Executive Certificate Cybersécurité :

Sécurisation avancée et gestion des cybermenaces moderne

Maîtrisez les outils et stratégies pour protéger les systèmes critiques et prévenir les cybermenaces

Code EC : DFTLV-EC-CYB-202505-FR

La cybersécurité vise à protéger les systèmes, réseaux et données sensibles contre les cyberattaques et les accès non autorisés. Les professionnels du domaine travaillent à identifier les vulnérabilités, à prévenir les menaces et à répondre aux incidents pour garantir la résilience des infrastructures critiques.
L'Executive Certificate Cybersécurité : Sécurisation avancée et gestion des cybermenaces modernes permet aux participants de maîtriser les outils et stratégies nécessaires pour sécuriser des environnements complexes, tout en développant des compétences techniques et stratégiques adaptées aux besoins des entreprises modernes.

15 jours - 105 heures - Présentiel

Prix : 7995 €*
Prix pour les particuliers : **5590 €***
* Inclus petit déjeuner et déjeuner 25 € par jour

Adresse : IUT de Cachan 9 Avenue de la Division Leclerc 94230 Cachan

Sessions 1 :
Novembre-Décembre 2025
Sessions 2 :
Février 2026
Sessions 3 :
Avril 2026

Objectifs :

• Comprendre les concepts fondamentaux et avancés de la cybersécurité et leur application dans des environnements Blockchain, IoT et Cloud
• Maîtriser les outils et stratégies pour protéger les systèmes connectés, sécuriser les données sensibles et prévenir les cybermenaces
• Développer des compétences pour anticiper les risques, gérer les crises cyber et garantir la conformité aux normes de sécurité

Public concerné

- Professionnels de l'informatique, ingénieurs systèmes et réseaux, responsables IT
- Consultants en transformation numérique et experts en cybersécurité souhaitant approfondir leurs compétences

Prérequis

- Connaissances générales en systèmes d'information, informatique et cybersécurité
- Bases en programmation et compréhension des enjeux numériques

Compétences acquises

Maîtrise des méthodologies et outils pour analyser, sécuriser et gérer les environnements numériques critiques face aux cybermenaces modernes

L'Executive Certificate Cybersécurité : Sécurisation avancée et gestion des cybermenaces modernes

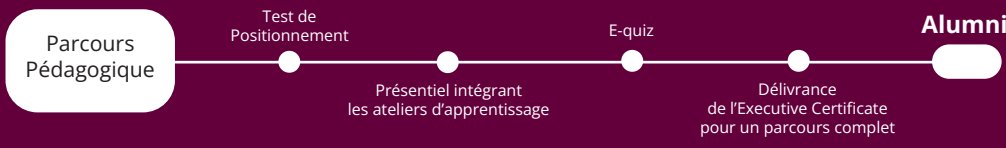
est une formation intensive de 15 jours, avec 7 heures de cours chaque jour, divisée en 4 blocs spécialisés.

- Bloc 1 : Cybersécurité : connaissances et anticipation
- Bloc 2 : Cybersécurité Cloud : Sécurisation des infrastructures
- Bloc 3 : Cybersécurité et Blockchain : Approfondissement
- Bloc 4 : Cybersécurité IoT : Protection des systèmes connectés

Plusieurs options d'inscription sont disponibles :

- En suivant l'ensemble des blocs, vous pouvez obtenir l'Executive Certificate de l'Université Paris-Saclay.
- En suivant un seul bloc spécifique, vous recevrez une attestation de participation pour le bloc suivi.
- Pour deux blocs choisis vous bénéficiez d'une réduction de 10% sur l'ensemble de la commande.

Vous trouverez ci-dessous les fiches descriptives détaillant le contenu de chaque bloc ainsi que la biographie de nos experts qui animent cette formation.



Bloc 4 : Cybersécurité IoT : Protection des systèmes connectés
SESSION 1 – 2025 : 1-3 décembre
SESSION 2 – 2026 : 23-25 février
SESSION 3 – 2026 : 27-29 avril

Bloc 1 : Cybersécurité : Connaissances et anticipation
SESSION 1 – 2026 : 13-14-15 mai
SESSION 2 – 2026 : 9-10-11 juillet

Bloc 3 : Cybersécurité et Blockchain : Approfondissement
SESSION 1 – 2025 : 24-27 novembre
SESSION 2 – 2026 : 16-19 février
SESSION 3 – 2026 : 20-24 avril

Bloc 2 : Cybersécurité Cloud : Sécurisation des infrastructure
SESSION 1 – 2025 : 24-27 novembre
SESSION 2 – 2026 : 16-19 février
SESSION 3 – 2026 : 20-24 avril

Cybersécurité : connaissances et anticipation

3 jours | 2175 € repas inclus | Initiation

Bloc 1

Réf.DFTLV-EC-CYB-20 2505-FR-MOD1CCA

Développez des compétences fondamentales pour diagnostiquer, sécuriser et gérer les crises cyber grâce à des outils et cas pratiques adaptés aux menaces modernes

2 SESSIONS AU CHOIX

SESSION 1 – 2026
13-14-15 mai

SESSION 2 – 2026
9-10-11 juillet

Objectifs :

• Apprendre les techniques nécessaires pour l'implémentation d'outils matériels et logiciels de diagnostic, d'audit et de sécurisation des réseaux locaux.

• Implémenter les solutions techniques et efficaces jusqu'à la mise en situation et la gestion de crise en cas d'attaques cyber.

Public concerné

Tout public

Compétences acquises

Maîtrise des bases de l'IoT, de la configuration des réseaux et des protocoles de communication filaire et sans fil

Prérequis

Connaissances minimales en architecture de réseaux locaux, commandes de bases pour l'administration réseaux, notions de bases en programmation (Python) et scripting

Intervenants

Mehdi AMMAR
Enseignant-Chercheur à l'Université Paris-Saclay, et responsable pédagogique de la Licence Professionnelle Métiers des Réseaux et des Télécommunications (LP MRT).

Bertrand HOUMEAU
Chef du Bureau de la Conduite et de la Réalisation Informatique (BCRI)
Centre de la donnée et des applications numériques, ministère des armées

Programme :

Introduction à la cybersécurité

• Présentation des concepts fondamentaux de la cybersécurité et de leur importance face aux menaces numériques actuelles.

Exercice d'application : analyse d'un scénario de cyberattaque basique pour identifier les principales vulnérabilités exploitées

Diagnostic et audit des réseaux locaux

• Apprentissage des outils et techniques d'évaluation de la sécurité des réseaux locaux, identification des failles potentielles.

Atelier pratique : utilisation d'outils tels que Nmap ou Wireshark pour auditer un réseau simulé et détecter les failles de sécurité.

Étude de cas : analyse d'un audit de sécurité réalisé dans une PME pour identifier les vulnérabilités et proposer des solutions.

Implémentation des mesures de sécurisation

• Mise en place de solutions matérielles et logicielles pour protéger les infrastructures critiques.

Étude de cas : évaluation des mesures de sécurité d'un réseau hospitalier et recommandations pour renforcer la résilience face aux cybermenaces

Gestion des incidents et réponse aux cyberattaques

• Développement de stratégies pour anticiper les risques et assurer la continuité des opérations après une attaque.

Atelier pratique : simulation d'un incident de sécurité (type ransomware) et mise en place d'un plan de réponse pour minimiser les impacts.

Conformité aux normes de sécurité

• Exploration des principales réglementations en cybersécurité et des démarches pour garantir la conformité organisationnelle.

Exercice d'application : rédaction d'un plan de conformité aligné sur une norme spécifique (par exemple, RGPD ou ISO 27001).

Étude de cas : mise en conformité d'une entreprise face aux exigences du RGPD et analyse des défis rencontrés.

Challenge de clôture :

• Un E-Quiz pour valider les acquis

Cybersécurité Cloud : Sécurisation des infrastructures

5 jours | 3375 € repas inclus | Perfectionnement

Bloc 2

Réf. DFTLV-EC-ACIT-202503-FR-MOD3SSII
EC-CYBMOD2

Protégez vos systèmes industriels avec des stratégies de sécurité avancées tout en maîtrisant les réglementations et normes de cybersécurité pour garantir la conformité de votre organisation

3 SESSIONS AU CHOIX

SESSION 1 – 2025
17-21 novembre

SESSION 2 – 2026
9-13 février

SESSION 3 – 2026
13-17 avril

Objectifs :

- Comprendre les concepts de base de la sécurité des systèmes d'information
- Identifier et analyser les risques spécifiques aux environnements informatiques industriels
- Mettre en œuvre des stratégies de gestion des risques pour sécuriser les systèmes d'information
- Anticiper les menaces émergentes et développer des plans de réponse adaptés aux environnements industriels
- Évaluer l'efficacité des mesures de sécurité mises en place et les ajuster en fonction des évolutions technologiques et des nouvelles menaces
- Comprendre les risques cyber dans le contexte actuel
- Identifier les réglementations et normes cyber et leur déclinaison opérationnelle
- Appliquer les méthodologies d'audit cyber et les mettre en œuvre

Public concerné

Professionnels de l'informatique, ingénieurs système, responsables IT, consultants en transformation numérique

Compétences acquises

Gérer les risques de sécurité dans les systèmes d'information industriels, et proposer des mesures correctives pour renforcer la sécurité
Maîtriser les réglementations et normes de cybersécurité et mettre en conformité une organisation industrielle, tout en gérant efficacement les risques et les crises cyber

Prérequis

Connaissances générales en gestion des risques ou en audit

Intervenants

Nadim Henoud
Ingénieur logiciel
et cybersécurité POTECH
Yacine Ladjici
Responsable de la cybersécurité
du groupe VALEO POWER

Programme :

Introduction à la sécurité des systèmes d'information

- Comprendre les principes fondamentaux de la sécurité des systèmes d'information industriels, tout en analysant les menaces émergentes telles que la cybercriminalité, les ransomwares, et les attaques sur les infrastructures critiques
Étude de cas : analyse d'un exemple concret d'infrastructure industrielle pour étudier les modèles de sécurité (confidentialité, intégrité, disponibilité) appliqués. Identification des failles courantes et évaluation des risques associés

Identification et analyse des risques

- Apprendre à identifier, évaluer et analyser les risques spécifiques aux environnements informatiques industriels tout en adoptant une approche proactive. Cette démarche permet d'anticiper et de détecter les failles potentielles avant qu'elles ne soient exploitées, en s'appuyant sur des méthodologies reconnues comme EBIOS et ISO 27005
Mise en situation : évaluation d'un système industriel réel, identification des vulnérabilités potentielles et mise en oeuvre d'une méthodologie pour analyser les risques. Proposition de mesures préventives pour limiter l'impact de ces failles

Mise en oeuvre de stratégies de gestion des risques

- Mettre en place des politiques et procédures efficaces pour atténuer les risques et sécuriser les systèmes d'information, tout en assurant une amélioration continue de la sécurité grâce à des audits réguliers et à l'actualisation des procédures face aux nouvelles menaces et évolutions technologiques, afin de garantir la résilience à long terme des infrastructures industrielles
Étude de cas : analyse d'exemples réels d'entreprises ayant implémenté des stratégies de gestion des risques, évaluation des approches utilisées, identification des améliorations possibles et élaboration d'un plan pour assurer une gestion continue des risques

Utilisation d'outils et de techniques de protection

- Se familiariser avec les outils de sécurité tels que les firewalls, systèmes de détection d'intrusion et cryptage, ainsi que leur déploiement efficace dans les environnements industriels, tout en adoptant les bonnes pratiques de configuration et de mise à jour pour éviter les erreurs humaines et maximiser la résilience des systèmes
Exercide d'application : configuration et déploiement de divers outils de sécurité dans un environnement simulé, puis application des mises à jour et des configurations de sécurité en suivant les meilleures pratiques pour assurer une protection optimale contre les menaces

Évaluation des vulnérabilités et propositions de mesures correctives

- Évaluer la sécurité des systèmes en analysant les résultats des tests de pénétration et des scans de vulnérabilités, recommander des mesures correctives pour renforcer la sécurité, établir des priorités d'intervention, développer un plan d'action correctif, et assurer l'efficacité à long terme des mesures à travers des audits post-implémentation
Études de cas : analyse de cas concrets pour comprendre les vulnérabilités et discuter des mesures correctives appropriées en comparant les différentes approches

Bloc 2

Introduction aux risques cyber dans l'industrie

• Introduction aux principaux risques de cybersécurité affectant les environnements industriels, avec une analyse approfondie des menaces actuelles, des vulnérabilités spécifiques et des tendances émergentes
Étude de cas : exemple réel d'entreprise industrielle ayant subi une cyberattaque, en analysant les menaces spécifiques, les impacts sur les systèmes industriels, les actions mises en place par l'entreprise pour limiter les dégâts et rétablir les systèmes, et les mesures adoptées pour renforcer la sécurité post-attaque

Normes et réglementations de cybersécurité

• Exploration des principales normes et réglementations de cybersécurité (NIS2, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, etc.), avec un focus sur leur application dans différents contextes industriels, ainsi que comparaison des réglementations européennes et internationales en matière de cybersécurité
Étude de cas : analyse d'entreprises ayant implémenté des normes spécifiques à travers l'identification des failles éventuelles et des ajustements ou des améliorations proposés pour optimiser l'implémentation des normes

Analyse de risques et gestion de crise cyber

• Approfondissement des méthodologies d'analyse des risques (EBios RM, ISO 19011) et des stratégies de gestion de crise cyber, y compris la gestion des incidents et la mise en place de plans de réponse aux cyberattaques
Mise en situation : gestion en direct d'une cyberattaque, pour coordonner une réponse, gérer les communications de crise et limiter les impacts sur les opérations

Audits cyber et tests de vulnérabilité

• Apprentissage des techniques d'audit cyber, englobant les aspects organisationnels et techniques, ainsi que des méthodes avancées pour évaluer la sécurité des systèmes. En parallèle, étude des tests de pénétration et des techniques de détection de vulnérabilités, telles que les scans de sécurité et le pentesting
Exercice d'application : réalisation d'un audit complet sur une organisation, incluant l'évaluation des aspects organisationnels et techniques

Challenge de clôture :

• Un E-Quiz pour valider les acquis

Cybersécurité et Blockchain : Approfondissement

4 jours | 3100 € repas inclus | Expertise

Bloc 3

Réf.DFTLV-ECBC-202402-FR-MOD2CB-EC-CYBMOD3

Maîtrisez la cryptographie blockchain et relevez les défis de la sécurité des systèmes distribués

3 SESSIONS AU CHOIX

SESSION 1 – 2025
24-27 novembre

SESSION 2 – 2026
16-19 février

SESSION 3 – 2026
20-24 avril

Objectifs :

• Cerner comment la cryptographie sécurise les transactions
• Maîtriser les principes de base de la cryptographie pour sécuriser les blockchains
• Explorer les avancées récentes en cryptographie appliquée aux blockchains, comme les protocoles zero-knowledge
• Explorer les applications concrètes de la blockchain dans différents domaines et comprendre comment elle est utilisée dans la vie réelle
• Acquérir une vue d'ensemble de la cybersécurité, des techniques criminelles utilisant la blockchain et les régulations en place pour sécuriser cette technologie

Prérequis
Connaissances de base sur le fonctionnement des blockchains

Public concerné
Tout public ayant une bonne maîtrise d'un langage de programmation

Compétences acquises
- Maîtriser les techniques cryptographiques utilisées pour sécuriser les blockchains
- Analyser les applications concrètes de la blockchain et aborder les défis de la cybersécurité dans divers contextes

Intervenants
Tarek Kamoun
CEO et fondateur de la société de conseil et développement Blockchain K2LIS

Programme :

Algorithmes de chiffrement et fonctions de hachage

• Comprendre DES, RSA, Diffie-Hellman, courbes elliptiques, et SHA256
Exercice d'application : appliquer les algorithmes à des scénarios pratiques pour renforcer la compréhension.

Signatures numériques et algorithmes de partage de secret

• Expliquer DSA, schéma de Shamir, et arbres de Merkle
Étude de cas : analyser les concepts à travers des exemples concrets pour illustrer leur utilisation et leurs implications.

Cryptographie avancée dans les blockchains

• Analyser les preuves à divulgation nulle (ZK) et leur application dans Bitcoin, Ethereum, Monero, et Zcash.
Mise en situation : simuler des transactions et utiliser ZK pour comprendre leur impact sur la sécurité et la confidentialité des données.

Applications de la blockchain

• Aperçu de l'écosystème blockchain
• Applications dans divers secteurs pour améliorer la transparence et la traçabilité
Étude de cas : utilisation de la blockchain dans des applications réelles comme Ripple & SWIFT, IBM Food Trust, MediLedger, etc.

Cybersécurité dans la blockchain

• Exploration des risques liés à l'utilisation criminelle de la blockchain, tels que le blanchiment d'argent et le ransomware
• Étude des escroqueries et hacks notables comme Mt. Gox, Bitfinex, FTX
Étude de cas et analyse : analyser des incidents notoires comme Mt. Gox, Bitfinex, FTX pour comprendre les défis de sécurité spécifiques et les leçons tirées

Challenge de clôture :

• Un E-Quiz pour valider les acquis

Intelligence artificielle et sécurité dans l'IoT

3 jours | 2675 € repas inclus | Expertise

Maîtrisez les techniques d'intégration de l'IA et les stratégies de sécurité dans les systèmes IoT

Bloc 4

Réf. DFTLV-EC-IOT-2025-FR-MOD3IAS-EC-CYBMOD4

3 SESSIONS AU CHOIX

SESSION 1 – 2025
1-3 décembre

SESSION 2 – 2026
23-25 février

SESSION 3 – 2026
27-29 avril

Objectifs :

- Maîtriser l'intégration de l'IA dans les systèmes IoT, en permettant des décisions basées sur les données à travers des algorithmes d'apprentissage automatique
- Concevoir des architectures IoT intelligentes avec des capacités d'IA, au niveau du Edge, du Fog et du Cloud, pour optimiser la réactivité et l'analyse en temps réel
- Comprendre les exigences de sécurité et les défis spécifiques aux environnements IoT, notamment liés à la gestion des accès, à l'authentification et à la protection des données
- Mettre en œuvre des mécanismes de sécurité tels que le contrôle d'accès, la gestion des identités, et les techniques cryptographiques pour protéger les réseaux IoT et prévenir les attaques courantes
- Élaborer des stratégies de protection des données dans les environnements IoT, en intégrant des solutions d'authentification multifactorielle et des techniques de sécurisation des données stockées dans le Cloud

Public concerné

Professionnels de l'informatique, data scientists, ingénieurs systèmes, responsables IT, consultants en transformation numérique

Compétences acquises

Maîtrise de l'IA et des architectures IoT sécurisées (Edge, Fog, Cloud), avec application des techniques de sécurité, d'authentification, et de cryptographie pour protéger les données, y compris celles stockées dans le Cloud

Prérequis

Connaissances de base en IoT et en intelligence artificielle

Intervenants

Gilbert Habib
Professeur en réseau sans fil et système discret contrôlé

Programme :

Introduction à l'IA dans l'IoT

- Présentation des concepts de base sur la synergie entre l'Intelligence Artificielle et l'Internet des Objets.
- Identification des avantages de l'intégration de l'IA dans les systèmes IoT pour permettre une gestion intelligente des données

Exercice d'application : identification d'exemples d'applications où l'IA améliore les performances des systèmes IoT, et exploration de leurs architectures

Algorithmes d'apprentissage automatique pour IoT

- Apprentissage des algorithmes de machine learning spécifiques aux systèmes IoT, avec une attention particulière aux techniques de classification, régression, et détection d'anomalies

Atelier pratique : mise en œuvre d'un modèle de machine learning pour prédire l'état des capteurs dans un système IoT et automatiser des décisions en fonction des résultats

Conception d'architectures IoT avec l'IA

- Conception d'architectures IoT avec des capacités d'IA intégrées au niveau du Edge, du Fog et du Cloud.
- Comparaison des avantages et des défis de ces trois niveaux d'architecture

Étude de cas : conception d'un réseau IoT intelligent pour un système de surveillance industrielle, avec intégration de l'IA à différents niveaux pour optimiser les performances et les prises de décisions en temps réel

Analyse des données IoT avec l'IA

- Introduction aux techniques d'analyse des données IoT en utilisant des méthodes d'intelligence artificielle, comme les réseaux de neurones ou les modèles prédictifs, pour obtenir des insights exploitables

Exercice pratique : mise en place d'une chaîne d'analyse en temps réel à partir de données IoT, avec détection des anomalies et recommandations automatiques

Applications industrielles de l'IA et IoT

- Exploration des différentes applications industrielles où l'IA et l'IoT sont combinées, comme les systèmes de maintenance prédictive, les réseaux énergétiques intelligents et la logistique automatisée

Étude de cas : analyse d'une application IoT dans l'industrie automobile pour prédire les pannes de véhicules à partir de données captées en temps réel et optimiser les cycles de maintenance

Exigences et défis de sécurité IoT

- Analyse des exigences de sécurité spécifiques aux systèmes IoT, avec une attention particulière sur la gestion des accès, l'authentification, et la gestion des données

Exercice d'application : identification des vulnérabilités dans un système IoT et proposition de solutions pour les atténuer

Techniques de sécurisation et gestion des risques

- Exploration des techniques cryptographiques et des solutions de contrôle d'accès pour sécuriser les communications et les données IoT

Atelier pratique : implémentation de mécanismes de chiffrement et d'authentification dans un réseau IoT pour garantir la sécurité des données

Sécurisation des données IoT dans le Cloud

- Présentation des stratégies de sécurité pour protéger les données IoT stockées et traitées dans des environnements cloud, avec un focus sur l'authentification multifactorielle

Étude de cas : mise en place de protocoles de sécurité pour garantir l'intégrité et la confidentialité des données IoT stockées dans le Cloud

Challenge de clôture :

- Un E-Quiz pour valider les acquis

Vos intervenants

Mehdi Ammar

Mehdi Ammar est enseignant - chercheur à l'Université Paris-Saclay au laboratoire C2N depuis 2009. Il enseigne dans la licence pro Métiers des Réseaux et Télécoms (MRT) depuis 2010 sur les thèmes des nouvelles technologies réseaux pour le très haut débit et la sécurité des infrastructures réseaux. Il est aussi le responsable pédagogique de la Lic. pro. MRT depuis 2011

Bertrand Houmeau

Bertrand Houmeau est Chef du Bureau de la Conduite et de la Réalisation Informatique (BCRI) au Centre de la Donnée et des Applications Numériques du Fort de Montrouge, au sein du ministère des Armées

Tarek Kamoun

Tarek KAMOUN est CEO et fondateur de la société de conseil et développement Blockchain K2LIS. Ingénieur informatique de formation, c'est durant ses 10 années d'expérience dans le conseil en architecture des systèmes d'information et en transformation digitale qu'il a croisé la route de cette technologie disruptive. Depuis plus de 7 ans il accompagne de bout en bouts des startups, PME et grands groupes, à comprendre, innover et créer de la valeur grâce aux technologies Blockchain : de la notarisation d'information à la finance décentralisée (DeFi)

Gilbert Habib

Gilbert Habib est docteur en réseaux sans fil et PDG de HEAD, une société spécialisée dans l'automatisation industrielle et la domotique. Il possède plus de 10 ans d'expérience en enseignement et est un expert en IoT, avec des compétences dans des technologies comme Lora, Zigbee, et Arduino pour des applications innovantes en environnement industriel. Il a dirigé plusieurs projets de recherche autour de l'intégration de l'IoT et des réseaux sans fil pour optimiser la connectivité et la sécurité dans les systèmes industriels

Nadim Henoud

Nadim Henoud est ingénieur logiciel et expert en cybersécurité avec plus de 15 ans d'expérience. Il combine une connaissance technique approfondie et une expertise stratégique en méthodologie agile pour concevoir des architectures évolutives et livrer des solutions technologiques complexes. Il intervient également à Télécom Paris, EPITA, ESIEA et à l'USJ de Beyrouth, où il enseigne sur des sujets liés à l'ingénierie, la sécurité, l'intelligence artificielle et l'apprentissage automatique

Yacine Ladjici

Yacine Ladjici est responsable de la cybersécurité du groupe Valeo Power, avec un parcours solide dans l'industrie automobile en conception et sécurisation de produits pour la mobilité intelligente et connectée. Il est intervenant à la Société des Ingénieurs de l'Automobile, Télécom ParisTech et à l'Université de Paris-Saclay. Il préside également la communauté des experts cybersécurité de la SIA

Executive Certificate Cybersécurité

INFORMATIONS PRATIQUES

INSCRIPTION

Pour vous inscrire, veuillez compléter le formulaire en ligne en cliquant ici.

CONTACT & ACCESSIBILITÉ

Maria FAHED, PhD
Responsable de l'offre Executive Certificate Cybersécurité : Sécurisation avancée et gestion des cybermenaces modernes
maria.fahed@universite-paris-saclay.fr

Titulaire d'un Phd, Maria est en charge de créer les nouvelles formations certifiante et diplômantes de la Direction de la Formation Tout au Long de la Vie à l'université Paris-Saclay, première université d'Europe classée 12ème au classement Shangaï 2024. Maria a débuté sa carrière en tant que chercheuse et enseignante, notamment au CEA et dans une école d'ingénieurs en numérique.

handicap.cfadftlv@universite-paris-saclay.fr
Plus d'informations sur le site de l'Université Paris-Saclay :
www.universite-paris-saclay.fr
Rubrique Vie de Campus > Handicap

LIEU DE LA FORMATION

Université Paris-Saclay, 9 Rue Joliot Curie, 91190 Gif-sur-Yvette
IUT de Cachan 9 Avenue de la Division Leclerc 94230 Cachan

université PARIS-SACLAY