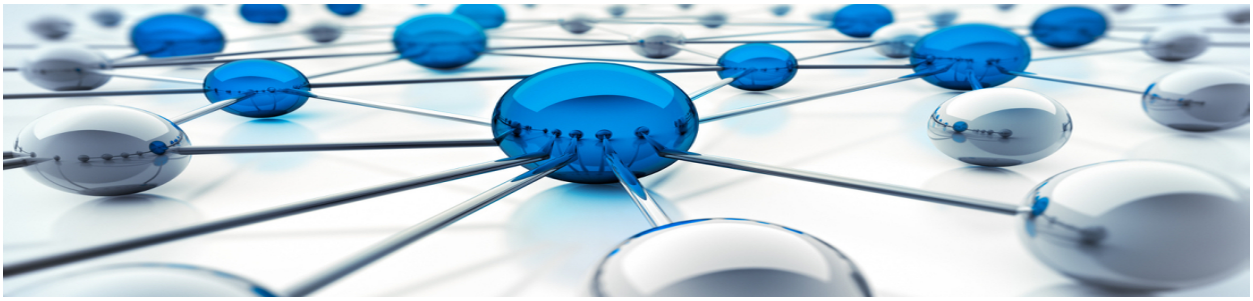

TECHNICIEN(NE) d'ASSISTANCE EN RÉSEAU INFORMATIQUE

Titre de Niveau III **Code RNCP : 28121**

DUREE : 875 heures
560 heures en formation incluant une conduite de projet
315 heures d'application pratique en entreprise

Arrêté du 07 avril 2017 publié au Journal Officiel du 21 avril 2017 portant enregistrement au répertoire national des certifications professionnelles. Enregistrement pour trois ans, au niveau III, sous l'intitulé "Technicien(ne) d'assistance en réseau informatique" avec effet au 07 septembre 2014, jusqu'au 21 avril 2020.

OBJECTIFS

- Installer, mettre en service et dépanner des équipements informatiques (PC, périphériques et logiciels) et numériques (voix, images et données) reliés en réseau.
- Intégrer de nouveaux outils de communication, harmoniser, sécuriser et fiabiliser les échanges de données.
- Organiser la veille technologique et de maitriser les techniques des réseaux informatiques et télécom
- Assister, à distance ou sur site, les utilisateurs et les clients afin de résoudre au plus vite leurs incidents et de les aider à optimiser l'utilisation de leurs outils bureautiques, informatiques et numériques. Chercher à satisfaire leurs demandes tout en respectant le cadre des contrats de services.

PUBLIC CONCERNE

- Personnes à la recherche d'un emploi répondant aux conditions suivantes :
  Âgées de 18 ans au moins ; non dispensées de recherche d'emploi par le Pôle Emploi à la date de début de la formation ; dont le projet professionnel a été validé ou non par une agence locale du Pôle emploi de Paris ou par une Mission Locale. Niveau d'anglais pré intermédiaire – Connaissance de l'outil bureautique

PRE REQUIS

- Niveau IV plus expérience dans le secteur de 5 ans mini ou niveau III de la formation professionnelle

OUTILS PEDAGOGIQUES

- La pédagogie alterne les **cours théoriques**, les **exercices** et les **mises en situation**
- Les stagiaires travailleront sur des exercices et des études de cas pratiques personnalisés.
- Matériel informatique
- Support vidéo
- Supports audio (développement de la compréhension orale)
- Supports écrits : Les supports pédagogiques seront fournis par le CFAS et remis aux stagiaires
- Accès à une plateforme collaborative 24h/24 pour les supports pédagogiques téléchargeables sous format PDF.

PROGRAMME DE FORMATION

Connaissances des métiers et secteurs – Positionnement emploi – suivi individuel 28 heures

Architectures informatiques et organisation de la maintenance 49 heures

- Architectures matérielles des micro-ordinateurs
- Études des périphériques associés
- Méthode d'analyse et de résolution de problèmes
- Maintenance des matériels et logiciels
- Méthode d'organisation de la maintenance curative/préventive
- Coût de la maintenance et optimisation
- Gestion des stocks

Logiciels courants

Sécurité réseaux et systèmes 182 heures

Rappel sur le réseau

- Bref historique, topologie, infrastructures physiques et câblage
- Modèles OSI et IPV4
- Les routeurs : leurs interfaces, leurs tables, etc.
- Hubs, switches et Vlan
- Accès à distance RTC/ADSL – configuration, sécurité, résolutions d'incidents
- Les pare-feu – architecture de sécurité
- Installation configuration et sécurisation d'un LAN avec Internet
- Ajout de ressources, configuration d'imprimantes réseau
- Processus client/serveur

Introduction à la cryptographie

- Introduction
- Chiffrement de flux (Stream Ciphers)
- Chiffrement par blocs (Block Ciphers)
- Chiffrement asymétrique
- Fonctions de hachage
- Intégrité et authentification
- Gestion des clés
- Tierces parties de confiance
- Standards divers

Sécurité des systèmes d'information, synthèse

Introduction

- RSSI : chef d'orchestre de la sécurité
- Les cadres normatifs et réglementaires
- L'analyse de risque
- Les audits de sécurité
- Plan de sensibilisation et de communication
- Le coût de la sécurité
- Plans de secours
- Concevoir des solutions optimales
- Supervision de la sécurité
- Les principes juridiques applicables au SI
- Les atteintes juridiques au STAD
- Recommandations pour une sécurisation « légale » du SI

Sécurité systèmes et réseaux, niveau 1

- Risques et menaces
- Architectures de sécurité
- Sécurité des données
- Sécurité des échanges
- Hardening
- Audit sécurité et exploitation
- Mise en situation

Sécurité systèmes et réseaux, niveau 2

- Rappels
- Les solutions de sécurité
- L'authentification
- Evaluer le niveau de sécurité du SI
- La sécurité des réseaux Wi-Fi
- La voix sur IP et la sécurité
- Gestion des événements de sécurité

Réseaux Privés Virtuels

- Introduction au VPN
- Le VPN pour assurer l'interconnexion de sites et de nomades
- Sécurisation du VPN : l'approche IPSec
- Quelle offre retenir pour son VPN
- Construction d'un VPN
- Les solutions d'interconnexion IP au cours du temps
- Cryptographie
- Tunnels, les protocoles
- ISAKMP et IKE
- Sécurité de l'infrastructure réseau
- Panorama des solutions VPN IPSec

Sécuriser Windows server

- Introduction
- Gestion de la sécurité dans Windows 2008 server
- L'analyseur de sécurité
- Etude détaillée des paramètres de sécurité
- Gestion des correctifs sous Windows 2008 server
- Active Directory
- Kerberos
- Cryptage, gestion des certificats et architecture PKI
- Sécurisation de l'accès distant

Sécurité des applications et Unix / Linux 114 heures

Linux/Unix

- Introduction
- La sécurité et l'Open source
- L'installation trop complète : l'exemple de Linux
- La sécurité locale du système
- Les utilitaires d'audit de sécurité
- Unix/Windows : CLI, shells, commandes indispensables
- Le scripting et l'adminsitration (shell, perl)

Java, sécurité des applications

- Présentation des concepts liés à la sécurité
- Mécanismes de sécurité de la machine virtuelle Java
- Java Authentication and Authorization Service (JAAS)
- SSL avec Java
- La sécurité d'une application J2EE
- La sécurité d'une application J2ME
- Présentation de la problématique de sécurité
- Mécanismes de protection dans le CLR
- Cryptage, certificats et signature
- Gestion de l'authentification et des habilitations en .NET
- Mécanismes de sécurité dans le cadre des standards de Web Services

Sécurisez votre réseau avec les outils Open Source
- Rappels
- Le firewall, brique indispensable
- L'accès Internet des utilisateurs
- Protection virale
- Interconnexion et nomadisme
- La détection d'intrusions
- Recherche de vulnérabilités

Web / sécurité — 106 heures

Introduction Internet
- Rappels des connaissances Internet, fonctionnement DNS
- Services Internet (clients / serveurs)
- Connexions Internet et service d'accès à distance
- Installation et configuration Active Directory, DNS, messagerie, ntp
- Installation et configuration Serveurs Web et FT
- Configuration SSL des serveurs Web
- Partage de fichiers, droits d'accès, contrôle d'accès
- Pratique Wi-Fi

Sécurité des applications Web

Introduction
- Constituants d'une application Web
- Le protocole HTTP en détail
- Les risques inhérents aux services Web
- Le firewall réseau dans la protection d'application HTTP
- Confidentialité des informations
- Configuration du système et des logiciels
- Principe du développement sécurisé
- L'authentification des utilisateurs
- Le firewall « applicatif »
- Supervision de la sécurité

Détection d'intrusions
- Le monde de la sécurité informatique
- TCP/IP pour firewalls et détection d'intrusions
- Rappel sur les techniques de firewalling / proxy
- Comprendre les attaques sur TCP/IP
- Intelligence Gathering : l'art du camouflage
- Protéger ses données
- Détecter les trojans et les backdoors
- Défendre les services en ligne
- Comment gérer un incident ?
- Conclusion : quel cadre juridique ?

- Sécurité Wifi
- Techniques cryptographiques

L'helpdesk 35 heures

- L'alimentation de la file de tickets
  - Par l'utilisateur dans l'interface
  - Par un technicien
  - Par un collecteurs mail
- Les notifications
  - Les modèles
  - Configuration des envois
- Les SLA
  - Principe
  - Les escalades
- La gestion des tickets
  - Les types de tickets
  - Les notions d'urgence, d'impact et de priorité
  - Les statuts
  - Les suivis
  - Les validations
  - Les attributions
  - Les tâches
  - Les coûts
  - Les solutions
- La base de connaissance
- La FAQ
- Les règles métiers pour les tickets
- Les plannings
- Les statistiques
- Logiciels contrôle à distance

Autres fonctions

- L'administration
- La configuration générale
- La maintenance
- Les journaux
- Les actions automatiques
- Les liens externes
- Les notes
- Les réservations
- Les rapports
- Les plugins
  - Installation
  - Exemple

Anglais : vocabulaire général et informatique 28 heures

- Maîtriser l'emploi : du présent simple, du passé simple, du 'present perfect simple, du futur
- Savoir utiliser les modaux pour : Exprimer la possibilité ou l'impossibilité, la nécessité,
- Manier les chiffres
- Lexique informatique
- Expression orale

Conduite projet 14 heures

travail tutoré – réalisation d'une conduite d'un projet Réseau –

stage pratique – 315 heures

Un stage pratique en entreprise est mis en place pour valider in situ une problématique portant sur les réseaux (analyse, besoins,….) permettant ainsi au stagiaire de mettre en application les savoirs faire étudiés lors de la formation afin de lui permettre la juste restitution dans un mémoire de fin d'études.

Accompagnement emploi - projet professionnel 70 heures

Objectif professionnel du module : Aborder une recherche d'emploi efficace en maîtrisant les nouveaux outils de communication

Stratégie de recherche d'emploi :

- Les incontournables offres d'emploi
- Le réseau et la recherche d'emploi
- Le ciblage et les candidatures spontanées
- Votre visibilité
- Définition d'un plan d'action
- Construction d'outils de planification et de suivi des démarche

Optimiser l'identité numérique

- Mesurer l'intérêt et les limites de l'identité numérique
- Et vous, quelle image sur le Web ?
- Les différents supports de l'image numérique
- Image numérique et candidatures : bonnes et mauvaises pratiques
- Définir sa (nouvelle) stratégie de visibilité sur le Net et choisir ses supports
- Mettre à jour ou créer ses espaces de visibilité sur Internet
- Les réseaux sociaux : (twitter, Viadeo, Linkedin, …, - choisir le bon réseau - les bonnes pratiques, être efficace – soigner son image

Constuire le CV

- Comprendre les enjeux du CV
- Etudier les différentes rubriques d'un CV
- Faire le point sur son CV
- S'enrichir de nouvelles pratiques et explorer de nouvelles pistes
- Faire des choix de contenus et de mise en page
- Modifier ou construire son CV

Rédiger une lettre de motivation

- Quand et pourquoi adresser une lettre de motivations ?
- Décrypter les attentes du recruteur pour plus de cohérence
- La présentation générale d'une lettre de motivations
- Les contenus et les styles : exercices pratiques
- Rédaction de différentes lettres : candidature spontanée et réponse à une offre

Convaincre en entretien d'embauche

- Se préparer à l'entretien
- Mesurer l'impact du « non-verbal »
- Entretien semi-directif, reformulation et construction de réponses concrètes
- Suivre ses candidatures
- Simulations d'entretiens d'embauche
- Simulations jeux de rôle

Réalisation un bilan personnel et professionnel

- Acquérir la méthodologie de bilan
- Repérer les points forts de votre parcours et votre profil
- Identifier ses compétences et ses ressources
- Valoriser l'ensemble de son parcours au travers la réalisation d'un tableau récapitulatif
- Simulations jeux de rôle

Chaque stagiaire termine ce module avec en sa possession, un CV, deux lettres de motivation adaptées à la réponse à une offre et à une candidature spontanée,. une simulation individuelle d'entretien d'embauche et une fiche de suivi de sa propre recherche d'emploi.
Il sera évalué au TOSA « Office » permettant la vérification et la validation des aptitudes à maîtriser les outils et à naviger sur internet mais aussi de sa capacité à utiliser un logiciel de messagerie et d'adopter une attitude pro active de recherche via le digital.