LE RENDEZ-VOUS
CÔTE D'IVOIRE 2030
GROUPE CONSULTATIF
POUR LE FINANCEMENT DU PND 2026-2030

MINISTÈRE DU PLAN
ET DU DÉVELOPPEMENT

GROUPE CONSULTATIF POUR LE FINANCEMENT DU PND 2026-2030

08 - 09 JUILLET 2026

FICHE D'OPPORTUNITÉ D'INVESTISSEMENT

TRANSITION NUMÉRIQUE

Cybersécurité et protection des systèmes d'information

02

DESCRIPTION DU SECTEUR

AMBITION DE LA CÔTE D'IVOIRE DANS LE SECTEUR/DOMAINE

La Côte d'Ivoire ambitionne de bâtir un écosystème numérique sécurisé, résilient, souverain et de confiance, en positionnant la cybersécurité et les services de confiance numérique comme des leviers stratégiques de transformation digitale, de croissance économique et de protection des citoyens.

IMPORTANCE DU SECTEUR/DOMAINE DANS L'ÉCONOMIE IVOIRIENNE

Le secteur de l'économie numérique et de la poste contribue à plus de 6% du PIB en 2025 avec 1318,4 milliards de chiffre d'affaires réalisé dont un investissement global dans le secteur de 304,7 milliards. (Cf. discours MTNIT FRATEL mai 2025 et ARTCI 2025)

Cette contribution est portée par une forte croissance des usages numériques perceptible par la généralisation de la téléphonie mobile (60,7 millions d'abonnements actifs mobile), de l'Internet mobile (35,5 millions d'abonnements actifs à l'internet mobile), des services financiers numériques (fintech, Mobile Money (27,9 millions d'abonnement au mobile money)), et de la dématérialisation des procédures administratives.

Cette augmentation des services numériques sensibles entraîne une exposition croissante aux risques cybernétiques.

Dans ce contexte, la cybersécurité constitue, un prérequis à la continuité des services publics numériques, un facteur clé de confiance des usagers, un élément déterminant de la souveraineté numérique nationale.

La montée des cybermenaces ciblant les infrastructures critiques, les services financiers numériques et les plateformes de e-gouvernement renforce la nécessité d'un cadre robuste de cybersécurité et de gestion des risques.

PERFORMANCES / PALMARÈS DE LA CÔTE D'IVOIRE DANS LE SECTEUR/DOMAINE AU NIVEAU ÉCONOMIQUE ET SOCIAL

ÉCONOMIQUE

- Secteur TIC : 6% du PIB en 2025
- 232 procédures administratives dématérialisées en 2025 (Cf. PADCI 2025)
- Processus de mise à disposition de service d'audit de sécurité, de certification et de supervision et de gestion des incidents déjà entamé par l'ANSSI.

SOCIAL

- Protection des données personnelles de millions d'usagers numériques (60,7 millions abonnements actifs mobiles, 27,9 millions abonnements actifs Mobile Money)
- Renforcement de la confiance des citoyens dans les services numériques publics
- Résilience accrue des services essentiels face aux cyberattaques

RAPPEL DE DOCUMENTS STRATÉGIQUES SECTORIELS

- Plan National de Développement (PND) 2026–2030
- Stratégie Nationale de Cybersécurité (SNC) 2021-2025
- Politique de Sécurité des Systèmes d'Information de l'administration publique (PSSI)
- Référentiel Général de Sécurité des Systèmes d'Information (RGSSI)
- Plan de Protection des Infrastructures Critiques (PPIC)
- Stratégie Nationale de Développement du Numérique (SNDN) 2021-2025
- Stratégie Nationale de la Gouvernance des Données SNGD 2030
- Stratégie Nationale de la Cybersécurité 2026-2030 (en cours d'élaboration)
- Stratégie Nationale de l'Intelligence Artificielle 2030

COMPARAISON DES STATISTIQUES AU NIVEAU MONDIAL, AFRICAIN OU RÉGIONAL

MONDIAL

Le marché de la cybersécurité connaît une croissance rapide, tirée par la sophistication des cyberattaques et l'augmentation des exigences réglementaires. La Côte d'Ivoire s'aligne sur les standards internationaux via la Convention de Budapest.

AFRICAIN

La Côte d'Ivoire figure parmi les pays africains pionniers en matière de cadre juridique cybersécurité, avec une loi sur la cybercriminalité et la ratification de la Convention de Malabo sur la cybersécurité et la protection des données.

RÉGIONAL

Dans la zone UEMOA, la Côte d'Ivoire se distingue par la modernisation de son arsenal législatif et la création de structures dédiées à la gouvernance de la sécurité numérique.

03 LE POTENTIEL DU SECTEUR

DEMANDE

La cybersécurité n'est plus seulement une contrainte technique (IT), mais un pilier stratégique de souveraineté et de croissance économique. Elle se transforme en un écosystème dynamique qui génère de la valeur, stimule l'innovation et devient une nouvelle frontière pour l'exportation de services.

A ce titre, elle génère une forte croissance des besoins en cybersécurité liée à la transformation digitale de l'État, à la digitalisation des entreprises et à l'essor des services financiers numériques.

Ces besoins portent sur :

- les centres de supervision (SOC nationaux et sectoriels),
- la gestion des incidents,
- la protection des données (gestion des identités numériques (IAM)),
- la continuité des activités (PCA/PRA),
- les solutions d'audit, de certification, de supervision et de continuité des services numériques,
- la nécessité de sécuriser les systèmes d'information de l'État, des collectivités et des opérateurs stratégiques,
- les demandes émergentes du secteur privé (banques, télécoms, PME) en solutions de cybersécurité externalisées.

AVANTAGES COMPARATIFS

- Cadre juridique modernisé et aligné sur les standards internationaux
- Première économie de l'UEMOA avec un écosystème numérique parmi les plus développés d'Afrique de l'Ouest
- Infrastructure numérique nationale (RNHD, data centers) offrant un socle pour les solutions de sécurité
- Engagement institutionnel fort avec la création du CNDigit et des référentiels de sécurité

CAPITAL HUMAIN

- Développement de formations spécialisées en cybersécurité dans les universités et instituts techniques
- Communauté croissante d'experts en sécurité informatique et en protection des données
- Programmes de certification internationale en cours de déploiement (ISO 27001, CISM, etc.)

DISPONIBILITÉ / ACCÈS AUX MATIÈRES PREMIÈRES

- Infrastructure numérique nationale existante (RNHD, câbles sous-marins) à sécuriser
- Proximité avec des fournisseurs régionaux et internationaux de solutions de cybersécurité
- Accès aux plateformes Cloud internationales certifiées pour l'hébergement sécurisé des données

NOMBRE D'EMPLOIS ATTENDUS

Le développement de l'écosystème cybersécurité en Côte d'Ivoire est estimé créateur de plusieurs milliers d'emplois qualifiés dans les domaines de l'audit, de la supervision, de l'ingénierie sécurité et de la protection des données, dans le cadre du PND 2026–2030.

04

LES ATOUTS

CADRE RÉGLEMENTAIRE / INSTITUTIONS PUBLIQUES

- Loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité
- Loi n°2023-593 du 7 juin 2023 modifiant les articles 17, 33, 58,60,62 et 66 de la Loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité
- Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel
- Loi n°2013-546 du 30 juillet 2013 relative aux transactions électroniques
- Loi n°2024-352 du 6 juin 2024 relative aux communications électroniques
- Décret n°2024-958 du 30 octobre 2024 portant création, attribution, organisation et fonctionnement de l'Agence Nationale de la Sécurité des Systèmes d'Information
- Décret n°2026-59 du 7 février 2026 portant modification des attributions de l'Agence Nationale de la Sécurité des Systèmes d'Information
- Décret n°2021-915 du 22 décembre 2021 portant adoption de la politique de sécurité des systèmes d'information de l'administration publique
- Décret n°2021-916 du 22 décembre 2021 portant adoption du Référentiel Général de Sécurité des Systèmes d'Information et du Plan de Protection des Infrastructures Technologiques
- Décret n°2021-917 : audit, contrôle et certification des systèmes d'information
- Ratification de la Convention de Malabo sur la cybersécurité et la protection des données 08/03/2023)
- Création du Comité National de Digitalisation dénommé CNDigit par Arrêté n°0910/pm/cab du 26 septembre 2022 portant création, attribution, organisation et fonctionnement du comité national de digitalisation

ÉLIGIBILITÉ AU CODE DES INVESTISSEMENTS

Les investissements dans la cybersécurité sont éligibles au Code des investissements ivoirien, permettant l'accès à des régimes préférentiels selon la nature, la taille et la localisation du projet.

INCITATIONS FISCALES À L'INVESTISSEMENT

- Exonération partielle ou totale de droits de douane sur les équipements de sécurité
- Exonération et/ou suspension de TVA sur certains services de cybersécurité
- Exonération d'impôt sur les sociétés sur une période de 5 à 15 ans selon le régime
- Crédits d'impôt à l'investissement et facilités administratives à l'implantation

DISPONIBILITÉ DE LA QUALITÉ DE MAIN D'ŒUVRE ET D'INFRASTRUCTURES DE SOUTIEN AU SECTEUR

- Main-d'œuvre qualifiée en informatique et sécurité des systèmes, en croissance
- VITIB : espace dédié aux entreprises technologiques avec services mutualisés
- Infrastructure numérique nationale (RNHD, data centers) constituant un socle opérationnel
- Réseau de câbles sous-marins garantissant la connectivité internationale sécurisée
- Abidjan, hub financier et technologique offrant un environnement de classe mondiale

LIEN AVEC LA PRÉSERVATION DE L'ENVIRONNEMENT (INVESTISSEMENT VERT)

- Développement de solutions de sécurité hébergées sur des data centers à faible empreinte carbone
- Promotion de la dématérialisation sécurisée des processus, réduisant la consommation de ressources physiques
- Cybersécurité des systèmes de gestion de l'énergie et des infrastructures environnementales critiques

INFORMATIONS GÉNÉRALES RELATIVES À L'ENVIRONNEMENT DES AFFAIRES

- CEPICI : guichet unique pour la création d'entreprise en 24 à 48 heures
- Cadre PPP structuré avec modalités BOT/BOOT, concessions et joint-ventures
- Délégation de services de cybersécurité à des opérateurs privés spécialisés

	• Stabilité macroéconomique favorable aux investissements technologiques de long terme • Appartenance à la CEDEAO et à l'UEMOA offrant un marché régional élargi
05 **LES OPPORTUNITÉS D'INVESTISSEMENTS**	• Solutions de sécurisation des systèmes d'information publics et privés • Création et exploitation de centres de supervision et de surveillance de la sécurité (SOC) • Services d'audit, de contrôle et de certification des systèmes d'information • Solutions de protection des données à caractère personnel • Sécurisation des infrastructures numériques critiques (énergie, finances, administration) • Solutions de continuité et de résilience des services numériques (PRA/PCA) • Plateformes de formation et de sensibilisation à la cybersécurité • Développement de compétences spécialisées et de services de conseil en sécurité informatique • Fourniture de solutions de cybersécurité pour les PME et startups numériques • Développement d'un écosystème national de certification et de labellisation en cybersécurité
06 **LES ACTEURS CLÉS DU SECTEUR**	SECTEUR PUBLIC • Ministère de la Transition Numérique et de l'Innovation Technologiques • Autorité de Régulation des Télécommunications/TIC (ARTCI) • Agence Nationale de Sécurité des Systèmes d'Informations (ANSSI) • Société Nationale de Développement Informatique (SNDI) • Agence Nationale du Service Universel des Télécommunications / Tic (ANSUT) • École Supérieure Africaine de TIC (ESATIC) • École Multinationale Supérieure des Postes (EMSP) • Village des technologies de l'information et de la Biotechnologie (ZBTIC / VITIB) • Fondation Jeunesse Numérique (FJN) • CNDigit – Comité National de Digitalisation • CEPICI – Centre de Promotion des Investissements en Côte d'Ivoire SECTEUR PRIVÉ • Entreprises spécialisées en cybersécurité (nationales et internationales) • Opérateurs de télécommunications et fournisseurs d'accès Internet • Éditeurs de logiciels de sécurité, sociétés d'audit et de conseil en SI • Startups de la cybersécurité et de la protection des données COMMUNAUTÉ • Union Internationale des Télécommunications (UIT) • Partenaires financiers : Banque Mondiale, AFD, BAD • Organisations régionales : CEDEAO, ARTAO • Universités, grandes écoles et centres de certification en sécurité informatique LE SECTEUR • VITIB – Village des Technologies de l'Information et de la Biotechnologie • Fondation Jeunesse Numérique (FJN) • Comité National de Pilotage des Partenariats Public-Privé • Incubateurs et accélérateurs spécialisés dans les technologies de sécurité
07 **LES RÉGIONS CONCERNÉES**	L'ensemble du territoire national est concerné, avec une priorité sur : • Abidjan : concentration des acteurs publics et privés, sièges des opérateurs stratégiques • Centres administratifs régionaux : Yamoussoukro, Bouaké, San-Pédro, Korhogo — sécurisation des systèmes déconcentrés

	• Zones d'extension du RNHD : sécurisation des nouvelles infrastructures numériques déployées
08 **QUELQUES LIENS UTILES**	• **Ministère de la Transition Numérique et de l'Innovation** Technologiques : www.telecom.gouv.ci • **ARTCI – Autorité de Régulation des Télécommunications/TIC :** www.artci.ci • **ANSSI- Agence Nationale de Sécurité des Systèmes d'Informations** : www.anssi.ci • **ANSUT- Agence Nationale du Service Universel des Télécommunications / Tic** – www.ansut.ci • **ESATIC- École Supérieure Africaine de TIC** – www.esatic.ci • **EMSP- École Multinationale Supérieure des Postes** – www.emsp.ci • **CEPICI – Centre de Promotion des Investissements :** www.cepici.gouv.ci • **Union Africaine – Convention de Malabo sur la cybersécurité** : www.au.int • **Union Internationale des Télécommunications – Cybersécurité** : www.itu.int • **VITIB – Village des TIC et Biotechnologie** : www.vitib.ci • **Plan National de Développement 2026–2030** : www.pnd.gouv.ci