2019

White paper series
Édition 5

CADRE DE CYBERSÉCURITÉ DU NIST

Une approche intégrale de la cybersécurité

OEA Plus de droits pour plus de personnes

aws

— CADRE DE CYBERSÉCURITÉ —

DU NIST

Une approche intégrale
de la cybersécurité

CRÉDITS

Luis Almagro

Secrétaire général
de Organisation des États
Américains (OEA)

Équipe technique de l'OEA

Farah Diva Urrutia
Alison August Treppel
Belisario Contreras
Santiago Paz
Fabiana Santellán
Kerry-Ann Barrett
Nathalia Foditsch
Diego Subero
David Moreno
Mariana Cardona
Jaime Fuentes
Miguel Ángel Cañada

Équipe technique de AWS

Abby Daniell
Michael South
Andres Maz
Melanie Kaplan
Min Hyun

CONTEU

1. Introduction

Compte tenu de la constante augmentation des attaques cybernétiques enregistrées aux États-Unis, le 12 février 2013, le président Barack Obama a émis le décret 13636 [1] visant à charger l'Institut national des standards et de la technologie (NIST, National Institute of Standards and Technology) d'élaborer le Cadre de cybersécurité pour la protection des infrastructures critiques, également connu comme le Cybersecurity Framework (CSF). Les États-Unis ont identifié 16 secteurs d'infrastructures comme étant critiques : le secteur des produits chimiques, des installations commerciales, des communications, de la fabrication essentielle, des barrages, des bases industrielles de défense, des services d'urgence, de l'énergie, des services financiers, de l'alimentation, de l'agriculture, des installations gouvernementales, de la santé et de la santé publique, des technologies de l'information, des réacteurs nucléaires, des matériaux et déchets, des systèmes de transport et des réseaux d'aqueduc et d'assainissement. [18]

Le Cadre a été conçu dans le but d'identifier les normes et directrices en matière de sécurité, applicables à tous les secteurs d'infrastructures critiques. Il propose une approche flexible et reproductible, permettant de prioriser les activités et d'obtenir de bonnes performances de la part des infrastructures, tout en demeurant rentable pour les entreprises.

Il s'agit, sans aucun doute, d'un outil de gestion des risques en matière de cybersécurité, qui permet l'innovation technologique et s'adapte à tout type d'organisation (quelle que soit sa taille ou son secteur d'activité).

Le Cadre s'est fondé sur les normes industrielles déjà acceptées par l'écosystème de la cybersécurité (NIST SP 800-53 Rev.4[2], ISO/IEC 27001:2013[3], COBIT 5[4], CIS CSC[5], etc…). Il offre une approche simple de la gouvernance en matière de cybersécurité, qui permet de traduire facilement des concepts techniques en objectifs et besoins pour les entreprises. Ce cadre a été élaboré suivant une méthodologie participative, à laquelle toutes les parties prenantes (gouvernement, industrie, académie) ont pu participer et apporter des améliorations.

Le CSF est innovant car il propose de laisser de côté les normes rigides qui étaient d'usage. Toutefois, il n'a pas été le premier à développer une initiative visant à protéger les infrastructures critiques. L'OTAN avait déjà élaboré une série de guides axés sur la protection des infrastructures critiques pour la défense nationale, tels que le « Guide du cadre de travail en matière de cybersécurité nationale » (National Cyber Security Framework Manual) [14]. Cela ne signifie donc pas que le CSF du NIST ne tienne pas compte de ces documents. Bien au contraire, il les complète et les améliore.

La grande différence du CSF par rapport à ses prédécesseurs est sa simplicité et sa flexibilité. En effet, simplicité car il permet d'exprimer une stratégie technique en des termes compréhensibles pour l'entreprise puis, flexibilité car il peut être adapté à toute organisation. C'est cette différence qui, jusqu'à maintenant, explique que l'industrie et la communauté technique à travers le monde aient accueilli favorablement ce cadre. Les entreprises, les universités et les gouvernements ont volontairement intégré le CSF à leur stratégie de cybersécurité. Les principales organisations d'élaboration de normes et standards ont également intégré le CSF à leurs stratégies. Tel est le cas de ISACA et ISO. De fait, ISO a élaboré la norme ISO/IEC TR 27103:2018 [6] qui fournit des orientations sur la manière de tirer parti des normes existantes dans le cadre de la cybersécurité. En d'autres termes, sur la façon d'utiliser le CSF.

2. Cadre de cybersécurité du NIST (CSF)

2.1. Histoire du CSF

Le processus d'élaboration du Cadre a débuté aux États-Unis par le Décret-loi numéro 13636, publié le 12 février 2013. Le décret-loi a permis de développer des initiatives visant à partager les informations en matière de menaces à la cybersécurité et à élaborer un ensemble d'approches actuelles et efficaces, soit un cadre permettant de réduire les risques liés aux infrastructures critiques. Par ce décret-loi, le NIST a pris en charge l'élaboration du « Cybersecurity Framework » (Cadre de Cybersécurité).

Pour son élaboration, il a été nécessaire de définir certaines exigences telles que : identifier des normes et règlements en matière de sécurité, applicables à tous les secteurs d'infrastructures critiques, fournir une approche prioritaire, souple, reproductible et axée sur le rendement et la rentabilité, aider à identifier, évaluer et gérer le cyberrisque, inclure des recommandations pour mesurer l'efficacité de la mise en œuvre du Cadre de Cybersécurité et déterminer les domaines d'améliorations devant être abordés par une collaboration future avec des secteurs spécifiques et organismes d'élaboration de normes.

Création du Cadre

Le Cadre a été, et continue d'être, développé et promu au travers de l'engagement continu et des contributions des parties prenantes du gouvernement, de l'industrie et du milieu académique. Afin d'élaborer le cadre, le NIST a procédé, pendant toute une année, à une demande d'information (RFI) et à un appel aux commentaires (RFC), ainsi qu'à une large diffusion et réalisation d'ateliers à travers les États-Unis pour : (i) identifier les normes, directives, cadres et meilleures pratiques en matière de cybersécurité, appliqués pour renforcer la sécurité des infrastructures critiques et d'autres secteurs concernés, (ii) préciser les brèches, hautement prioritaires, pour lesquelles des normes nouvelles ou révisées ont été nécessaires et (iii) prévoir des plans d'action en collaboration permettant de combler ces brèches.

Pour la mise à jour du CSF à la version 1.1, publiée en avril 2018, le NIST a poursuivi sa stratégie de développement participatif en comptant sur la participation d'experts, du secteur de l'industrie, des gouvernements ainsi que des entreprises non américaines, tels que le gouvernement israélien et la société Huawei Technologies. [17]

2.2. Structure du CSF

Le Cybersecurity Framework (CSF) se compose de trois éléments principaux :

- Framework Core
- Niveaux de mise en œuvre (Tiers)
- Profils

Framework Core

Le Core représente un ensemble d'activités et résultats escomptés en matière de cybersécurité, organisés en catégories et alignés sur des références informationnelles par rapport aux normes acceptées par l'industrie. Il est conçu pour être intuitif et servir d'interface pour permettre la communication entre les différentes équipes multidisciplinaires grâce à l'utilisation d'un langage simple et non technique.

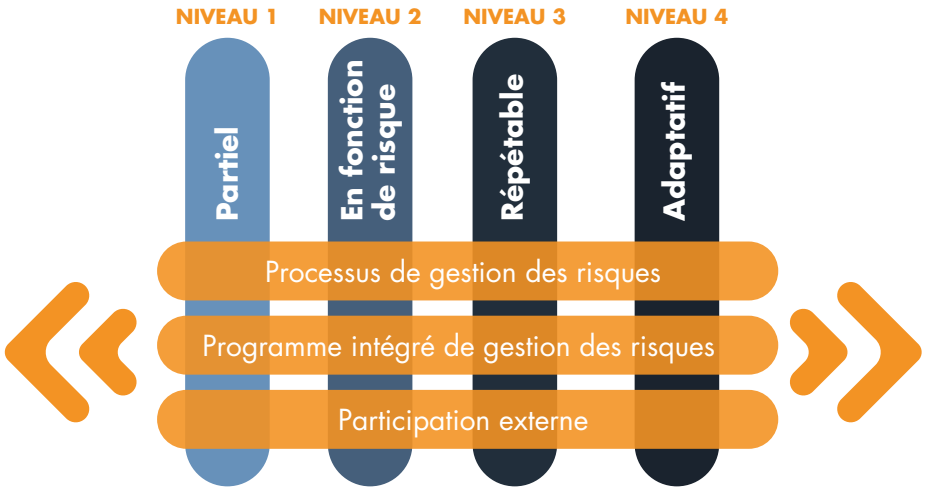
Le Core se compose de trois parties : Fonctions, Catégories et Sous-catégories. Il comprend cinq **fonctions** de haut niveau : Identification, Protection, Détection, Réponse et Reprise.

Ces cinq fonctions se divisent elles-mêmes en 23 **catégories**. Ces dernières ont été conçues pour couvrir l'ensemble des objectifs de cybersécurité d'une organisation, sans rentrer trop dans le détail. Elles permettent d'aborder tous les sujets liés aux aspects techniques, aux personnes et aux processus et mettent l'accent sur les résultats.

Les **sous-catégories** représentent le niveau le plus profond d'abstraction du Core. Il y a 108 sous-catégories. Il s'agit de recommandations fondées sur des résultats qui permettent de fournir des observations permettant de créer ou améliorer un programme de cybersécurité. Etant donné que le Cadre est axé sur les résultats et ne précise pas comment une organisation devrait atteindre ces dits résultats, il permet des mises en œuvre basées sur les risques et qui s'adaptent aux besoins des différentes entreprises.

Niveaux de mise en œuvre du CSF

Ces niveaux décrivent les caractéristiques représentatives des pratiques de gestion des risques en matière de cybersécurité des entreprises. Les niveaux vont de Partiel (niveau 1) à Adaptatif (niveau 4). Ils décrivent un degré croissant de rigueur, la mesure dans laquelle les décisions liées aux risques de cybersécurité sont intégrées dans les décisions plus générales en matière de risques ainsi que la mesure dans laquelle l'organisation partage et reçoit des informations de sources externes sur la cybersécurité.



Bien que le NIST insiste sur le fait que les niveaux ne représentent pas nécessairement les niveaux de maturité des entreprises, dans la pratique, ils sont similaires. L'essentiel est que les organisations déterminent le niveau souhaité (tous les contrôles ne doivent pas être mis en œuvre au plus haut niveau), en s'assurant que le niveau choisi réponde au moins aux objectifs de l'organisation. Cela permet, ainsi, de diminuer le risque de cybersécurité à des niveaux acceptables, a un coût raisonnable et que sa mise en œuvre soit réalisable.

Profils

Les profils représentent l'alignement unique d'une organisation sur ses exigences, ses objectifs organisationnels, sa tolérance au risque et ses ressources par rapport aux résultats escomptés du Framework Core. Ils peuvent être utilisés pour identifier les opportunités d'amélioration de la position adoptée en matière de cybersécurité en comparant un profil "actuel" avec un profil "cible".

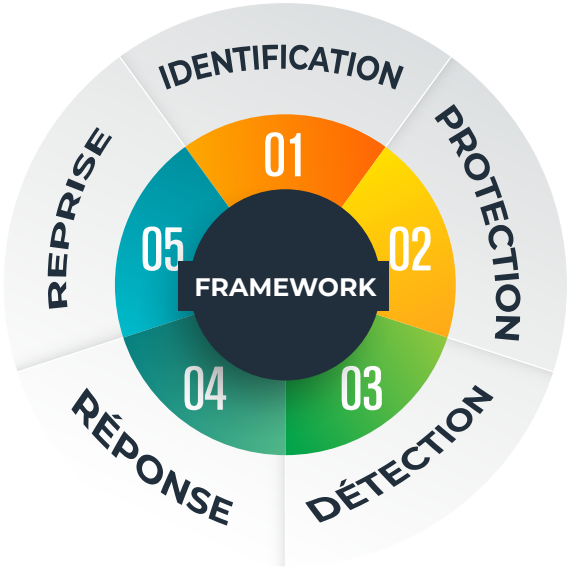
L'identification du profil actuel permet aux organisations d'effectuer un examen objectif (sans que cela n'implique d'audit formel ou d'autres évaluations techniques) de leur programme de cybersécurité par rapport au CSF et de connaître exactement leur situation actuelle en matière de sécurité.

En tenant compte de l'évaluation des risques organisationnels, des exigences en matière de conformité et des objectifs organisationnels, il est possible de créer un Profil Cible qui, comparativement au profil actuel, renseignera sur la stratégie de leadership, les priorités en matière de recrutement, la formation, les changements de politiques, les changements de procédures et l'acquisition de technologies.

2.3. Fonctions du CSF

Les cinq fonctions incluses dans le Framework Core sont les suivantes :

1. Identification
2. Protection
3. Détection
4. Réponse
5. Reprise



Les fonctions représentent le plus haut niveau d'abstraction du Cadre. Ils constituent l'épine dorsale du Framework Core autour de laquelle s'organisent tous les autres éléments.

Ces cinq fonctions ont été choisies parce qu'elles représentent les cinq principaux piliers de tout programme de cybersécurité efficace et intégral. Elles aident les organisations à exprimer facilement leur gestion des risques liés à la cybersécurité à un niveau élevé et permettent de prendre des décisions en matière de gestion des risques.

Identification

Cette fonction aide à développer une compréhension organisationnelle permettant de gérer le risque en matière de cybersécurité des systèmes, des personnes, des actifs, des données et des capacités. La compréhension du contexte commercial, des ressources qui soutiennent les fonctions critiques et des risques associés à la cybersécurité permettent à une organisation de concentrer et de prioriser ses efforts conformément à sa stratégie de gestion des risques et à ses besoins commerciaux.

Protection
Cette fonction décrit les mesures de sécurité appropriées permettant de garantir que les infrastructures critiques puissent assurer la prestation de leurs services. Cette fonction envisage la possibilité de limiter ou de contenir l'impact d'une menace potentielle en matière de cybersécurité.

Détection
Il s'agit ici de définir les activités nécessaires d'identification de survenue d'un incident de cybersécurité pour permettre ainsi la détection à temps de ceux-ci.

Réponse
Cette fonction regroupe toutes les activités nécessaires visant à prendre des mesures à l'égard d'un incident de cybersécurité ayant été détecté. Elle permet de développer la capacité à pouvoir contenir l'impact d'un incident potentiel.

Reprise
Il s'agit d'identifier les activités nécessaires pour maintenir les programmes de résilience et pour rétablir toute compétence ou service ayant été détérioré en raison d'un incident de cybersécurité. Cette fonction permet la reprise rapide des opérations normales afin de réduire l'impact d'un incident de cybersécurité.

2.4. Versions et mécanismes d'évolution

Le CSF a été développé et promu au travers de l'engagement continu et des contributions des parties prenantes du gouvernement, de l'industrie et du milieu académique. Cela comprend un processus public ouvert d'examen et de commentaires, d'ateliers et d'autres moyens de participation.

Le graphique ci-dessous présente l'évolution du Cadre de cybersécurité :

3. ¿Comment utiliser le CSF?

Le CSF est présenté comme un outil permettant de gérer les risques liés à la cybersécurité, de façon flexible et adaptable à la réalité de toute organisation, quelle que soit sa taille ou son secteur d'activité.

Il est important de souligner que le Cadre ne propose pas de nouveaux contrôles ou processus, mais regroupe les contrôles proposés par les principales normes de l'industrie, reconnues au niveau international (exemple : le NIST SP 800-53, ISO 27001, COBIT 5 etc…). Par conséquent, il ne remplacera pas les processus et les contrôles déjà mis en place par l'organisation. Cette dernière continuera d'utiliser ce qu'elle a déjà développé et pourra éventuellement les compléter, afin de présenter une stratégie avec une approche plus exécutive et axée sur les résultats.

3.1. Stratégie d'adoption du CSF

Ci-dessous nous présenterons trois stratégies possibles, proposées dans le Cadre [11], pour l'utilisation du CSF. Celles-ci ne sont pas les seules stratégies envisageables.

Examen de base des pratiques en matière de cybersécurité

Une organisation peut utiliser le Cadre comme un élément clé de son processus systématique de gestion des risques en matière de cybersécurité. En effet, celui-ci n'est pas conçu pour remplacer les processus existants, mais pour déterminer les lacunes dans son approche actuelle des risques en matière de cybersécurité et élaborer une feuille de route pour une amélioration au travers d'une optimisation des coûts et des résultats.

Créer ou améliorer un programme de cybersécurité

Le Cadre est conçu pour compléter les opérations commerciales et de cybersécurité existantes. Il peut servir de base à la création d'un nouveau programme de cybersécurité ou comme outil visant à améliorer un programme existant.

Les 7 étapes suivantes peuvent guider la création d'un nouveau programme de cybersécurité ou améliorer un programme existant. Ces étapes doivent être répétées, au besoin, afin d'améliorer et évaluer continuellement la cybersécurité :

Étape 1 : Établir l'ordre de priorité et déterminer la portée. Les objectifs commerciaux et les priorités de haut niveau de l'organisation doivent être identifiés. Cette information permet alors de déterminer la portée du programme de cybersécurité : quels business units ou processus seront abordés.

Étape 2 : Orientation. Les systèmes et actifs liés à la portée, aux exigences légales ou réglementaires, ainsi qu'à l'approche globale du risque, sont ici identifiés.

Étape 3 : Créer un profil actuel. Une évaluation du programme de cybersécurité est effectuée afin de créer un profil actuel qui indiquera la catégorie et la sous-catégorie du Framework Core à laquelle vous appartenez. Il est essentiel que cette évaluation porte sur les personnes (nombre d'employés, rôles, compétences, formation des professionnels de la sécurité et connaissances générales des utilisateurs), les processus (stratégie, politiques, procédures, manuel ou automatisation, canaux de communication avec les parties prenantes etc...) et la technologie (capacités, configurations, vulnérabilités, correctifs, opérations et contrats d'assistance etc…)

Étape 4 : Réaliser une évaluation des risques. L'environnement opérationnel est analysé pour repérer la probabilité de survenue d'un incident cybernétique et l'impact que cet incident pourrait avoir sur l'organisation. Il est important que les organisations identifient les risques émergents en déterminant les vulnérabilités des actifs et en prenant en compte les informations provenant de sources internes et externes, sur les menaces afin de mieux entrevoir les probabilités et l'impact des incidents cybernétiques. Bien que cette étape soit axée sur l'identification des risques liés à la cybersécurité, il est important que ce processus soit aligné sur l'évaluation des risques organisationnels ainsi que sur l'évaluation des risques opérationnels afin d'obtenir un feedback des évaluations.

Étape 5 : Créer un Profil Cible. L'on doit s'axer sur l'évaluation des catégories et sous-catégories du Cadre qui décrivent les résultats escomptés de l'organisation en matière de cybersécurité, en gardant toujours à l'esprit la mission, les objectifs de l'entreprise et toutes les exigences légales ou réglementaires. Les entreprises peuvent également développer leurs propres Catégories additionnelles, en fonction des exigences commerciales, des parties prenantes externes, telles que les entités du même secteur, de leurs clients et leurs partenaires commerciaux. Il ne faut pas non plus oublier que les exigences ne sont pas seulement techniques ou technologiques, mais aussi associées au personnel, à la formation, aux politiques, aux procédures et autres besoins administratifs.

Étape 6 : Identifier, analyser et prioriser les lacunes. Le profil actuel et le Profil Cible sont comparés pour déterminer les brèches. Puis, un plan d'action priorisant les lacunes à combler (reflétant les moteurs, les coûts, les avantages et les risques de la mission) doit être créé afin d'atteindre les résultats du Profil Cible. L'organisation détermine ensuite les ressources nécessaires pour combler les lacunes, y compris le financement et la main-d'œuvre.

Étape 7 : Mettre en œuvre le plan d'action. Les actions à mettre en œuvre pour combler les lacunes identifiées à l'étape précédente, le cas échéant, seront développées. Puis, les pratiques actuelles en matière de cybersécurité seront réajustées pour atteindre le Profil Cible. Il est important que les actions tiennent compte de tous les aspects de la gouvernance en matière de cybersécurité : Personnel (recrutement, formation, éducation etc...), Technologie (solutions actuelles, solutions commerciales disponibles, nouveaux développements, innovation etc...) et les processus (politiques, processus et procédures adaptés aux besoins et à la réalité de l'organisation).

Communiquer les exigences en matière de cybersécurité aux parties prenantes

Le Cadre peut fournir un moyen d'exprimer les exigences en matière de cybersécurité aux partenaires commerciaux, aux clients et aux fournisseurs, en particulier aux fournisseurs de services ou de produits liés à l'infrastructure critique de l'organisation.

3.2. Principaux défis

Le CSF doit faire face au grand défi de s'adapter à différents secteurs, industries et même pays. Il n'utilise pas de normes spécifiques pour satisfaire aux contrôles de cybersécurité, mais s'en abstient en utilisant une approche conceptuelle et en proposant une liste de diverses normes possibles pour satisfaire ces exigences de contrôle. De cette façon, il peut être utilisé dans différents domaines tels que celui des infrastructures critiques, du gouvernement ou du secteur privé.

De toute évidence, pour d'identifier les principaux défis, la mise en œuvre du CSF dépendra du point de départ de chaque organisation. D'une manière générale, la plupart des organisations se heurtent à certaines difficultés qui, en grande partie, sont dues au manque d'engagement de la part de la haute direction dans l'adoption d'une stratégie de cybersécurité, le développement d'une culture organisationnelle en matière de risque [16] et le manque de professionnels qualifiés pour diriger ces processus [15].

Selon le rapport de l'OEA intitulé : « Cybersécurité : Sommes-nous prêts en Amérique latine et dans les Caraïbes ? » [12] publié en 2016, les aspects liés à la politique et la stratégie de cybersécurité des pays sont l'un des points à renforcer dans toute la région de l'Amérique latine et des Caraïbes. Nous comprenons que l'adoption de ce type de cadre peut contribuer, de façon positive, au développement de stratégies de cybersécurité des gouvernements (en particulier, pour la protection de leurs infrastructures critiques) et au renforcement des processus de collaboration dans la région.

4. Études de cas

Le CSF est, de nos jours, un cadre reconnu par la communauté technique, qui envisage les meilleures pratiques à développer en matière de cybersécurité. Ce cadre a été adopté par un certain nombre de pays pour leur stratégie de cybersécurité et certains l'ont même inclus dans leur législation nationale. Parmi tous les pays qui ont adopté le CSF, se trouvent : Les Bermudes, les États-Unis, Israël, l'Italie, le Japon, le Royaume-Uni, la Suisse et l'Uruguay [13].

Nous présenterons ci-dessous deux cas ayant optés pour des approches d'adoption différentes.es.

4.1. Royaume-Uni - Une approche ouverte

Le Royaume-Uni dispose d'un cadre de politiques de sécurité (HMG Security Policy Framework - SPF) [7] qui est obligatoire pour tous les ministères du gouvernement. Pour faciliter la mise en œuvre du dit Cadre, une série de guides ont été élaborés afin d'aborder les divers aspects de la sécurité, y compris de la Norme minimale de cybersécurité (MCSS - Minimum Cyber Security Standard) [8].

La Norme minimale de cybersécurité a été développée conjointement entre le gouvernement britannique et le centre national de cybersécurité (NCSC). Elle a été publiée en juin 2018 et est celle qui se rapproche le plus du CSF en droit britannique.

Cette norme définit les mesures de sécurité minimales à mettre en œuvre par les ministères du Royaume-Uni pour la protection de leurs informations, leur technologie et leurs services numériques, pour satisfaire aux exigences de SPF et de stratégie nationale de cybersécurité.

Cette norme reprend les cinq fonctions du CSF (Identification, Protection, Détection, Réponse et Reprise). Toutefois, même si certaines de ces fonctions et catégories ont été modifiées, de même que leur rédaction, elles sont, de façon générale, semblables à celles du CSF original.

Les fonctions proposées par le MCSS sont les suivantes :

1. **Identification :** Les ministères doivent mettre en place des processus appropriés de gouvernance en matière de cybersécurité.
2. Les ministères devront identifier et classer les informations sensibles dont ils disposent.
3. Les ministères devront identifier et classer les principaux services opérationnels qu'ils fournissent.
4. Le besoin des utilisateurs d'accéder à des informations sensibles ou à des services opérationnels clés, doit être compris et géré en permanence.

5. **Protection :** L'accès aux informations sensibles et aux services opérationnels clés ne sera permis qu'aux utilisateurs ou aux systèmes identifiés, authentifiés et autorisés.

6. Les systèmes traitant des informations sensibles ou des services opérationnels clés devront être protégés contre l'exploitation des vulnérabilités connues.

7. Les comptes hautement privilégiés ne doivent pas être vulnérables aux cyberattaques les plus courantes.

8. **Détection :** Les ministères devront prendre des mesures pour détecter les cyberattaques les plus courantes.

9. **Réponse :** Les ministères devront avoir une réponse définie, planifiée et éprouvée face aux incidents de cybersécurité visant des informations confidentielles ou des services opérationnels clés.

10. **Reprise :** Les ministères devront établir des processus bien définis et sûrs pour assurer la continuité des services opérationnels clés en cas d'incident ou problème.

Tout comme le CSF, le MCSS laisse à chacun la liberté de mettre en œuvre les directives de façon différentes. En effet, l'on comprend qu'il est presque impossible de définir une approche unique en matière de cybersécurité pour différentes industries, plateformes et situations. En revanche, les entreprises sont encouragées à interpréter la norme de manière indépendante et à adapter leurs propres processus de sécurité pour assurer la conformité.

4.2. Uruguay - Une approche guidée

Le Cadre de cybersécurité de l'Uruguay (MCU) [9] a pour objectif principal de créer de la confiance dans l'utilisation de la technologie, d'unifier toutes les ressources existantes en matière de cybersécurité et de soutenir l'évolution numérique du gouvernement. Ainsi, il cherche à promouvoir une vision intégrale et multisectorielle de la cybersécurité, en misant sur l'amélioration continue de la sécurité de l'information et en contribuant à la définition de plans d'action.

Sa mise en œuvre s'est fondée sur le Core CSF v1.0 (ISO/CEI 27001:2013, ISO 27799:201 [10], COBIT 5 et NIST 800-53 rev.4), ainsi que sur les travaux des spécialistes de la sécurité de l'information, des consultants internationaux et l'académie. Une fois le premier projet du MCU élaboré, il a été soumis à l'Université de la République qui, après analyse, a fourni ses recommandations. Il a ensuite été présenté à des consultants privées du pays et leurs commentaires ont également été recueillis. Finalement, la version 1.0 a été publiée en août 2016.

Aujourd'hui, ce cadre a déjà été utilisé pour le diagnostic et l'évaluation de tous les ministères du gouvernement central, des gouvernements départementaux, des institutions de santé et des institutions financières.

Adaptation du CSF au MCU

Si bien le MCU se fonde sur le Framework Core du NIST v1.0, il ne prend en compte qu'un ensemble de sous-catégories, laissant la mise en œuvre des sous-catégories manquantes à des étapes ultérieures.

Ce cadre présente une série **d'exigences** qui comprennent des bonnes pratiques sur la gouvernance en matière de sécurité, de gestion des risques, de contrôle d'accès, de sécurité des opérations, de gestion des incidents et de la continuité des opérations associées aux différentes sous-catégories du CSF du NIST. En outre, il comprend un **profil** organisationnel et un **modèle de maturité** grâce auxquels les organisations pourront définir des lignes d'action pour améliorer leur cybersécurité. Ces exigences ont été adaptées pour les agences de l'administration centrale de l'Uruguay et pour les établissements de santé. Aujourd'hui, des travaux sont en cours pour adapter ce cadre aux institutions financières.

Exigences propres

Le MCU propose un ensemble de 65 exigences issues des contrôles ISO/IEC 27001 et des normes uruguayennes en matière de cybersécurité.

Profil de l'organisation
Les organisations sont divisées en trois profils : basique, standard et avancé. L'assignation du profil est définie par la perception du risque technologique. Il est important de préciser que seul le profil avancé inclut la totalité des sous-catégories adoptées par le MCU.

Classement par ordre de priorité des sous-catégories
Étant entendu que les organisations ne sont pas toutes pareilles et que, selon leur profil, elles peuvent être amenées à donner la priorité à la mise en œuvre de certaines sous-catégories par rapport à d'autres, le MCU donne la priorité aux sous-catégories du CSF afin de faciliter l'approche et l'élaboration des plans d'action.

Modèle de maturité
Ce modèle permet aux organisations d'évaluer leur situation actuelle et d'établir, en fonction de leur ordre de priorité, l'objectif de maturité à atteindre dans chaque sous-catégorie présentée. De façon générale, les niveaux sont les suivants :

- **Niveau 0:** Les actions liées à la cybersécurité sont quasi inexistantes ou totalement inexistantes.

- **Niveau 1:** Il existe certaines initiatives en matière de cybersécurité. Approches ad hoc. Forte dépendance à l'égard du personnel. Attitude réactive face aux incidents de sécurité.

- **Niveau 2:** Il existe certaines directives quant à l'exécution des tâches. Il y a une dépendance à l'égard du personnel. Des progrès ont été réalisés dans l'élaboration de processus et de documentation des tâches.

- **Niveau 3 :** Il se caractérise par l'officialisation et la documentation des politiques et des procédures. Gouvernance en matière de cybersécurité. Indicateurs de suivi.

- **Niveau 4:** Le responsable de sécurité de l'information (RSI) joue un rôle clé dans le contrôle et l'amélioration du SGSI. Un contrôle interne est effectué. L'on travaille continuellement sur de potentielles améliorations. La cybersécurité est alignée sur les objectifs et les stratégies de l'organisation.

Tout organisme public ou privé pourra utiliser ce document en tant qu'outil pour la connaissance de soi et l'amélioration de ses niveaux de sécurité. Jusqu'à présent, l'adoption de tels cadres n'est pas obligatoire, bien qu'à court terme, on s'attende à ce qu'ils le soient pour certains secteurs critiques.

5. Conclusions

Les menaces cybernétiques continuent de croître et de poser problème à toutes les organisations, quel que soit leur secteur d'activité ou taille.

Bien que le CSF ait été initialement conçu comme un outil d'évaluation de la cybersécurité pour les infrastructures critiques des États-Unis, son approche, agnostique du point de vue des normes et exigences technologiques, a montré qu'il s'adapte parfaitement aux différents secteurs et pays et qu'il est facile à intégrer aux processus d'audit.

Le CSF peut être utilisé pour créer un nouveau programme de cybersécurité ou en tant qu'outil d'analyse et d'amélioration des lacunes des programmes de cybersécurité existants. Il est présenté de façon à permettre une approche intégrale de la gouvernance en matière de cybersécurité et peut facilement s'aligner sur les besoins de l'entreprise.

Les sous-catégories du CSF ont été mises en correspondance avec les contrôles des principales normes de l'industrie, ce qui permet de renforcer ces dernières. De plus, elles permettent une approche plus flexible et claire.

Finalement, le CSF doit être considéré comme un outil de gestion des risques en matière de cybersécurité qui permet d'évaluer l'efficacité des contrôles et leur rentabilité.

Les programmes de cybersécurité les plus efficaces sont ceux qui ne reposent pas sur une simple application de contrôles techniques, mais qui définissent une stratégie soit un cadre permettant d'aborder chacune des fonctions essentielles de la cybersécurité : identifier le contexte, protéger les systèmes et les biens, détecter les anomalies, fournir une réponse aux incidents, et reprendre les opérations commerciales. En bref, la cybersécurité est un problème qui ne peut être résolu qu'au travers d'une vision plus globale des personnes, des processus et de la technologie.

6. Références

[1] Casa Blanca (2013), *Orden ejecutiva 13636:* https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[2] NIST (2013), *NIST 800-53 Rev.4:* https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

[3] ISO (2013), *ISO/IEC 27001:* https://www.iso.org/standard/54534.html

[4] ISACA (2012), *COBIT 5:* http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

[5] CIS (2018), *Critical Security Controls (CSC):* https://www.cisecurity.org/controls/

[6] ISO (2018), *ISO/IEC TR 27103:* https://www.iso.org/standard/72437.html

[7] Gobierno de Reino Unido (2013), *Marco de Políticas de Seguridad de Reino Unido:* https://www.gov.uk/government/collections/government-security

[8] Gobierno de Reino Unido (2018), *Marco de ciberseguridad de Reino Unido:* https://www.gov.uk/government/publications/the-minimum-cyber-security-standard

[9] AGESIC (2018), *Marco de Ciberseguridad de Uruguay:* https://www.agesic.gub.uy/innovaportal/v/5823/1/agesic/marco-de-ciberseguridad-v40.html

[10] ISO (2016), *ISO 27799:* https://www.iso.org/standard/62777.html

[11] NIST (2018), *CSF v1.1 (en español):* https://www.nist.gov/sites/default/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

[12] OEA (2016), *Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?:* https://publications.iadb.org/es/publicacion/17071/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe

[13] NIST, *Adaptaciones internacionales del CSF:* https://www.nist.gov/cyberframework/international-resources

[14] OTAN (2012), *National Cyber Security Framework Manual:* https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

[15] ISC2 (2017), 2017 *Global Information Security Workforce Study - Benchmarking Workforce Capacity and Response to Cyber Risk (LATAM):* https://iamcybersafe.org/wp-content/uploads/2017/06/LATAM-GISWS-Report.pdf

[16] Deloitte (2016), *La Evolución de la Gestión de Ciber-Riesgos y Seguridad de la Información:* https://www2.deloitte.com/pe/es/pages/risk/articles/la-evolucion-de-la-gestion-de-ciber-riesgos-y-seguridad.html

[17] NIST (2018), RFC - *Cybersecurity Framework Draft Version 1.1:* https://www.nist.gov/cyberframework/rfc-cybersecurity-framework-draft-version-11

[18] Homeland Security, *Sectores de infraestructura crítica:* https://www.dhs.gov/cisa/critical-infrastructure-sectors

7. Sources

NIST, *Sitio web oficial del CSF*:
https://www.nist.gov/cyberframework/

NIST, *Historia y creación del CSF:*
https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework

NIST, *Estructura del CSF:*
https://www.nist.gov/cyberframework/online-learning/components-framework

NIST, *Funciones del CSF:*
https://www.nist.gov/cyberframework/online-learning/five-functions

NIST, *Evolución del CSF:*
https://www.nist.gov/cyberframework/evolution

AWS, *NIST Cybersecurity Framework – Aligning to the NIST CSF in the AWS Cloud*:
https://d1.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.246c0a886c7d16d2b370c20a04f99511d212613a.pdf

— CADRE DE CYBERSÉCURITÉ —

DU NIST

Une approche intégrale
de la cybersécurité

2019

White paper series
Édition 5

OEA Plus de droits pour plus de personnes | aws

CADRE DE CYBERSÉCURITÉ DU NIST

Une approche intégrale de la cybersécurité