En accueillant un(e) apprenti(e), vous lui transmettez votre savoir-faire, votre expérience. Vous allez lui confier des missions concrètes, en adéquation avec le contenu de sa formation. Définir la mission de l'apprenti(e) est une étape fondamentale pour le bon déroulement de la formation et intervient avant la signature du contrat, avec l'approbation du responsable pédagogique.

Ce guide a été conçu pour vous aider dans cette démarche

Quelques rappels sur la formation...

Intitulé	Licence Professionnelle Qualité Sécurité des Systèmes d'Information
Début	septembre
Lieu	IUT de Blois
Durée	12 mois
Alternance	alternances de 2 à 3 semaines en entreprise et en formation

Pas d'apprentissage sans contrat...

Formulaire	contrat de travail écrit «cerfa FA13» secteur privé/CCI ou «cerfa FA19» secteur public/DIRECCTE
Mentions obligatoires	- signature employeur et apprenti(e) - cachet du CFAIURC
Type	CDD avec période d'essai 2 mois
Début	- au plus tôt 3 mois avant - au plus tard 3 mois après } le début de la formation
Statut	salarié
Horaires	35 h/sem
Congés	5 semaines sur période entreprise
Rémunération	% du SMIC ou du SMC (salaire minimum conventionnel)

Formalités de l'entreprise

. Établissement du contrat de travail
. Désignation du maître d'apprentissage (ou équipe tutorale)
. Déclaration unique d'embauche (URSSAF)
. Programmation de la visite médicale d'embauche
. Déclaration de l'apprenti(e) auprès de la Caisse de Retraite

Les missions que vous pouvez proposer à votre apprenti(e)...

Université	Structure d'accueil	
Connaissances	Applications	Missions
Sécurité des données	- Plan de sauvegarde - Respect de la confidentialité dans les bases de données	- Réalisation de maquettes - Réalisation de sauvegardes / restaurations - Mise en place du chiffrement d'une base
Sécurité des réseaux	- Prévention des attaques - Définition de réseaux robustes	- Réalisation de maquettes - Construction de canaux chiffrés entre composants, VPN - Choix et déploiement de firewalls
Sécurité des systèmes	- Conservation des preuves en vue d'analyse ou d'audits - Protection des accès	- Réalisation de maquettes - Durcissement des OS - Administration de la sécurité logique - Mise en œuvre et sécurisation annuaires - Installation de boitiers sécurisés
Sécurité des applications	- Amélioration de la disponibilité des services fournis - Extension de plage d'utilisation d'application	- Réalisation de maquettes - Réalisation de procédures de tests - Mise en place de clusters - Déploiement d'une solution de partage de données ou de disques - Virtualisation
Qualité des réseaux	- Equilibrage de charge - Accroissement des performances et de la disponibilité du réseau	- Cahier des charges, choix puis installation d'un outil de mesure de QoS - Déploiement de Load Balancers
SI d'entreprise : solution interne, ERP, applications métier	- Etude et réalisation de la sécurisation dans le contexte d'un ERP	- Tests et recette des évolutions - Gestion et suivi de projet, sur les aspects sécurité
Mesures et supervision	- Contrôle et monitoring des infrastructures d'entreprise, des réseaux - Veille de sécurité	- Mise en place d'un système de monitoring tel Nagios, Zabix, etc. - Mise en place d'un processus de suivi et de gestion des correctifs de sécurité (Logiciels Microsoft, Adobe, Cisco, etc.)
Normes, certifications, audits (ISO 9001, ISO 20000)	- Certification d'entreprise ou de service - Passage d'audit - Mise en place de PAQ, de gestion de Qualité	- Participation à un processus de certification : rédaction de procédures - Pilotage de plan d'actions régulières
Gestion des services, ITIL	- Mise en place et gestion des fonctions et processus ITIL (Centre de services, changements, gestion des actifs et configurations, gestion des niveaux de service, catalogue, fournisseurs, etc.)	- Audits internes, cartographies - Pilote d'exploitation en centre de services - Mise en place et/ou maintien de la qualité d'une CMDB (pour une gestion des actifs ou une gestion d'incidents, demandes, etc.) - Rédaction de fiches catalogues
Gestion de la sécurité, ISO 27000	- Mise en place d'un Système de Management de la Sécurité Informatique (pilotage de la sécurité) - Prévention des risques (attaques, piratage) - Plan de continuité d'activité	- Evaluation du taux d'application des règles de sécurité - Mise à jour des politiques de sécurité - Mise en place/maintien en condition opérationnelle de tableaux de bord SSI - Mise en place de contrôles opérationnels sur des process - Tests de plan de secours informatique - Sensibilisation des collaborateurs à la SSI

Secteurs d'activité

- Gestion des Services Informatiques
- Sécurité informatique
- Conseil
- Tout secteur s'appuyant sur les services de l'informatique
  Banques, Assurances, Défense, Santé, Education

Structures d'accueil

- Équipes opérationnelles en :
  SSII, data center, sociétés d'infogérance, etc.
  Banques, assurances, opérateurs de téléphonie, grosses entreprises, etc.
  Administrations (défense, éducation, collectivités locales et territoriales, hospitalières, etc.)
- Toutes entreprises dotées d'un service informatique y compris PME/PMI

Débouchés professionnels

- responsable informatique en PME/PMI
- administrateur réseaux
- administrateur système
- pilote de systèmes de sécurité (détection, prévention, surveillance, supervision, …)
- gestionnaire de parc informatique
- assistant responsable sécurité du système d'information
- gestionnaire de processus (gestion des services)

Qualités acquises côté métier

- Maîtrise des techniques pour :
  Maintenir l'intégrité des données (ACID), leur sauvegarde-restauration
  Protéger les réseaux : VLAN, firewalls, VPN (IPsec, SSL/TLS), IPS et IDS
  Assurer la sécurité système : gestion des accès, LDAP/ Active Directory, durcissement, antivirus
  Mettre en place des solutions de continuité des services (clusters)
  Réaliser le monitoring (métrologie et supervision) et la QoS réseaux
- Bonnes connaissances en :
  Systèmes d'Information d'entreprise
  Gestion de projet, communication, anglais
  Normes : ISO 9001 et ISO 20000
  Gestion des services – ITIL
  Aspects financiers (gestion des services)
  Management de la sécurité – ISO 27000
  Aspects juridiques (sécurité)

Qualités requises côté humain

- Méthode et rigueur
- Bon relationnel
- Ecoute
- Goût du travail en équipe

Avantages financiers

Aides (secteur privé)	Montants	Conditions d'application
Indemnité Compensatrice Forfaitaire	1 000 €	Versement et modalités de calcul incombent aux régions. Majorations possibles sous certaines conditions.
Crédit d'impôt	1 600 €	Barème applicable à toutes entreprises quels que soient son département et sa taille. (sous certaines conditions)

Exonérations des Cotisations Sociales (secteur privé et secteur public)

- Entreprises : effectif jusqu'à 11 salariés
  exonération totale des cotisations patronales et salariales
  (sauf les cotisations d'accident du travail)
- Entreprises : effectif de 11 salariés et +
  exonération totale des cotisations salariales
  exonération partielle des cotisations patronales

–Pour tout calcul précis, veuillez contacter l'URSSAF–

Pour nous joindre

Adresse de la formation
IUT de Blois
15 rue de la Chocolaterie
CS 2903
41000 BLOIS
http://iut-blois.univ-tours.fr/

Secrétariat
02.54.55.21.50
02.54.55.71.85
corinne.legras@univ-tours.fr
www.cfaiurc.fr

Contact : Corinne LEGRAS
Responsable Formation : Béatrice BOUCHOU MARKHOFF

CFAIURC SOUTENU PAR LE CONSEIL RÉGIONAL DE LA RÉGION CENTRE ET LE FSE

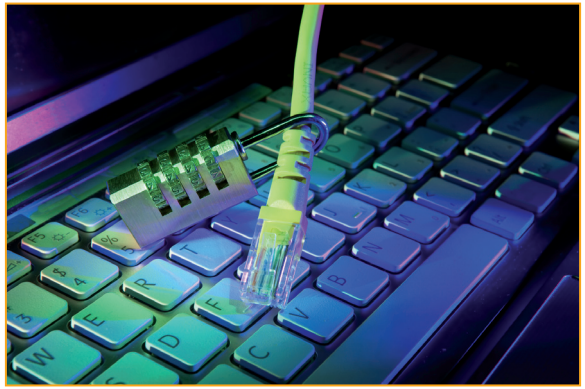
l'Europe s'engage en région Centre avec le FSE
Région Centre
UNE FORMATION UNIVERSITAIRE UNE EXPÉRIENCE PROFESSIONNELLE UN PASSEPORT POUR L'EMPLOI

cfaiurc - mars 2012 - Service communication

LICENCE PROFESSIONNELLE

QUALITÉ - SÉCURITÉ DES SYSTÈMES D'INFORMATION

PAR APPRENTISSAGE



Objectif MISSIONS

IUT BLOIS
CFAIURC Centre de Formation d'Apprentis Inter Universitaire Région Centre
afaq ISO 9001 Qualité AFNOR CERTIFICATION