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

Enquête d'identification des métiers cibles et des besoins de formation en sécurité informatique

MOLDOVA

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Content

1. Introduction
2. Méthodologie utilisée
3. Analyse des données collectées
4. Conclusions

1. Introduction

Le rapport est fait conformément aux exigences de la méthodologie GIP FIPAG (Méthodologie pour «Enquête d'identification des métiers cibles et des besoins de formation dans le champ de la sécurité informatique en Moldavie»).

Le projet Erasmus + LMPI vise à contribuer à renforcer la sécurité des systèmes et des réseaux informatiques des entreprises moldaves en améliorant la formation professionnelle (initiale et continue, face à face ou à distance) des ressources humaines dans le domaine ainsi que les compétences des citoyens.

Les objectifs du projet sont:

• Surmonter le déficit de compétences dans la conception et le maintenance de la sécurité des systèmes et des réseaux informatiques des entreprises, améliorer l'employabilité des étudiants et profesionnaliser les employés dans ce domaine.

• Professionnaliser des programmes d'enseignement universitaire dans le développement, l'administration, la gestion et la protection des systèmes et des réseaux informatiques conformément au processus de Bologne et au cadre européen des certifications et à leur délocalisation vers les entreprises.

• Créer deux nouveaux programmes d'enseignement accessibles en IDD (Open E- Learning) pour développer et protéger les applications, les systèmes et les réseaux informatiques dans des entreprises adaptées à leurs besoins:

- au cycle I - Licence pour l'administration et la gestion des systèmes et des réseaux informatiques;
- au cycle II - Master professionnel dans l'administration et la gestion des systèmes et des réseaux informatiques dans les entreprises;

• Former au moins 270 étudiants en première année sur ces deux nouveaux programmes d'enseignement (180 en première année de licence et 90 en première année de master);

• Perfectionner 8 enseignants en UE, digitaliser les cours et les ressources pédagogiques;

• Créer un parcours modulaire tout au long de la vie dans le même domaine d'enseignement et former 50 professionnels.

• Créer 1 pôle d'excellence à UTM, un centre de ressources à l'appui de la nouvelle offre.

• Rédiger le programme et contenus des cours, y compris les ressources numériques à mettre à disposition en IDD

Le projet contient 10 lots de travail.

Pour répondre aux recommandations du processus de la Bologne sur la professionnalisation des programmes d'enseignement universitaire, en prenant en compte la correspondance entre les matières enseignés et les compétences requises par la profession, dans le deuxième lot du projet il est prévu d'élaborer un questionnaire et lancer une enquête en ce qui concerne cette profession.

Étant donné le fait que toutes les compétences et les connaissances que l'étudiant doit maîtriser à la fin du programme de formation, pour que l'étudiant puisse s'engager dans la profession donnée, les données recueillies dans le cadre de l'enquête doivent permettre l'étude des besoins des compétences génériques et spécifiques en entreprises (fiche métier), besoins de formation qui se traduiront par une spécialisation de licence et master. Ainsi, le questonnaire doit permettre:

- identifier les professions à couvrir par les nouveaux programmes d'enseignement universitaire;
- identifier les compétences nécésaires pour ces professions;
- identifier les besoins de formation requis par ces professions.

2. La méthodologie utilisée

Pour l'enquête on a utilisé le questionnaire présenté à l'annexe. Il a été élaboré par la coordonnatrice du projet, Anne Delaballe, avec la participation des représentants de toutes les universités participantes dans le projet LMPI. Le questionnaire a été placé sur l'Internet dans Microsoft Forms accessible en ligne à
https://forms.office.com/Pages/AnalysisPage.aspx?id=SB9tG5OIiUi9vx-4QbyuRvrWeCotU1pMtYzOZpQGFBtUQVk5NlRRUzROVDQ0UUI1NFQ1S0dTTlc4UC4u&AnalyzerToken=3lexxkdmDW4d4OZ8mqg6gR2p2WIZgNd4

Il contient 23 questions, la dernière se référant aux coordonnées. On y trouve:

• 9 questions à choix unique à sélectionner: 1, 2, 4, 5, 16, 18, 20-22;

• 10 questions avec plusieurs options possibles à sélectionner: 6-15;

• 4 questions ouvertes: 3, 17, 19 et 23.

Pour mieux s'orienter, une liste de 711 entreprises a été créée: 11 banques; 153 entreprises, dont l'activité centrale est l'informatique, et 547 compagnies fournissant des services de communications électroniques. La demande de compléter le questionnaire par les spécialistes dans le domaine ou en relation avec a été faite:

• par l'intermédiaire de l'Agence nationale de régulation dans les communications électroniques et la technologie de l'information (directeur adjoint Serghei Pocaznoi);

• par demandes personnelles des participants au projet (par e-mail, téléphone, etc.).

Période de l'enquête: du 10 juillet au 31 octobre 2017.

3. Analyse des données collectées

Le questionnaire a été complété par 199 personnes. Selon l'opinion de l'ancien président du conseil d'administration de l'Association nationale des entreprises TIC en Moldavie, M. Veaceslav Cunev, c'est le seul cas dans la pratique moldave où un questionnaire sur le terrain a été rempli par un si grand nombre de personnes.

Dans l'annexe 1, les options des questions 6-15 et 21 sont présentées non dans l'ordre de leur affichage dans le questionnaire original soumis aux répondants pour l'achèvement, mais dans l'ordre de diminution du nombre de leurs sélections par les répondants. Cela facilite la détermination des préférences des répondants.

Les résultats obtenus montrent le suivant (selon les questions).

1. La grande majorité des répondants ont jusqu'à 40 ans (82,9%), plus de la moitié ayant jusqu'à 30 ans (53,8%).

2. Plus d'un tiers des répondants sont des ingénieurs ou des gestionnaires dans le domaine (37,2%). La plupart sont chefs d'entreprise (5,5%).

3. Plus de 81% des répondants (162) ont brièvement décrit leurs tâches de service systématisées dans le tableau 3.1. Ceux-ci sont classés en fonction du nombre de répondants.

Tableau 3.1 Tâches de service de 81% des participants à l'enquête

ID	Tâches de service	No répondants
1.	Développement, maintenance et administration d'applications et de sites Web	18
2.	Conception d'applications et des systèmes informatiques	13
3.	Gestion de la sécurité informatique, y compris: surveillance des logiciels malveillants, identification des vulnérabilités et des risques de sécurité, prévention des incidents informatiques	11
4.	Audit et conseil en TI et sécurité de l'information	9
5.	Mise en place et administration des réseaux informatiques	9
6.	Directeur TI	9
7.	Enseigner des cours travaux pratiques, recherche scientifique	9
8.	Développeurs back-end	8
9.	Prévention, identification et lutte contre la cybercriminalité	8
10.	Conception et administration des bases de données	7
11.	Développement et maintenance des applications	6
12.	Développeurs Java	6
13.	Recherche en informatique	4
14.	Services de soutien aux TIC	4
15.	Surveillance Internet	3
16.	Test d'applications informatiques	3
17.	Gestion des systèmes informatiques	2
18.	Collection et analyse de données sur la cybercriminalité et les crimes connexes	2
19.	Luttee contre la fraude avec des moyens de paiement électroniques	2
20.	Utilisation d'applications informatiques dans la conception de bâtiments	2
21.	Etudiant	2

22.	Support technique et opérationnel pour les dispositifs de cybercriminalité	1
23.	Tester les moyens et schémas des transactions électroniques	1
24.	Autres	34

On peut noter que la troisième position est «Gestion de la sécurité de l'information» (11 répondants), suivie par «Audit et conseil informatique et sécurité de l'information» (9 répondants), «Prévention, identification et lutte contre la cybercriminalité» (8 répondants) etc.

4. Nous nous sommes heureux que plus de 58% des répondants (116) ont une expérience informatique professionnelle.

5. Près de 23% des répondants viennent des entreprises avec plus de 500 employés, et les entreprises de 51 à 100 employés représentent 41%.

En résumant l'information sur l'échantillon des répondants au sondage obtenue en réponse aux questions 1 à 5, on peut dire qu'il s'agit d'un échantillon représentatif.

6. Les répondants croient que les spécialistes de la sécurité informatique travaillent principalement dans: les banques (73,9%); de services informatiques et sociétés de consultants (72,9%); télécommunications (72,4%); unités militaires (60,3%), mais aussi en général dans toutes les entreprises assistées par l'ordinateur (54,8%).

7. Le plus grand besoin de spécialistes en sécurité informatique se trouve dans: les banques (72,4%); dans toutes les entreprises équipées d'ordinateurs (70,9%); télécommunications (66,8%); services informatiques et sociétés de consultants (64,3%); unités militaires (60,8%); administration publique (56,3%); grandes entreprises (56,3%).

8. Comme activités de base, ce que les spécialistes de la sécurité informatique doivent être capables de faire, sont sélectionnées les 12 activités explicitement spécifiées à la question 8 (plus de 66,8%), en particulier les activités telles que:

1) Détection fréquente, détection des vulnérabilités du système (86,4%);

2) Mise en place des systèmes de détection, prévention et détection des intrusions (80,9%);

3) Rapport, analyse et prédiction des attaques de sécurité (78,4%);

4) Surveillance du réseau et du système, réponse aux incidents (77,4%);

5) Mise en œuvre du codage des informations, authentification et construction de l'infrastructure PKI (73,9%).

L'option 13 «Autres activités» a été sélectionnée par seulement 5,5% des répondants.

9. Les problèmes rencontrés dans l'entreprise concernant la sécurité informatique comprennent:

1) Faible niveau de connaissance de l'ensemble du personnel, de la direction, non seulement des enseignants en informatique sur l'importance de la sécurité de l'information (50,8%);

2) Problèmes de confidentialité de l'information (48,2%);

3) Stratégie de gestion des risques adéquate n'est pas encore faite (36.7);

4) Difficultés (temps, argent, personnel) dans la mise en œuvre et l'application des politiques de sécurité au sein de l'entreprise) (35,2%);

5) Problème de disponibilité de l'information (34,7%);

6) Problème de modification de l'information (34,2%).

7) Difficultés rencontrées lors de la mise en place des processus de sécurité conformément à la norme ISO 17799 (27,6%) et ainsi de suite.

10. Comme outils utilisés pour la sécurité informatique (logiciels et matériels) par les agents économiques, toutes les 9 options explicitement spécifiées à la question 10 ont été sélectionné (plus de 35,2% des répondants), ayant mentionné des outils comme:

1) Accès contrôlé (71,9% des répondants);
2) Outils de protection software (70,4%);
3) Contrer les virus et programmes malveillants (69,8%);
4) Encryptage des données (56,8%);
5) Outils de protection hardware (hardware) (50,8%);
6) Obstacle physique (49,2%).

11. De ces 15 compétences génériques, qui pourront être nécéssaires à un spécialiste dans la sécurité informatique, spécifiés dans le questionnaire, la moins sélectionnée est «Conception et gestion de projets» (31,2% des répondants), même si le pourcentage reste élevé. Les plus nécessaires sont considérées:

1) Capacité d'analyse et de synthèse (82,9% des répondants);
2) Capacité de vulgarisation des enjeux et des risques (77,4%);
3) Capacité de gérer les situations d'urgence (74,4%);
4) Travail en équipe (61,8%);
5) Capacité d'organisation et de planification (57,3%);
6) Souci de la qualité (54,8%);
7) Efficacité (53,3%);
8) Créativité (51,3%).

12. Les enseignements de formation, qui peuvent permêtre d'acquérir les compétences génériques nécéssaires à un spécialiste dans la sécurité informatique sont pris en compte (tous les six spécifiés dans le questionnaire):

1) Stages pratiques (91,0% des répondants);
2) Techniques (80,4%);
3) Théoriques (76,4%);
4) Etudes de cas (73,9%);
5) Travail en équipe (61,3%);
6) Enseignements en ligne (37,2%).

Notez que l'option "Autres" n'a pas été sélectionnée que par 5,0% des répondants.

13. Comme compétences spécifiques nécéssaires à un spécialiste dans la sécurité informatique, toutes les 19 spécifiées dans le questionnaire ont été sélectionné, la moins sélectionnée étant "Faire évoluer les réseaux" (39,7% des répondants), bien que le pourcentage reste élevé. Les plus nécessaires sont:

1) Mettre en place les différents processus de sécurité (83,9% des répondants);
2) Réaliser un diagnostic du système d'information (80,9%);
3) Apporter différentes solutions de protection (74,9%);
4) Connaître le Firewall (74,4%);
5) Maîtriser les protocoles de sécurité (73,4%);
6) Maîtriser les VPN (72,9%);
7) Recenser les points faibles (72,9%);

8) Maîtriser la cryptologie (67,3%).

L'option «Autre» a été sélectionnée par seulement 3,5% des répondants.

14. Au niveau des unités de contenu des disciplines, pour acquérir les compétences spécifiques nécéssaires à un spécialiste dans la sécurité informatique, il s'agit de:

1) Politique de sécurité (77,9% des répondants);
2) Langues modernes (Anglais) (76,9%);
3) Administration de services réseaux (73,9%);
4) Administration système (71,9%);
5) Dispositifs et équipements de sécurité (VPN, Firewall, etc.) (70,4%);
6) Supervision et management de Réseaux (68,8%);
7) Cryptographie (68,8%);
8) Wireless et sécurité (67,3%);
9) Sécurisation de serveur et de l'e-mail des clients (65,8%);
10) Méthodologie de la mise en place d'une PSSI (60,8%);
11 Audit/Pentesting réseau (60,8%);
12) Sécurité de la couche application LSA (Layer Security Application) (57,8%);
13) Configuration des routeurs (51,3%).

15. Modalités de formation d'enseignement à privilégier afin d'acquérir des compétences spécifiques nécessaires à un spécialiste dans la sécurité informatique, sont (toutes les six spécifiées dans le questionnaire):

1) Stages pratiques (87,4% des répondants);
2) Techniques (78,4%);
3) Théoriques (72,4%);
4) Etudes de cas (70,4%);
5) Travail en équipe (63,3%);
6) Enseignements numériques (45,7%).

L'option «Autres» a été sélectionnée par seulement 3,0% des répondants. Il est à noter que l'ordre coïncide avec celle de la modalité de formation, ce qui permettrait d'obtenir des compétences génériques (voir question 12).

16. Près de 69% des professionnels dans le domaine (137 répondants) ont déclaré d'avoir besoin d'une formation en sécurité informatique.

17. Quatre-vingt-huit professionnels, c'est-a-dire plus de 44,2% des répondants, ont précisé que leur formation en sécurité informatique devrait inclure les unités du contenu systématisées dans le tableau 3.2.

Tableau 3.2 Unités du contenu en sécurité informatique demandées par 88 participants au sondage – professionnels

ID	Unités de contenu requises pour la formation en sécurité informatique	No répondants,
1.	Toutes spécifiés à la question 14	8
2.	Formation professionnelle en sécurité informatique, y compris les nouveaux développements dans le domaine	31
3.	Sécurité informatique, techniques et normes de cryptage des données, niveaux de	1

	protection des données, fournir une protection et intégrité des données	
4.	Conception et protection des réseaux informatiques	5
5.	Administration et sécurité des services réseau	1
6.	Firewall, VPN, protocoles de sécurité	1
7.	Routage intérieur et extérieur avancé, surveillance et gestion du réseau, WiFi et sécurité, configuration du routeur	1
8.	Sécurité dans les réseaux publics du transport des données	1
9.	Sécurité des réseaux de telecommunication	2
10.	La gestion de crise dans le contexte des cyberattaques sur les infrastructures critiques	1
11.	Méthodes et techniques d'interconnexion sécurisée des systèmes de paiement électroniques	2
12.	Test du degree de la sécurité d'accès	1
13.	Prenez le contrôle d'un autre appareil à distance. Obtenir des capacités d'espionner d'autres appareils et d'autres capacités qui peuvent contribuer à l'accomplissement de leurs responsabilités professionnelles	1
14.	Sécurité des bases de données	2
15.	Sécurisez les ressources d'information exclusives, les comptes électroniques personnels, etc	2
16.	Appliquer les outils informatiques, y compris dans l'entreprise et dans la vie personnelle	3
17.	Méthodologies d'implementation, politiques de sécurité informatique	1
18.	Sécurité des applications et des systèmes informatiques	2
19.	Instrumentaire pour assurer un niveau acceptable de sécurité informatique dans l'organisation	1
20.	Solutions IDS / IPS, solutions de filtrage anti-spam, solutions de gestion des logs, types d'attaques, vulnérabilités et méthodes de protection / prevention	1
21.	Études de cas et stages pratiques en sécurité informatique	7
22.	Identifier et traiter les risques de sécurité des applications informelles	2
23.	Programmes d'analyse de l'information	2
24.	Documenter les délinquants dans Darknet	1
25.	Procédures de gestion de la sécurité de l'utilisateur finale	1
26.	Autres	7

Les unités de contenu visées dans le tableau 3.2 sont regroupées par domaines. Ainsi (ID1), 8 répondants ont directement spécifié les 13 unités de contenu de la question 14, et 32 (ID2 et ID3) ont pratiquement spécifié une formation dans la sécurité informatique en général, sans spécifier des unités de contenu (en un total de 40 répondants, cela veut dire 45,5% des 88 répondants).

Les unités de contenu ID4-ID13 (16 répondants, 18,2%) se réfèrent à la sécurité des réseaux informatiques et leurs composants avec certains concrétisations pour les unités de contenu (3), (5), (6), (80, (9) et (13) précisées dans la question 13, y compris:

a) La gestion de crise dans le contexte des cyberattaques sur les infrastructures critiques (ID10);

b) Test de sécurité de l'accès (ID12);

c) Obtenir le contrôle d'un autre dispositif a distance (ID13);

d) Méthodes et techniques d'interconnexion sécurisé des systèmes de paiement électronique (ID11).

Les unités de contenu ID14 et ID15 (4 répondants) se réfèrent directement à la sécurité des bases de données et des ressources d'information des utilisateurs.

Il est nécessaire de mentionner les demandes en ce qui concerne les études de cas et des stages pratiques en sécurité informatique (ID21, 7 répondants, 0,08%).

18. Près de 66% des répondants (131) ont précisé que personnellement ils ont besoin d'une formation en sécurité informatique.

19. L'information sur le type de formation en sécurité informatique requise par 75 répondants est systématisée dans le tableau 3.3.

Tableau 3.3 Le type de formation en sécurité informatique demandée par 75 répondants

ID	Le type de formation requis en sécurité informatique	No répondants
1.	Théorique et pratique	24
2.	Tous	2
3.	Etudes de cas et stages pratiques	16
4.	L'enseignement en ligne	7
5.	Travail en équipe	4
6.	Fonctionnement et administration des systèmes de sécurité	2
7.	Sécurité VoIP et réseaux informatiques	2
8.	Audit/Pentesting réseau	2
9.	Dispositifs et équipements de sécurité (Firewall, VPN, etc.)	1
10.	Sécurité Cisco	4
11.	Assurer un Internet plus sûr pour les enfants et les adultes	2
12.	Sécurité des applications Web	1
13.	Mettre en œuvre des normes de sécurité telles que ISO 27001 et ISO 27002	2
14.	Gestion des risques de sécurité informatique	1
15.	Sécurité bancaire	1
16.	Méthodes de briser la sécurité des systèmes informatiques	1
17.	Auditeur des systèmes de sécurité informatique	1
18.	Connaissances de base et de précaution	1
19.	Autres	

Les informations du tableau 3.3 montrent que la majorité des répondants (32%) préféreraient la formation «Théorique et pratique» (ID1), 16 répondants (21%) - «Études de cas et stages pratiques» et 7 répondants (9.3 %) - " L'enseignement en ligne ". Certaines réponses spécifiques ont complété la liste des unités de cours du tableau 3.2, telles que: «Sécurité VoIP» (ID7), «Sécurité Cisco» (ID10), «Implémentation des normes de sécurité» (ID13).

20. Près de 61% des répondants ont précisé que l'entreprise dans laquelle ils travaillent accepterait que les étudiants suivent un stage pratique en sécurité informatique.

21. Un stage pratique en sécurité informatique pour les étudiants, qui serait accepté par les organisations dans lesquelles ils travaillent 61% des répondants (voir question 20) se réfère aux stages:

a) d'observation - 45 réponses (24%);

b) opérationnel pour développer son employabilité - 72 réponses (39%);

c) fonctionnel pour embaucher - 70 réponses (37%).

Ainsi, les possibilités de stages en sécurité informatique pour les étudiants sont prometteuses.

22. La durée du stage, préférée par les organisations qui accepteraient des stagiaires en sécurité informatique, est:

1) Un mois (28,1%);
2) Trois mois (18,6%);
3) 1-2 semaines (13,6%).

23. 117 répondants ont spécifié leurs coordonnées. Les plus connus sont: Banque Nationale de Moldavie; Endava; Moldtelecom; Le Centre du gouvernement électronique rattaché à la Chancellerie du gouvernement; Institut pour le développement de la société de l'information de l'Académie des sciences de Moldova; Fiscservinform rattaché au Service de l'impôt de l'État; Centre de lutte contre les crimes d'information; Trimetrica; Allied Testing; Deeplace; Molddata; Cedacri International; Moore Stephens; Pentalog; Centre de Télécomunications Speciales; Mobiasbanca – Groupe Société Générale; Agence des relations foncières et du cadastre; Tacit Knowledge.

4. Conclusions

L'échantillon des participants au sondage est représentatif pour la République de Moldova. Le questionnaire a été compleété par 199 répondants, représentant des entreprises bien connues telles que: Endava, Moldtelecom, Fiscservinform rattaché au Service de l'impôt de l'État; Centre de lutte contre les crimes d'information; Trimetrica; Allied Testing; Deeplace; Molddata; Cedacri International; Moore Stephens; Pentalog; Centre de Télécomunications Speciales et d'autres. Près de 23% des répondants viennenent des entreprises avec plus de 500 employés. Plus de 58% des répondants ont une expérience professionnelle en sécurité informatique.

Des connaissances générales de la sécurité informatique sont nécessaires pour tous les utilisateurs qui utilisent les ressources informatiques. Le besoin des spécialistes dans la sécurité informatique concerne principalement: les banques; les télécommunications; les services informatiques et les sociétés de conseil; les unités militarisées; l’administration publique et les grandes entreprises. Bien que dans une moindre mesure, mais aussi des spécialistes peuvent être nécessaires dans les grandes entreprises et même les petites.

Comme les tâches de base des spécialistes en matière sécurité informatique sont marqués les 12 activites spécifiés explicitement en question 8 (plus 66,8%), et comme moyens de sécurité informatique (physique et logique) utilisés par des agents economiques ont ete choisies toutes les 9 options explicitement spécifiés dans la question 10 (plus de 35,2%), parmi lesquelles 5 options ont été sélectionnées par plus de 50% des répondants.

Des 15 compétences génériques qui pourraient être nécessaires pour un spécialiste en sécurité informatique spécifiées dans le questionnaire, 8 ont été sélectionnés par plus de 50% des répondants, et des 19 compétences spécifiques, 14 ont été sélectionnés par plus de 50% des répondants . De même, des 24 candidats, 13 unités de contenu des disciplines, pour acquérir des compétences

spécifiques nécessaires pour un spécialiste de la sécurité informatique, ont été sélectionnés par 50% des répondants.

Près de 69% des professionnels du domaine (137 répondants) ont indiqué qu'ils avaient besoin d'une formation en sécurité informatique, dont une bonne partie consistait à sélectionner toutes les 13 unités de contenu de la question 14. Comme moyen de formation, toutes les six ont ete précisé dan le questionnaire, y compris la formation en ligne (45,7%).

Près de 61% des répondants ont précisé que l'organisation dans laquelle ils travaillent accepterait les étudiants pour les stages pratiques en sécurité informatique.

Dans l'ensemble, les résultats de l'enquête peuvent servir comme base pour le développement des programmes d'études universitaires en sécurité informatique.

Annexe 1. Le questionnaire pour l'Enquête d'identification des métiers cibles et des besoins de formation dans le champ de la sécurité informatique est les réponses obtenu

No	Question	Resp.	%
1.	Votre âge		
	1) 18-30	**107**	**53.8**
	2) 31-40	**58**	**29.1**
	3) 41-50	**13**	**6.5**
	4) 50+	**21**	**10.6**
2.	Votre profession:		
	1) Chef d'entreprise	**11**	**5.5**
	2) Professeur / manageur	**22**	**11.1**
	3) Ingénieur	**74**	**37.2**
	4) IT Technicien	**17**	**8.5**
	5) Autre	**75**	**37.7**
3.	Décrivez brièvement (3-4 phrases) votre tâches de service:	**162**	**81.4**
	1) Développement, maintenance et administration d'applications et de sites Web	**18**	**9.0**
	2) Conception d'applications et des systèmes informatiques	**13**	**6.5**
	3) Gestion de la sécurité informatique, y compris: surveillance des logiciels malveillants, identification des vulnérabilités et des risques de sécurité, prévention des incidents informatiques	**11**	**5.5**
	4) Audit et conseil en TI et sécurité de l'information	**9**	**4.5**
	5) Mise en place et administration des réseaux informatiques	**9**	**4.5**
	6) Directeur TI	**9**	**4.5**
	7) Enseigner des cours travaux pratiques, recherche scientifique	**9**	**4.5**
	8) Développeurs back-end	**8**	**4.0**
	9) Prévention, identification et lutte contre la cybercriminalité	**8**	**4.0**
	10) Conception et administration des bases de données	**7**	**3.5**
	11) Développement et maintenance des applications	**6**	**3.0**
	12) Développeurs Java	**6**	**3.0**
	13) Recherche en informatique	**4**	**2.0**
	14) Services de soutien TIC	**4**	**2.0**
	15) Surveillance Internet	**3**	**1.5**
	16) Test d'applications informatiques	**3**	**1.5**
	17) Gestion des systèmes informatiques	**2**	**1.0**
	18) Collection et analyse de données sur la cybercriminalité et les crimes connexes	**2**	**1.0**
	19) Luttee contre la fraude avec des moyens de paiement électroniques	**2**	**1.0**
	20) Utilisation d'applications informatiques dans la conception de bâtiments	**2**	**1.0**
	21) Etudiant	**2**	**1.0**
	22) Support technique et opérationnel pour les dispositifs de cybercriminalité	**1**	**0.5**
	23) Tester les moyens et schémas des transactions électroniques	**1**	**0.5**
	24) Autres	**34**	**17.1**
4.	Votre expérience professionnelle dans le domaine de la sécurité informatique, ans		
	1) Sans expérience	**83**	**41.7**
	2) 1-5	**71**	**35.7**
	3) 6-10	**23**	**11.6**
	4) 10+	**22**	**11.1**
5.	Quelle est la taille de votre entreprise, persons:		

	1) < 10	**34**	**17.1**
	2) 10-50	**69**	**34.7**
	3) 51-100	**15**	**7.5**
	4) 101-500	**36**	**18.1**
	5) 500+	**45**	**22.6**
6.	Selon vous, où travaillent les spécialistes de la sécurité informatique? (plusieurs choix possibles)		
	1) Banques	**147**	**73.9**
	2) Services informatiques et sociétés de consultants	**145**	**72.9**
	3) Télécommunications	**144**	**72.4**
	4) Armées	**120**	**60.3**
	5) Dans toutes les entreprises où il y a des ordinateurs	**109**	**54.8**
	6) Grandes entreprises	**107**	**53.8**
	7) Administrations publiques	**89**	**44.7**
	8) Industries	**79**	**39.7**
	9) Biotechnologies	**63**	**31.7**
	10) Petites et moyennes entreprises de production de services	**62**	**31.2**
	11) Petites et moyennes entreprises de production de produits	**45**	**22.6**
	12) Autre	**16**	**8.0**
7.	Selon vous, où a-t-on le plus besoin de spécialistes de la sécurité informatique? (plusieurs choix possibles)		
	1) Banques	**144**	**72.4**
	2) Dans toutes les entreprises où il y a des ordinateurs	**141**	**70.9**
	3) Télécommunications	**133**	**66.8**
	4) Services informatiques et sociétés de consultants	**128**	**64.3**
	5) Armées	**121**	**60.8**
	6) Administrations publiques	**112**	**56.3**
	7) Grandes entreprises	**112**	**56.3**
	8) Industries	**93**	**46.7**
	9) Biotechnologies	**75**	**37.7**
	10) Petites et moyennes entreprises de production de services	**74**	**37.2**
	11) Petites et moyennes entreprises de production de produits	**62**	**31.2**
	12) Autre	**11**	**5.5**
8.	Précisez les activités, tâches que peuvent réaliser ces spécialistes (plusieurs choix possibles)		
	1) Détection fréquente, détection des vulnérabilités du système	**172**	**86.4**
	2) Mise en place des systèmes de détection, prévention et détection des intrusions	**161**	**80.9**
	3) Rapport, analyse et prédiction des attaque	**156**	**78.4**
	4) Surveillance du réseau et du système, réponse aux incidents	**154**	**77.4**
	5) Mise en œuvre du codage des informations, authentification et construction de l'infrastructure PKI	**147**	**73.9**
	6) Mise en œuvre de la conformité de sécurité	**141**	**70.9**
	7) Assistance régulière des ateliers, des séminaires sur la sécurité de l'information, mise à jour des informations sur les vulnérabilités de sécurité des systèmes/ logiciels	**139**	**69.8**
	8) Audit de sécurité	**139**	**69.8**
	9) Mise en place du système correctif aux pièces des failles de sécurité	**137**	**68.8**
	10) Suggestion et mise en œuvre des normes de sécurité de l'information	**136**	**68.3**
	11) Test de pénétration	**135**	**67.8**
	12) Formation des procédures de sécurité aux utilisateurs des organisations	**133**	**66.8**
	13) Autre	**11**	**5.5**

9.	Précisez quels problèmes vous rencontrer dans votre entreprise concernant la sécurité informatique (plusieurs choix possibles)		
	1) Faible niveau de connaissance de l'ensemble du personnel, de la direction, non seulement des enseignants en informatique sur l'importance de la sécurité de l'information	**101**	**50.8**
	2) Problème de confidentialité de l'information	**96**	**48.2**
	3) Stratégie de gestion des risques adéquate n'est pas encore faite	**73**	**36.7**
	4) Difficultés (temps, argent, personnel) dans la mise en œuvre et l'application des politiques de sécurité au sein de l'entreprise)	**70**	**35.2**
	5) Problème de disponibilité de l'information	**69**	**34.7**
	6) Problème de modification de l'information	**68**	**34.2**
	7) Manque de ressources pour suivre / mettre en œuvre des normes de sécurité telles que ISO 27001	**55**	**27.6**
	8) Ecart entre la sécurité et la facilité d'utilisation	**48**	**24.1**
	9) Manque d'engagement des gestionnaires de haut niveau pour s'assurer que les mécanismes de sécurité sont en place	**41**	**20.6**
	10) Bonne combinaison sur la politique de gestion et la technologie de déploiement n'est pas encore faite	**37**	**18.6**
	11) Problème de substitution d'identité	**32**	**16.1**
	12) Difficultés rencontrées lors de la mise en place des processus de sécurité conformément à la norme ISO 17799	**32**	**16.1**
	13) Difficultés rencontrées de l'ensemble du personnel, de la direction lors de l'élaboration et de la mise en œuvre des processus de sécurité en traitement de l'information, des données et du système d'exploitation	**31**	**15.6**
	14) Manque de coopération entre service commercial et service de sécurité de l'entreprise	**24**	**12.1**
	15) Autre	**26**	**13.1**
10.	Précisez les outils utilisés dans votre entreprise pour la sécurité informatique (logiciels et matériels) (plusieurs choix possibles)		
	1) Accès contrôlé	**143**	**71.9**
	2) Outils de protection software	**140**	**70.4**
	3) Contrer les virus et programmes malveillants	**139**	**69.8**
	4) Encryptage des données	**113**	**56.8**
	5) Outils de protection hardware	**101**	**50.8**
	6) Obstacle physique	**98**	**49.2**
	7) Outils de protection organisationnels	**87**	**43.7**
	8) Outils de protection legaux, moraux, ethiques	**76**	**38.2**
	9) Outils de protection physique	**70**	**35.2**
	10) Autre	**5**	**2.5**
11	Selon vous, qu'elles sont les compétences génériques que doit avoir un spécialiste de la sécurité informatique? (plusieurs choix possibles)		
	1) Capacités d'analyse et de synthèse	**165**	**82.9**
	2) Capacité de vulgarisation des enjeux et des risques	**154**	**77.4**
	3) Capacité à gérer des situations d'urgence	**148**	**74.4**
	4) Travail d'équipe	**123**	**61.8**
	5) Capacité d'organisation et de planification	**114**	**57.3**
	6) Souci de la qualité	**109**	**54.8**
	7) Efficacité	**106**	**53.3**
	8) Créativité	**102**	**51.3**

	9) Esprit critique	**95**	**47.7**
	10) Aptitude à travailler dans un contexte international	**84**	**42.2**
	11) Respect de la confidentialité	**82**	**41.2**
	12) Capacité à communiquer avec des publics divers et variés	**71**	**35.7**
	13) Esprit d'initiative et capacité à entreprendre	**69**	**34.7**
	14) Capacité à manager	**68**	**34.2**
	15) Conception et gestion de projets	**62**	**31.2**
	16) Autre	**8**	**4.0**
12.	Selon vous, quels sont les enseignements qui peuvent permettre d'acquérir ces compétences génériques? (plusieurs choix possibles)		
	1) Stages pratiques	**181**	**91.0**
	2) Techniques	**160**	**80.4**
	3) Théoriques	**152**	**76.4**
	4) Etudes de cas	**147**	**73.9**
	5) Travail de groupe	**122**	**61.3**
	6) Enseignements en ligne	**74**	**37.2**
	7) Autre	**10**	**5.0**
13.	Selon vous, qu'elles sont les compétences spécifiques que doit avoir un spécialiste de la sécurité informatique? (plusieurs choix possibles)		
	1) Mettre en place les différents processus de sécurité	**167**	**83.9**
	2) Réaliser un diagnostic du système d'information	**161**	**80.9**
	3) Apporter différentes solutions de protection	**149**	**74.9**
	4) Connaître les pare-feu	**148**	**74.4**
	5) Maîtriser les protocoles de sécurité	**146**	**73.4**
	6) Maîtriser les VPN	**145**	**72.9**
	7) Recenser les points faibles	**144**	**72.4**
	8) Maîtriser la cryptologie	**134**	**67.3**
	9) Garantir la pérennité des systèmes de sécurité	**129**	**64.8**
	10) Actualiser les systèmes de sécurité en fonction des nouvelles menaces et des dernières technologies	**129**	**64.8**
	11) Rédiger des politiques et des standards de sécurité	**128**	**64.3**
	12) Evaluer la conformité du réseau par rapport aux attentes des métiers	**126**	**63.3**
	13) Concevoir et mettre en œuvre des architectures matérielles et logicielles	**110**	**55.3**
	14) Sensibiliser et former les collaborateurs aux règles de sécurité	**110**	**55.3**
	15) Elaborer des indicateurs de suivi	**99**	**49.7**
	16) Anticiper les négligences et erreurs lourdes	**97**	**48.7**
	17) Ecrire des rapports	**93**	**46.7**
	18) Evaluer les besoins d'accès aux informations et au réseau de chaque service	**84**	**42.2**
	19) Faire évoluer les réseaux	**79**	**39.7**
	20) Autre	**7**	**3.5**
14.	Selon vous, quels sont les enseignements qui peuvent permettre d'acquérir ces compétences spécifiques?		
	1) Politique de sécurité	**155**	**77.9**
	2) Langes modernes (Anglais)	**153**	**76.9**
	3) Administration de services réseaux	**147**	**73.9**
	4) Administration système	**143**	**71.9**
	5) Dispositifs et équipements de sécurité (VPN-Firewall, etc.)	**140**	**70.4**
	6) Supervision et management de Réseaux	**137**	**68.8**
	7) Cryptographie	**137**	**68.8**
	8) Wireless et sécurité	**134**	**67.3**
	9) Sécurisation de serveur et des postes clients	**131**	**65.8**

	10) Méthodologie de la mise en place d'une PSSI	**121**	**60.8**
	11) Audit/Pentesting réseau	**121**	**60.8**
	12) Sécurité de la couche application (Layer Security Application)	**115**	**57.8**
	13) Configuration des routeurs	**102**	**51.3**
	14) Stage professionnel	**94**	**47.2**
	15) Routage avancé intérieur et extérieur	**93**	**46.7**
	16) Architecture hiérarchique d'interconnexion	**88**	**44.2**
	17) IPV6	**86**	**43.2**
	18) Télécommunications haut débit (3G, LTE)	**76**	**38.2**
	19) Expression et Communication	**75**	**37.7**
	20) Téléphonie sur IP	**69**	**34.7**
	21) Conduite de projet	**68**	**34.2**
	22) Droit	**47**	**23.6**
	23) Projet tuteuré	**41**	**20.6**
	24) Economie et Gestion	**23**	**11.6**
	25) Autre	**5**	**2.5**
15.	Selon vous, qu'elles sont les modalités d'enseignement à privilégier afin d'acquérir ces compétences spécifiques?		
	1) Stages pratiques	**174**	**87.4**
	2) Techniques	**156**	**78.4**
	3) Théoriques	**144**	**72.4**
	4) Etudes de cas	**140**	**70.4**
	5) Travail de groupe	**126**	**63.3**
	6) Enseignements numériques	**91**	**45.7**
	7) Autres	**6**	**3.0**
16.	En tant que professionnel avez-vous des besoins en formation sur la sécurité informatique?		
	1) Oui	**137**	**68.8**
	2) Non	**62**	**31.2**
17.	Si vous, avez des besoins en formation sur la sécurité informatique, précisez vos besoins**:**	**88**	**44.2**
	1) Toutes spécifiées à la question 14	**8**	**9.1**
	2) Formation professionnelle en sécurité informatique, y compris les nouveaux développements dans le domaine	**31**	**35.2**
	3) Sécurité informatique, techniques et normes de cryptage des données, niveaux de protection des données, fournir une protection et intégrité des données	**1**	**1.1**
	4) Conception et protection des réseaux informatiques	**5**	**5.7**
	5) Administration et sécurité des services réseau	**1**	**1.1**
	6) Firewall, VPN, protocoles de sécurité	**1**	**1.1**
	7) Routage intérieur et extérieur avancé, surveillance et gestion du réseau, WiFi et sécurité, configuration du routeur	**1**	**1.1**
	8) Sécurité dans les réseaux publics du transport des données	**1**	**1.1**
	9) Sécurité des réseaux de telecommunication	**2**	**2.3**
	10) La gestion de crise dans le contexte des cyberattaques sur les infrastructures critiques	**1**	**1.1**
	11) Méthodes et techniques d'interconnexion sécurisée des systèmes de paiement électroniques	**2**	**2.3**
	12) Test du degree de la sécurité d'accès	**1**	**1.1**
	13) Obținerea controlului asupra altui dispozitiv de la distanță. Obținerea capacităților de a spiona alte dispozitive și alte capacități ce pot contribui la îndeplinirea atribuțiilor de serviciu	**1**	**1.1**

	14) Sécurité des bases de données	**2**	**2.3**
	15) Sécurisez les ressources d'information exclusives, les comptes électroniques personnels, etc	**2**	**2.3**
	16) Appliquer les outils informatiques, y compris dans l'entreprise et dans la vie personnelle	**3**	**3.4**
	17) Méthodologies d'implementation, politiques de sécurité informatique	**1**	**1.1**
	18) Sécurité des applications et des systèmes informatiques	**2**	**2.3**
	19) Instrumentaire pour assurer un niveau acceptable de sécurité informatique dans l'organisation	**1**	**1.1**
	20) Solutions IDS / IPS, solutions de filtrage anti-spam, solutions de gestion des logs, types d'attaques, vulnérabilités et méthodes de protection / prevention	**1**	**1.1**
	21) Études de cas et stages pratiques en sécurité informatique	**7**	**8.0**
	22) Identifier et traiter les risques de sécurité des applications informelles	**2**	**2.3**
	23) Programmes d'analyse de l'information	**2**	**2.3**
	24) Documenter les délinquants dans Darknet	**1**	**1.1**
	25) Procédures de gestion de la sécurité de l'utilisateur finale	**1**	**1.1**
	26) Autres	**7**	**8.0**
18.	Seriez-vous personnellement intéressé par une formation en sécurité informatique?		
	1) Oui	**131**	**65.8**
	2) Non	**68**	**34.2**
19.	Si vous personnellement a été intéressé par une formation en sécurité informatique, sur quoi aimeriez-vous être formé?	**75**	**37.7**
	1) Théorique et pratique	**24**	**32.0**
	2) Tous	**2**	**2.7**
	3) Etudes de cas et stages pratiques	**16**	**21.3**
	4) L'enseignement en ligne	**7**	**9.3**
	5) Travail en équipe	**4**	**5.3**
	6) Fonctionnement et administration des systèmes de sécurité	**2**	**2.7**
	7) Sécurité VoIP et réseaux informatiques	**2**	**2.7**
	8) Audit/Pentesting réseau	**2**	**2.7**
	9) Dispositifs et équipements de sécurité (Firewall, VPN, etc.)	**1**	**1.3**
	10) Sécurité Cisco	**4**	**5.3**
	11) Assurer un Internet plus sûr pour les enfants et les adultes	**2**	**2.7**
	12) Sécurité des applications Web	**1**	**1.3**
	13) Mettre en œuvre des normes de sécurité telles que ISO 27001 et ISO 27002	**2**	**2.7**
	14) Gestion des risques de sécurité informatique	**1**	**1.3**
	15) Sécurité bancaire	**1**	**1.3**
	16) Méthodes de briser la sécurité des systèmes informatiques	**1**	**1.3**
	17) Auditeur des systèmes de sécurité informatique	**1**	**1.3**
	18) Connaissances de base et de précaution	**1**	**1.3**
	19) Autres	**1**	**1.3**
20.	Seriez-vous intéressé par accueillir des stagiaires en formation sécurité informatique?		
	1) Oui	**121**	**60.8**
	2) Non	**78**	**39.2**
21.	Si votre organisation accepte des stagiaires, pour quel type de stage?		
	1) Le stage opérationnel pour développer son employabilité	**72**	**36.2**
	2) Le stage fonctionnel pour embaucher	**70**	**35.2**
	3) Le stage d'observation	**45**	**22.6**
22.	Si votre organisation accepte des stagiaires, sur quelle durée accueillerez-vous des stagiaires?	**75**	**37.7**
	1) 1 à deux semaines	**27**	**13.6**

	2) 1 mois	**56**	**28.1**
	3) 3 mois	**37**	**18.6**
	4) Plus de 3 mois	**14**	**7.0**
23.	Souhaitez-vous nous laisser vos coordonnées afin de recevoir des informations sur nos formations?	**117**	**58.8**
	Molddata, Chirev Pavel, pavel.chirev@gmail.com		
	Cedacri International, Andrei Anghelov, Cell.: +37379854798 e-mail: andrei.anghelov@cedacrinternational.md		
	Universitatea Agrară de Stat din Moldova, l.vacarciuc@uasm.md, tel: +373 69043418, rue. Mircesti, 46, Chisinau.		
	Centre du gouvernement électronique rattaché à la Chancellerie du gouvernement, Igor Bercu, igor.bercu@egov.md		
	Centre du gouvernement électronique rattaché à la Chancellerie du gouvernement, Mihail Croitoru, mcroitor@gmail.com		
	Moore Stephens, Valeriu Cernei, valeriu.cernei@bsdm.md		
	Endava SRL, rue. Sfatul Tarii 15, MD 2012, info.chisinau@endava.com, avanovski@gmail.com		
	Centre de lutte contre les crimes d'information		
	Centre de Télécomunications Speciales		
	BC „Mobiasbancă – Groupe Société Générale" S.A., Lilian Rusu, lilian.rusu@mobiasbanca.md rusu.lilian.l@gmail.com		
	Tacit Knowledge, antonioprepelita@gmail.com		
	Pentalog		
	Trimaran SRL, Sergiu Gafton, sgafton@gmail.com, t. 069112300		
	Info-Trust Consulting, Marin Prisacaru, marin.prisacaru@infotrust.md		
	Info-Trust Consulting, Alexandru Plesca, alex.plesca@infotrust.md		
	Allied Testing		
	Institut pour le développement de la société de l'information de l'Académie des sciences de Moldova, Igor Cojocaru, idsi@asm.md		
	Institut pour le développement de la société de l'information de l'Académie des sciences de Moldova, Ion Coșuleanu, cosuleanu.ion@gmail.com		
	Institut pour le développement de la société de l'information de l'Académie des sciences de Moldova, Irina Cojocaru, irina.cojocaru@idsi.md		
	Agence des relations foncières et du cadastre de Moldova, Mihail Nișcii, m.niscii@gmail.com		
	Moldtelecom		
	Starnet		
	Orange		
	Moldcell		
	BNM		
	MAIB		