LE GUIDE POUR LES TPE/PME

Assurez la continuité de votre activité



Hexatel

SOMMAIRE

Assurez la continuité de votre activité

01 Pourquoi la continuité d'activité est un enjeu vital pour les entreprise ? *p3*

02 Identifier les 3 risques qui menacent votre activité *p4*

03 PRA/PCA : comprendre les différences pour mieux se protéger *p6*

04 Les bonnes pratiques pour maintenir votre activité *p7*

05 Construire un plan de continuité d'activité *p9*

06 Anticiper la reprise après un incident (PRA) *p10*

07 Faites appel à un prestataire externe *p11*

POURQUOI LA CONTINUITÉ D'ACTIVITÉ EST UN ENJEU VITAL ?

La continuité d'activité est un enjeu vital pour toute entreprise, quelle que soit sa taille, car elle conditionne directement sa capacité à rester opérationnelle face à l'imprévu. Une panne informatique, une cyberattaque, une coupure réseau ou un sinistre matériel peuvent suffire à interrompre brutalement votre production, vos échanges commerciaux ou votre service client.

Pour une TPE ou une PME, ces interruptions se traduisent rapidement par des pertes financières, une baisse de productivité et parfois une atteinte durable à la réputation. Dans un contexte économique où chaque heure compte, anticiper ces situations n'est plus une option, c'est devenu une nécessité stratégique.

Mettre en place un plan de continuité d'activité permet de garantir la résilience de son entreprise, de protéger ses données, ses collaborateurs et ses clients, et d'assurer la pérennité de son activité, même en cas de crise.

> ***“Plus de la moitié des décideurs informatiques déclarent avoir subi au moins 4 pannes réseau de plus de 30 minutes au cours des 12 derniers mois. Parmi elles, 39% des pannes réseaux mettent plus d'une journée à être corrigées.”***

Une panne de réseau à des impacts importants, elle provoque :

des pertes de données	une insatisfaction client	un impact sur la réputation de l'entreprise
40%	36%	28%

Sources : l'usine digitale, Cybermalveillance.gouv, Opengear

pourtant...

80% des PME reconnaissent ne pas être préparées aux cyberattaques

68% investissent moins de 2 000 € par an en cybersécurité

IDENTIFIER LES RISQUES QUI MENACENT VOTRE ACTIVITÉ

01 Risques techniques

Les risques techniques regroupent l'ensemble des défaillances liées à vos infrastructures informatiques, réseaux, équipements et systèmes numériques. Ils constituent la première cause d'interruption d'activité pour une TPE/PME.

Les potentiels risques :

- Pannes matérielles
- Défaillances logicielles
- Problèmes de connectivité
- Cyberattaques
- Absences de sauvegarde

Quels impacts ? Une panne technique peut entrainer des pertes de productivité et un risque de perte de données. Sans plan de continuité, la reprise peut prendre plusieurs jours, voire semaines, selon la gravité de l'incident.

02 Risques humains

Le facteur humain représente une dimension souvent sous-estimée du risque d'interruption de service. Il regroupe à la fois les erreurs involontaires, les comportements inadaptés et les absences qui perturbent la continuité du fonctionnement de votre activité.

Les potentiels risques :

- Erreur de manipulation
- Manque de formation ou de sensibilisation
- Dépendance à une personne clé
- Acte de malveillance interne

Quels impacts ? Les erreurs humaines peuvent provoquer des interruptions de service, des pertes de données sensibles ou un non-respect des obligations légales (RGPD, sécurité des systèmes). Elles créent également un stress organisationnel : absence de coordination, perte de repères et difficultés à rétablir une situation normale.

03 Risques externes

Les risques externes proviennent d'événements sur lesquels l'entreprise n'a pas ou peu de contrôle. Ils sont souvent imprévisibles et peuvent impacter simultanément plusieurs maillons de la chaîne d'activité.

Les potentiels risques :

- Catastrophes naturelles ou sinistres physiques
- Crises sanitaires ou sociales
- Dépendance à des prestataires ou fournisseurs
- Coupures d'énergie ou de réseau étendues
- Cybermenaces globales

Quels risques ? Ces événements peuvent provoquer un arrêt total ou partiel de l'activité, un isolement opérationnel, une perte de communication interne/externe et des retards importants dans les livraisons ou le service client.

PRA/PCA : COMPRENDRE LES DIFFÉRENCES POUR MIEUX SE PROTÉGER

Dans une démarche de continuité d'activité, deux notions sont souvent évoquées : le Plan de Continuité d'Activité (PCA) et le Plan de Reprise d'Activité (PRA). Bien qu'ils soient complémentaires, ils répondent à des objectifs différents.

Le PCA vise à maintenir l'activité de l'entreprise pendant une perturbation, tandis que le PRA intervient après un sinistre pour restaurer les systèmes et les opérations. Bien comprendre leur rôle respectif est essentiel pour construire une stratégie de résilience efficace. C'est la combinaison des deux dispositifs qui permet d'avoir une continuitéd'activité efficace.

Critère	PCA (plan de continuité d'activité)	PRA (plan de reprise d'activité)
Objectif	Assurer la continuité de l'activité en cas d'incident	Restaurer les systèmes après un sinistre
Temporalité	Pendant la crise	Après la crise
Approche	Préventive et organisationnelle	Curative et technique
Périmètre	Processus métiers, organisation, ressources humaines	Systèmes informatiques, données, infrastructures
Exemples d'actions	Télétravail, redéploiement des équipes, procédures dégradées	Restauration des sauvegardes, redémarrage des serveurs
Enjeu principal	Limiter l'impact sur l'activité	Réduire le temps d'indisponibilité (RTO) et la perte de données (RPO)

LES BONNES PRATIQUES POUR MAINTENIR VOTRE ACTIVITÉ

Mettre en place des solutions techniques est essentiel, mais la résilience d'une entreprise repose avant tout sur la rigueur et la régularité dans le respect des bonnes pratiques internes. En adoptant des gestes simples et des réflexes collectifs, une TPE/PME peut réduire de manière significative les risques et limiter les impacts d'une panne, d'une attaque ou d'un sinistre.



METTRE À JOUR VOS LOGICIELS ET SYSTÈMES

Les mises à jour ne sont pas qu'une question de confort, elles corrigent des failles de sécurité connues. Il est donc recommandé de **planifier des créneaux** réguliers de maintenance et **d'activer les mises à jour automatiques** lorsque cela est possible. Un poste non à jour peut devenir le point d'entrée d'un ransomware ou provoquer des incompatibilités techniques critiques.

SENSIBILISER VOS ÉQUIPES

Les collaborateurs représentent la première entrée face aux menaces numériques. Une simple erreur peut compromettre l'ensemble du réseau. Organiser des sessions de **sensibilisation régulières** permet d'ancrer les bons réflexes : reconnaître un mail suspect, sécuriser ses mots de passe, verrouiller son poste, ou encore signaler rapidement un incident. Une culture numérique partagée est le socle d'une continuité d'activité maîtrisée.





PLANIFIER ET VÉRIFIER VOS SAUVEGARDES

Une sauvegarde n'a de valeur que si elle fonctionne au moment critique. Il est indispensable de définir une **politique de sauvegarde claire** (fréquence, durée de conservation, type de données concernées) et de **vérifier régulièrement la restauration effective des fichiers.** Les sauvegardes doivent être externalisées pour garantir la récupération des données même en cas de sinistre physique dans vos locaux.

DOCUMENTER VOS PROCÉDURES INTERNES

Une procédure documentée doit décrire les étapes à suivre, les contacts à mobiliser, les accès nécessaires et les délais de reprise attendus. Cette documentation, accessible à tous les responsables clés, **évite les pertes de temps et les mauvaises décisions** dans un moment de stress. L'objectif est que chaque collaborateur sache exactement quoi faire pour contribuer à une reprise rapide de l'activité.





TESTER RÉGULIÈREMENT VOS SCÉNARIOS

Organiser des exercices de simulation (coupure réseau, défaillance serveur, indisponibilité d'un poste clé…) permet d'évaluer la réactivité de vos équipes et de repérer les points faibles du dispositif. Ces tests sont aussi l'occasion **d'ajuster vos procédures, d'actualiser les contacts ou de mettre à jour vos outils.** Une entreprise entraînée réagit plus vite et limite les pertes économiques et opérationnelles.

CONSTRUIRE UN PLAN DE CONTINUITÉ D'ACTIVITÉ

1 ANALYSE DES RISQUES

Identifiez les risques potentiels auxquels sont soumis votre organisation (panne, cyberattaque...) Vous devrez, pour cela, procéder à une analyse rigoureuse de votre environnement interne et externe. A l'issue de cette démarche, vous connaîtrez les processus à maintenir en fonctionnement.

2 ÉVALUATION DES IMPACTS

Analysez les conséquences financières, opérationnelles, et en termes de réputation en cas d'interruption de vos processus critiques. Définissez les durées d'indisponibilité acceptables pour chaque activité essentielle et priorisez les mesures à prendre.

3 DÉFINITION DES STRATÉGIES DE CONTINUITÉ

Prévoyez des solutions de secours adaptées à chaque risque (plans de redondance, externalisation, solutions cloud...). L'objectif et de garantir au maximum la continuité des services tout en tenant compte des ressources disponibles.

4 CRÉATION DU PLAN DÉTAILLÉ

Rédigez votre plan de continuité d'activité en définissant les actions concrètes à suivre en cas d'incident, les équipes responsables et les délais de mise en œuvre (RTO, RPO). La documentation doit être facilement accessible en cas de besoin et compréhensible.

5 FORMATION ET SENSIBILISATION DES ÉQUIPES

Formez les collaborateurs aux procédures à suivre en cas d'incident. Ils seront ainsi prêt à réagir efficacement en cas de déclenchement du plan de continuité d'activité.

6 TEST ET MISES À JOUR RÉGULIÈRES

Tester régulièrement votre plan de continuité d'activité a travers des simulations. Si besoin, adaptez le en fonction de vos retours d'expérience, de l'évolution des risques et des changements dans l'entreprise.

ANTICIPER LA REPRISE APRÈS UN INCIDENT (PRA)

Si le Plan de Continuité d'Activité permet de maintenir l'entreprise en fonctionnement en situation dégradée, le Plan de Reprise d'Activité (PRA) intervient lorsque l'incident a provoqué une interruption totale ou partielle des systèmes.

Son objectif est clair : remettre en service les infrastructures informatiques et les données critiques dans les meilleurs délais, afin de permettre à l'entreprise de reprendre une activité normale.

01 Les composants clés d'un PRA

Un Plan de Reprise d'Activité efficace repose sur plusieurs éléments essentiels :

- **Analyse des risques : i**dentification des menaces potentielles et de leur impact
- **Priorisation des systèmes :** définition des applications et données critiques
- **Objectifs de reprise :**
  - RTO (Recovery Time Objective) : durée maximale d'interruption acceptable
  - RPO (Recovery Point Objective) : perte de données maximale acceptable
- **Solutions de sauvegarde :** backups réguliers, externalisés et testés
- **Infrastructure de secours :** site de repli, cloud ou datacenter secondaire
- **Procédures documentées :** étapes précises pour restaurer les systèmes
- **Tests réguliers :** simulations pour valider l'efficacité du plan

02 Les grandes étapes d'un PRA

1. **Détection de l'incident**
2. **Activation du PRA** (cellule de crise, décision de bascule)
3. **Restauration** des données (à partir des sauvegardes)
4. **Redémarrage** des systèmes sur une infrastructure de secours
5. **Vérification et reprise** progressive de l'activité

FAITES APPEL À UN PRESTATAIRE EXTERNE

Beaucoup de TPE et PME gèrent seules la continuité de leur activité faute de moyens ou par méconnaissance des risques. Elles estiment souvent qu'un arrêt complet de leur système est peu probable ou qu'un prestataire spécialisé représenterait un coût trop important. Pourtant, **les incidents sont fréquents** : panne serveur, cyberattaque, coupure réseau, erreur humaine ou sinistre matériel peuvent à tout moment bloquer la production, les ventes ou le service client.

En réalité, **aucune entreprise n'est à l'abri**. Les conséquences d'un arrêt d'activité peuvent être lourdes : perte de chiffre d'affaires, retards de livraison, mécontentement des clients, voire atteinte durable à la réputation.

Faire appel à un prestataire spécialisé permet d'**anticiper ces situations** et de mettre en place des solutions fiables, testées et adaptées à la taille de votre structure. C'est bénéficier d'un accompagnement expert pour analyser vos risques, concevoir un plan de continuité sur mesure et garantir une reprise rapide en cas d'incident. Au-delà de la sécurité technique, c'est un investissement dans la pérennité, la sérénité et la crédibilité de votre entreprise.

6 raisons de mettre en place une solution de continuité d'activité

- Protéger la pérennité de votre entreprise
- Préserver vos données et votre savoir-faire
- Maintenir la confiance de vos clients et partenaires
- Réduire l'impact financier des interruptions
- Gagner en sérénité et en réactivité
- Bénéficier d'une expertise technique complète

Hexatel

Un projet ? Une question ?

Nos équipes sont là pour vous accompagner à chaque étape de vos projets télécoms, réseaux et informatiques.

Contactez-nous sur notre site internet