MASTER GOUVERNANCE DE LA SÉCURITÉ DE L'INFORMATION ET CYBERSÉCURITÉ

PROGRAMME DE MASTER À DISTANCE *CHARLES LE MAISTRE* À L'EPA

1. CONTEXTE ET JUSTIFICATION

À l'ère du numérique, la transformation digitale des organisations s'accompagne de nouveaux défis liés à la protection des données, à la sécurité des systèmes d'information et à la gouvernance cyber. Les menaces informatiques, de plus en plus complexes et fréquentes, exposent les entreprises, les administrations et les institutions à des risques majeurs : atteintes à la confidentialité des données, sabotage des infrastructures critiques, escroqueries numériques, pertes financières, atteintes à l'image, et contentieux juridiques. La souveraineté numérique devient ainsi un enjeu stratégique. Face à ce contexte en constante évolution, le besoin de professionnels hautement qualifiés capables de concevoir, piloter et auditer des dispositifs de sécurité et de conformité en cybersécurité est devenu impératif. Les cadres décisionnaires doivent pouvoir compter sur des experts capables d'aligner les politiques de sécurité de l'information aux objectifs de gouvernance, de conformité réglementaire (RGPD, ISO/IEC 27001, 27002, 27701, 37301, etc.), et de performance organisationnelle. C'est dans cette dynamique que l'École Polytechnique d'Abidjan (EPA) propose un Master professionnel structuré et innovant en Gouvernance de la sécurité de l'information et cybersécurité, destiné à renforcer les capacités stratégiques et opérationnelles des acteurs publics et privés face aux menaces numériques. Le programme s'inscrit pleinement dans les priorités nationales et régionales en matière de cybersécurité, de digitalisation responsable et de gestion des risques technologiques.

2. OBJECTIFS DU PROGRAMME

Ce Master a pour objectif de former des cadres supérieurs et experts capables de concevoir, mettre en œuvre, auditer et améliorer des dispositifs de sécurité de l'information en cohérence avec les normes internationales et les cadres de gouvernance les plus exigeants.

À l'issue du programme, les diplômés seront en mesure de :

- maîtriser les concepts fondamentaux, les outils et les normes de la sécurité de l'information (ISO/IEC 27001, ISO 22301, NIST, COBIT, etc.) ;
- développer et piloter une politique de sécurité de l'information adaptée aux besoins stratégiques de l'organisation ;
- analyser les risques numériques et élaborer des plans de continuité et de réponse aux incidents ;
- conduire des audits internes et externes en sécurité de l'information selon les exigences de la norme ISO/IEC 19011 ;
- intégrer les principes de gouvernance IT, d'éthique numérique, et de conformité réglementaire dans les processus décisionnels ;
- encadrer des équipes pluridisciplinaires, piloter des projets de cybersécurité et accompagner le changement organisationnel.

La formation est fondée sur une pédagogie interactive et professionnalisante, avec des études de cas, des simulations, des stages en entreprise et un accompagnement individualisé, favorisant une insertion rapide dans les postes à responsabilité.

3. PUBLIC CONCERNÉ

Ce Master s'adresse à un public varié composé de professionnels en activité, de cadres en reconversion et de jeunes diplômés à fort potentiel, issus des domaines suivants :

- titulaires d'un diplôme de niveau Bac+4 ou équivalent (informatique, réseaux, télécommunications, droit du numérique, systèmes d'information, gestion des risques, audit, etc.) ;
- professionnels disposant d'un Bac+3 avec au moins trois (3) années d'expérience significative dans le secteur IT, la sécurité, l'audit ou la gestion des systèmes d'information ;
- responsables de la sécurité informatique, auditeurs SI, gestionnaires de risques, consultants, chefs de projet IT, juristes numériques, administrateurs réseau ou systèmes ;
- agents des ministères, collectivités territoriales, banques, assurances, télécoms et organisations internationales, souhaitant se spécialiser dans la gouvernance de la sécurité de l'information.

Le programme est particulièrement adapté aux personnes désireuses de renforcer leur employabilité, de viser des certifications internationales, ou d'accéder à des fonctions stratégiques à l'échelle locale, régionale ou internationale.

4. COMPÉTENCES VISÉES

Le Master en Gouvernance de la sécurité de l'information et cybersécurité est conçu pour développer un socle robuste de compétences techniques, managériales, méthodologiques et réglementaires, permettant aux diplômés de répondre efficacement aux exigences du marché de l'emploi numérique.

À l'issue de la formation, les diplômés seront capables de :

- concevoir et déployer une politique de sécurité de l'information conforme aux référentiels internationaux (ISO/IEC 27001, 27701, 22301, etc.) ;
- réaliser des analyses de risques numériques, mettre en œuvre des plans de sécurité et de continuité des activités (PCA/PRA) ;
- conduire des audits de conformité et d'efficacité des dispositifs de sécurité en s'appuyant sur la norme ISO/IEC 19011 ;
- intégrer la cybersécurité dans la gouvernance des systèmes d'information et des projets de transformation numérique ;
- interpréter les cadres législatifs et réglementaires applicables à la cybersécurité (lois locales, RGPD, directives de l'UEMOA/CEDEAO, etc.) ;
- développer des outils de veille technologique, de sensibilisation des utilisateurs et de gestion des incidents de sécurité ;
- mobiliser des équipes autour d'une culture proactive de cybersécurité, et accompagner la conduite du changement dans les organisations ;
- communiquer efficacement avec les parties prenantes internes et externes, tout en assurant la confidentialité, l'intégrité et la disponibilité des informations.

Ces compétences permettent aux diplômés de s'insérer dans les postes de responsables sécurité SI, auditeurs cybersécurité, délégués à la protection des données (DPO), RSSI, consultants ou encore chefs de projet IT Risk.

5. CONDITIONS D'ADMISSION

L'accès au Master est conditionné par la validation d'un parcours académique ou professionnel pertinent, selon les modalités suivantes :

Profil académique :

- Être titulaire d'un diplôme de niveau Bac+4 (ou équivalent) dans les domaines des technologies de l'information, de la sécurité, du droit du numérique, de la gestion des risques ou des sciences de l'ingénieur.

Profil professionnel :

- Être titulaire d'un diplôme de niveau Bac+3, complété par une expérience professionnelle d'au moins trois (3) années dans le domaine informatique, la sécurité des systèmes d'information, l'audit ou le conseil.

Dossier de candidature à fournir :

- Une lettre de motivation circonstanciée, exprimant clairement les objectifs professionnels du candidat ;
- Un CV actualisé ;
- Les copies certifiées des diplômes et relevés de notes ;
- Les attestations de travail ou de stage, le cas échéant ;
- Une copie de la pièce d'identité en cours de validité.

La sélection se fait sur étude de dossier et, si nécessaire, entretien de motivation ou test écrit. L'admission définitive est conditionnée par le paiement de la première tranche des frais de scolarité.

6. DURÉE ET LOCALISATION DE LA FORMATION

Le Master s'étend sur deux années universitaires, réparties en quatre semestres pour un total de 120 crédits ECTS, selon le système LMD reconnu par le CAMES.

Les cours sont assurés à distance via la plateforme de l'École Polytechnique d'Abidjan (EPA), équipé pour l'enseignement multimodal (en ligne et hybride).

Le programme est organisé de façon à favoriser la participation des professionnels en activité :

- Cours en soirées et/ou sessions intensives le week-end,
- Modules compacts adaptés aux rythmes professionnels,
- Plateforme numérique pour l'accès aux ressources, QCM, et interactions pédagogiques à distance.

La formation inclut également :

- Des enseignements théoriques et pratiques,
- Des études de cas contextualisées (secteur public, finance, énergie, télécoms),

- Des jeux de rôle et simulations de crise cyber,
- Un stage ou projet tutoré en cybersécurité,
- Et la rédaction d'un mémoire professionnel fondé sur une problématique réelle.

Ce dispositif permet une montée en compétences progressive, alignée sur les besoins stratégiques des entreprises et des institutions.

7. MÉTHODES PÉDAGOGIQUES

La pédagogie adoptée pour le Master professionnel en Gouvernance de la sécurité de l'information et cybersécurité repose sur une approche résolument professionnalisante, interactive et centrée sur les compétences. Elle vise à favoriser l'acquisition de savoirs actualisés, le développement de savoir-faire techniques, ainsi que la maîtrise de savoir-être essentiels à la gouvernance des systèmes numériques complexes.

Les modalités pédagogiques mobilisées sont les suivantes :

- Cours magistraux dynamiques, assurés par un corps professoral composé d'universitaires expérimentés et de professionnels certifiés (CISA, ISO/IEC Lead Auditor, CISSP, DPO, etc.) ;
- Études de cas réels, tirés d'organisations africaines et internationales, afin de contextualiser l'enseignement et d'ancrer les apprentissages dans des situations pratiques ;
- Classes inversées, qui favorisent l'autonomie des apprenants et renforcent leur capacité à mobiliser les ressources documentaires avant les séances de mise en pratique ;
- Simulations de crise, jeux de rôle et exercices de gestion d'incidents cyber, permettant aux étudiants de s'entraîner à la prise de décision rapide et à la coordination d'équipes sous contrainte ;
- Projets tutorés, encadrés par des professionnels, sur des problématiques concrètes en cybersécurité, gouvernance IT, audit ou conformité ;
- Plateforme numérique d'apprentissage, offrant un accès continu à des supports de cours, des outils de veille, des QCM, des forums d'échanges et des documents normatifs de référence (ISO/IEC, NIST, CNIL, etc.) ;
- Séminaires thématiques et conférences spécialisées, animés par des experts internationaux issus de cabinets de conseil, d'organismes de régulation, ou de directions cybersécurité d'entreprises multinationales.

Chaque module est structuré autour d'un syllabus détaillé, précisant les objectifs pédagogiques, les compétences visées, les contenus abordés, les méthodes d'évaluation et les prérequis éventuels.

8. PROGRAMME DU MASTER

Le programme du Master professionnel en Gouvernance de la sécurité de l'information et cybersécurité est structuré sur quatre semestres académiques, correspondant à deux années d'études, pour un total de 120 crédits ECTS, en conformité avec le système Licence-Master-Doctorat (LMD) reconnu par le CAMES.

La formation articule des unités d'enseignement théoriques, pratiques, transversales et professionnalisantes. Elle intègre les normes internationales (ISO/IEC 27001, ISO 27002, ISO 22301, ISO

19011, ISO 27701), les standards de gouvernance informatique (COBIT, ITIL, NIST) et les approches réglementaires en droit numérique et éthique cybernétique.

MASTER 1 – Semestre 1 (30 ECTS)

Unité d'Enseignement (UE)	Contenu des cours	Crédits ECTS	Unité d'Enseignement (UE)
UE 1 : Fondamentaux des systèmes d'information	Architecture et fonctionnement des systèmes d'information – Introduction aux bases de données relationnelles – Protocoles de réseaux – Notions de virtualisation	6	UE 1 : Fondamentaux des systèmes d'information
UE 2 : Introduction à la cybersécurité	Panorama des menaces informatiques actuelles – Principes de cryptographie symétrique et asymétrique – Typologies d'attaques – Détection et prévention	6	UE 2 : Introduction à la cybersécurité
UE 3 : Gouvernance des risques cyber	Introduction à la gestion des risques – Cartographie des actifs critiques – Élaboration de politiques SSI – PCA et PRA	6	UE 3 : Gouvernance des risques cyber
UE 4 : Cadres juridiques et conformité numérique	Analyse du RGPD et de ses équivalents en Afrique – Législation sur les données personnelles – Responsabilité juridique et audit de conformité	6	UE 4 : Cadres juridiques et conformité numérique

Unité d'Enseignement (UE)	Contenu des cours	Crédits ECTS	Unité d'Enseignement (UE)
UE 5 : Compétences transversales et culture scientifique	Communication écrite et orale – Anglais spécialisé cybersécurité – Vulgarisation et diffusion scientifique	6	UE 5 : Compétences transversales et culture scientifique
Unité d'Enseignement (UE)	Contenu des cours	Crédits ECTS	Unité d'Enseignement (UE)
UE 1 : Fondamentaux des systèmes d'information	Architecture et fonctionnement des systèmes d'information – Introduction aux bases de données relationnelles – Protocoles de réseaux – Notions de virtualisation	6	UE 1 : Fondamentaux des systèmes d'information

MASTER 1 – Semestre 2 (30 ECTS)

Unité d'Enseignement (UE)	Contenu des cours	Crédits ECTS	Unité d'Enseignement (UE)
UE 6 : Principes et méthodes d'audit SSI	Norme ISO 19011 appliquée à la sécurité – Rédaction de check-lists – Conduite d'audits internes et rapports d'audit	6	UE 6 : Principes et méthodes d'audit SSI
UE 7 : Sécurité des réseaux et systèmes	Firewalls, VLAN, VPN, IDS/IPS – Protocoles sécurisés – Supervision et logging	6	UE 7 : Sécurité des réseaux et systèmes
UE 8 : Protection des données à caractère personnel	Privacy by design – Fonction du DPO – Gestion des	6	UE 8 : Protection des données à caractère personnel

Unité d'Enseignement (UE)	Contenu des cours	Crédits ECTS	Unité d'Enseignement (UE)
	violations de données – ISO/IEC 27701		
UE 9 : Atelier de simulation cybernétique	Scénarios d'attaques réalistes – Réponse coordonnée – Gestion de crise – Communication en situation critique	6	UE 9 : Atelier de simulation cybernétique
UE 10 : Projet tutoré I	Évaluation des dispositifs SSI d'une organisation – Diagnostic critique et plan de recommandations – Soutenance interne	6	UE 10 : Projet tutoré I
Unité d'Enseignement (UE)	Contenu des cours	Crédits ECTS	Unité d'Enseignement (UE)
UE 6 : Principes et méthodes d'audit SSI	Norme ISO 19011 appliquée à la sécurité – Rédaction de check-lists – Conduite d'audits internes et rapports d'audit	6	UE 6 : Principes et méthodes d'audit SSI

MASTER 2 – Semestre 1 (30 ECTS)

Unité d'Enseignement (UE)	Contenu des cours	Crédits ECTS	Unité d'Enseignement (UE)
UE 11 : Intégration des systèmes de management	Déploiement intégré des normes ISO 27001, ISO 22301, ISO 37301 – Veille réglementaire – Audit de conformité multi-normes	6	UE 11 : Intégration des systèmes de management

Unité d'Enseignement (UE)	Contenu des cours	Crédits ECTS	Unité d'Enseignement (UE)
UE 12 : Enquête numérique et forensic	Investigation forensique – Saisie et chaîne de conservation des preuves – Rédaction de rapports d'expertise judiciaire	6	UE 12 : Enquête numérique et forensic
UE 13 : Leadership cyber et sensibilisation	Conduite du changement organisationnel – Formation des utilisateurs – Leadership et management en cyberéthique	6	UE 13 : Leadership cyber et sensibilisation
UE 14 : Méthodologie scientifique et publication	Construction d'un protocole de recherche – Rédaction d'articles scientifiques – Préparation à la publication	6	UE 14 : Méthodologie scientifique et publication
UE 15 : Projet tutoré II : Audit terrain	Audit complet d'un Système de Management de la Sécurité de l'Information – Rapport écrit et soutenance préparatoire	6	UE 15 : Projet tutoré II : Audit terrain
Unité d'Enseignement (UE)	Contenu des cours	Crédits ECTS	Unité d'Enseignement (UE)
UE 11 : Intégration des systèmes de management	Déploiement intégré des normes ISO 27001, ISO 22301, ISO 37301 – Veille réglementaire – Audit de conformité multi-normes	6	UE 11 : Intégration des systèmes de management

MASTER 2 – Semestre 2 (30 ECTS)

Unité d'Enseignement (UE)	Contenu des cours	Crédits ECTS
UE 16 : Recherche appliquée et innovation SSI	Enquête terrain – Traitement et interprétation des données – Analyse critique – Rédaction mémorielle	6
UE 17 : Stage professionnel de spécialisation	Immersion de 8 à 12 semaines en entreprise – Résolution d'un problème concret – Rapport validé par le maître de stage	12
UE 18 : Soutenance de fin de cycle	Défense publique du mémoire devant un jury scientifique et professionnel – Valorisation des apports du travail	12

9. COÛT DE LA FORMATION

L'École Polytechnique d'Abidjan propose un coût de formation accessible et compétitif, adapté à la réalité du marché local tout en garantissant un enseignement de qualité supérieure. Le montant annuel des droits de formation s'élève à : 1840€ (payable en plusieurs tranches selon un échéancier fixé par l'administration). Ce montant couvre :

- les frais pédagogiques,
- l'accès à la plateforme numérique,
- le suivi du mémoire,
- l'encadrement professionnel et académique,
- l'accès aux ressources numériques. Des facilités de paiement sont offertes pour permettre à chacun de suivre la formation sans compromettre ses obligations personnelles ou professionnelles.

Les frais annexes (transport, logement, restauration, impression du mémoire, etc.) restent à la charge de l'étudiant.

10. MODALITéS DE CANDIDATURE ET D'INSCRIPTION

L'admission à ce Master repose sur une sélection rigoureuse, fondée sur la motivation, le potentiel professionnel et la cohérence du projet du candidat avec les objectifs du programme.

Dossier de candidature à constituer :

- une lettre de motivation personnalisée, démontrant l'intérêt du candidat pour le domaine;
- un CV détaillé et actualisé ;
- les copies certifiées conformes des diplômes obtenus (au moins Bac+4 ou Bac+3 avec expérience professionnelle) ;
- les relevés de notes du dernier diplôme ;
- les attestations ou certificats justifiant des expériences professionnelles ou stages.

Procédure d'inscription :

1. Remplissage et soumission du formulaire de demande d'admission en ligne avant la date limite indiquée
2. Entretien éventuel de motivation ou test écrit (selon profil).
3. Notification d'admission et réception de la convention de formation.
4. Confirmation d'inscription par le paiement de la première tranche des frais de scolarité.
5. Carte d'étudiant et code d'accès à la plateforme numérique des cours

Les candidats sont invités à anticiper les démarches de financement (prise en charge par l'employeur, bourse institutionnelle, etc.).

11. CALENDRIER PRéVISIONNEL

Afin de garantir une organisation optimale et un démarrage dans les meilleures conditions, le calendrier suivant est mis en place :

- Lancement de l'appel à candidature : 23 Juin 2025
- Clôture des dépôts de dossier : 30 septembre 2025
- Publication des résultats d'admission : au fur et à mesure des validations de dossier
- Date limite de confirmation d'inscription (1ère tranche) : 3 semaines après réception de l'avis d'admission
- Rentrée académique : 20 octobre 2025

Les inscriptions seront closes dès que le nombre maximal de 30 places sera atteint. Les candidats sont donc encouragés à soumettre leur dossier le plus tôt possible.

12. CONTACTS ET FINALISATION

Pour toute information complémentaire, les candidats peuvent s'adresser à :

École Polytechnique d'Abidjan (EPA)

Service des admissions – Campus d'Abidjan

Téléphone : +225 0788322713 ou whatsapp +225 0768076777

Email : scolaritemaster@campus-epa.com

Site web : www.campus-epa.com

APPEL À CANDIDATURE

Master Gouvernance de la sécurité de l'information et cybersécurité

Programme de Master à distance Charles le Maistre à l'EPA

L'École Polytechnique d'Abidjan (EPA), établissement d'enseignement supérieur reconnu par l'État ivoirien, lance un appel à candidature pour l'admission au Master professionnel en Gouvernance de la sécurité de l'information et cybersécurité, une formation de haut niveau conforme aux standards du système LMD du CAMES.

Dans un contexte marqué par l'accroissement des cybermenaces, la multiplication des régulations sur la protection des données et l'importance stratégique des systèmes d'information, les organisations publiques et privées recherchent des experts capables de sécuriser, gouverner et auditer les environnements numériques complexes.

Ce Master, rigoureusement structuré sur deux années (Master 1 et Master 2), totalise 120 crédits ECTS et combine des enseignements théoriques, des études de cas réels, des mises en situation, des projets tutorés et un stage de spécialisation. Il prépare à des fonctions telles que :

- Responsable de la sécurité des systèmes d'information (RSSI)
- Auditeur en cybersécurité certifié
- Consultant en gouvernance IT
- Délégué à la protection des données (DPO)
- Chef de projet cyber-risque ou conformité réglementaire

Atouts du programme

- Formation conçue par des experts et praticiens certifiés (ISO/IEC, CISA, CISSP)

- Approche pédagogique hybride (cours du soir, week-end, e-learning) adaptée aux professionnels
- Ancrage dans les normes internationales : ISO 27001, 22301, 27701, 19011, RGPD, NIST, COBIT
- Simulations de crise cyber, audits réels, rédaction scientifique et mémoire appliqué
- Forte employabilité dans les secteurs public, privé, financier, énergétique et technologique

Public cible

- Titulaires d'un Bac+4 ou équivalent en informatique, réseaux, sécurité, droit du numérique, gestion des risques ou disciplines connexes ;
- Titulaires d'un Bac+3 justifiant d'au moins 3 années d'expérience professionnelle dans un domaine pertinent (sur validation des acquis professionnels) ;
- Cadres en reconversion, jeunes diplômés à fort potentiel, agents publics ou consultants.

Modalités de candidature

Le dossier de candidature comprend :

- Une lettre de motivation personnalisée, précisant les objectifs professionnels du candidat
- Un CV détaillé et actualisé
- Les copies certifiées des diplômes et relevés de notes
- Les attestations ou certificats de travail/stage (si applicables)
- Une copie de la pièce d'identité en cours de validité

Dates clés

- Ouverture des candidatures : 23 juin 2025
- Clôture des candidatures : 30 septembre 2025
- Publication des résultats : au fur et à mesure de la validation des dossiers
- Rentrée académique : 20 octobre 2025

Le nombre de places est strictement limité à 30 étudiants par cohorte. Les candidatures sont traitées selon l'ordre d'arrivée des dossiers complets.

Coût de la formation

Le montant annuel des droits de formation s'élève à :

1840€ (payable en plusieurs tranches selon un échéancier fixé par l'administration).

Postulez ICI

Cliquez ICI pour découvrir les autres filières