SIO Compétences professionnelles

1. Support et mise à disposition de services informatiques

1.1 Gérer le patrimoine informatique

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

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

- Collecter, suivre et orienter des demandes
- Traiter des demandes concernant les services réseau et système, applicatifs
- Traiter des demandes concernant les applications

1.3 Développer la présence en ligne de l'organisation

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

1.4 Travailler en mode projet

- Analyser les objectifs et les modalités d'organisation d'un projet
- Planifier les activités
- Évaluer les indicateurs de suivi d'un projet et analyser les écarts

1.5 Mettre à disposition des utilisateurs un service informatique

- Réaliser les tests d'intégration et d'acceptation d'un service
- Déployer un service
- Accompagner les utilisateurs dans la mise en place d'un service

1.6 Organiser son développement professionnel

- Mettre en place son environnement d'apprentissage personnel
- Mettre en œuvre des outils et stratégies de veille informationnelle
- Gérer son identité professionnelle
- Développer son projet professionnel

2. Conception et développement d’applications

2.1 Concevoir et développer une solution applicative

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

2.2 Assurer la maintenance corrective ou évolutive d’une solution applicative

- Recueillir, analyser et mettre à jour les informations sur une version d’une solution applicative
- Évaluer la qualité d’une solution applicative
- Analyser et corriger un dysfonctionnement
- Mettre à jour des documentations technique et d’utilisation d’une solution applicative
- Élaborer et réaliser les tests des éléments mis à jour

2.3 Gérer les données

- Exploiter des données à l’aide d’un langage de requêtes
- Développer des fonctionnalités applicatives au sein d’un système de gestion de base de données (relationnel ou non)
- Concevoir ou adapter une base de données
- Administrer et déployer une base de données

3. Cybersécurité des services informatiques

3.1 Protéger les données à caractère personnel

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

3.2 Préserver l'identité numérique de l’organisation

- Protéger l’identité numérique d’une organisation
- Déployer les moyens appropriés de preuve électronique

3.3 Sécuriser les équipements et les usages des utilisateurs

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

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

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

3.5 Assurer la cybersécurité d'une solution applicative et de son développement

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

Document original : Référentiel SIO v2