DIPLÔME

Certificat de compétence Gestionnaire de la sécurité des données, des réseaux et des systèmes

Code : CC14800A

Niveau d'entrée : Aucun
Niveau de sortie : Aucun
ECTS : 36

Déployabilité
A la carte : Formation pouvant s'effectuer au rythme de l'élève, en s'inscrivant aux unités du cursus
Package : Formation pouvant se suivre en s'inscrivant à un "package" (groupe d'enseignements indissociables)

Objectifs pédagogiques

Répondre aux enjeux de l'analyse et de l'audit de sécurité des systèmes d'information

Compétences et débouchés

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

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

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

- Mener une analyse de risque EBIOS, PIA, MEHARI ,
- Participer à la mise en 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 en lien avec les 12 bonnes pratiques de la sécurité informatique

- 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 systemes informatiques, réseaux, 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, 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'enquête à forte exposition de risque
- collecte des données : problématiques organisationnelles, méthode
- établissement de la chaîne de preuves
- timeline et enquête criminelle

Méthodes pédagogiques

Les enseignements théoriques, couplés à des mises en application en travaux dirigés et travaux pratiques sur matériels et logiciels métiers permettront une professionnalisation rapide. L'espace numérique de formation du Cnam (Moodle) permet à chaque enseignant de rendre accessible des ressources spécifiques à ses enseignements. Des modalités plus détaillées seront communiquées au début de chaque cours.

Prérequis et conditions d'accès

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

Mentions officielles

Mots-clés

Cybercrime

Cybersécurité

Informations complémentaires

Type de diplôme

Certificat de compétence

Codes ROME

Administrateur / Administratrice sécurité informatique[M1801]
Responsable sécurité des systèmes d'information[M1802]
Analyste en cybersécurité[M1805]
Responsable sécurité informatique[M1802]

Formacode

Sécurité informatique [31006]

Code du parcours

CC14800A

Modules d'enseignement

- → Analyse de risques des données, réseaux et systèmes
- → Analyses de sécurité : vulnérabilités et attaques
- → Architecture d'Entreprise et Urbanisation des Systèmes d'Information
- → Conception et urbanisation de services réseau
- → Contrôle d’accès et Gestion des Identités Numériques
- → Criminalistique
- → Droit, enjeux de sécurité, conformité
- → Projet final
- → Systèmes d'exploitation : principes, programmation et virtualisation

Blocs de compétences

Un bloc de compétences est constitué d'un ensemble d'Unités qui répond aux besoins en formation de l'intitulé du bloc.
Les unités ci-dessus sont réparties dans les Blocs de compétences ci-dessous.
Chaque bloc de compétences peut être validé séparément.
Information non disponible, pour plus d'information veuillez contacter le Cnam