Sujet élaboré par une cellule pédagogique nationale

EXAMEN PROFESSIONNEL D'AVANCEMENT DE GRADE DE TECHNICIEN PRINCIPAL TERRITORIAL DE 1ère CLASSE

SESSION 2021

ÉPREUVE DE RAPPORT AVEC PROPOSITIONS OPÉRATIONNELLES

ÉPREUVE D'ADMISSIBILITÉ :

Rédaction d'un rapport technique portant sur la spécialité au titre de laquelle le candidat concourt. Ce rapport est assorti de propositions opérationnelles.

Durée : 3 heures
Coefficient : 1

SPÉCIALITÉ : INGÉNIERIE, INFORMATIQUE ET SYSTÈMES D'INFORMATION

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni initiales, ni votre numéro de convocation, ni le nom de votre collectivité employeur, de la commune où vous résidez ou du lieu de la salle d'examen où vous composez, ni nom de collectivité fictif non indiqué dans le sujet, ni signature ou paraphe.
- Sauf consignes particulières figurant dans le sujet, vous devez impérativement utiliser une seule et même couleur non effaçable pour écrire et/ou souligner. Seule l'encre noire ou l'encre bleue est autorisée. L'utilisation de plus d'une couleur, d'une couleur non autorisée, d'un surligneur pourra être considérée comme un signe distinctif.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 24 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.

S'il est incomplet, en avertir le surveillant.

Vous êtes technicien principal territorial de 1ère classe au sein de la direction des systèmes d'information de la communauté d'agglomération de Techniagglo (1 500 agents / 200 000 habitants).

La direction générale souhaite anticiper et maîtriser les risques opérationnels de grande envergure.

La direction des systèmes d'information est donc chargée d'élaborer un plan d'actions afin d'analyser et de réduire les impacts potentiels d'une interruption d'activité.

Dans un premier temps, le directeur des systèmes d'information vous demande de rédiger à son attention, exclusivement à l'aide des documents joints, un rapport technique sur les enjeux d'un Plan de Reprise d'Activité informatique (PRA).

10 points

Dans un deuxième temps, il vous demande d'établir un ensemble de propositions opérationnelles permettant la mise en œuvre du Plan de Reprise d'Activité informatique (PRA) de Techniagglo.

Pour traiter cette seconde partie, vous mobiliserez également vos connaissances

10 points

Liste des documents :

Document 1 : « PRA/PCA : Qu'est-ce que c'est et quels sont leurs avantages ? » - *Hoster.com* - juillet 2019 - 1 page.

Document 2 : « Pourquoi et comment mettre en place un PCA / PRA ? » - *Ivision.fr* - novembre 2017 - 2 pages.

Document 3 : « Pourquoi le plan de reprise d'activité ne doit plus être envisagé comme une option par votre entreprise ? » - *Cyres.fr* – 16 juillet 2018 - 4 pages.

Document 4 : « Administration numérique et sécurité informatique : quels enjeux dans les communes ? » - *Cogitis.fr* - site consulté en mars 2020 - 4 pages.

Document 5 : « Les bonnes pratiques d'un PRA réussi » - *Silicon.fr* - site consulté en mars 2020 - 2 pages.

Document 6 : « L'ISO 27701, une norme internationale pour la protection des données personnelles » - *cnil.fr* - 2 avril 2020 - 2 pages.

Document 7 : « PRA en cloud : à quoi faut-il s'attendre ? » - Erin SULLIVAN - *Le MagIT* - 25 juillet 2019 - 2 pages.

Document 8 : « La Politique de Sécurité des Systèmes d'Information de l'État (PSSIE) - Agence nationale de la sécurité des systèmes information » - *SSI.gouv.fr* - 17 juillet 2014 - 1 page.

Document 9 : « Coronavirus - Comment les collectivités ajustent leur plan de continuité » - Emeline LE NAOUR - *lagazettedescommunes.com* - mars 2020 - 3 pages.

DOCUMENT 1

« PRA/PCA : Qu'est-ce que c'est et quels sont leurs avantages ? »

Hoster.com - Juillet 2019

Aujourd'hui le bon fonctionnement des systèmes informatiques est primordial pour l'activité des entreprises. L'inaptitude de faire face à un incident majeur peut engendrer des pertes de revenus et avoir même des conséquences fatales.
Dans cet article, nous nous arrêterons sur la différence entre le PRA et le PCA pour voir ensuite pourquoi et comment votre société pourrait-elle en profiter.

Le PRA : Qu'est-ce que c'est ?

Le PRA ou le plan de reprise d'activité est une procédure qui permet aux entreprises de reprendre vite leurs activités après avoir vécu un sinistre majeur (inondation, incendie, perte de données vitales, etc.).
Il s'agit d'un document qui décrit les démarches à suivre afin de reconstruire son système informatique et de minimiser les effets négatifs de la crise survenue.

Le PCA : Qu'est-ce que c'est ?

Le PCA ou le plan de continuité d'activité doit assurer la continuité des services de l'entreprise en cas de panne ou d'accident majeur. Ce dernier a pour but aussi de diminuer au maximum le temps d'interruption ainsi que d'éviter les pertes de données.

Pourquoi mettre en place un PCA / PRA ?

L'interruption d'activité d'une entreprise peut avoir des conséquences variées.

- Conséquences financières
- Conséquences négatives sur la réputation de l'entreprise
- Conséquences juridiques (si l'entreprise n'arrive pas à respecter ses obligations contractuelles)

Ces problèmes peuvent également déclencher des réactions internes et diminuer la satisfaction des employées ainsi que celle des partenaires de la société.

Comment mettre en place un PCA / PRA ?

La mise en place d'un PCA/PRA demande une organisation préalable qui définit les seuils critiques à ne pas dépasser en cas d'incident ou de panne.
La rédaction de cahiers de charges détaillées par l'entreprise permet au fournisseur de services de s'orienter et de mieux comprendre les enjeux spécifiques qui sont propres au métier de son client. L'identification des ressources critiques qui sont indispensables au bon fonctionnement de l'entreprise aident le prestataire à définir la priorité de ses tâches.
Une fois que les besoins de l'entreprise sont définies, cette dernière doit décider où le PRA /PCA sera mis en place : sur un de ses sites ou sur un Datacenter externe. Ensuite un plan de gouvernance et de gestion de crise est élaboré par le prestataire et testé par ce dernier en collaboration avec le client.

Conclusion

La mise en place de PRA/PCA permet aux entreprises de se protéger en cas de sinistre et de minimiser leurs pertes de revenus. Il s'agit d'un processus élaboré qui demande du temps et de l'organisation.
Mais c'est avant tout une procédure qui évolue au fur et à mesure avec le développement de la société. Voilà pourquoi nous vous conseillons de confier cette tâche importante à des spécialistes expérimentés.

DOCUMENT 2

« Pourquoi et comment mettre en place un PCA / PRA ? »

Ivision.fr - Novembre 2017

Menaces informatiques, problèmes de réseau, d'infrastructure, panne électrique, panne matérielle ou encore catastrophes naturelles, les incidents qui peuvent affecter le système d'information sont nombreux.

Selon une enquête réalisée auprès de plus de 1500 décideurs en entreprise et dans l'IT, le rapport Veeam Data Protection 2020, **51%** des répondants ont subis une **perte de confiance** de clients **à la suite d'interruptions de leurs systèmes**.

Comment traiter un risque d'indisponibilité

Il existe plusieurs démarches ou mécanismes possibles pour réduire les risques d'indisponibilité :

- **Accepter :** Accepter la menace et ses impacts potentiels pour l'entreprise
- **Éviter :** Ne pas lancer ou arrêter une activité à cause des risques encourus
- **Transférer :** Déporter le risque sur un tiers (prise d'une assurance, transfert d'une activité à un prestataire, …)
- **Réduire la probabilité :** Traiter le risque en amont, en réduisant sa probabilité d'occurrence
- **Limiter les impacts** : en mettant en place un **PCA (Plan de Continuité d'Activité)** ou **PRA (Plan de Retour à l'Activité)**.

Pourquoi mettre en place un PCA / PRA

Mettre en place un PCA (Plan de continuité d'activité) ou PRA (Plan de retour à l'activité) permet de limiter l'ensemble des impacts liés à une interruption d'activité. Et comme nous allons le voir ci-dessous, les conséquences d'une interruption d'activité sont à la fois variés et lourdes pour l'entreprise, du fait que les systèmes informatiques ont pris le pas sur la majorité des processus des entreprises.

Les conséquences d'une interruption d'activité peuvent ainsi être :

- **Conséquences financières** : La suspension de certaines activités critiques de l'entreprise (production, support etc.) peuvent rapidement se chiffrer en plusieurs milliers d'euros.
- **Conséquences** concernant la **satisfaction des clients :** la réputation de l'entreprise, son image de marque.
- **Conséquences internes,** avec des problèmes de **fonctionnement de l'entreprise** et de **satisfaction des employés**, ou des **partenaires**.
- **Conséquences juridiques**, avec éventuellement des poursuites en cas de manquement à ses obligations.

Comment mettre en place un PCA / PRA

Mettre en place un PCA ou un PRA, c'est mettre en place une **cellule de crise**, des moyens et des procédures permettant de **gérer l'incident** et d'assurer la **continuité** ou la **reprise** de l'activité.

Cette organisation doit comprendre l'ensemble des éléments suivants :

- **Les fournisseurs** : il s'agit de vérifier l'engagement contractuel avec les fournisseurs clés, de mettre en place une stratégie d'achat multifournisseurs, et de contrôler sa capacité à ré-internaliser…
- **Les sites** : bien souvent, une stratégie de continuité ou de reprise d'activité implique de pouvoir disposer de sites de substitution en cas de problème sur le site de l'entreprise.

Cela implique notamment une sauvegarde des données sur un ou plusieurs hébergement distants et redondants.

- **Les ressources informatiques et télécom** : Il s'agit de mettre en place des procédures, des stratégies de secours, et de manager efficacement les ressources humaines ou techniques en cas de nécessité.
- **L'organisation et le personnel** : Il s'agit de disposer de procédures RH exceptionnelles permettant d'assurer l'acheminement, la suppléance du personnel, le travail à distance ou le travail via d'autres support / matériels.
- **La documentation des procédures :** Il est nécessaire de disposer d'un référentiel documentaire explicitant les mesures d'anticipation, de contournement, les formulaires métiers…

PCA / PRA : en interne ou accompagné

La reprise ou la continuité d'activité étant des enjeux stratégiques important, l'entreprise doit s'assurer que ces démarches sont traitées avec professionnalisme :

- Il est possible d'élaborer son PRA ou son PCA **en interne**, si l'on dispose des compétences nécessaires au sein de son personnel.

- Dans le cas contraire, il sera recommandé de confier cette démarque à **une entreprise spécialisée**, disposant d'une maîtrise technique et d'une expertise reconnue.

PCA / PRA : la démarche

Une fois la décision de traiter en interne ou d'externaliser prise, il reste à mettre en place le PCA ou le PRA en question. Une démarche de PCA/PRA comporte généralement les étapes suivantes :

- **Définition des enjeux, des exigences et des besoins** en matière de disponibilité des données et de processus critiques
- **Classification des informations et des actifs de l'entreprise**
- **Analyse des risques** du système d'information
- **Définition du PCA ou du PRA**
- Définition des **processus de gouvernance** et de **gestion de la crise**
- Accompagnement lors des **phases de tests**

Ainsi, nous venons de mettre en évidence les différents **enjeux liés à la continuité ou à la reprise d'activité**. Lors d'une panne ou d'un incident, les conséquences pour l'entreprises peuvent être importantes. Mettre en place un PCA ou un PRA c'est **établir une organisation et des procédures** permettant de **limiter ou de supprimer les impacts subis par le système d'information**. Cette démarche étant relativement technique et pointue, il est important de la confier à un ou plusieurs collaborateurs compétents, ou encore de l'externaliser en faisant appel à un prestataire spécialisé expert.

DOCUMENT 3

« Pourquoi le plan de reprise d'activité ne doit plus être envisagé comme une option par votre entreprise »

Cyrès.fr - 16 juillet 2018

Les causes d'incidents sur l'infrastructure du système d'information peuvent être diverses : panne matérielle, panne logicielle, panne de backup, cyberattaque, erreur humaine, catastrophe naturelle, etc. Mais une solution existe pour s'y préparer : le plan de reprise d'activité.

Une entreprise sur trois a déjà subi un incident ou une panne qui a nécessité le déclenchement d'un plan de reprise d'activité après sinistre (Etude de Evolve IP, 2015).
Comme l'indique Evolve IP, il ne s'agit pas de savoir si le système d'information d'une entreprise va ou non un jour rencontrer un sinistre, mais plutôt de savoir quand il surviendra.

Et lorsqu'il surviendra, est-ce que l'entreprise sera prête à y faire face ?

En raison de la multiplication des réseaux informatiques, les entreprises doivent à présent établir leurs stratégies de protection de données en tenant compte également des potentielles attaques et des intrusions fréquentes sur les systèmes d'informations (ransomware, cryptolocker, phishing, etc.). L'ouverture d'un marché de solutions destinées à combattre les cyberattaques, reflète clairement cette problématique devenue majeure pour de nombreuses entreprises.

En 2017, ces cyberattaques ne devraient plus être considérées comme des épiphénomènes dans l'activité d'une entreprise.

Pourtant, 54 % des organisations sondées lors de l'étude de Evolve IT dépenseraient moins de 50.000 $ par an à la mise en place d'un plan de reprise d'activité ou de continuité d'activité.
Statistique qui nous indique que l'effort consenti par les entreprises à la sauvegarde de leur patrimoine numérique, au regard de ce que peut coûter à une organisation la perte totale ou partielle de ses données, reste faible.

Quels risques court une entreprise sans plan de reprise d'activité face à un sinistre sur son activité

93% des entreprises ayant perdu leurs données ou l'accès à celles-ci pendant 10 jours ou plus, ont fait faillite dans l'année suivant la catastrophe.
Cette donnée rapportée par Continuity Central peut faire peur, mais elle indique concrètement la conséquence à court termes d'une rupture d'activité ou de discontinuité des services d'une entreprise.
Alors, quels sont les risques auxquels s'expose une entreprise n'ayant pas élaboré de plan de reprise d'activité ou n'ayant pas entamé à minima une réflexion en ce sens ?

LES IMPACTS D'UN SINISTRE SUR L'ENTREPRISE

Les effets ressentis seront tout d'abord d'ordre opérationnel et fonctionnel. Si aucune mesure n'existe en faveur du rétablissement des services, les équipes peuvent être directement impactées dans leur travail (arrêt de machine, de serveur, d'accès au réseau, etc.), les outils de communication internes et externes peuvent être inutilisables, etc.

Assez rapidement, le pouls de l'entreprise ralenti et son activité, tout comme sa visibilité, peuvent disparaître des radars de ses fournisseurs, de ses partenaires, de ses clients et de ses prospects. En d'autres termes plus le « délai d'invisibilité » sera court, moins l'impact sera négatif pour l'entreprise.

D'un point de vue commercial et financier, il peut s'en suivre des pertes sur les ventes ou la signature de contrats. Mais c'est également la perte de clients, voir de parts de marché qui peuvent être observées. Plus le cycle de vente propre au business modèle de l'entreprise sera court, plus les pertes d'un point de vue commercial seront immédiates.
Imaginons un instant que la plate-forme web d'Amazon France ne soit plus accessible pendant 1 heure de forte affluence.

Pour essayer de se représenter cela, le lundi 8 décembre 2014, Amazon enregistrait un nombre record de plus de 1 million de colis expédiés en une journée, depuis le réseau de distribution France. On peut supposer que l'heure d'inaccessibilité au service, lors de cette journée, aurait fortement impactée les revenus financiers d'Amazon.

A l'inverse, avec un cycle de vente moyen à long, l'entreprise a des chances d'essuyer moins de pertes directes. Il s'agira alors pour elle de rétablir au plus vite ses services.
Cependant cela pourra avoir d'autres impacts, comme sur l'image et la réputation de l'entreprise ou encore sur la confiance des partenaires. Une Marketplace, un système de paiement en ligne, une plateforme de réservation de chambre d'hôtel pourraient voir une part des utilisateurs s'orienter vers de nouveaux prestataires ou communiquer négativement à l'encontre du service défaillant.

Comment se préparer en prévision d'un sinistre sur l'activité de son organisation ?

Bien que la réponse comporte de multiples volets selon les types de sinistres, leur envergure, la structure de l'organisation impactée, il est impératif de construire en amont un plan de reprise d'activité, c'est-à-dire de récupération des données et de réactivation des services perdus qui, sera éprouvé et testé avant sa mise en application, le jour du sinistre.

L'objectif pour une entreprise sera donc de monter un plan de reprise d'activité qui idéalement, devra être couplé avec un plan de continuité d'activité.
Lors du processus d'élaboration du plan de reprise d'activité, il sera obligatoire d'identifier les activités de l'entreprise considérées comme critiques, d'interviewer les responsables de chaque activité, de déceler l'origine probable de futurs sinistres, de définir les besoins humains et matériels qui soutiendrons la mise en œuvre du plan, d'estimer les coûts liés à la réalisation et au déroulement du plan de reprise, etc.

Autant de critères à appréhender, qui plus ils seront nombreux et collectés de manière précise, favoriseront le déclenchement et la réalisation du plan de reprise informatique par tous les acteurs concernés.

11 ÉTAPES À SUIVRE POUR BIEN DOCUMENTER UN PRA INFORMATIQUE

Que le PRA informatique soit construit en s'appuyant sur un site de secours, un Datacenter ou qu'il soit construit dans le Cloud sur des ressources informatiques virtualisées, il convient d'adopter une démarche logique et parfaitement documentée pour assurer la performance d'un plan de reprise d'activité informatique.

Pour repère voici 11 étapes préalables et essentielles à avoir en tête pour mener à bien la constitution d'un plan de reprise d'activité pour son entreprise :

1. Faire un audit de tous les risques de pannes possibles sur le système d'information et identifier les causes probables : panne matérielle, panne logicielle, cyberattaque, coupures électriques, incendie, catastrophe naturelle, erreur humaine, etc.

2. Détecter et évaluer chaque risque pour identifier les applications métiers qui ne pourront pas fonctionner en mode dégradé. Il faut donc bien appréhender et mesurer la tolérance aux pannes de l'ensemble du système d'information.

3. Définir la criticité des environnements applicatifs et les besoins de sauvegarde et réplication ainsi que de restauration qui devront s'appliquer. Devront être définis ici le RTO (Recovery Time Objective) et le RPO (Recovery Point Objective).

4. Prévoir des sauvegardes automatiques à une fréquence correspondant au besoin de l'organisation.

5. Faire du « Crisis Management », c'est-à-dire attribuer des rôles et des tâches à des personnes précises qui auront la responsabilité d'intervenir le moment venu.

   En d'autres termes, il faut organiser et mobiliser ses équipes pour agir efficacement lors du sinistre.

6. Définir des priorités et un coût de reprise d'activité : évaluer des seuils d'indisponibilité des services et les prioriser afin de définir le coût de remise en service de l'infrastructure.

   Selon les cas, la reprise d'activité devra pouvoir s'effectuer en moins d'une minute.

   La mise en place nécessaire d'environnements synchrones élèvera alors rapidement les coûts par exemple.

7. Définir le choix de l'équipement de sauvegarde et de reprise d'activité ainsi que le budget qui y sera consacré. Il faut savoir que le doublement simple du matériel existant sur un site distant peut ne pas suffire selon les cas. Le choix du matériel est donc important si l'on veut qu'il puisse supporter la charge d'une remise en service.

8. Tester régulièrement le plan de reprise d'activité : bien que le coût d'un test de PRA informatique soit conséquent, il est impératif d'évaluer régulièrement sa fiabilité à minima deux fois par an.

9. Faire évoluer le plan de reprise d'activité en fonction des changements apportés au système d'information : le SI d'une entreprise évoluant constamment, il est essentiel de répercuter ces changements sur le PRA informatique construit initialement afin d'en assurer sa fiabilité.

10. Documenter précisément le PRA: il faut encourager le retour d'expériences des acteurs garants de la fiabilité du PRA en le documentant précisément. Le partage de la connaissance du SI va directement impacter les performances d'un PRA informatique.

    Ainsi, les phases de tests ou les remontées d'échecs doivent être systématiquement documentées, ce qui est généralement peu souvent le cas.

11. Prendre en compte les contraintes réglementaires auxquels certaines typologies d'organisations doivent se conformer dans l'exécution de leurs activités.

Quels critères retenir pour le maintien d'un plan de reprise d'activité fiable et performant dans son entreprise ?

Chaque entreprise avance différemment dans sa stratégie de sauvegarde et de protection de ses données numériques. Certaines disposent déjà d'un PRA associé à un PCA, d'autres ont initié des démarches préliminaires auprès de prestataires spécialisés ou évaluent simplement la pertinence d'un PRA / PCA pour leur organisation.

Parmi ces stades d'avancement autour d'un projet de PRA informatique, certaines interrogations doivent être levées en amont :

- Quel périmètre peut couvrir un prestataire dans la réalisation d'un PRA informatique ?

- Quels sont les éléments qui doivent être pris en charge par le prestataire et consignés dans le contrat de plan de reprise d'activité ?

- En cas de panne, quelles sont les garanties de retrouver ses services, ses données et sous quels délais ?

- Quelle sera la capacité du prestataire à détecter d'éventuels risques futurs et quelle sa réactivité pour en alerter l'entreprise ?

Que l'on parle d'un plan de reprise d'activité sur site ou dans un Datacenter, la transparence des informations et la nature des communications entre le prestataire et l'entreprise sont essentielles à la tenue d'un PRA qui soit performant. La qualité du plan de reprise d'activité reposera également sur la capacité d'une équipe technique à remettre en cause régulièrement la fiabilité de son infrastructure et ce, pendant toute la durée du contrat.

DOCUMENT 4

« Administration numérique et sécurité informatique : quels enjeux dans les communes ? »

Cogitis.fr - site consulté en mars 2020

Avec le développement du numérique, et sa présence de plus en plus importante au cœur de l'organisation des collectivités, les Communes se trouvent aujourd'hui confrontées à un réel défi.

Intéressons-nous tout d'abord à l'environnement informatique des Communes.

L'environnement informatique des Communes

Sur la base de nos retours d'expérience issus de nos interventions pour les Communes, nous pouvons faire plusieurs constats :

L'informatique d'une Commune peut se résumer en une série d'outils (logiciels et postes de travail) mis à disposition des différents métiers (finances, RH, services techniques, secrétariat…) et fonctionnant sur un équipement (serveur) centralisant les informations traitées (données).

Cette informatisation a démarré il y a déjà de nombreuses années et elle est, dans la plupart des Communes, bien intégrée. Aujourd'hui, les collectivités échangent de plus en plus avec des interlocuteurs externes variés (Etat, autres collectivités, citoyens, prestataires…) dans le cadre notamment des projets de dématérialisation mis en place (site Internet, portail usagers, Comedec, Acte, Hélios, plateforme de Marchés publics…).

Or, ces interactions complexifient la mise en œuvre de cette informatisation, du fait de son impact sur l'organisation et des risques liés à la sécurité informatique.

Le premier constat est donc que la complexité vient principalement des échanges entre la collectivité et son environnement extérieur.

Le deuxième constat concerne l'organisation mise en œuvre par les Communes pour gérer l'informatique. Lorsqu'elles sont de taille moyenne, elles peuvent disposer de ressources en interne (informaticiens) et/ou de prestataires sur lesquels s'appuyer pour gérer tout ou partie de l'informatique (infogéreurs, mainteneurs…).

Pour ces Communes, le constat est que l'organisation de la gestion de l'informatique est souvent perfectible : informaticien accaparé par les tâches quotidiennes, difficulté de compréhension entre l'informaticien et les utilisateurs, prestataires non suffisamment cadrés…

Pour les petites et très petites Communes, le constat est en revanche très souvent qu'il n'y a pas de compétence en interne et qu'elles ne savent donc pas à qui s'adresser, sauf à faire confiance à un prestataire local, qui bien souvent les conseille, fournit le matériel préconisé et le met en œuvre.

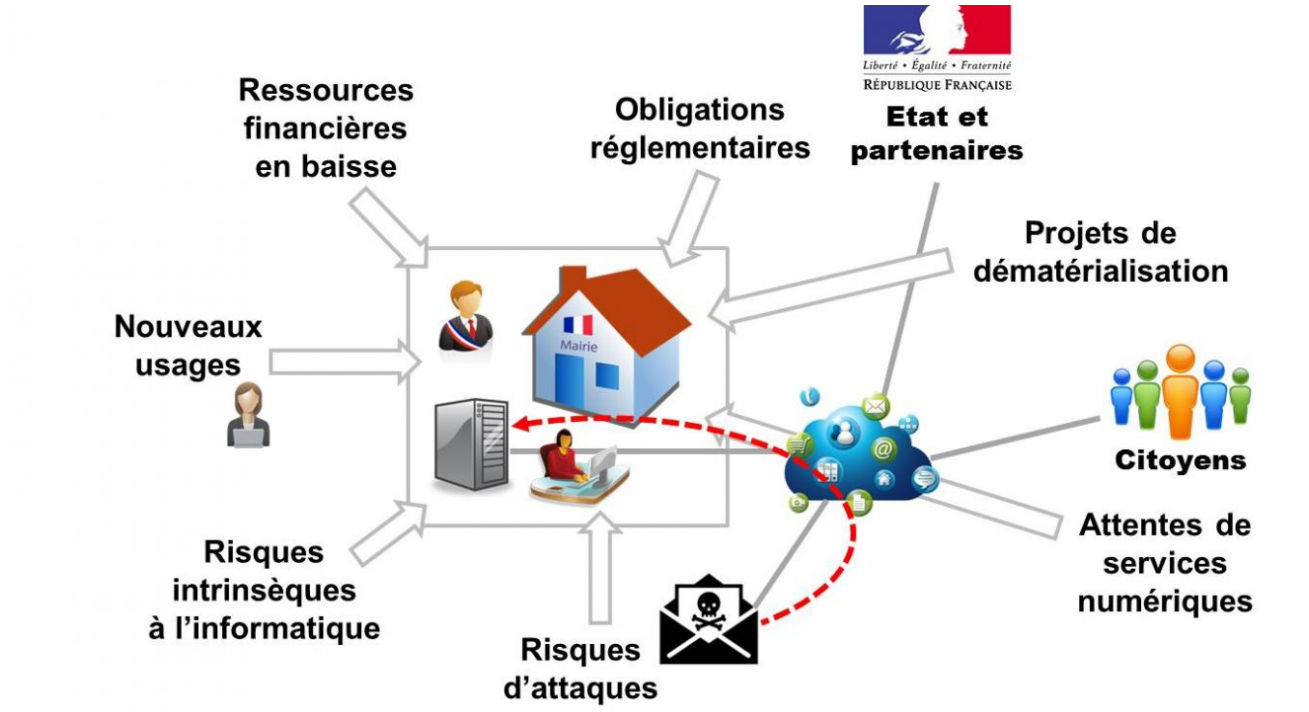
Une alternative, qui pourrait se développer d'avantage à court terme, consiste à mutualiser la gestion de l'informatique avec une structure de taille plus importante : Communauté de Communes, Agence technique départementale, Syndicat mixte…

Dans les deux cas, que les Communes soient de petites tailles ou de taille plus importante, les budgets alloués à l'informatique sont souvent trop réduits pour s'inscrire dans une vraie stratégie numérique. Il est en effet plus aisé pour les élus de donner leur aval pour un investissement qui semble évident et directement utile pour les administrés (comme une extension de la cantine scolaire) que pour un investissement informatique plus difficile à appréhender et utile pour le fonctionnement interne de la structure (virtualisation du serveur de la mairie, par exemple).

Intéressons-nous à présent à l'environnement extérieur des Communes.

L'environnement extérieur des Communes

L'informatique de la collectivité, ou son appellation plus récente d'administration numérique, subit des contraintes fortes, que nous pouvons regrouper en 7 catégories :
Schéma administration numérique communes



Source : Cogitis

- Tout d'abord, il faut tenir compte des contraintes intrinsèques à l'informatique : pannes, investissement non pérenne, organisation non efficiente, pertes de temps pour les utilisateurs…Il

- faut citer, aussi, les contraintes liées aux nouveaux usages : mobilité des agents et des élus, mise en place de la vidéosurveillance, présence sur les réseaux sociaux, objets connectés…

- Nous ne pouvons bien évidemment pas passer sous silence la contrainte budgétaire forte qui conditionne l'ensemble du fonctionnement de la Commune sans épargner l'administration numérique.

- Viennent ensuite les obligations réglementaires auxquelles la Commune ne peut se soustraire (Saisine par Voie Electronique, désignation d'un « Data Protection Officer » pour la protection des données personnelles…).

- Nous avons déjà évoqués les nombreux projets de dématérialisation mis en place par l'Etat : Acte (contrôle de légalité), Hélios (finances), Comedec (données de l'état civil), réponse électronique à un marché public…

- Autre contrainte majeure, avec le développement des usages, les exigences des citoyens en termes de services numériques sont de plus en plus fortes : services fiables, simples, accessibles depuis n'importe quel équipement, disponibles 24h/24 et 7j/7…

- Enfin, nous terminerons avec les risques d'attaques, via Internet bien souvent, qui ont beaucoup alimenté la presse ces dernières années.

Attardons-nous un peu sur ces derniers…

Lorsque l'on pense « attaque informatique », on se dit souvent, « je ne suis pas concerné, qui s'intéresse à mes données ? ». Malheureusement, les attaques ne sont pas l'apanage des sociétés du CAC 40 ou des start-up high tech. Toutes les structures sont des cibles potentielles, en particulier avec les fameux « crypto-virus » (ou « rançon-wares »), qui cryptent les données et les rendent inutilisables sauf à verser une rançon contre un hypothétique décryptage de celles-ci.

Dans ce cas, du point de vue du pirate informatique, il est plus intéressant d'attaquer beaucoup de petites structures (ou individus), dont une petite proportion payera la fameuse rançon, qu'une structure de taille plus importante, probablement mieux protégée, qui laisserait s'échapper des données à forte valeur ajoutée dans le cadre d'une attaque sophistiquée.

Autre phénomène qui peut toucher les Communes plus facilement qu'on ne le pense : l'ingénierie sociale. Cette technique consiste à recueillir des informations, a priori, peu sensibles mais qui mises bout à bout finissent par ouvrir une brèche dans le système d'information. Par exemple, si l'on demande à une secrétaire de Mairie son code d'accès pour se connecter au réseau informatique ou à un logiciel important, il est peu probable qu'elle le donne.

En revanche, si on l'appelle en demandant celui du logiciel qui gère la bibliothèque et en se faisant passer pour l'éditeur de ce logiciel, il est plus probable qu'elle le fournisse. Et si ce mot de passe est le même que celui utilisé pour se connecter au réseau, ou permet facilement de le déduire, le tour est joué.

Nous ne listerons pas ici toutes les attaques possibles mais la liste est longue et variée, les pirates informatiques étant toujours inventifs et très réactifs pour utiliser les dernières failles connues.

On comprend donc que l'environnement de l'administration numérique des Communes est en constante évolution et de plus en plus contraignant. Mais, quoi qu'il en soit, il ne faut pas oublier que cette dématérialisation est une source d'opportunités majeures pour les Communes : gains d'efficacité, nouveaux services, meilleure capacité à appréhender les évolutions…

La question n'est donc plus de savoir si les Communes doivent aller, ou non, vers l'administration numérique, mais comment s'organiser pour limiter les risques et gérer au mieux la sécurité informatique ?

Gérer la sécurité informatique

En cas de sinistre informatique, deux questions clés se posent :

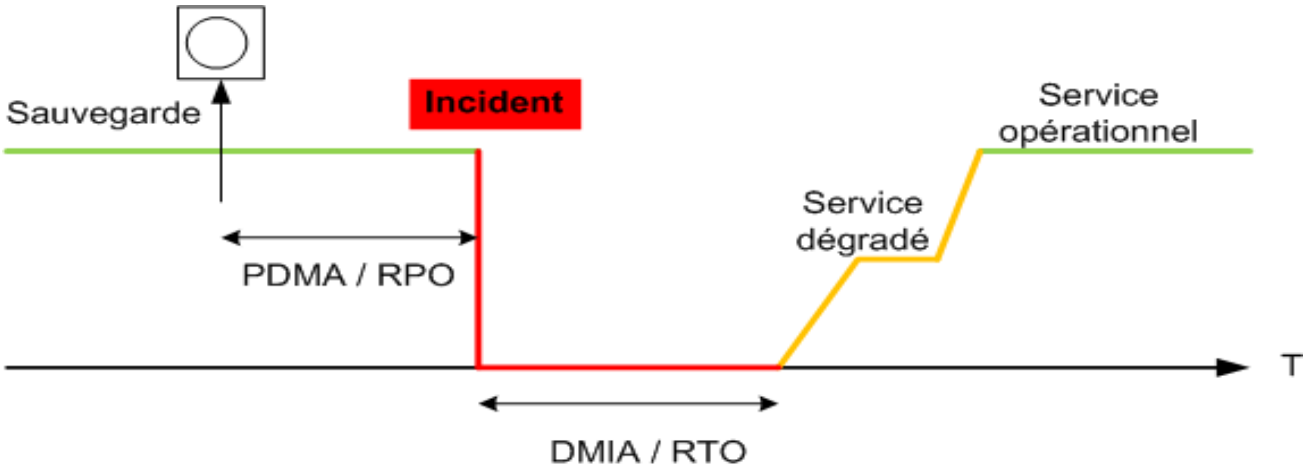
Premièrement, pendant combien de temps les agents de la Commune seront-ils dans l'incapacité de travailler avec leur outil informatique ? C'est ce que les anglo-saxons appelle le « RTO » pour « Recovery Time Objective » ou Durée Maximale d'Interruption Admissible (DMIA), en français.

Cette question renvoie à la sécurisation des équipements. Il faut donc redonder (doublonner) les équipements les plus importants, sécuriser l'accès physique au local informatique, disposer de contrats de maintenance avec pénalités si les délais ne sont pas respectés, mettre à jour les logiciels des principaux composants…

La deuxième question est : de quand datent les données (ou les traitements) que nous allons pouvoir récupérer, pour redémarrer l'activité ? C'est le « RPO » pour « Recovery Point Objective » ou Perte de Données Maximale Admissible (PDMA), en français.

Cette deuxième question renvoie, quant à elle, à la sécurisation des données. Il faut donc mettre en place des sauvegardes exploitables, disposer d'outils pour filtrer les accès depuis l'extérieur, sensibiliser les utilisateurs, gérer les mots de passe…

Ces deux concepts clés sont illustrés dans le schéma ci-après :



Les principales actions préventives sont, en général, mises en œuvre par les informaticiens des Communes ou les prestataires, mais comment s'assurer que des mesures importantes n'ont pas été oubliées ?

Pour cela l'Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI), organisme de référence en France, fournit et tient à jour un précieux « guide d'hygiène informatique » regroupant 42 mesures permettant d'éviter, théoriquement, 80% des risques liés à la sécurité informatique. Il ne faut donc pas hésiter à s'en servir (www.ssi.gouv.fr).

Enfin, dernier conseil pour gérer cette sécurité : commencer modestement par le traitement des risques les plus importants, « accepter » provisoirement les autres risques et mettre en place une démarche d'amélioration continue selon le principe de la « roue de Deming ». Ainsi, après un premier tour de roue et la mise en œuvre des premières mesures (au cours de la 1ière année, par exemple) vous pouvez vérifier que celles-ci sont efficaces, le cas échéant les corriger, et entamer un deuxième « tour » pour traiter la série de risques suivants et éventuellement de nouveaux risques apparus depuis.
Le RGPD, Règlement Général pour la Protection des Données, qui entre en vigueur en mai 2018 et dont il est beaucoup question ces derniers temps, est basé sur ce principe.

Ainsi, vous mettez en place progressivement mais surement un Système de Management de la Sécurité de l'Information (SMSI).

Accompagner la transformation numérique des collectivités

Pour conclure, il faut retenir que l'administration numérique et sa sécurité font aujourd'hui partie intégrante de la vie de la Commune et que l'on ne peut les ignorer.

Si sa gestion semble compliquée, c'est avant tout car cette problématique est relativement récente et qu'elle demande un niveau de connaissance minimum. Il est donc important pour les élus et les décideurs de s'y intéresser afin de monter en compétence progressivement.

Des solutions existent pour accompagner la transformation numérique des collectivités : assistance, formation, infogérance, externalisation, mutualisation…
L'enjeu est principalement de trouver le bon niveau d'accompagnement en regard des ressources humaines et financières disponibles.

Enfin, retenez que comme dans la plupart des évolutions majeures, c'est la première marche qui est la plus dure à gravir.

DOCUMENT 5

« Les bonnes pratiques d'un PRA réussi »

Silicon.fr - site consulté en mars 2020

Un Plan de Reprise d'Activité Informatique met en œuvre les procédures et les moyens matériels, technologiques et humains nécessaires à l'entreprise pour faire face à un sinistre. Le PRA permet de maintenir les fonctions stratégiques du SI.

Incendie, inondation, panne électrique, virus, avarie ou perte d'un serveur. Aucune entreprise n'est à l'abri de dommages susceptibles de dégrader ou de paralyser son système d'information. Or, aujourd'hui, plus aucune entreprise ne peut fonctionner sans son informatique. C'est pourquoi les sociétés se doivent d'anticiper d'éventuels sinistres en déployant, dans des lieux distants ou dans le Cloud, l'infrastructure matérielle et logicielle, les processus de transfert de données, et les procédures d'intervention, pour être en mesure de reprendre leur activité le plus rapidement possible.

Baptisées PRA, ou Plan de Reprise d'Activité, ces solutions de secours nécessitent quelques bonnes pratiques de déploiement pour assurer une reprise dans les meilleurs délais et conditions. Mise en place d'un PRA efficient en sept points.

1. Nommer un responsable

Si le PRA est un projet d'entreprise qui nécessite l'implication du comité de direction, il est impératif de confier cette activité à un chef de projet lié à la DSI.

En concertation avec les autres directions métiers et la direction générale, il aura pour mission de réaliser des audits et des analyses technologiques et organisationnelles du système d'information afin de définir le périmètre du PRA et son fonctionnement.

Par ailleurs, il est pertinent de s'appuyer sur un prestataire de services spécialisé qui offre des garanties de moyens technologiques et humains et de résultats, tout en diminuant les coûts grâce à la mutualisation de ses prestations avec d'autres clients.

2. Faire l'inventaire de l'existant

Le chef de projet doit, pour mettre en œuvre un PRA efficient, avoir une connaissance exhaustive et à jour de l'existant informatique et télécom de l'entreprise. « Ainsi, il doit dresser un inventaire des applicatifs (identification de toutes les solutions logicielles et leurs process), du réseau (débit, type de lien) et de l'infrastructure (serveurs physiques et virtuels) présents sur tous les sites de l'entreprise », explique Christian Laporte chef de produit Storage Division chez HPE.

Il doit notamment réaliser une classification des différentes activités par niveau de criticité, tout en précisant les différents liens entre ces activités. Enfin, il doit faire un état des lieux de tous les types de sauvegardes mis en œuvre dans l'entreprise : périodicité, délai de sauvegarde, volumétrie.

3. Définir le périmètre du PRA

La mise en place d'un PRA nécessite de définir une priorité dans la remise en service des applications. « Quelles sont les activités les plus stratégiques pour l'entreprise ? Quelles sont celles qui peuvent souffrir d'un arrêt temporaire de fonctionnement ? Dans une entreprise d'e-commerce, par exemple, il est crucial de faire repartir au plus vite le système de commandes, pour éviter un impact préjudiciable à l'activité et à l'image de l'entreprise. Citons les milliers de coordonnées d'abonnés de plusieurs grands titres nationaux qui auraient été perdus par un prestataire de services et qui auraient donc bloqué la facturation de leurs abonnements » illustre Christian Laporte. Un PRA nécessite donc de bien identifier le degré de criticité des applicatifs.

Autres points importants : le RTO (Recovery Time Objective) c'est-à-dire la durée maximale d'interruption admissible de l'activité et le RPO (Recovery Point Objective), correspondant à la durée maximale d'enregistrement des données qu'il est acceptable de perdre. « Généralement le RPO exprime l'âge des données qui pourront être utilisées en remplacement lors de leur restauration. Les entreprises doivent donc se poser la question du niveau de pertes de données acceptable pour définir la périodicité de la réplication et de la sauvegarde des données, et le délai maximal acceptable de remise en service des applications, » explique Christian Laporte.

4. Définir l'infrastructure

L'idéal pour une entreprise est de disposer de deux sites dotés d'une infrastructure IT pouvant se protéger mutuellement tout en hébergeant leurs propres applications.
Dans cette configuration, un processus de réplication assure la duplication des données critiques d'un site à l'autre permettant ainsi, en cas d'incident majeur sur l'un des sites, de redémarrer les applications critiques à partir du second site.

Toutefois, pour des questions de coûts, il n'est pas nécessaire de disposer d'une infrastructure strictement identique sur chacun des sites. « En revanche, insiste notre interlocuteur, si la réplication est assurée par des baies de stockage, celles-ci doivent provenir du même constructeur et être issues de la même gamme. Cette option est la plus onéreuse. »

Dans le cas où l'entreprise ne dispose que d'un site, souscrire un contrat auprès d'un prestataire informatique permet de disposer à distance d'une infrastructure partagée ou dédiée en fonction du budget de l'entreprise. « Toutefois, il faudra s'assurer de son expertise en matière de PRA/PCA et vérifier les niveaux de service et les engagements inclus dans le contrat », prévient Christian Laporte.

5. Mise à jour et tests récurrents du PRA

Pour être performant, un PRA doit suivre toutes les évolutions d'infrastructure et de logiciels (nouveaux applicatifs, nouvelles mises à jour) de l'entreprise ainsi que les changements de ses process. « Il faut tester la plate-forme pour vérifier que les process de réplication et de protection des données sur les baies de stockage fonctionnent bien », insiste notre interlocuteur.
Il est également important d'évaluer régulièrement le PRA afin d'étudier les difficultés techniques, logistiques ou humaines qui pourraient intervenir en cas de basculement de l'informatique.

6. Définir les procédures d'intervention

Différents standards, recommandations et normes de type ISO, BSI ou ITIL existent en matière de PRA, dont les niveaux de précision sont variables. Certains secteurs d'activité, comme les banques notamment, ont des obligations en matière de reprise d'activité. L'Autorité des Marchés Financiers (AMF) demande ainsi à ce que toutes les sociétés de gestion de portefeuilles agréées par l'AMF disposent d'un PRA.
Par ailleurs « toutes les actions à effectuer en cas d'incidents doivent être documentées et les personnes en charge du rétablissement doivent être formées aux procédures », souligne Christian Laporte.

7. Définir le budget

Bien qu'essentiel dans la continuité de l'activité de l'entreprise, le PRA est généralement perçu comme un centre de coût. Or, en cas de sinistre, ce plan limite les lourdes pertes financières infligées par l'arrêt de l'activité.
Mettre en place un PRA nécessite donc d'effectuer un calcul comparatif entre son coût et le coût des temps d'immobilisation. C'est au responsable de projet que revient la délicate mission d'évaluer la probabilité des risques, leur impact sur l'activité de l'entreprise, le budget du PRA, et la pertinence de la solution technique envisagée.

DOCUMENT 6

« L'ISO 27701, une norme internationale pour la protection des données personnelles »

cnil.fr - 2 avril 2020

La norme ISO 27701 est une norme internationale qui décrit la gouvernance et les mesures de sécurité à mettre en place pour les traitements de données personnelles, en étendant deux normes bien connues de la sécurité informatique.

La norme ISO 27701, publiée en août 2019, se base sur deux normes ISO de sécurité de L'information et les étend pour intégrer la protection des données personnelles :

- l'ISO 27001, qui certifie un système de management de la sécurité informatique ;
- l'ISO 27002, qui détaille les bonnes pratiques pour la mise en œuvre des mesures de sécurité nécessaires.

Les exigences de l'ISO 27701

Afin de standardiser et de renforcer la protection des données personnelles, l'ISO 27701 :

- étend le système de management de la sécurité de l'information pour inclure les particularités des traitements de données personnelles :
    - détermination du rôle de l'organisme à certifier (responsable de traitement, sous-traitant) ;
    - gestion unifiée des risques informatiques pour l'organisme et des risques pour la vie privée des personnes concernées, désignation d'un responsable pour la protection de la vie privée (dans le cadre de l'ISO 27701, il s'agit du délégué à la protection des données) ;
    - sensibilisation des personnels, classification des données, protection des supports amovibles, gestion des accès et chiffrement des données, sauvegarde des données, journalisation des événements ;
    - conditions de transferts de données, protection de la vie privée dès la conception et par défaut (*privacy by design and by default)*, gestion des incidents ;
    - conformité aux exigences légales et réglementaires, etc.

- apporte des mesures spécifiques aux traitements de données personnelles, en tenant compte du rôle de l'organisme (responsable de traitement, sous-traitant, sous-traitant de sous-traitant) :
    - principes fondamentaux : finalité de traitement, base légale, recueil et retrait du consentement, inventaire des traitements, évaluation des impacts pour la vie privée ;
    - droits des personnes : information, accès, rectification, suppression, décision automatisée ;
    - protection de la vie privée dès la conception et par défaut (*privacy by design and by default)* : minimisation, dé-identification et suppression des données, durée de conservation ;
    - contrats de sous-traitance, transferts et partage de données.

Des contributions d'experts et d'autorités de protection des données

Cette norme a été rédigée au niveau international, avec les contributions d'experts provenant de tous les continents et la participation de nombreuses autorités de protection des données. Les experts de la CNIL y ont activement œuvré, avec le soutien de l'AFNOR et du Comité européen de la protection des données (CEPD).

Le RGPD a été pris en compte, ainsi que les autres grands textes de protection des données (dont ceux adoptés par l'Australie, le Brésil, la Californie, le Canada). La proximité de la norme avec le RGPD est ainsi matérialisée par une annexe dédiée, qui établit la correspondance entre les articles de la norme et ceux du RGPD. Et la mise en place d'un système de management, avec la gestion et la documentation de la protection des données, répond au principe général de responsabilité (*accountability)* du RGPD.

En résumé, la norme ISO 27701 a une portée mondiale : elle n'est pas spécifique au RGPD et ne constitue pas, en tant que telle, une certification au sens de l'article 42 du RGPD.

Mais elle présente l'état de l'art en protection de la vie privée et elle permet aux organismes qui l'adoptent de monter en maturité et de démontrer une démarche active de protection des données personnelles.

Sa traduction en français est actuellement soumise à enquête publique par l'AFNOR.

DOCUMENT 7

« PRA en cloud : à quoi faut-il s'attendre ? »

Erin SULLIVAN - *Le MagIT* - 25 juillet 2019 - 2 pages

Le Plan de Reprise d'activité est un processus critique que toutes les entreprises doivent considérer. La montée en puissance des services en cloud suggère qu'elles pourraient même opter pour du PRA en ligne. Mais est-ce une option viable ?

Le cloud est-il une option envisageable pour un Plan de Reprise d'Activité (PRA) ? Alors que l'on imagine tout de suite que des questions de sécurité vont se poser, il est indéniable qu'utiliser le cloud comme plateforme de secours présente des avantages.

Les avantages d'utiliser des ressources en cloud pour un PRA comprennent un meilleur contrôle des coûts et un accès à distance aux données en cas d'incident, qui répondront aux attentes des entreprises de toutes tailles. Revers de la médaille, un tel processus en ligne présente certaines particularités auxquelles il faudra prêter attention et leur importance diffère selon le type d'organisation dans lequel on travaille.

Voici les cinq questions-type à se poser avant de passer à la reprise d'activité en cloud et les réponses que donnent les experts IT que nous avons consultés.

Quelles sont les caractéristiques à considérer dans une offre de PRA en cloud ?

Plusieurs facteurs sont à considérer lorsque l'on évalue une solution de PRA en cloud. Évidemment, la sécurité arrive au premier chef. Pour y répondre, il est nécessaire de s'assurer que toutes les données stockées en ligne seront chiffrées. Il faut aussi déterminer ce qui doit être protégé, le degré d'importance des informations et en combien de temps elles devront être restaurées.

Après la sécurité, vient la faculté de gérer les données avec une forte granularité.

Ne serait-ce qu'à cause du RGPD, les entreprises doivent pouvoir accéder très rapidement au moindre fichier sans avoir besoin de débloquer tout un lot d'autres données. Fort heureusement, la plupart des fournisseurs de cloud autorisent un haut niveau de granularité, néanmoins la bonne pratique consiste à toujours vérifier ce détail avant de souscrire à une offre.

Le PRA en cloud peut-il aussi servir de PCA ?

La continuité d'activité (PCA) va de pair avec la reprise d'activité. Restaurer les ressources IT et relancer dessus la production en un minimum de temps est un objectif de plus en plus souvent vital pour l'activité. En clair, il ne doit y avoir ni échec ni retard dans la restauration.

Dans les faits, la simple utilisation du cloud à des fins de PRA s'avère une bonne option pour atteindre la continuité d'activité. Pour peu que les bonnes options aient été déployées, il devient possible de rendre les opérations les plus critiques résistantes aux pannes, sans pour autant avoir écrit des scripts de résilience.

Revers de la médaille, le PRA en cloud serait si efficace qu'il menacerait l'emploi des experts de la continuité d'activité.

Comment le cloud sauve-t-il l'activité en cas de sinistre ?

Le terme de sinistre est vague ; il va de la coupure de courant sur un serveur à l'incendie qui ravage les locaux. Peut-on se préparer au pire ? En conservant une copie des données hors-site, un PRA permet aux salariés de continuer à travailler à distance sans se soucier des infrastructures encore en état de marche.

Outre s’assurer que les données sont sauvegardées ailleurs, régulièrement et de manière fiable, l’entreprise ne devra pas négliger de déployer des accès réseau avec une bande passante suffisante pour permettre à chacun de continuer à travailler.

Quel est l’avis des entreprises sur le PRA en cloud ?

Selon les professionnels, le problème du PRA n’est pas le cloud, il est avant tout que trop peu d’entreprises sont sûres que le leur fonctionne.

Seules 22 % des entreprises ont confiance dans leur Plan de Reprise d’Activité, Etude de TechTarget Research

Et il ne s’agit pas nécessairement de celles qui ont un PRA en cloud, puisque seule une entreprise sur cinq sauvegarde ses données en cloud et que 17 % indiquent que le cloud n’est chez elles qu’un composant de leur PRA.

Dans la pratique, le cloud n’est pas le problème. Le palmarès des caractéristiques qui posent vraiment question est, dans l’ordre, la capacité à monter en charge, la compatibilité avec les infrastructures en place, la taille disponible, la simplicité d’utilisation et la compatibilité avec les serveurs virtuels.

On notera que ces problématiques sont toutes listées par les fournisseurs parmi les principaux avantages qu’apporte un PRA en cloud.

Quel est l’avenir du PRA en cloud ?

Certains prédisaient que le cloud aurait un succès éphémère. A l’évidence, ce n’est pas le cas. Au contraire, le cloud s’est imposé sur tous les aspects de l’IT et rien n’empêche qu’il fasse de même sur le domaine particulier du PRA.

L’évolution prévisible est celle vers le cloud hybride et des outils de gestion simplifiés. Une mode récente chez les fournisseurs de cloud, est de positionner leurs services de reprise d’activité comme étant aussi fiables que les ressources virtuelles qui se relancent dans la seconde même après un incident.

Même si la technologie ne permet pas de parler véritablement de Plan de continuité d’activité (dans lequel des ressources de secours sont déjà en production au moment de l’incident), c’est pourtant bien le chemin qu’elle prend. Les géants du cloud public, AWS, Microsoft et Google, travaillent à améliorer leurs offres et il est peu probable que le PRA en cloud n’évolue pas encore plus.

DOCUMENT 8

« La Politique de Sécurité des Systèmes d'Information de l'État (PSSIE) - Agence nationale de la sécurité des systèmes information »

SSI.gouv.fr - 17 juillet 2014

La PSSIE fixe les règles de protection applicables aux systèmes d'information de l'État.

Ce document est l'aboutissement de travaux pilotés par l'ANSSI qui s'appuient sur l'expérience des participants ministériels et de l'Agence en matière de prévention et de réaction aux attaques informatiques.

RÉFÉRENCE

Politique de sécurité des systèmes d'information (PSSIE) portée par la circulaire du Premier ministre n° 5725/SG du 17 juillet 2014.

CONTEXTE

Essentiels à l'action publique, les systèmes d'information sont porteurs d'efficacité, mais aussi de risques : menaces d'exfiltration de données confidentielles, d'atteinte à la vie privée des usagers, voire de sabotage des systèmes d'information. Afin de prendre en compte ces risques, le Premier ministre a défini une politique volontariste, mais également pragmatique par laquelle l'État affiche sa volonté de se montrer exemplaire en matière de cyber sécurité.

La PSSIE s'inscrit dans le cadre des mesures annoncées en Conseil des ministres le 25 mai 2011 pour faire face à la montée des cyber-attaques. La première version a été publiée par circulaire le 17 juillet 2014.

CHAMP D'APPLICATION

La PSSIE s'applique à tous les systèmes d'information des administrations de l'État : ministères, établissements publics sous tutelle d'un ministère, services déconcentrés de l'État et autorités administratives indépendantes.

Ces administrations sont dénommées « entités » dans le texte. La PSSIE concerne l'ensemble des personnes physiques ou morales intervenant dans ces systèmes d'information, qu'il s'agisse des administrations de l'État et de leurs agents ou bien de tiers agissant au nom et pour le compte des administrations de l'État (prestataires ou sous-traitants) et de leurs employés.

DESTINATAIRES

La PSSIE s'adresse à l'ensemble des agents de l'État, et tout particulièrement :

- aux autorités hiérarchiques, qui sont responsables de la sécurité des informations traitées au sein de leurs services ;
- aux agents chargés des fonctions de directeurs des systèmes d'information (DSI) ;
- aux personnes chargées de la sécurité et de l'exploitation des systèmes d'information.

CONTENU

La PSSIE décline dix principes fondamentaux portant sur le choix d'éléments de confiance pour construire les systèmes d'information, sur la gouvernance de la sécurité et sur la sensibilisation des acteurs. Parmi ces principes, la circulaire met en exergue la nécessité pour les administrations de l'État de recourir à des produits et à des services qualifiés par l'ANSSI ainsi qu'à un hébergement sur le territoire national de leurs données les plus sensibles.

Chaque ministère est désormais responsable de l'application de la PSSIE entrée en vigueur le 29 août 2014. Celle-ci a également été conçue pour constituer une base méthodologique pour tout organisme ou institution, extérieur à l'État, ayant à élaborer un document de cette nature.

DOCUMENT 9

« Coronavirus - Comment les collectivités ajustent leur plan de continuité »

Emeline LE NAOUR - *lagazettedescommunes.com* - Mars 2020

Face à l'allongement de la durée de confinement, les communautés de communes, les villes ou les départements doivent réadapter leur plan de continuité d'activité (PCA) tout en anticipant, dans la mesure du possible, la suite des événements.

« Depuis la mise en place du PCA, il n'y a pas eu de souci majeur. Le seul hic, c'est que cette organisation doit tenir dans le temps malgré la fatigue des agents et les arrêts maladies qui peuvent tomber », signale Sophie Guihard, DGS du département des Côtes-d'Armor (3 300 agents, 598 814 hab.).

Activés en catastrophe dès la fin du mois de février pour certaines collectivités, dans le courant de la première semaine de mars pour les autres, les plans de continuité d'activité (PCA), permettant à une collectivité de fonctionner même en cas de désastre ou de crise majeure, doivent être maintenus dans le temps et réadaptés en fonction de l'évolution de la crise sanitaire.

Une gestion au jour le jour qui demande aux cadres, qui travaillent bien souvent à distance, une réactivité sans faille.

« Nous avons mis en place des roulements de demi-journée pour chaque membre de la direction générale et nous faisons le point deux fois par jour avec les différentes directions de services », détaille encore Sophie Guihard, qui chapeaute 250 agents sur le terrain et presque autant en télétravail.

Définir les missions essentielles

Le service public minimum s'articule autour des services sociaux organisés au sein de cinq antennes qui maillent l'ensemble du territoire. Les agents de ces maisons départementales assurent, également en roulement, la mise à l'abri des personnes vulnérables ainsi que les services liés à la protection maternelle et infantile.

L'émission de bons alimentaires (lettres-chèque) a également été maintenue, le but étant de ne surtout pas rompre la chaîne solidaire au risque que les plus vulnérables « ne paient la note » de cette crise sanitaire.

En parallèle, le conseil départemental a conservé une équipe en charge des interventions liées à la sécurité routière, mais aussi à l'approvisionnement et le service de cantine au sein des collèges destinés aux enfants de personnel soignant.

Autre mission définie dans ce PCA, la gestion des paies et le paiement des fournisseurs, ainsi qu'une permanence téléphonique pour les agents départementaux.

Gestion de crise

De son côté, Laurent Semavoine, DGS de l'agglomération Dracénie Provence Verdon (Var, 442 agents, 23 communes, 115 000 hab.) envisage déjà un PCA en mode « très dégradé ».

Il faut dire que l'intercommunalité est malheureusement rompue à l'exercice, après les inondations de juin 2010 qui avaient coûté la vie à 25 personnes à Draguignan.

« Un PCA avait été établi en 2013 après les crues tragiques. Nous avions donc déjà évalué les différents stades de crise et envisagé notre fonctionnement en mode dégradé », explique Laurent Semavoine qui a réactualisé et activé le plan dès le 28 février.

Pour lui, nul doute que l'anticipation est l'une des clés d'un service public minimal efficient : « Dans le meilleur des cas, il faut envisager cette situation jusqu'à fin avril. Nous sommes prêts », affirme-t-il.

Paiement des agents et des fournisseurs

Pour le moment, en plus du volet RH interne à la collectivité, le service de transports à la demande urbain et interurbain est maintenu, tout comme la gestion des déchets et les services d'eau et d'assainissement ainsi que l'entretien des équipements communautaires. Dans les mairies de l'intercommunalité, seuls les bureaux de l'état civil (naissance et décès) sont toujours occupés. En tout, environ 145 agents restent à la manœuvre de la troisième intercommunalité du Var.

Et si d'aventure le nombre d'agents en capacité d'assurer leur mission chutait drastiquement, seules les missions définies au préalable comme prioritaires subsisteraient. Certains services jugés non-essentiels, comme l'instruction des permis de construire, seraient ainsi stoppés.

Organisation en binôme

Autre impératif inhérent à la gestion de crise : le maintien de la coordination des directions de services. Pour limiter le risque de paralysie de la collectivité, Laurent Semavoine et son équipe fonctionnent toujours en binôme : « Chaque directeur travaille avec son adjoint. Quand l'un se rend à la communauté d'agglomération, l'autre est à distance. Comme ça, nous veillons à garder toujours un « homme fort » en réserve. »

Une règle tacite qui n'est pas sans rappeler celle interdisant au Président de la République, au président du Sénat ainsi qu'au Premier ministre de voyager dans le même avion afin d'assurer la continuité de l'exercice du pouvoir en cas de crash.

Une expérience de la gestion de crise et une connaissance de son territoire partagées également par François Dupouy, DGS de la ville de Metz (2 500 agents et 120 000 hab.).

Dès le début de la pandémie en Italie, le directeur des services a rapidement pris la mesure de la rapidité avec laquelle la crise sanitaire pouvait déferler sur sa région.

Réactualisation du PCA

« Le PCA, qui datait de l'épidémie de H1N1, a été réactualisé très rapidement. Au vu des liens étroits qui existent entre nos voisins transalpins et la Moselle, qui fut pendant longtemps une terre

d’immigration pour les ouvriers italiens, le risque de propagation était assez élevé », retrace François Dupouy qui précise que 300 agents assurent la continuité du service.

A cette anticipation s’ajoute la mise en place d’exercices grandeur nature d’évacuation de quartiers entiers de la ville qui sont réalisés ponctuellement. D’une part en raison du risque majeur de crue de la Moselle et d’autre part afin de mettre rapidement à l’abri la population lors des opérations de désamorçage de bombes datant de la Seconde Guerre mondiale.

« Le 16 mars, tout était en place. Nous avons conservé les services liés à la sécurité des personnes, sécurité des biens, l’état civil, un système de garde d’enfants pour le personnel soignant ainsi qu’une astreinte de veille sociale pour l’accompagnement des personnes isolées et assurer le relogement en urgence », détaille François Dupouy qui indique également qu’un petit nombre de juristes restent d’astreinte pour la prise d’arrêtés.