CONCOURS INTERNE D'INGÉNIEUR TERRITORIAL
SESSION 2021

ÉPREUVE DE PROJET

SPÉCIALITÉ « SYSTEMES D'INFORMATION ET COMMUNICATIONS »

NOTE OBTENUE : 14.63 / 20

Communauté d'agglomération d'Ingagglo,
Direction des Systèmes d'Informations

le 17 juin 2021

NOTE À L'INTENTION
du Directeur des Systèmes d'Information

Objet : Plan de Continuité d'Activité informatique

Chef de projet à la Direction des Systèmes d'Information, il m'est demandé par mon DSI d'élaborer un plan de continuité d'activité informatique et sa déclinaison opérationnelle afin d'analyser et de réduire les impacts potentiels d'une interruption de l'activité. En effet, le système d'information est un enjeu stratégique pour la collectivité et le préserver est vital pour assurer le bon fonctionnement des activités.
Pour faire face à cet enjeu, je répondrai à 5 questions qui permettront préparer l'organisation du projet de mise en place du PCA.

Question 1

A – Objectifs et enjeux à prendre en compte dans le cadre de continuité du service public de la collectivité

Avec la crise sanitaire du COVID-19 qui a impacté la vie économique et sociale à l'échelle mondiale, toutes les entreprises et collectivités se sont posées la question de leur organisation pour survivre à la crise. Le plan de continuité d'activité (PCA) doit permettre de répondre à cette question. Un PCA est donc un processus permettant d'identifier les actions à maintenir de façon prioritaire pour continuer d'atteindre ses objectifs et honorer ses obligations.
Concrètement, il permet donc à une collectivité de préparer l'organisation de son activité en cas de crise. Il peut s'agir de crises internes (incendie, grève, panne informatique) ou de crises externes (crise financière, sanitaire ou mouvement social). En l'anticipant, la collectivité augmente sa résilience et peut ainsi en limiter l'impact. Sa mise en place vise donc à maintenir un minimum d'activité pendant la crise, l'organiser et favoriser un retour à la normale rapide via un Plan de Reprise d'Activité (PRA). Le PCA a des impacts sur l'activité de la collectivité, son fonctionnement, son budget et son image.
De plus, un PCA couvre un champ plus large que le PCA informatique. Il ne se limite donc pas à la continuité du système d'information (SI). Il prend également en compte la mise en place du télétravail, le risque sanitaire, l'organisation permettant la gestion de crise (astreinte, cellule de crise) et la communication de crise. Il s'agira donc de définir pour une collectivité quelles sont les activités à maintenir, celle à réorienter, à stopper. Comment s'organiser pour continuer à accueillir le public, comment organiser le travail des agents à distance et celui des agents encore sur site. Enfin comme évoqué précédemment, comment organiser le retour à la normale de manière rapide, efficace, tout en veillant à ce que cela soir bien vécu par les agents.

B – Différences entre un PRA informatique et un PCA informatique

Comme nous avons vu précédemment, le PCA information est intégré au PCA. Celui-ci doit permettre une reprise du SI en cas de sinistre ou de défaillance majeure. L'objectif principal est donc de redémarrer, le plus rapidement possible. Le PRA est une composante du PCA. Le PCA informatique a pour but d'anticiper les problèmes en répertoriant des éléments du SI indispensables à la poursuite de l'activité. Une bonne pratique pour ces composants est de les redonder. Le PCA précise aussi par activité le service minimum acceptable. Il répertorie les risques afin de réaliser un bilan des conséquences directes en termes : de durée, d'indisponibilité, de perte d'informations et d'atteinte à l'image de la collectivité. Enfin, le PCA permettra de

mettre en place des mesures préventives : le plan de sauvegarde, la sécurité logique (antivirus, pare-feu, anti-spam), la sécurité physique (accès aux locaux dont la salle serveur), le facteur humain à ne pas négliger via une information et des formations réguliers auprès des agents.
Le PRA quant à lui devra gérer la reprise d'activité. C'est-à-dire la restauration des dernières sauvegardes, la réinstallation éventuelle de serveurs, le redémarrage des machines et des applications. Le temps de remise en route du système dépend donc de l'endommagement occasionné par le sinistre. Si un renouvellement matériel est nécessaire ce temps sera allongé. Dans le cas d'équipement ou d'applications redondés, la procédure consistera à basculer sur l'équipement de secours. Cela permet donc de raccourcir le temps de coupure voire de le rendre inexistant comme ce qui se pratique sur Internet.

Question 2

Communauté d'Agglomération d'Ingagglo — le 17 juin 2021
Direction des Systèmes d'Information

NOTE À L'ATTENTION
du Directeur des Systèmes d'Information

Avec le développement du numérique et sa présence de plus en plus importante au cœur de l'organisation des collectivités, la continuité du fonctionnement du système d'information est un enjeu majeur. La mise en place d'un Plan de Continuité Informatique (PCI) devient indispensable.
Au travers de cette note, nous présenterons tout d'abord des préconisations en termes d'organisation et le pilotage de la démarche de mise en place du PCI. Puis nous préciserons les étapes de la conception à la mise en œuvre.

I. Organisation et pilotage de la mise en place du PCI

En premier lieu, il faut nommer un responsable du PCI. Cette personne devra réunir plusieurs compétences :
- une bonne connaissance de la sécurité informatique ;
- une vision transparente de l'activité de la collectivité ;
- une aptitude à communiquer pour mener des campagnes de sensibilisation du personnel ;
- des capacités d'organisation, il sera le chef d'orchestre de la gestion du sinistre.

Cette personne pourrait être le responsable de la sécurité du système d'information (RSSI).
La démarche de mise en place du PCI doit se dérouler comme un projet classique avec la constitution d'un comité de pilotage composé de l'élu en charge du numérique, du directeur général des services, du DSI et du chef de projet. Sur les différents sujets seront créés des comités techniques qui se réuniront régulièrement. La particularité du PCI sera son organisation et son pilotage au moment de la crise avec la création d'une cellule de coordination, d'équipes d'intervention et des services utilisateurs.
Ce PCI devra, au terme de sa conception, être validé par le COPIL. L'important sera aussi de vérifier que ce plan est réalisable en termes de procédures, de budget ou de temps nécessaire au redémarrage. Par ailleurs, il devra être actualisé en continu pour rester en phase avec les missions de la collectivité. EN dernier lieu, le PCI devra bénéficier d'une communication et d'un accompagnement fort auprès des agents.
Par ailleurs, ce PCI devra avoir un soutien des élus et de la direction générale afin d'être compris et accepté de tous.

A – Les étapes de la conception à la mise en œuvre

Lors de la mise en place d'un PCI, les questions à se poser sont :
- quelle est la quantité maximale d'informations que je peux perdre sans mettre en péril la collectivité ?
- quel est le délai maximum de reprise d'activité normal où delà duquel le fonctionnement de la collectivité est mis en péril ?

Une analyse de l'existant est donc nécessaire pour répondre à ces deux questions. Cela définira le périmètre du PCI. Cela passera par un recensement des données du SI qui seront catégorisées de cette manière : données basiques, sensibles ou stratégiques.

Il s'agira ensuite de déterminer les menaces qui pèsent sur le SI de la collectivité. Elles peuvent être d'origine humaine ou technique, et être interne ou externe à la collectivité. L'analyse d'impact consiste à mesurer les conséquences d'un risque qui se matérialise.
Une fois le constat et les objectifs définis et partagés, il faudra mettre en place des mesures préventives (sauvegarde, sécurité logique et physique et facteur humain) et les mesures curatives en cas de sinistre. Il s'agira ici de définir les procédures de reprise d'activité via un PRA comme évoqué précédemment.
Ce plan devra être évalué pour vérifier que les mesures appliquées soient en phase avec les objectifs et l'état des lieux initial.
Dernier point, un focus important devra être fait sur la communication et la sensibilisation car la sécurité du SI dépend de chacun.
Pendant la vie du PCI, et dans l'idéal, il faudrait procéder à des exercices de reprise de l'activité pour envisager ce qui devra être fait en situation réelle. Un parallèle peut être fait avec la sécurité incendie pour laquelle des tests sont effectués régulièrement.

Question 3

A – Propositions opérationnelles et techniques permettant la mise en œuvre du PCI

Le premier chantier du PCI est l'étude de l'existant pour répondre aux deux questions suivantes :
- pendant combien de temps les agents seront-ils dans l'incapacité de travailler avec leur outil informatique ? Ce que les anglophones nomment « RTO » pour « Recovery Time Objective » ou Durée Maximale d'Interruption Admissibles (DMIA) ;
- de quand datent les données que nous allons récupérer, pour redémarrer l'activité ? C'est le RPO pour « Recovery Point Objective » ou Perte de Données Maximale Acceptable (PDMA).

On procèdera donc à un inventaire des traitements et des données de la collectivité pour les répartir en trois catégories. Les informations basiques : elle est utile mais pas prioritaire en matière de préservation et de restauration des informations. Les informations sensibles : son intégrité doit être préservée mais sa restauration en cas de sinistre n'est pas prioritaire. Les informations stratégiques : elle doit être restaurée en priorité en cas de sinistre, son intégrité doit être préservée.
Cet inventaire et cette répartition permettront de définir pour chaque application la DMIA et la PDMA en prenant en compte l'atteinte à l'image de la collectivité que pourrait avoir un service indisponible. Pour les données et applications hébergées à l'extérieur chez un prestataire, on vérifiera l'adéquation du PCI de la collectivité avec ce qui a été défini précédemment dans le marché. Il faudra aussi intégrer ces nouvelles règles dans les futurs appels d'offres.

Une fois l'analyse de l'existant terminée et validée par le COPIL, il faudra mettre en œuvre les moyens pour atteindre les objectifs définis par le PCI. Ceux-ci demanderont d'adapter notre architecture informatique pour répondre au besoin. Le PCI est complémentaire du projet de fusion et d'homogénéisation des deux sites informatiques. Celui-ci a pour but d'assurer la sécurité, la résilience et la haute disponibilité du nouveau système d'information. Il poursuit donc des objectifs similaires au PCI. À la différence que le PCI donnera un cadre de gestion de crise et la reprise d'activité. Dans le cadre du PCI, on préconise pour les applications stratégiques un serveur de secours dédié, géographiquement distant et une architecture à haute disponibilité. Pour les applications sensibles aussi, un serveur de secours dédié mais seulement un système prêt à fonctionner. Enfin, pour les applications « normales », des moyens de secours géographiquement distants.
On voit donc que le projet de mutualisation des SI pourra répondre à une architecture haute disponibilité mais pas à des serveurs de secours dédiés. Il faut donc intégrer dans ce projet et à moyen terme la possibilité de redonder une partie du premier site dans le deuxième au niveau du traitement des données.
La mise en place de PCI aura des impacts organisationnels et fonctionnels forts car les dispositifs à déployer seront importants avec la mobilisation de ressources humaines pour gérer les crises, le déploiement des équipements de secours informatique, réseaux et téléphonie, la gestion de la reprise des activités, du service d'assistance utilisateur, de la communication de crise et les mécanismes de reprise via le PRA.
Une attention particulière devra être portée sur la documentation des différentes procédures ainsi que leur maintien en condition opérationnelles. Le PCI devra vivre dans le temps et être régulièrement amendé. Les efforts budgétaires qu'il engendre demanderont une priorisation pour étaler les actions dans le temps mais en gardant à l'esprit que cette mise en place initiale doit avoir une fin comme tous les projets.

B – Alternatives possibles dans le cloud

Le développement du cloud depuis quelques années est indéniable. Beaucoup d'entreprises et aussi maintenant des collectivités utilisent pour héberger tout ou partie de leur système d'information. Il devient donc une possibilité pour gérer la reprise d'activité du PRA. LE cloud devient alors la sauvegarde du système d'information. Il comporte des avantages comme un meilleur contrôle des coûts (on ne paie que ce que l'on consomme ou utilise) et accès à distance aux données en cas d'incident. Dans le même temps, il y a aussi des contraintes et des particularités qu'il faut prendre en compte.
La première d'entre elles est la sécurité. Il est nécessaire de s'assurer que toutes les données stockées en ligne sont chiffrées. Il faut aussi déterminer ce qui doit être protégé et en combien de temps restaurer les données. La granularité de l'accès aux données est aussi prépondérante pour accéder facilement à un fichier en particulier.
Le PCA va de pair avec la reprise d'activité. L'utilisation du cloud à des fins de PRA peut s'avérer une bonne option pour atteindre la continuité d'activité. Il permet de réaliser l'objectif de serveurs de secours dédiées géographiquement distants. Il y a cependant une nuance importante entre sauvegarder ses données à distance dans le cloud et être en capacité de faire fonctionner ces services dans le cloud en lieu et place du data center de la collectivité. Sachant que la bascule de l'un à l'autre en toute transparence peut avoir un coût humaine et financier non négligeable.
Une solution hybride peut être envisagée avec la sauvegarde des données dans le cloud et seulement des applications critiques entièrement redondées avec des mécanismes de bascule intégrés.

Question 4 : Cahier des charges pour la mise en place d'un PCA

Suite aux évènements récents, la communauté d'agglomération d'Ingagglo souhaite revoir son PCA dont la PCI est une composante importante. Pour cela, elle souhaite se faire accompagner pour sa réécriture. Voici la trame du cahier des charges pour le choix d'un cabinet d'expertise.

1. Besoins fonctionnels
   On devra identifier les missions essentielles d'Ingagglo et comment les poursuivre. Il faudra donc définir et lister les métiers nécessitant d'être effectués en présentiel et ceux pouvant être faits à distance.
   Chacun devra avoir les moyens d'effectuer correctement sa mission. Il faudra donc lister les besoins de nouveaux matériels pour le télétravail.
   Au niveau du PCI, il faudra analyser l'existant du SI, définir les PDMA et DMIA pour chaque service et mettre en adéquation les moyens pour y parvenir. Enfin, il faudra définir une communication pour les agents.

2. Besoins réglementaires
   Voici les compétences de la communauté d'agglomération, elles aideront à définir les besoins fonctionnels obligatoires :
   - le développement économique ;
   - l'aménagement de l'espace communautaire ;
   - l'équilibre social de l'habitat sur le territoire communautaire ;
   - la politique de la ville ;
   - accueil des gens du voyage ;
   - collecte et traitement des déchets des ménages et déchets assimilés.

   Pour les autres compétences, se reporter à l'annexe A.

3. Besoins organisationnels
   Le PCA devra définir comment doivent fonctionner les services en cas de crise. Des propositions devront être faites pour chaque type de crise. Concernant le PCI, on détaillera l'organisation à déployer en décrivant les interactions entre chacun.

4. Besoins de sécurité
   Comme en matière d'organisation, le PCA décrira les besoins de sécurité et les actions à mener pour garantir la sécurité des agents et des citoyens. Cela devra être décliné pour chaque cas.

5. Plan de Reprise d'Activité
   Le PRA est une des composantes du PCA. Il devra donc décrire comment la reprise d'activité se fait.

Question 5

A – Préconisations RH pour la mobilisation des équipes et le fonctionnement du PCI

Les différentes tâches de pilotage et de mise en œuvre du PCI en cas de sinistre doivent être affectées à des agents. Ils devront être en nombre suffisant, de manière à ce que, en cas de sinistre, la réalisation de la tâche soit garantie. Les agents impactés par le PCI seront donc informés de leur éventuelle participation en cas de sinistre. Cela devra être stipulé dans leur fiche de poste et précisé les contraintes que cela peut engendrer en terme d'astreinte par exemple.
En terme de déroulement, les premiers intervenants sont chargés d'appliquer les consignes et de donner l'alerte, selon les procédures d'escalade définies.
En cas de sinistre, on distinguera ensuite : le comité de crise, la cellule de coordination, les équipes d'intervention et les services utilisateurs. Le comité sera composé d'un représentant de chaque direction : direction des ressources et moyens généraux, direction des services techniques, direction de l'environnement et des transports, direction de l'aménagement et de la cohésion sociale, direction générale des services. Le DSI et le RSSI (responsable du PCI) en seront aussi membres. Le comité de crise prend les principales décisions concernant le secours.
Le pilotage opérationnel sera confié à une cellule de coordination. La réalisation des tâches secours incombera aux équipes d'intervention définies selon les compétences requises, la disponibilité et le lieux d'intervention. Il faudra s'assurer que les fiches de poste soient compatibles avec un déplacement sur un autre site.
EN dernier lieu, les services utilisateurs prenant en charge leur propre plan de secours et de reprise d'activité en fonction des moyens mis à leur disposition. Parmi les tâches qui incombent aux responsables de ces services, on notera les tâches d'attente du secours, l'organisation du redémarrage (normal ou dégradé), des procédures de contournement éventuelles, l'organisation de travaux exceptionnels (ressaisie ou rattrapage de données).

B – Organisation avec les services utilisateurs

Ceux qui connaissent le mieux la valeur et le contenu du système d'information sont les utilisateurs. Ce sont eux qui sont le plus à même de définir les risques et les impacts en cas de sinistre. Ils seront donc fortement mobilisés pour cet inventaire.
La première étape sera de répertorier les différents traitements de données et nommer un responsable métier pour chacun d'entre eux. On fera ensuite appel à eux pour classifier les données de leurs applications dans les trois catégories : stratégiques, sensibles et basiques. À partir de cela, le responsable du PCA rédigera conjointement les DMIA et PDMA pour chaque application. Cela permettra ainsi de partager l'information en toute transparence.
Les responsables seront aussi des relais pour la communication des bonnes pratiques de sécurité et seront sollicités pour toute évolution de leurs applications afin de rendre le PCA évolutif au cours du temps.