Avenue des Facultés
80000 Amiens

Plan de Continuité d'Activité(PCA)

SAE Semestre 5

Liam TARGET, Justin LARGILLIÈRE Malcolm WALTER, Lucas GONTHIER, Lorenzo VATRIN, Victor DA SILVA LOURENCO MARQUES.

BUT3 Informatique
Tous parcours

Année 2024 - 2025

Plan de Continuité d’Activité(PCA) v1.1

Un **Plan de Continuité d’Activité (PCA)** est un ensemble de procédures et de stratégies qu’une organisation met en place pour garantir la continuité de ses activités essentielles en cas d’incident majeur ou de crise. L'objectif principal du PCA est d'assurer que l'organisation puisse fonctionner même en situation de perturbation grave, en minimisant les impacts sur ses services, ses opérations et sa réputation.

Précautions :

- **Analyse d'impact sur l'activité** :
  Il est essentiel d'identifier les activités critiques et d’évaluer les impacts potentiels des interruptions sur ces activités. Cela permet de définir les priorités en cas de crise, en déterminant quelles fonctions doivent être rétablies en premier pour limiter les perturbations.

- **Évaluation des risques** :
  L'organisation doit identifier les risques susceptibles d'affecter ses opérations, comme les cyberattaques, les catastrophes naturelles, les pannes de systèmes, etc. Il est crucial d’analyser la probabilité et l'impact de chaque risque sur les activités de l'entreprise afin de mieux se préparer à y faire face.

- **Mises en situation** :
  Il est recommandé d’effectuer des simulations de conditions réelles, telles que des catastrophes naturelles, des coupures d’électricité, des intrusions dans les locaux ou des attaques sur le système de sécurité. Ces tests permettent de vérifier l'efficacité des mesures mises en place et de former le personnel à réagir correctement en situation de crise.

Le PCA est conçu pour **maintenir l'activité en cas de problème majeur**, en garantissant la continuité des services essentiels et en limitant les impacts sur l'entreprise. Toutefois, en cas de problème d'une ampleur trop importante, le **Plan de Reprise d'Activité (PRA)** prend le relais pour assurer la récupération complète des services et la reprise des opérations.

Le but de la manœuvre **est que personne ne remarque le problème**. Si cela est inévitable, il faut choisir entre garder un gros client ou tous les plus petits. Il est important d'être **prêt à toutes les éventualités** pour maintenir le service actif, tout en prenant d'autres précautions en fonction des moyens employés.

Marche à suivre pour certaines situation grave :

- Démission d'un développeur, impact sur les corrections de bugs et fragilisation du reste de l'équipe :
    - Identifier immédiatement les tâches critiques en cours et la répartition du travail.
    - Déplacer un développeur d'un autre projet (si possible) pour prendre en charge les corrections urgentes.
    - Prioriser les corrections de bugs majeurs qui peuvent entraîner des failles de sécurité ou des dysfonctionnements graves.
    - Ralentir la production d'autres fonctionnalités si nécessaire pour se concentrer sur la correction des bugs critiques.
    - Revoir la répartition des tâches dans l'équipe pour que l'activité continue sans compromettre la qualité.
    - Mettre en place un suivi renforcé pour garantir que les corrections de bugs soient traitées rapidement.

- Imprévu : Serveurs HS, perturbation de l'aspect financier, du marché et des utilisateurs :
    - Prévoir des solutions de secours (serveurs externes ou cloud) pour réduire l'impact sur les revenus et maintenir la continuité de service.
    - Louer temporairement des serveurs externes si la panne affecte des services essentiels.
    - Prioriser certains services essentiels, en réduisant temporairement la capacité de services moins critiques pour minimiser les pertes financières.
    - Communiquer avec les utilisateurs pour les tenir informés des interruptions ou ralentissements éventuels.
    - Mettre en place un plan de communication clair et régulier pour maintenir la transparence et gérer les attentes des clients.
    - Effectuer des tests pour vérifier la stabilité des services sur les serveurs externes avant la mise en production.

- Bugs et défaillance du système, alerte de sécurité :
    - Prévenir immédiatement tous les services concernés par l'incident.
    - Vérifier si des vulnérabilités de sécurité ont été exploitées.
    - Appliquer des mesures de sécurité supplémentaires pour protéger les données sensibles et éviter d'autres failles.
    - Identifier précisément la source du problème et l'étendue de la défaillance.
    - Si l'incident est grave, envisager de mettre en œuvre un **Plan de Reprise d'Activité (PRA)**. Sinon, tenter de résoudre le problème en parallèle sans interrompre les services essentiels.
    - Tester les solutions mises en place pour résoudre la défaillance.
    - Si la solution parallèle ne fonctionne pas, rediriger les services vers des ressources de secours (par exemple, un serveur de secours ou une solution cloud).
    - Relancer les services après avoir vérifié la stabilité du système.

- Effectuer des tests supplémentaires pour s'assurer que tout fonctionne normalement avant de remettre l'ensemble des services en production.

Autres mesures de précaution :

- Mettre en place des sauvegardes régulières et des solutions de reprise rapide pour éviter de perdre des données critiques.
- Effectuer des simulations régulières pour tester le PCA et évaluer la réaction de l'équipe face à des scénarios de crise.
- Former l’ensemble du personnel aux procédures d’urgence et à la gestion des incidents afin qu’ils puissent réagir efficacement en cas de problème.
- Maintenir une communication claire et cohérente à travers tous les niveaux de l'organisation pour assurer une gestion efficace des crises.