BAC +5 - NIVEAU 7

CERTIFICATION PROFESSIONNELLE
INGÉNIEUR SYSTÈMES, RÉSEAUX ET CYBERSÉCURITÉ



RNCP [1] 38117 (JO 18/10/2023)

NIVEAU 7 : Cadre Européen des Certifications

CODE DIPLÔME : 16X32630

CODE NSF : 326 : Informatique, traitement de l'information, réseaux de transmission

DIPLÔME DÉLIVRÉ PAR : CERTIFICATEUR : INSTITUT EUROPÉEN F2I

PUBLIC
Alternants, salariés, étudiants, demandeurs d'emploi, travailleurs indépendants

Accessible aux personnes en situation d'handicap (PSH)

ADMISSION
Candidature en ligne ou sur Parcoursup.
Recrutement sur dossier, entretien, étude personnalisée de votre projet de formation avec un conseiller en réussite professionnelle et courrier d'admission.

Prérequis

Intégration en 1ère année : Niveau 6
OU avoir une expérience de 2 ans dans le secteur.

Niveau 6 › Année 1 › Année 2 › Validation : Certification professionnelle Niveau 7

Autre situation : contacter GFS

Voies d'accès à la formation

L'accès à une action de formation varie en fonction de votre vécu antérieur, de votre situation actuelle et de votre projection future.

Alternance

> Acquérir une expérience significative, se professionnaliser

Contrat d'apprentissage ou de professionnalisation.
Formation en alternance financée par un Opérateur de Compétences (OPCO) ou un établissement public.
La formation est gratuite pour le bénéficiaire.

Initiale alternée

> Découvrir le monde de l'entreprise avec une immersion professionnelle

Formation initiale alternée financée par l'apprenant :
Frais d'inscription annuels : 150 € net*
Frais de scolarité annuels : 6275 € net
*350 € net pour les étudiants qui viennent de l'étranger.

Possibilité de demander un financement total ou partiel à l'entreprise, dans le cadre d'un partenariat éducatif.

Formule pro

> Se réorienter (reconversion), développer et valider ses compétences

Pour les salariés, demandeurs d'emploi, indépendants, avec expérience professionnelle (selon votre statut) :
Compte personnel de formation (CPF), Plan de Développement des Compétences (PDC), CPF de Transition, Promotion par l'alternance (Pro-A), Contrat de Sécurisation Professionnelle (CSP).

Votre validation peut être réalisée en VAE (Validation des Acquis de l'Expérience).
Parcours individualisé et financement sur devis en fonction de l'expérience.

Rythme de la formation

Grâce à des périodes alternées en entreprise et en centre de formation, le rythme de formation permet de concilier une formation complète avec une immersion professionnelle.

Durée de la formation

Nombre d'heures : 900 h. La durée du parcours de formation est modulable selon la voie d'accès.

Objectifs et exemples de missions

L'Ingénieur systèmes réseaux et cybersécurité est responsable de la mise en place, de l'intégration et de la maintenance des matériels et logiciels d'un système d'exploitation sur des serveurs internes ou situés dans des data centers hors de l'entreprise. Il peut intervenir dans le cadre de la mise en service de plateformes informatiques et de traitements distants, à la demande et mutualisés. Il définit les besoins et l'architecture informatique de l'entreprise. Il est garant du bon fonctionnement, de la stabilité et de la qualité du réseau, participe à son évolution, pilote l'accès aux utilisateurs et assure l'équilibre entre le matériel, l'intégralité du système et les logiciels associés.
De manière générale, la fonction d'Ingénieur systèmes, réseaux et cybersécurité varie selon le type de structure et l'organisation de la DSI de l'entreprise, on peut distinguer trois types d'activités : il peut travailler pour des entreprises, des constructeurs ou pour des SSII.

> Mise en oeuvre d'un processus d'audits des systèmes et réseaux d'une organisation
> Analyse critique des architectures systèmes et réseaux existantes
> Conception d'une stratégie de développement des systèmes et réseaux sécurisée
> Mise en place de la stratégie de configuration de routage
> Mise en place de la stratégie de paramétrage des serveurs
> Pilotage du déploiement de l'environnement logiciels et applicatifs
> Gestion des comptes et contrôle des accès
> Management des équipes intervenant sur les systèmes et les réseaux
> Pilotage des projets de développement des organisations
> Analyse et prévention des risques d'intrusion et de rupture des systèmes et réseaux
> Évaluation des investissements nécessaires
> Accompagnement à la conduite du changement auprès des utilisateurs

Suite de parcours et débouchés professionnels

Cette formation permet d'accéder à un emploi :

> Ingénieur/Expert·e systèmes et réseaux
> Expert·e réseaux et telecoms
> Ingénieur sécurité web
> Responsable sécurité informatique
> Architecte réseaux informatiques
> Ingénieur/Expert·e en sécurité informatique
> Consultant·e réseaux informatiques
> Ingénieur plateformes de services

Encadrement

Chaque apprenant bénéficie d'une formation et d'un suivi pédagogique individualisé, encadré par les formateurs, un responsable pédagogique et un conseiller en réussite professionnelle. Les membres de cette équipe sont les interlocuteurs privilégiés de l'apprenant pour la réussite de son parcours pédagogique et professionnel.
La liste des formateurs correspondant à la formation suivie est remise avant l'entrée en formation, lors de l'entretien avec le conseiller en réussite professionnelle.
Un accompagnement individualisé se crée avant, pendant et après la formation.

Pour aller plus loin, passerelles et équivalences

Pour plus de détails sur ce parcours de formation, rendez-vous sur le site de **France Compétences** *https://francecompetences.fr* puis entrez le code RNCP de cette fiche. Vous pourrez également télécharger la fiche **Europass** de la formation.
Pour valoriser vos compétences et gérer votre carrière en France ou en Europe, rendez-vous sur la plateforme Europass : *https://europa.eu/europass/fr*

GRIMP Recherche d'entreprise
GFS ONLINE ENT, planning, notes, ressources
Microsoft 365 Adresse email et applications
Wi-Fi & écrans interactifs dans chaque salle
Logiciels métiers et/ou certifications
Bibliothèque & ludothèque à disposition
Accès photocopieur et numérisation
Espace de vie sur place

GFS Clermont-Fd • 4 place Charles de Gaulle, 63400 Chamalières • 04 73 19 53 00 • contact@gfs63.com • www.groupeformationsystemes.com

PRO-SYSTÈMES SARL au capital de 152 449 € - RCS Clermont-Ferrand B 377 891 999 - Établissement d'enseignement supérieur privé et technique - Centre de Formation des Apprentis (CFA) - Édition 09/2026

INGÉNIEUR SYSTÈMES, RÉSEAUX ET CYBERSÉCURITÉ

EN PARTENARIAT AVEC IEF2I EDUCATION

ORGANISATION ET MODALITÉS DE LA FORMATION

Formation de 1 à 2 ans, adaptée selon parcours antérieur.
La formation est multimodale avec présence en centre, formation à distance (FOAD), formation en situation de travail (FEST).
Pour chaque stagiaire, un planning adapté à son statut est joint à la convention de formation.
La répartition horaire par matière ou par module est susceptible de subir des modifications en fonction du niveau initial de l'apprenant et/ou du groupe, de son parcours individualisé et de son accompagnement. Il en est de même pour le programme.

MÉTHODES PÉDAGOGIQUES

Pédagogie active : cas pratiques, participation à des concours, pédagogie inversée, partenariats pédagogiques avec des entreprises, thématiques professionnelles.

DÉLAI D'ACCÈS À LA FORMATION

De 1 jour à 3 mois en fonction du financeur.

HORAIRES

La formation se déroule par demi-journées : de 8h15 à 12h00 et de 13h00 à 16h45. Des ateliers peuvent être proposés en sus après 17h00.

NOMBRE DE STAGIAIRES

Un groupe de 5 à 25 participants.

SUIVI DE L'EXÉCUTION DU PROGRAMME

Un émargement est réalisé par demi-journée : il est signé par l'apprenant et le formateur. L'apprenant reçoit à son inscription des codes personnels pour consulter son planning, des ressources pédagogiques et ses résultats d'évaluations sur l'ENT [2].

RÈGLEMENT D'EXAMENS

Pour les personnes ayant suivi le cycle de formation :
Évaluations écrites et orales en cours et en fin de formation avec remise de bulletins de notes et appréciation de l'équipe pédagogique.
L'apprenant reçoit une attestation de fin de formation mentionnant les objectifs, la nature, la durée de l'action ainsi qu'un résultat de l'évaluation.
La validation des 5 blocs (moyenne >10/20 par bloc) et de la compétence transversale en anglais technique permet de valider la Certification Professionnelle « Ingénieur Systèmes, Réseaux et Cybersécurité » délivrée par l'IEF2I, après réussite aux examens.

1ÈRE ANNÉE	FORME	COEFF.
BLOC 2 : SUIVRE ET METTRE EN OEUVRE LE DÉPLOIEMENT DE L'INFRASTRUCTURE SYSTÈMES ET RÉSEAUX SÉCURISÉE ADAPTÉE AUX BESOINS		
· CCNA - TECHNOLOGIES LAN & WAN	TP + QCM	5
· ADMINISTRATION WINDOWS SERVER	TP + QCM	
· MICROSOFT ENDPOINT CONFIGURATION MANAGER	TP + QCM	
· PROGRAMMATION WEB (HTLM / CSS / JAVASCRIPT)	TP + QCM	
· PROGRAMMATION PHP ET MYSQL	TP + QCM	
· AUTOMATISER L'ADMINISTRATION AVEC POWERSHELL	TP + QCM	
· LINUX - SYSTÈMES ET RÉSEAUX	TP + QCM	
· MICROSOFT 365 - ADMINISTRATION ET SÉCURITÉ	TP + QCM	
· DOCKER ET KUBERNETES	TP + QCM	
· DEVOPS	TP + QCM	
· AZURE - IDENTITÉS, STOCKAGE, RÉSEAUX ET SÉCURITÉ	TP + QCM	
BLOC 3 : ÉLABORER LA STRATÉGIE DE SÉCURISATION DE L'INFRASTRUCTURE INFORMATIQUE		
· GESTION DE CRISE ET PCA	QCM	4
· PKI - MISE EN OEUVRE DE SERVICES DE CERTIFICATS	TP + QCM	
· ANALYSE DE MALWARES	TP + QCM	
· PYTHON POUR TESTS D'INTRUSION	TP + QCM	
· EBIOS RISK MANAGER	QCM	
· VMWARE	TP + QCM	
BLOC 4 : MANAGER LA PERFORMANCE DES SYTÈMES ET RÉSEAUX D'UNE ORGANISATION		
· MICROSOFT SYSTEM CENTER OPERATIONS MANAGER	TP + QCM	1
2ÈME ANNÉE	**FORME**	**COEFF.**
BLOC 1 : PILOTER LA CONCEPTION D'UNE INFRASTRUCTURE SYSTÈMES ET RÉSEAUX SÉCURISÉE ET RESPECTUEUSE DE LA POLITIQUE RSE D'UNE ORGANISATION		
· ISO 27001 - LEAD IMPLEMENTER	QCM	2
· AMAZON WEB SERVICES (AWS)	TP+QCM	
BLOC 2 : SUIVRE ET METTRE EN OEUVRE LE DÉPLOIEMENT DE L'INFRASTRUCTURE SYSTÈMES ET RÉSEAUX SÉCURISÉE ADAPTÉE AUX BESOINS		
· LINUX - SÉCURITÉ RÉSEAUX ET SYSTÈMES	TP + QCM	5
· AUTOMATISATION AVEC ANSIBLE	TP + QCM	
· GESTION DE PROJET	ÉTUDE DE CAS	
BLOC 3 : ÉLABORER LA STRATÉGIE DE SÉCURISATION DE L'INFRASTRUCTURE INFORMATIQUE		
· CISCO FIREWALL ASA	TP + QCM	4
· DEVSECOPS	TP + QCM	
· HAUTE DISPONIBILITÉ - WINDOWS SERVER	TP + QCM	
· SÉCURITÉ DE L'IOT	TP + QCM	
· SIEM SPLUNK - COLLECTE ET ANALYSE DES LOGS	TP + QCM	
· SÉCURITÉ CLOUD ET IAM - MICROSOFT	TP + QCM	
· PRÉPARATION À LA CERTIFICATION CEH	QCM	
· PRÉPARATION ENCADRÉE DE PROJET	ÉCRIT	
· VEEAM BACKUP	TP + QCM	
· BLOCKCHAIN - LES TOKENS ET CRYPTO-MONNAIES	QCM	
· ANALYSE FORENSICS	TP + QCM	
· RGPD - RÈGLEMENT ET AUDIT DE CONFORMITÉ	QCM	
· PRÉPARATION TOEIC	QCM	
BLOC 4 : MANAGER LA PERFORMANCE DES SYSTÈMES ET RÉSEAUX D'UNE ORGANISATION		
· ISO 27005 - RISK MANAGER	QCM	1
BLOC 5 : ÉLABORER UNE STRATÉGIE DE GESTION DES NOUVEAUX PROJETS INFORMATIQUES D'UNE ORGANISATION		
· PRÉPARATION ENCADRÉE DE PROJET	ORAL	1

Pour les personnes en activité professionnelle ou ayant eu une activité professionnelle significative :

· VAE
La Validation des Acquis de l'Expérience permet de valider un certificat ou un diplôme représentant des compétences acquises lors de votre parcours professionnel. Pour ce type de parcours, consultez votre conseiller en réussite professionnelle ainsi que : *https://vae.gouv.fr/* ou *https://www.fede.education/vae/*

APPRÉCIATION DES RÉSULTATS

Taux de réussite : ***pas de promotion antérieure***

Taux d'employabilité à 6 mois : ***pas de promotion antérieure***

PROGRESSION PÉDAGOGIQUE

1ÈRE ANNÉE

BLOC 2 : Suivre et mettre en oeuvre le déploiement de l'infrastructure systèmes

CCNA - Technologies LAN & WAN
· Fondamentaux des réseaux
· Accès au réseau LAN
· Connectivité IP
· Services IP
· Sécurité de base
· Évolution vers des réseaux intelligents
Administration Windows Server
· Vue d'ensemble de l'administration de Windows Server
· Services d'identité dans Windows Server
· Services d'infrastructure réseau dans Windows Server
· Gestion des serveurs de fichiers et du stockage dans Windows Server
· Virtualisation Hyper-V
Microsoft Endpoint Configuration Manager & Intune
· Gestion des ordinateurs et des périphériques mobiles dans l'entreprise
· Préparation de l'infrastructure de gestion pour supporter les PCS et les périphériques mobiles
· Déploiement et gestion du client configuration manager
· Gestion des inventaires pour les PCS et les applications
· Déploiement et gestion des applications
· Maintenance des mises à jour logicielles pour les PCS gérés
Programmation Web (HTLM/CSS/ JavaScript)
· Présentation du développement web
· Langage HTLM
· Les feuilles de style CSS
· Langage JavaScript
Programmation PHP et MySQL
· Présentation générale
· Syntaxe
· PHP5 et MySQL
· Étude de cas
Automatiser l'administration avec Powershell
· Windows PowerShell : généralités
· Cmdlets pour l'administration
· Gestion des modules PowerShell, des packages
· Administration des ordinateurs à distance
· WMI & CIM
· Scripts Windows PowerShell
Microsoft 365, administration et sécurité
· Planificationde Microsoft 365
· Gestion des utilisateurs et des groupes Microsoft 365
· Planification et configuration des services Exchange Online
· Planification et déploiement de Microsoft Teams
· Configurer les services Sharepoint Online
· Vue d'ensemble des fonctionnalités de conformité dans Office 365
Docker et Kubernetes
· Docker introduction
· Manipulation des images
· Manipulation des conteneurs
· Les conteneurs
· Orchestration des conteneurs
· Docker swarm
· Kubernetes
Devops
· Introduction
· Vue d'ensemble de Jenkins
· Projets Jenkins
· Intégration avec les outils de versioning
· Qualité de code et taux de couverture de tests
· Projets parametres
· Déploiements automatisés
· Jenkins pipeline
· Architecture maître esclave
· Administration de Jenkins
Azure - Identités, stockage, réseaux et sécurité
· Généralités
· Machines virtuelles Azure
· Mise en réseau virtuelle
· Connectivité intersites
· Gestion du trafic du réseau
· Stockage Azure
Linux, systèmes et réseaux

BLOC 3 : Élaborer la stratégie de sécurisation de l'infrastructure informatique

PKI, mise en oeuvre de services de certificats
· Introduction au chiffrements
· Introduction aux systèmes d'infrastructure à clés publiques
· PKI dans un environnement d'entreprise
Analyse de malwares
· Introduction aux malwares
· Éradication
· Détection
· Identification
Python pour tests d'intrusion
· Introduction à la programmation avec Python
· Comprendre le principe des tests d'intrusion
· Réseau
· Système
· Web
· Cryptographie
· Antivirus et portes dérobées
EBIOS Risk Manager
· Introduction à la méthode EBIOS
· Cadrage et socle de sécurité
· Sources de risques (SR) et objectifs visés (OV)
· Scenarios stratégiques
· Scénarios opérationnels
· Traitement du risque
VMWare - Stockage, réseaux, VMs et haute disponibilité
· Présentation de vSphere et de la virtualisation
· Installation et configuration d'Esxi
· Déploiement et configuration de vCenter
· Configuration de la mise en réseau vSphere
· Configuration du stockage vSphere
· Déployer des machines virtuelles
· Gestion des machines virtuelles
· Déploiement et configuration des clusters vSphere
· Gestion du cycle de vie de vSphere
Gestion de crise et PCA

BLOC 4 : Manager la performance des systèmes et réseaux d'une organisation

Microsoft System Center Operations Manager - Administration
· Introduction à SCOM
· Déploiement de l'infrastructure
· Déploiement des agents
· Déploiement et administration des management packs
· Administration des moniteurs
· Supervision des équipements réseaux et des systèmes UNIX/LINUX
· Rapports

2ÈME ANNÉE

BLOC 1 : Piloter la conception d'une infrastructure systèmes et réseaux sécurisée et respectueuse de la politique RSE d'une organisation

ISO 27001 - Lead Implementer
· Introduction à la norme et initialisation d'un SMSI
· Planification de la mise en oeuvre d'un SMSI
· Mise en oeuvre du SMSI
· Surveillance, amélioration continue et préparation à l'audit de certification du SMSI
Amazon Web Services (AWS) - Stockage, réseaux et sécurité
· Examen des fondamentaux de l'architecture
· Sécurité du compte
· Réseautage
· Calculer
· Stockage
· Conteneurs
· Architecture sans serveur

BLOC 2 : Suivre et mettre en oeuvre le déploiement de l'infrastructure systèmes

Linux, sécurité réseaux et systèmes
· Les enjeux de la sécurité
· Les utilisateurs et les droits
· Les bibliothèques PAM
· Le système SELinux ou la sécurité dans le noyau
· Les principaux protocoles cryptographiques en client/serveur
· Les pares-feux
· Les VPN
· La sécurisation des applications
· Les techniques d'audit
Automatisation avec Ansible
· Introduction
· Installation et configuration
· Présentation du format YAML
· Playbooks
· Commandes Ad Hoc
· Les rôles
· Les modules
Gestion de projet - ITIL
· Introduction
· Concepts clés de la gestion des services
· Concepts clés d'ITIL
· Principes directeurs
· Pratiques de gestion ITIL

BLOC 3 : Élaborer la stratégie de sécurisation de l'infrastructure informatique

Cisco Firewall ASA - Configuration et administration
· Introduction
· Traduction d'adresses et connexions
· ACL et content filtering
· Routage et commutation
· VPN
· Failover
DevSecOps
· Introduction
· Culture et management
· Considérations stratégiques
· Considérations générales sur la sécurité
· Sécurité des applications
· Sécurité opérationnelle
· Logging, monitoring et reponse
Haute disponibilité - Windows Server
· Haute disponibilité et reprise d'activité
· Configuration matérielles et logicielles
· Mise en place de cluster applicatifs
· Clustering pour les machines virtuelles Hyper-V
· Répartition de charge réseau (NLB)
Sécurité de l'IOT
· Panorama de l'IOT
· Attaques réseaux
· Hardware hacking
· Radio hacking
SIEM Splunk - Collecte et analyse des logs
· Installer Splunk : récupérer/injecter les données
· Exploration de données
· Tableaux de bord (Base)
· Tableaux de bord (Avance)
· Installation d'application
· Modèles de données
· Enrichissement de données
· Alertes
Sécurité Cloud et IAM - Microsoft
· Mettre en oeuvre une solution de gestion des identités
· Mettre en oeuvre une solution d'authentification et de gestion des accès
· Mettre en oeuvre la gestion des accès pour les applications
· Planifier et mettre en oeuvre une stratégie de gouvernance des identités
Veeam Backup - Mise en oeuvre, gestion et récupération des données
· Introduction
· Création de capacités de sauvegarde
· Création de capacités de réplication
· Sauvegardes secondaires
· Capacités avancées du référentiel
· Protection des données dans le cloud
· Restauration à partir d'une sauvegarde
· Restauration à partir du replica
· Tester la sauvegarde et la replication
· Veeam Backup Enterprise Manager et Veeam One
· Configuration de la sauvegarde
Blockchain - Les tokens et crypto-monnaies
· Les impacts stratégiques
· Les aspects juridiques
· Les actifs numériques
· Les tokens
· La crypto-monnaie
· Les perspectives
Analyse Forensics
· Introduction à la SSI
· Digital forensic
· L'analyse forensique réseau
· L'analyse forensique mémoire
· L'analyse de disque dur
· L'analyse de fichiers
RGPD - Règlement et audit de conformité
· Connaître les nouveautés apportées par le règlement
· Prévoir un plan d'actions pour se mettre en conformité
Préparation à la certification CEH
Préparation au TOEIC

BLOC 4 : Manager la performance des systèmes et réseaux d'une organisation

ISO 27005 - Risk Manageer
· Introduction au programme de gestion des risques conforme à la norme
· Connaître le cadre normatif et règlementaire
· Mettre en oeuvre un programme de management du risque
· Établir le contexte mission, objectifs, valeurs, stratégies
· Identifier les risques
· Analyser et évaluer les risques
· Apprécier les risques avec une méthode quantitative
· Notion de ROSI
· Traiter les risques
· Apprécier les risques et gérer les risques résiduels
· Communiquer sur les risques

BLOC 5 : Élaborer une stratégie de gestion des nouveaux projets informatiques d'une organisation

Préparation encadrée de projet

ACCOMPAGNEMENT, CONDUITE DE PROJET, ET ÉVALUATIONS

· Accompagnement individualisé et collectif (entreprise, formation, dossiers...)
· Thématiques
· Évaluations sommatives et formatives

Ingénieur Systèmes, Réseaux et Cybersécurité - Fiche RNCP N° 38117 - Codes NSF 326 - Décision du 18 octobre 2023 portant enregistrement au répertoire national des certifications professionnelles pour cinq ans, au niveau 7, avec effet au 18 octobre 2023 jusqu'au 18 octobre 2028 sous l'autorité et délivré par INSTITUT EUROPÉEN F2I - Certification accessible via le dispositif VAE.

[1] *RNCP : Répertoire National de la Certification Professionnelle*
[2] *ENT : Espace Numérique de Travail*
[3] *CCP : Certificat de Compétence Professionnelle*

PRO-SYSTÈMES SARL au capital de 152 449 € - RCS Clermont-Ferrand B 377 891 999 - Établissement d'enseignement supérieur privé et technique - Centre de Formation des Apprentis (CFA) - Édition 09/2026