

ROYAUME DU MAROC
ADMINISTRATION DE
LA DÉFENSE NATIONALE



LA STRATÉGIE NATIONALE DE CYBERSÉCURITÉ 2030

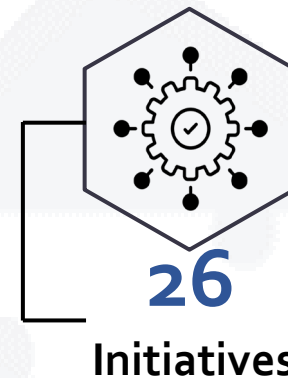
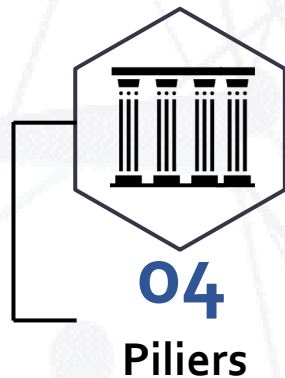


DIRECTION GÉNÉRALE DE LA SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Vision

Pour un cyberspace national fiable, sécurisé et résilient, à même de soutenir la transformation digitale du Royaume, de promouvoir la prospérité économique et d'assurer le bien-être des citoyens

Stratégie en chiffres



Pilier 1



Maintenir et renforcer le cadre juridique et normatif

- Procéder de manière périodique à la révision et au renforcement de l'arsenal juridique et normatif national régissant la cybersécurité
- Procéder à la déclinaison sectorielle du cadre juridique et normatif

Améliorer les mécanismes de coordination nationale

- Améliorer la coordination et le partage d'informations entre les intervenants en matière de protection des IIV
- Améliorer la coordination entre les organes en charge de l'application de la loi et les organes en charge du renseignement cyber
- Promouvoir et développer des mécanismes de coordination avec les acteurs privés



Pilier 2 : Sécurité et résilience du cyberspace national



Appuyer la prise de décision et soutenir les politiques fondées sur les données

- Disposer d'un état des lieux du paysage national de cybersécurité
- Mettre en place des mécanismes de recueil de données, de métriques et d'indicateurs sur les capacités nationales en matière de cybersécurité

Renforcer les capacités nationales de prévention, de gestion et de réaction aux incidents et crises cybernétiques

- Renforcer la préparation nationale et la réactivité pour faire face aux crises cybernétiques
- Développer des capacités sectorielles en matière de gestion des incidents cybernétiques

Promouvoir la mise en œuvre de standards et de normes de cybersécurité

- Renforcer l'offre existante par la mise en place de nouveaux schémas de qualification et de labellisation des produits, prestations ou prestataires de cybersécurité
- Mettre en place des schémas nationaux de certification en matière de cybersécurité pour les organismes publics et privés

Renforcer la protection des systèmes d'information des infrastructures vitales

- Tenir à jour une cartographie des IIV et de leurs SIS et clarifier les dépendances intersectorielles
- Renforcer les activités d'audit et de contrôle pour la vérification de la conformité des IIV
- Renforcer la résilience des opérateurs télécom et opérateurs de services numériques





Pilier 3 : Développement des capacités et sensibilisation



Pilier 3

Développer une culture de cybersécurité au sein de la société

- Sensibiliser les citoyens sur les menaces et les risques de sécurité inhérents au cyberspace
- Mettre en place des campagnes de sensibilisation au profit des secteurs public et privé
- Introduire des modules de sensibilisation à la cybersécurité au niveau scolaire

Renforcer les capacités des ressources humaines en matière de cybersécurité

- Mettre à niveau et augmenter les cursus de formation en cybersécurité dans les universités et les centres de formation professionnelle
- Encourager la certification professionnelle afin de constituer un vivier d'experts certifiés en cybersécurité
- Améliorer l'offre de la formation continue pluridisciplinaire au profit des gestionnaires de la cybersécurité
- Adapter l'offre de formations en cybersécurité aux besoins métiers

Soutenir le développement de l'écosystème national de cybersécurité et encourager l'innovation

- Encourager le développement de l'écosystème de cybersécurité à l'échelle nationale
- Soutenir la recherche et développement au sein des universités et des centres de formation



Pilier 4 : Coopération régionale et internationale

Pilier 4



Renforcer et promouvoir une participation active à l'échelle régionale et internationale sur les thématiques de la cybersécurité

- Participer activement aux différents forums et processus internationaux
- Soutenir et renforcer le positionnement du Royaume à l'échelle régionale et internationale dans le domaine de la cybersécurité

Développement de la coopération bilatérale

- Multiplier les actions de coopération bilatérale avec les différents pays dans les domaines du partage des informations et du développement des capacités