EXAMEN PROFESSIONNEL D'INGÉNIEUR TERRITORIAL 2022

SPÉCIALITÉ « INFORMATIQUE ET SYSTÈMES D'INFORMATION »

OPTION « SYSTÈMES D'INFORMATION ET DE COMMUNICATION »

ÉPREUVE DE PROJET

NOTE OBTENUE : 16.75 / 20

Question 1

Angers le 16/06/2022

À l'attention du Président d'INGEDEP

Note sur la Transformation d'INGEDEP

La crise sanitaire a eu pour effet de mettre la DSISN en pleine lumière. Notre adaptation rapide à ce changement a été bénéfique mais pas suffisant, c'est pourquoi je me permets de vous aiguiller vers les chantiers nécessaires pour achever cette évolution.

La mise en place du télétravail doit se poursuivre en insistant sur la sécurité du process (authentification à double facteur, mise en œuvre d'outils de sécurité pro-actifs, fourniture de postes légers portables et utilisables en télétravail, disponibilité de l'ensemble de nos outils en usage déporté, fiabilisation de l'accès aux réseaux (mise en œuvre de sites et secours avec redondance).

La signature électronique devra être une possibilité pour l'ensemble des démarches liées aux usagers. L'utilisation de France Connect pour le public doit devenir un standard, tout comme la signature avancée pour nos agents et la signature qualifiée pour les directeurs et leurs adjoints. Une attention particulière sera à apporter à l'archivage des documents pour satisfaire aux obligations légales.

La réduction de la fracture numérique de nos usagers et aussi de nos agents doit être prise en compte. Nous pouvons développer et agrandir le réseau de points numériques, renforcer la formation initiale et continue des agents d'accueil et des travailleurs sociaux.
Permettre l'usage d'une méthode non-numérique pour l'ensemble des démarches serait toutefois utiles aux personnes souffrant de handicaps ou dépendantes.
La sécurité et la conformité étant un chantier dont le donneur d'ordre ne peut être que la DSISN, je vous soumets un tour d'horizon afin de réduire les risques et d'obtenir le niveau de conformité voulu (RGS).

Question 2

A. Il existe un recueil de bonnes pratiques en terme de sécurité pour les administrations, c'est le référentiel général de sécurité (RGS) créé par la loi du 2 février 2010 (n°2010-112).

On peut aussi s'appuyer sur la documentation et les bonnes pratiques que l'agence nationale de la sécurité des systèmes d'information (ANSSI) prodigue.
Le RGPD (Règlement Général de la Protection des Données) est à prendre en compte bien naturellement.
La CNIL peut aussi être une bonne source d'informations.
Les principales menaces et leurs sources sont les suivantes :

- intrusion dans le SI : systèmes mal configurés ou non mis à jour (feuilles de sécurité)
- usurpation d'identité : campagne de phishing
- corruption de données : rançongiciel

Toutes les menaces peuvent arriver en simultané et provoquer la paralysie complète d'un SI (exemple : la ville d'Angers et le CHU de Rouen).
La démarche à suivre est donc de suivre le référentiel RGS dans le cas d'un SI déjà constitué comme le nôtre.
Pour la sécurité :

1. réalisation d'un audit de la sécurité du SI en interne ou externe
2. réalisation d'une analyse des risques simplifiée
3. mise en œuvre des mesures correctives fixées dans le rapport d'audit
4. décision d'homologation de sécurité du SI
5. suivi opération de la sécurité du SI

La sécurité, pour être conforme, doit satisfaire aux domaines classiques du SI :

- disponibilité et intégrité des données et du système
- confidentialité des données et du SI
- authentification de la personne
- traçabilité des actions sur les données et les processus

Des prestations techniques seront nécessaires, comme des produits de sécurité matériels (pare-feu, proxy, netscalers) aussi bien que le logiciel (analyse de log en temps réel, antivirus, analyse de l'accès aux données).
Une organisation des responsabilités et une bonne gestion des ressources humaines feront partie de cette mise en conformité.

Le RSSI (Responsable Sécurité du SI) et le DPO (Date Protection Officer) nous seront d'une grande utilité pour mettre à bien cette démarche. Nous pouvons aussi demander une aide de France Relance.

B. Sensibilisation des agents utilisateurs du SI.

- une charte informatique sera à valider pour chaque agent dès sa mise en œuvre
- un bulletin d'information avec une littérature accessible et des exemples concrets pourrait être créé avec l'aide de la cellule communication, sous la responsabilité du RSSI et DPO.
- pastilles vidéos sur l'intranet avec l'aide des agents eux-mêmes (intégration forte)
- informer les agents sur les tentatives d'intrusion sur notre SI pour une meilleure sensibilisation (ça n'arrive pas qu'aux autres)
- une formation continue sur les risques informatiques

Question 4

La mise en œuvre du cloud computing dit aussi informatique en nuage permet une meilleure adoption du SI aux changements d'usage.

Cette nouvelle stratégie n'est pas sans conséquences, je vous propose un panorama de ses possibilités.

Il est possible d'utiliser un seul logiciel via le cloug (SaaS : exemple : messagerie collaborative), ou bien d'y héberger une infrastructure SI complète (IaaS). L'opportunité qu'apporte le cloud est une remise en cause complète du SI pour pouvoir se remettre à la page.
Néanmoins, en fonction des usages voulus, il faut voir les atouts mais aussi les faiblesses du cloud. Pour ce faire, je vous propose un SWOT qui va au-delà de votre demande.

Les forces :
- il y a différents acteurs possibles (Microsoft, Amazon, Google, OVH,…) et certains sont même labellisés (SECNUM CLOUD, Cloud de confiance…)
- Acteurs européens possibles (OVH)
- Un délai de réactivité excellent pour déployer une solution
- Un temps moyen de disponibilité de 99.99%
- Cadre légal pour le respect des données personnelles

Les opportunités :
- il existe différents types de cloud en fonction de l'usage voulu
- l'émergence de nouveaux usages est facilitée
- la modification et l'adaptabilité rapide
- accompagnement par France Relance

Les faiblesses :
Principalement liées au coût.
- coût du changement de solution / rapatriement des données
- coût de l'abonnement modifiable sans préavis et quasiment à la hausse à chaque foi : pas de visibilité de son évolution
- déploiement de fonctionnalités non voulues ou arrêt de fonctionnalités utilisées

Les menaces :
- possibilité de s'enfermer dans un modèle propriétaire
- garantie de l'intégrité de mes données (incident data center OVH)
- localisation de mes données et qui peut y accéder sans mon accord (loi américaine ou russe)

Question 3

A. Le renforcement de la dématérialisation va permettre un meilleur déploiement de nouveaux usages et des facilités pour créer et suivre son dossier (24h/24 et 7J/7) pour l'usager. Il lui sera par contre demandé de valider son identité par des moyens plus robustes (exemple : France Connect).
Cette disponibilité pour l'usager va obliger la DSISN à revoir ses critères de redondance de système, de sauvegarde de base de données pour respecter cette demande.
Une mise à niveau des matériels, logiciels et compétences des agents de la DSISN sera donc obligatoire. Une mise à jour du stockage sera à prendre en compte pour l'archivage des données.
Pour les directions métiers, comme pour les agents, de nouvelles règles sont nécessaires.
La possibilité de fournir à l'usager des documents infalsifiables et authentiques sont possibles grâce à la signature électronique. Une mise à disposition de ce dispositif sera la règle pour tous les agents soit en version avancée via une double authentification (code numérique reçu par mail/SMS/système d'authentification) ou pour les personnes à fortes responsabilités une authentification avec une vérification de son identité au préalable et une clé de signature physique. Ceci est valable aussi pour les documents où l'authentification est fondamentale.

La mise en place de la signature va aussi devoir s'accompagner d'une évolution des logiciels métiers pour en tenir compte. Je vous propose donc une méthodologie ainsi qu'une organisation pour suivre le Plan de Transformation Numérique.

B. Pour que la DSISN puisse mener rapidement à bien ces projets, nous allons mettre en œuvre 2 moyens différents : la méthode agile et un nouvel acteur : le BRM. Voici une courte présentation de ces 2 éléments.

La méthode agile : c'est une méthode de gestion de projet récente qui permet une adaptation rapide au changement ou à une demande. On y travaille avec de petits cycles de développement, une forte collaboration avec les demandeurs et un focus fort sur le résultat plutôt que la documentation.
Les avantages sont la flexibilité, la qualité grâce aux fréquentes livraisons, la compétitivité grâce aux fonctionnalités et améliorations constantes et enfin un retour rapide des utilisateurs.
Les défauts sont le manque de documentation, en effort sur la gestion des demandes qui sont plus nombreuses et un résultat pas forcément prévisible à long terme.

Le BRM ou BUSINESS RELATIONSHIP MANAGER est un intermédiaire entre les fournisseurs de technologie, la DSISN et les directions métiers.
Son rôle consiste à comprendre les besoins métiers, mettre en œuvre de nouvelles technologies en identifiant les impacts sur les services déjà existants. Il est là, entre autre, pour mettre de « l'huile » entre les directions métiers et la DSISN en cas de souci.
Il appartient à la DSISN et doit être vu comme une de ses vitrines.

La méthodologie de projet sera donc la méthode agile dans la version la plus adaptée à la demande (SCRUM, KANBAN, eXteme Programming…).
L'organisation verra le BRM au cœur de la direction métier en ant que Product Owner (garant de la vision du projet), un SCRUM MASTER qui s'assurer que la méthodologie est correctement suivie.
Une équipe projet avec des agents de la DSISN et/ou des prestataires externes.