BTS SIO – Catalogue des compétences

Bloc de compétences n°1

Support et mise à disposition de services informatiques

Activité	Compétences	Sem 1	Sem 2	Sem 3 & 4
1.1 Gérer le patrimoine informatique	1. Recenser et identifier les ressources numériques			
	2. Mettre en place et vérifier les niveaux d'habilitation associés à un service			
	3. Exploiter des référentiels, normes et standards adoptés par le prestataire informatique			
	4. Gérer des sauvegardes			
	5. Vérifier les conditions de la continuité d'un service informatique			
	6. Vérifier le respect des règles d'utilisation des ressources numériques			
1.2 Répondre aux incidents et aux demandes d'assistance et d'évolution	1. Traiter des demandes concernant les services réseau et système, applicatifs			
	2. Traiter des demandes concernant les applications			
	3. Collecter, suivre et orienter des demandes			
1.3 Développer la présence en ligne de l'organisation	1. Participer à l'évolution d'un site Web exploitant les données de l'organisation.			
	2. Référencer les services en ligne de l'organisation et mesurer leur visibilité.			
	3. Participer à la valorisation de l'image de l'organisation sur les médias numériques en tenant compte du cadre juridique et des enjeux économiques			
1.4 Travailler en mode projet	1. Analyser les objectifs et les modalités d'organisation d'un projet			
	2. Évaluer les indicateurs de suivi d'un projet et analyser les écarts			
	3. Planifier les activités			
1.5 Mettre à disposition des utilisateurs un service informatique	1. Déployer un service			
	2. Réaliser les tests d'intégration et d'acceptation d'un service			
	3. Accompagner les utilisateurs dans la mise en place d'un service			
1.6 Organiser son développement professionnel	1. Mettre en place son environnement d'apprentissage personnel			
	2. Gérer son identité professionnelle			
	3. Développer son projet professionnel			
	4. Mettre en œuvre des outils et stratégies de veille informationnelle			

Bloc de compétences n°2

Option A « Solutions d'infrastructure, systèmes et réseaux » - Administration des systèmes et des réseaux

Activité	Compétences	Sem 1	Sem 2	Sem 3 & 4
A2.1. Concevoir une solution d'infrastructure réseau	1. Analyser un besoin exprimé et son contexte juridique			
	2. Étudier l'impact d'une évolution d'un élément d'infrastructure sur le système informatique			
	3. Maquetter et prototyper une solution d'infrastructure permettant d'atteindre la qualité de service attendue			
	4. Choisir les éléments nécessaires pour assurer la qualité et la disponibilité d'un service			
	5. Élaborer un dossier de choix d'une solution d'infrastructure et rédiger les spécifications techniques			
	6. Déterminer et préparer les tests nécessaires à la validation de la solution d'infrastructure retenue			
A2.2. Installer, tester et déployer une solution d'infrastructure réseau	1. Installer et configurer des éléments d'infrastructure			
	2. Rédiger ou mettre à jour la documentation technique et utilisateur d'une solution d'infrastructure			
	3. Tester l'intégration et l'acceptation d'une solution d'infrastructure			
	4. Déployer une solution d'infrastructure			
	5. Installer et configurer des éléments nécessaires pour assurer la continuité des services			
	6. Installer et configurer des éléments nécessaires pour assurer la qualité de service			
A2.3. Exploiter, dépanner et superviser une solution d'infrastructure réseau	1. Administrer sur site et à distance des éléments d'une infrastructure			
	2. Automatiser des tâches d'administration			
	3. Gérer des indicateurs et des fichiers d'activité des éléments d'une infrastructure			
	4. Identifier, qualifier, évaluer et réagir face à un incident ou à un problème			
	5. Évaluer, maintenir et améliorer la qualité d'un service			

Bloc de compétences n°2

Option B « Solutions logicielles et applications métiers » - Conception et développement d'applications

Activité	Compétences	Sem 1	Sem 2	Sem 3 & 4
B2.1. Concevoir et développer une solution applicative	1. Analyser un besoin exprimé et son contexte juridique			
	2. Modéliser une solution applicative			
	3. Identifier, développer, utiliser ou adapter des composants logiciels			
	4. Utiliser des composants d'accès aux données			
	5. Exploiter les fonctionnalités d'un environnement de développement et de tests			
	6. Rédiger des documentations technique et d'utilisation d'une solution applicative			
	7. Participer à la conception de l'architecture d'une solution applicative			
	8. Exploiter les technologies Web pour mettre en œuvre les échanges entre applications, y compris de mobilité			
	9. Exploiter les ressources du cadre applicatif (framework)			
	10. Réaliser les tests nécessaires à la validation ou à la mise en production d'éléments adaptés ou développés			
	11. Intégrer en continu les versions d'une solution applicative			
B2.2. Assurer la maintenance corrective ou évolutive d'une solution applicative	1. Évaluer la qualité d'une solution applicative			
	2. Recueillir, analyser et mettre à jour les informations sur une version d'une solution applicative			
	3. Analyser et corriger un dysfonctionnement			
	4. Élaborer et réaliser les tests des éléments mis à jour			
	5. Mettre à jour des documentations technique et d'utilisation d'une solution applicative			
B2.3. Gérer les données	1. Exploiter des données à l'aide d'un langage de requêtes			
	2. Concevoir ou adapter une base de données			
	3. Développer des fonctionnalités applicatives au sein d'un système de gestion de base de données (relationnel ou non)			
	4. Administrer et déployer une base de données			

Bloc de compétences n°3

Cybersécurité des services informatiques

Activité	Compétences	Sem 1	Sem 2	Sem 3 & 4
A3.1 Protéger les données à caractère personnel	1. Recenser les traitements sur les données à caractère personnel au sein de l'organisation			
	2. Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel			
	3. Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel			
	4. Sensibiliser les utilisateurs à la protection des données à caractère personnel			
A3.2 Préserver l'identité numérique de l'organisation	1. Protéger l'identité numérique d'une organisation			
	2. Déployer les moyens appropriés de preuve électronique			
A3.3 Sécuriser les équipements et les usages des utilisateurs	1. Informer les utilisateurs sur les risques associés à l'utilisation d'une ressource numérique et promouvoir les bons usages à adopter			
	2. Identifier les menaces et mettre en œuvre les défenses appropriées			
	3. Gérer les accès et les privilèges appropriés			
	4. Vérifier l'efficacité de la protection			
A3.4 Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques	1. Caractériser les risques liés à l'utilisation malveillante d'un service informatique			
	2. Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité			
	3. Identifier les obligations légales qui s'imposent en matière d'archivage et de protection des données de l'organisation			
	4. Organiser la collecte et la conservation des preuves numériques			
	5. Appliquer les procédures garantissant le respect des obligations légales			

Option A (SISR)

Activité	Compétences	Sem 1	Sem 2	Sem 3 & 4
A3.5 Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service	1. Participer à la vérification des éléments contribuant à la sûreté d'une infrastructure informatique			
	2. Prendre en compte la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure			
	3. Mettre en œuvre et vérifier la conformité d'une infrastructure à un référentiel, une norme ou un standard de sécurité			
	4. Prévenir les attaques			
	5. Détecter les actions malveillantes			
	6. Analyser les incidents de sécurité, proposer et mettre en œuvre des contre-mesures			

Option B (SLAM)

Activité	Compétences	Sem 1	Sem 2	Sem 3 & 4
Assurer la cybersécurité d'une solution applicative et de son développement	7. Participer à la vérification des éléments contribuant à la qualité d'un développement informatique			
	8. Prendre en compte la sécurité dans un projet de développement d'une solution applicative			
	9. Mettre en œuvre et vérifier la conformité d'une solution applicative et de son développement à un référentiel, une norme ou un standard de sécurité			
	10. Prévenir les attaques			
	11. Analyser les connexions (logs)			
	12. Analyser des incidents de sécurité, proposer et mettre en œuvre des contre-mesures			