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

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

Présentation

Publics / conditions d'accès

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

Objectifs

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

Compétences

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

Mis à jour le 22-04-2024

Code : CC14800A

36 crédits

Certificat de compétence

Responsabilité nationale : EPN05 - Informatique / Véronique LEGRAND

Niveau CEC d'entrée requis : Sans niveau spécifique

Niveau CEC de sortie : Sans niveau spécifique

Mode d'accès à la certification :

- Validation des Acquis de l'Expérience
- Formation continue

NSF :

Métiers (ROME) : Administrateur / Administratrice sécurité informatique (M1801) , Responsable sécurité des systèmes d'information (M1802) , Analyste en cybersécurité (M1805) , Responsable sécurité informatique (M1802)

Contact national :

EPN05 - Informatique

2 rue Conté
75003 Paris

Sandra Bosse
sandra.bosse@lecnam.net

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

Enseignements

36 ECTS

Droit, enjeux de sécurité, conformité	SEC103 6 ECTS
Analyse de risques des données, réseaux et systèmes	SEC104 6 ECTS
Architectures et bonnes pratiques de la sécurité des réseaux, des systèmes, des données et des applications	SEC105 6 ECTS
Analyses de sécurité : vulnérabilités et attaques	SEC106 6 ECTS

Une UE à choisir parmi : 6 ECTS

Criminalistique	CRM211 6 ECTS
Architecture d'Entreprise et Urbanisation des Systèmes d'Information	NFE107 6 ECTS
Systèmes d'exploitation : principes, programmation et virtualisation	SMB101 6 ECTS
Conception et urbanisation de services réseau	RSX103 6 ECTS

Projet final	UASI1E 6 ECTS