Sujet élaboré par une cellule pédagogique nationale

CONCOURS INTERNE D'INGÉNIEUR TterritorIAL

SESSION 2021

ÉPREUVE DE PROJET OU ÉTUDE

ÉPREUVE D'ADMISSIBILITÉ :

L'établissement d'un projet ou étude portant sur l'une des options, choisie par le candidat lors de son inscription, au sein de la spécialité dans laquelle il concourt.

Durée : 8 heures
Coefficient : 7

SPÉCIALITÉ : INFORMATIQUE ET SYSTEMES D'INFORMATION

OPTION : SYSTEMES D'INFORMATION ET DE COMMUNICATION

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.
- L'utilisation d'une calculatrice électronique programmable ou non-programmable sans dispositif de communication à distance n'est pas autorisée.
- 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 54 pages dont 2 annexes.
Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.
S'il est incomplet, en avertir le surveillant.

- Vous répondrez aux questions suivantes dans l'ordre qui vous convient, en indiquant impérativement leur numéro.
- Vous répondrez aux questions à l'aide des documents et de vos connaissances.
- Des réponses rédigées sont attendues et peuvent être accompagnées si besoin de tableaux, graphiques, schémas…

Vous êtes ingénieur territorial, chef de projet à la Direction des Systèmes d'Information (DSI) de la Communauté d'Agglomération d'INGAGGLO (800 agents / 200 000 habitants).

Les événements de l'année 2020 (crises climatique, sanitaire, cybercriminalité …) ont montré combien il est important pour toute organisation de disposer d'un plan de reprise de l'activité. Dans ce contexte particulier, les collectivités doivent faire face au double enjeu de la continuité de leurs missions de service public et de la protection de leurs agents.

La récente crise sanitaire a été l'occasion de vérifier que les Collectivités doivent réadapter leur plan de continuité d'activité (PCA) tout en anticipant, dans la mesure du possible, la suite des événements.

En effet, pour organiser le déconfinement, la Communauté d'Agglomération a dû aménager les locaux, rassurer les agents tout en réactivant les services de façon progressive. Une relance bien loin d'un retour à la normale.

Dans ce contexte, le système d'information est un enjeu stratégique pour votre organisation. Le préserver est un sujet majeur pour assurer le bon fonctionnement des activités vitales. En cas de crise majeure, il s'agit d'anticiper et d'en atténuer les effets sur la pérennité des activités.

Fort de ce constat, la Direction Générale souhaite anticiper et maîtriser les risques opérationnels de grande envergure.

La DSI est donc chargée 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.

A l'aide des documents et des annexes, le Directeur des systèmes d'information (DSI) vous demande donc de préparer l'organisation du projet, en répondant aux questions suivantes :

Question 1 (5 points)

a) Au regard des risques encourus et de l'ensemble des risques actuels, quels sont les objectifs et les enjeux à prendre en compte de manière prioritaire dans le cadre de la continuité du service public de la collectivité ? (3 points)

b) Vous analyserez les différences entre un PRA informatique et un PCA informatique et vous préciserez les différents dispositifs possibles, leur finalité et leur articulation.
(2 points)

Question 2 (3 points)

Vous rédigerez une note argumentée en présentant vos préconisations en termes d'organisation et de pilotage de la démarche de mise en place d'un Plan de Continuité

Informatique au service du PCA de la collectivité. Vous préciserez les étapes de la conception à la mise en œuvre.

Question 3 (6 points)

a) Vous établirez un ensemble de propositions opérationnelles et techniques permettant la mise en œuvre d'un Plan de Continuité Informatique, en précisant la démarche méthodologique, les actions immédiates et à moyen terme, les impacts organisationnels et fonctionnels. (4 points)

b) Vous compléterez vos propositions en intégrant les alternatives possibles dans le cloud en argumentant sur leur pertinence. (2 points)

Question 4 (3 points)

La Direction Générale envisage l'assistance d'un cabinet spécialisé pour l'aider dans l'écriture du PCA (dont le PCI serait une composante). En reprenant l'ensemble des données précédentes, vous présenterez la trame d'un cahier des charges.

Question 5 (3 points)

a) La mise en œuvre du PCI est une opération complexe par le nombre d'acteurs appelés à y jouer un rôle et par la nécessité d'avoir une connaissance transverse du fonctionnement de l'organisation. Le DSI vous demande donc de formaliser des préconisations en termes de gestion des RH pour la mobilisation des équipes et pour le bon fonctionnement du PCI. (2 points)

b) Au-delà des questions d'infrastructures techniques, le PCI concerne les applicatifs métiers. Il est absolument nécessaire de prendre en compte les besoins des utilisateurs. Vous indiquerez comment organiser le travail avec les services. (1 point)

Liste des documents :

Document 1 : « La non-continuité des activités, pire menace pour les entreprises » (extrait) - Cecile Desjardins - *Echos Executives* - 6 février 2019 - 1 page

Document 2 : « Pourquoi et comment mettre en place un PCA informatique ? » - *AXIDO* - 2 décembre 2019 - 2 pages

Document 3 : « Administration numérique et sécurité informatique : quels enjeux dans les Communes ? - *Cogitis (conseil informatique aux collectivités publiques)* » - Mars 2020 - 5 pages

Document 4 : « Qu'est-ce qu'un PCA (Plan de Continuité de l'Activité) ? » *Cadre Emploi* - 29 juin 2020 - 4 pages

Document 5 : « La ville d'Angers est en proie à un ransomware, ses services en ligne sont indisponibles » - Alice Vitard - *Usine Digitale* - janvier 2021 - 2 pages

Document 6 : « Un déconfinement à pas comptés dans les services » - *La Gazette* - juin 2020 - 4 pages

Document 7 : « PRA en cloud : à quoi faut-il s'attendre ? » - Erin Sullivan - *Site Editor* - 25 juillet 2019 - 4 pages

Document 8 : « Comment les collectivités ajustent leur plan de continuité » La Gazette - 18 mai 2020 - 3 pages

Document 9 : « ISO 22301 : continuité d'activités » - *Iso.org* - 2019 - 5 pages

Document 10 : « L'ISO 27701, une norme internationale pour la protection des données personnelles » - *CNIL* - 2 avril 2020 - 3 pages

Document 11 : « Faire face à un sinistre informatique. Fiches pratiques TIC » - *CCI alpes de Haute Provence* - 2019 - 3 pages

Document 12 : « Plan de secours d'après "Plan de continuité d'activité publié par le CLUSIF" » - Marie-pascale Delamare - *docplayer.fr* - 2016 - 5 pages

Document 13 : « Comment sécuriser votre SI en appliquant un Plan de Continuité Informatique » - *Synoméga* - 9 mai 2019 - 4 pages

Liste des annexes :

Annexe A : « Présentation synthétique de la collectivité » - 1 page

Annexe B : **«** Descriptif des SI de la collectivité » - 2 pages

DOCUMENT 1

La non-continuité des activités, pire menace pour les entreprises.

Extrait des Echos Executives, Cecile Desjardins Le 06/02/2019

Tendance : les dirigeants s'inquiètent avant tout de la vulnérabilité de leurs systèmes d'information mais, dans la majorité des cas, les crises qu'ils ont connues étaient liées à des défaillances opérationnelles.

La crise n'arrive pas que chez les autres. Le Baromètre relatif aux risques majeurs des entreprises que publie, mardi 5 février, le groupe d'audit et de conseil Grant Thornton, en atteste : 57 % des entreprises estiment avoir vécu un ou plusieurs événements qualifiés de « crise » au cours des cinq dernières années.

Réalisée à l'automne auprès d'un panel de plusieurs centaines de dirigeants, l'enquête souligne que la première cause de ces crises est en lien avec le métier : dans 65% des cas, les défaillances impactent les activités opérationnelles. Viennent ensuite les crises de réputation (46 %), les événements de type RH ou social (38 %), ceux rattachés à la sécurité et la sûreté (31 %), puis au cyber (27 %) et à l'environnement (12 %).

Mais les événements « vécus » ne sont pas ceux qui inquiètent le plus pour l'avenir. Les dirigeants redoutent aujourd'hui d'autres types de crises, celles liées à la vulnérabilité des systèmes d'information (45 %), à des événements sociétaux ou éthiques (32 %) et à la gouvernance (13 %).

« On constate une dichotomie entre la menace redoutée et les crises avérées qui sont souvent liées aux opérations, et donc à des éléments que les entreprises devraient mieux maîtriser », prévient Clotilde Marchetti, associée et responsable de l'offre risques extrêmes de Grant Thornton.

Prise de conscience

Les trois quarts des dirigeants interrogés jugent que les crises pourraient se multiplier. On comprend alors que la direction générale *« accorde un intérêt particulier à la gestion de crise »* dans 63 % des entreprises. *« Il y a eu une forte évolution au cours des cinq dernières années : il n'est plus nécessaire, aujourd'hui, d'évangéliser les directions générales. Elles ont compris l'importance de protéger leurs collaborateurs, tout comme de se protéger elles-mêmes face à la responsabilité pénale. La gestion de crise est aussi devenue un atout concurrentiel important dans certains appels d'offres »*, remarque Clotilde Marchetti.

Pourtant, seules 39% des structures disposent d'un service ad'hoc pour assurer un pilotage de crise. Quand il existe, il est alors majoritairement composé d'une à cinq personnes et dépend du top management. Par ailleurs, un quart des entreprises interrogées n'ont pas de « plan de continuité d'activités » (PCA). *« Le risque de non-continuité des activités est aujourd'hui perçu comme l'une des menaces les plus redoutées au sein des entreprises privées. Toutefois, dans beaucoup d'entreprises, le périmètre du PCA est encore limité à la continuité informatique. En outre, 55 % des répondants reconnaissent que le lien entre dispositif de gestion de crise et PCA n'est pas efficace »*, explique Clotilde Marchetti, qui juge essentiel de mener *« des exercices de crise pour mieux impliquer et faire adhérer l'ensemble des collaborateurs à la gestion des événements sensibles »*.

Pourquoi et comment mettre en place un PCA informatique ?

- 12 décembre 2019
- Sécurité, Services hébergés

En cas de sinistre, le système informatique d'une entreprise doit être garanti afin de reprendre l'activité le plus rapidement possible. Des équipes dédiées élaborent des politiques de sécurité, ainsi que des outils informatiques afin de minimiser les pertes de données. Elles définissent un **plan de continuité d'activité (PCA)** pour assurer les activités essentielles au fonctionnement de leur organisation.

Pourquoi mettre en place un PCA ?

Quel que soit le scénario : panne électrique, défaillance technique, catastrophe naturelle ou menace informatique, l'entreprise met en place des outils de gestion de crise.

Un PCA définit la stratégie informatique la plus adaptée en cas de crise selon les spécificités de l'entreprise. Il coordonne les différentes actions à mettre en place afin de maintenir les activités des services clés de l'entreprise. Le PCA informatique minimise ainsi les conséquences d'une situation critique sur l'activité de l'entreprise.

En définissant un dispositif fiable avec des outils de gestion de crise, les entreprises se protègent des conséquences financières et du mécontentement de leurs clients. En France, 53% des entreprises évaluent régulièrement les **risques informatiques** de leur société et testent leur PCA afin de l'optimiser. Toutefois, 46% des entreprises n'ont aucun dispositif dédié.

Définir un PCA informatique clair et détaillé

Mettre en place un PCA informatique détaillé pour différentes situations critiques n'est pas simple. L'entreprise identifie les principaux risques informatiques et en mesurer l'impact. Elle pourra ensuite effectuer un audit de sécurité du système d'informations, un test d'intrusion et cartographier les risques de fraude. Ces équipes réfléchissent à différents scénarios et, prévoient des mesures comme

une délocalisation des employés sur un site alternatif mais aussi des télécommunications et des serveurs.

Un plan de continuité informatique doit comprendre des mesures préventives mais aussi un plan d'action en cas de situation catastrophique. Le plan inclut le planning des actions à mettre en place dans les situations de crise avec une liste détaillée de processus informatiques. Le PCA doit également inclure les **procédures de continuité informatique** afin de protéger mais aussi de sauvegarder les données. Il est utile d'avoir à disposition différents environnements de production avec des serveurs de secours. Un système de sécurité fiable avec antivirus et pare-feu doit être envisagé. Enfin, il est essentiel de définir les rôles et les responsabilités de chaque équipe et de s'assurer que chacun respecte ces mesures de sécurité.

Choisir un partenaire IT fiable

De nombreuses technologies comme le cloud introduisent une complexité, de sorte que la **maintenance informatique** nécessite l'intervention d'équipes compétentes. Pour garantir la continuité des activités de l'entreprise, nous vous recommandons d'externaliser votre PCA informatique à un spécialiste informatique comme Axido.

Nos experts Axido analysent et mettent en place votre Plan de Continuité d'Activité informatique. Nos experts définissent l'architecture mais aussi les procédés nécessaires afin d'optimiser votre **PCA**. Vous mettez en place un mode opératoire de qualité pour maintenir vos infrastructures informatiques en sécurité et assurer un service ininterrompu.

20 Mar

Administration numérique et sécurité informatique : quels enjeux dans les Communes ?

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 :

- 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.

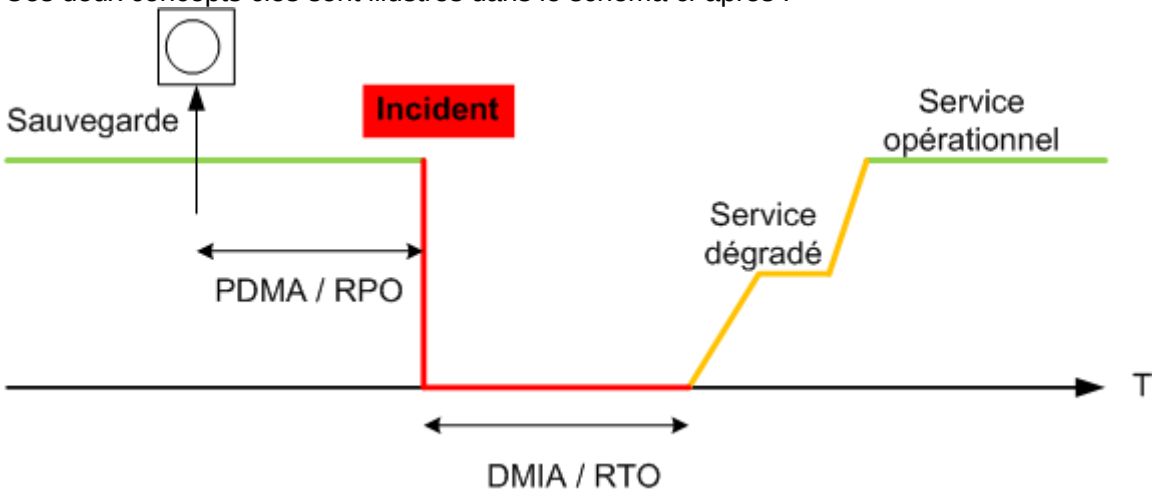
Dans ce cas, du point de vue du pirate informatique, il est plus intéressant d'attaquer beaucoup de petites structures (ou individus), dont une petite proportion payera la fameuse rançon, qu'une structure de taille plus importante, probablement mieux protégée, qui laisserait s'échapper des données à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



Source : Speculos – Wikipedia.org

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.

Quel accompagnement pour votre collectivité ?

COGITIS peut accompagner votre collectivité dans la mise en place d'une gestion optimisée de votre système d'information et de sa sécurité, par une mission d'audit suivi de préconisations concrètes.
Notre expérience de l'accompagnement des collectivités de toutes tailles nous permet d'adapter nos propositions à votre contexte et vos contraintes, notamment financières.
Grâce à notre centre d'appels mutualisé et à nos ingénieurs et techniciens présents sur le terrain, nous pouvons aussi vous assister au quotidien dans la gestion de vos infrastructures.
Contactez-nous pour en savoir plus !

DOCUMENT 4

Qu'est-ce qu'un PCA (Plan de Continuité de l'Activité) ?

Publié le 29 juin 2020 Fleur Chrétien

Avec la crise sanitaire du Covid-19 qui a paralysé l'activité économique à l'échelle mondiale, toutes les entreprises se sont posé la même question : comment s'organiser pour survivre à la crise ? Mise en place du télétravail, organisation du temps partiel, management à distance, mise à disposition de nouveaux outils : face à cette situation inédite, les entreprises ont dû faire preuve d'agilité en un temps record. Pour certaines, de manière improvisée. Pour d'autres, qui avaient déjà envisagé un risque de crise majeure, le déploiement du Plan de Continuité d'Activité (PCA) a permis d'organiser le travail lors de la pandémie. Qu'est-ce qu'un PCA ?, Cadremploi vous détaille tout ce que vous devez savoir sur le Plan de Continuité d'Activité.

Comment définir un PCA ?

Le PCA (Plan de Continuité d'Activité), appelé BCP outre-Atlantique (Business Continuity Planning) est un processus permettant d'identifier les menaces potentielles pour une organisation, et de définir les actions à maintenir de façon prioritaire pour continuer d'atteindre ses objectifs et honorer ses obligations.

Selon la définition donnée par la norme ISO 22301, la gestion de la continuité d'activité constitue un « processus de management holistique qui identifie les menaces potentielles pour une organisation, ainsi que les impacts que ces menaces, si elles se concrétisent, peuvent avoir sur les opérations liées à l'activité de l'organisation, et qui fournit un cadre pour construire la résilience de l'organisation, avec une capacité de réponse efficace préservant les intérêts de ses principales parties prenantes, sa réputation, sa marque et ses activités productrices de valeurs ».

Concrètement, un Plan de Continuité d'Activité permet donc à une entreprise 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, mouvement social, Covid-19). En l'anticipant, l'entreprise augmente son niveau de résilience et peut ainsi en limiter l'impact.

Pourquoi mettre en place un PCA ?

La mise en place d'un Plan de Continuité d'Activité est une **obligation légale** pour certaines structures, dans les secteurs bancaires, financiers et de la santé par exemple.

Pour les entreprises qui ne sont pas soumises à cette obligation, le PCA est apparu comme inévitable suite aux crises de ces dernières années. Mouvement social des gilets jaunes, pandémie mondiale du Coronavirus, crise financière de 2008 avec la liquidation de Lehman Brothers : l'environnement dans lequel les entreprises évoluent est de plus en plus instable. Les crises sont nombreuses, brutales et de nature variée. Elles entraînent des conséquences économiques lourdes, dont la cessation d'activité pour de nombreuses entreprises.
La mise en place d'un PCA vise donc à **maintenir un minimum d'activité pendant la crise**, et à favoriser un **retour à la normale rapide** en limitant

les effets de la crise.
Le Plan de Continuité de l'Activité a des impacts sur :

- l'activité de l'entreprise ;
- le fonctionnement de l'organisation ;
- sa situation financière ;
- l'image de l'entreprise ;
- l'implication du dirigeant en terme de RSE.

Comment mettre en place un Plan de Continuité de l'Activité ?

En période de crise et de nécessité de maintien de l'activité, la principale problématique des entreprises est d'assurer la continuité de l'activité malgré une perte de ressources. L'entreprise doit en effet composer avec une perte de revenus, une diminution de ses effectifs, une dimension logistique revue à la baisse.

Compte tenu des multiples aspects - et conséquences - que peut revêtir une crise, le PCA permet d'anticiper plusieurs scénarios, de prévoir les stratégies adéquates et d'organiser leur mise en œuvre.

Le PCA doit donc :

- **Définir le contexte et les objectifs**. Quelle est la nature de la crise ? À quelle échelle est-elle présente ? Quels objectifs l'entreprise doit-elle atteindre pour assurer sa survie ? Quelles sont les actions prioritaires à mettre en place ?
- **Élaborer différents scénarios de crise**. Même s'il est difficile d'anticiper une pandémie mondiale, le principe du PCA reste d'envisager tous les possibles. Le premier niveau consiste à élaborer des scénarios, avec les conséquences et la liste des actions prioritaires à mener. Un PCA plus abouti intégrera l'analyse des causes.

- **Mettre en place une stratégie de continuation de l'activité**. Quelles sont les activités essentielles ? Quel est le niveau de ressources requis ? Quelle est la durée d'interruption maximale d'activité pour garantir la pérennité de l'entreprise ?
- **Définir les responsables du PCA, les procédures et les moyens à mettre en œuvre :**
  * Dans l'équipe chargée du PCA - qui peut être dirigée par un directeur des risques - chaque personne doit avoir un rôle bien défini, comprendre la finalité de son action et maîtriser les enjeux globaux du PCA.
  * Concernant les procédures à mettre en œuvre, le PCA doit intégrer différents paliers : les actions permettant de limiter les effets de la crise, et si le seuil de vulnérabilité de l'entreprise est dépassé, les actions liées au processus de crise.
  * Au quotidien, il s'agit également d'organiser le management de crise, le management à distance.
- Détailler le **dispositif de gestion de crise** : définition du seuil de vulnérabilité, pilotage des actions, organisation des cellules de crise, déclenchement des dispositifs.
- Définir les **éléments de maintenance opérationnelle** : indicateurs permettant d'évaluer l'efficacité du plan au regard des objectifs, et évaluation du niveau d'activité effectif pendant la crise.

En sortie de crise, le PCA peut être relayé par un PRA, un Plan de Reprise d'Activité qui organise le retour à la normale.

L'USINEDIGITALE

La ville d'Angers est en proie à un ransomware, ses services en ligne sont indisponibles

Après le Grand Annecy, La Rochelle, Aix Marseille, c'est la ville d'Angers qui a été prise pour cible par des hackers qui ont réussi à pénétrer dans son système d'information. Les sites de la mairie et de la collectivité d'Angers Loire métropole sont actuellement indisponibles. Un retour à la normale n'est pas à prévoir tout de suite.

ALICE VITARD

PUBLIÉ LE 18 JANVIER 2021 À 16H55
CYBERSÉCURITÉ, **INFORMATIQUE** , **GESTION DES DONNÉES**

Une cyberattaque de type "ransomware" a frappé le système d'information de la ville d'Angers, dans le Maine-et-Loire, dans la nuit du vendredi 15 au samedi 16 janvier 2021. Les sites de la ville et de la collectivité d'Angers Loire métropole sont indisponibles. Mais "les services accueillant du public restent ouverts", a précisé la collectivité.

Dès le samedi matin, la mairie rapporte que les équipes de la direction du système d'information de la ville ont établi un protocole de sauvegarde et de restauration du système en collaboration avec l'Agence nationale de la sécurité des systèmes d'information (Anssi). "Ce processus de restauration va être long", prévient la ville.

DEUX VAGUES DE CYBERATTAQUES

D'après les informations de *Ouest France*, la cyberattaque s'est composée de deux salves successives : la première a provoqué des problèmes de badges pour entrer dans la mairie puis une seconde a paralysé les services de bibliothèques municipales et les sites d'Angers et de la métropole. Dans un tweet, le conservatoire d'Angers a fait savoir que son système d'information était également paralysé et que ses services étaient uniquement joignables par téléphone.

En revanche, aucune information n'a été donnée sur le montant de la demande exigée par les cybercriminels et si des données personnelles avaient été dérobées lors de cet incident de sécurité.

Angers s'ajoute à la liste, dorénavant longue, des acteurs publics qui ont été ces derniers mois victimes d'une cyberattaque, aux côtés de La Rochelle, Aix Marseille, Vincennes… Récemment, des hackers ont réussi à pénétrer dans le système d'information du Grand Annecy en Haute-Savoie.

DES RISQUES D'HAMEÇONNAGE

Au-delà des conséquences directes, les suites de l'incident inquiètent également. Ainsi, en septembre dernier, la ville de Besançon a été cyberattaquée et alertait ses habitants sur les risques d'hameçonnage. En effet, les hackers avaient réussi à dérober de nombreuses données personnelles et s'en servaient pour envoyer des emails frauduleux.

ALICE VITARD

lagazette.fr

DOCUMENT 6

Adresse de l'article https://www.lagazettedescommunes.com/681561/un-deconfinement-a-pas-comptes-dans-les-services/

ORGANISATION

Un déconfinement à pas comptés dans les services

Emeline Le Naour | A la une | A la Une RH | France | Toute l'actu RH | Publié le 04/06/2020 | Mis à jour le 03/06/2020

Aménager les locaux, rassurer les agents tout en réactivant les services… Un mois après l'annonce du déconfinement, les collectivités ont adapté leur reprise d'activité de façon progressive. Une relance bien loin d'un retour à la normale.

« Dès que nous avons eu des certitudes sur la date du 11 mai, je me suis mise en quête d'un PRA, mais rien de tel n'existait à l'échelle d'une collectivité. Des guides sur la question sont parus, mais trop tard. Nous avons donc construit, service par service, les conditions de retour. » Un mois après le déconfinement, Marie Blondel, directrice générale adjointe des services de la ville de Rouen (2 600 agents, 110 100 hab.), continue de moduler ce plan de reprise au gré de l'évolution de la situation sanitaire et des annonces gouvernementales. Car si le confinement a pu laisser place à une certaine forme d'improvisation, le déconfinement, lui, a dû être longuement réfléchi par les collectivités, sans qu'elles n'aient pour autant toutes les cartes en main. « Nous avons ouvert les services administratifs, les cimetières et l'accueil au public. Mais la grosse interrogation tourne autour de la date d'ouverture des services culturels et des espaces sportifs », explique Marie Blondel.

- Comment les collectivités ajustent leur plan de continuité [1]

« Paradoxalement, les plans de continuité sont plus faciles à construire, même dans l'urgence, que ceux concernant la reprise », témoigne Johan Theuret, directeur général adjoint chargé du pôle ressources humaines de la ville et de la métropole de Rennes (43 communes, 4 600 agents, 447 400 hab.). « La principale difficulté du PRA, c'est qu'il varie en fonction de la nature de la crise. Il s'agit davantage d'une logique de flux. Aujourd'hui, il faut assurer la sécurité des agents en aménageant les locaux et en fournissant des équipements nécessaires, car le virus circule toujours. Ce n'est pas comme s'il s'agissait de réactiver les services après le passage d'une catastrophe naturelle », illustre Johan Theuret, qui prône le pas à pas : « La priorité reste la progressivité pour

être en mesure d'assurer la protection des usagers et des agents. » A Rennes, le télétravail a été largement maintenu lorsqu'il était possible. Ainsi, le 11 mai, 30 % des effectifs effectuaient encore leurs missions à distance.

Horaires décalés

Le retour de tous les agents reste, de toute façon, bien incertain, car étroitement lié à la réouverture des établissements scolaires. Certains étant encore en autorisation spéciale pour garde d'enfants, les services RH doivent jouer d'agilité afin d'anticiper au mieux les besoins des services et les effectifs disponibles. Pour beaucoup de collectivités, le 11 mai n'a donc pas pris des allures de big bang.

Du côté des agents en présentiel, le retour sur site a tout de même bousculé les habitudes. Les bureaux accueillant trois à quatre postes se sont transformés en bureaux aménagés, les horaires des équipes ont été décalés pour que le moins de personnes possible se croisent dans les vestiaires ou les couloirs, et les pauses repas sont désormais prises en dehors du réfectoire.

- Comment les services planchent sur le déconfinement [2]

Une série de précautions qui donnent à cette « rentrée » le sentiment que le spectre d'une contamination reste présent. « Il a fallu rassurer les agents qui ont été, pour certains, confinés durant deux mois chez eux et ont donc développé des craintes vis-à-vis du monde extérieur. Certains voulaient presque des tenues de cosmonautes pour revenir », ironise François Dupouy, directeur général adjoint à la ville de Metz, (2 500 agents, 116 400 hab.).

Dans cette région durement touchée par la crise sanitaire, la communication interne a été fondamentale. Alors, sans tomber « dans l'excès pour rassurer », il a travaillé de façon resserrée avec les cadres de chaque service pour répondre à deux questions : quelles missions relancer ? Et avec quel type de protection ? « Nous avons fini par trouver les solutions les moins contraignantes pour que les métiers techniques qui interviennent à l'extérieur soient malgré tout en sécurité », reprend François Dupouy, estimant qu'un peu plus de 50 % des agents sont de retour sur le terrain. « Nous serons peut-être au complet dans le courant du mois de juin mais, là encore, il n'y a pas de dogme, il faut faire du cas par cas », conseille-t-il.

Dialogue social réussi

Selon Patrick Coroyer, directeur des ressources humaines de la ville et de la métropole de Nantes (7 500 agents, 646 500 hab.), l'une des clés d'un déconfinement réussi est un dialogue social nourri. Un levier à activer afin d'éviter l'impasse que pourraient représenter les droits de retrait. A Nantes, la mobilisation hebdomadaire du comité d'hygiène, de sécurité et des conditions de travail a permis une reprise sereine des agents. « Au niveau local, la période de la crise sanitaire a été un effort phénoménal en termes de dialogue social. Avant le déconfinement, nous avons organisé 30 visioconférences, répondu à 700 courriers ou emails des organisations syndicales. Cela a été très intense, mais c'est le prix à payer pour que cela fonctionne », assure Patrick Coroyer.

Manque de visibilité

Marie Mennella, secrétaire fédérale de la CFDT Interco, partage cet avis tout en regrettant que trop peu d'employeurs aient adopté cette démarche : « Il n'y a pas de mystère. Quand les décisions sont uniquement descendantes, les reprises se passent mal. Or nous avons bien senti qu'au niveau local, on laissait la main aux employeurs pour déterminer les conditions de retour. Pourtant, et au-delà du dialogue social, il est essentiel de parler des missions, de l'organisation du travail des agents durant cette période charnière. »

Une consultation des partenaires sociaux facilitée grâce aux audioconférences, largement généralisées ces derniers mois dans les collectivités territoriales équipées. « Certaines n'ont prévu de réunir les instances qu'à la mi-juin. Aujourd'hui, on dispose de la technologie nécessaire pour s'organiser en amont. Il n'y a plus de prétexte », fait valoir Marie Mennella.

- Quand manager ses équipes à distance renforce la proximité [3]

Selon Sophie Guihard, directrice générale des services du département des Côtes-d'Armor (3 300 agents), la contrainte de ce retour ne s'est pas concentrée sur la logistique sanitaire des agents, dont la majorité travaille encore à distance, mais plutôt sur le service à la population : « Nos prérogatives sociales ont entraîné des inquiétudes chez les travailleurs sociaux. Ils posaient beaucoup de questions concernant le suivi des missions, la situation de certains usagers. Il est important d'expliquer le déroulé d'un plan de reprise et de rassurer sur le fait qu'on ne laissera personne sur le bord de la route », développe Sophie Guihard.

- Déconfinement et télétravail : les DRH attentifs aux signaux faibles [4]

Un mois après le top départ de cette course de fond, ce qui pèse peut-être le plus sur le quotidien tient au manque de visibilité. « Nous essayons vraiment de nous inscrire dans le temps, mais nous n'avons pas de cap clair ou d'échéance quant au retour à la normale », concède la directrice des services du département breton, qui s'interroge sur l'après-crise du Covid-19 : « Demain, le port du masque, le télétravail ou les gestes barrières deviendront peut-être la nouvelle norme, qui sait ? »

Les risques psychosociaux à la loupe

« Lors du déconfinement, certaines collectivités feront peut-être le choix de privilégier telle ou telle mission, au détriment d'une autre. Comment accepter cela quand on est manager ou agent de la mis sion non prioritaire ? Comment gérer ce sentiment de moindre importance ? Ce n'est pas évident. Il faut que la direction générale accompagne cela d'un discours et d'actes qui rappellent le commun, l'essentiel, et ce qui nous rassemble. Il y aura nécessairement un avant et un après. Il faut qu'il y en ait un, sinon notre organisation sera en décalage avec la société. » Dans un document d'une quinzaine de pages, « Du confinement au déconfinement : repenser le lien dans une dimension humaine » [5], publié en avril 2020, le centre de gestion du Nord a réuni les expertises d'une directrice des ressources humaines et d'une psychologue du travail qui analysent les enjeux du retour à l'activité.(*) publication du 23 avril 2020, à retrouver sur : bit.ly/3c8zM7q

« Nous ne savons pas quand la crise sera terminée, mais il faut déjà penser l'après »

Fabienne Chol, directrice générale adjointe chargée des ressources humaines au conseil régional d'Ile-de-France (10 000 agents)

« Durant deux mois, nous avons dû être réactifs pour résoudre des problèmes que nous n'avions jamais rencontrés. En plus de nos missions habituelles, nous avons dû répondre à l'urgence et toute l'équipe s'est mobilisée à 200 %, s'est adaptée et réinventée ; mais un tel rythme ne peut pas durer indéfiniment. Au bout d'un moment, on s'épuise. La difficulté étant que nous ne savons pas quand la crise sera terminée et pourtant, il faut déjà penser l'après. C'est notre rôle d'encadrants de réfléchir à l'éventail des scénarios de sortie de l'urgence et d'anticiper.

Désormais, il faut débriefer pour trouver les solu tions de demain. « Est-ce que nos réponses organisationnelles étaient les bonnes ? », « Est-ce que les circuits de décisions étaient pertinents ? » Il y a forcément des marges d'amélioration. Car si une crise de cette ampleur, sanitaire ou autre, venait à se reproduire, les choses devraient se mettre en place avec moins de stress, plus de fluidité. »

Les consignes à respecter pour les réunions d'équipe

Privilégier les réunions par visioconférence et/ou audioconférence. Mettre à disposition les consignes d'utilisation de l'audio et de la visio, et s'assurer que tous les postes bénéficient des équipements nécessaires. Le cas échéant, prévoir un poste mutualisé, dédié à cela, qui sera systématiquement désinfecté après usage.

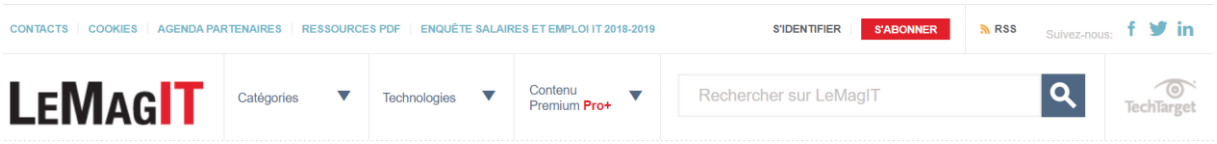
Si la réunion ne peut avoir lieu qu'en présentiel, envisager de la tenir en extérieur (selon la météo) en respectant les gestes barrières et le port du masque. Sinon, faire la réunion dans une salle permettant de respecter les distances d'un mètre entre chaque participant. Afficher sur la porte l'effectif maximal admissible (50 % de la capacité normale).

Enlever la moitié des chaises, désinfecter les supports de contact (tables, accoudoirs) avant et après la réunion, aérer la salle avant et après la réunion dans la mesure du possible.

Offrir la possibilité de se laver les mains avec du savon ou du gel hydroalcoolique. Se munir de sa papeterie personnelle (stylo, papier…).

POUR ALLER PLUS LOIN

- Déconfinement, phase 2 : le décret est publié
- Déconfinement : l'application StopCovid est lancée
- Déconfinement : comment faire renaître une cohésion d'équipe ?
- Déconfinement et télétravail : les DRH attentifs aux signaux faibles
- Déconfinement : piloter le retour au travail des agents
- Déconfinement : des ressources et des outils en ligne
- Le rapport de Jean Castex, le « Monsieur déconfinement », est en ligne
- Webinaire : comment réussir le déconfinement de vos services avec vos agents
- Maire employeur : comment organiser la reprise



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

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 ?

- **Erin Sullivan,** Site Editor Publié le: **25 juil. 2019**

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.

DOSSIER : Coronavirus : les services publics face à la crise sanitaire
Dossier publié à l'adresse https://www.lagazettedescommunes.com/671599/comment-les-collectivites-ajustent-leur-plan-de-continuite/

CORONAVIRUS

Comment les collectivités ajustent leur plan de continuité

Emeline Le Naour | A la une | A la Une RH | actus experts technique | Dossiers d'actualité | France | Toute l'actu RH | Publié le 31/03/2020 | Mis à jour le 18/05/2020

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.

[1]

« 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.

- « On a un boulot à faire, on a signé pour, on le fait » [2]

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.

- Autorisation spéciale d'absence, mode d'emploi [3]

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.

- « La crise sanitaire démontre l'utilité des plans communaux de sauvegarde » [4]

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.

- Actes des collectivités : les délais prolongés [5]

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

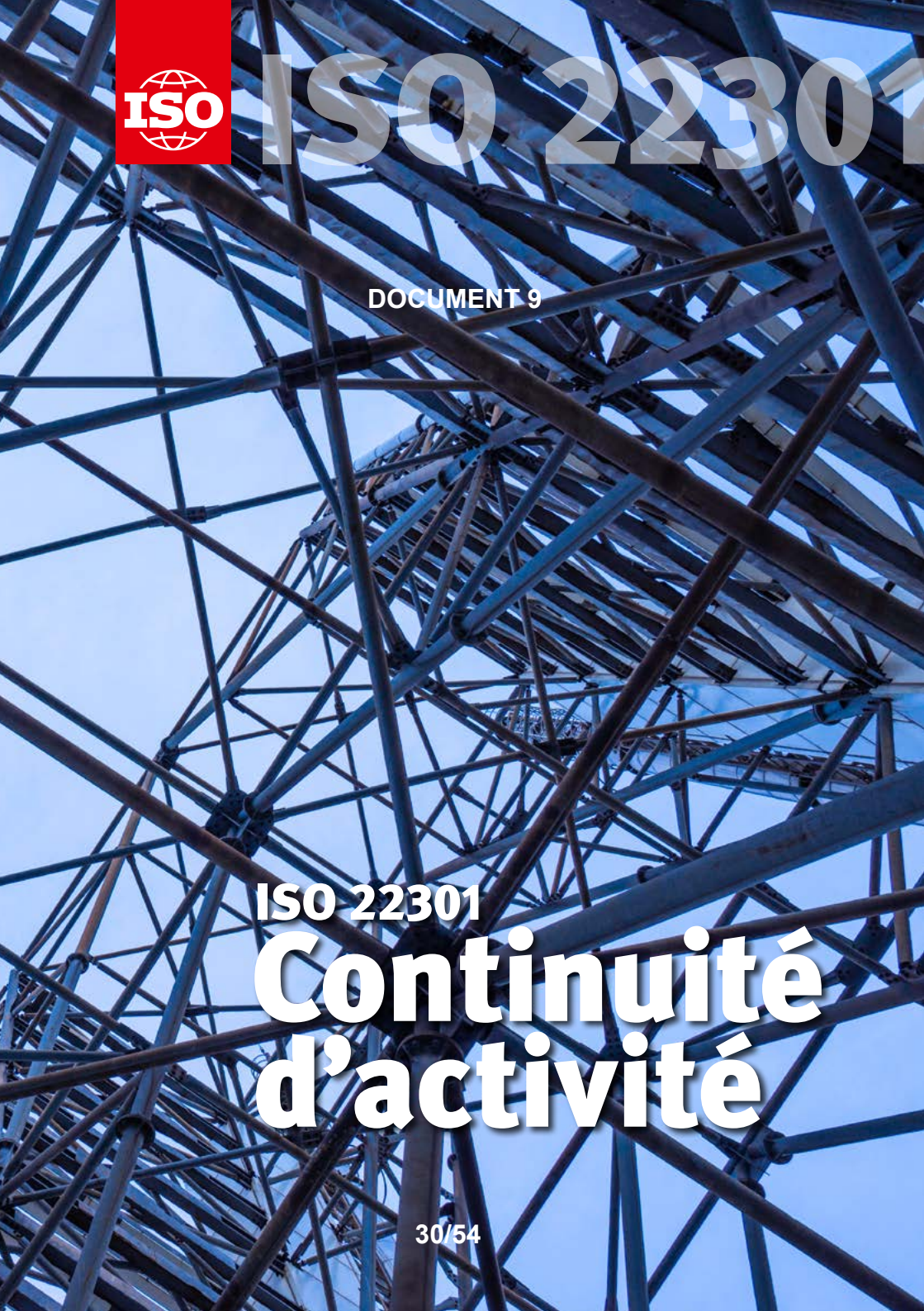
« Le PCA, qui datait de l'épidémie de H1N1, a été réactualisé très rapidement. Au vu des liens étroits qui existent entre nos voisins transalpins et la Moselle, qui fut pendant longtemps une terre d'immigration pour les ouvriers italiens, le risque de propagation était assez élevé », retrace François 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.

POUR ALLER PLUS LOIN

- Coronavirus : la progression de l'épidémie dans les territoires
- Une note ministérielle confirme un usage restreint du droit de retrait
- « On a un boulot à faire, on a signé pour, on le fait »
- Coronavirus : le télétravail devient un impératif durant la crise



DOCUMENT 9

ISO 22301
Continuité d'activité

30/54

Inondations, cyber-attaques, défaillances informatiques, problèmes d'approvisionnement ou perte de personnel qualifié ne sont que quelques exemples des dangers qui menacent le bon fonctionnement d'une organisation. Sans réponse adéquate, ces menaces peuvent obliger une entreprise à interrompre ses activités, ou même conduire à sa faillite. Or disposer d'un plan d'action cohérent en cas de sinistre est l'assurance d'une capacité de réponse plus efficace et d'une reprise plus rapide de l'activité.

Lors de sa publication en 2012, ISO 22301, *Sécurité et résilience – Systèmes de management de la continuité d'activité – Exigences*, était la première Norme internationale au monde consacrée à la mise en œuvre et à la mise à jour de plans, de systèmes et de processus efficaces pour aider les entreprises à assurer la continuité de leur activité. Cette norme a récemment été révisée pour inclure les approches et les bonnes pratiques les plus récentes dans le domaine.

À qui s'adresse **ISO 22301** ?

ISO 22301 s'applique à toute organisation, indépendamment de sa taille, de son secteur d'activité et de la nature de ses activités. Elle est également utile aux organismes de certification et de réglementation dans la mesure où elle leur permet d'évaluer l'aptitude d'une organisation à respecter les exigences légales ou réglementaires.

Comme de nombreuses autres normes de systèmes de management reconnues au niveau international, telles qu'ISO 9001 (management de la qualité) et ISO 14001 (management environnemental), elle adopte la structure-cadre (HLS) de l'ISO. Elle a ainsi été conçue pour être intégrée aux processus de management existants des organisations.

ISO 22301 s'adresse aux professionnels du management des risques liés à la continuité d'activité, aux responsables des chaînes d'approvisionnement, aux partenaires et aux responsables d'audit, aux rédacteurs de rapports sur la responsabilité sociétale de l'entreprise, aux organismes de réglementation et à tout autre acteur participant ou intéressé à la continuité d'activité.

Quels sont les **avantages** de cette norme pour **mon entreprise** ?

ISO 22301 rassemble les meilleures pratiques internationales afin d'aider les organisations à répondre efficacement aux perturbations et à reprendre rapidement leur activité. En cas de problème, les coûts pour l'entreprise sont ainsi moins importants et ses performances, moins affectées. En outre, les entreprises comportant plusieurs sites ou divisions peuvent adopter la même approche harmonisée à l'échelle de l'organisation.

Cette norme présente d'autres avantages :

- La capacité à démontrer à toutes les parties prenantes, et notamment aux clients, aux fournisseurs et aux organismes de réglementation, qu'elles disposent de systèmes et de processus efficaces pour garantir la continuité de l'activité
- L'amélioration des performances et de la résilience organisationnelle
- Une meilleure compréhension de l'activité grâce à l'analyse des principaux problèmes et domaines de vulnérabilité

ISO 22301 donne un aperçu clair et détaillé du fonctionnement d'une entreprise et fournit des informations précieuses pour la planification stratégique, le management du risque, la gestion de la chaîne d'approvisionnement, la transformation du modèle commercial et la gestion des ressources de l'entreprise.

Quelles sont les **améliorations** apportées à cette norme ?

ISO 22301 a été révisée à la fin de l'année 2019 pour refléter les changements dans le domaine de la continuité d'activité et offrir aux utilisateurs une plus grande valeur ajoutée. Le texte a également été amélioré pour assurer plus de clarté et de cohérence.

Certains changements sont à souligner :

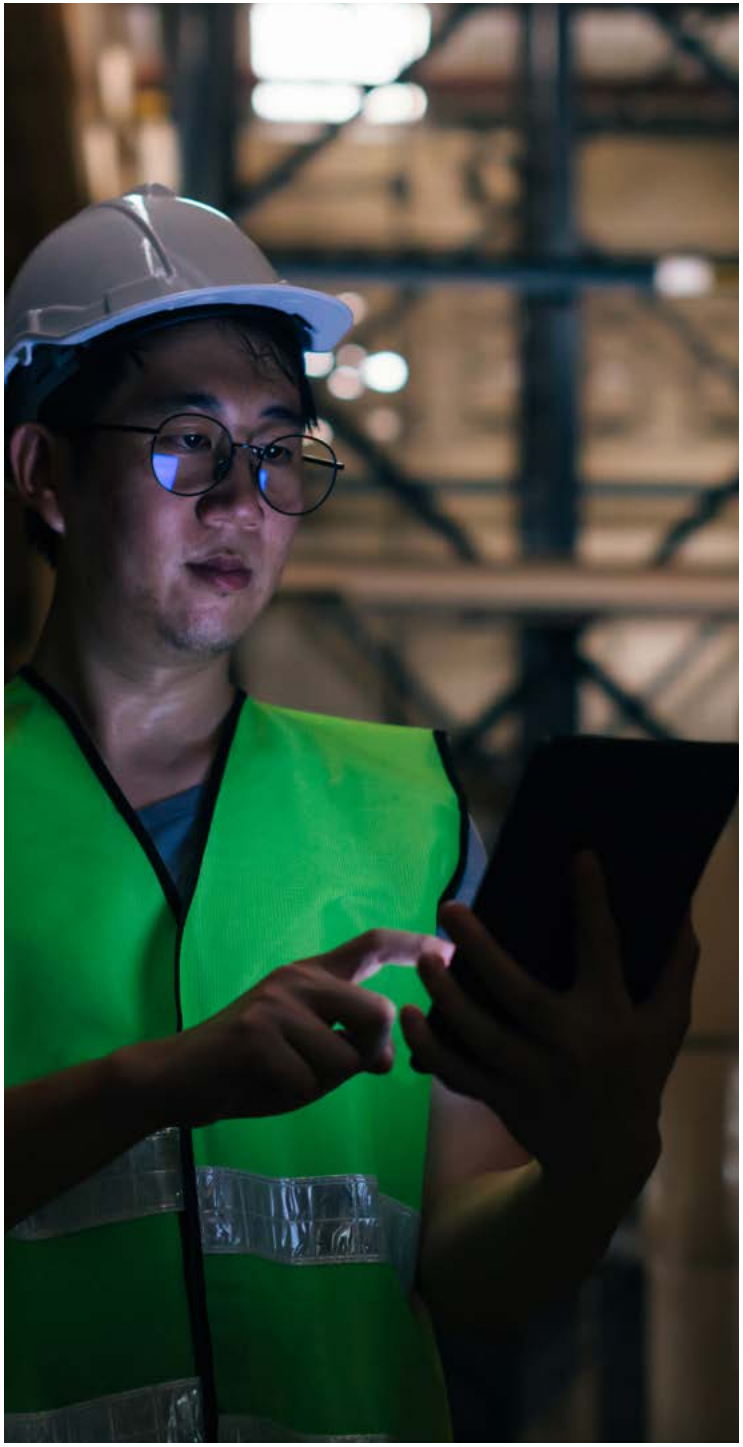
- La structure de la norme a été révisée pour en faciliter la lecture et la mise en œuvre, et en clarifier davantage les exigences.
- La formulation et la terminologie ont été simplifiées pour éviter les doublons et mieux refléter les tendances actuelles dans le domaine de la continuité d'activité.
- La structure-cadre (HLS) a été rationalisée afin de rester cohérente avec toutes les autres normes de systèmes de management ISO.

Puis-je **intégrer ISO 22301** à mon **système de management existant** ?

ISO 22301 partage une structure-cadre (c'est-à-dire un texte de base, des termes et des définitions identiques) avec d'autres normes de systèmes de management ISO, comme ISO 9001 (qualité) et ISO 14001 (environnement). Ce cadre vise à faciliter l'intégration de nouveaux domaines de management dans les systèmes de management existants d'une organisation.

Qu'en est-il de la **certification** ?

La certification ISO 22301 n'est pas une exigence de la norme, mais peut être utile pour démontrer que votre organisation se conforme à ses critères et qu'elle a adopté les meilleures pratiques internationales.



33/54

Par où **commencer** ?

Si vous envisagez de mettre en œuvre ISO 22301, voici quelques conseils pour démarrer :

- Assurez-vous d'avoir le soutien de votre direction. Un système de management de la continuité d'activité n'est efficace que s'il est soutenu et traité comme une priorité par les personnes à même de prendre les décisions.
- Réalisez une évaluation qui permettra de déterminer dans quelle mesure vous respectez déjà les exigences de la norme et quel niveau de ressources vous sera nécessaire pour satisfaire l'ensemble des exigences définies.
- Procédez à un exercice de reprise de l'activité pour envisager avec soin ce que vous feriez en cas de perturbation de l'une de vos activités. Vous verrez ainsi clairement si la capacité de réponse de votre organisation est suffisante face à de tels événements et en quoi ISO 22301 peut vous aider.

Pour plus d'informations, consultez notre page Web consacrée aux normes de systèmes de management ISO (**www.iso.org/management-system-standards.html**) ou contactez le membre de l'ISO dans votre pays.

Pour plus d'informations

Site Web de l'ISO : **www.iso.org**
Magazine *ISOfocus* : **www.iso.org/isofocus**
Vidéos ISO : **www.iso.org/youtube**
Suivez-nous sur Twitter : **www.iso.org/twitter**
Rejoignez-nous sur Facebook : **www.iso.org/facebook**
Rejoignez-nous sur Linkedin : **www.iso.org/linkedin**

À propos de **l'ISO**

L'ISO (Organisation internationale de normalisation) est une organisation internationale non gouvernementale, indépendante, composée de 164* organismes nationaux de normalisation. Par ses membres, l'Organisation réunit des experts qui mettent en commun leurs connaissances pour élaborer des Normes internationales d'application volontaire, fondées sur le consensus, pertinentes pour le marché, soutenant l'innovation et apportant des solutions aux enjeux mondiaux.

L'ISO a publié plus de 22500* Normes internationales et publications associées, couvrant la quasi-totalité des secteurs, des technologies à la sécurité des denrées alimentaires, en passant par l'agriculture et la santé.

Pour plus d'informations, consultez le site **www.iso.org**.

*Octobre 2019

Organisation internationale de normalisation

Secrétariat central de l'ISO
Chemin de Blandonnet 8
Case Postale 401
CH – 1214 Vernier, Genève
Suisse

iso.org

La préservation de notre planète nous tient à coeur.
Cette publication a été imprimée sur du papier recyclé.

ISBN 978-92-67-21085-8

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

02 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.

Faire face à un sinistre informatique

Protéger son système d'information[1] avec des solutions techniques ne suffit pas toujours pour faire face à un sinistre. En cas de perte, de vol ou de dégradation des données, chaque collaborateur sait comment réagir ? Qui contacter ? Quand ou comment le système sera remis en état ?
Par ailleurs, sauriez-vous évaluer la perte de chiffre d'affaires si votre système d'information était indisponible ? A combien évaluez-vous le coût d'un salarié dans l'incapacité de travailler ?

Pour anticiper ce type d'imprévu, il est toujours utile de formaliser quelques procédures. Ainsi l'entreprise peut redémarrer plus efficacement son activité sans céder à la panique.

Les grands comptes disposent de documents détaillés dans ce domaine, appelés « plan de reprise d'activité » et/ou « plan de secours informatique ». Cette notice vous donne les clés pour formaliser les principes et les règles à appliquer en cas de sinistre informatique.

Qu'est ce qu'un plan de secours ?

Le PCA

Un plan de continuité d'activité (PCA) ou plan de reprise d'activité (PRA) couvre un champ plus large que le plan de secours informatique (PSI). Un PCA ne se limite pas à la continuité du système d'information, « *il prend également en compte le repli des utilisateurs, le risque sanitaire (pandémie), l'organisation permettant la gestion de crise (astreinte, cellule de crise), et la communication de crise, entre autres* » (Source : Wikipédia).

[1] Système d'information : ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de regrouper, de classifier, de traiter et de diffuser de l'information sur un phénomène donné. (source : Wikipédia).

Le PSI

Le PSI vise la reprise d'activité de l'entreprise après un sinistre important ayant atteint le système d'information. Il traite principalement de la restauration de l'infrastructure informatique et des données.
Le PSI représente un maillon capital de la politique de sécurité informatique de l'entreprise. Sa réalisation découle d'un large diagnostic des données à protéger et des risques potentiels. Cette phase amont peut être parfois assez longue si le système d'information est complexe et le volume de données conséquent. L'organisation des ressources humaines est aussi structurée : constitution d'un comité de crise, d'une cellule de coordination, d'équipes d'intervention, etc.

Les moyens de secours sont parfois très importants lorsque l'entreprise ne peut se permettre une interruption de service, comme dans le secteur bancaire par exemple. Certaines organisations doublent l'intégralité de leur infrastructure afin de pouvoir transférer leurs utilisateurs dans un autre site identique et reprendre très vite leur activité.

Remarque

Dans une enquête publiée en 2008, le CLUSIF[2] estime que 61% des entreprises de plus de 200 salariés disposent d'un PSI.
Source : *Menaces informatiques et pratiques de sécurité en France*, 2008. Disponible sur www.clusif.fr

Le plan de secours simplifié

Quel est son utilité ?

Une TPE ou une PME n'a souvent pas le temps de déployer autant de ressources humaines et financières pour mettre en œuvre une telle démarche.

Elle n'est pas pour autant à l'abri d'un sinistre :

- Mauvaise manipulation volontaire ou involontaire,
- Incendie ou dégât des eaux,
- Panne de matériel informatique,
- Vol,
- Intrusion dans le réseau,
- Etc.

C'est pour ces raisons qu'il semble nécessaire de formaliser un plan de secours, mais de manière simplifiée.

En quoi consiste t-il ?

Voici les 3 étapes clés de construction de ce document de référence :

1. Analyse de risque et d'impact
2. Mise en place du plan de secours
3. Maintenance du plan de secours

[2] Le Club de la Sécurité de l'Information Français (CLUSIF), est une association œuvrant pour la sécurité de l'information dans les organisations. Il publie régulièrement des notes techniques et méthodologiques sur le sujet. Il réalise également des enquêtes depuis 1984 sur les politiques de sécurité de l'information et la sinistralité informatique en France.

Pré requis

- **Nommer un responsable**

Avant tout, il convient de désigner une personne responsable de l'élaboration et de la mise en œuvre du plan de secours. Dans les PMI / PME, cette fonction est très souvent assurée par le responsable informatique lui-même, ou le responsable qualité.

Cette personne doit réunir plusieurs compétences :

- Une bonne connaissance dans le domaine de la sécurité, sans pour autant connaître en détail le fonctionnement des technologies. Il y a donc un minimum de connaissances à acquérir et à maintenir pour être crédible vis-à-vis des techniciens en sécurité informatique, mais aussi pour savoir apprécier les risques liés à l´utilisation du système d´information.
- Une vision transversale de l'activité de l'entreprise.
- Une aptitude à communiquer pour mener des missions de sensibilisation du personnel.
- Des capacités en matière d'organisation, car il sera le chef d'orchestre de la gestion du sinistre.

- **Maîtriser le contenu et la valeur du système d'information**

Si cela n'a pas encore été fait, il convient de commencer par inventorier les données à protéger, puis d'en évaluer la valeur.

Dans un premier temps, commencez par recenser les données internes à l'entreprise : messagerie électronique (courriels, contacts, calendriers), fichiers, données des logiciels (fichier client, comptabilité-gestion…), parc informatique, etc.

Hiérarchisez ensuite la valeur des informations selon l'importance de leur disponibilité et de leur intégrité. L'objectif de cette classification de l'information est de définir le degré de valeur ajoutée pour chaque type de données.
Pour vous aider lors de cette phase d'état des lieux, vous pouvez vous inspirer librement du tableau suivant :

Types de données	**Information basique**	**Information sensible**	**Information stratégique** (forte valeur ajoutée)
Contacts et dossiers du personnel			
Factures clients			
Factures fournisseurs			
Listes fournisseurs			
Données comptables			
Relevés de compte			
Propositions commerciales			
Contrats commerciaux			
Contrats de travail			
Données de production			
Grille tarifaire des produits			
Plans stratégiques			
Procédés de fabrication			
Veille concurrentielle			

Information stratégique. Elle doit être restaurée en priorité en cas de sinistre. Son intégrité doit être préservée au maximum.

Information sensible. Son intégrité doit être préservée, mais sa restauration en cas de sinistre n'est pas prioritaire.

Information basique. Elle est utile, mais n'est pas prioritaire en matière de préservation et de restauration de l'information.

Remarque :

Dans le cas où l'entreprise sous-traite l'exploitation de ses données à un prestataire extérieur (ex : gestion de la paie) ou que ses données sont hébergées chez un prestataire, elle doit veiller à l'existence d'un plan de secours et prendre connaissance de son contenu.

Analyse de risque et d'impact

Il s'agit de déterminer les menaces qui pèsent sur l'informatique de l'entreprise. Elles peuvent être d'origine humaine (maladresse, attaque, malveillance) ou technique (panne), et être interne ou externe à l'entreprise. Il convient d'estimer la probabilité que chaque menace se concrétise.

L'analyse d'impact consiste à mesurer les conséquences d'un risque qui se matérialise. Cette évaluation essentiellement financière peut être segmentée en paliers pour lesquels les coûts s'aggravent.
Ex : à H(heure du sinistre)+2h : ….
H+10h : …
H+1 jour : …

Remarque :

Le CLUSIF a établi une grille des menaces types et de leurs conséquences dans un document intitulé *Plan de continuité d'activité – Stratégie et solutions de secours du SI,* publié en 2003.
Ce dossier est téléchargeable sur le site http://www.clusif.fr/

Mise en place du plan de secours

Il s'agit de mettre en place des mesures préventives et curatives. Certaines de ces mesures reposent sur des outils, tandis que d'autres sont davantage liées au comportement des utilisateurs.

Mais avant de mettre en place ces mesures, l'entreprise doit d'abord statuer sur 2 questions :

- quelle est la quantité maximale d'informations que je peux perdre mettre en péril mon activité ?
- quel est le délai maximum de reprise d'activité normal au-delà duquel le suivi de la société est compromis ?

La réponse à ces questions va déterminer le niveau de sécurité à mettre en place. Autrement dit, quelles informations faut-il protéger et rétablir en priorité en cas de sinistre pour perdre le moins d'agent possible ?

- **Les mesures préventives**

Elles permettent d'éviter une discontinuité de l'activité. Voici les principaux points de vigilance (le détail de ces mesures est disponible dans les notices indiquées).

- **Le plan de sauvegarde** : il s'agit de déterminer la fréquence et le type de sauvegarde (complète, différentielle, incrémentale) pour chaque catégorie d'information (basique, sensible, stratégique).
- Important : ne pas stocker les supports de sauvegarde à côté du serveur ou de la machine qui contient les données.
- **La sécurité logique** : il convient de mettre en place des outils de protection de base (anti-virus, firewall, anti-spam) et de les maintenir à jour. A cela peuvent s'ajouter des contrôles d'accès aux données par mot de passe ou certificat électronique.
- **La sécurité physique** : il s'agit de la sécurité des locaux. Une attention particulière doit être portée à la sécurité du serveur de l'entreprise
- **Le facteur humain** : la sécurité des systèmes d'information n'est pas qu'une affaire d'outils. C'est aussi - voire surtout - une information régulière diffusée auprès des collaborateurs. Une charte informatique permet de responsabiliser et sensibiliser les salariés à la sécurité informatique.

- **Mesures curatives**

Ces mesures sont nécessaires car aucune mesure préventive n'est efficace à 100%. Elles interviennent lorsqu'un sinistre survient.

- Restauration des dernières sauvegardes
- Redémarrage des applications (bureautiques, métiers, etc).
- Redémarrage des machines (serveurs, imprimantes / copieurs, boitiers, etc.).

Le temps de remise en route du système va dépendre de l'endommagement occasionné par le sinistre. Un renouvellement de matériel peut parfois être nécessaire.

Maintenance du plan de secours

Il est important de vérifier que le plan est réalisable en termes de procédures, de budget ou de temps nécessaires au redémarrage.
Par ailleurs, le plan de secours doit être actualisé pour être en phase avec le développement de l'entreprise : création d'une nouvelle activité, mise en œuvre d'une nouvelle infrastructure, croissance externe, recrutement, etc.

POUR ALLER PLUS LOIN

Plan de continuité d'activité – Stratégie et solutions de secours du SI publié par la commission technique du CLUSIF en 2003 (disponible sur le site http://www.clusif.fr/).

DOCUMENT 12

Plan de secours

Un plan de continuité de service (PCS) contient à la fois un plan de secours informatique (PSI) et un plan de reprise d'activité (PRA).

Avant de commencer une étude de Plan de Secours Informatique, il faut donc définir le Plan de Continuité de Service pour faire valider par la Direction de l'entreprise, via un comité de pilotage, les activités concernées et les types de risques à prendre en compte.

I LE PLAN DE CONTINUITÉ DE SERVICE (PCS)

On commence par définir pour chaque activité les exigences de continuité. Il convient pour cela d'examiner les enjeux, d'identifier les activités essentielles et d'évaluer les conséquences d'interruption ou de dégradation de ces activités (arrêt temporaire ou définitif, perte de données, dégradation du service). La comparaison de ces différentes situations doit permettre d'étalonner les niveaux d'impacts (définition du caractère «non supportable» d'une situation) qui seront utilisés ultérieurement, dans la phase d'analyse des risques.

Il faut donc :

- répertorier les éléments du système d'information indispensables à la poursuite de l'activité (applications, moyens de communication, informations) ;
- préciser par activité le service minimum acceptable :
  - les applications nécessaires ;
  - les ressources humaines ;
  - les locaux ;
  - les équipements (postes de travail, téléphones, imprimantes, réseau ...) ;
  - le délai de reprise d'activité ;
  - la durée du service minimum ;
  - le niveau de dégradation du service acceptable (temps de réponse, activités pouvant être manuelles...) ;
  - les conditions de retour à la normale ;
  - les fournitures externes indispensables.

La phase d'analyse des risques a pour objet la classification des risques d'indisponibilité totale ou partielle du système d'information et la mise en évidence des priorités dans le traitement des risques. La réalisation d'un plan de secours est une opération lourde. La définition de priorités peut faciliter sa réalisation par tranches.

Il s'agit donc de répertorier pour chaque objet à risque un ou plusieurs risques significatifs, puis, pour chaque risque retenu, à étudier et décrire les conséquences directes de sa réalisation sur le système d'information. L'objectif est de réaliser un bilan des conséquences directes en termes :

- de durée d'indisponibilité des moyens (applications, services, ...) ;
- de perte d'information (dernières mises à jour, flux, archives, ...) ;
- de potentialité du risque qui sera soit directement attribuée, soit calculée.

Sur la base de ces scénarios de sinistres, il faudra estimer la durée d'interruption de service associée à chaque fonction vitale, en tentant de les regrouper selon des critères de gravité (4 à 5 maximum) et pouvant aller d'une situation de « désastre » à un simple arrêt du service.

Au regard de ces éléments, il sera dès lors possible d'envisager et d'évaluer des moyens de secours appropriés (PSI) et des scénarios de reprise (PRA) pour ramener l'impact estimé à un niveau acceptable.

1 Marie-pascale Delamare d'après "Plan de continuité d'activité publié par le CLUSIF"

II LE PLAN DE SECOURS INFORMATIQUE (PSI)

Après élaboration du plan de continuité de service, une étude des solutions doit être menée tant sur les aspects techniques que sur les aspects organisationnels. A l'issue de cette étude, un dossier de choix de solutions sera soumis aux instances de décision afin de définir le contenu définitif du Plan de Secours Informatique. A ce stade de l'étude, le chiffrage des solutions peut conduire à un ajustement des moyens demandés.

Un plan de secours est composé de dispositifs élémentaires (procédures techniques ou organisationnelles) dont l'activation dépendra de l'événement survenu et du contexte général.

Les dispositifs d'un plan de secours peuvent être classés par types d'activité :

- la mobilisation des ressources nécessaires :
  - ressources humaines : mobilisation des équipes d'intervention ;
  - réservation des moyens de secours (réquisition de moyens, alerte d'un prestataire externe, ...) ;
  - récupération des sauvegardes ;
  - récupération de la documentation ;
- le secours des équipements informatiques :
  - restauration des environnements système ;
  - adaptations techniques (le matériel de secours n'est pas toujours identique au matériel d'origine) ;
  - restauration des applications ;
  - validation des restaurations ;
- le secours des réseaux :
  - mise en place des équipements de secours ;
  - basculement sur liaisons de secours ;
  - paramétrage des différents équipements ;
- le secours de la téléphonie :
  - re-routage des appels ;
  - mise en place d'équipements de secours ;
  - paramétrage ;
- la reprise des traitements :
  - adaptations logicielles ;
  - adaptation des procédures d'exploitation ;
  - récupération de flux et synchronisation des données ;
  - traitements exceptionnels ;
  - validations fonctionnelles ;
- la reprise des activités des services utilisateurs :
  - tâches utilisateurs avant mise en place des moyens de secours ;
  - organisation d'un service minimum ;
  - travaux exceptionnels (procédures de contournement, rattrapages, ...) ;
- la communication de crise :
  - interne (personnel, autres entités, ...) ;
  - externe (clients, partenaires, public, ...) ;
- les dispositifs de post-reprise :
  - dispositifs préalables et d'accompagnement (assurance, remise en état des locaux, sauvetage des matériels, ...) ;

- dispositifs de retour à la normale (constituent un plan spécifique le plan de reprise d'activité ou PRA).

Pour être opérationnels, ces dispositifs de secours doivent être accompagnés de dispositifs permanents destinés à les maintenir à niveau (exemples : le plan de sauvegarde, les procédures de mise à jour et de formation des acteurs du PSI, ...).

II.1 LA PARTIE ORGANISATIONNELLE DU PLAN DE SECOURS INFORMATIQUE

Les différentes tâches de pilotage et de mise en œuvre du plan de secours doivent être affectées à des «acteurs ». Ces acteurs sont des entités opérationnelles prédéfinies composées de personnes en nombre suffisant, de manière à ce que, en cas de sinistre, la réalisation de la tâche soit garantie.

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 ;
- les services utilisateurs.

Le comité de crise doit être composé au minimum des Directions suivantes : Direction Générale, Principales Directions utilisatrices, Direction des Services Généraux et des Ressources Humaines, Direction Informatique, Direction de la Communication, Responsable du Plan de Secours. Le comité de crise prend les principales décisions concernant le secours.

Le pilotage proprement dit des opérations de secours peut être confié à une cellule de coordination, qui déchargera le comité de crise de tâches de coordination.

La réalisation des tâches de secours incombe aux équipes d'intervention définies selon les compétences requises, la disponibilité et le lieu d'intervention. On devra s'assurer que les contrats de travail sont compatibles avec un déplacement des équipes concernées sur un autre site.

Les services utilisateurs prennent en charge leur propre plan de reprise d'activité en fonction des moyens de secours 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) ;
- la mise en place de procédures de contournement éventuelles ;
- l'organisation de travaux exceptionnels (exemple : rattrapages).

II.2 LA PARTIE TECHNIQUE DU PLAN DE SECOURS INFORMATIQUE

La solution globale est la résultante de plusieurs solutions adaptées en fonction des exigences de reprise demandées et des pertes de données acceptées par les utilisateurs.

Dans un contexte d'informatique répartie, le scénario retenu sera le plus souvent constitué d'un ensemble de solutions techniques et / ou organisationnelles qui seront combinées selon la situation. Ces solutions élémentaires seront des solutions de secours propres à différents domaines tels que:

- le réseau local ;
- les accès réseau externes ;
- le cas particulier des accès Internet ;
- le secours de serveurs stratégiques devant assurer un service 24h / 24;
- le secours de serveurs pouvant supporter une indisponibilité de 24h;
- etc

Les critères d'évaluation d'une solution de secours peuvent être les suivants :

- le délai de reprise : le délai total de reprise est la somme des délais de déclenchement, temps de mise en œuvre (approvisionnement, restauration, tests, ...), et temps de re-synchronisation des données. Ce facteur, ainsi que la durée maximale de disponibilité des installations de secours sont des paramètres essentiels pour calculer les pertes d'exploitation résiduelles éventuelles, donc l'efficacité de la solution ;
- l'évolutivité de la solution : traduit sa capacité à prendre en compte les évolutions au sein de l'entreprise (architecture technique, organisation, enjeux, nouveaux risques, ...) ,
- les coûts : chaque type de solution entraîne un cortège de frais fixes, variables, récurrents.

II.2.1 DES STRATÉGIES DE SECOURS EN FONCTION DE LA DISPONIBILITÉ DEMANDÉE

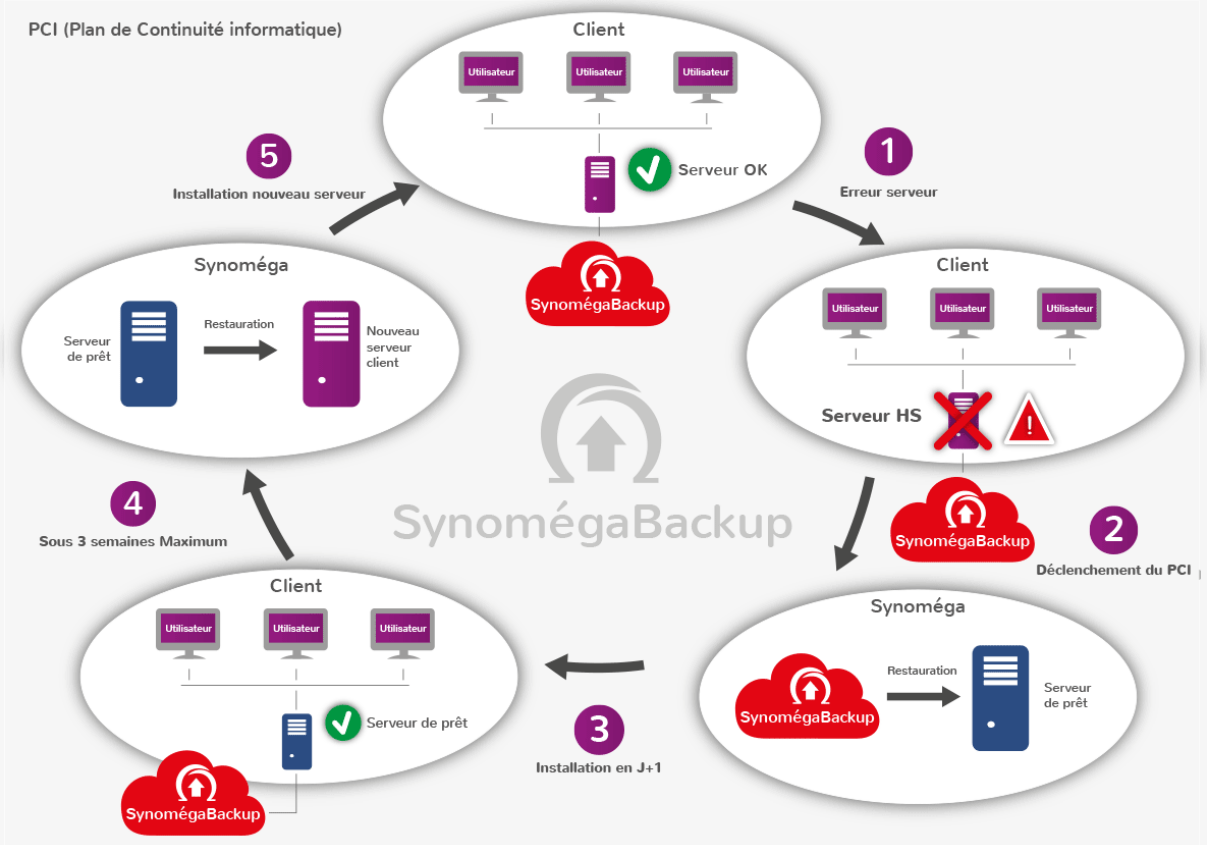
	Haute Disponibilité	Moyenne Disponibilité	Faible disponibilité
Serveurs stratégiques	Serveurs de secours dédiés, géographiquement distants, internes ou externes, en fonctionnement (applications et données). Architecture à haute disponibilité : solutions de type load balancing, cluster de serveurs, mirroring (applications et données).	Serveurs de secours dédiés, géographiquement distants, internes ou externes, interconnectés avec les serveurs à secourir. Système prêt à fonctionner, de type : mirroring distant où copie distante des mises à jour et mise à niveau périodique des bases de données de secours.	Moyens de secours géographiquement distants, internes ou externes et pouvant être mutualisés.
Réseau local	Redondance des équipements. Matériels et rocades de secours avec bascule automatique.	Matériels et rocades de secours.	Kit de câblage volant Existence de locaux de secours utilisateurs externes pré-câblés et pouvant être équipés rapidement (postes de travail, fournitures, ...).
Accès réseaux externes (voix, images et données)	Au moins deux arrivées externes séparées, si possible sur deux sites distincts et via des opérateurs différents. Basculement des communications sur le site de secours en cas de sinistre, avec un maximum d'automatismes. Maillage du réseau d'entreprise.	Nœud de secours externe avec basculement automatique ou manuel (paramétrage). Contrat prévoyant l'intervention de l'opérateur pour une remise en état des liaisons dans un délai déterminé. Matériels de secours.	Engagement d'intervention du fournisseur avec obligation de résultats. Transfert des appels par le fournisseur vers un site de secours.
Téléphonie (équipements)	Secours de l'autocommutateur, si possible dans un local éloigné et basculement automatique des communications.	Contrat prévoyant le transfert des appels par le fournisseur vers un site de secours prêt à prendre les appels (équipements téléphoniques et humains en place).	Autocommutateur de secours. Transfert des appels par le fournisseur vers un site de secours. Mise en place d'un message préenregistré.
Cas particulier des accès Internet (site web)	Double connexion à Internet sur chaque site (site principal et site de secours) avec des fournisseurs d'accès différents, Le basculement peut être automatique par mise à jour des DNS notamment..	Connexion Internet sur le site de secours avec basculement manuel des connexions du site principal vers le site de secours par mise à jour des DNS notamment.	Connexion Internet sur le site de secours avec basculement manuel des connexions du site principal vers le site de secours par mise à jour des DNS notamment.

Comment sécuriser votre Système d'information en appliquant un Plan de Continuité Informatique (PCI) ?

9 mai 2019

PCI : Plan de continuité informatique

Le plan de continuité informatique (PCI) est intégré au plan de continuité d'activité (PCA). Ce plan doit permettre une reprise du système d'information (SI) en cas de sinistre ou de défaillance majeure. L'objectif principal est donc de redémarrer, le plus rapidement et le plus efficacement possible l'activité de celui-ci.



Dans quelles situations la mise en place d'un PCI est-elle nécessaire ?

Le Plan de Continuité Informatique permet de réagir lorsque le Système d'information est impacté lors des situations suivantes :

- Accidents technologiques et industriels
- Catastrophes naturelles (séismes, inondations, tempêtes…),
- Incendies
- Actes de malveillance (hacking, espionnage industriel ..)
- Erreurs humaines

Quelles sont les étapes pour déployer un plan de continuité informatique efficace ?

Étape 1 : identifier les impacts et les risques associés

Un plan de continuité est personnalisé en fonction du contexte de chaque entreprise. Mais la première étape repose souvent sur une analyse des impacts et des risques : c'est une démarche d'audit.

- L'analyse des impacts permet d'évaluer précisément la gravité des dommages en analysant chaque partie du SI.
- L'analyse des risques consiste principalement à identifier les menaces sur le système informatique, puis à les hiérarchiser par ordre de priorité. Par

exemple, une menace bloquante pour le SI nécessite une action de remédiation immédiate. Tant que l'activité de l'entreprise n'est pas impactée, il est possible de temporiser l'intervention visant à endiguer les éventuels risques.

Étape 2 : activer les actions de remédiation technique

Après la phase d'analyse, plusieurs actions techniques sont à activer pour assurer opérationnellement la continuité de service d'un système d'information.

Les trois actions suivantes doivent être effectuées :

- Activer un site de secours, "clone" du site principal pour assurer une continuité du SI et de l'activité de l'entreprise.
- Activer la restauration des données, lorsqu'une politique de sauvegarde automatique en interne ou en externe est en place.
- Activer un LAN (réseau local) de secours pour permettre la communication entre les serveurs.

Ces trois étapes permettent à l'entreprise de redémarrer rapidement son activité et donc de diminuer les pertes occasionnées lors d'un défaut technique du SI.

Étape 3 : tester régulièrement le plan de continuité informatique et organiser des actions de sensibilisation

Le plan doit être régulièrement testé lors d'exercices à organiser chaque année. Les objectifs de ces tests sont les suivants :

- Vérifier l’efficacité des procédures
- Vérifier que le plan est complet et réalisable en situation réelle
- Maintenir un niveau de compétence technique au sein des équipes informatiques

D’autres actions complèteront ces tests “grandeur nature”. Des sessions de formation et de sensibilisation auprès des utilisateurs des SI permettront, par exemple, de vérifier si les procédures, les normes d’utilisation et la confidentialité des codes d’accès sont respectées.

Un plan de continuité informatique efficace doit donc être revu et régulièrement mis à jour en prenant en compte l’évolution des technologies et le SI de l’entreprise ciblée.

ANNEXE A

« Présentation synthétique de la collectivité »

Les agents et les services communautaires de INGAGGLO

800 agents, organisés de la manière suivante, travaillent pour la Communauté d'Agglomération :

- Siège (regroupe les services administratifs et fonctions supports)
- Centre Technique Communautaire (l'essentiel des services techniques)
- Service des autorisations du droit des sols

Sous l'autorité du Président, la Direction Générale des Services s'appuie sur :

- La Direction des ressources et moyens généraux
- La Direction des services techniques
- La Direction de l'environnement et des transports
- La Direction de l'aménagement et de la cohésion sociale

Les compétences de la Communauté d'Agglomération sont les suivantes :

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

OPTIONNELLES

- Assainissement ;
- La protection et la mise en valeur de l'environnement et du cadre de vie ;
- La construction, l'aménagement, l'entretien et la gestion d'équipements culturels et sportifs d'intérêt communautaire ;
- La création ou l'aménagement et l'entretien de la voirie d'intérêt communautaire et des parcs de stationnement d'intérêt communautaire.

FACULTATIVES

- Aménagement numérique du territoire ;
- Tourisme
- Réalisation aménagement gestion d'équipements touristiques structurants
- Gestion des Milieux Aquatiques et Protection des inondations (animation et concertation)
- Participation facultative, en particulier, aux animations culturelles, sportives ou touristiques d'intérêt communautaire (animations ayant un rayonnement communautaire, et supra-communautaire)

ANNEXE B

« Descriptif des SI de la collectivité »

Les services communautaires sont répartis sur 2 sites :

- Siège (et service Autorisation droit du sol)
- Centre Technique Communautaire

Les deux sites disposent chacun d'un réseau local (LAN) à 1 Gbit/s (« backbone ») et d'une vingtaine de serveurs pour le site n°1, d'une quinzaine pour le site n°2 (Applications « métier » Active Directory, DNS, Antivirus, site Web, serveurs de fichiers, serveur d'impressions,..)

Ces sites sont interconnectés en VPN-IP via une liaison SDSL à 8 Mbit/s.

Une différence subsiste néanmoins entre les deux sites.

Le premier site (Site n°1) possède un réseau SAN (Storage Area Network) réalisé à base de commutateurs Fiber Channel (FC), qui permet le stockage de données « métier » conséquentes (~20 To pour une dizaine de disques montés en Raid)

Le plan d'adressage IP du site n°1 respecte sensiblement un adressage de type classe B (RFC1597 à partir de l'adresse IP 172.16.16.0) avec un masque de réseau fixé à 20.

Quant à celui du site n°2, il est défini en CIDR (Class Inter Domain Routing) à partir d'un adressage de type classe C (192.168.0.0/21)

Mandatée par la Direction Générale, la Direction des Systèmes d'Information (DSI) mène actuellement une réflexion dans le but d'homogénéiser ces deux systèmes d'information, notamment au niveau applicatif.

Il s'agit de concevoir une future infrastructure réseau à mettre en place (virtualisation des serveurs, SAN, lien d'interconnexion de réseau) et d'assurer la résilience, la haute disponibilité et la sécurité du nouveau système d'information

La DSI souhaite mettre en place un seul et unique système d'information (« Datacenter »), avec comme site principal, le site n°1 (Siège)

Le site n°2 serait alors considéré comme un site distant, qui ne conserverait que ses serveurs locaux de proximité (fichiers, impressions,..) et son réseau local (LAN) existant

Le site principal hébergerait ainsi la totalité des applications « métier » et les serveurs associés.

Le projet ne prend pas en compte la téléphonie, qui évoluera dans un second temps, vers une solution dite de convergence en IP.

Dans la future infrastructure, un VLAN « spécifique » sera créé pour la mise en œuvre de la téléphonie sur IP.

L'accès aux données doit être sécurisé à partir du futur réseau, qu'il soit local ou distant, voire nomade.

La mise en place de cette architecture doit permettre :

- De remplacer certains serveurs physiques obsolètes par des serveurs « virtualisés »
- De « Virtualiser » la plupart des serveurs grâce à la technologie « VMWare »
- De mettre en place ces serveurs rack dans de nouvelles baies (datacenter)
- De sécuriser l'accès aux données « métier » et aux applications « métier »
- De gérer l'interconnexion du réseau de stockage SAN actuel avec le nouveau réseau ainsi constitué.