REFERENTIEL EMPLOI ACTIVITES COMPETENCES

DU TITRE PROFESSIONNEL

Administrateur d'infrastructures sécurisées

Niveau II

Site : http://travail-emploi.gouv.fr

SOMMAIRE

Pages

Introduction

Présentation de l'évolution du Titre Professionnel

Ce nouveau titre professionnel « Administrateur d'infrastructures sécurisées » (AIS), créé en date du 06/04/2018, répond aux besoins repérés sur le marché de l'emploi dans le domaine des infrastructures informatiques. Il correspond aux exigences de qualification qui accompagnent les évolutions des infrastructures (complexité accrue, hybridation, sécurisation, recherche d'automatisation). Ces évolutions interviennent dans un contexte où les pouvoirs publics et les entreprises accordent une importance croissante aux enjeux majeurs de la cybersécurité.
La création du titre professionnel sera déclinée en trois activités-types pour l'emploi visé.

- Administrer et sécuriser les composants constituant l'infrastructure.
- Intégrer, administrer et sécuriser une infrastructure distribuée.
- Faire évoluer et optimiser l'infrastructure et son niveau de sécurité.

Contexte de l'examen du Titre Professionnel

La veille 2017 du secteur informatique et télécommunications fait ressortir un certain nombre d'évolutions impactant l'ensemble des filières de la production – exploitation et de la maintenance –support.

- le développement de l'informatique en nuage se poursuit et s'accélère (cloud computing) avec une mise à disposition d'applications, de plateformes et d'infrastructures en tant que services (SaaS, PaaS, IaaS) ;
- les technologies de virtualisation se généralisent, y compris dans le domaine des réseaux informatiques ;
- les tâches d'exploitation s'automatisent à des niveaux plus complexes (scripting) ;
- les besoins en sécurité des systèmes d'informations augmentent.

Une analyse du marché de l'emploi et des offres correspondantes sur l'intitulé « Administrateur » associé aux mots-clés : système, réseaux, sécurité et infrastructure fait apparaître de manière récurrente un nombre de recrutements important sur la période observée (un an).
Enfin, une enquête complémentaire menée auprès des professionnels du secteur confirme les tendances observées, et conduit à la proposition d'un titre de niveau II, ce nouveau titre étant construit sur trois activités.
L'activité « Administrer et sécuriser les composants constituant l'infrastructure » correspond à la maîtrise et la mise en œuvre des technologies liées aux systèmes, aux réseaux et à la virtualisation, dans un contexte professionnel de respect de l'état de l'art et des bonnes pratiques, incluant la sécurité. La maîtrise de ce socle de fondamentaux constitue la base du métier, dans le contexte d'une infrastructure que l'entreprise héberge sur ses propres sites (On-premise), ou dans le contexte d'une infrastructure hébergée chez un fournisseur de services.
L'activité « Intégrer, administrer et sécuriser une infrastructure distribuée » regroupe les compétences nécessaires à la mise à disposition des services dans un environnement d'infrastructure distribuée, où tout ou partie des services sont externalisés (infrastructure hybride ou totalement hébergée dans le cloud), ce qui nécessite de répondre à des besoins d'interconnexion, de synchronisation et de sécurité.
L'activité « Faire évoluer et optimiser l'infrastructure et son niveau de sécurité » recouvre l'analyse et la conception de solutions permettant de faire évoluer l'infrastructure (besoins nouveaux, optimisation). Elle intègre les compétences liées à la sécurité à un niveau plus approfondi. Dans le cadre de la gestion des risques, l'Administrateur d'Infrastructures Sécurisées participe aux réflexions menées à un niveau technique, en lien avec les responsables métiers, et met en place des solutions adaptées.
La prise en compte de la sécurité revêt donc une importance particulière et se déclinera de deux manières dans l'exercice de cet emploi-type.

1. De manière transverse, par l'application opérationnelle de règles et de recommandations génériques adaptées au contexte de l'infrastructure. Il s'agit de bonnes pratiques mises en œuvre de manière systématique, notamment pour des tâches récurrentes.
2. Lors de l'évolution de l'infrastructure, en réponse à l'expression de besoins nouveaux, avec la mise en place de solutions techniques, ou à travers des opérations de mesure et d'audit.

Cette prise en compte de la sécurité s'appuie largement sur les recommandations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), tant pour l'application de mesures opérationnelles « d'hygiène informatique » par exemple, que pour la participation à des analyses à périmètre plus large, faisant appel à des méthodes de gestion de risques.

Liste des activités

Nouveau TP : Administrateur d'infrastructures sécurisées
Activités :
- Administrer et sécuriser les composants constituant l'infrastructure
- Intégrer, administrer et sécuriser une infrastructure distribuée
- Faire évoluer et optimiser l'infrastructure et son niveau de sécurité

Vue synoptique de l'emploi-type

N° Fiche AT	Activités types	N° Fiche CP	Compétences professionnelles
1	Administrer et sécuriser les composants constituant l'infrastructure	1	Administrer et sécuriser le réseau d'entreprise
		2	Administrer et sécuriser un environnement système hétérogène
		3	Administrer et sécuriser une infrastructure de serveurs virtualisée
		4	Appliquer les bonnes pratiques et participer à la qualité de service
2	Intégrer, administrer et sécuriser une infrastructure distribuée	5	Créer des scripts d'automatisation
		6	Intégrer et gérer les différents environnements de travail des utilisateurs
		7	Administrer les services dans une infrastructure distribuée
3	Faire évoluer et optimiser l'infrastructure et son niveau de sécurité	8	Superviser, mesurer les performances et la disponibilité de l'infrastructure et en présenter les résultats
		9	Proposer une solution informatique répondant à des besoins nouveaux
		10	Mesurer et analyser le niveau de sécurité de l'infrastructure
		11	Participer à l'élaboration et à la mise en œuvre de la politique de sécurité

FICHE EMPLOI TYPE

Administrateur d'infrastructures sécurisées

Définition de l'emploi type et des conditions d'exercice

L'Administrateur d'Infrastructures Sécurisées administre les infrastructures informatiques dont il assure l'installation, le paramétrage, la sécurisation, le maintien en condition opérationnelle et en condition de sécurité.
Il propose et met en œuvre des solutions permettant de faire évoluer les infrastructures et contribue à la gestion des risques et à la politique de sécurité de l'entreprise.

Il installe, sécurise et met en exploitation les composants de l'infrastructure (serveurs, réseaux, hyperviseurs). Il en supervise le fonctionnement et en assure le support, dans le respect des bonnes pratiques méthodologiques.
Il met en œuvre et administre les moyens techniques permettant aux utilisateurs d'accéder aux données et aux applications pouvant être hébergées sur différentes infrastructures (internes, externalisés, clouds privés ou publics), en assurant la sécurité des accès et la protection des données.
Il intègre les besoins liés à la mobilité dans la gestion de l'environnement de travail des utilisateurs.
L'Administrateur d'Infrastructures Sécurisées applique la politique de sécurité de l'entreprise et contribue à son renforcement par l'étude et la mise en œuvre de solutions techniques et également par des actions de sensibilisation et de diffusion de bonnes pratiques.
Il exerce ses missions dans le respect des méthodes, des normes et standards du marché, des règles de sécurité, et des contrats de service.
Ces missions s'exercent avec les contraintes des différents environnements (développement, test, recette, production).

Il est l'interlocuteur des clients (internes ou externes), des responsables métier et des décideurs (maîtrise d'ouvrage), ainsi que des partenaires externes, prestataires et fournisseurs.
L'utilisation de l'anglais est nécessaire pour comprendre des documentations techniques, utiliser les outils et logiciels ainsi que pour échanger avec des correspondants étrangers.
Afin d'être opérationnel dans l'emploi, et par rapport au Cadre Européen Commun de Référence pour les Langues, le minimum requis est le niveau B1 en compréhension de l'écrit, en compréhension de l'oral, en expression écrite et A2 en expression orale.

L'Administrateur d'Infrastructures Sécurisées peut être amené à travailler les jours non ouvrés, avec des possibilités d'astreintes.

Secteurs d'activité et types d'emplois accessibles par le détenteur du titre

Les différents secteurs d'activités concernés sont principalement :

- Entreprise de Services du Numérique (ESN) ;
- DSI ;
- PME/PMI ;
- Collectivités territoriales ou service public.

Les types d'emplois accessibles sont les suivants :

- Administrateur systèmes et réseaux (et sécurité).
- Administrateur systèmes (et sécurité).
- Administrateur réseaux (et sécurité).
- Administrateur d'infrastructures.
- Superviseur infrastructure et réseaux.
- Responsable infrastructure systèmes et réseaux.

Réglementation d'activités (le cas échéant)

Néant.

Equivalences avec d'autres certifications (le cas échéant)

Néant.

Liste des activités types et des compétences professionnelles

1. Administrer et sécuriser les composants constituant l'infrastructure
Administrer et sécuriser le réseau d'entreprise
Administrer et sécuriser un environnement système hétérogène
Administrer et sécuriser une infrastructure de serveurs virtualisée
Appliquer les bonnes pratiques et participer à la qualité de service

2. Intégrer, administrer et sécuriser une infrastructure distribuée
Créer des scripts d'automatisation
Intégrer et gérer les différents environnements de travail des utilisateurs
Administrer les services dans une infrastructure distribuée

3. Faire évoluer et optimiser l'infrastructure et son niveau de sécurité
Superviser, mesurer les performances et la disponibilité de l'infrastructure et en présenter les résultats
Proposer une solution informatique répondant à des besoins nouveaux
Mesurer et analyser le niveau de sécurité de l'infrastructure
Participer à l'élaboration et à la mise en œuvre de la politique de sécurité

Compétences transversales de l'emploi (le cas échéant)

Communiquer par écrit avec les professionnels et les utilisateurs de l'informatique
Utiliser l'anglais dans son activité professionnelle en informatique

Niveau et/ou domaine d'activité

Niveau II (Nomenclature de 1969)
Convention(s) :
Code(s) NSF :
326 - Informatique, traitement de l'information, réseaux de transmission (niv100)

Fiche(s) Rome de rattachement

M1801 Administration de systèmes d'information
M1810 Production et exploitation de systèmes d'information
M1806 Expertise et support technique en systèmes d'information

FICHE ACTIVITÉ TYPE N° 1

Administrer et sécuriser les composants constituant l'infrastructure

Définition, description de l'activité type et conditions d'exercice

L'Administrateur d'Infrastructures Sécurisées installe, paramètre, administre et sécurise les éléments constituant l'infrastructure, qu'il maintient en condition opérationnelle, afin de garantir les niveaux de service (disponibilité, performances, sécurité) attendus par les entités utilisatrices.
Il veille à respecter dans chacune de ses missions, l'état de l'art et les recommandations en la matière.

L'Administrateur d'Infrastructures Sécurisées installe, paramètre et sécurise les environnements de virtualisation (hyperviseurs, systèmes de gestion, stockage). Il installe, paramètre, administre et sécurise les serveurs.
Il installe, paramètre, administre et sécurise les équipements réseaux. Il supervise les flux et les priorise en fonction de la qualité service associée (QoS), définit et met en place les règles de contrôle et de sécurisation de ces flux.
Il participe au choix des différentes solutions d'interconnexion (liaisons nomades, site à site).
Il met en place et administre les contrôles d'accès à l'infrastructure pour l'ensemble des périphériques utilisateurs.
L'Administrateur d'Infrastructures Sécurisées participe aux mises en production dans le respect des bonnes pratiques, et contribue à la gestion des actifs et des configurations.
Il assure le support à l'exploitation (niveaux 2 et 3).

L'Administrateur d'Infrastructures Sécurisées travaille dans le respect des niveaux de service contractualisés, et prend en compte :
- les contraintes techniques (spécificités de chaque environnement technique, plan de sécurité informatique) ;
- les engagements contractuels avec les fournisseurs et prestataires, et les clients externes dans le cas d'une ESN.

L'Administrateur d'Infrastructures Sécurisées est autonome dans les limites de sa délégation. Dans les entités importantes, l'activité se réalise sous le contrôle du responsable du système d'information ou du responsable de la sécurité du système d'information (RSSI).
L'exercice de l'activité peut présenter des possibilités d'astreintes.
L'Administrateur d'Infrastructures Sécurisées a pour interlocuteurs :

- le responsable du système d'information ;
- le responsable de la sécurité du système d'information (RSSI) ;
- l'équipe informatique ;
- les utilisateurs ;
- les experts techniques ;
- les opérateurs de télécoms, les constructeurs, les éditeurs et les fournisseurs.

Réglementation d'activités (le cas échéant)

Néant.

Liste des compétences professionnelles de l'activité type

Administrer et sécuriser le réseau d'entreprise
Administrer et sécuriser un environnement système hétérogène
Administrer et sécuriser une infrastructure de serveurs virtualisée
Appliquer les bonnes pratiques et participer à la qualité de service

Compétences transversales de l'activité type (le cas échéant)

FICHE ACTIVITÉ TYPE N° 2

Intégrer, administrer et sécuriser une infrastructure distribuée

Définition, description de l'activité type et conditions d'exercice

L'Administrateur d'Infrastructures Sécurisées met en œuvre, administre et sécurise les moyens permettant l'interconnexion et la synchronisation entre les différents éléments constituant l'infrastructure distribuée, afin de garantir l'accès à l'ensemble des services fournis, dans le respect des contrats passés avec les entités utilisatrices.

L'Administrateur d'Infrastructures Sécurisées adapte ou élabore des scripts d'automatisation.
Il permet l'interopérabilité des composants de l'infrastructure (annuaires, applications), met en œuvre et gère la synchronisation des données et en contrôle l'accès.
Il prend en compte les différents environnements de travail des utilisateurs, en incluant la mobilité, et permet aux utilisateurs d'accéder aux ressources via différents périphériques.
Il déploie les applications, et en contrôle l'accès et l'usage.
Il réalise les sauvegardes et l'archivage des données et teste les restaurations.

Cette activité a pour périmètre l'infrastructure distribuée, qui peut être constituée à la fois d'éléments internes à l'entreprise et de ressources externes (applications, plateformes, infrastructures) hébergées dans le cloud, le cas échéant chez différents fournisseurs.

L'Administrateur d'Infrastructures Sécurisées exerce dans le respect des niveaux de service établis, et prend en compte :
- les contraintes techniques (spécificités de chaque environnement technique, plan de sécurité informatique) ;
- l'organisation (besoins des utilisateurs en fonction de leur activité, contrats de service passés avec les clients internes) ;
- les engagements contractuels avec les fournisseurs (prestataires, opérateurs) et les clients externes dans le cas d'une ESN ;

Il est autonome dans les limites de sa délégation. Dans les entités importantes, l'activité se réalise sous le contrôle du responsable du système d'information.
L'exercice de l'activité peut présenter des possibilités d'astreintes.
L'Administrateur d'Infrastructures Sécurisées a pour interlocuteurs :

- le responsable du système d'information ;
- le responsable de la sécurité du système d'information (RSSI) ;
- l'équipe informatique ;
- les utilisateurs ;
- les experts techniques ;
- les opérateurs de télécoms, les constructeurs, les éditeurs et les fournisseurs.

Réglementation d'activités (le cas échéant)

Néant.

Liste des compétences professionnelles de l'activité type

Créer des scripts d'automatisation
Intégrer et gérer les différents environnements de travail des utilisateurs
Administrer les services dans une infrastructure distribuée

Compétences transversales de l'activité type (le cas échéant)

FICHE ACTIVITÉ TYPE N° 3

Faire évoluer et optimiser l'infrastructure et son niveau de sécurité

Définition, description de l'activité type et conditions d'exercice

L'Administrateur d'Infrastructures Sécurisées supervise l'infrastructure, mesure les niveaux de performance et de disponibilité. Il propose des solutions permettant de répondre à des besoins nouveaux ou d'optimiser l'infrastructure. Il participe sur les aspects techniques aux audits de sécurité et aux analyses associées à la gestion des risques, afin d'améliorer les services fournis et leur niveau de sécurité.

L'Administrateur d'Infrastructures Sécurisées met en œuvre les moyens de suivi et de mesure des indicateurs associés aux performances et à la disponibilité, met en forme les résultats de la supervision et les exploite en menant des actions correctives et préventives.
Suite à un besoin repéré ou caractérisé, il évalue et propose des solutions techniques, prévoit et définit les étapes nécessaires au projet d'intégration d'une nouvelle ressource dans l'infrastructure.
L'Administrateur d'Infrastructures Sécurisées évalue le niveau de sécurité de l'infrastructure ou d'un sous-ensemble de celle-ci, sa capacité de résilience, et participe à l'identification des vulnérabilités.
Il élabore des mesures de sécurité et les met en œuvre.
Il veille à la conformité permanente des infrastructures, vis-à-vis de la politique de sécurité de l'entreprise et des bonnes pratiques en la matière.
Il sensibilise et forme les utilisateurs aux bonnes pratiques de sécurité, et contribue au maintien des compétences des équipes techniques.

L'Administrateur d'Infrastructures Sécurisées prend en compte :

- l'analyse des processus de production du système informatique en place (indicateurs de qualité de service) ;
- les besoins exprimés par les entités métier ou repérés par lui-même ;
- les évolutions technologiques, normatives et réglementaires ;
- les recommandations et méthodes émanant d'organismes de référence sur la sécurité.

L'Administrateur d'Infrastructures Sécurisées participe, en tant que force de proposition et initiateur de solutions techniques aux scénarios d'évolution de l'infrastructure. Il est autonome dans ses champs d'expertise, et dans le cadre de ces évolutions il travaille généralement à son initiative, en collaboration avec le RSSI et sous le contrôle de la direction.
Dans le cadre particulier de la gestion de la sécurité, en lien avec les responsables métier, il traduit en termes techniques les besoins de sécurisation des actifs critiques du patrimoine informationnel.
L'Administrateur d'Infrastructures Sécurisées a pour interlocuteurs :

- le responsable du système d'information ;
- le responsable de la sécurité du système d'information (RSSI) ;
- les responsables métier ;
- l'équipe informatique ;
- les utilisateurs ;
- les experts techniques ;
- les opérateurs de télécoms, les constructeurs, les éditeurs et les fournisseurs.

Réglementation d'activités (le cas échéant)

Néant.

Liste des compétences professionnelles de l'activité type

Superviser, mesurer les performances et la disponibilité de l'infrastructure et en présenter les résultats
Proposer une solution informatique répondant à des besoins nouveaux

Mesurer et analyser le niveau de sécurité de l'infrastructure
Participer à l'élaboration et à la mise en œuvre de la politique de sécurité

Compétences transversales de l'activité type (le cas échéant)

FICHE COMPÉTENCE PROFESSIONNELLE N° 1

Administrer et sécuriser le réseau d'entreprise

Description de la compétence – processus de mise en œuvre

A partir du cahier des charges et de la documentation caractérisant les différents flux réseaux (qualité de service, sécurité, disponibilité), mettre en œuvre, installer et paramétrer les composants constituant les réseaux de l'entreprise. Contrôler la conformité des services fournis par les prestataires. Assurer que les règles de sécurité et les niveaux de service attendus sont respectés, et mettre à jour la documentation.

Contexte(s) professionnel(s) de mise en œuvre

Cette compétence est mobilisée lors de la mise en œuvre ou de l'évolution du réseau de l'entreprise et de ses interconnexions. Elle associe des technologies de réseaux physiques et virtuels. Le recours à des fournisseurs et prestataires externes nécessite une vigilance particulière sur les problématiques de performances, de coûts et de sécurité. La mise en œuvre de l'infrastructure peut imposer certaines contraintes liées à l'intégration dans le système existant et en production, telles que la limitation des interruptions de service.

Critères de performance

L'infrastructure réseau est opérationnelle conformément aux niveaux de service attendus
L'ensemble du processus de mise en œuvre est réalisé avec méthode
Les règles de sécurité sont respectées
L'infrastructure est documentée et les procédures d'exploitation sont rédigées de façon claire et opérationnelle
Les logiciels, documents et sources d'information en anglais sont utilisés de façon fiable et sans erreur de compréhension

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Evaluer les performances du réseau : taux de disponibilité, temps de réponse, évolution des flux
Installer et configurer les équipements d'interconnexion physiques et virtuels
Configurer et sécuriser les réseaux sans fil
Installer et configurer les outils de sécurisation des accès (règles de filtrage, authentification)
Mettre en œuvre les solutions de prévention et détection d'intrusion (IPS, IDS)
Installer et configurer les dispositifs permettant la redondance et l'équilibrage de charge
Mettre en œuvre la qualité de service au niveau des flux réseau (QoS)
Utiliser un outil de gestion centralisé des équipements réseaux (inventaire, version logicielle, configuration)
Administrer les accès distants sécurisés des utilisateurs nomades (VPN à distance)
Administrer et sécuriser les connexions inter sites (VPN site à site)
Rédiger et mettre à jour la documentation d'exploitation : plans d'infrastructure physique et logique, procédures d'exploitation et de configuration
Collecter et mettre à jour les caractéristiques des éléments du réseau dans l'outil de gestion des configurations
Mettre en œuvre le plan d'adressage réseau
Appliquer les recommandations de l'ANSSI en matière de sécurité réseau

Appliquer la politique de la sécurité du système d'information de l'entreprise

Assurer la relation avec les fournisseurs

Connaissance des protocoles réseaux

Connaissance des principales technologies et des normes utilisées dans les réseaux convergents (voix, données, images)
Connaissance des normes et protocoles de sécurité réseau
Connaissance des bases de la cryptographie
Connaissance des méthodes et protocoles les plus courants permettant des communications sécurisées (chiffrement, contrôle de l'intégrité)
Connaissance des risques et principales menaces sur les accès réseau externes, et des moyens de protection associés
Connaissance des protocoles de redondance (VRRP, HSRP)
Connaissance des solutions d'interconnexion proposées par les opérateurs

FICHE COMPÉTENCE PROFESSIONNELLE N° 2

Administrer et sécuriser un environnement système hétérogène

Description de la compétence – processus de mise en œuvre

Dans un contexte d'environnement hétérogène comportant des systèmes d'exploitation différents, mettre en œuvre les différents serveurs et gérer la redondance. Administrer les systèmes et les services réseaux, afin de garantir l'interconnexion dans le respect des règles de sécurité et des niveaux de service attendus.

Contexte(s) professionnel(s) de mise en œuvre

Cette compétence est mise en œuvre sur des infrastructures où cohabitent des systèmes Windows, Linux, ou autres. L'utilisation de protocoles respectant les standards garantit en principe l'interopérabilité, l'Administrateur d'Infrastructures Sécurisées doit néanmoins s'en assurer, dans un contexte où la sécurisation de l'infrastructure doit être appliquée de manière homogène, quel que soit le système hôte.

Critères de performance

L'environnement système est opérationnel conformément aux niveaux de service attendus
L'ensemble du processus de mise en œuvre est réalisé avec méthode
Les règles de sécurité sont appliquées
L'infrastructure est documentée et les procédures d'exploitation sont rédigées de façon claire et opérationnelle
Les logiciels, documents et sources d'information en anglais sont utilisés de façon fiable et sans erreur de compréhension

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Configurer et paramétrer un serveur
Installer et configurer les connexions au réseau et les services associés (DNS, DHCP, certificats, services de mises à jour)
Prendre le contrôle à distance des différents types de serveurs en mode sécurisé
Identifier, analyser et résoudre les incidents systèmes, à partir des messages d'erreurs et des journaux
Partager des ressources en environnement hétérogène (CIFS, SMB, NFS, HTTPS…)
Mettre en place et configurer un annuaire de réseau en environnement hétérogène (NIS, AD, LDAP…)
Mettre en œuvre des échanges sécurisés (SSH, IPsec, TLS…)
Mettre en œuvre et administrer une infrastructure à clés publiques
Administrer les différents types de serveurs en ligne de commande (Powershell, shell Unix et/ou Linux)
Automatiser un traitement simple (scripting)
Sauvegarder et restaurer les environnements systèmes
Gérer et mettre en œuvre les mises à jour système
Collecter et mettre à jour les caractéristiques d'un serveur dans l'outil de gestion des configurations
Rédiger ou mettre à jour les documents d'exploitation

Appliquer la politique de la sécurité du système d'information de l'entreprise

Connaissance des spécificités de chaque environnement système
Connaissance des services réseaux
Connaissance des normes et standards relatifs aux échanges sécurisés (authentification, chiffrement)
Connaissance des principes d'une Infrastructure à clés publiques (PKI)
Connaissance des règles de gestion relatives aux licences logicielles

FICHE COMPÉTENCE PROFESSIONNELLE N° 3

Administrer et sécuriser une infrastructure de serveurs virtualisée

Description de la compétence – processus de mise en œuvre

A partir d'un cahier des charges fourni et précisant l'environnement technique, dimensionner et proposer une infrastructure de serveurs dans un environnement de virtualisation et répondant aux niveaux de service attendus (performances, disponibilité, sécurité). Mettre en œuvre, documenter et administrer cette infrastructure de serveurs en tenant compte des contraintes de production et d'exploitation.

Contexte(s) professionnel(s) de mise en œuvre

Cette compétence peut être mobilisée, lors de la définition et de la première mise en œuvre d'une nouvelle infrastructure, lors de l'intégration de nouvelles ressources dans un environnement virtualisé existant, ou lors d'une migration (version d'OS, changement d'hyperviseur ou changement d'hébergeur). La mise en œuvre de l'infrastructure peut imposer certaines contraintes liées à l'intégration dans le système existant ainsi que des possibilités de retour arrière (réversibilité).

Critères de performance

L'environnement de virtualisation est opérationnel et conforme au cahier des charges
L'ensemble du processus de mise en œuvre est réalisé avec méthode
Les recommandations et règles de sécurité spécifiques aux environnements virtualisés sont prises en compte et appliquées
Les délais de réalisation sont conformes au cahier des charges
L'infrastructure est documentée et les procédures d'exploitation sont rédigées de façon claire et opérationnelle
Les logiciels, documents et sources d'information en anglais sont utilisés de façon fiable et sans erreur de compréhension

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Mettre en œuvre la haute disponibilité et la répartition de charge
Migrer des composants de virtualisation d'une technologie à une autre
Administrer l'environnement de virtualisation en ligne de commandes
Administrer les composants de virtualisation à l'aide d'une solution de gestion centralisée
Mettre en œuvre des techniques d'automatisation de déploiement de machines virtuelles
Gérer et mettre en œuvre la mise à jour des composants de virtualisation
Administrer les machines virtuelles et gérer les privilèges
Mettre en œuvre et superviser la sauvegarde et la restauration de l'environnement virtualisé
Diagnostiquer et dépanner un dysfonctionnement en environnement de virtualisation
Maintenir et faire évoluer la documentation technique
Collecter et mettre à jour les caractéristiques d'une infrastructure virtualisée dans l'outil de gestion des configurations

Appliquer la politique de la sécurité du système d'information de l'entreprise

Connaissance des principales solutions de gestion d'environnements virtualisés
Connaissance des fonctions avancées de la gestion des environnements virtualisés (clustering, stockage, migration)
Connaissance des solutions convergentes et/ou hyper-convergentes
Connaissance de l'impact de la virtualisation sur la consommation d'énergie et l'optimisation des équipements

Connaissance des spécificités d'un data center (énergie, refroidissement, réseau, sécurité d'accès)
Connaissance des équipements matériels du cluster (serveurs, baies de stockage, switch)
Connaissance des règles de gestion relatives aux licences logicielles

FICHE COMPÉTENCE PROFESSIONNELLE N° 4

Appliquer les bonnes pratiques et participer à la qualité de service

Description de la compétence – processus de mise en œuvre

Dans le cadre du support à l'exploitation, diagnostiquer les incidents, identifier, classifier, et enregistrer les problèmes afin de minimiser leur impact sur les services fournis en prévenant leur réapparition. A partir d'une demande de changement ou de déploiement, établir des procédures fiables afin de garantir la qualité de la distribution et de l'installation des changements. Tracer les changements matériels et logiciels afin de fournir une information actualisée sur les éléments de configuration de l'infrastructure.

Contexte(s) professionnel(s) de mise en œuvre

Cette compétence est mobilisée lors de la mise en œuvre, de l'évolution ou de la restauration d'un service fourni. Au sens ITIL (Information Technology Infrastructure Library), elle correspond aux principaux processus associés à la gestion des problèmes, la gestion des changements et des mises en production, ainsi que la gestion des actifs et des configurations.
La mise en œuvre de cette compétence est récurrente. Elle repose sur la connaissance des infrastructures informatiques que l'administrateur acquiert au quotidien.

Critères de performance

Les procédures établies sont conformes aux règles de bonne pratique
Les changements matériels et logiciels de l'infrastructure sont documentés, planifiés et testés
Les problèmes sont résolus ou une solution de contournement est validée

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Utiliser un outil de gestion des actifs et des configurations (type GLPI, SCCM, Lansweeper)
Exploiter les données d'un outil de gestion des incidents (type GLPI)
Mettre en œuvre les outils permettant le test et la mesure des indicateurs de performance (outils de benchmark)
Vérifier l'adéquation de la qualité de service mesurée avec les engagements des contrats de service
Mettre en œuvre une démarche structurée de diagnostic
Etablir une procédure de traitement d'incident
Etablir une procédure de mise en production

Prendre en compte les référentiels de bonne pratique ou les normes en vigueur dans les propositions d'amélioration

Connaissance des principes généraux d'ITIL
Connaissance des processus de gestion des incidents et des problèmes
Connaissance du processus de gestion des changements
Connaissance du processus de gestion des actifs et des configurations
Connaissance du processus de gestion des mises en production
Connaissance des principes des accords de niveau de service (SLA)

FICHE COMPÉTENCE PROFESSIONNELLE N° 5

Créer des scripts d'automatisation

Description de la compétence – processus de mise en œuvre

A partir de besoins de traitements récurrents, ou complexes, ou spécifiques, dans un environnement pouvant être hétérogène, adapter ou créer un script et le documenter afin d'automatiser le traitement en garantissant le respect des contraintes de fonctionnement et de sécurité des infrastructures informatiques.

Contexte(s) professionnel(s) de mise en œuvre

L'automatisation de traitement répond à des besoins multiples. Il peut s'agir de créations de comptes dans une architecture distribuée, nécessitant des accès multiples à des services (applications, accès réseau, ressources). Il peut s'agir aussi de tâches répétitives ou non, massives et devant être exécutées rapidement. Le déploiement de ressources telles que des machines virtuelles de l'infrastructure, des modifications de configurations peuvent également faire l'objet d'un traitement automatisé. L'automatisation des traitements nécessite le respect d'une méthodologie rigoureuse afin de ne pas affecter l'environnement.

Critères de performance

Les scripts sont testés, validés et conformes aux attendus
Les scripts sont documentés, diffusables et réutilisables
Les scripts prennent en compte les règles de sécurité
Les logiciels, documents et sources d'information en anglais sont utilisés de façon fiable et sans erreur de compréhension

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Identifier ce qui peut être automatisé
Rechercher un script d'automatisation de tâche et l'adapter à un besoin donné
Créer et documenter des scripts d'automatisation de tâche en utilisant différents langages (ex. : Powershell, shell, python)
Appliquer les bonnes pratiques de sécurité associées au langage utilisé
Utiliser des requêtes de définition et de manipulation de données structurées dans des scripts d'automatisation de tâche.
Intégrer la gestion des erreurs dans un script d'automatisation de tâche
Mettre en place un environnement de test intégrant les contraintes de la production.
Qualifier un script d'automatisation de tâches
Gérer une bibliothèque de scripts

Rédiger et mettre à jour la documentation d'exploitation

Connaissance des langages de script en environnement Windows et Unix/Linux
Connaissance des bases de programmation nécessaires à l'écriture d'un script (principes d'algorithme, variables et structures de contrôle, fonction et procédure avec passage de paramètre, fonction récursive)
Connaissance des structures de données (bases de données, fichier plat, XML)
Connaissance de la méthodologie de qualification d'un script
Connaissances des risques liés à l'exécution des scripts et des règles de sécurisation associées

FICHE COMPÉTENCE PROFESSIONNELLE N° 6

Intégrer et gérer les différents environnements de travail des utilisateurs

Description de la compétence – processus de mise en œuvre

A partir d'un cahier des charges décrivant l'environnement de travail utilisateur et les différents types d'équipements numériques pris en compte par l'entreprise, proposer, mettre en œuvre et maintenir en condition opérationnelle une solution permettant le déploiement et la gestion centralisée des terminaux. Mettre à disposition des utilisateurs les applications, afin de leur fournir leur espace de travail depuis les différents équipements dans le respect des règles de sécurité.

Contexte(s) professionnel(s) de mise en œuvre

Cette compétence est mobilisée lorsque les utilisateurs accèdent aux services et applications mis à leur disposition à travers des équipements numériques de types très différents (postes fixes physiques ou virtualisés, terminaux clients légers, portables, tablettes, smartphones), qui sont fournis par l'entreprise, mais qui peuvent aussi être des équipements personnels de l'utilisateur (BYOD). Dans tous les cas, il est indispensable que ces usages multiples et leur cadre d'emploi soient contrôlés et gérés par l'entreprise, en particulier pour des raisons de sécurité.

Critères de performance

L'environnement de travail de l'utilisateur est conforme au cahier des charges
Les services fournis sont disponibles conformément au niveau requis pour l'ensemble des utilisateurs et des équipements numériques concernés
Les règles de sécurité sont respectées, quel que soit le type d'équipement numérique accédant à l'infrastructure
Les procédures de déploiement sont rédigées de façon claire et opérationnelle
Les logiciels, documents et sources d'information en anglais sont utilisés de façon fiable et sans erreur de compréhension

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Mettre en œuvre les fonctions de la gestion de la mobilité d'entreprise (MDM, MAM, MCM)
Mettre en œuvre un dispositif de gestion et de déploiement de postes de travail physiques et virtuels
Mettre en œuvre différentes méthodes de déploiement d'applications (télédistribution, virtualisation par sessions distantes, packages, conteneurs)
Mettre en œuvre un dispositif de gestion et de déploiement d'applications
Gérer les mises à jour des systèmes et des applications
Mettre en place un environnement de test intégrant les contraintes de la production
Qualifier le déploiement des périphériques et des applications
Intégrer les différents périphériques dans le système de gestion des configurations

Appliquer et faire appliquer les recommandations de sécurité en matière de gestion des périphériques utilisateurs et d'accès aux applications et aux données de l'entreprise

Rédiger et mettre à jour la documentation d'exploitation

Connaissance des principes de la gestion de la mobilité d'entreprise (EMM)
Connaissance des techniques de virtualisation des applications
Connaissance des méthodes de déploiement des applications
Connaissance des techniques de virtualisation des postes de travail
Connaissance des règles de gestion des licences

FICHE COMPÉTENCE PROFESSIONNELLE N° 7

Administrer les services dans une infrastructure distribuée

Description de la compétence – processus de mise en œuvre

A partir d'un cahier des charges, et en tenant compte des interdépendances avec les autres composants du système d'information, mettre en œuvre, administrer et maintenir en condition opérationnelle les applications, plateformes et infrastructures en tant que service (SaaS, PaaS, IaaS) internes ou externalisées selon les termes du contrat de service, afin que les utilisateurs accèdent aux services de façon transparente et homogène, dans le respect des règles de sécurité et des contrats de service.
Assurer l'interface avec les fournisseurs des différents services.

Contexte(s) professionnel(s) de mise en œuvre

Cette compétence est mise en œuvre quand les ressources et les services sont réparties sur différentes infrastructures privées et/ou publiques, chez des fournisseurs qui peuvent être multiples, ou lorsque l'Administrateur d'Infrastructures Sécurisées gère ces ressources pour le compte des clients.
L'Administrateur d'Infrastructures Sécurisées doit s'approprier les fonctionnalités et les différentes interfaces de gestion et d'administration proposées par les fournisseurs, tout en s'assurant du respect des niveaux de service attendus et de la réglementation relative à la gestion des données personnelles. Il peut être amené à dialoguer en anglais avec certains interlocuteurs.

Critères de performance

Les interdépendances entre les composants du système d'information sont prises en compte
L'accès aux services distribués est conforme au niveau requis pour l'ensemble des utilisateurs
Les règles de sécurité sont respectées
Les niveaux de service conclus avec les fournisseurs sont identifiés
Les procédures d'exploitation sont rédigées et mise à jour de façon claire et opérationnelle
Les logiciels, documents et sources d'information en anglais sont utilisés de façon fiable et sans erreur de compréhension
La communication orale en anglais avec le fournisseur ou le support se déroule de façon fiable et autonome

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Intégrer une application hébergée dans le cloud (Saas) dans le système d'information de l'entreprise
Intégrer un élément d'infrastructure hébergé dans le cloud (IaaS) dans le système d'information de l'entreprise
Intégrer une plateforme hébergée dans le cloud (PaaS) dans le système d'information de l'entreprise
Administrer les applications, plateformes et infrastructures hébergées dans le cloud à partir des différentes interfaces graphiques proposées
Administrer les applications, plateformes et infrastructures hébergées dans le cloud à partir de la ligne de commande et de scripts
Mettre en œuvre et administrer le référencement public de services souscrits (DNS)
Mettre en œuvre un système permettant une authentification unique (SSO)
Mettre en œuvre et administrer une infrastructure de cloud hybride
Migrer des services locaux vers le cloud et inversement
Mettre en œuvre et superviser la sauvegarde et la restauration des données
Appliquer les recommandations de sécurité particulières aux infrastructures hybrides et distribuées
Intégrer et référencer les ressources et services dans le système de gestion des actifs et des configurations
Appliquer une démarche structurée de diagnostic dans le contexte d'une infrastructure distribuée
Identifier les possibilités de réversibilité dans la contractualisation des services externalisés

Suivre les « consommations à l'usage »
Appliquer les recommandations de sécurité spécifiques au recours à l'infogérance et aux services externalisés

Rédiger et mettre à jour la documentation d'exploitation
Gérer la relation avec les fournisseurs

Connaissance des architectures applicatives distribuées
Connaissances des principes, des enjeux et des risques du cloud computing
Connaissance des risques inhérents à l'infogérance et à l'externalisation des systèmes d'information
Connaissance des principes de l'authentification unique (centralisation, fédération, coopération)
Connaissances des techniques de virtualisation basées sur les conteneurs

FICHE COMPÉTENCE PROFESSIONNELLE N° 8

Superviser, mesurer les performances et la disponibilité de l'infrastructure et en présenter les résultats

Description de la compétence – processus de mise en œuvre

A partir des contrats de niveaux de service établis, mettre en œuvre les moyens permettant de suivre les indicateurs de performance et de disponibilité. Activer la journalisation des composants les plus importants. Superviser les éléments de l'infrastructure et recueillir les informations issues des outils de la supervision permettant de déclencher les actions correctives et préventives. Présenter les résultats afin d'améliorer la qualité des services fournis.

Contexte(s) professionnel(s) de mise en œuvre

La supervision de l'infrastructure est assurée au quotidien et fait partie des tâches récurrentes. Outre les actions correctives consécutives aux remontées d'alertes, il est également nécessaire de mettre en place une analyse synthétique des résultats de la supervision, afin de les comparer aux niveaux de services contractualisés, et de s'inscrire dans un processus d'amélioration continue.
Au sens ITIL, la mise en œuvre de cette compétence contribue à la gestion des niveaux de service, en lien avec la gestion de la disponibilité.

Critères de performance

Les indicateurs sont pertinents
Les composants importants et critiques de l'infrastructure sont définis
L'action corrective proposée en réponse aux remontées d'informations est pertinente
Les résultats présentés sont structurés et exploitables
Les logiciels, documents et sources d'information en anglais sont utilisés de façon fiable et sans erreur de compréhension

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Définir les éléments de l'infrastructure qui doivent être suivis
Définir les seuils d'alerte et les indicateurs principaux et les mettre en œuvre (configuration)
Définir et mettre en œuvre les moyens à utiliser pour suivre les indicateurs de performance et de disponibilité
Mettre en œuvre et exploiter une solution de supervision dans une infrastructure distribuée
Mettre en œuvre une solution de centralisation des journaux d'événements dans une infrastructure hétérogène
Mettre en œuvre des outils permettant d'analyser les journaux d'événements afin d'alimenter des tableaux de bord et/ou de déclencher des alarmes
Définir et mettre en œuvre une action corrective à partir d'éléments issus de la supervision
Élaborer des tableaux de bord de suivi de production informatique
Appliquer les recommandations en matière de sécurisation des données de supervision et de journalisation

Rédiger et mettre à jour la documentation d'exploitation
Présenter par écrit ou lors d'un exposé les résultats de la production informatique

Connaissance de la gestion des niveaux de services
Connaissance du protocole SNMP
Connaissance du standard WBEM et sa déclinaison WMI
Connaissance du protocole Syslog

Connaissance des protocoles d’analyse de flux réseaux (type Netflow)

FICHE COMPÉTENCE PROFESSIONNELLE N° 9

Proposer une solution informatique répondant à des besoins nouveaux

Description de la compétence – processus de mise en œuvre

A partir de besoins nouveaux, exprimés dans une demande, ou repérés par l'Administrateur d'Infrastructures Sécurisées, et en tenant compte de l'état de l'art et des contraintes budgétaires, proposer une solution technique afin d'ajuster la capacité de l'infrastructure aux évolutions des organisations métiers. Anticiper les changements des services et de l'infrastructure en apportant une solution évolutive. Réaliser l'évaluation et préparer l'intégration de la solution en tenant compte des contraintes de production et de sécurité.

Contexte(s) professionnel(s) de mise en œuvre

Cette compétence est mise en œuvre lors des scénarios d'évolution de l'entreprise, afin de pouvoir proposer des solutions adaptées. Les besoins peuvent être mis en évidence par l'Administrateur d'Infrastructures Sécurisées, par exemple lors de la revue des résultats de la production (supervision). Au sens ITIL, la mise en œuvre de cette compétence fait partie du processus de gestion des capacités et fait appel à la gestion des changements pour la préparation des phases d'intégration, qui s'inscrivent dans une démarche de gestion de projet.

Critères de performance

Le service prévu par la solution est conforme aux besoins et attentes des utilisateurs
Les contraintes budgétaires sont prises en compte
La solution proposée est évolutive
L'évaluation de la solution est réalisée avec méthode
L'intégration proposée est conçue avec méthode et prend en compte les contraintes de production et de sécurité
Les propositions sont présentées de façon claire et structurée
Les documents et sources d'information en anglais sont utilisés de façon fiable et sans erreur de compréhension

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Repérer, tester et évaluer préalablement une solution technique, en réalisant une maquette
Etablir un comparatif entre une solution d'achat, une solution de location et une solution externalisée
Evaluer l'impact de la solution sur le système d'information
Rédiger une proposition de solution argumentée (chiffrage financier compris)
Se tenir informé de l'évolution des techniques et des offres des prestataires, fournisseurs et opérateurs
Sélectionner des équipements conformes au respect des normes environnementales

Définir, évaluer, planifier et ordonnancer les tâches à effectuer pour mener à bien une intégration
Repérer les grandes fonctions de l'entreprise et son fonctionnement

Reformuler la demande de l'utilisateur pour s'assurer de la bonne compréhension du besoin
Argumenter auprès d'un client interne ou externe une proposition de solutions

Connaissance générale de la conception des services
Connaissance générale de la transition des services
Connaissance des méthodes de test et de recette et des principes du Proof of Concept (PoC)
Connaissance d'une méthode de gestion de projet
Connaissance des éléments constitutifs du TCO (Total Cost of Ownership)

Connaissance des notions comptables liées aux investissements (amortissement, mise au rebut d'une immobilisation)

FICHE COMPÉTENCE PROFESSIONNELLE N° 10

Mesurer et analyser le niveau de sécurité de l'infrastructure

Description de la compétence – processus de mise en œuvre

Dans le cadre d'un contrôle régulier, ou à partir d'une demande d'évolution de la sécurité du système d'information, ou en réaction à une attaque, planifier, spécifier les points de contrôle et effectuer les mesures afin de vérifier et évaluer le niveau de sécurité. Fournir un rapport afin de comparer les résultats au référentiel de sécurité de l'entreprise. Participer à une démarche d'analyses de risques afin d'identifier les menaces, les vulnérabilités et la criticité des risques numériques pouvant affecter les composants de l'infrastructure.

Contexte(s) professionnel(s) de mise en œuvre

Cette compétence est mise en œuvre lors de la participation à la gestion des risques, lors des phases de réflexion menées à un niveau davantage technique que fonctionnel.
Dans le cadre d'un audit, généralement réalisé par des spécialistes externes, cette compétence est mobilisée lors de l'exploitation des résultats, sur une partie ou la totalité de l'infrastructure, selon la complexité de celle-ci et en fonction du périmètre défini par la politique de sécurité. L'audit fournit des éléments exploités lors des phases de l'analyse des risques. Quand l'entreprise n'a pas défini de référentiel de sécurité spécifique, l'Administrateur d'Infrastructures Sécurisées peut s'appuyer sur les référentiels génériques proposés par des organismes de référence (ANSSI).

Critères de performance

Les points de contrôle sont pertinents
Les vulnérabilités des composants sont identifiées
Les risques et leurs menaces associées sont caractérisés
Le rapport de mesures est clair et exploitable
Les outils, documents et sources d'information en anglais sont utilisés de façon fiable et sans erreur de compréhension

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Caractériser les types de risques informatiques encourus (intrusion, piratage, malveillance, fraude)
Définir une typologie de menaces
Analyser un scénario de menace
Evaluer un scénario pour une menace
Utiliser une méthode d'évaluation de la sécurité d'accès aux ressources
Réaliser un audit de configuration
Réaliser des tests d'intrusion
Analyser des évènements de sécurité
Réaliser une veille sur les menaces, les failles, vulnérabilités et non conformités à la PSSI

Connaissance du processus de gestion de la sécurité et des principes du PDCA (Plan, Do, Check, Act)
Connaissance des risques informatiques encourus et leurs causes
Connaissance de base sur les organismes et la réglementation relatifs à la protection des données en France et en Europe (CNIL, RGPD)
Connaissance générale d'une méthode de gestion des risques (EBIOS, MEHARI)
Connaissance des principales fonctions d'une supervision de la sécurité
Connaissance des principes d'un SOC (Security Operations Center)

Connaissance des principes du SIEM (Security Information Event Management) et des fonctions associées SIM, SEM (Security Information Management, Security Event Management)

FICHE COMPÉTENCE PROFESSIONNELLE N° 11

Participer à l'élaboration et à la mise en œuvre de la politique de sécurité

Description de la compétence – processus de mise en œuvre

A partir de l'analyse des risques et leur criticité associée, et en fonction des besoins de sécurité de l'entité, contribuer à la définition et à la mise en œuvre des actions de sécurité correspondant aux traitements choisis pour répondre à ces menaces, et à leur suivi. Participer à la définition des procédures permettant d'assurer la continuité et la reprise de l'activité et les mettre en place. Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique, et participer à la mise à niveau des équipes techniques, afin de contribuer à la prise en compte globale de la politique de sécurité.

Contexte(s) professionnel(s) de mise en œuvre

Cette compétence est mise en œuvre lors de la participation à une gestion des risques, lors des phases de traitement des risques, par la définition des mesures de sécurité à appliquer, et au suivi de la réalisation du plan d'action correspondant. Au sens ITIL, la mise en œuvre de cette compétence s'inscrit également dans la gestion de la continuité. L'Administrateur d'Infrastructures Sécurisées peut également être sollicité pour animer ponctuellement des actions de sensibilisation aux risques informatiques et à la sécurité, et éventuellement pour participer à une cellule de crise.

Critères de performance

Les actions proposées répondent aux scénarios de menaces retenus
Le suivi de la mise en œuvre est pris en compte et organisé
Les procédures sont testées et documentées
L'action de sensibilisation est adaptée aux besoins des utilisateurs (niveau de langage et vocabulaire)

Savoir-faire techniques, savoir-faire organisationnels, savoir-faire relationnels, savoirs

Mettre en œuvre une stratégie de sauvegarde, en réaliser les procédures et tester les restaurations
Assurer le suivi des mesures de sécurité mises en œuvre (journalisation, alarmes)
Participer à la configuration d'un dispositif SIEM (définition d'équipements supervisés, de tableaux de bord, d'alertes)
Mettre en œuvre un dispositif de redondance et de répartition de charge

S'approprier le vocabulaire, les techniques et méthodes de l'entreprise et son domaine d'intervention
Réaliser une veille et analyser les offres des prestataires de services de sécurité managés
Définir avec les utilisateurs la politique de sauvegarde

Prendre en compte le niveau de connaissance et les besoins des utilisateurs à sensibiliser ou à former
Animer une action de sensibilisation ou de formation courte

Connaissance des concepts des différents types de plans (Plan de Reprise d'Activité, Plan de Continuité d'Activité, Plan de Continuité Informatique)
Connaissance des principes de haute disponibilité et des systèmes redondants
Connaissance des protocoles de redondance (VRRP, HSRP)

FICHE DES COMPÉTENCES TRANSVERSALES DE L'EMPLOI TYPE

Communiquer par écrit avec les professionnels et les utilisateurs de l'informatique

Description de la compétence – processus de mise en œuvre

Dans le cadre de son activité professionnelle en informatique, être capable de lire et de comprendre des documents, des contrats décrivant des produits et services. Rédiger un courriel, un compte-rendu de réunion, une procédure, en respectant les règles d'orthographe et de grammaire. Réaliser un document de synthèse, une présentation, un argumentaire, un rapport à partir de sources et de données multiples.

Critères de performance

Les documents sont lus sans erreur de compréhension
Les écrits sont rédigés de façon claire et correctement orthographiés
Les écrits sont structurés
La communication écrite est adaptée à l'interlocuteur (niveau de langage et vocabulaire)

Utiliser l'anglais dans son activité professionnelle en informatique

Description de la compétence – processus de mise en œuvre

Installer et utiliser des logiciels sans erreur d'interprétation des consignes et des messages fournis par l'interface ou l'aide en ligne. Comprendre une documentation technique sans contresens. Poser un problème technique ou une question commerciale à l'écrit ou à l'oral auprès des fournisseurs, des éditeurs de logiciels, des constructeurs. Dans le cadre de sa veille technologique, rechercher des informations en anglais sur Internet.

Critères de performance

Les documents techniques en anglais sont exploités sans erreur de compréhension
Les exposés et présentations en ligne en anglais sont écoutés sans erreur de compréhension
Les logiciels en anglais sont utilisés de façon fiable et autonome
Les courriels sont rédigés correctement en anglais
La communication orale avec le fournisseur ou le support se déroule de façon fiable et autonome

Glossaire technique

BYOD

Abréviation de l'anglais « *bring your own device* » (« apportez vos appareils personnels ») ; est une pratique qui consiste à utiliser ses équipements personnels (smartphone, ordinateur portable, tablette) dans un contexte professionnel.
Cette pratique pose des questions relatives à la sécurité de l'information et à la protection des données.

IaaS

Infrastructure as a Service « *C'est un modèle où l'entreprise dispose sur abonnement payant d'une infrastructure informatique (serveurs, stockage, sauvegarde, réseau) qui se trouve physiquement chez le fournisseur. Cela peut représenter pour certaines directions des systèmes d'information (DSI) un moyen de réaliser des économies, principalement en transformant des investissements en contrats de location » (source Wikipedia 5/10/2017)*.
Dans ce modèle, l'administration des serveurs reste à la main de l'entreprise. Seule la gestion du matériel est sous la responsabilité du fournisseur de service.Seule la gestion du matériel est sous la responsabilité du fournisseur de service.

ITIL

Information Technology Infrastructure Library *"ITIL® est un référentiel de bonnes pratiques orienté processus destiné aux organisations informatiques qui délivrent des services complets à ses clients."(Source ITILFrance)*

On-Premise

Les solutions « On-premise » (sur site) s'opposent au modèle « As a Service » dans le sens où elles sont détenues, gérées ou hébergées physiquement par l'entreprise utilisatrice.

PaaS

Platform as a Service : «*est l'un des types de cloud computing, principalement destiné aux entreprises, où l'entreprise cliente maintient les applications proprement dites ; le fournisseur cloud maintient la plate-forme d'exécution de ces applications » (source Wikipedia 5/10/2017)*
La plateforme comprend le matériel, le système d'exploitation le réseau et le stockage.

PoC

Proof of concept : il s'agit de créer un environnement de test permettant de reproduire l'environnement de production dans le but de tester une nouvelle application ou une mise à jour.

SaaS

Software as a Service : *« est un modèle d'exploitation commerciale des logiciels dans lequel ceux-ci sont installés sur des serveurs distants plutôt que sur la machine de l'utilisateur. Les clients ne paient pas de licence d'utilisation pour une version, mais utilisent librement le service en ligne ou, plus généralement, payent un abonnement. » (source Wikipedia 5/10/2017)*

Glossaire du REAC

Activité type

Une activité type est un bloc de compétences qui résulte de l'agrégation de tâches (ce qu'il y a à faire dans l'emploi) dont les missions et finalités sont suffisamment proches pour être regroupées. Elle renvoie au certificat de compétences professionnelles (CCP).

Activité type d'extension

Une activité type d'extension est un bloc de compétences qui résulte de l'agrégation de tâches qui constituent un domaine d'action ou d'intervention élargi de l'emploi type. On la rencontre seulement dans certaines déclinaisons de l'emploi type. Cette activité n'est pas dans tous les TP. Quand elle est présente, elle est attachée à un ou des TP. Elle renvoie au certificat complémentaire de spécialisation (CCS).

Compétence professionnelle

La compétence professionnelle se traduit par une capacité à combiner un ensemble de savoirs, savoir faire, comportements, conduites, procédures, type de raisonnement, en vue de réaliser une tâche ou une activité. Elle a toujours une finalité professionnelle. Le résultat de sa mise en œuvre est évaluable.

Compétence transversale

La compétence transversale désigne une compétence générique commune aux diverses situations professionnelles de l'emploi type. Parmi les compétences transversales, on peut recenser les compétences correspondant :

- à des savoirs de base,
- à des attitudes comportementales et/ou organisationnelles.

Critère de performance

Un critère de performance sert à porter un jugement d'appréciation sur un objet en termes de résultat(s) attendu(s) : il revêt des aspects qualitatifs et/ou quantitatifs.

Emploi type

L'emploi type est un modèle d'emploi représentatif d'un ensemble d'emplois réels suffisamment proches, en termes de mission, de contenu et d'activités effectuées, pour être regroupées : il s'agit donc d'une modélisation, résultante d'une agrégation critique des emplois.

Référentiel d'Emploi, Activités et Compétences (REAC)

Le REAC est un document public à caractère règlementaire (visé par l'arrêté du titre professionnel) qui s'applique aux titres professionnels du ministère chargé de l'emploi. Il décrit les repères pour une représentation concrète du métier et des compétences qui sont regroupées en activités dans un but de certification.

Savoir

Un savoir est une connaissance mobilisée dans la mise en œuvre de la compétence professionnelle ainsi qu'un processus cognitif impliqué dans la mise en œuvre de ce savoir.

Savoir-faire organisationnel

C'est un savoir et un savoir faire de l'organisation et du contexte impliqués dans la mise en œuvre de l'activité professionnelle pour une ou plusieurs personnes.

Savoir-faire relationnel

C'est un savoir comportemental et relationnel qui identifie toutes les interactions socioprofessionnelles réalisées dans la mise en œuvre de la compétence professionnelle pour une personne. Il s'agit d'identifier si la relation s'exerce : à côté de (sous la forme d'échange d'informations) ou en face de (sous la forme de négociation) ou avec (sous la forme de travail en équipe ou en partenariat etc.).

Savoir-faire technique

Le savoir-faire technique est le savoir procéder, savoir opérer à mobiliser en utilisant une technique dans la mise en œuvre de la compétence professionnelle ainsi que les processus cognitifs impliqués dans la mise en œuvre de ce savoir-faire.

Titre professionnel

La certification professionnelle délivrée par le ministre chargé de l'emploi est appelée « titre professionnel ». Ce titre atteste que son titulaire maîtrise les compétences, aptitudes et connaissances permettant l'exercice d'activités professionnelles qualifiées. (Article R338-1 et suivants du Code de l'Education).