CONTINUITÉ D'ACTIVITÉ INFORMATIQUE

Les clés pour anticiper les interruptions et renforcer la résilience de votre PME

CELESTE

La transformation numérique a profondément modifié le fonctionnement des entreprises. Applications métiers, données, outils collaboratifs, infrastructures Cloud... le système d'information est désormais indispensable à la continuité des activités. Pourtant, de nombreuses PME ne disposent pas encore d'une véritable stratégie de continuité d'activité informatique pour faire face à une interruption, qu'elle soit provoquée par une cyberattaque, une panne matérielle, une erreur humaine ou un incident technique.

Assurer la continuité d'activité informatique ne consiste plus uniquement à protéger ses données : il s'agit de garantir la disponibilité des services essentiels, de limiter les impacts sur l'activité et de permettre une reprise rapide en cas d'incident. À travers ce guide, découvrez les enjeux, les bonnes pratiques et les solutions qui permettent de renforcer durablement la résilience de votre entreprise.

Sommaire

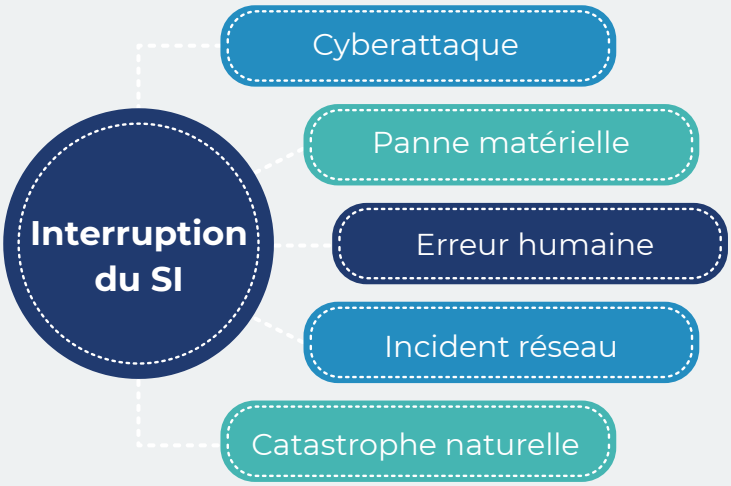
1. Pourquoi la continuité est essentielle 03
2. Les impacts d'une interruption 04
3. Comprendre le PRA et le PCA 05
4. Les 5 bonnes pratiques 06
5. Construire une stratégie adaptée 07
6. Êtes-vous prêt à faire face à un incident ? 08

1 Pourquoi la continuité d'activité informatique est essentielle

Le système d'information est aujourd'hui au cœur des activités des PME. Une interruption, qu'elle soit liée à une cyberattaque, une panne matérielle ou une erreur humaine, peut rapidement perturber les opérations, ralentir les équipes et impacter les clients.

Assurer la **continuité d'activité informatique** permet d'anticiper ces situations, de limiter leurs conséquences et d'assurer une reprise rapide des services essentiels grâce à un **plan de continuité d'activité (PCA)** et un **plan de reprise d'activité (PRA)** adaptés aux besoins de l'entreprise.

Les principales causes d'une interruption



Le saviez vous ?

Un incident informatique n'entraîne pas forcément une perte de données.

En revanche, il peut rendre vos applications et vos services indisponibles, avec des conséquences directes sur votre activité.

Les PME sont confrontées à de nouveaux questionnements, notamment sur la conduite à tenir en cas d'interruption. Elles n'ont pas nécessairement la même maturité que les grandes entreprises concernant le PRA ou le PCA, l'apport de ceux-ci mais aussi leurs modalités.

Terry Weber
Ingénieur commercial

2 *Une interruption informatique ne s'arrête pas à votre infrastructure*

Lorsqu'un système d'information devient indisponible, les conséquences dépassent largement le cadre informatique. Les collaborateurs ne peuvent plus accéder à leurs outils, les échanges avec les clients sont ralentis et certaines activités peuvent être totalement interrompues.

Plus l'interruption dure, plus les impacts sur l'entreprise sont importants.

Domaine impacté	Conséquence
Production	Activité ralentie ou arrêtée
Collaborateurs	Perte d'accès aux applications
Clients	Retards, indisponibilité des services
Finances	Perte de chiffre d'affaires
Image	Perte de confiance

⚠️ Les erreurs les plus fréquentes

- ❌ Penser que les sauvegardes suffisent.
- ❌ Ne jamais tester son PRA.
- ❌ Sous-estimer les délais de reprise.
- ❌ Ne pas identifier les applications critiques.

À retenir

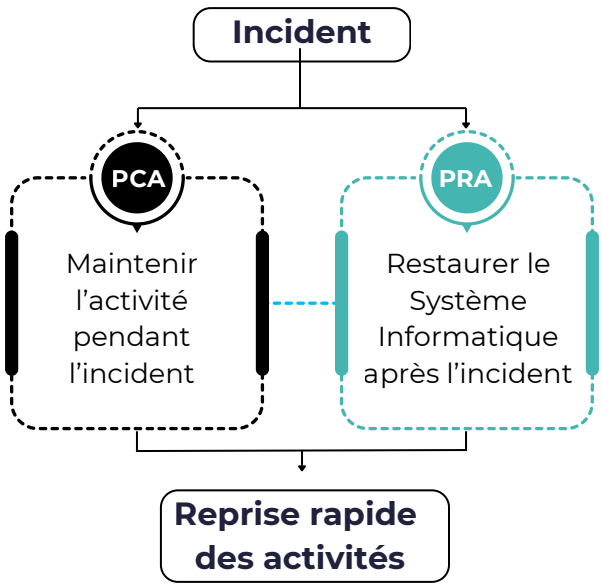
Une interruption, même de courte durée, peut avoir des conséquences durables sur l'activité si aucune stratégie de continuité n'a été anticipée.

3 PRA et PCA : deux approches complémentaires

Le **Plan de Continuité d'Activité (PCA)** permet de maintenir les services essentiels pendant un incident. Le **Plan de Reprise d'Activité (PRA),** véritable stratégie de reprise après sinistre, permet de restaurer le système d'information dans les meilleurs délais.

Ces deux dispositifs poursuivent un même objectif : limiter les conséquences d'une interruption et assurer la continuité des activités de l'entreprise.

Le **PCA** et le **PRA** constituent deux piliers complémentaires d'une stratégie de **continuité d'activité informatique.**



Bon à savoir

Toutes les entreprises n'ont pas besoin du même niveau de reprise.

Selon les enjeux métiers, il est possible de protéger uniquement les applications et les données les plus critiques afin d'adapter les coûts et les délais de reprise.

➤ **Découvrir le PRA & PCA CELESTE**

Nous pouvons fournir des PRA dormants ou ne dupliquer qu'une partie de l'environnement. C'est aussi notre rôle de proposer des solutions au plus près des besoins vitaux d'un client.

Terry Weber
Ingénieur commercial

4 5 bonnes pratiques pour renforcer votre résilience informatique

Mettre en place une stratégie de continuité d'activité informatique ne consiste pas uniquement à investir dans des technologies. Elle repose sur une démarche progressive, adaptée aux besoins de chaque entreprise

Les 5 étapes clés

1. Identifier les applications critiques
2. Définir les priorités de reprise
3. Sécuriser les sauvegardes
4. Tester régulièrement les procédures
5. Mettre à jour le plan en continu

Le bon réflexe

Ne construisez pas votre stratégie uniquement autour de la technologie. Identifiez d'abord les **activités essentielles** de votre entreprise, puis définissez les niveaux de protection adaptés à chacune.

Les éléments à définir avant de construire son PRA

1. Applications critiques
2. Durée Maximale d'Interruption Admissible (DMIA)
3. Données prioritaires
4. Responsables en cas d'incident
5. Procédures de test

5 Une stratégie adaptée à chaque entreprise

Chaque entreprise possède ses propres contraintes, son infrastructure et ses objectifs. C'est pourquoi une stratégie de continuité d'activité doit être construite à partir des besoins réels de l'entreprise et de ses applications critiques.

L'objectif est d'identifier les ressources essentielles, de définir les délais de reprise attendus et de mettre en place une solution évolutive.

Parcours d'accompagnement

- Audit
- Analyse des risques
- Définition de la stratégie
- Déploiement
- Tests
- Amélioration continue

Une approche adaptée à chaque PME

Aucune PME ne présente les mêmes enjeux en matière de continuité d'activité informatique. Chaque organisation doit prendre en compte :

- ✔ ses applications métiers
- ✔ ses exigences de disponibilité
- ✔ ses objectifs de reprise
- ✔ ses ressources critiques

Une stratégie de continuité efficace doit donc être construite sur mesure.

"C'est de ce travail d'écoute et d'audit que découlera l'offre que fournira CELESTE. Cette conversation se poursuivra bien sûr à chaque étape, jusqu'à la mise en production et même au-delà.

Terry Weber
Ingénieur commercial

6 *Êtes-vous prêt à faire face à un incident ?*

Les 5 questions à vous poser dès aujourd'hui

1. Avez-vous identifié vos applications les plus critiques ?
2. Savez-vous combien de temps votre activité peut fonctionner sans votre système d'information ?
3. Vos sauvegardes sont-elles régulièrement testées ?
4. Vos équipes connaissent-elles les procédures à suivre en cas d'incident ?
5. Votre stratégie de continuité d'activité est-elle toujours adaptée à votre entreprise ?

Conclusion

La continuité d'activité informatique ne consiste pas uniquement à réagir lorsqu'un incident survient. Elle permet d'anticiper les risques, de protéger les activités essentielles de votre entreprise et d'assurer une reprise rapide lorsque chaque minute compte.

Anticiper aujourd'hui, c'est permettre à votre entreprise de poursuivre sereinement ses activités demain, quelles que soient les circonstances.

Chaque entreprise est différente.
Votre stratégie de continuité doit l'être aussi.

Contactez-nous

info@celeste.fr

www.celeste.fr