RESSOURCES HUMAINES

Déploiement d'un plan de continuité d'activité

Contexte

La pandémie de coronavirus Covid-19 de l'année 2020 nous le rappelle de façon criante : nos structures, qu'elles soient publiques, privées ou mixtes, sont toutes égales face à la crise. Leurs fonctions principales sont fragilisées et peuvent être brutalement mises à l'arrêt ; les modes d'organisation du travail sont affectés et nécessitent d'être repensés au pied levé ; c'est toute une structure donnée en tant que telle qui doit trouver l'alternative pour assurer la continuité, ou la reprise dans les meilleurs délais, de ses activités.

Si les enjeux économiques et sociaux de la continuité d'activité des entreprises font régulièrement la une des médias, la nécessaire continuité d'activité des structures publiques fait moins de bruit. Et pourtant... La bonne réalisation des missions de service public des collectivités territoriales, syndicats, établissements publics, SDIS, etc. est essentielle au fonctionnement des territoires et des sociétés - tellement évidente, aussi, qu'on oublierait presque de la souligner.

Cette fiche-synthèse, rédigée spécifiquement à l'intention des acteurs publics, se veut un outil pratique et un levier opérationnel pour préparer à froid et, si besoin, déployer à chaud, un plan de continuité d'activité. Elle s'appuie sur une longue expérience éprouvée au sein de structures publiques et enrichie au contact des acteurs privés en matière de déploiement de plans de continuité d'activité.

La démarche PCA

Nous nous intéresserons uniquement aux plans de continuité d'activité ici, partant du postulat que les plans de reprise d'activité ne sont pas l'objectif optimal à viser ; nous traiterons par ailleurs le sujet sous un angle à la fois technique (informatique) et organisationnel (modes de travail).

Qu'est-ce qu'un plan de continuité d'activité, usuellement abrégé « PCA » ?

La définition proposée par Wikipédia semble suffisamment précise et explicite pour la reprendre telle quelle : « *Dans le cadre d'une gestion de crise, le plan de continuité, aussi appelé plan de continuité d'activité (PCA) ou parfois plan de continuité des opérations (...) est un document devant permettre à une entité (gouvernement, collectivité, institution, entreprise, centrale énergétique, hôpital, école, service public délégué etc.) de fonctionner même en cas de désastre ou de crise majeure, quitte à ce que [cela s'effectue] en "mode dégradé". Il a pour but d'anticiper un événement qui perturbe gravement l'organisation normale de l'entité et de mettre en place une stratégie qui permet d'en limiter l'impact* ».

Autrement, un PCA vise à anticiper, lister et documenter l'ensemble des mesures à déployer dans un temps minimal en cas d'événement inattendu qui affecte la continuité de l'activité d'une structure. L'ISO 22301:2012 définit ainsi le PCA comme l'ensemble des « *procédures documentées servant de guide aux organisations pour répondre, rétablir, reprendre et retrouver un niveau de fonctionnement prédéfini à la suite d'une perturbation* ».

Pourquoi préparer son plan de continuité d'activité ?

Toute crise ou événement majeur entraîne invariablement la fragilisation des processus métiers et de l'organisation du travail. La sentence peut être sans appel lorsqu'aucun rempart n'existe pour endiguer rapidement et efficacement les conséquences d'un tel événement.

Préparer un plan de continuité d'activité ne permet pas seulement de procéder au sauvetage des activités d'une structure lorsque le contexte politique, économique, sociétal, environnemental, etc. affecte gravement le bon fonctionnement des processus métiers. Préparer un plan de continuité d'activité est une démarche proactive visant à ne pas subir mais, au contraire, anticiper, les conséquences d'une crise ou d'un événement majeur – ou, *a minima*, les limiter tant que faire se peut.

✔

Le plan de continuité d'activité est une démarche stratégique, clairement documentée et formalisée, permettant de prévoir l'ensemble des mesures et processus techniques et organisationnels qui permettront notamment d'épargner et d'adapter les outils informatiques, les modes d'organisation du travail et la collaboration à distance, avec l'objectif de maintenir un niveau d'activité (i) optimal au vu des contraintes soudainement imposées par une crise ou un événement majeur (ii) justement proportionné aux exigences de continuité propres à chaque structure.

Comment penser son plan de continuité d'activité ?

Un plan de continuité d'activité nécessite d'inclure l'ensemble des Directeurs et Responsables des fonctions principales d'une structure donnée. Typiquement, une collectivité territoriale va impliquer tous ses Responsables techniques et métiers, sous l'égide des Directeurs adjoints et généraux des services, pour prendre en considération l'intégralité des besoins de ses collaborateurs et partenaires dans son plan de continuité d'activité. On parle ici d'une démarche collégiale qui consiste à penser, ensemble, aux moyens techniques et organisationnels qui permettront d'assurer la continuité de toutes les activités identifiées comme critiques pour la bonne marche de la structure. Cette démarche doit naturellement intégrer la dimension E-Administration des processus métiers et la dématérialisation des documents associés, aujourd'hui largement répandues au sein des gammes logicielles pour les acteurs publics – lesquels doivent en outre s'assurer de pouvoir continuer à utiliser les outils et services d'État pour mener à bien leurs missions quotidiennes.

La mise en place d'un PCA vise à anticiper les conséquences d'une crise.

Pourquoi s'appuyer sur des experts en la matière pour assurer son plan de continuité d'activité ?

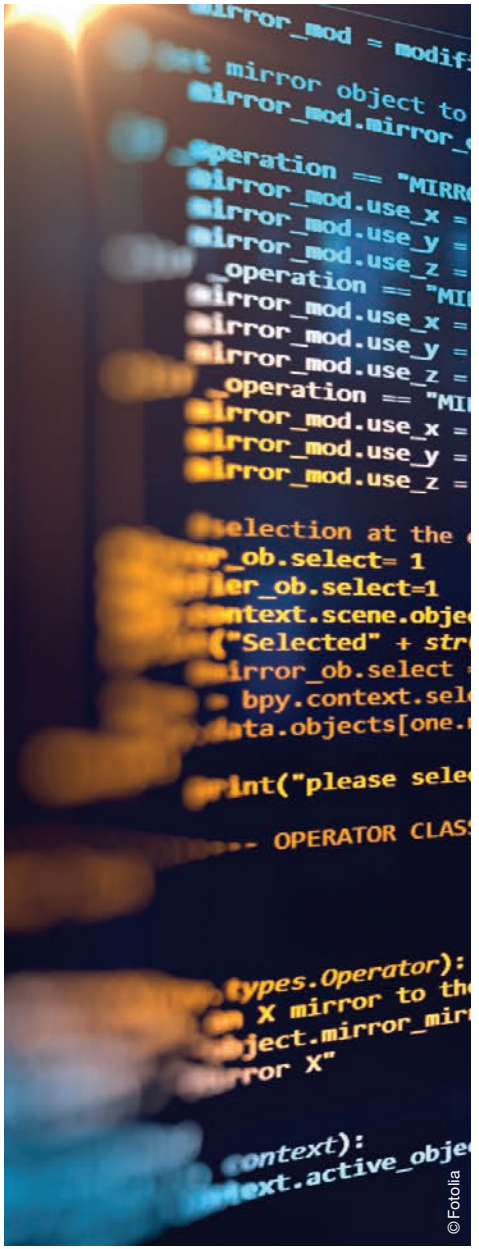
Anticiper un plan de continuité d'activité efficace et opérationnel, sans interruption brutale et critique, ni bouleversement des processus métiers, nécessite une somme de savoir-faire de niveau Expert. Il ne s'agit pas de mettre quelques jours ou plus à permettre aux utilisateurs d'accéder à leurs outils informatiques quotidiens pour assurer la continuité de leurs activités. Il ne s'agit pas non plus de compromettre la sécurisation des données, des flux de données et des documents associés au nom de la nécessaire « survie » des activités, ni même de s'affranchir des contraintes réglementaires en vigueur.

Préparer un plan de continuité d'activité implique donc également de prévoir du matériel et des infrastructures informatiques qui, mis bout à bout, s'avèrent extrêmement coûteux. Il ne s'agit pas seulement d'équiper ses collaborateurs d'ordinateurs portables et de téléphones mobiles reliés de façon sécurisée aux applications métiers, aux systèmes d'information voire à l'ensemble de l'ERP. Si ces frais matériels sont à imputer sur le budget propre à chaque structure, l'infrastructure informatique et les dispositifs PCA qui permettront *réellement* d'assurer une continuité d'activité efficace et une bascule immédiate en mode PCA sont l'affaire des spécialistes en la matière. Des experts qui investissent des millions d'euros pour bâtir des infrastructures informatiques interconnectées à l'ensemble des opérateurs télécoms et fournisseurs d'accès à Internet, totalement dupliquées et redondées d'un point de vue physique et réseau, et sécurisées de bout en bout à l'aide de plusieurs couches matérielles et logicielles destinées à assurer la totale étanchéité des applicatifs et la parfaite intégrité des données pour assurer les plans de secours informatiques.

« Attention !
Un PCA informatique n'est pas une sauvegarde isolée, ni un serveur de backup, ni même un accès dégradé aux applicatifs nécessaires à la continuité d'activité des structures.
Un PCA est un ensemble de ressources informatiques et humaines complet et auto-suffisant, immédiatement opérationnel en cas de crise, visant à rendre transparente, ou quasiment transparente, la discontinuité d'activité pour les utilisateurs ».

Rémi GRIVEL,
Vice-Président du Clusir Rhône-Alpes,
Directeur général de SynAApS
et de Ciril GROUP.

Préparer un PCA implique donc également de prévoir du matériel et des infrastructures informatiques.



© Fotolia

Parole d'expert

Rémi GRIVEL, vous êtes Vice-Président du Club de la Sécurité des Systèmes d'Information de la région Auvergne-Rhône-Alpes (Clusir Rhône-Alpes), mais aussi Fondateur et Directeur général de SynAApS, en sus de vos fonctions de Directeur général de Ciril GROUP.

Sans rentrer dans les spécifications techniques et organisationnelles d'un PCA, quels conseils, ou points de vigilance, transmettez-vous à vos clients et partenaires lorsque vous les accompagnez dans leurs plans de continuité d'activité ?

« Préparer son plan de continuité d'activité implique de savoir analyser les vulnérabilités des applicatifs, systèmes d'information, plateformes applicatives et infrastructures informatiques en place. Ce, pour permettre d'évaluer finement les risques, puis de définir précisément des objectifs et besoins de continuité en fonction du niveau de service minimum visé et de la durée d'indisponibilité maximale acceptée par chaque structure, en cas d'événement qui viendrait affecter la disponibilité et la sécurisation des outils et données.

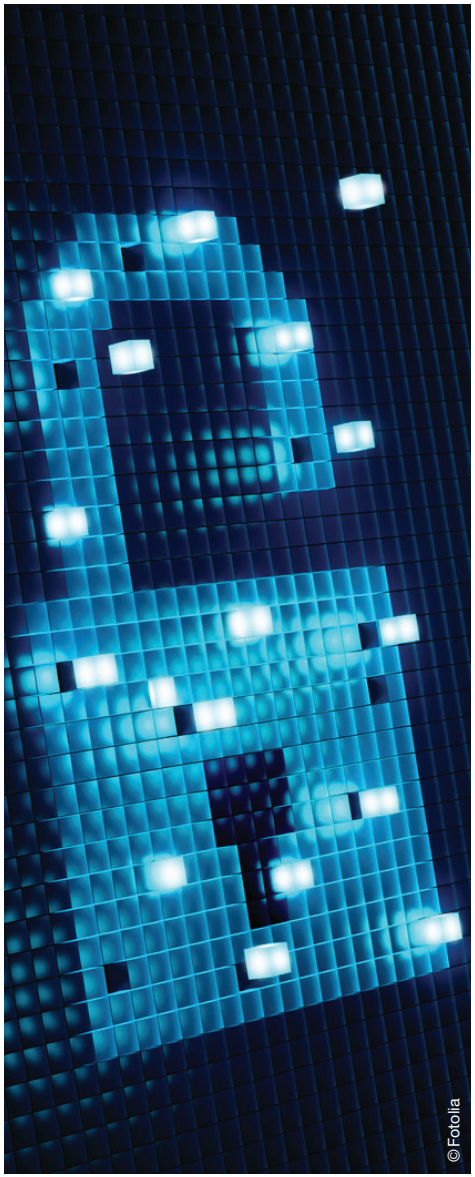
Il s'agit donc de mobiliser des compétences de niveau Expert dans les domaines :

- ***des infrastructures, des systèmes et des réseaux*** *- pour concevoir l'architecture et bâtir les infrastructures informatiques aptes à absorber la charge attendue au vu des modes d'utilisation des applicatifs qu'elles hébergent ;*
- ***des systèmes de management de la sécurité de l'information (SMSI)*** *- pour garantir l'étanchéité des environnements de production, la sécurisation des données, flux de données et documents associés, ainsi que l'intégrité des données exploitées sur ces infrastructures informatiques ;*
- ***des dispositifs de reprise d'activité et de continuité d'activité (PRA et PCA)*** *- pour pouvoir superviser en temps réel les infrastructures informatiques et pouvoir monitorer à distance les applicatifs, allouer ou réallouer à la volée des ressources informatiques (CPU, RAM, bande Internet, capacité de stockage) et machines virtuelles nécessaires à la continuité des applicatifs, effectuer des bascules informatiques de plateformes applicatives, etc.*

Si ces opérations s'effectuent le plus souvent « à froid » et au gré des nouveaux besoins des utilisateurs, elles doivent également pouvoir être déclenchées « à chaud », en cas de sinistre soudain sur une application, une plateforme ou une infrastructure hébergée.

✓

Dans ce second cas de figure, il est primordial de pouvoir réagir très rapidement - pour ne pas dire immédiatement, et d'infogérer au pied levé les applications, plateformes et infrastructures impactées, avec des processus documentés, extrêmement complets et détaillés, afin de rétablir la continuité des services impliqués... et ne pas engendrer de problèmes dans la complexité liée à une situation d'urgence et de stress.


© Fotolia

Dès lors, à moins de disposer dans sa structure d'une Direction des Services Informatiques très hautement qualifiée, dotée de toutes les compétences de gestion de crise d'une part, de toutes les couches hardware, systèmes, réseaux, logicielles et sécurité nécessaires à la mise en œuvre et au maintien opérationnel de son propre plan de continuité d'activité d'autre part, il convient impérativement de se tourner vers un acteur dont c'est le métier que de concevoir, préparer et déployer des plans de continuité d'activité en un temps record.

✔

Faites-vous accompagner par un spécialiste de l'hébergement Cloud certifié Sécurité (typiquement, ISO 27001:2013) et doté de l'ensemble des moyens techniques et humains pour parer aux situations de crise. Prévenez plutôt que de guérir ; une fois le sinistre arrivé, les dommages induits sont souvent cher payés, irrémédiables dans les pires des cas. N'attendez pas d'être au pied du mur pour préparer votre plan de continuité d'activité, épargner votre production et vos services et préserver la bonne marche de votre structure. Au même titre que vous souscrivez une assurance pour protéger vos actifs, prévoyez un plan de continuité d'activité pour protéger votre activité.

À ce titre, les engagements contractuels de votre prestataire en matière de GTI (garantie de temps d'intervention) et de GTR (garantie de temps de rétablissement) doivent être étudiés scrupuleusement, de même que ses moyens techniques et humains réellement mobilisables en situation de crise, afin de vous protéger de toute mauvaise surprise. Assurez-vous qu'il propose de véritables dispositifs PCA natifs. Vérifiez également qu'il est dans l'obligation tangible de déployer des moyens proportionnés aux divers scenarii susceptibles d'affecter vos outils et que vous avez les moyens d'exercer de la pression et de vous faire entendre en cas de manquement de service contractuel. Dans la lignée de ces prérequis, vérifiez les dires de votre hébergeur Cloud quant au périmètre de ses certifications et dispositifs PCA, afin de ne pas découvrir trop tard que vous pensiez bénéficier des meilleures garanties là où cela pourrait bien ne pas être le cas ».

✔

La lecture et la validation de vos contrats d'hébergement Cloud par un juriste spécialisé, de même qu'un audit de l'infrastructure et des équipes de votre hébergeur seront un gage de confiance pour vous et vos équipes, *a fortiori* si vous pilotez un ou plusieurs services critiques pour votre activité.

Propos recueillis auprès de
Rémi GRIVEL, Vice-Président
du Clusir Rhône-Alpes,
Directeur général de SynAApS
et de Ciril GROUP.

RETOUR D'EXPÉRIENCE

Amaël GRIVEL
et Rémi GRIVEL,
de la Direction générale
de Ciril GROUP

Ciril GROUP, éditeur de logiciels, systèmes d'information et portails web spécialisé depuis 40 ans auprès des acteurs publics, témoigne de la mise en œuvre de son plan de continuité lors de la crise générée par la pandémie de coronavirus Covid-19 de l'année 2020, ainsi que de l'accompagnement de ses clients et partenaires dans leurs propres plans de continuité d'activité.

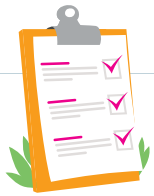
« Ciril GROUP accompagne, parmi l'ensemble de ses clients publics et privés, plus de 2 000 collectivités territoriales dans l'exercice de leurs métiers et la réalisation de leurs missions de service public... en temps normal comme en temps de crise ! Nous avons tout d'abord déployé notre plan de continuité d'activité, qui était en réalité déjà prêt, pour assurer le maintien de l'intégralité de nos prestations vis-à-vis de nos clients et partenaires. Nous avons donc pu communiquer très rapidement auprès de nos clients et partenaires pour leur apporter la sérénité nécessaire et les engager dans une dynamique de résilience commune.

Nous avons ensuite mobilisé d'importants moyens techniques et humains pour faciliter et accélérer la mise en œuvre des plans de continuité de service de nos clients et partenaires, mais aussi de ceux qui n'avaient pas encore préparé leurs plans de continuité d'activité. Nous avons, pour ces derniers, ouvert des accès à distance totalement sécurisés à leurs logiciels, plateformes et infrastructures applicatives hébergées dans nos datacenters SynAApS ; nous avons également redimensionné leurs ressources à la demande, avec des garanties exemplaires en matière de cybersécurité (certification ISO 27001:2013 pour tous, certification HDS plus particulièrement pour le secteur de la santé et des laboratoires de biologie médicale).

Nous avons en outre ouvert gracieusement notre plateforme SIG GEO Software à toutes les collectivités territoriales françaises qui avaient un besoin urgent de déployer rapidement et efficacement une ou plusieurs solutions cartographiques grand public en mode web HTML5 responsive. Cette opération de solidarité et d'entraide a largement contribué à aider les collectivités territoriales pas ou mal équipées en matière de solutions SIG à rester au plus proche de leurs territoires, en leur rendant accessibles les outils web et mobiles aptes à leur permettre de communiquer par la carte avec les citoyens, professionnels de santé et acteurs économiques locaux ».

Aujourd'hui, nos clients et partenaires qui n'avaient pas encore réfléchi à leurs plans de continuité d'activité ont pris la mesure de la nécessité absolue de s'y atteler, car la crise Covid-19 de 2020 n'est qu'un déclencheur d'un risque qui peut survenir à nouveau … et à tout moment.

Le PCA dans la pratique : la check-list en 12 points pour préparer son PCA



D'UN POINT DE VUE TECHNIQUE :

vérifier la qualité et la fiabilité d'un PCA

1. Avez-vous fait cartographier précisément le système d'information de votre structure, afin de disposer d'une vision complète et immédiate de l'ensemble de vos applications métiers ?

2. Avez-vous fait évaluer vos besoins et attentes en matière de fonctionnement en mode PCA ?

- services indispensables au fonctionnement de votre activité ;
- PCA global ou plusieurs PCA spécifiques à chaque service et/ou application de votre structure ?
- scenarii et critères de bascule en mode PCA ;
- outils mis à disposition pour assurer la continuité de vos services ;
- périmètre et viabilité globale du mode PCA pour votre structure et votre organisation.

3. Faites-vous tester et superviser les différents composants de votre plan de continuité d'activité ?

- tests de fonctionnement de vos applications en mode PCA ;
- tests de sécurité et d'analyse de la vulnérabilité de vos applications en mode PCA ;
- tests de détection de bascule en mode PCA, y compris lorsque l'incident majeur a déjà démarré ?

4. Avez-vous formé et sensibilisé les acteurs internes et externes de votre structure à l'utilisation de vos processus et outils de continuité d'activité ?

5. Avez-vous prévu un plan de communication interne et externe ?

6. Faites-vous vivre votre plan de continuité d'activité en fonction de l'évolution de votre système d'information, en vue de vérifier le bon fonctionnement de vos applications en mode PCA dès lors que votre infrastructure informatique évolue ?

D'UN POINT DE VUE ORGANISATIONNEL :

assurer la connexion à distance au système d'information

7 Vos collaborateurs sont-ils équipés du matériel utile et nécessaire à la continuité de leurs activités : ordinateurs portables, téléphones portables pour les équipes de contact, tablettes pour les équipes mobiles, etc. ?

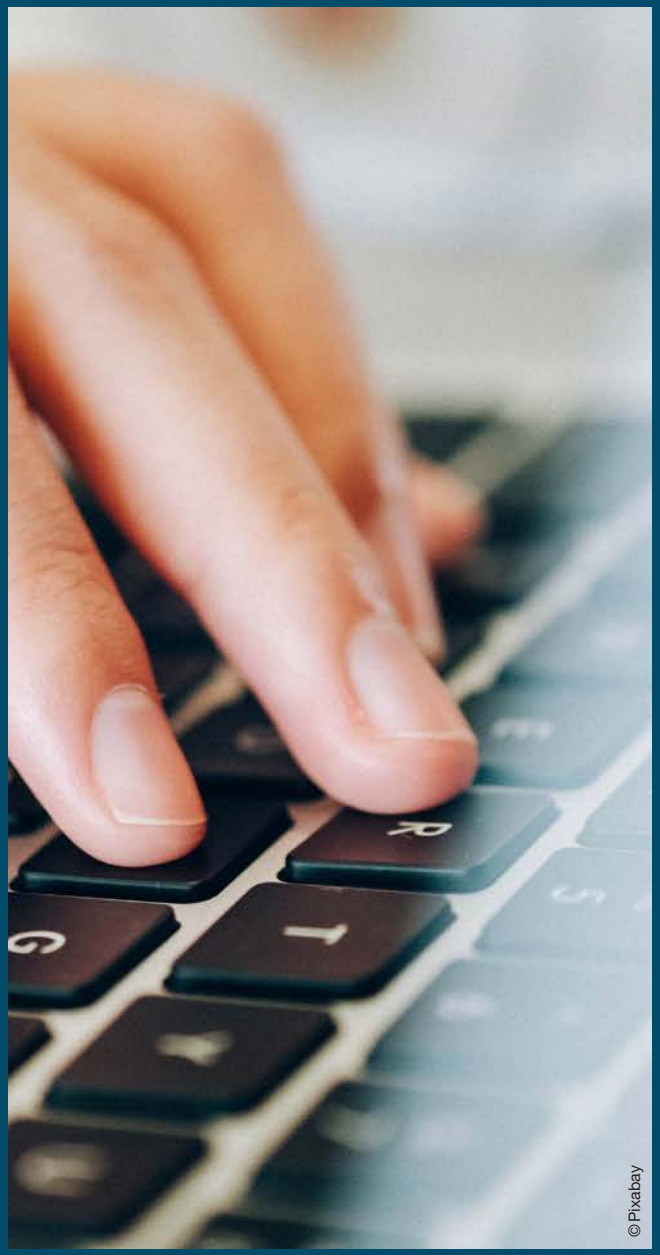
8 Vos collaborateurs sont-ils reliés à votre système téléphonique et à vos applicatifs métiers : solutions de renvoi d'appels de leurs lignes directes sur les lignes mobiles professionnelles, annuaire interne, VPN, reverse-proxy, etc. ?

9 Vos collaborateurs se connectent-ils de façon sécurisée à vos applicatifs, vos systèmes d'information et/ou vos plateformes applicatives : systèmes d'exploitation et antivirus à jour, authentification et VPN sécurisés, règles réseaux de filtrage des domaines web, etc. ?

10 Vos utilisateurs disposent-ils des technologies de communication modernes pour faciliter la collaboration : messagerie email, outil de visioconférence, solution de tchat, etc. ?

11 Vos collaborateurs bénéficient-ils d'une GED pour pouvoir accéder aux documents nécessaires à leur travail à distance (typiquement, bons de commandes dématérialisés, avec processus de validation interne et signatures électroniques du Maire ou Président), pour pouvoir envoyer plus rapidement et efficacement les documents financiers et comptables nécessaires à la passation de commandes de première nécessité ?

12 Vos collaborateurs bénéficient-ils d'une vision globale de la situation interne à un instant T : Intranet ou ERP offrant l'accès à la planification des ressources, la consultation des messages et circulaires internes, la visualisation de l'activité des services, etc. ?



© Pixabay

SOURCES

- **Ministère de l'Économie et des Finances**
  Les grandes fonctions d'entreprise
  https://www.economie.gouv.fr/facileco/dossier-fonctions-lentreprise
- **Wikipédia**
  Le plan de continuité d'activité
  https://fr.wikipedia.org/wiki/Plan_de_continuit%C3%A9
- **Clusir Rhône-Alpes**
  Club de la Sécurité des Systèmes d'Information Régional de Rhône-Alpes
  https://www.clusir-rha.fr/
- **SynAApS**
  La division hébergement Cloud certifiée Sécurité (ISO 27001:2013) et Santé (HDS) de Ciril GROUP
  https://www.synaaps.com/fr/
- **PRA informatique et même humain**
  Des dispositifs essentiels en cas de crise
  https://www.synaaps.com/fr/offres/pra-pca-synaaps.html

POUR ALLER PLUS LOIN

- **Secrétariat général de la Défense et de la Sécurité nationale (SGDSN)**
  Guide pour réaliser un Plan de continuité d'activité
  http://www.sgdsn.gouv.fr/uploads/2016/10/guide-pca-sgdsn-110613-normal.pdf

CONTACTS

ADGCF . **Katia Paulin** . **katia.paulin@adgcf.fr**

CIRIL GROUP . **Luc Payssan** . **lpayssan@cirilgroup.com** . **04 72 69 16 80** . **06 82 55 57 84**