Co-funded by the
Erasmus+ Programme
of the European Union

lmpi
licence master professionnel
en protection informatique

LMPI - Licence, Master professionnels pour le développement, l'administration, la gestion, la protection des systèmes et réseaux informatiques dans les entreprises en Moldavie, au Kazakhstan, au Vietnam

Project N° 573901-EPP-1-2016-1-IT-EPPKA2-CBHE-JP

Fiches métier LICENCE et MASTER
MOLDAVIE

Co-funded by the Erasmus+ Programme of the European Union

lmpi licence master professionnel en protection informatique

Licence, Master professionnels pour le développement, l'administration, la gestion, la protection des systèmes et réseaux informatiques dans les entreprises en Moldavie, au Kazakhstan, au Vietnam/LMPI

Project N° 573901-EPP-1-2016-1-IT-EPPKA2-CBHE-JP

Fiche métier: Expert en sécurité informatique – MOLDAVIE (Master)

Intitulé du métier	Expert en sécurité informatique Analyste de la sécurité de l'information
Mission	La mission principale de l'expert en sécurité informatique est d'assurer la protection des données. Il doit mettre en échec les tentatives d'intrusion des pirates informatiques. Pour cela, il évalue le niveau de vulnérabilité du system et établit des solutions pour le sécuriser. Il peut être épaulé dans sa mission par des "hackers éthiques": ces professionnels de l'intrusion l'aident à déceler les failles.
Secteur professionnel	Toutes les entreprises où les systèmes d'information sont utilisés. Un diplôme de niveau master est le minimum requis pour pouvoir postuler au poste *Expert en sécurité informatique* ou *Analyste de la sécurité de l'information*. Le choix se fait alors entre des masters professionnels universitaires dans le secteur de l'informatique (sécurité des systèmes d'information, management de la sécurité des systèmes industriels et des systèmes d'information, etc.) L'expert en cybersécurité est rattaché au RSSI (Responsable de la Sécurité des Systèmes Informatiques) qui lui-même est généralement rattaché au Directeur Général ou au directeur informatique, selon la taille de l'entreprise. L'expert en cybersécurité intervient sur l'ensemble du réseau en relation avec les différentes directions ou services. Ses fonctions s'exercent dans le domaine de la sécurité des réseaux, des serveurs, l'ensemble des domaines des systèmes d'information.
Conditions d'accès	Baccalauréat en Informatique, Sécurité de l'information, Technologie de l'information, Génie logiciel, Systèmes d'information, Réseaux des ordinateurs, Gestion de bases de données, Gestion de l'information…
Activités et tâches professionnelles	Protéger les données et la fiabilité du système informatique d'une entreprise, telle est la mission qui incombe à l'expert en sécurité informatique. Pour cela, l'expert en sécurité informatique est amené à réaliser un diagnostic du système d'information d'une entreprise dans le but de déceler les éventuels points faibles; apporter différentes solutions de protection pour sécuriser les informations et les données d'une entreprise; mettre en place les différents processus de sécurité;

garantir la pérennité des systèmes de sécurité; actualiser les systèmes de sécurité en fonction des nouvelles menaces et des dernières technologies.

Activités 1 **Administrer les accès au réseau et aux données**

Tâches

Analyser:

- Le fonctionnement de l'ensemble de l'entreprise
- Les besoins d'accès aux informations et au réseau de chaque service

Qualifier la typologie des contributeurs en fonction des accès autorisés:

- Contribution
- Validation
- Administration

Activités 2 **Contrer les intrusions et les virus**

Tâches

Eviter piratages, vols, destruction de données:

- Achat de pare-feu, d'antivirus
- Mise en place de tunnels sécurisés
- Utilisation de la cryptographie

S'assurer de l'emploi des logiciels de protection par les salariés:

- Indicateurs de suivi ·
- Mécanismes d'alerte ·
- Analyse des logs

Mener des audits: ·

- Recensement des points faibles ·
- Rédaction des rapports ·
- Mise à jour des systèmes de protection ·
- Évolution de la structure du réseau

Activités 3 **Mettre en place les processus de sécurité**

Tâches

Assurer: ·

- Efficacité des sauvegardes ·
- Bon niveau de sécurité des serveurs ·
- Revue et validation des architectures en lien avec les services techniques

Créer des alertes: ·

- Notification de mise à jour ·
- Programmation d'échéance

Mettre en place les processus adaptés: ·

- Sauvegarde des données sur plusieurs serveurs ·
- Externalisation des données

	Lutter contre: · • La sortie d'information de l'entreprise · • Les importations de données potentiellement dangereuses *Activités 4* **Assurer la continuité de l'activité** *Tâches* Définir avec les différents services le plan de reprise d'activité en cas de: • Sinistre (incendie, inondation) · • Mouvement social (grèves des transports, occupation des locaux) · • Acte malveillant (sabotage, terrorisme) Assurer la continuité de l'activité d'un point de vue technique: · • Back up des serveurs · • Accès aux logiciels clés pour l'activité · • Locaux adaptés Assurer la continuité de l'activité d'un point de vue humain: · • Recenser les métiers et les postes clés · • Mettre en place des back up · • Informer les personnes *Activités 5* **Sensibiliser les utilisateurs aux risques** *Tâches* *Activités 6* *Effectuer une veille technologique* *Tâches* Identifier les évolutions nécessaires des réseaux et des systèmes de sécurité: • Adaptations et ajustements • Modifications • Sécurité • Fonctionnalités et services Anticiper les risques: • Adaptation et formation • Renouvellement «Benchmarke » les réseaux: • Bonnes pratiques • Références
Compétences génériques	Exécution responsable des tâches professionnelles, dans des conditions restreintes et avec une assistance qualifiée CT1. Appliquer les principes, les normes et les valeurs de l'éthique professionnelle Se familiariser avec les rôles et les tâches spécifiques au travail d'équipe et la répartition des tâches pour les niveaux subordonnés

	CT2. Identifier, décrire et animer les activités organisées en équipe avec le développement des capacités de communication et de collaboration, ainsi qu'assumer les différents rôles (exécution et leadership) Sensibilisation au besoin de formation continue l'utilisation efficace des ressources et des techniques d'apprentissage pour le développement personnel et professionnel CT3. Démontrer l'esprit d'initiative et d'action pour mettre à jour votre propre culture professionnelle, économique et organisationnelle *Savoir être* Sens de la communication vis-à-vis de différents publics: • Diplomatie • Adaptabilité • Souplesse • Force de persuasion • Curiosité d'esprit • Vif intérêt pour les nouvelles technologies et leurs enjeux Sens pédagogique : • Goût pour l'échange • Aptitude à la communication vis à vis des utilisateurs variés • Capacité de vulgarisation des enjeux et des risques Gestion du Stress: • Excellente gestion des situations d'urgence • Hiérarchisation pertinente des priorités Intégrité prouvée: • «Hacker éthique» (il cherche et repère les failles du système pour mieux les contrer); • Respect de la confidentialité • Rigueur Sens de l'engagement : • Implication et motivation • Goût pour le travail en équipe • Charisme et entraînement • Force de proposition
Compétences spécifiques (professionnelle)	**C1. Les fondements scientifiques et techniques de la SI** C1.1 Identifier et définir les concepts, théories et méthodes de soutien aux sciences fondamentales et appliquées pour l'ingénierie de la sécurité de l'information C1.2 Expliquer les solutions d'ingénierie en utilisant les techniques, concepts et principes des sciences exactes et appliquées C1.3 Résoudre des problèmes dans les activités humaines en appliquant

	notamment des techniques et des méthodes de protection C1.4 Choisir les critères et les méthodes pour analyser les avantages et les inconvénients des méthodes et procédures appliquées pour résoudre les problèmes de sécurité C1.5 Modélisation de problèmes typiques en sciences appliquées à l'aide d'un instrument mathématique **C2 Les aspects organisationnels et informationnels de la SI:** C2.1 Identifier et définir les concepts, théories et méthodes utilisés pour effectuer des analyses axées sur la protection des personnes et des informations sur les systèmes opérant au niveau des organisations. C2.2 Expliquer les concepts, théories et méthodes utilisés dans l'analyse des systèmes fonctionnant au niveau organisations C2.3 Application de concepts, de théories et de méthodes de base pour la préparation des informations nécessaires au développement de systèmes de sécurité opérant au niveau des organisations C2.4 Choisir les critères et les méthodes d'évaluation de la qualité, des performances et des limites des systèmes de sécurité en fonction des besoins de l'organisation, y compris ceux requis pour définir un système de gestion de la qualité et de la sécurité C2.5 Elaboration d'un projet (spécification du système) dans les conditions d'un système de gestion de la qualité et de la sécurité. **C3 Les mesures de sécurité et de contrôle** C3.1 Identifier et définir les concepts, procédures et méthodes de sécurité de l'information utilisés pour effectuer les mesures de contrôle découlant des besoins de l'activité humaine C3.2 Expliquer les bonnes technologies pour mettre en œuvre les systèmes de sécurité requis dans les activités des organisations C3.3 Utilisation des technologies modernes dans la définition de solutions de sécurité C3.4 Utilisation de critères et de méthodes basés sur la technologie pour évaluer la conformité aux normes d'interopérabilité C3.5 Développement de mesures de contrôle et de sécurité utilisant des technologies modernes pour la transmission, le stockage et le traitement des données en fonction des besoins d'une organisation **C4 Les méthodes et technologies pour développer des solutions de sécurité** C4.1 Identification et définition de concepts et de méthodes axés sur le développement, la mise en œuvre et l'utilisation de solutions de sécurité C4.2 Explication des concepts et méthodes utilisés pour

	élaborer, mettre en œuvre et utiliser des mesures de contrôle et de sécurité C4.3 Application des langages de programmation, environnements de modélisation et de développement, méthodologies de création de systèmes de sécurité C4.4 Utilisation de critères et de méthodes pour évaluer le processus de développement de systèmes de sécurité en termes de qualité et de performance C4.5 Développement et implémentation de logiciels de sécurité pour des problèmes concrets dans divers domaines de l'activité humaine **C5 L'architecture de sécurité et l'infrastructure** C5.1 Identification et définition du matériel architectural, des logiciels et des composants de communication, ainsi que de ceux qui sont nécessaires pour décrire une infrastructure de protection C5.2 Expliquer l'interaction et le fonctionnement des composants architecturaux et de sécurité C5.3 Application de méthodes de base pour spécifier des solutions architecturales et d'infrastructure pour des problèmes de sécurité typiques C5.4 Utilisation de critères et de méthodes pour évaluer les caractéristiques fonctionnelles et non fonctionnelles des composants du système de sécurité C5.5 Mise en place d'une solution architecturale et d'infrastructure basée sur les contraintes imposées par les projets de sécurité *Savoir faire* Pratique et expérience rédactionnelle: • Actualités/brèves • Articles de fond • Dossiers Maîtrise expérimentée «terrain» de l'outil informatique: • Architecture des systèmes et réseaux • Procédures d'exploitation et des standards d'échange des données employées • Procédures de Sécurité Informatique • Systèmes d'exploitation (Solaris, Linux) et des langages de programmation associés Maîtriser les outils bureautiques: • Traitement de texte, tableur, outil de présentation Utilisation de logiciels spécifiques: • Outils de chiffrement de disques durs ou de serveurs • Pare feu (Firewalls) • Outils d'identification Maîtrise de l'anglais courant:

	• Ecrit • Oral
Connaissances nécessaires	*Savoirs* Connaissance de: • L'entreprise • Ses services/produits • Sa structure • Son organisation • Son environnement juridique Vision globale et complète des systèmes d'information • De l'entreprise • Des organisations similaires Connaissance technique approfondie des: • Concepts et techniques d'architecture des systèmes et réseaux · • Procédures d'exploitation et des standards d'échange des données employées • Procédures de Sécurité Informatique • Systèmes d'exploitation et langages de programmation associés • Bases de données
A sortir	Des connaissances approfondies des systèmes de sécurité informatique, un très large panel de connaissances informatiques (cryptologie, pare-feu, limitation des accès au réseau) et surtout régulièrement mises à jour. Esprit de synthèse et vision d'ensemble d'un système. Extrêmement réactif tout en étant capable de réagir très rapidement à un problème de sécurité, être pédagogue et un très bon communicant pour entretenir de bonnes relations de travail avec ses collaborateurs.
Observations	

Co-funded by the Erasmus+ Programme of the European Union

licence master professionnel en protection informatique

Licence, Master professionnels pour le développement, l'administration, la gestion, la protection des systèmes et réseaux informatiques dans les entreprises en Moldavie, au Kazakhstan, au Vietnam/LMPI

Project N° 573901-EPP-1-2016-1-IT-EPPKA2-CBHE-JP

Fiche métier: Expert en sécurité informatique – MOLDAVIE (Licence)

Intitulé du métier	Responsable de la sécurité des systèmes d'information (RSSI) Ingénieur sécurité
Secteur professionnel	Toutes les entreprises où les systèmes d'information sont utilisés
Conditions d'accès	Lycée ou collège
Activités professionnelles	Le RSSI est chargé de la définition et de la mise en œuvre de la politique de sécurité de l'entreprise. Il s'agira de garantir la disponibilité, la confidentialité et l'intégrité du système d'information et des données. Cela passe par l'analyse des risques, et la mise en place de solutions qui permettent de s'assurer du niveau de sécurité requis. Ensuite, l'audit et le contrôle des solutions de sécurité sur un rythme défini doivent permettre d'assurer l'adéquation de la politique de sécurité choisie avec l'évolution des techniques et des pratiques. L'autre domaine d'activité du RSSI va consister à sensibiliser les collaborateurs de l'entreprise aux enjeux de sécurité. Cela permettra d'éduquer aux pratiques de sécurité, et par là même de parvenir à un niveau de sécurité satisfaisant pour l'ensemble de la structure. Les actions de sensibilisation et de formation seront les outils adéquats pour réaliser cette mission. Le RSSI se devra d'informer, de conseiller et d'alerter la direction générale et les fonctions sur les enjeux de la sécurité du SI, et ce dans une perspective métier. Pour ce faire, un travail de veille technologique et légale doit être réalisé pour prendre en compte les évolutions du cadre d'action du RSSI. La réalisation de ces activités s'effectue dans le cadre d'un travail d'équipe. C'est pourquoi il ne faut pas négliger la dimension managériale du poste, avec un encadrement d'ingénieurs et de techniciens d'exploitation qui ne lui seront pas nécessairement directement rattachés, mais seront plus sous la responsabilité directe du Département Sécurité de l'Information.

Compétences génériques	Exécution responsable des tâches professionnelles, dans des conditions restreintes et avec une assistance qualifiée CT1. Appliquer les principes, les normes et les valeurs de l'éthique professionnelle Se familiariser avec les rôles et les tâches spécifiques au travail d'équipe et la répartition des tâches pour les niveaux subordonnés CT2. Identifier, décrire et animer les activités organisées en équipe avec le développement des capacités de communication et de collaboration, ainsi qu'assumer les différents rôles (exécution et leadership) Sensibilisation au besoin de formation continue l'utilisation efficace des ressources et des techniques d'apprentissage pour le développement personnel et professionnel CT3. Démontrer l'esprit d'initiative et d'action pour mettre à jour votre propre culture professionnelle, économique et organisationnelle Réparties en savoir, savoir-faire
Compétences spécifiques (professionnelle)	**Compétences techniques.** Réseaux, systèmes, et sécurité globale des systèmes d'information. **Le cadre réglementaire**, la formation, la communication: connaissances en droit, en pédagogie, en communication d'entreprise, en techniques de management et de gestion de projet. **Qualités humaines et savoir-être.** Sens de l'écoute, rigueur de l'analyse, sang-froid dans les moments clés de prise de décision, capacités d'anticipation et d'analyse. **C1. Les fondements scientifiques et techniques de la SI** C1.1 Identifier et définir les concepts, théories et méthodes de soutien aux sciences fondamentales et appliquées pour l'ingénierie de la sécurité de l'information C1.2 Expliquer les solutions d'ingénierie en utilisant les techniques, concepts et principes des sciences exactes et appliquées C1.3 Résoudre des problèmes dans les activités humaines en appliquant notamment des techniques et des méthodes de protection C1.4 Choisir les critères et les méthodes pour analyser les avantages et les inconvénients des méthodes et procédures appliquées pour résoudre les problèmes de sécurité C1.5 Modélisation de problèmes typiques en sciences appliquées à l'aide d'un instrument mathématique **C2 Les aspects organisationnels et informationnels de la SI:**

	C2.1 Identifier et définir les concepts, théories et méthodes utilisés pour effectuer des analyses axées sur la protection des personnes et des informations sur les systèmes opérant au niveau des organisations. C2.2 Expliquer les concepts, théories et méthodes utilisés dans l'analyse des systèmes fonctionnant au niveau organisations C2.3 Application de concepts, de théories et de méthodes de base pour la préparation des informations nécessaires au développement de systèmes de sécurité opérant au niveau des organisations C2.4 Choisir les critères et les méthodes d'évaluation de la qualité, des performances et des limites des systèmes de sécurité en fonction des besoins de l'organisation, y compris ceux requis pour définir un système de gestion de la qualité et de la sécurité C2.5 Elaboration d'un projet (spécification du système) dans les conditions d'un système de gestion de la qualité et de la sécurité. **Savoir-faire** **C3 Les mesures de sécurité et de contrôle** C3.1 Identifier et définir les concepts, procédures et méthodes de sécurité de l'information utilisés pour effectuer les mesures de contrôle découlant des besoins de l'activité humaine C3.2 Expliquer les bonnes technologies pour mettre en œuvre les systèmes de sécurité requis dans les activités des organisations C3.3 Utilisation des technologies modernes dans la définition de solutions de sécurité C3.4 Utilisation de critères et de méthodes basés sur la technologie pour évaluer la conformité aux normes d'interopérabilité C3.5 Développement de mesures de contrôle et de sécurité utilisant des technologies modernes pour la transmission, le stockage et le traitement des données en fonction des besoins d'une organisation **C4 Les méthodes et technologies pour développer des solutions de sécurité** C4.1 Identification et définition de concepts et de méthodes axés sur le développement, la mise en œuvre et l'utilisation de solutions de sécurité C4.2 Explication des concepts et méthodes utilisés pour élaborer, mettre en œuvre et utiliser des mesures de contrôle et de sécurité C4.3 Application des langages de programmation, environnements de modélisation et de développement, méthodologies de création de systèmes de sécurité C4.4 Utilisation de critères et de méthodes pour évaluer le processus de

	développement de systèmes de sécurité en termes de qualité et de performance C4.5 Développement et implémentation de logiciels de sécurité pour des problèmes concrets dans divers domaines de l'activité humaine **C5 L'architecture de sécurité et l'infrastructure** C5.1 Identification et définition du matériel architectural, des logiciels et des composants de communication, ainsi que de ceux qui sont nécessaires pour décrire une infrastructure de protection C5.2 Expliquer l'interaction et le fonctionnement des composants architecturaux et de sécurité C5.3 Application de méthodes de base pour spécifier des solutions architecturales et d'infrastructure pour des problèmes de sécurité typiques C5.4 Utilisation de critères et de méthodes pour évaluer les caractéristiques fonctionnelles et non fonctionnelles des composants du système de sécurité C5.5 Mise en place d'une solution architecturale et d'infrastructure basée sur les contraintes imposées par les projets de sécurité Lister les compétences spécifiques (propres) au métier Réparties en savoir, savoir-faire
Connaissances nécessaires	Lister les domaines de savoirs dans lesquels doivent être formés tant les étudiants à l'université que les salariés en poste sur ces métiers
Observations	Autres commentaires pouvant guider la définition du «profil de sortie».