Identification du module

Numéro du module	166
Titre	Assurer la sécurité de base des TIC
Compétences	Identifier la situation des infrastructures TIC en matière de risques et en déduire des mesures de sécurité propres à limiter ces risques dans les domaines de l'organisation, des ressources humaines, de l'infrastructure et de la technique.
Actions	1. Décomposer les infrastructures TIC en sous-ensembles cohérents et documenter les objets qu'ils contiennent et leurs interrelations de manière adaptée aux destinataires. 2. Procéder à une analyse de risque pour déterminer le niveau de sécurité nécessaire des objets sur le plan de la confidentialité, de la disponibilité et de l'intégrité. Consigner les résultats dans un tableau des besoins de sécurité. 3. Définir, sur la base du tableau des besoins de sécurité, des mesures de sécurité organisationnelles, infrastructurelles et techniques pour chaque objet. En proposer la mise en œuvre aux instances responsables. 4. Planifier et implémenter les mesures de sécurité définies. En tester le bon fonctionnement et l'efficacité. 5. Vérifier périodiquement l'efficacité et la cohérence des mesures de sécurité, justifier les écarts et, si nécessaire, mettre en œuvre des mesures correctives. 6. Adapter une stratégie de sécurité informatique à l'évolution des conditions générales et en fonction de la survenance d'événements déterminants pour la sécurité. En vérifier la cohérence et l'exhaustivité et réaliser les adaptations.
Compétences personnelles	Avoir conscience de son rôle en ce qui concerne la garantie de la sécurité des données, donner l'exemple et inciter les autres personnes à y contribuer.
Domaine de compétences	Gestion de la sécurité
Objet	Sécurité de base de l'infrastructure TIC d'une PME avec accès Internet.
Test	Mini-étude de cas comprenant 2-3 questions qui contrôlent plusieurs actions et d'une durée totale de 45-60 minutes.
Niveau	5
Prérequis	Assurer l'exploitation de serveurs (127) Mettre en service des composants réseaux (129) Exploiter et étendre un réseau (145) Réaliser la sécurité des réseaux (184) Assurer la protection des données et la sécurité des traitements (176)
Nombre de leçons	40
Reconnaissance	Informaticienne/informaticien en technique des systèmes et réseaux TIC avec brevet fédéral
Version du module	V3.0
Version du TM	V5.0

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs nécessaires à l'exécution compétente des actions d'un module. Leur valeur est purement informative et leur définition non exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage incombent aux prestataires de formation.

Numéro du module			166
Titre			Assurer la sécurité de base des TIC
Domaine de compétences			Gestion de la sécurité
Version du module			V3.0
Version du TM			V5.0
Objectifs opérationnels et connaissances opérationnelles nécessaires	1	1.1	Pouvoir expliquer en quels sous-ensembles cohérents une infrastructure TIC donnée doit être décomposée (matériels, logiciels, composants réseau (actifs/passifs) ou applications et données, etc.).
		1.2	Connaître des techniques permettant d'identifier et d'analyser les objets d'une infrastructure TIC et leurs interdépendances (p. ex. analyse de la structure informatique selon le BSI) et savoir expliquer comment ces techniques contribuent à la mise à disposition d'une base complète et différenciée pour la définition du besoin de sécurité.
		1.3	Connaître des techniques permettant de documenter de manière adéquate l'infrastructure TIC ou certains de ses sous-ensembles et de les représenter sous forme graphique (plans de câblage, inventaires de matériels et de logiciels, diagrammes de réseau, etc.).
	2	2.1	Connaître des méthodes permettant de définir le besoin de sécurité des objets d'une infrastructure TIC (définition des besoins de sécurité selon le BSI, etc.).
		2.2	Connaître la démarche méthodologique qui permet de procéder à une analyse de risque ciblée des processus métier assistés par TIC, p. ex. analyse de risque conformément à la sécurité de base informatique (norme BSI 100-3).
		2.3	Connaître les consignes internes et les dispositions légales en matière de sécurité et de protection des données dans les processus métier assistés par TIC. Pouvoir en expliquer l'influence sur le stockage et le traitement d'informations.
		2.4	Connaître des techniques permettant de documenter les résultats d'une analyse des besoins de sécurité sous une forme adéquate.
	3	3.1	Connaître les principales menaces pour la sécurité de base des infrastructures TIC (défauts, erreurs, force majeure, lacunes organisationnelles, actes intentionnels) et pouvoir en expliquer l'influence sur la sécurité de base des TIC d'une entreprise.
		3.2	Connaître les mesures les plus courantes permettant de garantir la sécurité de base des TIC (pare-feu, scanners antivirus, patchs de sécurité, etc.) et pouvoir en expliquer la contribution à la sécurité des TIC à l'échelon de la sécurité de base.
		3.3	Connaître des techniques permettant de préparer des propositions / variantes de solution à l'intention d'instances supérieures. Savoir contribuer à leur préparation afin d'obtenir une validation rapide des mesures de sécurité.
	4	4.1	Pouvoir expliquer les mesures de sécurité protégeant les infrastructures TIC et les processus assistés par TIC. Pouvoir contribuer à leur implémentation rapide sans perturbation de l'activité normale.
		4.2	Pouvoir exposer les critères qui doivent être vérifiés pour assurer le bon fonctionnement et l'efficacité d'une mesure de sécurité.
		4.3	Connaître des techniques permettant de vérifier le bon fonctionnement et l'efficacité d'une mesure de sécurité et pouvoir en expliquer l'utilité pour la sécurité de base des TIC.

Connaissances opérationnelles nécessaires

	5	5.1	Connaître les conditions préalables de la vérification périodique de mesures de sécurité (responsabilités, directives, etc.).
		5.2	Connaître la méthode et les outils courants permettant de procéder efficacement et systématiquement à la vérification périodique de mesures de sécurité (scanners de port, scanners de vulnérabilité, visionneurs de journaux système, piratage éthique, analyse de tickets d'incidents informatiques, etc.).
		5.3	Identifier les mesures nécessaires sur la base des résultats d'une vérification de l'infrastructure de sécurité des TIC et pouvoir expliquer la nécessité d'une adaptation.
	6	6.1	Définir sur la base des adaptations apportées à l'infrastructure de sécurité des TIC si d'autres mesures sont nécessaires. Pouvoir expliquer ces mesures.
		6.2	Savoir comment les adaptations apportées à une infrastructure de sécurité des TIC doivent être intégrées dans la stratégie de sécurité des TIC pour garantir que la documentation soit complète et cohérente.