## 1.1. Environnement de travail

*Le technicien de maintenance des systèmes informatiques intervient dans tous types de secteurs (Primaire, Secondaire ou Tertiaire). De nombreuses entreprises disposent d'un service informatique composées à minima d'un technicien de maintenance. Celles qui ne disposent pas de ce service spécifique font appel à une entreprise de service du numérique.*

*Il travaille seul ou en équipe et possède un espace de travail composé d'un bureau équipé d'un ou plusieurs ordinateurs accompagnés de leurs périphériques (imprimantes, scanner, équipements de communications pour la téléphonie et la visioconférence). Il réalise ses activités sur site ou à distance.*

*Il utilise des outils de diagnostic (logiciels) pour tester un poste de travail informatique (in situ ou à distance) et des outils à mains (tournevis, clés…) pour démonter et remonter des ordinateurs ou périphériques.*

*Ses interventions doivent respecter la réglementation, les normes (ISO/CEI 27001 : 2013) et standards de qualité et de sécurité en vigueur, les contrats de services conclus avec l'organisation cliente et s'inscrit dans une démarche écoresponsable en participant à la réduction de l'impact de l'informatique sur l'environnement.*

*L'adoption de normes et standards a pour but de garantir la pérennité et la sécurité des solutions technologiques choisies par les organisations. La connaissance de ces normes et standards, de leurs avantages et inconvénients, permet d'éclairer les décisions d'une organisation et contribue à l'amélioration permanente de la qualité, de la sécurité et de la productivité des communications et des échanges.*

*Les règles juridiques nationales, européennes et internationales sont de plus en plus prégnantes. Sources de contraintes mais aussi d'opportunités, elles doivent être intégrées dans l'exercice du métier et prises en compte dans les choix techniques et organisationnels afin qu'ils soient conformes à la réglementation en vigueur.*

*Ainsi l'entrée en application le 25 mai 2018 du règlement européen sur la protection des données renforce la responsabilité des organisations. Elles doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité, ce qui influe sur la conception des services informatiques.*

## 1.2. Interactions dans l'environnement de travail

*Le technicien de maintenance des systèmes informatiques agit sous la responsabilité du Directeur des SI, du Responsable ou du Chef de projet informatique en fonction de la typologie de l'entreprise.*

*Il organise son travail et collabore avec d'autres salariés du prestataire informatique et de l'organisation cliente, le plus souvent au sein d'une équipe. Il exerce ses missions dans le respect de la satisfaction des besoins des utilisateurs, de la politique de l'organisation et de la réglementation en vigueur, en faisant preuve d'éthique professionnelle.*

*S'il exerce son métier le plus souvent en tant que salarié d'une organisation, le développement de l'entrepreneuriat l'amène à choisir de nouveaux statuts (autoentrepreneur, intérim, etc…)*

*Dans l'ensemble de ses activités, le technicien de maintenance en systèmes informatiques dispose d'une autonomie et d'un champ de délégation qui peuvent varier selon la nature du prestataire informatique qui l'emploie. Son niveau de responsabilité peut donc s'enrichir au fil de son parcours professionnel.*

*Sachant faire preuve d'initiative, il communique en permanence avec les autres membres de l'équipe projet dans le cadre d'un travail collaboratif et rend compte régulièrement à son responsable hiérarchique ou fonctionnel. Il l'alerte sur les événements susceptibles d'induire des risques nouveaux pour les systèmes informatiques.*

*Le technicien de maintenance des SI multiplie les contacts et interactions dans son entreprise ou son organisation, il dialogue avec les utilisateurs à chaque étape de ses activités, du déploiement logiciel ou matériel à la sensibilisation ou l'information technique pour garantir la continuité du service informatique.*

| **REFERENTIEL D'ACTIVITES**<br>*décrit les situations de travail et les activités exercées, les métiers ou emplois visés* | **REFERENTIEL DE COMPETENCES**<br>*identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités* | **REFERENTIEL D'EVALUATION**<br>*définit les critères et les modalités d'évaluation des acquis* | |
|---|---|---|---|
| | | **MODALITÉS D'ÉVALUATION** | **CRITÈRES D'ÉVALUATION** |
| **1. Le déploiement des matériels et des services informatiques**<br><br>Cette activité consiste à déployer de nouveaux équipements informatiques à destination des utilisateurs (installation d'un poste de travail (nouvel arrivant), d'un périphérique utilisateur (imprimante, scanner…)) ou de nouveaux équipements de structure (routeur, borne wifi, serveur…) et de les intégrer au système informatique de l'entreprise. Cette activité vise également à déployer les services informatiques (logiciels utilisateurs (Windows, serveur d'impression…)). Une installation de matériel et de logiciel est donc à réaliser.<br><br>L'intervention tient compte de la disponibilité du matériel et des logiciels à installer, et en prenant soin de perturber au minimum l'activité des utilisateurs. L'installation de matériels doit respecter les préconisations du fabriquant via une notice d'installation, généralement en anglais. On y trouve éventuellement la phase de montage mécanique, la phase de raccordement au secteur et au réseau informatique et la phase de configuration du matériel.<br><br>La phase de montage est limitée à la fixation mécanique des équipements (dans un ordinateur, dans des baies de câblage, sur des murs…). Au niveau del'utilisateur, le raccordement électrique des équipements au réseau informatique est principalement réalisé par des liaisons de câbles | **1 Installer et configurer des matériels informatiques**<br><br>A partir d'un ordre de travail précisant le lieu de leurs installations et la date de l'intervention, des matériels à installer (Ordinateur, imprimante, scanner, cartes électroniques, mémoires, borne wifi, switch…), de la notice d'installation et de configuration du fabriquant, de l'outil de suivi des configurations. Le technicien de maintenance, après avoir débrancher les appareils ou coupé l'électricité au niveau du tableau électrique, démonte des éléments du système informatique pour pouvoir intégrer le matériel à installer, puis remonte le système informatique pour configurer le nouveau matériel. Enfin il réalise les tests pour garantir son bon fonctionnement. | L'UIMM territoriale centre d'examen définit les modalités d'évaluation en concertation avec l'entreprise et les acteurs concernés (entreprise, candidats, UIMM Territoriale...). Cette évaluation sera complétée par l'avis de l'entreprise.<br><br>Modalités d'évaluation :<br><br>- Evaluation en situation professionnelle réelle<br>Ou<br>- Présentation des projets ou activités réalisés en milieu professionnel<br>Ou<br>- Evaluation à partir d'une situation professionnelle reconstituée<br>Et<br>- Avis de l'entreprise | **<u>En matière de méthodes utilisées :</u>**<br><br>L'ordre de travail est compris et les matériels ((Ordinateur, imprimante, scanner, cartes électroniques, mémoires, borne wifi, switch…) à installer sont identifiés.<br>Les délais d'approvisionnement sont acceptables pour assurer la disponibilité des matériels auprès des utilisateurs.<br>La disponibilité du matériel à installer est vérifiée. La présence des constituants se trouvant dans l'emballage du matériel informatique (visseries, câbles, cartes…) est vérifié aux regards de la notice d'installation. L'inventaire informatique des matériels et logiciels est mis à jour, une fois le ou les matériels retirés du stock.<br>L'intervention est programmée afin de perturber le moins possible le ou les utilisateurs.<br>L'emplacement du matériel à installer est identifié (ordinateur, baies de brassage, bureau, salle informatique…).<br>Le ou les matériels informatiques sont montés et fixés mécaniquement (dans un ordinateur, dans des baies de câblage, sur des murs …).<br>Le raccordement du matériel informatique est réalisé en respectant la notice d'installation du fabriquant. Les interconnexions câblées ou sans fil et les dispositifs de jonction et de partage sont testés et opérationnelles.<br>L'installation et la configuration des pilotes des matériels informatiques sont réalisés de manière à connecter un poste de travail aux différents serveurs centralisés.<br>Un paramétrage fonctionnel et le test du matériel informatique installé est réalisé.<br>Les tests de communications du poste avec les serveurs et les matériels d'interconnexion sont réalisés pour valider l'installation et la configuration du nouveau matériel informatique.<br><br>L'outil de suivi des configurations est mis à jour.<br><br>**<u>En matière de moyens utilisés :</u>**<br><br>Les outils de montages sont utilisés conformément à leur fonction.<br>L'application permettant de configurer le matériel informatique (déclaration des paramètres réseaux en fonction des caractéristiques du réseau, adressage IP, administration des matériels d'interconnexion : switches, routeurs …) est identifié.<br><br>L'outil d'inventaire et de gestion du parc informatique de l'entreprise est utilisé pour référencer tous les matériels informatiques (ordinateurs, imprimantes, disques durs, casques audio…).<br><br>**<u>En matière de liens professionnels / relationnels :</u>**<br><br>En cas d'indisponibilité des matériels dans le stock de l'entreprise ou de constituants incomplet dans un emballage, une alerte est réalisée respectant les consignes et/ou procédures de l'entreprise. Les utilisateurs sont informés de l'intervention.<br>La maîtrise de l'anglais est caractérisée au minimum :<br>• par la compréhension des points essentiels de notes techniques ;<br>• en prenant part sans préparation à une conversation technique et en articulant des expressions techniques de manière simple en donnant des raisons et des opinions sur le réseau informatique de l'entreprise ; |

| | | | |
|---|---|---|---|
| à paires torsadés (appelé aussi câble informatique), mais il peut être aussi réalisé par des câbles à fibre optique. Dans la salle informatique, les liaisons sont généralement réalisées par des jarretières (paire de fils en cuivre), et par des câbles informatiques équipés de connecteurs RJ45 à chaque extrémité. La phase de configuration permet, via une application logiciel fourni par le fabriquant, de paramétrer l'équipement informatique afin de l'intégrer au réseau de l'entreprise puis de vérifier qu'il soit reconnu par les autres équipements du réseau avec lesquelles il sera en communication.<br><br>L'installation des services informatiques logiciels permet à un utilisateur d'utiliser des applications (pack office, logiciels de systèmes de gestion et de maintenance, anti-virus, boite mails, logiciel interne à l'entreprise (ERP)…) à partir de son ordinateur. Ces applications étant essentielles à l'utilisateur pour réaliser les différentes tâches relatives à son poste de travail.<br><br>Cette installation est réalisée via le lancement d'une application d'installation se trouvant sur un support mémoire (généralement un CD-ROM ou DVD, clé USB…) ou en le téléchargeant, préalablement, du serveur réseau de l'entrepriseou d'un site internet. Pour exécuter l'installation d'une application sur un ordinateur, la procession d'un code (numéro de licence) est généralement demandée. L'exécution de cette installation suit une série d'étapes, qui varie en fonction de l'application. L'application installée, une configuration du système informatique dans sa globalité est nécessaire (création de compte et mot de passe, paramétrage des droits d'accès utilisateurs (réseau internet, WIFI, configuration du | | | en écrivant un texte simple et cohérent sur un sujet relatif la modification du réseau informatique de l'entreprise.<br><br>**<u>En matière de contraintes liées au milieu et environnement de travail :</u>**<br><br>Les demandes des utilisateurs sont recueillies et orienté afin de les traiter dans les meilleurs délais tout en prenant en<br>compte les contraintes (période et durée d'intervention, coût des équipements à installer…) définies par l'entreprise.<br>Lors de l'installation les risques électriques sont pris en comptes.<br>Les utilisateurs sont conseillés et formés à l'utilisation des outils informatiques nouvellement installés ;<br><br>**<u>En matière de résultats</u>**<br><br>Les matériels informatiques sont installés dans le respect des préconisations du fabriquant et connectés au réseau informatique de l'entreprise.<br><br>La configuration des matériels informatiques permet leurs intégrations opérationnelles dans le réseau informatique de l'entreprise.<br><br>Les délais d'installation sont respectés. |

| | | | |
|---|---|---|---|
| VPN, accès aux données répertoires du réseau de l'entreprise)), pour permettre aux utilisateurs de bénéficier des ressources informatiques de l'entreprise ou de l'organisation. | | | |

| | | | |
|---|---|---|---|
| | **2** Erreur ! Source du renvoi introuvable.<br><br>A partir d'un ordre de travail précisant la date de l'intervention, des logiciels à installer (d'un accès à l'ordinateur (l'intervention pouvant réalisée In Situ ou en distanciel), des logiciels à installer (pack office, logiciels de systèmes de gestion et de maintenance, serveur d'impression, boite mails, logiciel interne à l'entreprise (ERP)…), des numéros de licence. Le technicien de maintenance intervient In Situ ou en distanciel sur un système informatique afin d'y installer un nouveau service informatique logiciel en utilisant ou demandant les codes d'accès qui lui sont nécessaires. Le service informatique logiciel étant installé sur le système informatique, le technicien le configure et vérifie son bon paramétrage. | L'UIMM territoriale centre d'examen définit les modalités d'évaluation en concertation avec l'entreprise et les acteurs concernés (entreprise, candidats, UIMM Territoriale...).<br>Cette évaluation sera complétée par l'avis de l'entreprise.<br><br>Modalités d'évaluation :<br><br>Evaluation en situation professionnelle réelle<br>Ou<br>Présentation des projets ou activités réalisés en milieu professionnel<br>Ou<br>Evaluation à partir d'une situation professionnelle reconstituée<br>Et<br>- Avis de l'entreprise | **<u>En matière de méthodes utilisées :</u>**<br><br>La configuration de l'ordinateur recevant le futur service informatique (ERP, service de gestion ou de supervision du réseau informatique…) nécessaires à l'utilisateur est vérifiée et permet son installation.<br>La disponibilité de la licence du logiciel à installer (bureautique, de communication, les applications collaboratives du site informatique, métier, antivirus…) est vérifiée.<br>Le système d'exploitation serveur est mis à jour pour permettre l'installation du service informatique.<br>L'installation et la configuration sont réalisées avec méthode dans le respect des procédures (gestion des configurations).<br>Les droits d'accès aux services sont configurés dans le respect de la stratégie de sécurité de l'entreprise.<br>Les différents services réseaux des serveurs (étendue d'adresses IP, durée du bail de location d'adresse, etc.) sont<br>paramétrés.<br>Les tests de validation de l'installation du logiciel sont effectués.<br><br>L'outil de suivi des configurations est mis à jour.<br><br>**<u>En matière de moyens utilisés :</u>**<br><br>Le support numérique stockant le logiciel à installer est disponible.<br>L'outil de gestion de maintenance assistée par ordinateur (GMAO) et/ou un logiciel de prise en main à distance (PMAD) est exploité pour intervenir en distanciel.<br><br>Les codes (Logging) d'accès pour se connecter sur le poste informatique de l'utilisateur ou sur réseau sont demandés.<br><br>**<u>En matière de liens professionnels / relationnels :</u>**<br><br>En cas d'indisponibilité des logiciels ou d'absence de licence logiciel une alerte est réalisée respectant les consignes et/ou<br>procédures de l'entreprise.<br>Les utilisateurs sont informés de l'intervention.<br>La modification réalisée sur le poste de travail de l'utilisateur est expliquée dans un langage courant lui permettant de la comprendre.<br>La maîtrise de l'anglais est caractérisée au minimum :<br>• par la compréhension des points essentiels de notes techniques ;<br>• en prenant part sans préparation à une conversation technique et en articulant des expressions techniques de manière<br>simple en donnant des raisons et des opinions sur le réseau informatique de l'entreprise ;<br><br>en écrivant un texte simple et cohérent sur un sujet relatif la modification du réseau informatique de l'entreprise. |

| | | | |
|---|---|---|---|
| | | | **<u>En matière de contraintes liées au milieu et environnement de travail :</u>**<br><br>Les outils collaboratifs de travail à distance sont Installés et paramétrés.<br><br>La conformité de l'installation de la conformité et du fonctionnement est contrôlée. |
| | | | **<u>En matière de résultats</u>**<br><br>Le logiciel est installé sur l'ordinateur de l'utilisateur.<br><br>Sa configuration permet l'accès au service informatique de l'entreprise alloués à l'utilisateur dans le respect de la stratégie de sécurité de l'entreprise.<br><br>Les délais d'installation et de configuration sont respectés. |
| **2 Le maintien en condition opérationnelle (MCO) du Système Informatique de l'entreprise**<br><br>Cette activité consiste à intervenir pour donner suite à un dysfonctionnement dusystème informatique déclaré par un utilisateur ou par l'intermédiaire d'une alerte logiciel, et pour anticiper les pertes de données en réalisant des sauvegardes des données des utilisateurs et du système. Cette activité consiste également à réaliserla mise à jour des logiciels.<br><br>Pour intervenir à la suite d'un dysfonctionnement, un diagnostic est réalisé en s'appuyant sur l'historique des pannes, un questionnement structuré et adapté versles utilisateurs, et une série de tests et de contrôles. Un diagnostic précis facilitera l'analyse du dysfonctionnement. L'intervention s'organise en prenant en compte la disponibilité dans le stock du service de l'entreprise des matériels informatiques et/ou logiciels, et en veillant à perturber le moins possible l'activité du ou des utilisateurs du système informatique. Lors du changement du matériel via le | **1 Remettre en état le système informatique**<br><br>Le maintien en condition opérationnelle porte sur les problèmes liés à l'utilisation courante des outils informatiques mis à la disposition des utilisateurs, tant sur le plan matériel que logiciel. A partir d'une demande d'utilisateurs constatant un dysfonctionnement, d'une remontée d'alarme ou d'indicateur quand le réseau est supervisé par un outil d'administration, de l'historique de maintenance du réseau informatique de l'entreprise, des messages d'erreur et des journaux, de l'outil de gestion des tickets, des fiches de procédure de résolution d'incident et du rapport périodique applicables dans l'entreprise, le technicien de maintenance analyse le dysfonctionnement en reposant sur une méthode et une collecte d'information structurées qui permet de conduire de manière logique à l'identification du dysfonctionnement. Ce dysfonctionnement peut provenir d'un matériel d'un système informatique ou d'un service informatique logiciel, il réalisera alors le remplacement du matériels et/ou l'installation du service informatique et réalisera leurs paramétrages. Les tests et contrôles sont réalisés et le rapport périodique contenant les mesures et statistiques des incidents informatiques est mis à jour. | L'UIMM territoriale centre d'examen définit les modalités d'évaluation en concertation avec l'entreprise et les acteurs concernés (entreprise, candidats, UIMM Territoriale...). Cette évaluation sera complétée par l'avis de l'entreprise.<br><br>Modalités d'évaluation :<br><br>- Evaluation en situation professionnelle réelle<br>Ou<br>- Présentation des projets ou activités réalisés en milieu professionnel<br>Ou<br>- Evaluation à partir d'une situation professionnelle reconstituée<br>Et<br>- Avis de l'entreprise | **<u>En matière de méthodes utilisées :</u>**<br><br>Les demandes des utilisateurs sont recueillies et orientées afin de les traiter dans les meilleurs délais. Les historiques de maintenance sont pris en compte.<br>La problématique de ou des utilisateurs en fonction de typologies spécifiques (logicielle, matérielle, manipulation, etc.) est identifiée.<br>L'opération de maintenance est organisée (planification, gestion des priorités…) et doit perturber le moins possible le ou les utilisateurs.<br>Les éléments constitutifs du parc informatique (matériels, pc, serveurs, etc.) est connue ainsi que leurs géolocalisations. L'analyse du dysfonctionnement repose sur une méthode et une collecte d'information structurées qui permet de conduire de manière logique à l'identification du dysfonctionnement :<br>- Sur le plan fonctionnel (panne totale : ex. poste informatique ne démarrant plus, ou une panne partielle : ex. impossibilité d'accéder au réseau de l'entreprise) ;<br>- Sur le plan matériel (écran, clavier, imprimante…).<br>Les matériels informatiques, les sous-ensembles ou applications défectueux sont identifiés.<br>Les délais d'approvisionnement sont acceptables pour assurer la disponibilité des matériels auprès des utilisateurs.<br>La disponibilité du matériel à installer est vérifiée. La présence des constituants se trouvant dans l'emballage du matériel informatique (visseries, câbles, cartes…) est vérifié aux regards de la notice d'installation. L'inventaire informatique des matériels et logiciels est mis à jour, une fois le ou les matériels retirés du stock.<br>Le démontage et le remontage des matériels informatiques ou la suppression et l'installation d'application sont réalisés méthodiquement conformément aux notices techniques.<br>Les opérations de tests et de contrôles sont réalisées.<br>Le recyclage des matériels usés, anciens ou défectueux et qui ont été remplacés est pris en compte. Les fiches de procédure de résolution de nouveaux incidents sont rédigées.<br><br>Le rapport périodique contenant les mesures et statistiques des incidents informatiques est mis à jour. |

| | | | |
|---|---|---|---|
| démontage/remontage du matériel en panne et/ou de la réinstallation/configuration du logiciel, des tests et contrôles sont réalisés pour vérifier que les fonctionnalités du matériel ou du logiciel sont rétablies de manières à garantir la continuité des services informatiques. Un rapport est ensuite rédigé pour tracer l'intervention réalisée.<br><br>La sauvegarde des données préserve l'activité de l'entreprise, notamment en cas de défaillance du système informatique (casse d'un ordinateur, casse d'un matériel de structure informatique, suppression involontaire de fichier ou à la suite d'une cyberattaque…). Elle permet aussi d'éviter les pertes financières liées à la disparition de fichiers ou d'applications sensibles (base de données clients, rapports financiers, etc.). La sauvegarde des données se trouvant dans les disques durs ou dans le Cloud sécurisé est réalisé de manière synchrone (programmation régulière à un jour et une heure fixe par exemple) ou asynchrone (à la demande d'un utilisateur ou lors d'une mise en place d'un nouveau service informatique dans l'entreprise).<br><br>Les mises à jour sont réalisées lors d'une maintenance évolutive logicielle, elles sont essentielles dans la protection des appareils et dans l'amélioration des systèmes informatiques afin de garantir la pérennité du système informatique de l'entreprise ou de l'organisation. Elles réparent les erreurs et réduisent les failles de sécurité. Ces mises à jour améliorent ainsi les logiciels installés en leurs apportant de nouvelles fonctionnalités, un nouveau design, et une meilleure ergonomie. Elles sont réalisées, généralement, en temps masqué à une fréquence usuelle ou annuelle et se lance automatiquement lors du démarrage de l'ordinateur. Les mises à jour sont renseignées dans l'outil de suivi des configurations pour garder une traçabilité. | | | **<u>En matière de moyens utilisés :</u>**<br><br>Les algorithmes simples sont utilisés.<br>L'outillage de contrôle et les logiciels d'administration réseau utilisés sont adaptés aux interventions réalisées.<br>L'outil de gestion de maintenance assistée par ordinateur (GMAO) et/ou un logiciel de prise en main à distance (PMAD) est exploité pour intervenir en distanciel.<br><br>L'enregistrement de ces activités (tickets d'incidents) est réalisé en utilisant l'application définie par le service informatique.<br><br>**<u>En matière de liens professionnels / relationnels :</u>**<br><br>La communication est adaptée à l'interlocuteur (niveau de langage et vocabulaire). Et suit un processus de questionnement logique.<br>Le dysfonctionnement et les opérations de maintenance sont exprimés de manière synthétique, précise et exhaustive aux utilisateurs.<br>En cas d'incidents complexes ou non résolus, des spécialistes (support technique) sont identifiés et contactés.<br>Les utilisateurs sont informés et conseillés dans le but de les rendre autonome sur l'utilisation des ressources informatiques de l'entreprise.<br><br>**<u>En matière de contraintes liées au milieu et environnement de travail :</u>**<br><br>Les délais d'intervention sont conformes aux attentes des utilisateurs.<br>Le délai d'approvisionnement des matériels à remplacer sont transmis auprès des utilisateurs.<br>La priorisation des opérations de maintenance (importance du dysfonctionnement, gestion du temps, des déplacements, délai d'approvisionnement ...) est réalisée en fonction de leur degré de criticité (impact individuel/collectif, ponctuel ou récurrent…).<br>Les stocks de remplacement des matériels défectueux et des consommables sont gérés en intégrant une démarche de développement durable. |

| | | | |
|---|---|---|---|
| | | | |
| | | | **<u>En matière de résultats</u>**<br><br>Les fonctionnalités, initialement défaillantes, du système informatique sont rétablies de manière àgarantir la continuité de service.<br><br>La note de synthèse de l'intervention est rédigée.<br><br>Les délais d'intervention sont respectés. |
| | **2 Réaliser la maintenance préventive du système informatique**<br><br>La maintenance préventive du système informatique est limitée à la sauvegarde des données et de la mise à jour des services informatiques. Pour cela le technicien doit créer les images informatiques du contenu des ordinateurs et les sauvegarder dans un espace sécurisé. Il doit sauvegarder ces données périodiquement de manière synchrone ou asynchrone. Il applique également le processus de déploiement et d'administration des mises à jour et évolutions du système d'exploitation et logiciel. | L'UIMM territoriale centre d'examen définit les modalités d'évaluation en concertation avec l'entreprise et les acteurs concernés (entreprise, candidats, UIMM Territoriale...). Cette évaluation sera complétée par l'avis de l'entreprise.<br><br>Modalités d'évaluation :<br><br>- Evaluation en situation professionnelle réelle<br>Ou<br>- Présentation des projets ou activités réalisés en milieu professionnel<br>Ou<br>- Evaluation à partir d'une situation professionnelle reconstituée<br>Et<br>- Avis de l'entreprise | **<u>En matière de méthodes utilisées :</u>**<br><br>L'image informatique du contenu de l'ordinateur (Master) de l'utilisateur est créée.<br>Les paramètres de configuration sont sauvegardés dans un espace sécurisé.<br>Les sauvegardes périodiques automatiques des données contenues sur les postes de travail et les serveurs sont programmés de manière synchrone ou asynchrone.<br>Les processus de déploiement et d'administration des mises à jour et d'évolutions (physiques, logiques) du système<br>d'exploitation et logiciels utilisés sont appliquées.<br>Les outils permettant d'automatiser les tâches de maintenance (mise à jour et déploiement d'application, création en masse de comptes ou de dossiers…) sont développés.<br>L'historique des mises à jour sont répertoriées dans l'outil de suivi des configurations. |
| | | | **<u>En matière de moyens utilisés :</u>**<br><br>L'outillage de contrôle et les logiciels d'administration réseau utilisés sont adaptés aux interventions réalisées.<br>L'outil de gestion de maintenance assistée par ordinateur (GMAO) et/ou un logiciel de prise en main à distance (PMAD) est exploité pour intervenir en distanciel.<br>L'enregistrement de ces activités (tickets d'incidents) est réalisé en utilisant l'application définie par le service informatique. |
| | | | **<u>En matière de liens professionnels / relationnels :</u>**<br><br>Les utilisateurs sont informés de l'intervention susceptible de perturber ou d'interrompre l'utilisation habituelle des moyens informatiques.<br>La communication est adaptée à l'interlocuteur (niveau de langage et vocabulaire).<br>Les opérations de maintenance préventives sont exprimées de manières synthétiques, précises et exhaustives. Les utilisateurs sont conseillés en s'assurant que les objectifs de l'assistance ont été atteints. |

| | | | |
|---|---|---|---|
| | | | **<u>En matière de contraintes liées au milieu et environnement de travail :</u>**<br><br>Les délais d'intervention sont conformes aux attentes des utilisateurs.<br>La priorisation des opérations de mise à jour est réalisée en fonction de leur degré de criticité (impact individuel/collectif, ponctuel ou récurrent…). |

| | | | |
|---|---|---|---|
| | | | **<u>En matière de résultats</u>**<br><br>Les données utilisateurs ainsi que celles dusystème informatique de l'entreprise sont sauvegardés.<br><br>L'actualisation des mises à jour garanti, aux utilisateurs, l'optimisation des ressources informatiques.<br><br>La continuité du service informatique de l'entreprise est garantie. |
| **3. Le maintien en condition de sécurité (MCS) du Système Informatique de l'entreprise**<br><br>Cette activité consiste à réaliser le déploiement de correctifs de sécurité du système informatique (SI) de l'entreprise, à accompagner et à vérifier l'application de mesures de sécurité des systèmes informatiques de l'entreprise et à traiter les incidents de sécurité.<br><br>L'identification des personnes légitimes à accéder à telles ou telles données permet d'attribuer les droits d'accès afin de garantir la confidentialité des données se trouvant dans les systèmes informatiques (copie de fichiers, transmission par mail, accès à des répertoires, stockage des données…). Ces droits sont gérés/affectés dans le service centralisé d'identification et d'authentification de l'entreprise et respect le règlement général sur la protection des données. Enfin les conditions de sécurité doivent permettre d'assurer les utilisateurs que les données disponibles sont garanties, c'est-à-dire fiables et accessibles aux utilisateurs dans des temps acceptables.<br><br>Les utilisateurs des systèmes informatiques sont, dès que possible, sensibilisés aux règles de sécurité relatives aux ressources informatique de l'entreprise (les règles et consignes de sécurité régissant l'activité quotidienne, les réglementations et obligations légales, l'utilisation des moyens disponibles et participant à la sécurité du | **1 Garantir la confidentialité, l'intégrité et la disponibilité des services informatiques**<br><br>Pour garantir la confidentialité, l'intégrité et la disponibilité des services informatiques, le technicien de maintenance doit identifier la stratégie de sécurité informatique de l'entreprise et le degré de criticité pour chacune des ressources du système informatique. Il caractérise les risques informatiques (intrusion, piratage, malveillance, fraude) et déploie régulièrement les correctifs de sécurité ainsi que les outils de prévention. Ce déploiement passe par la gestion des droits d'accès aux différents services informatiques de l'entreprise utilisateur par utilisateur. | L'UIMM territoriale centre d'examen définit les modalités d'évaluation en concertation avec l'entreprise et les acteurs concernés (entreprise, candidats, UIMM Territoriale...). Cette évaluation sera complétée par l'avis de l'entreprise.<br><br>Modalités d'évaluation :<br><br>- Evaluation en situation professionnelle réelle<br>Ou<br>- Présentation des projets ou activités réalisés en milieu professionnel<br>Ou<br>- Evaluation à partir d'une situation professionnelle reconstituée<br>Et<br>- Avis de l'entreprise | **<u>En matière de méthodes utilisées :</u>**<br><br>La stratégie de sécurité informatique de l'entreprise et le degré de criticité de chacune des ressources du système informatique sont identifiés, afin de leur appliquer les mesures de sécurité physique et logique adaptées.<br>Les types de risques informatiques encourus (intrusion, piratage, malveillance, fraude) sont caractérisés. Le déploiement de correctifs de sécurité du système informatique est réalisé.<br>Les outils de prévention sont mis en place pour garantir la protection physique d'accès aux équipements (salle, baies et postes sécurisés).<br>Les logs des tentatives d'intrusion sont analysés.<br>Le suivi des ressources liées à la sécurité est assuré.<br><br>**<u>En matière de moyens utilisés :</u>**<br><br>Les outils de protection du système informatique sont identifiés (Pare-feu, Antivirus, UTM (Unified Threat Management) …)<br>Les outils de test sont utilisés de manière appropriée.<br><br>**<u>En matière de liens professionnels / relationnels :</u>**<br><br>Les décideurs de l'entreprise sont sollicités pour définir avec eux le degré de criticité de chacune des ressources du système informatique.<br>Les informations sont communiquées aux personnes habilitées.<br>La communication est adaptée en fonction des interlocuteurs (termes techniques appropriés et explications compréhensibles) et leurs avis sont pris en compte.<br>Les non-conformités sont consignées afin de garantir l'intégrité, la confidentialité et la disponibilité des données.<br><br>**<u>En matière de contraintes liées au milieu et environnement de travail :</u>**<br><br>Le responsable de la sécurité informatique est informé immédiatement de toute tentative d'intrusion sur un système, ou de tout comportement d'utilisateur pouvant compromettre la sécurité du système informatique de l'entreprise, dont il aurait eu connaissance pendant l'exercice de ses missions. |

| | | | |
|---|---|---|---|
| système…). Une sensibilisation périodique est réalisée afin de vérifier la bonne application des règles à respecter et des bons comportements à adapter via des réunions d'information, des mails, une communication sur le réseau de l'entreprise… | | | **<u>En matière de résultats</u>**<br><br>Le réseau de l'entreprise est supervisé via des outils de prévention.<br>L'intégralité des données est garantie.<br>La confidentialité des informations échangées est garantie en toute circonstance.<br>L'accès à chaque ressource est limité aux personnes autorisées.<br>Les droits affectés aux utilisateurs sont conformes aux règles organisationnelles de l'entreprise.<br>Les équipements matériels et logiciels de sécurité sont adaptés au niveau de protection de l'entreprise. |

| | | | |
|---|---|---|---|
| | | | |
| | **2. Sécuriser les équipements et sensibiliser les utilisateurs**<br><br>Pour sécuriser les équipements et sensibiliser les utilisateurs, le technicien de maintenance doit contrôler l'utilisation des comptes utilisateurs, des serveurs, des postes de travail, des dossiers partagés, des imprimantes, etc. et leurs appliquer des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées.<br><br>Pour sécuriser les équipements et sensibiliser les utilisateurs, le technicien de maintenance doit contrôler l'utilisation des comptes utilisateurs, des serveurs, des postes de travail, des dossiers partagés, des imprimantes, etc. est réalisé en appliquant des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées Le technicien de maintenance contrôle et mesure les risques d'intrusions, de fraudes, concernant la sécurité afin de les éradiquer. Il réalise des actions de prévention (des réunions d'information, des mails, une communication sur le réseau de l'entreprise…) et sensibilise les utilisateurs aux règles de sécurité, et aux risques encourus. Pour cela, il organise des actions de sensibilisation et en mesure leurs efficacités. | L'UIMM territoriale centre d'examen définit les modalités d'évaluation en concertation avec l'entreprise et les acteurs concernés (entreprise, candidats, UIMM Territoriale...). Cette évaluation sera complétée par l'avis de l'entreprise.<br><br>Modalités d'évaluation :<br><br>- Evaluation en situation professionnelle réelle<br>Ou<br>- Présentation des projets ou activités réalisés en milieu professionnel<br>Ou<br>- Evaluation à partir d'une situation professionnelle reconstituée<br>Et<br>- Avis de l'entreprise | **<u>En matière de méthodes utilisées :</u>**<br><br>Les services centralisés d'identification et d'authentification (Active Directory) à un réseau d'ordinateurs utilisant le système Windows, MacOs et encore Linux sont identifiés.<br>Le contrôle de l'utilisation des comptes utilisateurs, des serveurs, des postes de travail, des dossiers partagés, des imprimantes, etc. est réalisé en appliquant des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées.<br>Les intrusions, les fraudes, les atteintes ou les fuites concernant la sécurité sont contrôlées et des mesures sont prises pour les éradiquer.<br>Des actions de prévention sont réalisées (des réunions d'information, des mails, une communication sur le réseau de l'entreprise…).<br>Afin de leur faire accepter les contraintes liées aux règles de sécurité, les utilisateurs des ressources informatique de<br>l'entreprise sont sensibilisés aux risques encourus.<br>Des actions de sensibilisation sont programmées et leurs efficacités mesurer.<br><br>**<u>En matière de moyens utilisés :</u>**<br><br>Les guides pédagogiques internes ou externes, les documents de sensibilisation et de prévention, éventuellement les liens des sites internet spécialisés sont adaptés à la situation et aux utilisateurs rencontrés.<br><br>**<u>En matière de liens professionnels / relationnels :</u>**<br><br>Le vocabulaire et la complexité du langage est adapté au niveau de compréhension de l'utilisateur, puis valider, par la reformulation, afin de vérifier sa bonne compréhension.<br>Les utilisateurs sont accompagnés et formés dans l'utilisation des outils matériels et logiciels mis à leur disposition ou exigés dans l'exercice de leur activité.<br><br>Les utilisateurs sont sensibilisés aux bonnes pratiques en matière de sécurité informatique, d'entretien et d'utilisation des équipements.<br><br>**<u>En matière de contraintes liées au milieu et environnement de travail :</u>**<br><br>Les contraintes liées aux règles de sécurité informatique imposées aux utilisateurs sont identifiées et appliquées. La politique de sécurité informatique spécifique liée à l'organisation ou l'entreprise est prise en compte. |

| | | | |
|---|---|---|---|
| | | | **<u>En matière de résultats</u>**<br><br>La gestion des accès à l'ensemble des plateformes logicielles et matérielles est conforme à la politique desécurisation de l'entreprise.<br><br>Les règles de sécurité sont transmises aux utilisateursdes ressources informatiques de l'entreprise.<br>Les utilisateurs sont sensibilisés aux risques encourus.Les contraintes liées aux règles de sécurité sont acceptées. |