GUIDE ADENIUM

PLAN DE CONTINUITE INFORMATIQUE (PCI)

2018

Mettre en œuvre un Plan de Continuité Informatique (PCI)

Adenium SAS
www.adenium.fr
+33 (0)1 40 33 76 88
adenium@adenium.fr

adenium
Think Continuity

Sommaire

Introduction

Le plan de continuité informatique (PCI) est une sous partie du plan de continuité d'activité (PCA), destinée à permettre la reprise du système d'information (SI) lorsque celui-ci est impacté par une situation de crise, sinistre ou défaillance majeure. Le but d'un tel plan est de contribuer à redémarrer l'activité du SI le plus rapidement possible et de minimiser la perte de données, les seuils en matière de temps de reprise et de pertes de données étant fixés au moment de l'analyse réalisée dans le cadre de l'élaboration du PCI, en fonction des besoins de l'entreprise et du budget accordé pour la continuité du SI.

Les entreprises d'aujourd'hui étant de plus en plus dépendantes de leur SI, la sécurisation des moyens informatiques est une démarche importante. Le plan de continuité informatique est l'un des éléments essentiels constituant la politique de sécurité du système d'information, abordé dans les normes ISO 22301, ISO 27001-27002, et détaillé dans la norme ISO 24762.

Ce guide est destiné aux entreprises désirant mettre en place un plan de continuité informatique afin de prévenir l'incapacité d'exploiter régulièrement leurs systèmes d'information face aux risques de :

- Catastrophes Naturelles (inondations, tempêtes…),
- Incendie,
- Actes de malveillances internes ou externes,
- Erreurs ou accidents,
- Risques technologiques et Industriels.

Ce guide, volontairement synthétique, présente les solutions techniques existantes pour la mise en œuvre d'un plan de continuité informatique. Ces solutions prennent en compte chaque élément de la chaîne qui constitue un système d'information, du poste client aux serveurs. Ce guide décrit également la démarche d'élaboration d'un plan de continuité informatique (PCI).

Mettre en œuvre un Plan de Continuité Informatique (PCI)

I. La démarche de mise en œuvre du PCI

1. Le phasage du projet

Le phasage pour la mise en œuvre d'un PCI s'articule en 5 étapes :

- Phase 1 : Initialisation du projet
- Phase 2 : Collecte d'informations auprès des acteurs clés du PCI (Expression des besoins)
- Phase 3 : Élaboration des stratégies de continuité – Elaboration du PCI (Solutions retenues)
- Phase 4 : Mise en œuvre du PCI – (Formalisation, procédures techniques)
- Phase 5 : Tests, formation et maintien en conditions opérationnelles (Amélioration continue)

2. Une démarche au service des utilisateurs

En complément de la démarche PRA (Plan de Reprise d'Activités) habituelle, centrée sur les solutions techniques, la démarche PCI repose avant tout sur l'analyse des besoins utilisateurs en matière de disponibilité du SI. La méthodologie d'analyse et de réduction des risques peut s'appuyer sur une méthode telle que MEHARI. Cette analyse doit permettre :

- d'identifier les activités critiques pour l'entreprise
- d'analyser les impacts qui résulteraient d'un arrêt de ces activités
- d'estimer les besoins en matière de ressources humaines, de bureaux, de postes de travail, et de reprise du SI pour fonctionner en mode dégradé

Cette approche permet d'identifier les mesures nécessaires pour réduire les risques, et dans certains cas, les annuler.

3. Une architecture du SI qui s'adapte aux besoins de l'organisation

Pour chaque élément du SI, deux indicateurs de temps sont définis, permettant ensuite de choisir la solution technique la plus adaptée aux besoins de l'entreprise.

- **Le RTO, Recovery Time Objective**, représente le temps d'arrêt de service que l'on peut tolérer.

- **Le RPO, Recovery Point Objective**, correspond à la quantité de données que l'on juge acceptable de perdre lors de la reprise.

D'une manière générale, plus une solution permet de redémarrer rapidement une activité du SI, tout en minimisant la perte de données, plus elle est coûteuse.

L'analyse des besoins utilisateurs permet de qualifier le niveau de disponibilité requis pour les différentes applications, et d'élaborer les solutions de continuité dont le coût est en adéquation avec les résultats attendus.

Haute Disponibilité	Moyenne Disponibilité	Faible Disponibilité
Reprise immédiate ou quasi-immédiate (quelques minutes). Perte de données très limitée	Secours en quelques heures (moins de 12 heures). Perte de données limitée (quelques minutes à quelques heures).	Secours en 48 heures ou plus. Perte de données en général inférieure à 24 heures.

Dans une démarche PRA centrée sur les solutions techniques, le risque est de mettre en place une architecture inutilement trop coûteuse, ou au contraire, une solution insuffisante pour répondre aux besoins en matière de disponibilité nécessaire à la survie de l'entreprise face à d'une crise majeure.

II. Les solutions de secours à envisager

1. Sites de secours

La mise en place d'un site de secours, dédié ou partagé, est nécessaire pour permettre la reprise du SI après un sinistre sur le site principal. Ce site secondaire peut être plus ou moins éloigné du site principal. Plus les deux sites sont éloignés, moins un sinistre qui affecte le site principal risque de toucher le site secondaire. En revanche, l'éloignement entre les deux sites limite les choix technologiques en matière de transfert de données et augmente les coûts de bande passante. Cet éloignement est pourtant indispensable lorsque que l'on prend en compte des scénarii de sinistres à l'échelle régionale de type « ouragan » ou « inondation ».

Voici les différentes solutions de sites de secours, de la moins coûteuse à la plus coûteuse :

- **Les salles blanches, appelées également « sites froids »**

Il s'agit d'une salle vide, prête à recevoir le matériel informatique en cas de déclenchement du plan de reprise.

- **Les salles oranges, appelées également « sites tièdes »**

Une salle orange est un intermédiaire entre une salle blanche et une salle rouge. Dans une salle orange, seuls les serveurs, dédiés aux applications les plus critiques du SI, sont déjà présents et prêts à fonctionner.

- **Les salles rouges, appelées également « sites chauds »**

Dans le cas d'une salle rouge, tous les équipements nécessaires à la reprise du SI, sont présents et prêts à fonctionner. Par contre, selon les choix technologiques mises en œuvre en matière de sauvegarde et de stockage (sauvegarde à distance, journalisation à distance, ou réplication asynchrone), les données applicatives seront disponibles plus ou moins rapidement en cas de besoin.

- **Les salles miroirs**

Une salle miroir est similaire à une salle rouge, sauf que dans le cas d'une salle miroir, les données applicatives sont disponibles instantanément, grâce à un mécanisme de réplication synchrone. On distingue deux catégories de salles miroirs. Soit la salle miroir est passive et ne traite aucune donnée de production. Elle ne devient active qu'en cas de déclanchement du plan de continuité informatique. Soit elle est pleinement active, et la production est partagée en permanence entre les deux sites.

Le choix technologique, entre ces différents moyens, doit être fait, en fonction de la durée d'indisponibilité tolérée par le SI. Bien entendu, cela peut varier d'une application à une autre, et des choix différents peuvent cohabiter au sein d'un même PCI.

2. Sauvegardes

La présence d'une politique de sauvegarde éprouvée est indispensable à la mise en place d'un plan de continuité informatique. Il faut en effet, avant toute chose, être capable de faire face aux incidents « ordinaires » avant de penser à un plan de secours. Si une telle stratégie n'existe pas dans l'entreprise, c'est le bon moment pour la développer.

Il faut ensuite réaliser des sauvegardes de secours, différentes des sauvegardes de production, dédiées au plan de secours. Ces sauvegardes seront réalisées soit à distance sur le site de secours, soit localement. Dans ce cas les bandes seront externalisées, soit sur le site distant, soit chez un prestataire spécialisé.

On distingue plusieurs modes de sauvegarde :

Les **sauvegardes physiques**, volume par volume, qui ne peuvent être utilisées que si le matériel de destination est identique au matériel d'origine (serveur ou baie de stockage)

Les **sauvegardes logiques**, qui peuvent être complètes, différentielles (sauvegarde des données modifiées depuis la dernière sauvegarde complète) ou incrémentales (la première sauvegarde incrémentale après une sauvegarde complète est une sauvegarde différentielle, les suivantes contiennent les données modifiées depuis la dernière incrémentale), et enfin les **sauvegardes applicatives**, contenant toutes les informations nécessaires au fonctionnement d'une application en particulier.

Certains modes de sauvegardes sont plus ou moins adaptés au PCI. Par exemple la sauvegarde physique n'est pas toujours possible si le matériel sur le site secours n'est pas identique à celui de production. On remarque également que la restauration d'une sauvegarde incrémentale peut nécessiter un grand nombre de supports (la dernière sauvegarde complète et toutes les incrémentales qui ont suivi) ce qui n'est pas idéal dans le cadre d'un PCI. Inversement, les sauvegardes complètes ou applicatives, sont plus longues à effectuer, mais parfaitement adaptées à la mise en œuvre d'un PCI.

3. LAN/WAN/Internet

Tout comme il est nécessaire de secourir les serveurs et leurs données, il faut également prévoir la mise en place d'un LAN de secours pour permettre la communication entre les serveurs et la communication entre les clients et les serveurs. Pour des raisons de simplicité, le secours du LAN, ou d'une sous partie du LAN, peut être assuré par une technologie sans fil de type « Wi-Fi ». Dans ce cas, il est primordial de prendre garde à la sécurité en utilisant un niveau de cryptage efficace (et invulnérable).

Il faut également prévoir un secours des différents liens WAN indispensables au bon fonctionnement du SI, qu'il s'agisse de la communication entre les serveurs et des applications distantes, ou l'interconnexion d'un site utilisateur distant. Dans le cas ou le SI se connecte à un site partenaire protégé par des firewalls, il faut aussi prévoir les ouvertures de flux nécessaires pour le plan d'adressage du site de secours.

Enfin, il est également nécessaire de prévoir le secours des accès Internet, pour assurer les besoins bureautiques (mail, web, …), les besoins du SI, et également pour assurer le secours des sites web liés au SI. Si parmi les solutions de secours pour les utilisateurs, le télétravail fait partie des solutions choisies, il faut également prévoir les infrastructures nécessaires à la connexion à distance (en général un accès VPN). Concernant le re-routage des flux Internet, deux cas de figure peuvent se présenter. Si l'entreprise dispose de son propre AS (Autonomous System) elle peut conserver le même plan d'adressage public sur le site de secours, dans le cas contraire, il faut prévoir une mise à jour DNS.

4. Postes clients

Dans le cas ou le site détruit accueillait des utilisateurs, il faut également prévoir un ou plusieurs moyens pour leur permettre la connexion au SI. Une grande entreprise peut envisager de reloger les utilisateurs du site sinistré sur leurs différents sites non sinistrés. Une plus petite devra se tourner vers la location de bureau. Si cela est possible, le télétravail est également une solution à envisager.

Dans tous les cas de figure, il est important de sensibiliser les utilisateurs, avant même la mise en place du plan, pour éviter qu'ils ne travaillent en local, mais sur des serveurs de fichiers sauvegardés.

5. Téléphonie

La téléphonie fait également partie des éléments à secourir pour assurer la survie du SI. Il existe diverses solutions de secours plus ou moins coûteuses à mettre en place avec un opérateur téléphonique. Il est par exemple possible de re-router à l'identique l'ensemble des numéros du site sinistré vers le site de secours, il est également possible de re-router tous les numéros vers un numéro unique. Si la situation des sites ne permet pas de telles solutions, il est toujours possible que l'opérateur mette en place un message personnalisé indiquant un nouveau numéro d'appel. L'utilisation du GSM n'est pas une solution fiable dans tous les cas. En effet lors d'un sinistre de grande envergure, il est possible que le réseau soit saturé, ou que les antennes soient détruites.

III. Plan de test et évolution du SI

L'efficacité opérationnelle d'un PCI doit être validée par des tests réguliers, au cours d'exercices à plus ou moins grande échelle, du test unitaire au niveau d'un serveur, aux tests en conditions réelles.

Il est conseillé de réaliser des tests unitaires chaque trimestre, et après chaque évolution du SI. Un test global devrait être réalisé une à deux fois par an. Pour minimiser les risques d'un test global, il est possible de réaliser un test « à blanc », c'est-à-dire sans arrêter la production. Bien entendu, un tel test ne permet pas de tester tous les éléments du PCI, comme un re-routage sur Internet. Par contre cela valide la capacité de reproduire l'environnement de production sur le site de secours.

Le bilan établi suite aux tests du PCI permet de valider son efficacité. Il permet également de prendre en compte les changements au sein du SI pour faire évoluer le PCI.

Présentation Adenium

1. Qui sommes-nous ?

Adenium est le spécialiste français indépendant des Plans de Continuité d'Activité (PCA) selon ISO 22301.

Depuis sa création en 2002, Adenium intervient régulièrement auprès des organisations (opérateurs vitaux, grands comptes publics ou privés, PME/ETI) pour déployer leur démarche en Plan de Continuité d'Activité (PCA), secours informatiques (PCI, PCIT, PRA/DRP), et continuité de la Supply Chain (Supply Chain Continuity Management - SCCM).

Partisan dès l'origine de la gestion globale des risques et fort d'un historique de spécialiste en gestion de crise, nous avons été pionniers des PCA et de la discipline Business Continuity en France. A ce titre, Adenium a mis en oeuvre le premier Système de Management de la Continuité d'Activités (SMCA) certifié ISO 22301* en France. Par la suite, Adenium a accompagné avec succès de nombreuses organisations jusqu'à la certification, ce qui a contribué à la reconnaissance des organisations professionnelles (AFNOR, HCFDC, CLUSIF, EuroCloud, INHESJ, AMRAE, CDSE, …) comme étant l'acteur de référence dans le domaine des PCA.

Par ailleurs, Adenium a cofondé le Club 22301 afin de fédérer les utilisateurs de PCA et de favoriser l'adoption de tels dispositifs par les organisations en France. Engagé activement à l'AFNOR, Adenium anime le groupe de travail « Continuité d'Activité et Résilience Organisationnelle » au sein de la commission de normalisation.

Soucieux de partager ses connaissances avec le plus grand nombre, Adenium est également le cofondateur du Master 2 RPCA et Gestion de Crise de l'Université Paris 13 sous le haut patronage du SGDSN.

Aujourd'hui nos équipes de consultants dédiées à 100% à la continuité d'activité, tous certifiés Lead Implementer ISO 22301, vous accompagnent dans la mise en oeuvre de votre Système de Management de la Continuité d'Activité (SMCA).

Les atouts d'Adenium sont ses compétences, son professionnalisme et le sens de l'engagement de ses équipes.

Adenium est une Société par Actions Simplifiée (SAS) au Capital de 150 000 Euros dont le siège social est basé à Paris. Adenium est également implanté à Lyon.

2. Notre valeur ajoutée

Respectueux des cadres normatifs, notre longue expérience en gestion des risques permet de garantir une approche opérationnelle et d'obtenir des résultats.

De taille humaine, la structure d'Adenium regroupe des spécialistes qui vous apporteront des services et conseils personnalisés en adéquation avec votre culture d'entreprise et votre appétence au risque.

Notre flexibilité et notre sens de l'écoute assurent un service de proximité et une véritable relation de confiance entre notre cabinet et nos clients.

3. Contacts utiles

Notre équipe se tient à votre disposition pour vous renseigner :

ADENIUM

Paris :
Siège social : 10, rue Emile Landrin - 75020 Paris
Téléphone : 01 40 33 76 88
Télécopie : 01 40 33 76 67
Email : adenium@adenium.fr
Web : www.adenium.fr

Lyon :
Adresse : 33, rue Saint-Maximin – 69003 Lyon
Téléphone : +33 (0)9 82 58 85 22