La mise en œuvre d'un Plan d'éducation à la cybersécurité***, identifie les actions détaillées que l'on peut intégrer à la stratégie d'enseignement et au cycle de développement de la main-d'œuvre. Finalement, la section intitulée ***Recommandations pratiques*** présente une liste compréhensive des recommandations pouvant être mises en œuvre pour mener à bien le plan d'éducation à la cybersécurité.

**5.** Veuillez consulter l'annexe pour obtenir des précisions additionnelles.

**6.** https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-draft-revision

# L'identification des objectifs généraux

Lors des premières étapes de conception d'un CEAP, les décideurs politiques doivent choisir un nombre restreint d'objectifs et tenir compte du contexte social et économique du pays, afin d'élaborer un plan d'action qui ait toutes les chances de réussir. En identifiant bien quelques objectifs pertinents et réalisables, les décideurs politiques seront en mesure de mieux définir le CEAP.

Pour être efficace, un CEAP devrait chercher : a) à répondre au manque d'éducation et d'expertise en matière de cybersécurité, et b) à conscientiser sur les lacunes de cybersécurité et l'importance du sujet. À titre d'exemple, le programme NICE propose trois objectifs visant à aborder les carences de l'éducation et de l'expertise en cybersécurité. D'autres objectifs peuvent être considérés, bien que les objectifs présentés plus bas ont une portée large et approfondie, et qu'ils peuvent être utiles lorsqu'on les adapte aux objectifs spécifiques que les décideurs politiques cherchent à atteindre.

1. Accélérer le développement des apprentissages et des habiletés : cet objectif décrit l'importance de la conscientisation des acteurs publics et privés quant aux besoins éducatifs en cybersécurité. Plus particulièrement, on recommande de cibler les travailleurs sans emploi qui sont susceptibles de combler un poste en cybersécurité, ainsi que d'entreprendre des expérimentations par le biais de programmes d'éducation coopératifs qui permettent aux individus de s'intégrer au marché du travail et de gagner des revenus tout en continuant d'acquérir les habiletés requises.

2. Encourager une communauté d'apprentissage diversifiée : cet objectif vise à garantir que l'éducation à la cybersécurité met l'accent sur la formation continue, demeure mesurable, et intègre la diversité. Afin de promouvoir la diversité, NICE recommande d'encourager activement les membres des minorités sous-représentées à profiter des opportunités d'apprentissage en cybersécurité. Cet objectif incite aussi les secteurs public et privé à faire entrevoir la possibilité de faire carrière en cybersécurité, dès le niveau scolaire élémentaire, et ainsi favoriser le développement de parcours académiques.

3. Orienter le cheminement de carrière et la planification des effectifs de personnel : cet objectif souligne la nécessité de soutenir les mesures adoptées par les employeurs pour recruter, retenir, et offrir une formation continue à leurs employés. Des moyens sont proposés, dont celui d'appuyer les professionnels des ressources humaines à développer des outils pour soutenir les gestionnaires, et analyser les banques de données en fonction de cibles de recrutement. Policymakers should take into consideration the views of those directly and indirectly involved in the creation and implementation of the CEAP. By involving stakeholders in this process, policymakers can reinforce the effectiveness of the strategy and achieve the goals set. The following section offers an overview on how to better identify and engage stakeholders.

Les décideurs politiques doivent tenir compte des points de vue de ceux qui sont impliqués directement et indirectement dans les processus d'élaboration et de mise en œuvre du CEAP. En impliquant les parties intéressées dans le processus, les décideurs politiques peuvent consolider l'efficacité de la stratégie et assurer l'atteinte des objectifs fixés. La section suivante présente un survol des moyens pour mieux identifier et impliquer les parties intéressées.

# L'inclusion des parties intéressées au Plan d'action en éducation à la cybersécurité

La collaboration des diverses parties intéressées est essentielle durant la formulation et la mise en œuvre d'un CEAP. Au cours de l'étape d'élaboration, le partenariat entre le gouvernement, le secteur privé et la société civile, permet d'évaluer les besoins du moment au niveau de la main-d'œuvre et d'identifier si des initiatives pertinentes sont déjà en place dans le système éducatif, de l'éducation primaire à l'enseignement postsecondaire.

Les gouvernements d'Amérique latine et des Caraïbes peuvent d'abord cartographier les acteurs clés de l'industrie, du monde académique et de la société civile, et les inviter à prendre part au processus de formulation du CEAP. À cette fin, il est fondamental d'informer clairement les parties intéressées des éléments suivants: 1) les objectifs généraux du Plan d'action en éducation à la cybersécurité et sa portée; 2) le calendrier, les balises et les produits livrables du processus de formulation; et 3) les mécanismes décisionnels du processus de formulation (par ex. concernant le processus d'adoption du plan d'action et la façon dont on tiendra compte et analysera les observations et suggestions des diverses parties prenantes et, à terme, comment celles-ci seront incorporées). Les décideurs politiques peuvent assurer l'implication des parties intéressées en créant des comités, en organisant des ateliers de travail, ou en menant des consultations publiques, entre autres mécanismes. Les pays qui ont déjà ficelé leurs Stratégies nationales de cybersécurité suite à des processus impliquant les diverses parties intéressées, pourraient aussi transposer cette expérience acquise au sein du processus d'élaboration de leurs CEAP.[7]

De plus, dans le but de mettre en œuvre un Plan d'action national en éducation à la cybersécurité, les décideurs politiques doivent envisager de créer un comité ou une commission d'agences gouvernementales, afin de coordonner la mise en œuvre des politiques éducatives, ainsi que des groupes de travail ouverts aux contributions et recommandations de divers secteurs. Le cas NICE offre un excellent exemple de mécanismes de coordination pouvant être mis en place, comme le Conseil de coordination inter-agences du NICE (ICC selon l'acronyme anglais) et le Groupe de travail. Tandis que le conseil réunit les agences gouvernementales responsables de la mise en œuvre du plan d'action, le groupe de travail vise à regrouper les représentants des différents secteurs. Il est souhaitable d'envisager la création de ces deux instances au moment de mettre en œuvre un CEAP au niveau national. Il est important de souligner que plusieurs pays d'Amérique latine et des Caraïbes ont développé un modèle similaire de mise en œuvre de leurs stratégies nationales de cybersécurité[8], ayant mis sur pied un comité ou une commission composée d'agences gouvernementales, ainsi que des groupes de travail visant à coopter les représentants d'autres secteurs à participer de façon volontaire. Il peut être souhaitable de répliquer ce modèle de gouvernance en vue de soutenir le CEAP au niveau national.

## Le secteur privé

Le secteur privé représente un acteur et un partenaire crucial pour mettre en œuvre un CEAP national. Jouant un rôle d'avant-plan dans le développement technologique, le secteur privé connaît bien les besoins de l'industrie et peut aussi fournir des outils précieux pour former la main-d'œuvre et offrir des ressources pour améliorer la prestation des offres de formation.

**7.** Les documents qui décrivent comment développer une approche auprès des diverses parties intéressées pour élaborer des stratégies nationales de cybersécurité, constituent un bon point de départ au moment de formuler un programme national d'éducation à la cybersécurité (Consultez les rapports de Global Partners Digital, dont «Framework for Multistakeholder Cyber Policy Development» et «Multistakeholder Approaches to National Cybersecurity Strategy Development»).

**8.** Par exemple, le Chili a mis sur pied le Comité interministériel de cybersécurité, regroupant plusieurs agences gouvernementales. Le Comité peut inviter les représentants du monde académique, de la société civile et du secteur privé à participer à ses travaux. De même, le Paraguay a institué une Commission nationale de cybersécurité avec des membres du gouvernement, et on a prévu la possibilité de créer des groupes réunissant les diverses parties prenantes afin d'aborder des enjeux spécifiques.

En plus des structures de gouvernance, les partenariats public-privé-monde académique jouent aussi un rôle important au sein d'un CEAP. Les établissements d'enseignement publics et privés sont bien placés pour tirer parti de l'expertise du secteur privé, y inclus les entreprises technologiques, afin d'améliorer les contenus et garantir l'efficacité et la pérennité globale de l'éducation à la cybersécurité. Favoriser ces partenariats peut faciliter l'allocation de ressources et favoriser les opportunités, les rendant accessibles à un plus grand nombre d'étudiants.

Par exemple, l'initiative Educate Cloud Degree de Amazon Web Services (AWS) aide à « transposer sur le nuage » les parcours académiques des institutions participantes, menant à un diplôme et une accréditation avec spécialisation ou concentration en informatique de nuage. Au Brésil et en Colombie, le Service national de formation industrielle brésilien (SENAI)[9] et le Service national d'apprentissage colombien (SENA)[10] ont tous deux établi un partenariat avec AWS pour offrir à leurs étudiants des programmes de formation en intelligence artificielle, en Internet des Objets (IdO) et en informatique de nuage, lesquels incluent des outils et modules touchant à la cybersécurité. Grâce à ce partenariat, le SENAI et le SENA ont formé respectivement 3 000 et 10 000 étudiants en 2019. De même, le gouvernement d'Argentine a offert à ses citoyens, en partenariat avec AWS, le programme AWS Educate par le biais du portail du Ministère de la modernisation ; offrant aussi à 28 établissements d'enseignement du pays le programme académique en informatique de nuage de AWS Educate, qui inclut des modules sur la cybersécurité.[11]

À l'instar de AWS, CISCO et Trend Micro offrent aussi des ressources pour soutenir des institutions postsecondaires et leurs étudiants. Le CISCO Networking Academy, par exemple, offre des programmes de formation en ligne et en personne sur plusieurs sujets, dont la cybersécurité, lesquels sont aussi disponibles en portugais et en espagnol.[12] Trend Micro, par l'entremise du programme «Sensibilisation à la cybersécurité pour les universités»[13] travaille avec les universités pour former les formateurs, orienter le parcours académique en cybersécurité, et offrir des séminaires techniques et des webinaires aux étudiants et aux enseignants.

## Le secteur académique

Grâce aux universités, aux groupes de réflexion et à d'autres institutions académiques, le monde académique réunit généralement plusieurs experts qui, par leurs recherches, font avancer le domaine de la cybersécurité. L'intégration des chercheurs aux partenariats public-privé-monde académique permet de partager des analyses objectives, scientifiques et révisées par les pairs, qui contribuent au développement d'orientations politiques. Le monde académique peut souvent être à l'origine d'innovations et d'avancées technologiques.

L'Université d'Oxford, par le biais du Global Cyber Security Capacity Centre (GCSCC), est devenu un centre de recherche de premier plan au niveau international, contribuant grandement au champ des connaissances sur la portée, le rythme, la nature et l'impact de la cybersécurité. L'université et le GCSCC ont établi des partenariats avec des organisations telles que l'OEA et la Banque interaméricaine de développement, afin de préparer des modèles d'évaluation objective de l'état des lieux dans la région en matière de cybersécurité. Le premier de ces partenariats a été mené à bien

9. https://noticias.portaldaindustria.com.br/noticias/educacao/senai-e-amazon-web-services-se-unem-para-incentivar-a-educacao-no-brasil/
10. https://aws.amazon.com/blogs/publicsector/president-of-colombia-joins-aws-in-bogota-talks-innovation-across-the-region/
11. https://aws.amazon.com/es/blogs/aws-spanish/aws-announces-amazon-cloudfront-edge-location-in-argentina/
12. https://www.netacad.com/fr
13. https://www.trendmicro.com/fr_fr/initiative-education/cybersecurity-education-universities.html

en 2016, menant à la publication Cybersecurity: Are we ready in Latin America and the Caribbean? (2016).[14] Cette publication a permis aux décideurs politiques et aux parties prenantes du secteur privé d'identifier les progrès en cybersécurité réalisés dans chaque pays, soulignant en outre les domaines clés où une mobilisation et un soutien sont nécessaires pour atteindre un plus fort niveau de maturité.

L'intégration du secteur académique devrait inciter les décideurs politiques à utiliser les conseils et les données disponibles, pour mettre en place des politiques efficaces qui garantissent l'inclusion des principes de la cybersécurité dans le système d'éducation. Et surtout, il s'agit d'entités primordiales qui méritent un soutien financier pour pouvoir continuer leurs travaux d'innovation et d'avancement en matière de cybersécurité et d'éducation.

## La société civile

La société civile et plusieurs associations de sécurité de l'information (par ex. (ISC)², CompTIA, ISACA, et SANS) ont développé des programmes d'éducation à la cybersécurité qui peuvent appuyer les gouvernements à tirer profit des compétences en cybersécurité acquises dans diverses institutions et régions du pays. En outre, au sein des projets visant à améliorer l'éducation des jeunes et l'employabilité, les partenariats public-privé tendent à être neutres et de durée déterminée, et souvent ils veillent à impliquer la société civile (IDB, 2018, p. 4). Les organismes à but non lucratif appuient les gouvernements et les acteurs privés au niveau de la surveillance de ces projets et la reddition de compte, garantissant que les objectifs sont atteints. De plus, « les ONG, les communautés et les institutions académiques occupent une place nécessaire dans l'équation, mettant à contribution leur propre avantage comparatif, leurs points de vue et leurs positionnements » (WEF, 2014, p. 11). D'autre part, les organisations d'Amérique latine sont plus susceptibles de recruter des professionnels de la cybersécurité au sein des institutions académiques ((ISC)2, 2019, p. 27), ce qui met en évidence l'importance des partenariats public-privé-société civile pour améliorer les compétences et les connaissances des professionnels de la cybersécurité de la région.

Toutes les parties intéressées devraient prendre part aux efforts pour soutenir le développement d'une main-d'œuvre qualifiée en cybersécurité, puisque ces acteurs, de par leur diversité, jouent un rôle unique au sein des différentes instances du cycle éducatif. Les sections qui suivent présentent quelques exemples où les secteurs public et privé, ainsi que la société civile, peuvent participer à l'avancement des connaissances en matière de cybersécurité et à former la main-d'œuvre requise pour combler le manque à gagner.

**14.** https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean

# L'identification des objectifs spécifiques et des instruments de mesure

L'identification d'objectifs mesurables et l'adoption d'instruments de mesure adéquats pour assurer une évaluation continue du progrès réalisé, et offrir une rétro-alimentation visant leur amélioration, contribuent directement à l'efficacité et au succès de CEAP ciblés. De façon à fonctionner correctement, les objectifs doivent être toutefois SMART : spécifiques, mesurables, atteignables et ambitieux, réalistes et temporellement définis.

Les gouvernements peuvent aussi envisager d'utiliser des indicateurs d'intrants (c.-à-d. en lien avec les ressources nécessaires, concernant par exemple la formation d'un enseignant et la pédagogie en salle de classe), des indicateurs de résultats (c.-à-d. en ce qui concerne l'impact de l'activité entreprise, par exemple les connaissances et habiletés acquises par l'étudiant), des indicateurs éducatifs et socioéconomiques d'ordre national, tels que les taux d'inscription dans le système d'éducation, et des indicateurs de coûts (c.-à-d. la comparaison des résultats d'une initiative par rapport à son coût, par une analyse de coûts et bénéfices par exemple (Wagner et al., 2005, pp. 21-30).

Les décideurs politiques peuvent aussi envisager d'adapter les indicateurs des Technologies de l'information et de la communication (TIC) pour mesurer l'impact des initiatives éducatives à la cybersécurité. Par exemple, le « Partenariat sur la mesure des TIC au service du développement »[15] de l'Union internationale des télécommunications comprend une liste d'indicateurs convenue entre diverses parties prenantes lors d'un processus de consultation, et inclut un certain nombre d'indicateurs TIC en éducation qui pourraient être ajustés et ensuite utilisés pour évaluer la mise en œuvre globale du CEAP au niveau national. En guise d'exemple, certains indicateurs se penchent sur :

- La proportion des écoles primaires et secondaires qui ont mis en place des programmes d'éducation à la cybersécurité.
- La proportion des étudiants de niveau postsecondaire qui se sont inscrits à des cours touchant à la cybersécurité.
- La proportion des enseignants qualifiés en cybersécurité dans les écoles.[16]

Les gouvernements et d'autres parties prenantes devraient envisager de ne pas s'appuyer uniquement sur des instruments traditionnels d'évaluation de l'impact, comme les sondages ciblés, mais explorer aussi d'autres sources de données (OECD, 2019, p. 18). Par exemple, grâce à l'avancement technologique, les décideurs politiques peuvent conjuguer différentes sources de données, identifier des corrélations, et même conduire des analyses prévisionnelles.

**15.** https://www.itu.int/en/ITU-D/Statistics/Pages/intlcoop/partnership/default.aspx

**16.** Ces indicateurs ont été préparés en s'appuyant sur la liste principale d'indicateurs TIC du Partenariat sur la mesure des TIC au service du développement, disponible à l'adresse internet https://www.itu.int/en/ITU-D/Statistics/Pages/coreindicators/default.aspx.

# La mise en œuvre d'un Plan d'éducation à la cybersécurité

Cette section présente de l'information sur les aspects cruciaux dont il faut tenir compte lors de la mise en œuvre d'un CEAP à chacune des phases du cycle de développement de la main-d'œuvre, ainsi que les meilleures pratiques ayant été adoptées dans le monde.

## L'éducation primaire et secondaire – Éduquer la prochaine génération

Le Plan stratégique de NICE représente un excellent exemple de la façon d'ébaucher un plan d'enseignement pour les niveaux primaire et secondaire. Le « National K-12 Cybersecurity Education Implementation Plan»[17] vise à: 1) encourager les élèves à entreprendre des activités liées à la cybersécurité; 2) soutenir les enseignants pour qu'ils incorporent des concepts de cybersécurité dans leurs cours en classe; et finalement 3) aider les élèves des niveaux primaire et secondaire à identifier des opportunités de carrière dans le domaine de la cybersécurité. De plus, le K-12 Cybersecurity Education Implementation Plan favorise aussi l'implication de la communauté en mettant sur pied une campagne de conscientisation quant aux opportunités de carrière en cybersécurité, ciblant les « enseignants, les élèves, les parents, les gestionnaires et les conseillers en orientation.» Ces objectifs constituent un excellent exemple des visées possibles que les gouvernements peuvent adopter afin de former la prochaine génération de professionnels de la cybersécurité.

Afin de soutenir les élèves du niveau primaire et secondaire, le National Integrated Cyber Education Research Center (NICERC)[18] aux États-Unis offre aux enseignants un programme de formation gratuit afin qu'ils intègrent des concepts de cybersécurité dans leurs cours en classe, ainsi que des occasions de développement professionnel.

Afin de former la main-d'œuvre de la prochaine génération, les décideurs politiques doivent envisager la mise sur pied d'un plan d'action spécifique comportant des activités pour les enseignants et pour les élèves. En ce qui a trait aux enseignants, la formation devrait offrir des ressources et des outils novateurs auxquels les enseignants pourraient puiser pour susciter l'intérêt dans leurs salles de classe. En ce qui concerne les élèves du primaire et du secondaire, il est essentiel de toucher aux enjeux de sécurité, au cheminement d'une carrière potentielle, et aux façons de tirer parti des approches ludiques et compétitives. Les gouvernements devraient aussi envisager d'établir des partenariats avec le secteur privé, les organismes à but non lucratif et les universités, au moment d'élaborer et mettre en œuvre leurs initiatives éducatives. Plusieurs outils pourraient être utilisés afin d'éduquer les enfants à la cybersécurité, que ce soit en ajustant le programme scolaire, ou en en développant de nouveaux, ou en appuyant les concours qu'organise le secteur privé.

*Étude de cas*

AWS s'est associé avec Code.org, une organisation à but non lucratif engagée à élargir l'accès à la science informatique dans les écoles et à accroître la participation des femmes et des minorités sous-représentées. Avec l'appui de AWS, la vision de Code.org est d'offrir à tous les élèves dans toutes les écoles, l'opportunité d'apprendre la science informatique, au même titre que la biologie, la chimie ou l'algèbre. Plus particulièrement, AWS soutient le site internet de Code.org tout au long de l'année afin d'améliorer sa capacité à gérer à grande échelle les millions d'enseignants et d'élèves qui participent, dans plus de 180 pays, à l'évènement « Une heure de code », une campagne annuelle qui touche mondialement 15% des élèves lors d'activités d'une heure d'introduction au codage. Par ailleurs, Code.org protège les données de

**17.** https://www.nist.gov/sites/default/files/documents/2017/04/26/nice_k12_implementation_plan.pdf

**18.** https://nicerc.org/student/

millions d'élèves et veille à contrer les cyberattaques en utilisant les outils de AWS Infrastructure Event Management, AWS Shield Advanced, AWS WAF – Web Application Firewall, et AWS GuardDuty. Au cours des trois dernières années, des milliers d'employés d'Amazon se sont portés volontaires durant l'Heure de code dans des salles de classe, allant de San Miguel au Chili à Cape Town en Afrique du Sud ; en 2019, les employés d'Amazon ont animé 280 évènements dans plus de 20 pays et 160 villes.

## L'enseignement postsecondaire et les stages de formation

C'est durant cette étape de leur apprentissage que les étudiants prennent souvent le premier virage vers une carrière en cybersécurité. Au niveau postsecondaire, l'éducation à la cybersécurité pourrait être favorisée tant à l'égard des étudiants qui sont sur la voie d'emplois techniques qu'à l'égard de ceux qui cherchent à faire carrière dans des domaines non techniques, comme le droit, les politiques publiques, les affaires, la défense et le secteur militaire. Plusieurs des professionnels de la cybersécurité d'aujourd'hui possèdent un bagage non relié aux TIC, dont 30% d'entre eux proviennent de domaines comme les affaires, le marketing, la finance, la comptabilité et le secteur militaire. En Amérique latine, 18% des professionnels de la cybersécurité ont débuté dans des carrières non techniques ((ICS)$^2$, 2017, p. 5).

Plusieurs des programmes de science informatique et de génie ne sont plus à jour pour être en mesure de répondre aux changements provoqués par la Quatrième Révolution industrielle, et l'une des premières étapes du processus serait de les inciter à se moderniser. De même, les cours de cybersécurité devraient être parties intégrantes des programmes de science informatique et d'ingénierie logicielle afin de garantir que les développeurs incorporent automatiquement des mesures de sécurité à même leurs activités de développement.

Les mesures éducatives devraient envisager d'inclure un plus grand nombre de cours interdisciplinaires ainsi que des programmes académiques plus dynamiques et réactifs, afin de suivre le rythme des nouvelles avancées technologiques (Gleason, 2018, p. 223). Par exemple, il existe un besoin réel de professionnels qui connaissent simultanément les enjeux du système de santé et de la cybersécurité. C'est dans cet esprit que certaines universités ont commencé à offrir des programmes académiques qui conjuguent les politiques de santé et la cybersécurité.[19]

Après leurs programmes de premier cycle universitaire, les étudiants ont l'option de se spécialiser en cybersécurité lors d'études supérieures. Il existe un certain nombre de programmes d'enseignement supérieur en cybersécurité, menant entre autres à des diplômes de Maîtrise professionnelle et de Maîtrise de recherche dans domaines comme la science informatique, la science politique et l'administration. De fait, quelques pays d'Amérique latine offrent des programmes d'études supérieures en cybersécurité, dont l'Instituto Tecnológico y de Estudios Superiores de Monterrey (l'Institut technologique et d'enseignement supérieur de Monterrey) au Mexique[20] et l'Escuela Superior de Guerra (l'École supérieure de guerre) en Colombie.[21]

L'Agence européenne de cybersécurité (ENISA selon l'acronyme anglais) a créé une cartographie des diplômes académiques en cybersécurité offerts dans ses États membres, incluant les programmes de premier cycle et d'études supérieures.[22] En plus d'aider les étudiants à faire des choix éclairés quant à leur choix d'un programme de cybersécurité, la création d'une cartographie de l'offre académique en cybersécurité permet aux gouvernements d'avoir un portrait plus fidèle des programmes de cybersécurité offerts au niveau des études supérieures.

**19.** Par exemple, l'Université de Sydney offre une Maîtrise en sécurité de la santé. Veuillez consulter l'adresse internet

**20.** https://maestriasydiplomados.tec.mx/posgrados/maestria-en-ciberseguridad

**21.** https://ciber.esdegue.edu.co/course/index.php?categoryid=6

**22.** https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities

Les gouvernements peuvent jouer un rôle essentiel pour promouvoir la disponibilité et la qualité des programmes d'enseignement supérieur en cybersécurité, en définissant les standards d'une éducation à la cybersécurité de qualité au niveau national. Par exemple, le NCSC au Royaume-Uni est chargé d'octroyer au niveau national la certification des diplômes de baccalauréat et de maîtrise en cybersécurité.[23] Cela aide les étudiants à prendre des décisions éclairées au moment de choisir leur programme d'études postsecondaires, et permet aux employeurs de recruter des individus plus qualifiés.

## Les programmes d'apprentissage en cybersécurité

Les étudiants peuvent se familiariser à la cybersécurité après le collège grâce à des programmes d'apprentissage. Plus précisément, les programmes d'apprentissage centrés sur les techniques émergentes, comme l'apprentissage machine et l'intelligence artificielle (IA), sont cruciaux pour l'avenir de la main-d'œuvre, compte tenu que ces technologies seront intégrées à pratiquement tous les nouveaux logiciels et sont devenues une priorité d'investissement pour les Dirigeants principaux de l'information (DPI).[24] Un sondage réalisé auprès de 800 experts et dirigeants en haute technologie prédit que d'ici 2025, la technologie IA sera largement intégrée et, de ce fait, on assistera à un accroissement de la place de l'IA et de postes IA, à divers niveaux, au sein des organisations. Parallèlement, plusieurs entreprises de sécurité de haute technologie sont intéressées à développer des programmes d'apprentissage qui conjuguent la cybersécurité et l'intelligence artificielle.[25]

Plusieurs programmes d'apprentissage en Amérique latine ont déjà commencé à former des étudiants à la cybersécurité, comme c'est le cas des programmes du SENAI au Brésil et du SENA en Colombie mentionnés précédemment. Dans le même esprit, la National Research Foundation (NRF) à Singapour, par exemple, a créé un programme national en IA, appelé AI Singapore, qui inclut le AI Apprenticeship Program (AIAP)[26] qui vise à préparer le talent local. En Allemagne[27] et en Corée du Sud,[28] les gouvernements ont mis en œuvre un modèle éducatif d'apprentissage à deux volets, conjuguant d'une part une formation pratique grâce aux partenariats avec des employeurs, et d'autre part, une formation plus traditionnelle (Deloitte, 2018b, p. 23). Ce système d'apprentissage à deux versants peut être un fantastique moyen pour favoriser le recrutement au sein d'entreprises technologiques, dont les besoins en main-d'œuvre qualifiée sont énormes.

## La formation continue et la certification

Les avancées technologiques et la mutation du panorama des menaces de cybersécurité exigent une constante mise à jour des compétences et des ajustements périodiques. Ce n'est plus une option, il est aujourd'hui incontournable que les travailleurs du 21è siècle continuent de développer leurs connaissances. Les formations de courte durée et les cours en ligne aident à combler rapidement les décalages de savoir et de compétence. En Amérique latine, il est possible de suivre de courtes formations en personne et de façon virtuelle. Il existe aussi plusieurs opportunités d'obtenir des bourses de perfectionnement des gouvernements, du secteur privé et des organisations internationales comme l'OEA.

---

**23.** https://www.ncsc.gov.uk/information/ncsc-certified-degrees

**24.** Gartner (July 2017). Gartner affirme que la technologie IA sera intégrée à pratiquement tous les nouveaux logiciels d'ici 2020. Disponible à l'adresse internet https://www.gartner.com/en/newsroom/press-releases/2017-07-18-gartner-says-ai-technologies-will-be-in-almost-every-new-software-product-by-2020.

**25.** American Association of Community Colleges (January 2019). Developing Apprenticeships for cybersecurity. Disponible à l'adresse internet http://www.ccdaily.com/2019/01/developing-apprenticeships-cybersecurity/.

**26.** On peut obtenir plus d'information à l'adresse internet https://www.aisingapore.org/industryinnovation/aiap/.

**27.** https://www.make-it-in-germany.com/en/study-training/training/vocational/system/

**28.** http://ncee.org/what-we-do/center-on-international-education-benchmarking/top-performing-countries/south-korea-overview/south-korea-school-to-work-transition/

Par exemple, l'Institut national espagnol de cybersécurité (INCIBE) et l'OEA organisent des Bootcamp d'été en cybersécurité, à León en Espagne. Il s'agit d'un programme de deux semaines en espagnol pour les techniciens, les professionnels responsables de l'application des lois, et toutes celles et ceux qui s'intéressent au développement de stratégies nationales de cybersécurité.[29] L'OEA offre des bourses pour les professionnels d'Amérique latine et des Caraïbes pour assister au Bootcamp d'été, ce qui les aide à couvrir leurs frais de participation. Le programme est devenu une initiative phare en cybersécurité, avec la participation, en 2019, de plus de 100 professionnels d'Amérique latine ayant obtenu une bourse offerte par l'OEA. De la même manière, l'Université internationale de Floride (FIU) organise pendant deux jours un certificat intensif de leadership en matière de cybersécurité, avec le soutien de l'OEA.[30] En 2020, le Bootcamp d'été en cybersécurité s'est tenu de façon virtuelle, et l'évènement a attiré la participation de plus de 800 étudiants en provenance de 80 pays.

Plusieurs organisations privées offrent aussi des formations et des occasions de certification qui incluent des modules en cybersécurité, comme l'AWS,[31] Microsoft,[32] et CISCO.[33] Bien que l'obtention d'un diplôme d'études supérieures certifie l'acquisition de connaissances en cybersécurité, certains employeurs peuvent considérer qu'une certification représente une meilleure façon d'acquérir des compétences en cybersécurité (McAfee, 2017, p. 4). En effet, la formation et la certification en cybersécurité peuvent fournir une expérience pratique dans des domaines concrets de la cybersécurité (Catota; Morgan; Sicker, 2019). De surcroît, les certifications peuvent avoir un impact direct sur les perspectives salariales. Le salaire moyen des professionnels de la cybersécurité qui détiennent des certificats de sécurité est plus élevé que le salaire moyen de ceux qui n'en ont pas acquis. Tandis qu'en Amérique latine, les professionnels certifiés gagnent autour de 21 000 dollars US, les autres gagnent en moyenne environ 16 000 dollars US ((ISC)$^2$, 2019, p. 17).

La formation continue et la certification représentent des mécanismes importants pour favoriser l'adaptabilité de la main-d'œuvre en cybersécurité, à un point tel que l'initiative NICE aux États-Unis a créé un sous-groupe de travail sur le sujet. Le Sous-groupe de travail en matière de formation et certification a développé une matrice cartographique, qui établit une connexion entre les certifications et le cadre de référence NICE sur les rôles des professionnels de la cybersécurité au sein d'une organisation.[34] Les certifications reconnues en cybersécurité incluent :

- Certified Ethical Hacker (CEH), une certification offerte par le Conseil international des Consultants en commerce électronique (EC-Council).[35]
- Certified Information Security Manager (CISM), une certification offerte par ISACA.[36]
- CompTIA Security+.[37]
- Certified Information Systems Security Professionals (CISSP), une certification offerte par (ISC)$^2$.[38]
- The Sans GIAC Security Essentials (GSEC).[39]
- NIST Cybersecurity Framework (NCSF), Foundation and Practitioner.[40]
- Certified Computer Security Incident Handler (CERT), une certification offerte par la Carnegie Mellon University.[41]

29. https://www.incibe.es/en/summer-bootcamp
30. https://gordoninstitute.fiu.edu/executive-education/cls/
31. https://www.aws.training/
32. https://www.microsoft.com/en-us/learning/default.aspx
33. https://www.cisco.com/c/en/us/training-events/training-certifications.html
34. https://www.nist.gov/itl/applied-cybersecurity/nice/illustrative-mapping-certifications-nice-framework
35. https://cert.eccouncil.org/application-process-eligibility.html
36. http://www.isaca.org/certification/cism-certified-information-security-manager/pages/default.aspx
37. https://certification.comptia.org/certifications/security
38. https://www.isc2.org/Certifications/CISSP
39. https://www.giac.org/certification/security-essentials-gsec
40. https://niccs.us-cert.gov/training/search/itsm-solutions-llc/nist-cybersecurity-framework-boot-camp-foundation-practitioner
41. https://www.sei.cmu.edu/education-outreach/credentials/credential.cfm?customel_datapageid_14047=14324

Les constantes opportunités de formation et de certification permettent aux professionnels de rester à jour et de combler rapidement tout décalage de connaissances.

## La recherche et développement en cybersécurité (R&D)

L'expertise issue de la recherche peut aider les gouvernements et l'industrie à formuler des solutions innovantes pour faire face aux défis actuels et futurs de la cybersécurité, à identifier les compétences requises, et à élaborer des plans de formation qui y répondent. La recherche peut prendre différentes formes, dont 1) des programmes de doctorat centrés sur l'étude de la cybersécurité ; 2) des centres de recherche d'excellence sur la cybersécurité; et 3) des programmes spécifiques de R&D par le biais de protocoles d'entente entre le monde académique et l'industrie/les gouvernements, entre autres.

Par exemple, le Bureau du Premier ministre de Singapour a inauguré le Programme national de R&D en cybersécurité, visant à favoriser la résilience et à élever le niveau de préparation de noyaux critiques de sa cyber-infrastructure. Ses initiatives incluent le Laboratoire national de R&D sur la cybersécurité (NCL) le Consortium sur la cybersécurité, des Bourses de recherche, ainsi que des bourses d'étude de deuxième et troisième cycle. De façon à illustrer comment ces programmes encouragent l'éducation à la cybersécurité, le NCL s'est récemment associé à la Singapore University of Technology and Design's iTrust Labs pour « offrir des expérimentations et services intégrés qui soutiennent les agences gouvernementales, le monde académique et l'industrie en ce qui a trait à la recherche, touchant les entreprises TIC et la cybersécurité en matière de technologie opérationnelle, les évaluations de la technologie, et la formation. »[42,]

Le National Cybersecurity Center of Excellence (NCCoE) aux États-Unis est un autre exemple. Le NCCoE fait partie du NIST et constitue une « plateforme de collaboration où les organisations de l'industrie, les agences gouvernementales et les institutions académiques travaillent ensemble pour traiter des enjeux de cybersécurité les plus pressants pour les entreprises. Ce partenariat public-privé favorise l'élaboration de solutions pratiques de cybersécurité pour des industries spécifiques, ainsi que pour répondre aux grands défis technologiques intersectoriels. »[43] Le NCCoE a entrepris plusieurs projets, dont les suivants : Transport Layer Security (TLS), Server Certificate Management, Mobile Device Security, Data Security Projects.[44]

Emboîtant le pas de gouvernements qui ont une vision nationale sur la R&D en cybersécurité, des parties prenantes telles que les universités, l'industrie, la société civile sont en mesure de se réunir avec le gouvernement pour collaborer à développer la recherche et des outils pouvant répondre aux besoins les plus pressants de cybersécurité des pays. Il est possible de créer des plateformes de collaboration en R&D lorsque les parties intéressées de divers secteurs conjuguent leurs efforts.

---

**42.** https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme

**43.** https://www.nccoe.nist.gov/about-the-center

**44.** thttps://www.nccoe.nist.gov/projects

# Bâtir une culture de la cybersécurité

Aujourd'hui, une part importante de nos vies personnelles et professionnelles se déploie en ligne. Tous les citoyens et citoyennes, y compris ceux et celles qui ne font pas carrière dans le domaine de la cybersécurité, ont besoin d'avoir un certain niveau de connaissance en matière de sécurité pour protéger leurs données personnelles et celles de l'organisation où ils travaillent. Selon le rapport McKinsey, l'erreur humaine est l'une des principales causes de violation des données au sein des organisations : de 2012 à 2017, 50% des cas de violation de données découlent d'un facteur de menace interne (McKinsey, 2018, p. 3). Indépendamment de leur cheminement de carrière, les professionnels peuvent et devraient apprendre les meilleures pratiques de cybersécurité.

La ***Boîte à outils de la Campagne de conscientisation de l'OEA sur la cybersécurité*** recommande que les campagnes de sensibilisation sur la cybersécurité soient simples et faciles, et qu'elles évitent les spécificités techniques.[45] Les messages de conscientisation sur la cybersécurité doivent être formulés de manière positive afin que le public se sente investi d'un pouvoir d'agir pour se protéger (OAS, 2016, p. 14). Les gouvernements devraient envisager de réaliser des sondages pour cerner les habitudes technologiques des jeunes et leur niveau de connaissance sur la sécurité en ligne et leur vie privée. Il existe un bon nombre d'outils pouvant être utilisés pour accroître la conscientisation aux enjeux de la cybersécurité, comme par exemple les assemblées d'école, les concours, les leçons en salle de classe, le matériel d'information disponible sur divers sites internet, les campagnes sur les médias sociaux, et bien d'autres.

Les partenariats entre le gouvernement, l'industrie et la société civile peuvent aussi contribuer à augmenter la sensibilité du public à l'égard de la cybersécurité. La campagne ***STOP.THINK. CONNECT*** [46] a été créée para la National Cybersecurity Alliance (NCSA) et le Anti-Phishing Working Group (APWG) en collaboration avec des entreprises privées, des organismes à but non lucratif et des organisations gouvernementales. L'OEA a désigné octobre comme le Mois de la conscientisation à la cybersécurité et le célèbre à chaque année depuis 2014. L'OEA a aussi invité ses États membres à accroître leurs efforts de mise en œuvre de politiques nationales de cybersécurité et à se joindre à l'initiative STOP.THINK.CONNECT qui « met en place une action mondiale coordonnée et unifiée pour conscientiser le public à la cybersécurité. »[47]

En Amérique latine, le gouvernement du Chili a lancé une campagne nationale de conscientisation à la cybersécurité, qui inclut plusieurs recommandations au public et aux employés de bureau.[48] Pareillement, la Campagne nationale de conscientisation à la cybersécurité de la Colombie, intitulée EnTIConfío, offre de l'information et des ressources à un large public, et plus particulièrement aux enfants.[49] Des pays comme l'Argentine, le Mexique, le Panama et l'Uruguay, pour ne nommer que ceux-ci, ont créé leur propre campagne de conscientisation afin de participer à l'effort de bâtir des sociétés plus cyber-résilientes.

**45.** https://www.thegfce.com/documents/publications/2015/10/01/cybersecurity-awareness-campaign-toolkit

**46.** https://www.stopthinkconnect.org/

**47.** OAS (October 2014). OAS Joins in Recognizing October as "Cybersecurity Awareness Month." Communiqué disponible à l'adresse internet https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-474/14.

**48.** https://www.concienciadigital.gob.cl/

**49.** https://www.enticconfio.gov.co/

# Des recommandations pratiques

Cette section offre un survol des différents outils et programmes que les décideurs politiques et les enseignants pourraient développer en Amérique latine et dans les Caraïbes pour accroître les connaissances et les compétences de l'actuelle main-d'œuvre de la région, et répondre activement aux objectifs généraux et spécifiques du Plan d'action en éducation à la cybersécurité.

## Les conférences et discussions en classe

Des cours innovateurs et dynamiques sur la cybersécurité qui encouragent la discussion des concepts de base et introduisent peu à peu des concepts plus complexes au cours du cycle éducatif, permettent de préparer les étudiants pour le marché du travail. Les enseignants pourraient introduire des concepts de cybersécurité dans les cours existants ou organiser des ateliers spécifiques sur le sujet. Par exemple, l'OEA, en partenariat avec la Citi Foundation, a développé le projet « Creating a Career Path in Digital Security, Pathways2Progress », qui offre un cours technique de 48 heures sur la sécurité numérique pour les étudiants collégiaux de 17 à 25 ans. L'Institut national espagnol de la cybersécurité (INCIBE) organise aussi des « Espaces sur la cybersécurité » où, pendant trois heures, on offre un cours technique et pratique à des classes de 20 à 30 étudiants âgés de 16 à 18 ans. Il s'agit là d'exemples de cours qui encouragent les jeunes à entreprendre une carrière en cybersécurité.

## Les foires aux carrières

Il est important d'encourager la réalisation de foires aux carrières et de campagnes d'information sur les carrières en cybersécurité, compte tenu que la plupart des étudiants des pays d'Amérique latine n'ont pas accès à des cours liés à la cybersécurité et connaissent très peu les opportunités existantes dans le domaine (Catota; Morgan; Sicker, 2019). Les foires aux carrières devraient non seulement s'adresser aux étudiants mais aussi aux parents, compte tenu que ceux-ci sont souvent appelés à aider leurs enfants à choisir leur plan de carrière. Par exemple, l'initiative NICE aux États-Unis organise la « NICE K-12 Cybersecurity Education Conference »,[52] qui réunit les enseignants, les professionnels, les chercheurs, les organismes à but non lucratif et les étudiants afin de discuter des stratégies possibles pour conscientiser les étudiants et les parents de l'existence de cheminements de carrière en cybersécurité.

## Les formations et laboratoires en ligne

Il existe un certain nombre de programmes en ligne et webinaires qui offrent une gamme de cours de divers niveaux sur la cybersécurité pour un public diversifié. Au sein de plusieurs pays d'Amérique latine, les personnes se rendent en ligne via les laboratoires publics d'innovation, et ces laboratoires pourraient inclure des formations en ligne. Les gouvernements devraient conjuguer leurs projets d'accessibilité aux TIC à une offre de formations en ligne sur la cybersécurité.

Des plateformes telles que AWS Educate et CISCO Academy, mentionnées précédemment, constituent de bons exemples de formations disponibles en ligne. Chaque trimestre, Microsoft offre aussi un Programme professionnel sur la cybersécurité qui s'étend sur trois mois.[53] Les MOOC (Massive Online Open Courses) sont devenus aussi des outils essentiels pour le renforcement des capacités en cybersécurité. Des plateformes telles que Coursera, edX,[54] Udacity, et Pluralsight, offrent une panoplie de cours et même des programmes de maîtrise en espagnol validés par des universités reconnues.[55]

En somme, les formations et laboratoires en ligne représentent une option intéressante pour les étudiants de pays où les formations en cybersécurité sont rares ou peu accessibles à cause de leur coût très élevé. Grâce aux partenariats public-privé, les gouvernements nationaux et locaux devraient saisir l'opportunité et utiliser ces plateformes en ligne pour former leur main-d'œuvre sur les enjeux de la cybersécurité. L'industrie a développé plusieurs de ces plateformes en fonction des qualifications qu'elle recherche d'un employé.

## Les concours / les approches ludiques

Les concours peuvent améliorer le niveau de conscientisation, encourager le travail en équipe, et permettre aux participants de faire face à un incident de cybersécurité tel qu'ils ont cours dans la réalité et ce, dans un environnement contrôlé sous la supervision d'experts. La structure de ces simulations se rapproche beaucoup des attaques réelles auxquelles se confrontent les organisations du monde. De plus, les concours offrent aux concurrents une occasion de se réseauter et de partager des informations, et représentent aussi une opportunité pour encourager la diversité dans le domaine de la cybersécurité.

Le National Cybersecurity Centre (NCSC) au Royaume-Uni, par exemple, organise le CyberFirst Girls Competition pour les jeunes filles du pays, encourageant ainsi la prochaine génération de femmes à faire carrière dans le domaine de la cybersécurité.[56] De la même façon, en Amérique latine, l'OEA organise le CyberWomen Challenge en partenariat avec Trend Micro, où des équipes composées exclusivement de femmes sont appelées à contrer efficacement des cyberattaques.[57] Les jeux et quiz en ligne représentent aussi une façon interactive de capter l'attention du grand public et l'amener à apprendre les bonnes pratiques de cybersécurité.

Les idées d'initiatives politiques ne manquent pas pour ancrer plus profondément la cybersécurité dans les stratégies éducatives. La mise en œuvre efficace de politiques d'éducation à la cybersécurité peut aboutir à une plus grande priorité accordée à la cybersécurité en général. Tel que l'a souligné ce Livre blanc, le premier pas que doivent franchir les décideurs politiques est de reconnaître la nécessité d'intégrer la cybersécurité au monde de l'éducation. Par la suite, il est fondamental de bâtir un Plan d'action en éducation à la cybersécurité qui permette de définir les objectifs généraux et spécifiques, et les instruments de mesure. Sur cette base, les décideurs politiques peuvent décider d'intégrer différents acteurs au processus, notamment le secteur privé, le monde académique, et même la société civile par l'entremise de partenariats public-privé-secteur académique. Suivant leur champ de compétence, ces acteurs déploieront de multiples efforts en fonction de l'objectif global d'éduquer le public sur la cybersécurité, de façon à ce que la population soit plus consciente des cyber-enjeux. Certains exemples relèvent de stratégies éducatives au niveau du primaire et du secondaire, d'autres à encourager les étudiants à entreprendre des études postsecondaires en cybersécurité, des stages d'apprentissage, ou encore à assurer leur formation continue et à obtenir des certifications. En vue d'une rapide intégration, on doit aussi envisager des initiatives politiques sur la cybersécurité à un niveau micro, comme les conférences et discussions en classe, les foires aux carrières, et les laboratoires de formation.

# Conclusion

Afin de formuler et mettre en œuvre un Plan d'action en éducation à la cybersécurité, les gouvernements d'Amérique latine et des Caraïbes doivent coordonner leurs efforts avec le secteur privé, la société civile et le monde académique. La pénurie de professionnels qualifiés en cybersécurité exige une action immédiate pour former les professionnels actuels de la cybersécurité et éduquer la main-d'œuvre de la prochaine génération. Afin de combler le manque de main-d'œuvre spécialisée, totalisant 600 000 personnes en Amérique latine et atteignant 4 millions de personnes au niveau mondial, il est nécessaire que les gouvernements adoptent une approche stratégique et collaborent avec le secteur privé et le monde académique pour élaborer et mettre en œuvre un Plan d'action en éducation à la cybersécurité, ou CEAP. Un CEAP est un modèle de référence qui oriente les décideurs politiques et les aident à formuler des politiques publiques efficaces qui permettent de consolider les stratégies nationales de cybersécurité et de développer une main-d'œuvre qualifiée en cybersécurité ; un CEAP peut contribuer à mieux préparer la main-d'œuvre en matière de cybersécurité et mieux conscientiser la population. Un CEAP est composé principalement :

(1) d'objectifs généraux clairs et définis qui donnent priorité et intègrent l'éducation à la cybersécurité à tous les niveaux, et orientent les actions des décideurs politiques ;

(2) d'une approche qui s'appuie sur la diversité des parties intéressées ;

(3) de mécanismes de suivi et d'indicateurs qui mesurent le progrès réalisé par rapport aux objectifs du plan d'action.

Une panoplie d'outils sont à la disposition des décideurs politiques afin de mettre en œuvre un CEAP et mettre sur pied des programmes adaptés en fonction des âges, pour stimuler l'éducation et la conscientisation à la cybersécurité, tant au niveau des écoles primaires que pour les professionnels qui souhaitent une formation continue. La gamme de programmes inclut les laboratoires en ligne, les foires aux carrières, les conférences et discussions en classe, en passant par les concours et les approches ludiques. Au fil de la maturation des étudiants, les opportunités se multiplient, dont les stages d'apprentissage en cybersécurité, les programmes d'études supérieures, les options de formation continue et les certifications.

Le Plan stratégique NICE représente un bon exemple des façons d'élaborer un plan d'action ciblant les niveaux du primaire et du secondaire. Le « National K-12 Cybersecurity Education Implementation Plan » vise à: 1) encourager les élèves à entreprendre des activités liées à la cybersécurité; 2) soutenir les enseignants pour qu'ils incorporent des concepts de cybersécurité dans leurs cours en classe; et finalement 3) aider les élèves des niveaux primaire et secondaire à identifier des opportunités de carrière dans le domaine de la cybersécurité. Le développement de l'éducation et de la main-d'œuvre comporte plusieurs phases, et le déploiement d'un plan d'éducation à la cybersécurité, quel qu'il soit, doit en tenir compte. L'éducation du primaire au postsecondaire, les programmes de formation continue et la R&D, jouent un rôle significatif pour renforcer la main-d'œuvre en cybersécurité. Plusieurs outils peuvent être développés

pour promouvoir l'éducation à la cybersécurité à chacune des phases du cycle de développement de la main-d'œuvre. Il est possible de renforcer les capacités au niveau national, à tous les stades éducatifs et de développement de la main-d'œuvre, en intégrant et adaptant à chaque phase des éléments spécifiques de cyber-éducation. Que ce soit aux niveaux du primaire et du secondaire qu'au niveau de la Recherche et Développement, chacun peut trouver son compte dans les diverses initiatives de cyber-éducation qui permettent l'acquisition de compétences relationnelles tangibles.

Les pays d'Amérique latine pourront récolter les bienfaits de la Quatrième Révolution industrielle dans la mesure où ils investissent dans leurs gens et dans la technologie. L'innovation émergera des nouvelles opportunités d'affaires et des interactions sociales uniquement quand la technologie et les travailleurs qualifiés entreront en synergie. L'Amérique latine, comme toutes les régions du monde, a besoin d'une main-d'œuvre qui détienne les connaissances et compétences nécessaires pour construire et opérer les technologies émergentes et futures, et qui soit capable de les sécuriser.

# Références

Catota, F. E.; Morgan, M.G.; and Sicker, D.C. (2019). Cybersecurity education in a developing nation: the Ecuadorian environment, Journal of Cybersecurity, Volume 5, Issue 1. Disponible à l'adresse internet https://doi.org/10.1093/cybsec/tyz001

Cybersecurity Ventures (2019). 2019 Official Annual Cybercrime Report. Disponible à l'adresse internet https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Deloitte (2019). Tech Trends 2019. Disponible à l'adresse internet https://www2.deloitte.com/content/dam/Deloitte/br/Documents/technology/DI_TechTrends2019.pdf

Deloitte (2018a). The jobs are here, but where are the people? Disponible à l'adresse internet https://www2.deloitte.com/us/en/pages/manufacturing/articles/future-of-manufacturing-skills-gap-study.html

Deloitte (2018b). Preparing tomorrow's workforce for the Fourth Industrial Revolution. Disponible à l'adresse internet https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-preparing-tomorrow-workforce-for-4IR.pdf.

ENISA (2019). Cybersecurity Culture Guidelines: Behavioral Aspects of Cybersecurity. Disponible à l'adresse internet https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

ENISA (2015). Status of Privacy and NIS course curricula in Member States. Disponible à l'adresse internet https://www.enisa.europa.eu/publications/status-of-privacy-and-nis-course-curricula-in-eu-member-states

Gleason, N. W. (Ed.). (2018). Higher education in the era of the fourth industrial revolution. Singapore: Palgrave Macmillan.

Global Cyber Security Capacity Centre (2016). Cybersecurity Capacity Maturity Model for Nations (CMM) – Revised Edition. Disponible à l'adresse internet https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf.

IBM (2018). IBM X-Force Threat Intelligence Index 2018. Disponible à l'adresse internet https://www.ibm.com/downloads/cas/MKJOL3DG

Inter-American Development Bank – IDB (2016). The Road toward Smart Cities: Migrating from Traditional City Management to the Smart City. Disponible à l'adresse internet https://publications.iadb.org/en/road-toward-smart-cities-migrating-traditional-city-management-smart-city

IDB (2018). Factores de éxito y aprendizajes obtenidos de la formación de alianzas público-privadas. Disponible à l'adresse internet https://publications.iadb.org/es/factores-de-exito-y-aprendizajes-obtenidos-de-la-formacion-de-alianzas-publico-privadas

(ISC)2 (2019). Strategies for Building and Growing Strong Cybersecurity Teams. (ISC)2 Cybersecurity Workforce Study, 2019. Disponible à l'adresse internet https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=D087F6468B4991E0BEFFC017BC1ADF59CD5A2EF7

(ISC)2 (2018). Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens. (ISC)2 Cybersecurity Study, 2018. Disponible à l'adresse internet https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0

(ISC)2 (2017). Global Information Security Workforce Study. Disponible à l'adresse internet https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx

International Telecommunication Union – ITU (2019). Global Cybersecurity Index (GCI) 2018. Disponible à l'adresse internet https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

Lewis, J. (2018). Economic Impact of Cybercrime – No Slowing Down. Disponible à l'adresse internet https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1ldhuHd&utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70-1940938

Kelly, K. (2016). The inevitable: understanding the 12 technological forces that will shape your future. New York, NY: Penguin Books.

McAfee (2017). Hacking the Skills Shortage: A study of the international shortage in cybersecurity skills. Disponible à l'adresse internet https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf

McKinsey & Company (2018). Insider Threat: The human element of cyberrisk. Disponible à l'adresse internet https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk.

National Cybersecurity Alliance – NCSA (2017). Securing our Future: Cybersecurity and the Millennial Workforce. Disponible à l'adresse internet https://www.raytheon.com/sites/default/files/2017-12/2017_cyber_report_rev1.pdf

National Initiative for Cybersecurity Education – NICE (2017). National K-12 Cybersecurity Education Implementation Plan. Disponible à l'adresse internet https://www.nist.gov/sites/default/files/documents/2017/04/26/nice_k12_implementation_plan.pdf

National Institute of Standards and Technology – NIST (2017). NIST Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Disponible à l'adresse internet https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

Open Web Application Security Project – OWASP (2016). Security by Design Principles. Disponible à l'adresse internet https://www.owasp.org/index.php/Security_by_Design_Principles

Organization of American States – OAS (2016). Cybersecurity Awareness Campaign Toolkit. Disponible à l'adresse internet https://www.thegfce.com/documents/publications/2015/10/01/cybersecurity-awareness-campaign-toolkit

Organization for Economic Cooperation and Development – OECD (2012). The Protection of Children Online: Recommendations of the OECD Council. Disponible à l'adresse internet

Organization for Economic Cooperation and Development – OECD (2016). Start-up Latin America 2016: building an innovative future. Disponible à l'adresse internet https://www.oecd.org/dev/americas/Startups2016-Assessment-and-Recommendations.pdf

Organization for Economic Cooperation and Development – OECD (2017). Latin America Economic Outlook 2017 – Youth, Skills and Entrepreneurship. Disponible à l'adresse internet https://www.oecd.org/dev/americas/Overview_LEO2017.pdf

Organization for Economic Cooperation and Development – OECD (2019). Measuring Innovation in Education 2019: What has changed in the classroom? Disponible à l'adresse internet

Ponemon Institute (2018). 2018 Cost of a Data Breach Study: Global Overview. Disponible à l'adresse internet https://www.ibm.com/downloads/cas/861MNWN2

Ponemon Institute (2019). Ninth Annual Cost of Cybercrime Study: Unlocking the Value of Improved Cybersecurity Protection. Disponible à l'adresse internet https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Schwab, K. (2016). The Fourth Industrial Revolution. New York, NY: Crown Business

Symantec (2018). Internet Security Threat Report. Disponible à l'adresse internet http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_

Symantec (2019). Internet Security Threat Report. Disponible à l'adresse internet https://img03.en25.com/Web/Symantec/%7Bdfc1cc41-2049-4a71-8bd8-12141bea65fd%7D_ISTR_24_2019_en.pdf

Wagner, D. A., et al. (2005). Monitoring and evaluation of ICT in education projects: a handbook for developing countries. Washington, DC: InfoDev.

World Economic Forum – WEF (2014). Creating New Models: Innovative Public-Private Partnerships for Inclusive Development in Latin America. Disponible à l'adresse internet http://www3.weforum.org/docs/GAC/2014/WEF_GAC_LatinAmerica_InnovativePublicPrivatePartnerships_Report_2014.pdf

World Economic Forum – WEF (2015a). Bridging the Skills and Innovation Gap to Boost Productivity in Latin America. Disponible à l'adresse internet https://www2.deloitte.com/content/dam/Deloitte/cr/Documents/finance/201501-Competitiveness_Lab_Latin_America_final.pdf

World Economic Forum – WEF (2015b). Deep Shift: technology tipping points and societal impact. Disponible à l'adresse internet http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

# _ ÉDUCATION A LA _
# CYBERSÉCURITÉ

## Planifier l'avenir par le développement de la main-d'œuvre

CICTE01316E05

OEA Plus de droits pour plus de personnes

aws

# _ ÉDUCATION A LA _ CYBERSÉCURITÉ

## Planifier l'avenir par le développement de la main-d'œuvre

White paper series
**Édition 9**

**2020**