



apprendre
au cnam
change votre vie

le cnam

Certificat de compétence - CC14800A

Gestionnaire de la sécurité des biens informationnels et des infrastructures réseaux et systèmes

Publics/conditions d'accès

Bac+ 2 scientifique, technique ou informatique, ou expérience professionnelle significative dans les métiers de l'informatique.

Objectif

Répondre aux enjeux de l'analyse et de l'audit d'infrastructures complexes.

Compétences visées

Organiser la conformité (compliance) données (RGPD) et IT (LPM)

- Appliquer les principes fondamentaux du droit aux normes et lois à l'échelle nationale et européenne : lois, règlements, politiques et éthique en matière de cybersécurité et de protection de la vie privée ;
- Articuler les règles de droit et les mesures techniques de sécurité en lien avec les données et les infrastructures : principes fondamentaux du droit appliqués aux nouvelles législations RGPD et LPM ;
- Participer en tout ou partie à l'élaboration de la PSSI : principes de cybersécurité et de confidentialité ;
- Participer à l'organisation des flux de données, de leur classification et cartographie : principes de la vie privée ;
- Participer aux choix d'architectures techniques ou des traitements.

Mener une analyse de risque à l'aide des outils PIA, EBIIOS, MEHARI

- Mener une analyse de risque EBIIOS, PIA, MEHARI ;
- Participer à la mise en place d'un ISMS, assister au pilotage du projet de conception et déploiement dans l'entreprise ;
- Auditer un SI vis-à-vis des 12 bonnes pratiques.

Mettre en place les mesures de sécurité de base : les 12 bonnes pratiques de l'ANSSI

- Appliquer les principes de cybersécurité et de protection de la vie privée aux exigences organisationnelles (pertinentes pour la confidentialité, l'intégrité, la disponibilité, l'authentification, la non-répudiation) ;
- Décider ou participer aux décisions de déploiement des bonnes pratiques dans l'entreprise : mécanismes informatiques réseau et développement logiciel de base ;
- Rédiger des procédures pour la mise en place des bonnes pratiques ;
- Intervenir sur les infrastructures informatiques, systèmes et bases de données.

Contrôler la conformité du déploiement des bonnes pratiques et de leurs usages :

- Identifier des problèmes de sécurité du SI à l'échelle systémique par l'analyse de journaux et des sondes (vulnérabilité, configuration) ;
- Vérifier et valider avec les opérationnels la configuration des équipements ;
- Piloter par un tableau de bord la mise en place et le maintien des bonnes pratiques, les tester ;
- Maintenir la sécurité du SI conformément aux PSSI : objectifs de sécurité, bonnes pratiques, applications et mesures adaptées à déployer sur un SI pour une hygiène informatique de base ;
- Maintenir les conditions de sécurité opérationnelles des données et des IT.

Mettre en place les bases de l'investigation après incident criminalistique :

- Recueil de l'information sensible dans le cadre d'une enquête à forte exposition de risques ;
- Collecte des données : problématiques organisationnelles, méthode ;
- Établissement de la chaîne de preuves ;
- Chronologie et enquête criminelle.

Modalités d'évaluation

Deux sessions de contrôle sont associées aux unités d'enseignements de cours/ED.

Projet de fin d'études : lorsque l'auditeur a validé les UE du certificat, il prend rendez-vous avec le responsable du certificat pour définir d'un commun accord le sujet du projet.

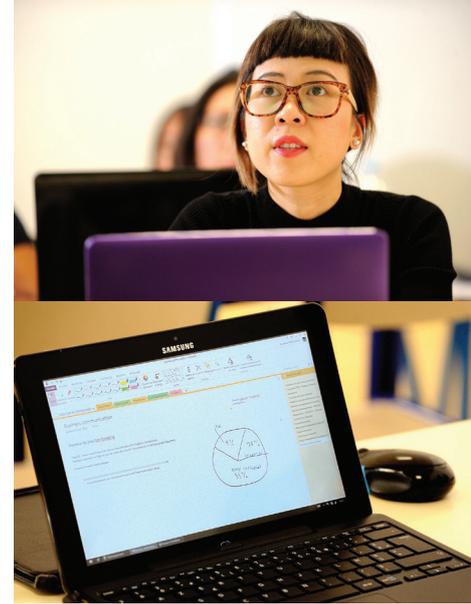
Rappel du règlement : valider les enseignements et le projet avec une moyenne générale supérieure ou égale à 10/20, sans note inférieure à 8, dans un délai maximum de 4 ans.

Tarifs

- 120 € pour une UE à 4 crédits
- 180 € pour une UE à 6 crédits

Responsable de la formation

Véronique Legrand



Programme du certificat		
Code UE	Intitulé de l'UE	Crédits
CRM211	Criminalistique	6
SEC103	Droit, enjeux de sécurité, conformité	6
SEC104	Analyse de risques des données, réseaux et systèmes	6
SEC105	Architectures et bonnes pratiques de la sécurité des réseaux, des systèmes, des données et des applications	6
SEC106	Analyses de sécurité : vulnérabilités et attaques	6
UASIIE	Projet final	6

Le Cnam
EPN Informatique
2, rue conté
75003 Paris
Bureau 31.1.79

deptinfo.cnam.fr

Contact

Agathe Froger,
gestionnaire pédagogique
01 40 27 20 38
agathe.froger@lecnam.net