BAC +3

BACHELOR INFORMATIQUE ET CYBERSÉCURITÉ

ADMINISTRATEUR D'INFRASTRUCTURES SÉCURISÉES

TITRE PROFESSIONNEL : RNCP [1] 37680

NIVEAU 6 : Cadre Européen des Certifications

CODE DIPLÔME 32032610

DIPLÔME DÉLIVRÉ PAR LE MINISTÈRE DU TRAVAIL, DU PLEIN EMPLOI ET DE L'INSERTION

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 3ème année : BAC +2 (BTS, DUT, etc.)

BAC > B1 > B2 > B3 > Validation : Titre BAC +3 Bachelor

BAC +2 > B3

Autre situation : contacter GFS

Voies d'accès à la formation

L'accès à une action de formation varie en fonction de votre parcours antérieur, de votre situation actuelle et de votre projet futur.

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 : 5500 €
*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).

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

Objectifs et exemples de missions

L'administrateur d'infrastructures sécurisées (AIS) met en œuvre, administre et sécurise les infrastructures informatiques locales et dans le cloud. Il conçoit et met en production des solutions répondant à des besoins d'évolution. Il implémente et optimise les dispositifs de supervision. Il participe à la gestion de la cybersécurité en analysant les menaces et en mettant en place des mesures de sécurité et de réaction en cas d'incident.

> Administrer et sécuriser les infrastructures
> Concevoir et mettre en oeuvre une solution en réponse à un besoin d'évolution
> Participer à la gestion de la cybersécurité

Suite de parcours et débouchés professionnels

Cette formation permet de poursuivre vos études vers un titre de **niveau 7** ou d'accéder à un emploi :

> Administrateur(trice) systèmes et réseaux
> Administrateur(trice) systèmes
> Administrateur(trice) réseaux
> Administrateur(trice) d'infrastructures
> Superviseur infrastructure et réseaux
> Responsable infrastructure systèmes et réseaux

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

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*

ENT Planning, notes, ressources
Microsoft 365 Adresse email et applications
WIFI & vidéoprojecteur dans chaque salle
Logiciels métiers et/ou certifications
Bibliothèque & revues 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 03/2024

ADMINISTRATEUR D'INFRASTRUCTURES SÉCURISÉES

ORGANISATION DE LA FORMATION

Formation de 1 an, 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.

MODALITÉS 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 8 h 15 à 12 h 00 et de 13 h 00 à 16 h 45. Des masterclass peuvent être proposées en sus après 17 h 00.

NOMBRE DE STAGIAIRES

Un groupe de 5 à 20 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 :
Examens écrits et oraux 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.
Les résultats de la soutenance et des contrôles détermineront l'obtention du titre professionnel « Administrateur d'Infrastructures Sécurisées » inscrit au RNCP niveau 6, délivré par le Ministère du Travail, du Plein Emploi et de l'Insertion, ainsi que du Bachelor Informatique et Cybersécurité, délivré par GFS.

ÉPREUVE	FORME	DURÉE
ADMINISTRER ET SÉCURISER LES INFRASTRUCTURES		
APPLIQUER LES BONNES PRATIQUES DANS L'ADMINISTRATION DES INFRASTRUCTURES		
ADMINISTRER ET SÉCURISER LES INFRASTRUCTURES RÉSEAUX		
ADMINISTRER ET SÉCURISER LES INFRASTRUCTURES SYSTÈMES		
ADMINISTRER ET SÉCURISER LES INFRASTRUCTURES VIRTUALISÉES	CCF	X
CONCEVOIR ET METTRE EN OEUVRE UNE SOLUTION EN RÉPONSE À UN BESOIN D'ÉVOLUTION	ÉCRIT	30 MIN
CONCEVOIR UNE SOLUTION TECHNIQUE RÉPONDANT À DES BESOINS D'ÉVOLUTION DE L'INFRASTRUCTURE	ORAL	40 MIN
METTRE EN PRODUCTION DES ÉVOLUTIONS DE L'INFRASTRUCTURE	ENTRETIEN TECHNIQUE	60 MIN
METTRE EN OEUVRE ET OPTIMISER LA SUPERVISION DES INFRASTRUCTURES	ENTRETIEN FINAL	20 MIN
PARTICIPER À LA GESTION DE LA CYBERSÉCURITÉ		
PARTICIPER À LA MESURE ET À L'ANALYSE DU NIVEAU DE SÉCURITÉ DE L'INFRASTRUCTURE		
PARTICIPER À L'ÉLABORATION ET À LA MISE EN OEUVRE DE LA POLITIQUE DE SÉCURITÉ		
PARTICIPER À LA DÉTECTION ET AU TRAITEMENT DES INCIDENTS DE SÉCURITÉ		

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/*

APPRÉCIATION DES RÉSULTATS

Consulter les indicateurs :
https://www.inserjeunes.education.gouv.fr
Taux de réussite : **pas de promotion antérieure**

PROGRESSION PÉDAGOGIQUE

Activité 1 : « Administrer et sécuriser les infrastructures »

Appliquer les bonnes pratiques dans l'administration des infrastructures
- Identifier, classifier et enregistrer un incident
- Diagnostiquer l'incident et le résoudre
- Etablir, planifier et réaliser les tâches préventives de type mise à jour, sauvegarde, vérification des dispositifs de reprise et de continuité informatique, remplacement ou paramétrage d'un élément de configuration
- Rédiger une procédure dans le respect des bonnes pratiques
- Documenter les actions et changements de configuration dans un outil de suivi

Administrer et sécuriser les infrastructures réseaux
- Administrer et sécuriser, en appliquant les bonnes pratiques, les éléments des infrastructures réseaux
- S'adapter aux différents environnements techniques
- Exploiter les sources d'information, les documentations techniques et échanger par écrit avec les professionnels y compris en anglais

Administrer et sécuriser les infrastructures systèmes
- Administrer et sécuriser, en appliquant les bonnes pratiques, les éléments des infrastructures systèmes
- S'adapter aux différents environnements techniques
- Exploiter les sources d'information, les documentations techniques et échanger par écrit avec les professionnels y compris en anglais

Administrer et sécuriser les infrastructures virtualisées
- Administrer et sécuriser, en appliquant les bonnes pratiques, les éléments des infrastructures virtualisées
- S'adapter aux différents environnements techniques
- Exploiter les sources d'information, les documentations techniques et échanger par écrit avec les professionnels y compris en anglais

Activité 2 : « Concevoir et mettre en oeuvre une solution en réponse à un besoin d'évolution »

Concevoir une solution technique répondant à des besoins d'évolution de l'infrastructure
- Concevoir et proposer dans les délais impartis une solution technique évolutive qui tient compte des contraintes budgétaires, environnementales, de production et de sécurité ainsi que des règlementations en vigueur
- Définir les critères et mettre en oeuvre les moyens qui permettent de vérifier que la solution technique est conforme au cahier des charges
- Présenter et argumenter dans un rapport ou une présentation la solution technique afin de la soumettre à la validation des décideurs

Mettre en production des évolutions de l'infrastructure
- À partir d'une solution, élaborée et testée en amont et répondant à une demande de changement, planifier, réaliser et valider son intégration en appliquant les bonnes pratiques afin qu'elle soit mise en production dans le respect des accords de niveau de service, des règles de sécurité et de la réglementation en vigueur
- Évaluer et valider chaque étape de la mise en production afin de limiter les risques sur la fourniture des services
- Tester et valider les procédures des plans de reprise et de continuité informatique (PRI, PCI) associés aux dispositifs mis en production
- Assurer le transfert de compétences et mettre à jour les documents d'exploitation

Mettre en oeuvre et optimiser la supervision des infrastructures
- Choisir les indicateurs et évènements associés à la disponibilité, aux performances, à la consommation de services qui doivent être supervisés
- Mettre en oeuvre ou optimiser les outils de supervision nécessaires au suivi des indicateurs et des évènements, en respect de la réglementation et des règles de sécurité
- Mettre à disposition des équipes d'exploitation et d'administration les tableaux de bords et les informations indispensables au support et au pilotage des infrastructures du système d'information
- Exploiter les sources d'information, les documentations techniques et échanger par écrit avec les professionnels y compris en anglais

Activité 3 : « Participer à la gestion de la cyber sécurité »

Participer à la mesure et à l'analyse du niveau de sécurité de l'infrastructure
- Planifier et spécifier les points de contrôle
- Effectuer les mesures afin d'évaluer le niveau de sécurité dans le respect de la réglementation
- Rédiger un rapport présentant les contrôles, les mesures effectuées et l'évaluation du niveau de sécurité
- Participer à une démarche d'analyse de risques afin d'identifier les menaces, les vulnérabilités et la criticité des risques pouvant affecter les composants de l'infrastructure
- Participer à l'élaboration d'une lettre de mission en vue d'un audit de sécurité réalisé par un tiers
- Vérifier si les exigences de la lettre de mission ont été respectées afin de qualifier le travail effectué
- Exploiter les sources d'information, les logiciels et échanger par écrit avec les professionnels y compris en anglais

Participer à l'élaboration et à la mise en oeuvre de la politique de sécurité
- A partir des règles de sécurité retenues dans la politique de sécurité du système d'information (PSSI), contribuer, dans son périmètre d'intervention, au choix, à l'implantation et l'évaluation des solutions permettant leur mise en oeuvre
- Participer à la définition, rédaction et la validation de procédures permettant la déclinaison opérationnelle de la PSSI
- S'assurer de la formation des utilisateurs au respect des bonnes pratiques de sécurité informatique et participer à la mise à niveau des équipes techniques afin de contribuer à l'application de la PSSI
- Afin de s'adapter aux différents environnements techniques, exploiter les sources d'information, les documentations techniques et échanger par écrit avec les professionnels y compris en anglais

Participer à la détection et au traitement des incidents de sécurité
- Configurer et exploiter un dispositif de détection d'évènements de sécurité afin de détecter et qualifier un incident
- Appliquer les mesures de réaction en réponse à un incident afin de minimiser l'impact sur les actifs de l'entreprise et d'informer les parties concernées
- Assurer la préservation des traces et des preuves numériques afin de les transmettre aux analystes cyber
- À la suite d'un incident de sécurité majeur, participer à la réalisation d'un retour d'expérience (RETEX) afin de capitaliser et renforcer la sécurité de l'entreprise
- Assurer sa veille en cybersécurité afin d'adapter les règles de détection et de traitement des incidents aux nouvelles menaces
- Exploiter les sources d'information, les documentations techniques et échanger par écrit avec les professionnels y compris en anglais

ACCOMPAGNEMENT, CONDUITE DE PROJET, ET ÉVALUATIONS

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

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

Envie d'avenir
Envie d'agir

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 03/2024