Programme détaillé de la formation

Administrateur Cyber-sécurité sur base de la Licence (L3) Sciences, technologies, santé,mMention informatique générale (LG02501A)

En délégation avec l'ECAM Strasbourg-Europe

Site de Strasbourg

Le Cnam est habilité à délivrer ce diplôme par arrêté du ministère de l'enseignement supérieur et de la recherche en date du 01 septembre 2019 jusqu'au 31 août 2024

Formation durant le premier semestre 2020 pour une durée totale de 1200 heures stages inclus (450 heures de formation, 750 heures de stage).

▸ Objectif de la formation

Permettre aux stagiaires de mettre à niveau leur expérience et leur formation pour se reconvertir vers le métier d'Administrateur Cybersécurité. Les enjeux de Cybersécurité deviennent de plus en plus critiques pour les entreprises, sujettes à des campagnes de malwares et de vol de données de plus en plus fréquentes.

La formation 'Administrateur Cybersécurité' prépare les stagiaires à la Licence 'Informatique Générale' du CNAM, dans une déclinaison adaptée aux métiers de la Cybersécurité. Elle valide les cinq domaines de compétences nécessaires à l'administration sécurisée d'un système d'information, avec validation d'un diplôme de Licence :

- Fondamentaux de l'informatique
- Industrialisation de la cybersécurité
- Cybersécurité, systèmes et réseaux
- Cybersécurité, données et logiciels
- Communication et entreprise

La formation technique est complétée par un module d'accompagnement vers l'emploi 'Technique de Recherche d'Emploi (TRE)'.

Le diplôme offre une formation générale couvrant les principaux domaines de l'informatique : développement, programmation, réseaux, multimédia, systèmes, architecture des machines, génie logiciel, recherche opérationnelle, systèmes d'informations, systèmes industriels. Il s'adresse plus particulièrement aux salariés du domaine informatique recherchant une valorisation de leur pratique quotidienne en vue d'une promotion ou d'un changement d'employeur, mais il peut accueillir également des salariés d'autres domaines en phase de reconversion.

▸ Public concerné et prérequis

Cette formation est proposée à un public de demandeurs d'emploi.
Les conditions d'accès sont les suivantes :
- être titulaire d'un diplôme de niveau III en informatique (DUT informatique, DPCT informatique, BTS informatique de gestion, diplôme analyste programmeur du Cnam, DUT GEII, certains titres Afpa homologués au niveau III) ou d'un diplôme qui dispense des niveaux L1 et L2.

▸ Compétences visées

Fondamentaux de l'informatique
Industrialisation de la cybersécurité
Cybersécurité, systèmes et réseaux
Cybersécurité, données et logiciels
Communication et entreprise

▸ Métiers

Conception, développement et maintenance en condition opérationnelle d'une architecture de sécurité tenant compte du contexte de l'entreprise, des attentes et besoins des utilisateurs et en veillant aux évolutions technologiques. A l'issu de sa formation, l'auditeur pourra, à titre d'exemple, exercer ses compétences dans le maintien en sécurité du système d'information de son entreprise. Administrateur systèmes et réseaux, Administrateur de bases de données, Technicien/technicienne en production et exploitation de systèmes d'information…

▸ Modalités de réalisation de la formation

La formation s'appuie sur les moyens pédagogiques et techniques suivants : cours en présentiel, cours à distance, travaux pratiques, travaux dirigés, selon une organisation (horaires, lieu de formation, enseignants,..) mise en œuvre par l'ECAM, sous la tutelle pédagogique du Cnam en grand Est dans le cadre des règlements du Conservatoire National des Arts et Métiers.

▸ Lieu de déroulement de la formation et horaires

Les cours auront lieu dans les locaux de l'ECAM Strasbourg au 2 rue de Madrid 67300 Schiltigheim.

La formation a lieu de 09h00 à 12h30 et de 13h30 à 17h00 du lundi au vendredi. L'accès à la salle de formation est possible de 8h45 à 17h45.

▸ Les contenus pédagogiques : vue globale

Intitulé	Code UE	ECTS	Nombre d'heures d'enseignements			
			FFP	TPAE	Évaluation	Total
Outils mathématiques pour l'informatique	UTC501*	3	8	20	2,5	30,5
Système	UTC502*	3	8	20	2,5	30,5
Paradigmes de programmation	UTC503*	3	8	20	2,5	30,5
Systèmes d'information et bases de données	UTC504	3	28	-	2,5	30,5
Introduction à la cyberstructure de l'internet	UTC505	3	28	-	2,5	30,5
Recherche opérationnelle et aide à la décision	RCP101	6	35	-	2,5	37,5
Systèmes d'exploitation : principes, programmation et virtualisation	SMB101	6	35	-	2,5	37,5
Cybersécurité : référentiels, objectifs et déploiement	SEC101	6	42	-	2,5	44,5
Menaces informatiques et codes malveillants : analyse et lutte	SEC102	6	42	-	2,5	44,5
Architectures et bonnes pratiques de la sécurité des réseaux, des systèmes, …	SEC105	6	42	-	2,5	44,5
Anglais professionnel en anglais	ANG300	6	35	-	2,5	37,5
Management de projet	GDN100	4	28	-	2,5	30,5
Techniques de recherche d'emploi	TRE	-	14	-	-	14
Expérience professionnelle (5 mois)	UAAL0T	17	-	-	7	7
	Total	**72**	**353**	**60**	**37**	**450**

**** UTC501, UTC502 et UTC503 dispensées en FOAD par le Cnam en Grand Est sous forme de TPAE et par l'ECAM pour les tutorats sous forme de FFP***

▶ Modalités de validation

Chaque unité d'enseignement de la formation ne peut être validée que si la présence du stagiaire est attestée sur l'ensemble des sessions de formation.

L'atteinte des compétences de la formation est validée par le CNAM.

Deux sessions de contrôle sont associées aux unités d'enseignements. Dans ce cadre l'unité d'enseignement est acquise lorsque l'élève a obtenu la note de 10/20 à l'une des deux sessions. La licence est délivrée à tout auditeur remplissant les conditions suivantes : avoir validé l'ensemble des unités d'enseignements composant la licence et avoir validé 17 crédits au titre de l'expérience professionnelle.

▶ Contenus détaillés des Unités d'Enseignement

❖ UTC501 OUTILS MATHEMATIQUES pour l'informatique

Objectifs pédagogiques : Présenter des notions mathématiques indispensables pour aborder des études d'ingénieur informaticien. L'objectif n'est pas d'étudier ces notions et outils pour eux-mêmes mais de montrer également leur utilité dans l'analyse de problèmes qui se posent en informatique.
Compétences visées : Acquérir des éléments de logique en particulier le mode de raisonnement par déduction ; Maîtriser les notions de relations et d'ordre total et partiel, indispensables pour les questions de structuration de données ; Se réapproprier les notions de base du calcul matriciel et de l'analyse utiles pour la résolution de systèmes linéaires et le traitement du signal ; Acquérir des notions d'arithmétique utiles en informatique, notamment pour la cryptographie ; Comprendre le formalisme des systèmes de transitions pour la description et le contrôle de l'évolution des systèmes informatiques ; Enfin aborder la modélisation de phénomènes aléatoires nécessaire à prendre en compte dans divers contextes comme les réseaux informatiques.
Eléments de contenu : Éléments de logique : proposition, prédicats, validité, satisfiabilité. Les techniques de raisonnement : direct, par cas, par contraposition, par récurrence, par l'absurde. Eléments d'arithmétique : divisibilité, nombres premiers, propriétés du PGCD, algorithme d'Euclide, décomposition en produit de facteurs premiers, arithmétique modulaire, algorithme RSA. Relations et ordres : relations binaires, d'équivalence, ordres partiels et totaux. Calcul matriciel et analyse : résolution de systèmes linéaires, méthode de Gauss, Gauss Jordan et manipulation de séries de Fourier avec l'aide d'un logiciel. Systèmes de transition : traces, exécutions, états accessibles, états récurrents, transitions récurrentes, systèmes de transitions étiquetées, propriétés générales (de sûreté, de vivacité), introduction aux réseaux de Pétri. Processus stochastiques et modélisation : chaînes de Markov à temps discret ; distribution stationnaire, processus de Markov continus ; processus de Poisson ; processus de naissance et de mort ; application aux files d'attente simples.
Modalités de validation : Examen écrit complété éventuellement d'un contrôle continu

❖ UTC502 SYSTEME

Objectifs pédagogiques : Comprendre les principes fondamentaux des systèmes d'exploitation multiprogrammés.
Compétences visées : Appréhender les mécanismes fondamentaux des systèmes d'exploitation
Eléments de contenu : Notions de base sur les systèmes d'exploitation, mise en œuvre de la protection/isolation : notion d'espace d'adressage, de modes d'exécution user/superviseur, introduction des appels système. Gestion des exécutions programmes, processus, ordonnancement, threads Synchronisation Gestion de la mémorisation, mémoire centrale pagination, problèmes de gestion mémoire et d'allocation de blocs de tailles variables Notion de base en administration système, comptes, droits, etc… Gestion des I/O asynchrones et des Ginterruptions.
Modalités de validation : Examen écrit complété éventuellement d'un contrôle continu

❖ UTC503 PARADIGME DE PROGRAMMATION

Objectifs pédagogiques : Connaître et approfondir les principaux paradigmes de programmation : impératif, logique, fonctionnel, réactif, objet ; savoir les mettre en œuvre ; comprendre leurs différences.
Compétences visées : Pouvoir aborder un nouveau langage de programmation ou une nouvelle bibliothèque en reconnaissant les usages dans ceux-ci des principaux paradigmes. La plupart des langages de programmation actuels étant hybrides, et s'ouvrant de plus en plus au paradigme fonctionnel, les connaissances dans un paradigme seront utilisables au-delà de celui-ci.
Eléments de contenu : Paradigme objet, généricité, héritage et polymorphisme, introspection ; paradigme fonctionnel, lambda expressions, clôtures, objets persistants, promesses ; paradigme logique. Divers langages de programmation pourront être abordés, par exemple Java ou C# pour le paradigme objet, Javascript, Scala, Haskell ou Kotlin pour la programmation fonctionnelle, Prolog pour la programmation logique. L'enseignement comprendra un noyau de cours magistraux, mais surtout un volume important de TD/TP. En particulier, on partira d'un problème donné, et on verra comment le résoudre dans les divers paradigmes.
Modalités de validation : Examen écrit complété éventuellement d'un contrôle continu

❖ UTC504 SYSTEME D'INFORMATION ET BASES DE DONNEES

Objectifs pédagogiques : Fournir les bases méthodologiques nécessaires à la conception et à la réalisation des systèmes d'information. Ce cours présentera à travers une étude de cas le processus de développement depuis l'acquisition des besoins jusqu'à la réalisation d'une base de données.
Compétences visées : Recueillir et analyser les besoins

Connaître le cycle de développement des logiciels
Concevoir les MCD et MLD
Concevoir les applications (spécification de la solution et de la structure de la base de données)

Eléments de contenu :

Introduction aux systèmes d'information et bases de données

Présentation du processus de développement d'un système d'information (traditionnel et agile)

Bases de données et leur conception

A travers une étude cas, développer les étapes d'analyse et de conception d'une application en utilisant une méthode orientée objet (UML et processus unifié)

- Capture et analyse des besoins
- Conception de l'application
- Spécification détaillée
- Implémentation de la base de données

Concepts abordés : MERISE, Notation UML : diagramme de cas d'utilisation, Conception d'une base de données relationnelle, normalisation.

Modalités de validation : Examen écrit complété éventuellement d'un contrôle continu

❖ UTC505 INTRODUCTION A LA CYBERSTRUCTURE DE L'INTERNET

Objectifs pédagogiques :

L'objectif de l'UE est d'introduire la problématique de la conception des réseaux, de leur architecture et des propriétés de sécurité de base.

Compétences visées :

Connaissances associées aux concepts fondamentaux des réseaux de données, protocoles Internet et liaison de données de type LAN essentiellement, architectures en couches du Modèle OSI ou Internet. L'auditeur pourra, à l'issue du cours, évaluer les principales contraintes réseaux et leur impact sur une application client/serveur ou distribuée.

L'auditeur sera en mesure de lire une proposition commerciale et être capable de chercher les informations clefs pour la comprendre et l'explorer plus en détail, de participer à la définition des principaux éléments d'un cahier des charges fonctionnels à destination d'une maîtrise d'ouvrage dont l'objectif est d'urbaniser une application distribuée. L'auditeur disposera de repères pour évaluer fonctionnellement une livraison d'équipements réseaux, et mettre en place une procédure de recette de ceux-ci dans un cadre applicatif.

Eléments de contenu :

Diviser pour régner (modèle OSI) : Découverte de l'architecture de communication en couches. Du modèle OSI à l'architecture Internet; introduction aux protocoles http, DNS et à l'outil d'analyse de traces Wireshark.
Les autoroutes de l'information : nids de poules et travaux en tous genres (couche physique). Concepts et problèmes de la transmission de données : erreurs de transmission, le contrôle d'erreur, notion de bande passante, traitement des signaux, atténuation, modulation, multiplexage, commutation, synchronisation d'horloge, problèmes de caractère et de bit stuffing.
Collectivisme ou Libre entreprise… à la recherche d'un modèle équitable (sous-couche MAC). Grandes familles de protocoles à compétition et à coopération, détail sur CSMA/CD et CSMA/CA en mode infrastructure. Ponts et commutation.
Croisements et Destination (couche réseau). Adressage, tables de routage et l'expédition de données dans le réseau IP. Evolution de IPv4 à IPv6.
Une lettre ou un appel ? (couche transport). Transport de données entre un client et un serveur à travers UDP et TCP avec le modèle datagramme, et les approches connecté et non connecté. Gestion et utilisation de l'API socket.
Où sont les clefs ? (Introduction à la sécurité). Aspects sécurité de base pour la confidentialité, l'intégrité, l'authentification et la notarisation : principes de cryptographie symétrique et asymétrique, fonctions de hachage cryptographique.

Modalités de validation : Examen écrit complété éventuellement d'un contrôle continu

❖ RCP101 RECHERCHE OPERATIONNELLE ET AIDE A LA DECISION

Objectifs pédagogiques :

Présenter des notions de recherche opérationnelle et d'aide à la décision indispensables pour de futurs ingénieurs, décideurs, responsables de projets.

Compétences visées :

Aptitude à modéliser des problèmes issus de l'Entreprise. Assimilation de méthodes et d'algorithmes fondamentaux en recherche opérationnelle et aide à la décision (en particulier pour l'optimisation de programmes linéaires).
Notions de fiabilité et de sûreté de fonctionnement.

Eléments de contenu :

GRAPHES ET ORDONNANCEMENTS EN GESTION DE PROJETS
Rappels des concepts élémentaires de théorie des graphes. Problème du chemin de valeur optimale entre deux sommets. Ordonnancement de projets : méthodes PERT et MPM (chemin critique, marges).
Traitement des contraintes cumulatives (budget).
PROGRAMMATION LINEAIRE ET APPLICATIONS
Généralités : origine, domaines d'application, pertinence.
Introduction géométrique puis algébrique à l'algorithme du simplexe.
Problème de la base initiale. Dualité. Analyse en sensibilité (paramétrages).
ANALYSE MULTICRITERE
Méthodologie : modélisation d'un problème de décision ; concept de critères, approches monocritère et multicritère. Méthodes de surclassement : méthodes ELECTRE, "Goal-programming" et liens avec la programmation linéaire.
ELEMENTS DE THÉORIE DES FILES D'ATTENTE ET DE SÛRETÉ DE FONCTIONNEMENT
Loi de Poisson, loi exponentielle. Processus de MARKOV : processus de naissance et de mort.
Présentation des files d'attentes, classification de Kendall, File d'attente M/M/1 et applications.

Modalités de validation : Examen écrit + éventuel projet

❖ SMB101 SYSTEMES D'EXPLOITATION : PRINCIPES, PROGRAMMATION ET VIRTUALISATION

Objectifs pédagogiques :

Ce cours a pour objectif de présenter les concepts des systèmes d'exploitation et leur programmation en étudiant les mécanismes de base des systèmes d'exploitation classiques mais aussi ceux des systèmes temps réel, des systèmes embarqués et des objets connectés. Les principes de virtualisation des systèmes d'exploitation sont aussi abordés dans ce cours.

Compétences visées :

Conception et programmation de tout type de système d'exploitation (système classique comme Linux, système temps réel, système embarqué pour objets connectés).

Architecture et fonctionnement des systèmes d'exploitation tels que Unix et Linux mais aussi des systèmes embarqués (comme par exemple Raspberry pi, Arduino, STM32, ou Android) et des systèmes temps réel (dans le domaine de l'avionique, des automobiles, etc.) pour maîtriser leur administration et le développement d'applications.

Maîtrise des principes sous-jacents à la virtualisation de systèmes afin de faciliter l'intégration et l'administration de ce type de service dans un système informatique (Cloud Computing, Haute Disponibilité, Tolérance aux pannes, etc.).

Eléments de contenu :

Concepts et paradigmes des systèmes d'exploitation classiques :
Mécanismes de mise en œuvre des primitives dans le noyau de systèmes tels que Linux ou Unix BSD : notion de processus, de thread, parallélisme et synchronisation, ordonnancement, gestion de la mémoire virtuelle, gestion des signaux, etc…
Concepts et paradigmes des systèmes temps réel :

Architecture, notion de tâche périodique et apériodique, gestion des interruptions, politiques d'ordonnancement temps réel, gestion des handlers, etc.
Concepts et paradigmes des systèmes embarqués et objets connectés :
Etude de quelques exemples microcontrôleurs
Programmation d'un système embarqué et d'un objet connecté
Principes de l'internet des objets
Concepts et principes de la virtualisation de systèmes et de la conteneurisation :
Etude des différentes techniques mises en œuvre dans les hyperviseurs logiciels (VMWare, Xen, KVM).Support matériel de la virtualisation de systèmes.
Etude du support de la virtualisation intégré dans les architectures matérielles récentes : processeurs Intel-VT, mécanismes de Direct I/Os, fonctions PCI virtuelles.
Etude des principes de la conteneurisation et de l'orchestration des conteneurs (exemple de Docker containers et Kubernetes).

Modalités de validation : Examen écrit + éventuel projet

❖ SEC101 CYBERSECURITE : REFERENTIELS, OBJECTIFS ET DEPLOIEMENT

Objectifs pédagogiques :

Savoir mener, argumenter et déployer une politique de sécurité informatique dans une entreprise en lien avec une analyse de risque.

Compétences visées :

Comprendre les enjeux d'une politique et de sécurité informatique cybersécurité et appliquer des méthodologies efficaces d'aguerrissement

Comprendre les différentes situations d'incident

Savoir mettre en place une gouvernance efficace dans le domaine de la cybersécurité

Savoir auditer, conseiller, accompagner le changement

Savoir mener et intégrer des solutions de sécurité suite à l'analyse de risque

Eléments de contenu :

Principaux enjeux de la sécurité pour la société numérique [VL2]
Présentation de l'écosystème : principales parties prenantes, la sécurité et les métiers (OIV, industrie, santé , finances,...)
L'identité numérique (vie privée,..)
L'intelligence économique, géopolitique : principales menaces, bonnes pratiques,...)
Panorama des obligations normatives, réglementaires et juridiques (RGS, Homologation ANSSI, LPM, ISO, CNIL, CLUSIF, etc.)
La continuité d'activité :[VL3]
Le SI (SSIV,SSI ,...)
Système de gestion de la sécurité de l'information (ISMS, ISO 2700
L'incident de sécurité,
Cycle de vie d'un incident de sécurité : veille (évitement, protection), alertes, détection et réponse (traitement, confinement, acceptation),
La réponse à incident (procédures, escalade,...)
Organisation de la sécurité et de ses métiers dans l'entreprise :
Acteurs et responsabilités : externes (clients, fournisseurs, assurances,...) , internes (employés, prestataires,...)
Acteurs internes et RSSI : DSI, RH, DAF, marketing,
Gouvernance de la sécurité : espaces normatifs (ISO 27001, ISO 22301, ISO 27035)
Implémentation de la sécurité
Volet organisationnel : L'analyse du risque, (panorama des méthodes)
De l'analyse de risque à la PSSI et schéma de sécurité,
Approfondissement d'une méthode d'analyse de risque en vue de l'élaboration d'une fiche FEROS pour l'homologation d'un SI,
Déploiement : projets de sécurité, produits et services.
Maintien en condition de sécurité, le RSSI et les SECOPS : définition des procédures opérationnelles, ...

Modalités de validation : Examen écrit + éventuel projet

❖ SEC102 CYBERSECURITE : MENACES INFORMATIQUES ET CODES MALVEILLANTS : ANALYSE ET LUTTE

Objectifs pédagogiques :

Être capable de faire de la remédiation adaptée aux contextes de menace.

Compétences visées :

Phase de veille : comprendre les modes d'action pour prévoir les effets
Phase d'alerte : Détecter les effets des codes malveillants
Phase de réponse : minimiser, stopper ou réduire l'impact du code malveillant

Eléments de contenu :

Typologies des codes et des effets : Virus, worm, botnet, etc.
Études des modes d'action des codes malveillants : analyse intrinsèque des codes malveillants, anatomies d'attaques type, à partir d'exemples réels.
Lutte contre le code malveillant- veille, alertes, détection des effets des codes, identification de la menace.
Caractérisation des effets, Impacts techniques, économiques, fonctionnels.
Réduction des effets, limitation des impacts techniques et fonctionnels.
Analyse postmortem (forensic)
Méthodologies de réponses à incidents
Audits

Modalités de validation : Examen écrit + éventuel projet/mémoire

❖ SEC105 ARCHITECTURE ET BONNES PRATIQUES DE LA SECURITE DES RESEAUX, DES SYSTEMES, DES DONNEES ET DES APPLICATIONS

Objectifs pédagogiques :

Ce cours présente les principaux aspects de la sécurité des réseaux. Il présente les problèmes généraux de sécurité (confidentialité, intégrité, authentification, protection, non répudiation) et les solutions types connues pour ces problèmes. Il présente la mise en œuvre de ces solutions dans l'architecture Internet

Compétences visées :

Pouvoir mettre en œuvre ces solutions dans l'architecture Internet.

Eléments de contenu :

Protection de l'accès aux données et protection des interfaces dans les systèmes
Protection dans les réseaux
Cryptographie
Protocoles de sécurité dans les réseaux
Mise en œuvre des protocoles de sécurité

Modalités de validation : Examen écrit + éventuel projet

❖ ANG300 ANGLAIS PROFESSIONNEL

Objectifs pédagogiques :

Communiquer en anglais à l'oral et à l'écrit dans des situations professionnelles. Exemples : se présenter professionnellement, accueillir un visiteur, communiquer au téléphone, participer à une réunion, gérer des rendez-vous ou des commandes, lire des documents sur l'activité de l'entreprise, analyser des offres d'emploi, rédiger des e-mails, parler de son travail et de son entreprise.

Compétences visées :

Développement de compétences de compréhension, d'expression et d'interaction.
Les compétences visées sont celles définies dans la grille du CECRL (Cadre Européen Commun de Référence pour les Langues).

Eléments de contenu :

Les contenus seront adaptés par l'enseignant en fonction du niveau du groupe.
La compréhension de l'écrit et de l'oral, l'expression à l'écrit et à l'oral, l'interaction à l'oral, la grammaire et le lexique de l'anglais de l'entreprise et du monde professionnel seront travaillés à partir de situations de communication. Le travail pourra être individuel ou collectif et pourra s'appuyer sur des activités en mode collaboratif entre des élèves regroupés en petits groupes.
A titre indicatif, les thèmes suivants pourront être abordés : informations personnelles et professionnelles, les tâches professionnelles quotidiennes, relations avec les collègues et les clients, voyager, santé, acheter et vendre, produits et services, résultats et accomplissement, …

Modalités de validation : Évaluation orale et écrite

❖ GDN100 MANAGEMENT DE PROJET

Objectifs pédagogiques :

D'une part de fournir aux auditeurs les bases du management de projet et les grilles de lecture nécessaires à leur compréhension, qu'il s'agisse de l'organisation des projets, des outils de gestion de projet ou de leur rôle dans la stratégie ;
D'autre part d'amener les auditeurs à réfléchir sur le domaine de pertinence de ces modèles et outils, à leurs avantages/inconvénients ou encore aux spécificités sectorielles. L'objectif est ici de permettre la prise de distance indispensable à un management de projet efficace.

Compétences visées :

Savoir gérer un projet, compétence transverse
Compréhension des enjeux du management de projet
Grilles de lectures de l'organisation des projets et des forces/faiblesses des différents types d'organisation selon la nature des projets
Connaissance des spécificités du travail en projet et des bonnes pratiques en matière de gestion des équipes projets
Principes de fonctionnement, intérêt et limites des principaux outils de gestion

Eléments de contenu :

Les projets : définition et enjeux pour l'entreprise

Les grands modèles d'organisation des projets

Le management des équipes projet

Les outils de pilotage des projets (gestion du temps et des coûts)

L'intégration des partenaires dans les projets

Introduction au management multi-projets : portefeuille, plateforme, lignées

Perspectives du management de projet

Modalités de validation :
Examen et rédaction d'un mémoire d'une trentaine de pages sur un projet auquel l'étudiant a participé dans son activité professionnelle ou sur un cas réel à choisir en accord avec l'enseignant.

❖ TRE Techniques de recherche d'emploi

Objectifs pédagogiques :
Par l'exercice de recherche d'emploi (de la définition de son projet jusqu'à la préparation à l'entretien), l'auditeur sera amené à comprendre les enjeux du recrutement. Au terme de cet enseignement, il sera capable de définir son projet professionnel à court terme, actualiser et marqueter son CV et sa LM pour être en cohérence avec sa cible de poste recherché, comprendre les enjeux et mobiliser les méthodes de prospection adéquates, comprendre les méthodes de recrutement pour pouvoir mieux s'y préparer.