Technicien Systèmes, Réseaux et Sécurité

Certification visée	**TSRS fiche RNCP N° (36462)**	Niveau	5

Le Technicien systèmes, réseaux et sécurité est le garant du bon fonctionnement des équipements informatiques et du réseau de l'entreprise. Son périmètre d'intervention peut s'étendre sur site, à distance et dans le Cloud. Il gère l'inventaire en appliquant une démarche écoresponsable, déploie le matériel, veille au maintien du parc informatique, recense les besoins des utilisateurs et préconise les solutions logicielles ou d'infrastructure. Il met en œuvre les mesures de sécurité et sensibilise les utilisateurs afin de minimiser les risques cyber. Il participe à la transformation digitale de l'entreprise en accompagnant les utilisateurs dans l'utilisation des nouveaux outils tels les plateformes collaboratives.

Cette qualification correspond à un poste de technicien voire d'agent de maîtrise sous l'autorité d'un responsable hiérarchique. C'est un métier qui demande de l'autonomie, de la rigueur et de l'organisation. Le sens de l'initiative associé à une bonne communication sont indispensables. Sa préoccupation principale est de veiller à l'opérationnalité et la disponibilité constantes du système d'informations.

BC01 : Déployer les matériels, les systèmes et le réseau.

Compétences attestées	Contextes et critères d'évaluation
Vérifier le bon fonctionnement des matériels en effectuant des tests de pré-déploiement pour éviter les retours et dysfonctionnements. Connaître l'architecture matérielle d'un poste de travail pour un déploiement adéquat aux besoins spécifiques des utilisateurs. Utiliser ses connaissances en gestion des annuaires pour déployer des serveurs physiques et virtuels. Intégrer les imprimantes dans le serveur d'impression afin de mutualiser leur gestion. Centraliser les connexions des téléphones IP et caméra des salles de réunions afin de faciliter leur gestion. Intégrer la flotte des équipements mobiles en les interconnectant dans le réseau de l'entreprise dans le respect des procédures établies et tenant compte des collaborateurs en situation de handicap.	Les tests de déploiement sont effectués et réussis, la procédure de déploiement est respectée. Les délais de déploiement sont respectés. Le matériel déployé correspond aux besoins, l'accessibilité numérique est établie pour tous les utilisateurs. Les serveurs sont intégrés dans l'annuaire de l'entreprise. Les tests d'impressions sont concluants. La procédure de déploiement est respectée.
Installer les systèmes d'exploitation hétérogènes grâce à un large spectre de savoir-faire associés en se référant rigoureusement aux notices techniques.	Les systèmes d'exploitation sont installés et à jours.

Se conformer strictement à des processus logiques et méthodologiques d'installation afin d'homogénéiser les processus de déploiement. Automatiser la configuration des systèmes d'exploitation à l'aide de scripts afin de réduire les coûts et les délais de déploiement.	Les processus de déploiement sont unifiés. Les scripts de configuration des systèmes sont opérationnels.
Réaliser des maquettes pour simuler l'intégration de nouveaux équipements et réduire les erreurs potentielles de configurations. Utiliser ses connaissances ou la documentation de la topologie du réseau afin d'interconnecter les différents équipements nécessaires au fonctionnement des réseaux de l'entreprise. Configurer le routage des différents réseaux pour assurer une communication optimale entre les différents sites de l'entreprise en respectant les contraintes de délai imposées.	Les maquettes de simulation sont concluantes. L'interconnexion entre les différents matériels réseaux est opérationnelle. La fiche d'intervention est rendue et correctement renseignée avec un délai respecté.
Appliquer le processus de déploiement des logiciels conformément à la gestion des licences et des autorisations de l'entreprise selon la demande du service tout en tenant compte des collaborateurs en situation de handicap. Configurer des logiciels de prise en main à distance sur les postes clients afin d'assurer un support sur les postes nomades. Automatiser l'installation des logiciels en fonction des besoins de l'utilisateur pour simplifier les procédures et réduire les délais. Configurer les plateformes collaboratives en respectant les contraintes de flux et débit réseau afin d'assurer la productivité de l'entreprise liée au travail hybride.	Les logiciels sont fonctionnels. Le support technique est assuré sur les postes nomades. Les délais sont réduits et les besoins de l'utilisateur sont satisfaits. L'accès aux données de l'entreprise sur site et à distance est opérationnel et ne produit de latence.

BC02 : Administrer des serveurs hétérogènes et un réseau multi-sites.

Compétences attestées	Contextes et critères d'évaluation
Paramétrer les différents systèmes d'exploitation en tenant compte de leurs contraintes d'interopérabilité, pour obtenir le niveau de service souhaité.	La communication entre serveurs est opérationnelle, le niveau de service attendu est respecté.
Utiliser les outils d'administration des services afin de centraliser la gestion des comptes utilisateurs et des droits d'accès aux applications métiers. Optimiser les tâches récurrentes d'administration des serveurs en produisant des scripts systèmes réutilisables. Établir des règles d'administration afin de veiller au bon fonctionnement de la remontée des logs et des alertes. Installer les solutions de sauvegarde grâce à un large spectre de savoir-faire technique associé aux politiques de sauvegarde. Configurer les outils de sauvegardes et de restauration conformément au plan de reprise d'activité.	La gestion des comptes est unifiée, et les accès contrôlés. Les scripts d'automatisations sont fonctionnels. Les alertes remontent conformément aux attentes. Les tests de restauration des sauvegardes sont concluants.
Utiliser ses connaissances sur les protocoles réseaux pour brasser les liens réseaux en vue d'assurer une connectivité de l'ensemble des équipements. Se conformer strictement à des processus logiques et méthodologiques en respectant les procédures établies et les plans et schémas réseaux fournis par l'administrateur réseau.	Les liens réseaux sont fonctionnels en respectant le schéma réseau fourni et les ressources réseaux sont accessible par les utilisateurs. Le niveau de service réseau attendu est respecté.

BC03 : Sécuriser l'environnement numérique d'exploitation.

Compétences attestées	Contextes et critères d'évaluation
Procéder aux sauvegardes des données de l'entreprise selon les modalités établies selon le plan de reprise ou de continuité	Les données sauvegardées sont pertinentes et fiables et la confidentialité des informations restaurées est respectée.
Appliquer une gestion stricte des droits et des identités des utilisateurs en contrôlant l'annuaire de l'entreprise pour éviter un accès inapproprié aux données.	L'intégrité, la disponibilité et la confidentialité des données des utilisateurs est vérifiable.
Tester régulièrement la redondance et l'opérationnalité des équipements du parc informatique pour éviter les interruptions de service.	La redondance des équipements du parc est contrôlée.
Identifier le matériel, les systèmes d'exploitation ou les logiciels à mettre à jour (virtualisé ou physique) afin de corriger les vulnérabilités.	Le matériel, les systèmes et les logiciels à mettre à jour sont identifiés.
Anticiper l'évolution de l'état des matériels, systèmes et logiciels pour minimiser les incidents de sécurité du parc informatique.	La politique de sécurité est respectée, les patchs de sécurités sont testés, installés et opérationnels.
Identifier les plateformes officielles de mise à jour pour les matériels, systèmes et logiciels (virtualisées ou physiques) pour éviter les erreurs de configuration.	Les mises à jour sont faites à partir des sites des fournisseurs.
Configurer les outils de surveillance afin de filtrer l'accès au réseau de l'entreprise à l'aide de listes permettant de bloquer l'accès aux sites malveillants connus.	Les sondes de détection d'anomalie sont paramétrées.
Sécuriser les équipements nomades (smartphone, tablettes, PC...) grâce à un chiffrement des données pour éviter l'exploitation frauduleuse des données de l'entreprise.	Les équipements nomades sont chiffrés, l'accès aux données est contrôlé.
Créer des canaux de sécurisation en utilisant ses connaissances sur les protocoles de sécurité.	Des canaux sécurisés sont opérationnels.
Limiter l'accès aux réseaux sans-fils publics des équipements nomades afin d'éviter les intrusions malveillantes.	L'accès aux réseaux publics des équipements nomades est limité.
Appliquer les procédures de sécurité liées à l'accès physiques et logiques des données en mettant en place des stratégies de groupes dans l'annuaire.	Les règles d'accès sont créées et respectées.

BC04 : Entretenir un parc informatique.

Compétences attestées	Contextes et critères d'évaluation
Appliquer les processus de réception pour éviter les erreurs de livraisons.	Absence d'écart entre la commande et la livraison, le bon de livraison est signé et classé.
Renseigner les documents de suivi afin de mettre à jour l'inventaire du parc informatique.	L'état de stock est à jour.
Mettre à jour des matériels, des systèmes d'exploitation et les logiciels clients pour garantir le fonctionnement optimal des équipements informatiques grâce à un serveur de mises à jour.	La liste des mises à jour du serveur est validée.
Reconditionner des équipements informatiques garantissant un environnement numérique durable et écoresponsable.	Durabilité des équipements informatiques augmentée, une démarche écoresponsable est appliquée.
Décider de la réparation ou du recyclage d'un matériel défectueux après contrôle de l'état de garantie en appliquant la méthode 4R (Réduire, réparer, réemployer et recycler) permettant d'augmenter le cycle de vie des postes utilisateurs.	La durée de vie des équipements numériques est allongée.
Recycler le matériel usagé et obsolète du parc informatique dans le respect d'une démarche de transition écologique.	Le taux d'équipements numériques reconditionnées est augmenté.
Collecter les informations permettant d'anticiper les innovations technologiques et de surveiller les nouvelles menaces informatiques en utilisant les différents outils de veille, selon le plan de veille établi.	Une alerte technologique est diffusée
Analyser les nouvelles technologies émergentes dans la limite de son périmètre d'intervention, dans le but de détecter leurs avantages et inconvénients sur le parc existant.	Les répercussions des nouvelles technologies sur le parc sont répertoriées.
Rédiger des comparatifs des nouveaux matériels et logiciels par rapport à ceux utilisées par l'entreprise dans l'objectif d'augmenter les performances du SI.	Une analyse comparative est fournie.

BC05 : Assurer le support technique auprès des utilisateurs.

Compétences attestées	Contextes et critères d'évaluation
Respecter les niveaux de services inhérents aux contrats de maintenance afin de garantir les délais d'interventions.	Les niveaux de services sont respectés, les délais de résolution sont respectés.
Gérer les conflits utilisateurs afin d'établir une relation de confiance.	L'utilisateur est rassuré.
Analyser une situation en toute autonomie afin d'apporter une solution appropriée sur son périmètre.	Les incidents techniques sont clôturés.
Rédiger un rapport d'interventions sur la résolution d'incidents afin de garantir leurs suivis.	La fiche d'intervention est signée par l'utilisateur ou le client.
Se référer rigoureusement aux procédures d'entreprise permettant de hiérarchiser ses interventions en utilisant et en enrichissant la base de connaissances.	Les incidents non résolus sont escaladés, la base de connaissances est renseignée et à jour.
Reformuler les requêtes des utilisateurs en faisant preuve d'empathie afin d'établir une relation de confiance dans l'objectif de faciliter la résolution de l'incident, en tenant compte des collaborateurs en situation de handicap.	La communication avec les utilisateurs est établie sur une base de confiance, l'utilisateur est satisfait.
Exposer une problématique technique ou organisationnelle en vue d'un partage d'informations au sein de l'équipe.	Les problèmes relationnels sont pris en charge.
Respecter les règles de base de la communication écrite et orale tant en français qu'en anglais.	Une relation de confiance est établie avec les utilisateurs.
Sensibiliser l'utilisateur en facilitant la compréhension d'éléments techniques ou de sécurités tout en s'assurant de la bonne compréhension par l'utilisateur des termes et procédures informatiques, en tenant compte des collaborateurs en situation de handicap.	La Charte informatique est diffusée, respect des préconisations de sécurité.
Diffuser les pratiques écoresponsables pour un systèmes d'information permettant de limiter l'impact des usages du numériques sur l'environnement.	Les gestes écoresponsables sont diffusés.
Assurer des démonstrations d'usages permettant la prise en main par l'utilisateur du matériel ou du logiciel livré.	L'utilisateur de l'entreprise est formé, le document de prise en charge est signé.