MASTER 2 INFORMATIQUE / ORGANISATION ET PROTECTION DES SYSTEMES D'INFORMATION EN ENTREPRISE (OPSIE) FC

- MASTER 2 INFORMATIQUE / ORGANISATION ET PROTECTION DES SYSTEMES D'INFORMATION EN ENTREPRISE (OPSIE) FC

Le parcours OPSIE, labellisé SecNumÉdu par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), vise à renforcer les compétences des informaticiens généralistes (niveau ingénieur) en leur apportant

Compte Personnel de Formation (CPF)

Cette formation est éligible au Compte Personnel de Formation (CPF) : consultez les détails

Horaires et Session de formation

Horaires : M2 OPSIE Groupe 2 (Soir) : tous les soir 18h-21h et les samedis Matin
Session de formation :

- Réunion de rentrée : troisième semaine de septembre 18h-20h
- Début des cours : dernière semaine de septembre 18h-21h
- Cours de remise à niveau : une semaine en septembre
- Début Stage : début avril
- Fin de formation : 30 septembre

Présentation

Infos clés et site web

Lieu de la formation

- Campus Porte des Alpes (PDA)

Public

Niveau(x) de recrutement

- BAC+4

Public ciblé

Titulaires d'une première année de Master dans le domaine de l'informatique, de l'Informatique Appliquée à la Gestion, Mathématiques ou des Mathématiques Appliquées, ou toute autre formation scientifique (bac+4) comportant

Durée de la formation

379h

Discipline(s)

- Informatique IA Data Infographie Jeu Vidéo

Responsable(s) de la formation

Nouria HARBI et Mohamed-Lamine MESSAI

Contact secrétariat

Le parcours OPSIE, labellisé SecNumÉdu par l'ANSSI (Agence Nationale de la

L'objectif est de former des professionnels capables de sécuriser les solutions mises en place de manière :

1- Opérationnelle et technique :
Grâce aux enseignements spécialisés en sécurité informatique, couvrant notamment la sécurité des infrastructures, la protection des données, la cryptographie, la sécurité applicative, ainsi que l'audit informatique et la qualité des systèmes d'information (en s'appuyant sur les normes ISO 27001, ISO 22301, et ISO 9001).

2- Préventive et stratégique :
À travers des enseignements dédiés à l'analyse des risques, à l'élaboration de plans de reprise et de continuité d'activité (PRA /PCA), aux aspects juridiques de la cybersécurité, ainsi qu'à l'organisation et la modélisation des systèmes d'information pour une gouvernance efficace de la sécurité.

Spécificités

Formation 100% en Formation Continue.

Candidature

Modalités de candidature

Les candidatures sont à déposer sur la plateforme eCandidat selon le calendrier de candidature

- pour les étudiantes et étudiants non inscrits à l'Université Lumière Lyon 2
- pour les étudiantes et étudiants inscrits à l'Université Lumière Lyon 2
- pour les candidates et candidats de l'Union Européenne, de l'Espace Économique Européen ou de la Suisse (dossier de "Demande d'accès" via eCandidat)
- pour les étudiantes et étudiants non européens qui résident en France ou dans un pays non équipé de Campus France (dossier de "Demande d'accès" via eCandidat)

Pour les étudiantes et étudiants non européens qui résident dans un pays équipé de Campus France : la procédure CEF/Campus France est en ligne sur le site Campus France de votre pays.

Et après ?

Niveau de sortie

- Master

Activités visées / compétences attestées

- Acquérir une expertise approfondie dans les techniques de sécurisation des applications, des données (notamment à travers la cryptographie et

icom-master2-informatique@univ-lyon2.fr

Coût de la formation

Pour les stagiaires en formations continue (hors contrat de professionnalisation)

Les droits nationaux lors de votre inscription administrative en ligne
Les coûts pédagogiques (consulter nos tarifs & modalités)

Pour tout renseignement sur les modalités de prise en charge et sur les tarifs spécifiques, contactez le Service de la Formation Continue
Bâtiment GAIA 2ème étage – 86 rue Pasteur, 69007 LYON

les mécanismes de protection avancés), ainsi que des infrastructures réseau et systèmes.
- Être capable d'évaluer, analyser et gérer les risques liés à la cybersécurité en entreprise, en identifiant les vulnérabilités, en mettant en place des stratégies d'atténuation et en proposant des plans de reprise d'activité (PRA) et de continuité pour assurer la résilience des systèmes d' information.
- Maîtriser les méthodologies et outils d'audit informatique et d'audit de sécurité, incluant l'évaluation des conformités réglementaires, la détection des failles et l'amélioration continue des systèmes de protection.
- Concevoir et développer des systèmes d'information sécurisés, en intégrant les meilleures pratiques en matière d'architecture, de gestion des accès, de surveillance des menaces et de conformité aux normes et réglementations en vigueur.

Secteur(s) d'activités ou types d'emploi accessibles

- Gestion de la sécurité et pilotage des projets de sécurité
- Directeur Cybersécurité
- Responsable de la Sécurité des Systèmes d'Information (RSSI)
- Déclinaison pour le Responsable de sécurité des SI au sein d'une PME / TPE
- Coordinateur sécurité
- Directeur de programme de sécurité
- Responsable de projet de sécurité.
- Conception et maintien d'un SI sécurisé
- Chef sécurité de projet
- Architecte sécurité

- Responsable du CSIRT
- Analyste réponse aux incidents de sécurité
- Gestionnaire de crise de cybersécurité
- Analyste de la menace cybersécurité
- Spécialiste sécurité d'un domaine technique
- Spécialiste en développement sécurisé
- Cryptologue
- Administrateur de solutions de sécurité
- Auditeur de sécurité organisationnelle

- Auditeur de sécurité technique
- Gestion des incidents et des crises de sécurité
- Responsable du SOC
- Opérateur analyste SOC
- Conseil, services et recherche
- Consultant en cybersécurité
- Formateur en cybersécurité
- Évaluateur de la sécurité des technologies de l'information
- Développeur de solutions de sécurité
- Intégrateur de solutions de sécurité
- Chercheur en sécurité des systèmes d'information