

Master en Systèmes et réseaux - Option Sécurité de l'information

Langue principale d'enseignement :

Français Anglais Arabe

Campus où le programme est proposé : CST

OBJECTIFS

Le Master en systèmes et réseaux - option sécurité de l'information vise à former des professionnels qualifiés ayant des compétences scientifiques et pratiques solides dans le domaine de la sécurité de l'information et capables de prendre en charge la protection des systèmes d'information complexes sur le marché local et international.

COMPÉTENCES

- Comprendre le fonctionnement de l'environnement numérique complexe de l'entreprise sur le plan de l'infrastructure, des systèmes, des applications et des données
- Analyser les risques de sécurité d'un système, d'un réseau ou d'une application
- Concevoir des politiques de sécurité en conformité avec les standards internationaux
- Implémenter et évaluer les mécanismes de sécurisation
- Collecter, enquêter et traiter efficacement les preuves numériques établies sur une scène de crime
- Comprendre les enjeux juridiques et éthiques liés à la sécurisation des systèmes d'information.

EXIGENCES DU PROGRAMME

UE obligatoires (112 crédits), UE optionnelles Institutions (8 crédits)

UE obligatoires (112 crédits)

Administration UNIX (6 Cr.). Architecture et gestion des réseaux (6 Cr.). Communications unifiées (4 Cr.). Cryptographie et applications sécurisées (4 Cr.). Cryptographie et Sécurité Informatique Avancées (6 Cr.). Digital forensics and incident management (4 Cr.). Gestion des risques (2 Cr.). Gouvernance des systèmes d'information (2 Cr.). Information security standards and best practices (4 Cr.). Information systems administration and security (2 Cr.). Introduction to entrepreneurship (2 Cr.). Modélisation et optimisation des réseaux (6 Cr.). Nouvelles technologies pour réseaux IP (6 Cr.). Piratage éthique (4 Cr.). Projet 1 (6 Cr.). Réseaux d'entreprise sécurisé (4 Cr.). Réseaux sans fil (6 Cr.). Sécurité des infrastructures réseaux (4 Cr.). Stage professionnel (30 Cr.). Windows system administration (4 Cr.).

UE optionnelles Institution de spécialisation (8 crédits)

8 crédits à choisir parmi les 18 crédits offerts.

Big Data (4 Cr.). Blockchain (4 Cr.). Droit informatique (2 Cr.). Innovation's management and design (4 Cr.). Gestion de projets (2 Cr.). Software defined data center (2 Cr.).

PLAN D'ÉTUDES PROPOSÉ

Semestre 1

Code	Intitulé de l'UE	Crédits
026ADUNM1	Administration UNIX	6
026AGREM1	Architecture et gestion des réseaux	6
026GOSIM1	Gouvernance des systèmes d'information	2
026MOREM1	Modélisation et optimisation des réseaux	6
026REFIM2	Réseaux sans fil	6
026WSADM1	Windows System Administration	4
	Total	30

Semestre 2 Obligatoires

Code	Intitulé de l'UE	Crédits
026COUNM2	Communications unifiées	4
026CRASM2	Cryptographie et applications sécurisées	4
026GEPRM2	Introduction to Entrepreneurship	2
026NTIPM1	Nouvelles technologies pour réseaux IP	6
026PRJ1M2	Projet 1	6
026SDDCM2	Software Defined Data Center	2
026BIGDM2 / 026BLCHM2 / 026INDTM2	Big Data / Blockchain / Innovation's Management and Design	4
026DRINM2 / 026INENM2	Droit informatique / Gestion de projets	2
	Total	30

Semestre 3

Code	Intitulé de l'UE	Crédits
026DIFOM3	Digital Forensics and Incident Management	4
026GERIM3	Gestion des risques	2
026ISSPM3	Information Security - Standards and Best Practices	4
026ISASM3	Information Systems Administration and Security	2
026PIETM3	Piratage éthique	4
026CSIAM3	Cryptographie et sécurité informatique avancées	6
026REESM3	Réseaux d'entreprise sécurisé	4
026SEREM3	Sécurité des infrastructures réseaux	4
	Total	30

Semestre 4

Code	Intitulé de l'UE	Crédits
026STAGM4	Stage professionnel	30
	Total	30

DESCRIPTIFS DES UE

026ADUNM1 Administration UNIX 6 Cr.

Cette UE offre une initiation aux techniques d'administration et de sécurité d'un réseau de stations de travail ayant Unix pour système d'exploitation. Elle couvre les thèmes suivants : Administration locale : rôle d'un administrateur - Démarrage et arrêt - Ouverture d'une session - Gestion des utilisateurs - Gestion des processus - Gestion du disque - Sauvegarde et Compression - Gestion des imprimantes - Tâches périodiques - Fichiers de trace. Administration d'un réseau des stations Unix : Configuration d'un serveur réseau - Outils de base - DNS - NIS - NFS et Automount - Mail - Serveur Web et Proxy - DHCP - PPP - Sécurité - Optimisation et paramétrage. Systèmes d'exploitation de confiance (Trusted Solaris, SELinux).

026AGREM1	Architecture et gestion des réseaux	6 Cr.
------------------	--	--------------

Cette UE introduit l'architecture des réseaux de communications et les concepts de base relatifs. Elle couvre les thèmes suivants : Rappel sur le modèle OSI et les fonctionnalités de chaque couche - Rappel sur les technologies niveau 2 et 3 utilisé dans les réseaux LAN, MAN et WAN (Ethernet/VLAN - WiFi – Frame Relay - ATM - IP - VPN, etc.) - Architecture des réseaux d'entreprise au niveau LAN et WAN - Architectures des unités d'interfonctionnement - Techniques d'interconnexion au niveau 2 et aux niveaux supérieurs - Évolution des réseaux vers le large bande - Réseaux Gigabit – Techniques de gestion de la bande passante - Architecture des centres de données - Réseaux de stockage - Contrôle d'accès et le filtrage réseau - les zones de sécurité - Problématique de la gestion des réseaux - Syntaxe abstraite et codage des données de gestion - Protocoles CMIS/CMIP et SNMP - Structure des informations de gestion (SMI) - MIB standards et RMON.

026BIGDM2	Big Data	4 Cr.
------------------	-----------------	--------------

Cette UE présente les différents aspects théoriques et pratiques pour la gestion des données massives : calcul distribué avec MapReduce et HDFS, analyse des liens dans les graphes, PageRank, recherche des ensembles et sous-ensembles similaires, identification des communautés dans les graphes, Traitement des flots de données, les systèmes de recommandation et de classification, détection des ensembles séparables (clustering).

026BLCHM2	Blockchain	4 Cr.
------------------	-------------------	--------------

This course delves into the fast-evolving realm of blockchain technology, showcasing its versatility beyond the realm of Fintech. Through this course, students gain a comprehensive understanding of blockchain and its practical applications, covering distributed ledger technology, bitcoins, keys and addresses, wallets, transactions, advanced transaction methods, the Bitcoin network, blockchain mining and consensus, business applications, cryptocurrency, Ethereum, smart contracts, decentralized applications, blockchain applications outside finance, Hyperledger, other distributed ledger technologies, advanced blockchain topics, and blockchain security.

026COUNM2	Communications unifiées	4 Cr.
------------------	--------------------------------	--------------

Ce cours couvre les standards de compression audio et vidéo qui constituent la partie majeure des flux multimédia, ainsi que les protocoles de transmission et de contrôle de ces flux. Le tout couronné par trois applications majeures : la téléphonie IP, la visioconférence et la diffusion vidéo (vidéo streaming).

026CRASM2	Cryptographie et applications sécurisées	4 Cr.
------------------	---	--------------

Cette UE offre les connaissances nécessaires pour la sécurisation de l'information en utilisant la cryptographie. Elle couvre les thèmes suivants : Services, mécanismes et techniques de sécurité - Algorithmes symétriques, asymétriques et Hash - Certificats - Mécanismes d'authentification, non-répudiation, confidentialité, intégrité et échanges de clés - Cartes à puces.

026CSIAM3	Cryptographie et sécurité informatique avancées	6 Cr.
------------------	--	--------------

Cette UE couvre les thèmes suivants : Définition de la cryptographie, terminologie de base, attaques de base - Différence entre les schémas asymétriques et symétriques - Schémas de cryptage importants et célèbres (RSA, AES) - Fonctions de hachage et MAC - Technologie Cloud : définition, importance et défis - Chiffrement homomorphe : définition, importance et propriétés - Schémas de cryptage homomorphes bien symétriques (MORE, PORE et Domingo Ferrer) - Schémas de cryptage homomorphes asymétriques bien connus (RSA, Paillier, DGHV) - Introduction à la cryptographie basée sur les réseaux et à l'apprentissage avec erreurs - Brakerski, Gentry et Vaikuntanathan (BGV) : schéma de cryptage homomorphe asymétrique bien connu - Définition de l'IoT et enjeux de sécurité - Types d'attaques et de menaces - Courbe elliptique pour la sécurité IoT - Sécurité de la couche liaison (IEEE 802.15.4) - Sécurité de la couche réseau IoT (IPSec) - Sécurité intégrée pour l'Internet des objets - La loi libanaise 81/2018 : relative aux transactions électroniques et aux données personnelles - Le Règlement général sur la protection des données (RGPD) - Gestion des cyber-crisis - Projets : Le cours contient deux projets, le premier est un projet technique où les étudiants doivent passer plusieurs semaines à concevoir un modèle de sécurité du système d'information en utilisant différentes connaissances enseignées dans ce cours (par exemple : une

application de vote électronique sécurisée utilisant HE et Technologie Blockchain, mise en œuvre matérielle d'un scénario ou d'une application IoT sécurisée). Quant au deuxième projet, les étudiants passeront la dernière semaine du semestre à enquêter sur l'un des sujets énumérés ci-dessus et liés aux réglementations, lois et politiques.

026DIFOM3	Digital Forensics and Incident Management	4 Cr.
------------------	--	--------------

This course explores digital forensics and incident management, encompassing the collection, analysis, and presentation of digital data and events for legal admissibility. It aids in detecting and preventing digital and cyber-crime, as well as resolving disputes involving digitally stored evidence. Digital forensics applies computer investigation and analysis techniques to uncover potential legal evidence in various forms of computer misuse, including hacking, intellectual property theft, and fraud. Topics covered include: the investigation process, relevant laws, seizing digital evidence, types of digital evidence, rules of evidence, examination processes, electronic crime considerations by category, roles of first responders, securing electronic crime scenes, conducting interviews, documenting scenes, evidence collection and preservation, packaging and transport, incident investigation (e.g., hacking, e-fraud, data leakage), and log capturing techniques and tools for digital evidence management.

026DRINM2	Droit informatique	2 Cr.
------------------	---------------------------	--------------

Ce cours expose les thèmes primordiaux et les problématiques essentielles de la législation de nos jours, en proposant une échelle de comparaison entre le Liban et les lois Européennes. Il couvre ce qui suit : Contexte et notions générales - Actualité juridique au Liban - Où sommes-nous par rapport à l'Europe? - La propriété intellectuelle au service des créations informatiques - Les contrats – Négociation et élaboration - La protection juridique et le droit pénal face à la criminalité informatique - Signature électronique, enjeux et application - La CNIL, pourquoi et comment ? - Perspectives du droit informatique pour les années à venir.

026INENM2	Gestion de projets	2 Cr.
------------------	---------------------------	--------------

Cette UE permet aux étudiants de connaître les différentes phases d'un projet qui sont indispensables pour la bonne gestion de ce dernier. Ces phases se résument en : la planification, le développement du schedule et le contrôle. De plus, plusieurs notions de management seront abordées dans ce cours et qui sont reconnues comme étant les meilleures pratiques managériales pour la réussite d'un Project Manager. Cette UE couvre les thèmes suivants : Introduction au Project Management - Planification d'un projet - Schedule du projet - Ressources humaines du projet - Management de la communication - Coût du projet - Contrôle du projet.

026GERIM3	Gestion des risques	2 Cr.
------------------	----------------------------	--------------

Cette UE a pour objectif de présenter la gestion des risques de sécurité des systèmes d'information afin de sensibiliser à la gestion des risques, savoir que la gestion des risques est maîtrisable, comprendre qu'il existe des méthodes pour analyser les risques et appréhender la mise en place d'un plan de gestion des risques. Elle couvre les thèmes suivants : Concept de la gestion des risques - Processus de gestion des risques - Bonnes pratiques pour la gestion des risques - Principes de gestion des risques du SI - Culture et communication – Dépendance avec la stratégie et objectifs métiers - Identification du risque - Scenarios de risques – Sensibilisation au niveau gestion des risques - Notions de " capacity, appetite, tolerance " - Différentes phases d'évaluation des risques - Méthodes d'analyse des risques - Définition et mise en œuvre des solutions - Contrôle des risques.

026GOSIM1	Gouvernance des systèmes d'information	2 Cr.
------------------	---	--------------

Comment améliorer l'efficacité et la productivité des entreprises ? Comment aligner les technologies de l'Information aux enjeux du métier de l'organisation ? Comment rentabiliser les investissements informatiques ? Comment piloter les évolutions des systèmes d'information ? Cette UE répond à l'ensemble de ces questions en présentant une démarche d'amélioration continue de production informatique, enrichie par des retours d'expérience et des références du marché européen. Cette UE couvre la gouvernance des SI : Concept, enjeux, bonnes pratiques - Processus, méthodes et outils - ITIL : vue d'ensemble et organisation, vue détaillée sur la démarche d'industrialisation des environnements, implémentation pratique des processus, infrastructures et outils au sein des entreprises – COBIT : structure, domaines et processus, application concrète et complémentarité

avec les autres standards (ITIL, CMMI, et autres) – Intégration de la gouvernance des SI dans l’approche globale de la sécurité d’entreprise - Gouvernance des SI : analyse et réflexions sur la pérennité et sur l’évolution.

026ISSPM3	Information Security - Standards and Best Practices	4 Cr.
------------------	--	--------------

Cette UE aborde l’initiation aux concepts clés de sécurité et d’analyse du risque, les différentes normes de sécurité informatique, les meilleures pratiques, les standards et les directives, le standard ISO 27001-2 2013, le PCI DSS, l’OWASP, SANS-CIS top 20 contrôles de cyber sécurité. Ce cours couvre les domaines suivants : politique et procédures de sécurité, sécurité des ressources humaines, sécurité physique et logique des systèmes et réseaux, gestion des incidents et gestion des plans de continuité des affaires.

026INDTM2	Innovation Management and Design	4 Cr.
------------------	---	--------------

This course on innovation management and design is essential in today’s fast-paced and complex world, particularly for professionals in engineering. It emphasizes the leader’s role as both an innovator and a facilitator of innovation. Students will develop fundamental skills in innovation and creative problem-solving, with a focus on finding innovative solutions to everyday social challenges. Innovation involves the practical transformation of ideas into new products, services, processes, systems, and social interactions, generating added value that satisfies various stakeholders and drives sustainable growth while enhancing quality of life and fostering a sustainable society. Innovation extends beyond technology to encompass all dimensions of the economy and society. Originating in the 1980s at Stanford University, the concept of innovation, inspired by designers, architects, and artists, centers on the needs of users and employs tools such as observation, inquiry, experimentation, and visual thinking to understand and communicate ideas effectively. While often associated with product design, innovation and design thinking are applicable to a wide range of problem-solving contexts, including business modeling and process improvement.

026GEPRM2	Introduction to Entrepreneurship	2 Cr.
------------------	---	--------------

This course introduces entrepreneurship fundamentals including innovation, ideation, and strategy. It explores the DNA canvas, encompassing design, needs, and aspirations, as well as visualizing business through the Business Model Canvas. Additionally, it delves into understanding the entrepreneurial environment and identity within the Lebanese ecosystem, covering legal registration and business identity such as SAL and SARL. The curriculum also includes digital entrepreneurship topics like e-commerce and virtual marketplaces, along with payment gateways. Furthermore, it examines the pricing strategies crucial for the sustainability and scalability of entrepreneurial ventures, concluding with insights into export opportunities.

026MOREM1	Modélisation et optimisation des réseaux	6 Cr.
------------------	---	--------------

Dimensionner et analyser la topologie et les performances des réseaux en utilisant les outils de modélisation mathématique de la théorie des graphes, de la recherche opérationnelle et des processus stochastique. Cette UE introduit les fondements de la modélisation et le dimensionnement des réseaux en utilisant plusieurs outils théoriques comme les graphes, la recherche opérationnelle et les files d’attente. Elle couvre les bases de la théorie des graphes, la représentation et le parcours des graphes, les problèmes classiques de la théorie des graphes comme l’arbre couvrant de poids minimal, le plus court chemin et les réseaux de transport, la manipulation et l’analyse des réseaux utilisant des bibliothèques logicielles pour les graphes. L’UE introduit aussi la théorie de télétrafic, l’utilisation des probabilités pour la modélisation du multiplexage et du trafic, les chaînes de Markov et leur application aux réseaux, les processus d’arrivées, les files d’attente de type M/M, et leurs applications, l’optimisation et les programmes linéaires, les outils de résolution numérique des problèmes d’optimisation.

026NTIPM1	Nouvelles technologies pour réseaux IP	6 Cr.
------------------	---	--------------

Cette UE permet d’analyser l’interconnexion des réseaux dans l’Internet et l’évolution des protocoles. Elle couvre l’interconnexion des systèmes autonomes, les accords de transit et de peering, le point d’échange Internet, les principes du routage externe, le protocole BGP, les stratégies de routage BGP, la sécurité de routage dans l’Internet, l’architecture MPLS - VPN MPLS, l’ingénierie de trafic, la transition vers IPv6, l’auto-configuration IPv6 et l’application double pile.

026PIETM3	Piratage éthique	4 Cr.
------------------	-------------------------	--------------

Ce cours apprend à identifier des faiblesses dans le réseau en utilisant les mêmes méthodes que les "hackers" : prise d'empreintes, énumération, exploitation et escalade de privilèges. Les étudiants apprendront également les contre-mesures à prendre, telles que les correctifs, pour atténuer les risques. Cette UE couvre les thèmes suivants : Classes des pirates - Anatomie d'une attaque - Test d'intrusion – Reconnaissance passive – Balayage : découverte des machines actives, balayage des ports, détection des systèmes d'exploitation, test de vulnérabilités - Craquage des mots de passe - Énumération – Attaque système : gagner l'accès, post-attaque - Attaques réseaux : les attaques par déni de service, le reniflement du réseau, l'usurpation d'identité - Attaque sur les applications Web – Ingénierie sociale.

026PRJ1M2	Projet 1	6 Cr.
------------------	-----------------	--------------

Projet pour la mise en application des connaissances acquises en 1^{re} année de Master.

026REESM3	Réseaux d'entreprise sécurisé	4 Cr.
------------------	--------------------------------------	--------------

Cette UE permet de maîtriser le fonctionnement et le déploiement d'un réseau d'entreprise sécurisé. Elle couvre : Différentes technologies des pare-feux : filtrage de paquets, filtrage applicatif (proxy), filtrage dynamique, filtrage de sessions - Analyse du contenu : lutte contre les SPAMs, protection contre les virus - Systèmes de détection d'intrusion - Rappel sur l'architecture des réseaux d'entreprise - choix des technologies et dimensionnement des équipements de sécurisation : l'authentification centralisée, le SSO, contrôle d'accès, NAC, les zones de sécurité, UTM, VPN (L2TP, IPsec, SSL) - Meilleur emplacement des différents dispositifs de sécurité - Travaux pratiques : mise en place d'un pare-feu dans un réseau avec écriture des règles - Scan de ports avant et après la mise en place du pare-feu - IDS – Mise en œuvre du proxy squid - Mise en œuvre de serveurs VPN - Étude de cas.

026REFIM2	Réseaux sans fil	6 Cr.
------------------	-------------------------	--------------

Cette UE introduit les principes de la communication radio, l'accès multiple Aloha et CSMA, les normes IEEE 802.11 et IEEE 802.15.4, les réseaux mobiles 3G, 4G et 5G et leur sécurité. Durant les séances pratiques les étudiants mettront en place différentes configurations de réseaux Wi-Fi. Les aspects suivants seront abordés : SSID - Association - Répéteur - Analyseur – Redondance - VLAN - Routage – NAT- Sécurité.

026SEREM3	Sécurité des infrastructures réseaux	4 Cr.
------------------	---	--------------

Cette UE introduit les techniques de sécurité offertes par les équipements réseaux. Elle couvre la sécurité offerte par les équipements réseaux du marché : Hub, commutateur, routeur, pare-feu, translation d'adresses - Spécificités de la sécurité Intranet - Sécurité téléphonie classique/PABX - Sécurité des réseaux radio-mobile, sans fils, multimédia sur IP - Disponibilité du réseau: fonctions de redondance, protection physique et/ou logique contre les attaques - Offres de services à partir des VPNs - Travaux pratiques : filtrage sur les routeurs - Mise en œuvre d'un VPN IPsec entre routeurs.

026SDDCM2	Software-Defined Data Center	2 Cr.
------------------	-------------------------------------	--------------

This course explains extending virtualization benefits across data center infrastructure components (networking, processing, storage) for improved service provisioning efficiency, availability, and security. It covers Traditional Data center technologies, Cloud computing, and Virtualization (Concepts, Models, Technologies, Security), including Systems virtualization, Storage virtualization, Network virtualization, Virtual network devices, and SDN, along with Converged and Hyper-Converged Infrastructures.

026STAGM4	Stage professionnel	30 Cr.
------------------	----------------------------	---------------

Stage professionnel de 4 mois dans une entreprise sur un thème lié à la sécurité.



o26WSADM1

Windows System Administration

4 Cr.

This course delves into Microsoft Windows architecture and hones the skills needed to manage a Microsoft Windows Server effectively. Through hands-on experience with the products and tools, participants gain proficiency in server features, roles, and services. It covers fundamental concepts such as PC and Server hardware architecture, Operating System, and Networking, as well as advanced topics including:

- Windows Server architecture
- Installation and Configuration
- Configuring Network Services (DHCP, DNS, Routing, Remote Access, VPN)
- Backup and Recovery
- Security and Identity Management (Active Directory, Group Policy Management, Certificate Services, Federated Services, Network Access Control and Policy Management, Server Hardening)
- Virtualization (Hyper-V)
- Overview of the Microsoft Ecosystem
- Setting up a Web presence using Internet Information Services (IIS): Web Site (HTTP, HTTPS), FTP, SMTP