1 Support et mise à disposition de services informatiques

1.1 Gestion du patrimoine informatique

1.1.1. Recenser et identifier les ressources numériques
1.1.2. Exploiter des référentiels, normes et standards adoptés par le prestataire informatique
1.1.3. Mettre en place et vérifier les niveaux d'habilitation associés à un service
1.1.4. Vérifier les conditions de la continuité d'un service informatique
1.1.5. Gérer des sauvegardes
1.1.6. Vérifier le respect des règles d'utilisation des ressources numériques

1.2 Réponse aux incidents et aux demandes d'assistance et d'évolution

1.2.1. Collecter, suivre et orienter des demandes
1.2.2. Traiter des demandes concernant les services réseau et système, applicatifs
1.2.3. Traiter des demandes concernant les applications

1.3 Développement de la présence en ligne de l'organisation

1.3.1. Participer à la valorisation de l'image de l'organisation sur les médias numériques en tenant compte du cadre juridique et des enjeux économiques
1.3.2. Référencer les services en ligne de l'organisation et mesurer leur visibilité.
1.3.3. Participer à l'évolution d'un site Web exploitant les données de l'organisation

1.4 Travail en mode projet

1.4.1. Analyser les objectifs et les modalités d'organisation d'un projet
1.4.2. Planifier les activités
1.4.3. Évaluer les indicateurs de suivi d'un projet et analyser les écarts

1.5 Mise à disposition des utilisateurs d'un service informatique

1.5.1. Réaliser les tests d'intégration et d'acceptation d'un service
1.5.2. Déployer un service
1.5.3. Accompagner les utilisateurs dans la mise en place d'un service

1.6 Organisation de son développement professionnel

1.6.1. Mettre en place son environnement d'apprentissage personnel
1.6.2. Mettre en œuvre des outils et stratégies de veille informationnelle
1.6.3. Gérer son identité professionnelle
1.6.4. Développer son projet professionnel

2 Conception et développement d'applications

2.1 Conception et développement d'une solution applicative

2.1.1. Analyser un besoin exprimé et son contexte juridique
2.1.2. Participer à la conception de l'architecture d'une solution applicative
2.1.3. Modéliser une solution applicative
2.1.4. Exploiter les ressources du cadre applicatif (framework)
2.1.5. Identifier, développer, utiliser ou adapter des composants logiciels
2.1.6. Exploiter les technologies Web pour mettre en œuvre les échanges entre applications, y compris de mobilité
2.1.7. Utiliser des composants d'accès aux données
2.1.8. Intégrer en continu les versions d'une solution applicative
2.1.9. Réaliser les tests nécessaires à la validation ou à la mise en production d'éléments adaptés ou développés
2.1.10. Rédiger des documentations technique et d'utilisation d'une solution applicative
2.1.11. Exploiter les fonctionnalités d'un environnement de développement et de tests

2.2 Maintenance corrective ou évolutive d'une solution applicative

2.2.1. Recueillir, analyser et mettre à jour les informations sur une version d'une solution applicative
2.2.2. Évaluer la qualité d'une solution Applicative
2.2.3. Analyser et corriger un dysfonctionnement
2.2.4. Mettre à jour des documentations technique et d'utilisation d'une solution applicative
2.2.5. Élaborer et réaliser les tests des éléments mis à jour

2.3 Gestion des données

2.3.1. Exploiter des données à l'aide d'un langage de requêtes
2.3.2. Développer des fonctionnalités applicatives au sein d'un système de gestion de base de données (relationnel ou non)
2.3.3. Concevoir ou adapter une base de données
2.3.4. Administrer et déployer une base de données

3 Cybersécurité des services informatiques

3.1 Protection des données à caractère personnel

3.1.1. Recenser les traitements sur les données à caractère personnel au sein de l'organisation
3.1.2. Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel
3.1.3. Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel
3.1.4. Sensibiliser les utilisateurs à la protection des données à caractère personnel

3.2 Préservation de l'identité numérique de l'organisation

3.2.1. Protéger l'identité numérique d'une organisation
3.2.2. Déployer les moyens appropriés de preuve électronique

3.3 Sécurisation des équipements et des usages des utilisateurs

3.3.1. Informer les utilisateurs sur les risques associés à l'utilisation d'une ressource numérique et promouvoir les bons usages à adopter
3.3.2. Identifier les menaces et mettre en œuvre les défenses appropriées
3.3.3. Gérer les accès et les privilèges appropriés
3.3.4. Vérifier l'efficacité de la protection

3.4 Garantie de la disponibilité, de l'intégrité et de la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques

3.4.1. Caractériser les risques liés à l'utilisation malveillante d'un service informatique
3.4.2. Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité
3.4.3. Identifier les obligations légales qui s'imposent en matière d'archivage et de protection des données de l'organisation
3.4.4. Organiser la collecte et la conservation des preuves numériques
3.4.5. Appliquer les procédures garantissant le respect des obligations légales

3.5 Cyber sécurisation d'une solution applicative et de son développement

3.5.1. Participer à la vérification des éléments contribuant à la qualité d'un développement informatique
3.5.2. Prendre en compte la sécurité dans un projet de développement d'une solution applicative
3.5.3. 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
3.5.4. Prévenir les attaques
3.5.5. Analyser les connexions (logs)
3.5.6. Analyser des incidents de sécurité, proposer et mettre en œuvre des contre-mesures