COMPÉTENCES VISÉES

Bac +5
Expert Réseaux, Infrastructures et Sécurité

BLOC 1 : GOUVERNER LES INFRASTRUCTURES SYSTÈMES ET RÉSEAUX

— Participer aux politiques de gouvernance IT dans le cadre du schéma directeur de la DSI, en s'appuyant sur des référentiels de bonnes pratiques, en mobilisant son expertise technique, et en contribuant à la structuration de la gestion des services IT, pour garantir que la gestion l'infrastructure répondent aux exigences de performance, de sécurité et de conformité.

— Auditer l'infrastructure de l'entreprise en évaluant systématiquement les volets techniques et organisationnels à l'aide de méthodes d'analyse, d'outils de surveillance et de cadres de référence pour contrôler la conformité réglementaire.

— Établir des accords de niveaux de service (SLA) en collaboration avec les clients internes et/ou externes, en définissant des indicateurs clés de performance (KPI) et leurs valeurs cibles associées, réunis en tableaux de bord et en utilisant des outils de gestion de SLA, afin d'offrir des prestations ou des réalisations répondant aux exigences et objectifs de l'entreprise.

— Élaborer, documenter et mettre en œuvre des processus et procédures standardisées en s'appuyant sur des normes et/ou référentiels tels que ISO 9001 et ITIL pour garantir la qualité et l'efficacité des services.

— Analyser les causes de non-respect des SLA en s'appuyant sur les KPI et des outils d'audit et d'analyse de données afin de proposer des actions correctives.

— Évaluer les risques pesant sur la production en lien avec l'informatique, en identifiant les menaces, en évaluant leurs probabilités et impacts afin de définir et documenter des plans de continuité et de reprise de l'activité.

— Élaborer un plan de continuité d'activité (PCA) en s'appuyant sur les SLA et l'analyse de risques, en produisant sa documentation et en définissant les moyens humains et techniques nécessaires à sa mise en place afin de respecter le niveau de service contractuel.

— Définir un plan de reprise d'activité (PRA) en priorisant les applications et services critiques et en établissant des stratégies de sauvegarde, avec respect du principe du 3-2-1, et de restauration, aussi bien matérielle et/ou logicielle qu'organisationnelle, afin d'assurer une protection optimale contre les risques de perte de données, et permettre une récupération rapide et efficace en cas de sinistre.

— Établir et mettre en œuvre des tests des plans de continuité (PCA) et des plans de reprise d'activité (PRA) en simulant des situations de crise réelles ou de pannes majeures sous forme d'exercices réflexifs, pratiques ou simulés afin d'améliorer la préparation aux incidents et assurer la résilience des infrastructures systèmes et réseaux.

— Mettre en œuvre le Numérique Responsable en adaptant des pratiques durables et d'accessibilité (personnes en situation de handicap), en se basant sur l'inventaire exhaustif des actifs informatiques et en utilisant les outils de référence afin de mesurer et d'améliorer la performance environnementale du SI et les pratiques RSE afférentes.

BLOC 2 : CONCEVOIR ET PILOTER LES INFRASTRUCTURES SYSTÈMES ET RÉSEAUX

— Concevoir une infrastructure système et réseau optimisée et sécurisée en analysant les besoins métiers et en proposant des solutions, en conformité avec le schéma directeur de la DSI, en combinant des ressources locales (on-premise) et/ou Cloud (SaaS, PaaS, IaaS) afin de fournir une base technique robuste et efficace soutenant les opérations de l'entreprise tout en garantissant la sécurité des données et des communications.

— Définir, implémenter et contrôler les règles d'accès aux données et aux services en retranscrivant les règles métiers dans une solution de gestion des identités (IAM*) afin de protéger les systèmes et les données sensibles contre les accès non autorisés.

— Arbitrer la technologie d'hébergement des systèmes et/ou applications (serveur dédié, virtualisation, conteneurisation/orchestration ou cloud) en évaluant et optimisant les ressources nécessaires à leur usage (telles que machine, stockage, bande passante, processeur, mémoire, consommation électrique), pour les déployer, les mettre en production et les gérer de manière fiable, flexible et scalable.

— Concevoir une topologie des réseaux de l'entreprise tant mono que multisites, en tenant compte des engagements de disponibilité, de capacité afin de garantir la qualité de service (QoS), la résilience (PCA) et la sécurité des communications.

— Contribuer à la mise en place, au contrôle et à l'administration de l'infrastructure, en mobilisant ses compétences techniques, en collaborant avec les équipes pluridisciplinaires et en documentant la solution pour déployer les éléments techniques de la solution.

— Automatiser les processus d'intégration, de déploiement et de maintenance des systèmes et applications en utilisant des outils d'orchestration, de gestion de déploiement et de DevOps et en contrôlant le résultat par l'analyse des logs produits pour assurer la fiabilité et la reproductibilité des mises en production.

— Organiser et piloter la gestion des incidents et du support en définissant les processus standardisés pour la création, l'attribution, le suivi des tickets et leur élévation, dans un cadre d'amélioration continue et en s'appuyant sur des outils de gestion des tickets (ITSM), pour suivre, prioriser et résoudre les incidents, ainsi qu'assurer une résolution rapide et efficace des problèmes techniques.

BLOC 3 : PILOTER LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

— Conduire une veille active en matière de cybersécurité, en analysant régulièrement les bulletins de sécurité, les publications des organismes de référence tant francophones qu'anglophones et en partageant les fruits de ses recherches conformément aux us de l'équipe (rapport/article, réseau social interne, plateforme collaborative), afin d'anticiper les menaces et vulnérabilités émergentes et mener des actions correctives.

— Participer à l'élaboration et à la mise en œuvre de la Politique de Sécurité des Systèmes d'Information (PSSI) de l'entreprise, en s'appuyant sur les standards, en s'appuyant sur une analyse des risques de sécurité, en définissant des mesures, rôles, responsabilités, procédures et protocoles, en collaboration avec le Responsable de la Sécurité des Systèmes d'Information (RSSI) pour protéger les données et les systèmes de l'entreprise.

— Auditer la sécurité en collaboration avec le Responsable de la Sécurité des Systèmes d'Information (RSSI) en couvrant les volets organisationnels, physiques et techniques afin de vérifier la mise en œuvre de la politique de sécurité et assurer son amélioration continue.

— Sensibiliser le personnel aux bonnes pratiques de la sécurité informatique en conformité avec les préconisations de l'ANSSI au moyen d'ateliers, de documentation, d'exercices de simulation d'attaque, et de campagnes de phishing afin de diminuer les comportements à risques et de

contribuer à l'amélioration continue de la sécurité de l'entreprise.

— Éprouver la sécurité de l'infrastructure sous la responsabilité du RSSI, au moyen de tests de pénétration, de simulations d'attaques, d'outils d'analyse de sécurité afin d'évaluer la robustesse des systèmes et la réactivité des équipes.

— Investiguer et analyser les incidents de sécurité, en conformité avec les recommandations de l'ANSSI, en examinant les systèmes compromis, en retraçant les actions malveillantes, et en collectant les preuves numériques afin de préparer des rapports en vue des audits de sécurité et conserver des preuves légales.

— Contribuer au fonctionnement du Centre Opérationnel de Sécurité (SOC), en gérant les incidents de sécurité au moyen de solutions SIEM, en analysant les données de sécurité, en détectant les anomalies, en orchestrant des réponses rapides et efficaces, en pilotant le déploiement des correctifs, s'il y a lieu de façon automatisée, et en assurant une surveillance continue afin de maintenir la sécurité et la résilience de l'infrastructure.

BLOC 4 : PILOTER LES PROJETS ET LA CONDUITE DU CHANGEMENT

— Piloter un projet au moyen d'une méthode de gestion de projet et des outils adaptés au contexte, en analysant le besoin, en rédigeant les documents d'initialisation et de suivi de projet adaptés à la méthode, en mobilisant les ressources et moyens nécessaires, pour gérer les équipes, s'assurer que les solutions déployées répondent aux attentes de l'entreprise et garantir la qualité des livrables, le respect des délais et des coûts.

— Assurer le suivi et le reporting du projet en s'adaptant aux parties prenantes concernées (COPIL, équipe projet, client) afin de garantir une communication claire, efficace et adaptée aux besoins, de faciliter la prise de décision, d'assurer la transparence sur l'avancement du projet, et de maintenir l'alignement des objectifs.

— Élaborer et mettre en œuvre la conduite du changement en s'appuyant sur des référentiels tels qu'ITIL, en réalisant une analyse de risques, en mettant au point une procédure de mise en production et au moyen de documentations et/ou de formations pour les utilisateurs concernés (acteurs comme usagers), afin de minimiser l'impact d'une évolution (mineure, delta ou majeure) de l'infrastructure sur l'environnement de production.

— Développer la performance de l'équipe en identifiant les besoins en compétences, en développant les talents, en planifiant la formation des collaborateurs, en participant à leur évaluation, et en mesurant l'écart entre les objectifs et le réalisé, pour améliorer la réussite des projets dans le respect des exigences fixées.

— Contribuer au recrutement des collaborateurs en participant aux rédactions de fiches de poste, en assurant une caution technique au moyen d'évaluations des compétences lors des entretiens, et en mettant l'accent sur l'inclusion notamment des personnes en situation de handicap, afin de contribuer à la construction d'une équipe diversifiée, reflétant les valeurs de l'égalité des chances et de la responsabilité sociétale (RSE).