MASTER

Mention : Cybersécurité

Référentiel d'activités, de compétences et d'évaluation

REFERENTIEL D'ACTIVITES	REFERENTIEL DE COMPETENCES	REFERENTIEL D'EVALUATION
- La gestion de la sécurité des systèmes d'information - La gestion de projets de sécurité - La conception et le maintien d'un SI et d'applications sécurisés - La formalisation de bonnes pratiques en matière de sécurité des systèmes d'information - L'évaluation des risques d'attaques et les conséquences potentielles sur une organisation - L'analyse de la sécurité des applications et des vulnérabilités - La réalisation d'audit de la sécurité des systèmes d'information - La réalisation de tests d'intrusion - La détection d'attaques et d'intrusions - La veille normative, technique et réglementaire sur les nouvelles attaques et vulnérabilités - Le suivi d'activités par la création et la mise à jour d'indicateurs et de tableaux de bord - La gestion des incidents et des crises de sécurité - La sensibilisation et la formation des collaborateurs à la sécurité informatique - Le respect des normes et réglementations en vigueur	**Compétences transversales** - Identifier les usages numériques et les impacts de leur évolution sur le ou les domaines concernés par la mention - Se servir de façon autonome des outils numériques avancés pour un ou plusieurs métiers ou secteurs de recherche du domaine - Mobiliser des savoirs hautement spécialisés, dont certains sont à l'avant-garde du savoir dans un domaine de travail ou d'études, comme base d'une pensée originale - Développer une conscience critique des savoirs dans un domaine et/ou à l'interface de plusieurs domaines - Résoudre des problèmes pour développer de nouveaux savoirs et de nouvelles procédures et intégrer les savoirs de différents domaines - Apporter des contributions novatrices dans le cadre d'échanges de haut niveau, et dans des contextes internationaux - Conduire une analyse réflexive et distanciée prenant en compte les enjeux, les problématiques et la complexité d'une demande ou d'une situation afin de proposer des solutions adaptées et/ou innovantes en respect des évolutions de la règlementation - Identifier, sélectionner et analyser avec esprit critique diverses ressources spécialisées pour documenter un sujet et synthétiser ces données en vue de leur exploitation - Communiquer à des fins de formation ou de transfert de connaissances, par oral et par écrit, en français et dans au moins une langue étrangère	Les modalités du contrôle permettent de vérifier l'acquisition de l'ensemble des aptitudes, connaissances, compétences et blocs de compétences constitutifs du diplôme. Ces éléments sont appréciés soit par un contrôle continu et régulier, soit par un examen terminal, soit par ces deux modes de contrôle combinés. Chaque ensemble d'enseignements à une valeur définie en crédits européens (ECTS). Pour l'obtention du grade de Master, une référence commune est fixée correspondant à l'acquisition de 120 crédits ECTS au-delà du grade de licence.

REFERENTIEL D'ACTIVITES	REFERENTIEL DE COMPETENCES	REFERENTIEL D'EVALUATION
- Le travail en équipe, la gestion d'équipe, la collaboration avec l'ensemble des services d'une organisation - Le conseil et l'expertise auprès d'organisations tierces	- Gérer des contextes professionnels ou d'études complexes, imprévisibles et qui nécessitent des approches stratégiques nouvelles - Prendre des responsabilités pour contribuer aux savoirs et aux pratiques professionnelles et/ou pour réviser la performance stratégique d'une équipe - Conduire un projet (conception, pilotage, coordination d'équipe, mise en œuvre et gestion, évaluation, diffusion) pouvant mobiliser des compétences pluridisciplinaires dans un cadre collaboratif - Analyser ses actions en situation professionnelle, s'autoévaluer pour améliorer sa pratique dans le cadre d'une démarche qualité - Respecter les principes d'éthique, de déontologie et de responsabilité sociale et environnementale - Prendre en compte la problématique du handicap et de l'accessibilité dans chacune de ses actions professionnelles **Compétences spécifiques** - Réaliser un état des lieux de l'organisation en cybersécurité et conduire une analyse des risques en utilisant la méthodologie la mieux adaptée - Définir la Politique Sécurité des Systèmes d'Information (PSSI) et la traduire en procédures et bonnes pratiques - Identifier les ressources nécessaires à la mise en œuvre et au maintien de la PSSI (humaines, techniques et financières) - Communiquer, sensibiliser et/ou former les employés de l'organisation au respect de la Politique Sécurité - Définir et/ou déployer les plans de reprise ou de continuité d'activités en fonction des menaces potentielles et de leurs impacts - Manager une équipe et/ou collaborer au sein d'une équipe autour de projets communs en y intégrant les préoccupations sociales, environnementales et éthiques	

REFERENTIEL D'ACTIVITES	REFERENTIEL DE COMPETENCES	REFERENTIEL D'EVALUATION
	- Rendre compte à la Direction de l'organisation et aux autorités compétentes du niveau de maturité de l'organisation en cybersécurité et des solutions mises en œuvre - Assurer une veille technique, réglementaire sur les nouvelles vulnérabilités et menaces émergentes ainsi qu'une veille des incidents géopolitiques - Veiller au respect des normes, de la réglementation française, européenne et internationale en vigueur, et des interfaces avec la CNIL (Commission Nationale de l'Informatique et Libertés), du CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques) et CSIRT (équipe spécialisée dans la gestion des incidents de sécurité informatique) - Gérer et/ou suivre un projet de sécurisation des infrastructures à partir d'un cahier des charges et d'un budget défini et en appliquant la méthodologie de projet la plus adéquate - Analyser la sécurité d'un SI ou Système et évaluer les risques de potentielles attaques et de nouvelles vulnérabilités - Concevoir, développer et intégrer des solutions sécurisées en respectant les normes et bonnes pratiques en vigueur - Choisir et intégrer un système de chiffrement adapté à un contexte donné - Choisir et implémenter des protocoles de sécurité - Utiliser et développer des outils d'analyse de code et de rétro-ingénierie - Rendre compte de l'avancée des projets et évaluer régulièrement l'efficacité des solutions mises en place afin d'implémenter les actions d'amélioration nécessaires - Anticiper, détecter les attaques et investiguer leur impact afin de mettre en place les mesures adéquates de remédiation - Identifier les partenaires internes et/ou externes pour réaliser des audits techniques de sécurité, des attaques et pentest (tests d'intrusion) du système d'information et des applications selon les normes en vigueur	

REFERENTIEL D'ACTIVITES	REFERENTIEL DE COMPETENCES	REFERENTIEL D'EVALUATION
	- Rédiger les rapports d'audits, d'incidents et des tests et les communiquer à l'organisation et aux autorités compétentes - Mettre en place une cellule de crise en mobilisant des ressources (humaines, techniques, financières), en définissant le périmètre d'actions, les règles de fonctionnement et les modes de réaction à adopter en cas de crise - Mettre en œuvre le plan de continuité d'activité ou de reprise d'activités en cas de crise majeure - Définir et mettre en place tout axe d'amélioration nécessaire en fonction de l'évolution des attaques et des nouvelles vulnérabilités - Etablir les enjeux de sécurité des SI des différents secteurs d'activités et profils d'organisation - Alerter la Direction d'une organisation tierce sur les risques encourus en matière de cybersécurité et préconiser les solutions à mettre en œuvre - Communiquer, conseiller et apporter une assistance technique aux utilisateurs afin que ceux-ci s'approprient les outils et respectent la stratégie définie en matière de sécurité - Réaliser des travaux de recherche et prospection en cybersécurité dans les domaines techniques, scientifiques et réglementaires *Dans certains établissements, d'autres compétences spécifiques peuvent permettre de décliner, préciser ou compléter celles qui sont proposées dans le cadre de la mention au niveau national. Pour en savoir plus se reporter au site de l'établissement.*	