| **ACTIVITES / TACHES**  **IMAGE DE L’EMPLOI** | **COMPETENCES :** l’organisme doit démontrer que son parcours permet réellement de développer chacune des compétences du parcours, dans le respect des critères de performance attendus | **Quels sont les modules / séquences de votre parcours préparent à chacune de ces compétences ?** | **A quel(s) thème(s) de formation raccrochez-vous vos propres modules (cf. Note de cadrage de la formation)?** | **Quelle durée type d’apprentissage estimez-vous pour chacune de ces compétences ?** | **Comment contextualisez-vous les contenus aux environnements professionnels futurs des candidats pour chacune de ces compétences** *(ex : projets, immersions,*  *benchmark, études de cas,…)* **?** |
| --- | --- | --- | --- | --- | --- |
| **BLOC DE COMPETENCES 1 Concevoir et améliorer l’utilisation de l’infrastructure** | | | | | | |
| **Contribution à la définition de scénario de déploiement de l’infrastructure** | C1.1 Recueillir les besoins des utilisateurs en collaboration avec les équipes de la DSI afin d’évaluer les besoins en équipements, matériels, logiciels et services cloud ainsi que les niveaux de service requis auprès des fournisseurs. |  |  |  |  |
| C1.2 Proposer des scénarios d’évolution et d’amélioration de l’infrastructure cloud ou cloud hybride en y intégrant les aspects budgétaires et les contrats de services afin de conseiller la DSI ou les métiers sur les choix finaux. |  |  |  |  |
| C1.3 Effectuer des choix d’implémentation détaillés (équipements, systèmes, réseaux) à partir du scénario validé, en s’appuyant sur les expertises des équipes internes et des prestataires afin de proposer une infrastructure optimisée et d’assurer la compatibilité des systèmes entre eux. |  |  |  |  |
| C1.4 Mettre à jour la documentation, les procédures et consignes d’exploitation en s’appuyant sur les actions de maintien en condition opérationnelle (MCO) réalisées afin de décrire l’architecture du système d’information. |  |  |  |  |
| **Mise en place d’une infrastructure sécurisée** | C1.5 Participer à l’évaluation des risques de cybersécurité avec l’appui des experts et des outils mis à disposition par l’ANSSI et les constructeurs/éditeurs afin de contrôler le niveau de sécurité des systèmes et de repérer les failles de sécurité potentielles. |  |  |  |  |
| C1.6 Prendre en compte les mesures nécessaires au respect de la protection des données personnelles et de l’accessibilité numérique afin de respecter la réglementation en vigueur. |  |  |  |  |
| **Collaboration avec l’équipe de réalisation de l’infrastructure** | C1.7 Collaborer avec des équipes internes et des prestataires en utilisant des techniques et des méthodes de gestion de projet afin de travailler efficacement avec les parties prenantes. |  |  |  |  |
| **Mise en œuvre d’une veille dans le domaine du numérique** | C1.8 Identifier les tendances technologiques et réglementaires en mettant en place des outils de veille afin de garantir l’optimisation des systèmes de l’entreprise avec les dernières évolutions |  |  |  |  |
| **BLOC DE COMPETENCES 2 : Tester et mettre en production les ressources et assurer leur amélioration continue** | | | | | | |
| **Déploiement de la solution informatique** | C2.1 Formaliser un plan de tests en déclinant les phases d’analyse afin que la solution mise en place réponde aux exigences fonctionnelles et de sécurité. |  |  |  |  |
| C2.2 Réaliser les mises en production des solutions à l’aide de la documentation d’exploitation, des outils d’automatisation et des outils de supervision afin de s’assurer de la répétabilité des actions et de la robustesse du SI. |  |  |  |  |
| C2.3 Assurer les mises à jour mineures / majeures et les montées de version en appliquant les bonnes pratiques du fournisseur ainsi que les règles définies par la direction informatique et/ou la direction de la sécurité afin de garantir l’intégrité du SI et de maintenir sa performance. |  |  |  |  |
|  |  |  |  |  |  |
| **Support de la solution informatique** | C2.4 Assurer le support aux utilisateurs et éventuellement aux équipes techniques lors de la mise en production en recueillant les dysfonctionnements repérés afin de résoudre les problèmes techniques. |  |  |  |  |
| C2.5 Mettre à jour les référentiels de production en s’appuyant sur des logiciels d’analyse et d’extraction afin de générer des rapports répondant aux besoins de la DSI. |  |  |  |  |
| **BLOC DE COMPETENCES 3 : Administrer l’infrastructure et la maintenir en activité** | | | | | |
| **Contrôle des éléments de sécurité et configuration des outils de supervision** | C3.1 Définir la configuration des composants de sécurité, des comptes utilisateurs et des postes de travail en appliquant les politiques de sécurité définies par l’entreprise afin de sécuriser l’environnement utilisateur (poste de travail, terminaux mobiles, etc.). |  |  |  |  |
| C3.2 Administrer les autorisations d’accès pour les utilisateurs en effectuant un suivi régulier afin de prévenir et de réduire les risques de malveillance internes ou externes. |  |  |  |  |
| C3.3 Réaliser le suivi des systèmes (contrôle des systèmes de sauvegarde, d’antivirus, des éléments de sécurité, etc.) en s’aidant des outils de supervision afin de les maintenir en condition opérationnelle. |  |  |  |  |
| C3.4 Assurer la supervision technique de l’infrastructure (matériels, réseaux, serveurs) en utilisant les outils de supervision mis en place afin de détecter et de traiter au plus tôt les incidents globaux. |  |  |  |  |
| **Résolution d’un incident et support aux utilisateurs** | C3.5 Assister les utilisateurs dans la résolution de leurs demandes en apportant des réponses adaptées afin de garantir leur satisfaction. |  |  |  |  |
| C3.6 Gérer un incident en conduisant une analyse des causes afin d’apporter un correctif ou un contournement et d’informer les parties prenantes. |  |  |  |  |