LA CONTINUITÉ D'ACTIVITÉ ET SON MANAGEMENT

Compte rendu de la rencontre du lundi 14 novembre 2016

François Tête
francois.tete.ext@devoteam.com
Rapporté par Alain Coulon
alain.coulon@adeli.org

Résumé :

Cet article rend compte de l'événement « Rencontre autour d'un verre », organisé par ADELI le 14 novembre 2016 au Café de la Mairie – Paris 3ème. Le conférencier, François Tête, ancien Président d'ADELI, nous expose comment assurer l'activité d'une entreprise malgré la survenue d'incidents majeurs ou pendant la gestion de crise.

Mots-clés :

ADELI, Rencontre, PCA, menaces, incidents, gestion de crise

« Nos entreprises doivent être en capacité d'affronter de nombreuses menaces, en particulier celles qui les paralyseraient en s'attaquant à leur système nerveux : le système d'information. Malheureusement d'autres menaces peuvent également paralyser l'entreprise : bâtiment impraticable, fournisseur indisponible, collaborateurs indisponibles (pandémie…).
Pour minimiser les conséquences d'un sinistre majeur, en permettant à l'entreprise de lui survivre, il convient de préparer, d'actualiser, de valider régulièrement un plan de continuité d'activité à mettre en œuvre au cas où…
Ces précautions ont un coût, à relativiser en fonction du coût des conséquences d'un sinistre majeur.

> *Les tuiles qui protègent de la pluie ont toutes été posées par beau temps - Proverbe chinois.*

DE L'INFORMATIQUE À LA CONTINUITÉ D'ACTIVITÉ

François Tête

Notre animateur, François Tête, a rejoint ADELI dès sa création et a maintenu son adhésion au fil des étapes de sa carrière professionnelle. Il a présidé l'association de 1982 à 1987, pendant le « quinquennat » qui a donné naissance au Méthodoscope, l'une des rampes de lancement de notre association.

Un événement à l'origine d'une évolution professionnelle

Le 1er mai 1977, le centre informatique d'une banque française a été endommagé par un incendie. François Tête fut désigné comme responsable de la reprise d'activité ; ce qui fut fait après 5 jours d'arrêt, délai qui, aujourd'hui (compte tenu de la rapidité des transactions) serait fatal à un établissement bancaire.

François Tête s'associa à Paul Théron (un autre président historique d'ADELI) pour créer une entreprise, TTA, spécialisée dans le domaine de la continuité d'activité ; laquelle entreprise intégra une plus grande structure XP Conseil. François Tête a poursuivi sa carrière professionnelle dans le cadre de Devoteam. Il y mit au point un logiciel de gestion des plans de continuité et de gestion de crise : RVR Parad. Il est l'un des créateurs et responsables du Club de la Continuité d'Activité (www.clubpca.eu).

LA CONTINUITÉ D'ACTIVITÉ : DE QUOI S'AGIT-IL ?

Dans les dernières décennies, les menaces se sont diversifiées, en particulier par des agressions techniques malveillantes qui s'ajoutent aux catastrophes naturelles.

La continuité d'activité dans le domaine professionnel consiste à se mettre en capacité de poursuivre ses activités après une perturbation majeure. Il importe de faire en sorte que les conséquences des perturbations provoquées par un sinistre ne soient pas fatales.
D'où la nécessité de mettre en place des plans dédiés appelés « Plans de Continuité d'Activité ».

Plan de continuité d'activité (PCA)

> *Un Plan de Continuité d'Activité (PCA) est un ensemble de mesures visant à assurer, selon divers scénarios de crises, y compris face à des chocs extrêmes et, le cas échéant, de façon temporaire, en mode dégradé, des prestations de services essentiels de l'entreprise puis la reprise planifiée des activités (paru le 26 février 2004 au Journal officiel de la République française).*

Le PCA vise à limiter les conséquences d'un sinistre auprès des clients, les impacts financiers, les pertes d'images et de répondre aux demandes des clients et des actionnaires.

Inventaire des risques

Les risques peuvent être totalement spécifiques à l'entreprise, mais il semble préférable (plus simple et plus facile à partager) de recourir à un portefeuille standard :

- six risques élémentaires portant sur les ressources : bâtiment, informatique, personnel, outils de production industriel et de pilotage (exemple : centre de commande), réseaux (énergie, télécoms, eau, électricité), prestataires et fournisseurs critiques (chaîne logistique);
- six risques « majeurs » : naturels (inondation, séisme, aléa climatique), pandémie, accident industriel externe (sites SEVESO, transport de matière dangereuse, installation nucléaire…), cyber-menace, mouvements sociaux, terrorisme (notamment par les progiciels).

Ces risques sont en partie interdépendants : une inondation peut affecter les installations, le personnel, les fournisseurs…

Bilan d'impact sur l'activité

Les responsables des différents métiers de l'entreprise doivent exprimer leurs besoins de continuité pour assurer le fonctionnement de leurs processus prioritaires, quoi qu'il arrive.

Le BIA (Business Impact Analysis en anglais, Bilan d'Impact sur l'Activité en français) définit les facteurs propres à chaque activité qui seront pris en compte dans le PCA. Il s'agit de déterminer et de justifier les niveaux d'activité à maintenir par processus ou par activité. L'évaluation en incombe aux métiers concernés qui doivent déterminer également les ressources nécessaires pour fonctionner. Leurs besoins devront être validés par la Direction Générale. En particulier, le BIA quantifie les principaux critères suivants :

- **la Durée Maximale d'Interruption Admissible** (DMIA) :
durée au-delà de laquelle les impacts sur l'organisme deviennent intolérables ;
- **la Perte Maximale de Donnée Tolérable** (PMDT) :
perte maximale de donnée tolérée à la reprise d'activité, au-delà de laquelle les conditions de récupération ne sont plus acceptables ;
- **le nombre de positions de travail** incluant les ressources humaines par fonction et les moyens matériels nécessaires pour assurer les activités critiques ;
- **le niveau de dégradation de service acceptable**, par exemple 60 % de la charge nominale ;
- **les stocks minimaux** pour assurer la continuité d'activité.

Deux stratégies : la robustesse et la résilience

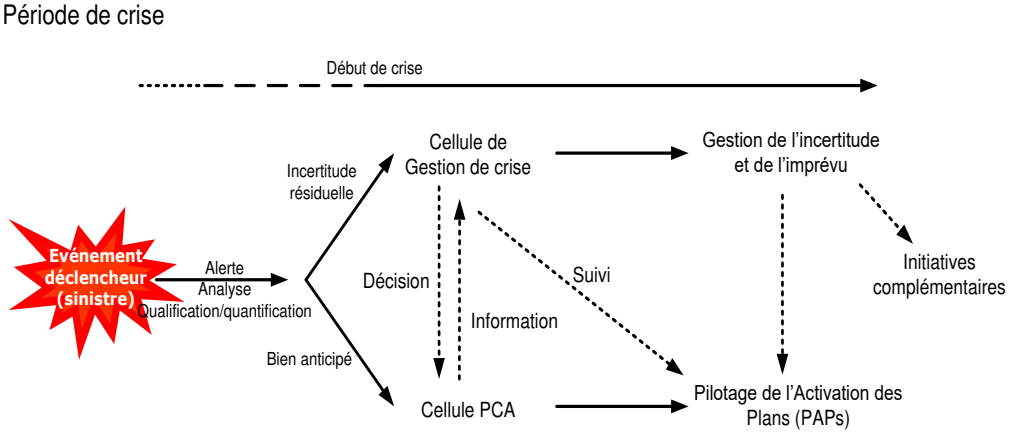
La continuité d'activité s'intègre dans la stratégie de gestion des risques de l'entreprise.
La stratégie de continuité d'activité doit prendre en compte deux types complémentaires de stratégie, la robustesse et la résilience pour protéger les ressources nécessaires au fonctionnement de l'entreprise :

- **Robustesse :** qualité d'un organisme pour absorber des chocs sans dégrader de façon visible son fonctionnement.
  Exemple : deux sites connectés de façon synchrone ;
  l'utilisateur du service ne perçoit aucune perturbation lors de la défaillance d'un site.
- **Résilience** : capacité d'un organisme d'absorber des chocs, de rebondir et de revenir à une situation normale rapidement.

  Suite de l'exemple précédent : si les deux sites connectés précédents sont indisponibles en même temps, une autre solution **résiliente** serait un site de secours distant connecté en asynchrone, non soumis aux mêmes risques ; l'utilisateur perçoit une légère perturbation de courte durée lors de la reprise sur le site de secours.

LA GESTION DE CRISE DANS LE CADRE DU PCA

La gestion de crise intervient lorsque les PCA sont dépassés ou non concernés par la situation constatée. Ils nécessitent alors l'implication d'un organe de décision.



Pour gérer une crise efficacement, il faut, avant la crise, disposer de fiches réflexes pratiques :

- Qui va activer la gestion de crise ?
- Comment s'organise-t-on (décision, anticipation, main courante, …) ?
- Quelles sont les obligations et les responsabilités des cellules de crise ?
- Quelles compétences, quels suppléants, quelle préparation, quel entraînement ?
- Quelle stratégie de gestion de crise adopter ?
- Quelle stratégie de communication interne et externe prévoir ?
- Quelle logistique de crise mettre en place ?

LA DÉMARCHE DE LA MISE EN ŒUVRE D'UN PCA

La mise en œuvre d'un PCA se fait en sept étapes. Le processus s'intègre dans un processus d'aménagement continu, basé sur la roue de Deming.

LE MAINTIEN EN CONDITION OPÉRATIONNELLE

Le Maintien en Condition Opérationnelle de la gestion de crise et du PCA a pour objectifs de :

- prendre connaissance des changements organisationnels, techniques et logistiques :
  - changements d'organisation,
  - changements de personnes,
  - changements de locaux,
  - évolutions des risques,
  - évolutions des besoins de continuité d'activité,
  - changements de la réglementation,
  - évolutions des ressources matérielles et logistiques,
  - évolutions des systèmes d'information ;
- mesurer l'impact de ces changements sur les dispositifs et notamment sur le PCA ,
- s'assurer de la mise à jour de tous les plans ;
- contrôler que le PCA continue à assurer la continuité d'activité conformément aux besoins des métiers prioritaires ;
- contrôler le caractère opérationnel et auditable des PCA des prestataires essentiels externalisés.

LA VALIDATION DES PCA

Un PCA insuffisamment validé risque de ne pas fonctionner, créant des difficultés de prise de décision au sein de la cellule de crise ; ce qui aurait un effet négatif sur les activités de l'organisme concerné.

Le caractère probant de la validation d'un PCA ne peut pas être atteint à 100% ; en revanche, on peut s'en approcher progressivement par des exercices réguliers.

Il convient de :

- s'entraîner en vue de l'avènement d'un éventuel sinistre ;
- s'assurer de l'efficacité des dispositifs de continuité mis en place ;
- prouver la capacité de continuité d'activité vis-à-vis de tiers ;
- promouvoir l'image du PCA auprès de la Direction Générale ;
- former et sensibiliser les acteurs concernés ;
- maintenir le PCA en condition opérationnelle ;
- corriger un point faible identifié lors d'une précédente validation.

La validation du PCA doit être réalisée régulièrement par des tests techniques et des exercices fonctionnels.

Pour valider le caractère opérationnel du PCA, il est nécessaire de réaliser au moins un exercice par an.

Ces différents tests et exercices doivent être suivis, planifiés au travers d'une campagne de validation et ce, sur les quelques années à venir.
Chaque exercice donne lieu à un suivi de la mise à jour du PCA.

En complément des tests, la mise en place d'un programme de revues de plans est nécessaire :

- relecture transverse des documents ;
- utilisation des documents sous forme de « jeu de rôle ».

Les exercices peuvent être :

- préparés (la date est connue de tous les participants) ;
- inopinés (la date est inconnue de la plupart des participants);
- simulés (les processus sont validés sur le site de repli sans impact sur le fonctionnement de l'entreprise) ;
- réels (un ou plusieurs processus sont arrêtés et fonctionnent réellement sur le site de repli).

LE SYSTEME DE MANAGEMENT DE LA CONTINUITÉ D'ACTIVITÉ

> *Le Système de Management de la Continuité d'Activité est un processus de management holistique qui identifie les menaces potentielles pour un organisme 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 améliorer 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 à valeur ajoutée (norme certifiante ISO 22301).*

Un Système de Management de la Continuité d'Activité SMCA intègre les éléments clés suivants :

- une politique ;
- des personnes ayant des responsabilités définies ;
- des processus de management se rapportant à :
  - la politique de continuité d'activité,
  - la planification,
  - la mise en œuvre et le fonctionnement,
  - l'évaluation des performances,
  - la revue de direction,
  - l'amélioration ;
- une documentation fournissant des preuves tangibles ;
- tous les processus du management de la continuité d'activité pertinents pour l'organisation.

La norme certifiante ISO 22301 définit les spécifications du Système de Management de Continuité d'Activité.

LES QUESTIONS SOULEVÉES PAR L'AUDITOIRE

La Continuité des grands services publics

Il existe des plans de continuité d'activité dans les Administrations et dans les services publics. Mais, un PCA reste confidentiel.

Position du Client d'un SaaS (Software as a Service)

Dans cette situation, le Client est en droit de demander, à son fournisseur, une clause contractuelle quant à la continuité de son service.

Mais une telle clause est difficilement négociable auprès des grandes multinationales qui imposent leur contrat.

Une solution peut consister à avoir plusieurs fournisseurs.

Cas des Datacenters

Un Datacenter est une ICPE (Installation Classée pour la Protection de l'Environnement).

Son exploitation doit satisfaire aux normes ISO 14000 (environnement) et 27000 (sécurité).

Pour éviter les catastrophes terrestres, il commence à exister des data centers flottants (à l'abri des inondations...).

La menace d'une nouvelle crue de la Seine

Une crue centennale de la Seine pourrait être catastrophique, étant donné la présence d'infrastructures logistiques en sous-sol…

Il faut noter que les services compétents prévoyaient une crue en hiver, mais aucun n'avait imaginé la crue printanière du mois de juin 2016.

Le coût des mesures préventives

A-t-on chiffré le surcoût du prix de revient d'un produit ou d'un service, inhérent à la superposition de l'application des normes de qualité, de sécurité et de continuité d'activité ?

Il semble qu'on ne dispose d'aucune statistique mais on peut imaginer que le respect de ces normes constitue un véritable avantage concurrentiel, lequel balance l'augmentation du prix de revient.

LE SUJET EST GRAVE ; TERMINONS PAR UN SOURIRE !

70 % des entreprises sinistrées
qui n'avaient pas de PCA
ont déposé leur bilan

Les limites de la redondance

Alain Coulon