EXAMEN PROFESSIONNEL D'INGÉNIEUR TERRITORIAL
SESSION 2020

SPÉCIALITÉ « INFORMATIQUE ET SYSTÈMES D'INFORMATION »
OPTION « SYSTÈMES D'INFORMATION ET COMMUNICATION (SIC) »

ÉPREUVE DE PROJET

NOTE OBTENUE : 14,5 / 20

QUESTION 1

A INGECO

Le 13 octobre 2020

Note à l'attention du Directeur
des Systèmes d'Information

Objet : Télétravail
Références : loi n°2012-347 du 12 mars 2012
décret n°2016-151 du 11 février 2016

Face aux demandes croissantes de télétravail et afin de fidéliser ses ressources humaines, INGECO souhaite se lancer dans la mise en œuvre du télétravail.
Nous définirons dans un premier temps le télétravail et ses modalités, puis nous verrons que peuvent être ses usages à INGECO et les enjeux pour notre DSI.

1. Télétravail : définition et modalités

Comme défini dans le décret du 11 février 2016, relatif aux conditions et modalités de mise en œuvre du télétravail désigne « toute forme d'organisation du travail dans laquelle les fonctions qui auraient pu être exercées par un agent dans les locaux de son employeur sont réalisées hors de ces locaux de façon régulière et volontaire en utilisant les technologies de l'information et de la communication ».
Le décret fixe en outre un certain nombre de modalités liées au télétravail : nombre de jours obligatoires sur site (2 jours par semaine), demande écrite doit être faite par l'agent intéressé, acte doit être formalisé au niveau de la collectivité et de l'agent (précisant les fonctions menées lors du télétravail, le lieu d'exercice, date de prise d'effet…).
Le télétravail se distingue donc des autres modalités d'organisation du travail à distance. Il n'est pas exercé par des agents dotés d'un statut particulier (travail en tiers lieu statutaire). Les activités ne s'exercent pas, par nature, en dehors des locaux (nomadisme). Il ne s'agit pas non plus d'un travail sur site distinct de ses autres collègues ou d'un travail mené dans le cadre d'un plan de continuité des activités. Enfin ce n'est pas une astreinte.

2. Télétravail à INGECO : usages possibles et enjeux pour la DSI

Compte tenu des compétences d'INGECI et de la nature de ses métiers, le télétravail pourrait être mis en place pour les services fonctionnels : DRH, DSI, Direction des finances, Direction juridique. Le télétravail se prête aux activités de gestion, d'instruction des demandes et dossiers. Cela peut être également mis en œuvre pour les agents qui n'exercent pas de mission sur le terrain, ou qui ne sont pas chargés d'accueillir le public, à l'instar de certains agents du service Petite Enfance. Enfin, le télétravail pourrait être proposé aux élus et au DGS.

En ce qui concerne notre DSI, le déploiement du télétravail a de multiples enjeux. Tout d'abord, un enjeu matériel afin d'équiper les futurs télétravailleurs du matériel informatique adéquat (PC portables), de mettre en place une connexion sécurisée correctement dimensionnée (nombre de connexions, performance du réseau). Il s'agit aussi d'un enjeu technologique afin de permettre le travail collaboratif à distance (outil de visioconférence notamment). L'enjeu est également financier, compte tenu du coût de ces équipements. L'enjeu est aussi celui des ressources, à savoir mobiliser les agents responsables du développement informatique, responsables du réseau et de la sécurité informatique et responsables du support auprès des agents télétravailleurs. Enfin, l'enjeu est celui de la sécurité, notamment en termes de protection des données personnelles et de la collectivité.

QUESTION 2

a) La méthodologie de projet proposée est la suivante : constitution de groupes de pilotage et phasage du projet en différentes étapes clés. Pour la constitution des instances de pilotage, voici ce qui pourrait être envisagé :

- création d'un comité de pilotage composé d'élus en charge du numérique, et des ressources humaines, le Président de la Communauté d'Agglomération, le DGS, la DSI et le DRH.
- création d'une équipe projet transverse composée de référent télétravail, du chef de projet DSI, du responsable de service RH, du responsable de service finance, du responsable de service juridique et du responsable de sécurité informatique.

Tout au long du projet, il faudra veiller à consulter les syndicats et représentants du personnel. Il pourra également être intéressant d'associer le médecin de prévention et l'agent chargé de la prévention des risques professionnels.

Pour le phasage du projet, il paraît opportun de distinguer trois phases :

- phase préparatoire, menée par l'équipe projet pour identifier les modalités de télétravail.

Les choix sont arbitrés et validés par le COPIL

- phase expérimentale auprès d'agents volontaires (sélectionner une centaine de candidatures) sur 6 mois, assortie d'un bilan
- phase de déploiement généralisé si la phase expérimentale a été concluante

b) Responsable du déroulement du projet, l'équipe projet transverse pourrait organiser des groupes de travail thématiques : charte et règlement du télétravail, outils de collaboration, support, management, équipement, réseau et sécurité.

En ce qui concerne le groupe charte et règlement du télétravail, les points suivants pourront être abordés :

- création d'une charte de télétravail à destination des télétravailleurs (principes et modalités)
- création d'un document de bonnes pratiques autour du télétravail et d'un guide d'utilisation
- mise à disposition du règlement du télétravail dans la fonction publique (=décret)

En ce qui concerne le groupe outils de collaboration, les points suivants pourront être abordés :

- étude sur les besoins de travail collaboratif
- analyse du marché relatif aux outils de travail collaboratif (visioconférence, partage de documents, co-édition en ligne)
- choix et expérimentation d'un outil

En ce qui concerne le groupe support, les points suivants pourront être abordés :

- modalités d'organisation du support (hotline, horaires, ressources)
- base de connaissances en ligne
- formation des télétravailleurs

En ce qui concerne le groupe management, les points suivants pourront être abordés :

- modalités d'organisation du travail en équipe
- missions confiées au télétravailleur
- modalités de suivi et d'évaluation

En ce qui concerne le groupe équipement, les points suivants pourront être abordés :

- achat des PC portables
- installation et configuration des PC portables
- modalités de déploiement
- renouvellement du parc
- mise à jour de la politique d'équipement et de communication auprès des agents

En ce qui concerne le groupe réseau et sécurité, les points suivants pourront être abordés :

- choix de la solution de connexion sécurisée (tunelling, VPN)
- dimensionnement de la connexion (achat de licences le cas échéant)
- mesures de performance
- droit à la déconnexion pour les télétravailleurs
- sensibilisation des télétravailleurs aux risques liés à la cybercriminalité
- sélection des applications et outils à rendre accessibles à distance
- mise à jour stratégies pare-feu et antivirus

QUESTION 3

a) Les agents peuvent accéder différemment au système d'information. D'un point de vue matériel tout d'abord, soit l'agent bénéficie d'un matériel professionnel, prêté et confisqué par la DSI.(poste fixe, PC portable, tablette ou smartphone). Soit l'agent utilise son équipement personnel (on parle de Bring Your Own Device – BYOD)

D'un point de vue réseau ensuite. L'agent peut accéder au système d'information via le réseau interne, sur site. Il peut aussi y accéder à distance via un réseau privé virtuel (VPN) sécurisé. Ou l'agent se connecte en mode hébergé via des ressources Cloud.

b) Ces solutions techniques possèdent chacune des bénéfices et des inconvénients.

D'un point de vue matériel d'abord. L'utilisation d'un matériel professionnel constitue un bénéfice certain pour la DSI car elle garde la maîtrise de l'installation et de configuration du matériel. L'utilisation de cde matériel est par ailleurs bien encadrée par la politique d'équipement et charte informatique associées. En revanche, cela constitue un coût conséquent (achat et maintenance). L'utilisation d'un matériel personnel à des fins professionnelles permet, elle, un cout allégé. Mais la DSI perd la maîtrise de son équipement et de son parc et le niveau sécuritaire est important. La DSI ne peut gérer notamment le pare-feu local ou l'antivirus ; dès lors, comment se prémunir contre les cyberattaques ?

D'un point de vue réseau ensuite. Les bénéfices d'un accès au système d'information par le réseau privé sont nombreux. La DSI peut maîtriser son environnement de sécurité et gérer ainsi les mises à jour des antivirus, des correctifs et des patchs de systèmes d'exploitation. Elle peut aussi tracer et contrôler ce qui correspond en outre à une exigence réglementaire en matière de cybercriminalité et de protection des données. Lorsque l'accès est distant, les inconvénients apparaissent : problème de routage réseau, difficulté voire impossibilité d'appliquer les mises à jour de sécurité ou d'interroger le système distant, ou encore problématiques concernant les contrôles de cyber-sécurité à l'instar des évaluations de vulnérabilité, gestion des correctifs ou antivirus. A noter que ce dernier inconvénient n'est pas valable pour les technologies Cloud qui facilitent la gestion de ces bases de sécurité.

QUESTION 4

a) La sécurité du système d'information repose sur la garantie de la disponibilité, de la confidentialité et de l'intégrité du système d'information. Cela signifie que l'information doit être disponible aux personnes autorisées et au bon moment et que seules les personnes autorisées et habilitées peuvent accéder à l'information et éventuellement la modifier.

Ces garanties doivent être maintenues dans le cadre d'un accès à distance, malgré les risques sécuritaires accrus du fait notamment d'une cybercriminalité en hausse.

Cela passe tout d'abord par une veille sur les conditions d'acceptation des nouvelles technologies, méthodologies et workflow facilitant la mise en œuvre des techniques de cyber sécurité. Il s'agit, entre autres, de prendre en compte le BHOD car l'accès au système d'information par des appareils mobiles personnels bouleverse les politiques de sécurité traditionnelles. Il s'agit aussi de regarder du côté des outils MDM (Mobile Device Management) et EMM (Enterprise Mobility Management) qui permettent d'étendre la politique de sécurité à tous les périphériques. Il s'agit également d'améliorer la surveillance des données. Cela passe enfin par la responsabilisation des agents. En matière de sécurité, tout le monde a son rôle à jouer. Pour aider et faciliter cette responsabilisation, des actions de formation à la sécurité informatique ainsi que des actions de sensibilisation (par exemple sur le choix d'un mot de passe robuste ou sur la vigilance à avoir dans les échanges sur la messagerie) peuvent être proposées. Le délégué à la protection des données pourra être sollicité sur ces points d'attention.

b) Pour sécuriser le système d'information, il convient d'intervenir à différents niveaux sur l'architecture technique. Tout d'abord, cela doit passer par la sécurisation des postes de travail (PC portables et fixes). Il s'agit de mettre en place un antivirus, un antimalware. Il s'agit aussi d'activer le pare-feu local et d'y associer des règles de sécurité en fonction des flux entrants et sortants. Il convient également de contrôler les périphériques. A noter que ces éléments de sécurisation sont aussi valables pour les terminaux mobiles (tablettes, smartphones…).

La sécurisation du système d'information repose aussi sur la sécurisation du réseau informatique. Il convient ici de mettre ne place un pare-feu pour se protéger contre les intrusions externes en mettant en place des règles de filtrage. Des zones dématérialisées (DMZ) spécifiques peuvent être ajoutées et intégrées à ces pare-feu en fonction des exigences de sécurité souhaitées. Un pare-feu applicatif (WAF) peut également être mis en place pour gérer les flux et diverses règles de redirection. Pour la navigation sur le web, des serveurs proxy/reverse proxy peuvent être spécifiquement utilisées pour sécuriser les échanges. Toutes ces règles de sécurité doivent être régulièrement à jour pour être toujours efficaces.