sonio.

La continuité des activités n‘est pas un projet informatique.

C‘est une stratégie de survie

La continuité des activités n'est pas un projet informatique.

C'est une stratégie de survie – et la plupart des entreprises s'y risquent au petit bonheur la chance.

Les catastrophes naturelles, les cyberattaques ou une malheureuse succession de problèmes techniques peuvent aujourd'hui paralyser une entreprise en un clin d'œil. Cela se vérifie très concrètement en Suisse : lors des inondations dans le Valais en 2024, les systèmes d'une trentaine de communes ont été perturbés après l'inondation d'un prestataire informatique. Et les attaques par ransomware ont entraîné à plusieurs reprises de graves pannes ces dernières années.

La plupart des incidents ne sont jamais rendus publics. Plus de 100 cas de ransomware ont été signalés chaque année au BACS (Office fédéral de la cybersécurité) ces dernières années. Toutefois, l'office estime lui-même que le nombre réel de cas non signalés est nettement plus élevé. La pratique ne fait que le confirmer : rares sont les entreprises qui n'ont pas encore été confrontées à une attaque de phishing réussie, à un incident lié à un logiciel malveillant ou à un incident de sécurité majeur.

RÉSUMÉ

Les cyberattaques, les catastrophes naturelles et les pannes techniques peuvent aujourd'hui paralyser une entreprise en quelques heures. De nombreuses organisations pensent qu'une sauvegarde suffit pour être préparées. La réalité est tout autre : une sauvegarde seule ne constitue pas un plan.

Ce livre blanc montre pourquoi la continuité des activités est un enjeu global qui va bien au-delà de la simple sauvegarde des données. L'interaction entre la reprise après sinistre, la cyber-résilience, des plans d'urgence clairs et un ancrage organisationnel est déterminante. Nous analysons les faiblesses typiques observées dans la pratique, mettons en évidence les principales lacunes et expliquons quelle approche structurée permet aux entreprises d'être réellement préparées.

Sonio accompagne les entreprises dans cette démarche – en tant que partenaire d'architecture et de mise en œuvre pour l'infrastructure informatique. Non pas en tant que fournisseur de produits, mais en tant que partenaire qui sait où il faut agir.

Et pourtant, de nombreuses entreprises ne sont pas préparées. Ceux qui utilisent une solution de sauvegarde se considèrent souvent comme suffisamment protégés. Cette erreur d'appréciation peut vous coûter cher.

Le malentendu : la sauvegarde n'est pas la continuité des activités

Lors de nos entretiens avec les responsables informatiques et les directions, nous sommes régulièrement confrontés à la même situation de départ : le service informatique a investi dans la sauvegarde, dispose peut-être même un site de reprise après sinistre dans un autre centre de données, et pourtant, en cas d'urgence, des conditions essentielles font défaut.

> De nombreuses entreprises ont sauvegardé leurs données, mais n'ont aucun plan pour réellement relancer leurs activités.

Pourquoi ?

Parce que ces sites de reprise après sinistre présentent souvent l'une des deux faiblesses suivantes. Soit ils sont utilisés en production au quotidien et sont donc également touchés en cas d'urgence. Soit ils constituent bien un site de sauvegarde, mais ne disposent pas des ressources nécessaires – à savoir des composants réseau, des serveurs et du stockage – pour une restauration complète. D'après notre expérience, nous pouvons le confirmer : les enquêtes menées après un cyber incident bloquent souvent les infrastructures pendant plusieurs jours. Pendant ce temps, même si une sauvegarde existe, aucune restauration n'est possible, car la plateforme nécessaire à cet effet n'est tout simplement pas disponible. Il ne s'agit malheureusement pas d'un cas isolé, mais plutôt de la règle.

Trois problèmes structurels

D'après notre expérience et les entretiens menés, trois schémas récurrents se dégagent, que nous parlions d'une PME ou d'une grande entreprise industrielle :

- **Manque de transparence sur les risques :** de nombreuses entreprises ne savent pas ce que coûte réellement une panne. Sans ce chiffre, toute déci-sion d'investissement dans le domaine de la continuité des activités revient à avancer à l'aveuglette.
- **Manque de sensibilisation au niveau de la direction :** la continuité des activités est considérée comme un sujet informatique. Le fait qu'il s'agisse d'une mission de direction qui doit être définie par l'entreprise n'a pas encore été compris dans de nombreuses entreprises.
- **Technologie sans stratégie :** des solutions sont acquises sans que le RTO (Recovery Time Objective) et le RPO (Recovery Point Objective) aient été coordonnés avec l'entreprise. L'infrastructure existe, mais elle ne correspond pas aux exigences réelles.

La réalité a changé.

Votre plan de continuité des activités y est-il préparé ?

La continuité des activités n'est pas un sujet nouveau. Cependant, le contexte a fondamentalement changé ces dernières années. Ce qui était autrefois considéré comme un risque théorique est aujourd'hui une réalité opérationnelle.

Le paysage des menaces s'est transformé

Il y a quelques années encore, les ransomwares étaient un phénomène marginal. Aujourd'hui, ils sont devenus la forme la plus courante de panne informatique grave. Les attaquants sont organisés de manière professionnelle, leurs connaissances sont échangées sur des plateformes spécialisées – et grâce à l'intelligence artificielle, les modèles d'attaque peuvent être développés et optimisés plus rapidement que jamais.

> La question n'est plus de savoir si une entreprise sera touchée, mais quand et dans quelle mesure elle y est préparée.

Ceux qui pensent encore aujourd'hui « cela ne nous arrivera pas » ferment les yeux sur la réalité. Dans le même temps, la complexité des infrastructures informatiques augmente. Les environnements hybrides comprenant des charges de travail dans le cloud, des applications SaaS, des systèmes sur site et des infrastructures OT créent de nouveaux vecteurs d'attaque. Une stratégie de sauvegarde conçue pour les environnements sur site classiques n'est tout simplement plus efficace dans le monde actuel.

Le poids économique des pannes

Que coûte réellement une panne ? Trop peu de gens se posent cette question – et c'est précisément là le problème.

Des projets concrets nous fournissent des chiffres qui nous ouvrent les yeux : une entreprise manufacturière peut subir des pertes quotidiennes de 200 000 francs suisses ou plus en cas de panne informatique totale, en raison de l'arrêt de la production, de l'impossibilité de livrer, de la perte de réputation et des pénalités contractuelles. Quiconque connaît ce chiffre relativise immédiatement le coût d'une stratégie de continuité des activités.

EXEMPLE DE CALCUL PRATIQUE

Une entreprise de 250 collaborateurs qui subit un préjudice quotidien de 200 000 CHF en cas de panne informatique :

Une semaine d'indisponibilité :	1,4 million de CHF
Deux semaines :	2,8 millions de CHF

L'investissement dans une solution BC complète ne représente généralement qu'une fraction de ce montant.

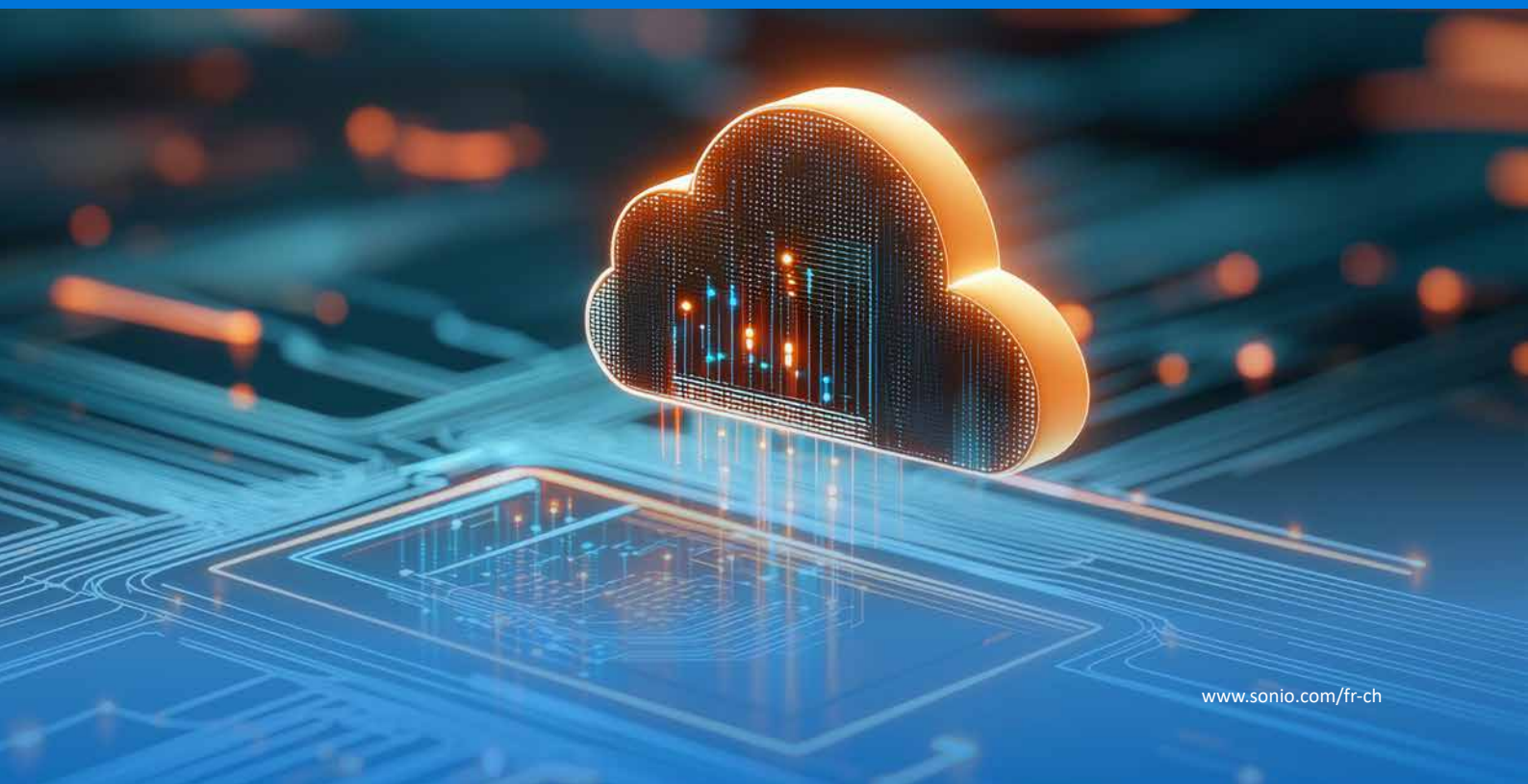
La sauvegarde est importante.

Même la meilleure sauvegarde ne sert à rien si l‘activité s‘arrête quand même.

Lorsque nous discutons de continuité des activités avec les entreprises, une observation revient presque systématiquement : la discussion commence par la sauvegarde et s’y termine souvent. C’est compréhensible, car la sauvegarde est l’élément le plus visible et le plus concret. Mais ce n’est qu’une partie d’un concept complexe.

La continuité des activités signifie : la capacité d‘une entreprise à reprendre ses activités le plus rapidement possible après un événement inattendu et surtout indésirable – qu‘il s‘agisse d‘une cyberattaque, une catastrophe physique ou une erreur humaine – de reprendre ses activités le plus rapidement possible. Cela nécessite bien plus que de simples copies de données. Cela nécessite une stratégie, une architecture, une organisation et une formation régulière.

> La sauvegarde protège les données. La continuité des activités protège l‘entreprise.



LES QUATRE ATOUTS D'UNE STRATÉGIE DE CONTINUITÉ DES ACTIVITÉS SOLIDE

L'AS – Une sauvegarde robuste
La sauvegarde constitue la base. Il ne s'agit pas seulement de sauvegarder les données, mais d'être résilient face à deux scénarios : premièrement, la défaillance physique ou la destruction de composants matériels ; deuxièmement, les attaques contre les données par le biais du chiffrement, de la compromission ou de la destruction. L'atout est important. Mais il ne fait pas à lui seul la partie.

LE NELL – Reprise après sinistre
La reprise après sinistre détermine la rapidité. La capacité à assurer la continuité des services en cas de sinistre physique. Des ressources situées sur des sites distincts pour un basculement, qui ne sont pas affectées par le même événement – et qui sont véritablement isolées et hors production. Le Nell est discret, mais décisif.

LE BOURG– Cyber-résilience
La cyber-résilience protège la sauvegarde elle-même. Des environnements isolés et propres, séparés de l'exploitation productive, qui restent disponibles même lorsque l'ensemble de l'infrastructure de production est bloquée à des fins d'analyse. Le Bourg contrôle le jeu et veille à ce que l'as reste jouable.

LE STÖCK – Plans d'urgence
Des plans détaillés et spécifiques à l'entreprise pour les incidents de catastrophe et les cybers incidents. Pas de modèles achetés, mais des instructions étape par étape, élaborées dans le cadre d'une restauration efficace et testées régulièrement. Seule la combinaison des quatre atouts permet d'assurer une véritable continuité des activités.

L'analogie avec le Jass : quand on a une bonne main, on ne joue pas au hasard

Le jeu de cartes Jass fait partie de l'ADN suisse, comme le « Amen » à l'église. Ceux qui savent jouer au Jass le savent : une bonne main commence par un bon atout. Et un bon atout signifie avant tout posséder les cartes les plus fortes – le valet («Buur»), le 9 («Nell») et l'as. Dans l'idéal, on aimerait aussi le roi avec le valet («Mariage»). Une bonne main aide à remporter toutes les plis – ce qu'on appelle un «match».

Si nous imaginons maintenant une urgence informatique, la pièce s'assombrit, tout s'arrête, quelque part un système de surveillance tourne à vide et, l'espace d'un instant, plus rien ne fonctionne. Dans de tels cas, nous devons pouvoir compter sur notre stratégie de continuité des activités – sur notre bonne main. Et cette main doit reposer sur les mêmes piliers pour chaque entreprise, quelle que soit sa taille.

Au jass, on peut remporter des plis individuels. Mais seul celui qui a une bonne main et qui la joue correctement remporte la partie. Il en va de même pour la continuité des activités.

La structure avant le logiciel.

La technologie seule ne résout pas le problème.

L'erreur la plus courante lors de la mise en place d'une stratégie de continuité des activités est de se lancer trop tôt dans la technologie. La question « Quel système de sauvegarde allons-nous acheter ? » se pose avant même que les questions fondamentales n'aient trouvé de réponse. Cela conduit à dépenser des millions pour des solutions qui ne répondent pas aux besoins réels.

La bonne approche commence par l'activité, et non par l'infrastructure.

Étape 1 : Comprendre l'impact sur l'activité

Avant de parler de technologie, il faut d'abord répondre aux questions suivantes :

- Quels sont les systèmes et applications critiques pour l'entreprise ?
- Combien de temps l'entreprise peut-elle se passer de tel ou tel système ?
- Quel est le coût d'une panne par heure, par jour, par semaine ?
- Quelles sont les interdépendances entre les systèmes et les processus ?

Ce n'est qu'une fois ces réponses obtenues qu'il est possible de définir le RTO (dans quel délai les systèmes doivent-ils être remis en service ?) et le RPO (quel est le délai maximal pour la restauration des données ?). Ces valeurs constituent la base de toute décision technique.

Étape 2 : analyser l'infrastructure et identifier les lacunes

Une fois les exigences définies, il convient de dresser un état des lieux honnête :

- De quoi dispose-t-on aujourd'hui ?
- L'infrastructure existante peut-elle répondre aux RTO et RPO définis ?
- Où se situent les faiblesses structurelles – au niveau de la sauvegarde, de la reprise après sinistre ou de la cyber-récupération ?
- Les données SaaS, les charges de travail dans le cloud et les stocks d'informations non structurées sont-ils également protégés ?

- Existe-t-il des sauvegardes immuables et des zones de reprise isolées ?

Étape 3 : mettre en place une architecture selon les principes adéquats

Une architecture de continuité des activités robuste dans le domaine de l'infrastructure suit des principes clairs :

PRINCIPE	CE QUE CELA SIGNIFIE
Règle 3-2-1-1-0	3 copies des données (1 original + 2 sauvegardes), sur 2 supports différents, 1 copie externe ou dans le cloud, 1 copie hors ligne et inviolable (Air Gap) – et 0 erreur après les tests de restauration automatiques effectués par le logiciel de sauvegarde.
Immuabilité	Les données de sauvegarde doivent être immuables – aucun pirate ne doit pouvoir les chiffrer ou les supprimer.
Isolation	Les environnements de restauration doivent être totalement séparés de l'environnement de production.
Privilège minimal	Droits d'accès minimaux pour les administrateurs de sauvegarde et les systèmes de restauration.
Tests réguliers	Les restaurations doivent être effectuées et documentées régulièrement – non pas en théorie, mais dans la pratique.
Copies hors ligne	Au moins une copie doit être complètement déconnectée du réseau.

Étape 4 : Plans d'urgence – un travail sous-estimé

Les plans d'urgence sont souvent mal abordés. Les concepts prêts à l'emploi achetés ne sont, au mieux, qu'un aide-mémoire. Les plans élaborés en interne restent souvent incomplets, car ils partent d'un état idéal qui ne se produit pratiquement jamais dans la réalité.

Seule une chose permet d'élaborer des plans d'urgence vraiment fiables : la simulation complète et réelle d'une restauration ou d'un basculement – étape par étape, en tenant compte de tous les obstacles. Voici quelques angles morts typiques qui n'apparaissent qu'en cas d'urgence :

- Où se trouvent les identifiants et les secrets – et sont-ils accessibles en cas d'urgence ?
- Les fichiers d'installation et les licences sont-ils disponibles hors ligne ?
- Dans quel ordre les systèmes doivent-ils être reconstruits ?
- Qui est responsable en cas d'urgence – et qui est son remplaçant ?
- Le plan d'urgence est-il disponible sous forme imprimée – ou se trouve-t-il sur le serveur qui est justement inaccessible ?

> La continuité des activités ne commence pas dans le centre de données, mais dans l'entreprise.

Ces questions peuvent sembler banales. Dans la pratique, ce sont elles qui font la différence entre une restauration rapide et une panne pouvant durer plusieurs semaines.

Étape 5 : Sensibilisation – le facteur humain

La technologie protège, mais c'est l'humain qui décide. Une stratégie de continuité des activités (BC) qui n'est ancrée que dans le service informatique n'est pas une stratégie durable. On constate régulièrement ce qui suit dans la pratique :

- **Sensibilisation au niveau de la direction :** si la direction ne traite pas ce sujet comme une priorité, aucun budget ne sera débloqué – quels que soient les arguments avancés par le responsable informatique.
- **Formation des collaborateurs :** les ransomwa res commencent souvent par un simple clic. Chaque collaboratrice et chaque collaborateur est à la fois une faille potentielle et un rempart de protection.
- **Exercices réguliers :** il ne suffit pas de tester les sauvegardes, il faut également tester les plans d'urgence. Quiconque n'a jamais mis en pratique son plan de reprise après sinistre dans un environnement réel échouera en cas d'urgence.

La résilience commence au niveau de l'infrastructure.

C'est là que Sonio fait la différence en cas d'urgence.

La continuité des activités est un vaste sujet qui s'étend de la gestion des installations aux systèmes OT, en passant par les applications et les processus. Sonio n'est pas un prestataire de services généraliste couvrant tous les domaines, mais notre spécialité réside clairement dans le domaine de l'infrastructure informatique. C'est là que nous pouvons faire une réelle différence grâce à notre expertise approfondie et à l'expérience acquise au cours de dizaines de projets.

Ce qui relève de la couche d'infrastructure informatique :

DOMAINE	MESURES CONCRÈTES ET SOLUTIONS
Sauvegarde et protection des données	Architectures de sauvegarde robustes, BaaS (Backup as a Service), stockage immuable, stratégie 3-2-1-1-0.
Reprise après sinistre	Environnements de reprise après sinistre sur des sites distincts, DRaaS (Disaster Recovery as a Service), architectures de basculement, respect des objectifs RTO/RPO.
Cyber-récupération	Volets de cyber-récupération isolés, environnements de restauration propres, séparés de l'exploitation en production.
Réseau et redondance	Composants réseau redondants, connectivité inter-sites, contrôle d'accès sécurisé.
Cloud et hybride	Stratégies de sauvegarde hybrides, reprise après sinistre intégrée au cloud, sauvegarde sécurisée des charges de travail dans le cloud.
Intégration de la sécurité	Droits d'accès minimaux, chiffrement, surveillance et alertes dans le domaine de la sauvegarde.
Planification d'urgence	Documentation pratique sur la reprise après sinistre, tests de restauration, guides de reprise au niveau de l'infrastructure.

Ce que nous ne traitons pas – et pourquoi cette clarté est importante

Sonio ne s'occupe délibérément pas de la couche applicative ni de la gestion complète de la continuité des activités au niveau organisationnel. Non pas parce que ces domaines ne sont pas importants – bien au contraire. Mais l'expertise, c'est savoir où l'on est vraiment fort et où un autre partenaire peut apporter davantage de valeur.

> Une infrastructure robuste est efficace lorsqu'elle continue de fonctionner même sous pression.

Une infrastructure robuste est efficace lorsqu'elle continue de fonctionner même sous pression. Ce principe de concentration protège nos clients d'un piège courant : acheter des solutions qui existent techniquement, mais qui ne répondent pas aux besoins réels. Nous préférons orienter nos clients vers les bons spécialistes plutôt que de proposer une pseudo-solution.

Le lien avec la gestion des données

La continuité des activités dans le domaine des infrastructures ne peut être envisagée indépendamment de la stratégie globale en matière de données. Celui qui ne connaît pas ses données – lesquelles sont critiques, où elles se trouvent, comment elles sont interdépendantes – ne peut pas non plus les protéger. Dans le domaine de la gestion moderne des données, les disciplines suivantes sont particulièrement pertinentes :

- Sécurité, confidentialité, protection et résilience des données : sauvegarde, restauration, immuabilité, reprise après sinistre et cyber-récupération en tant que partie intégrante d'une stratégie cohérente de protection des données.
- Architecture des données : celui qui sait comment les données sont structurées et interdépendantes peut élaborer des plans de reprise plus précis.
- Gouvernance et conformité : les exigences réglementaires, telles que les obligations de conservation et les dispositions en matière de protection des données, doivent être intégrées dans la stratégie de sauvegarde et d'archivage.

En cas d'urgence, la théorie ne sert à rien.

Comment des risques sous-estimés peuvent soudainement paralyser les entreprises.

La théorie est utile. Mais les arguments les plus convaincants en faveur d'une stratégie de continuité des activités solide proviennent de la réalité et des moments où l'on pensait être préparé.

Quand les tâches de sauvegarde en vert induisent en erreur

Pendant plus de six mois, une entreprise a été espionnée sans que personne ne s'en aperçoive. Les attaquants n'avaient qu'un seul objectif : s'assurer qu'au moment décisif, aucune échappatoire ne soit possible.

> Les failles les plus dangereuses sont souvent celles qui restent invisibles au quotidien.

Pendant ce temps, ils ont réécrit les pilotes des lecteurs de bandes. Le résultat était d'une simplicité perfide : dès lors, les lecteurs n'enregistraient plus que des données inutiles sur les bandes. Toutes les tâches de sauvegarde continuaient de s'exécuter. Tout était vert. Tout semblait fonctionner.

Lorsque l'entreprise a finalement été cryptée, elle s'est crue en sécurité. Les bandes constituaient Externalisées, elles n'étaient pas concernées. Telle était la conviction. Au moment où la restauration a été tentée, la dure réalité s'est imposée : les sauvegardes n'étaient que des données inutiles. L'entreprise n'avait plus le choix et a dû payer.

Ce qu'il faut retenir de ce cas : un job de sauvegarde « en vert » n'est pas la preuve d'une sauvegarde fonctionnelle. Des tests de restauration réguliers et réels – pas seulement des contrôles automatiques, mais des exercices de restauration complets – ne sont pas des mesures facultative. Elles sont la seule chose qui fait la différence en cas d'urgence.

La cyberattaque pendant le projet de reprise après sinistre

Au beau milieu de la phase où les risques sont encore en discussion, l'entreprise est effectivement piratée. Soudain, tous les centres de données sont inaccessibles. L'analyse forensic bloque l'infrastructure pendant des jours. Le bilan dressé par les parties prenantes était décevant : « Nous savions qu'il cela aurait pu arriver – mais nous avons sous-estimé la probabilité. Et puis, tout à coup, des fonds illimités se sont présentés. » La prévention aurait coûté une fraction de cette somme.

> En cas d'urgence, ce n'est pas la modernité d'une infrastructure qui compte, mais le degré de préparation réel d'une entreprise.

Des millions pour la mauvaise solution

Une grande entreprise lance un appel d'offres et opte pour une solution coûteuse Solution d'infrastructure avec site secondaire dédié. Coûts engagés sur cinq ans s'élevant à plusieurs millions.

Le problème : la solution a été conçue d'un point de vue purement infrastructurel. L'activité – les applications, les processus opérationnels proprement dits, les flux de données – n'a pas été prise en compte dans la décision. En cas d'urgence, l'infrastructure aurait certes fonctionné, mais les systèmes qui s'appuient sur elle n'auraient pas pu être restaurés. Des millions pour une solution qui passe à côté des besoins réels. C'est le résultat d'une technologie sans stratégie.

De la prise de conscience à la mise en œuvre.

Comment les entreprises mettent en place la continuité des activités étape par étape.

Comment procéder concrètement lorsque la direction a pris conscience que « nous devons prendre ce sujet au sérieux » ? D'après notre expérience, une approche en plusieurs étapes a fait ses preuves, permettant à la fois rapidité et durabilité.

Le modèle en 5 phases pour la continuité des activités dans le domaine des infrastructures :

PHASE 1 – SENSIBILISATION
Que nous coûte une panne ? Élaboration conjointe d'une compréhension de l'impact sur l'activité au niveau de la direction et de l'informatique. Concrétisation des risques à l'aide de scénarios réels.

PHASE 2 – ANALYSE
Où en sommes-nous aujourd'hui ? Inventaire de tous les systèmes et données critiques, recensement des mesures de sauvegarde et de reprise après sinistre existantes, évaluation par rapport aux exigences RTO/RPO définies.

PHASE 3 – CONCEPTION
De quoi avons-nous besoin ? Conception architecturale d'une infrastructure de continuité des activités robuste, comprenant une solution de sauvegarde, un site de reprise après sinistre, un coffre-fort de cyber-récupération et un plan d'urgence. Alignement sur les exigences métier.

PHASE 4 – MISE EN ŒUVRE
Mise en place progressive de l'infrastructure et des plans d'urgence – documentée par des tests de restauration complets et réels.

PHASE 5 – EXPLOITATION ET CONTINUITÉ
Tests réguliers, mises à jour des plans d'urgence, formations de sensibilisation, surveillance et reporting.

Comment aborder le sujet

Une discussion sur la continuité des activités ne doit en aucun cas commencer par la présentation d'une gamme de produits. Elle doit débuter par trois questions sincères :

- Combien vous coûte une journée d'indisponibilité de vos systèmes les plus importants ?
- Avez-vous déjà vraiment testé ce scénario – avec une restauration réelle ?
- Vos collaborateurs savent-ils ce qu'ils doivent faire en cas d'urgence – et qui est responsable ?

> La résilience n'est pas un état que l'on achète, mais une capacité qui se construit en permanence.

Celui qui peut répondre à ces questions est prêt.
Celui qui hésite a identifié les mesures à prendre.

Partenaire pour une véritable résilience.

Sonio accompagne les entreprises avec pragmatisme et responsabilité.

Sonio ne se considère pas comme un simple fournisseur de logiciels. Nous sommes un partenaire en infrastructure et en architecture disposant d'une expertise approfondie dans les domaines précisément décisifs pour une stratégie de continuité des activités (BC) efficace sur le plan technique.

Concrètement, cela signifie

Nous aidons les entreprises à :

- Établir le lien entre les exigences métier et l'infrastructure technique – non pas en tant que consultants théoriciens, mais en tant que praticiens dotés d'une expérience de mise en œuvre.
- De mettre en place une architecture de sauve garde et de reprise qui fonctionne réellement – incluant l'immuabilité, l'isolation et une validation régulière.
- De concevoir et d'exploiter des coffres-forts de cyber-récupération et des environnements de restauration isolés.
- D'élaborer des plans d'urgence basés sur de véritables tests de restauration et non sur des hypothèses théoriques.
- Intégrer les environnements cloud et hybrides dans la stratégie de continuité des activités.
- Sensibiliser les parties prenantes au bon niveau – en collaboration avec les responsables informatiques et les dirigeants.

Notre conception du partenariat

Au Jass, il ne suffit pas d'avoir de bonnes cartes. Il faut les lire, les évaluer et les jouer au bon moment. Et surtout : on ne gagne pas au Jass tout seul.

> La technologie est une carte. La stratégie permet de gagner la partie.

C'est exactement ainsi que nous concevons notre rôle. La technologie est une carte. La stratégie fait gagner la partie. Nous combinons des solutions de pointe avec une expertise en architecture, des scénarios testés, une gouvernance claire et une responsabilité opérationnelle, et nous gérons tout cela en Suisse. Quand on a à sa table un partenaire qui sait ce qui est en jeu, on joue différemment.

Agir avant que la situation d'urgence ne décide.

Celui qui considère la résilience comme une mission de direction reste capable d'agir même lorsque plus rien ne fonctionne.

La continuité des activités n'est pas un sujet que l'on peut aborder « un jour ou l'autre ». C'est un sujet qu'il faut aborder aujourd'hui, avant que la situation d'urgence n'impose ce que l'on aurait pu contrôler. **La bonne nouvelle :** ce n'est pas sorcier. Cela ne nécessite pas de moyens illimités ni de projets s'étalant sur des mois. Il faut de la clarté sur ses propres besoins, sur l'infrastructure existante, sur les lacunes critiques. Et il faut la volonté d'agir de manière cohérente. Celui qui transpose ces principes en une stratégie cohérente ne s'en remet pas au hasard en cas d'urgence. Celui qui a de bonnes cartes en main peut rester serein, même si la pièce s'assombrit et que tout s'arrête.

Les principales conclusions de ce livre blanc :

1. La sauvegarde est un début, pas une fin.
Celui qui croit être suffisamment préparé avec une solution de sauvegarde sous-estime fondamentalement le risque.

2. La continuité des activités relève de la direction.
Si la direction ne s'engage pas sur ce sujet, aucun budget ne sera débloqué, quelle que soit la qualité des arguments avancés par le service informatique.

3. Les RTO et RPO doivent être définis avec l'entreprise.
Pas par le service informatique seul, mais en concertation avec les responsables des processus métier.

4. Les plans d'urgence doivent être testés.
Une tâche de sauvegarde réussie ne suffit pas. Seule une restauration réelle permet de mettre en évidence les points faibles.

5. La sensibilisation est tout aussi importante que la technologie.
La meilleure infrastructure ne sert à rien si les collaborateurs ne savent pas ce qu'ils doivent faire – ni qui en est responsable.

6. La spécialisation l'emporte sur la complexité.
Sonio se concentre sur ce que nous savons vraiment faire : la résilience des infrastructures au plus haut niveau.

Commencez dès maintenant – pas plus tard.

Avec des mesures concrètes immédiates et un plan clair sur 90 jours pour une stratégie de continuité des activités (BC) efficace.

Après avoir lu ce livre blanc, de nombreuses entreprises savent qu'elles doivent agir. Cependant, la première étape achoppe souvent sur la question suivante : par où commencer ?

Voici une réponse claire à cette question.

Mesures immédiates – cette semaine

1. Chiffrer le coût d'une panne : réunissez-vous avec votre direction et calculez ce que coûte concrètement une journée d'indisponibilité de vos systèmes les plus importants. Si vous ne connaissez pas ce chiffre, c'est par là qu'il faut commencer.

2. Vérifier honnêtement l'état des sauvegardes : quand une restauration complète a-t-elle été effectuée pour la dernière fois – pas seulement un test automatique, mais une véritable restauration ? Si la réponse est « je ne sais pas » ou « jamais », vous savez ce qu'il vous reste à faire.

3. Clarifier les responsabilités : qui est responsable de la continuité des activités au sein de l'entreprise ? Qui est son suppléant ? Ces informations sont-elles disponibles hors ligne et accessibles ?

À moyen terme – dans les 90 prochains jours

1.Réaliser une analyse d'impact sur l'activité : recensez tous les systèmes critiques et leurs interdépendances, puis définissez les objectifs RTO et RPO en collaboration avec les services opérationnels.

2. Analyse des lacunes : comparez votre infrastructure existante aux exigences définies. Où se situent les principales lacunes : au niveau de la sauvegarde, de la reprise après sinistre ou de la cyber-résilience ?

3. Premier entretien de conseil : discutez avec un partenaire qui ne se contente pas de vendre des produits, mais qui analyse la situation et fournit un rapport honnête.

Stratégique – votre feuille de route BC

La continuité des activités n'est pas un projet ponctuel. C'est une capacité permanente. Fixez-vous comme objectif, dans un délai de douze mois :

- exploiter une architecture complète de sauvegarde et de reprise après sinistre selon la règle 3-2-1-1-0
- avoir effectué au moins un test complet de reprise après sinistre
- disposer de plans d'urgence basés sur des expériences de restauration réelles
- et d'avoir sensibilisé la direction et les collaborateurs

Ce n'est pas un idéal inatteignable. C'est tout à fait réalisable – avec le bon partenaire.

PRÊT POUR LA PROCHAINE ÉTAPE ?

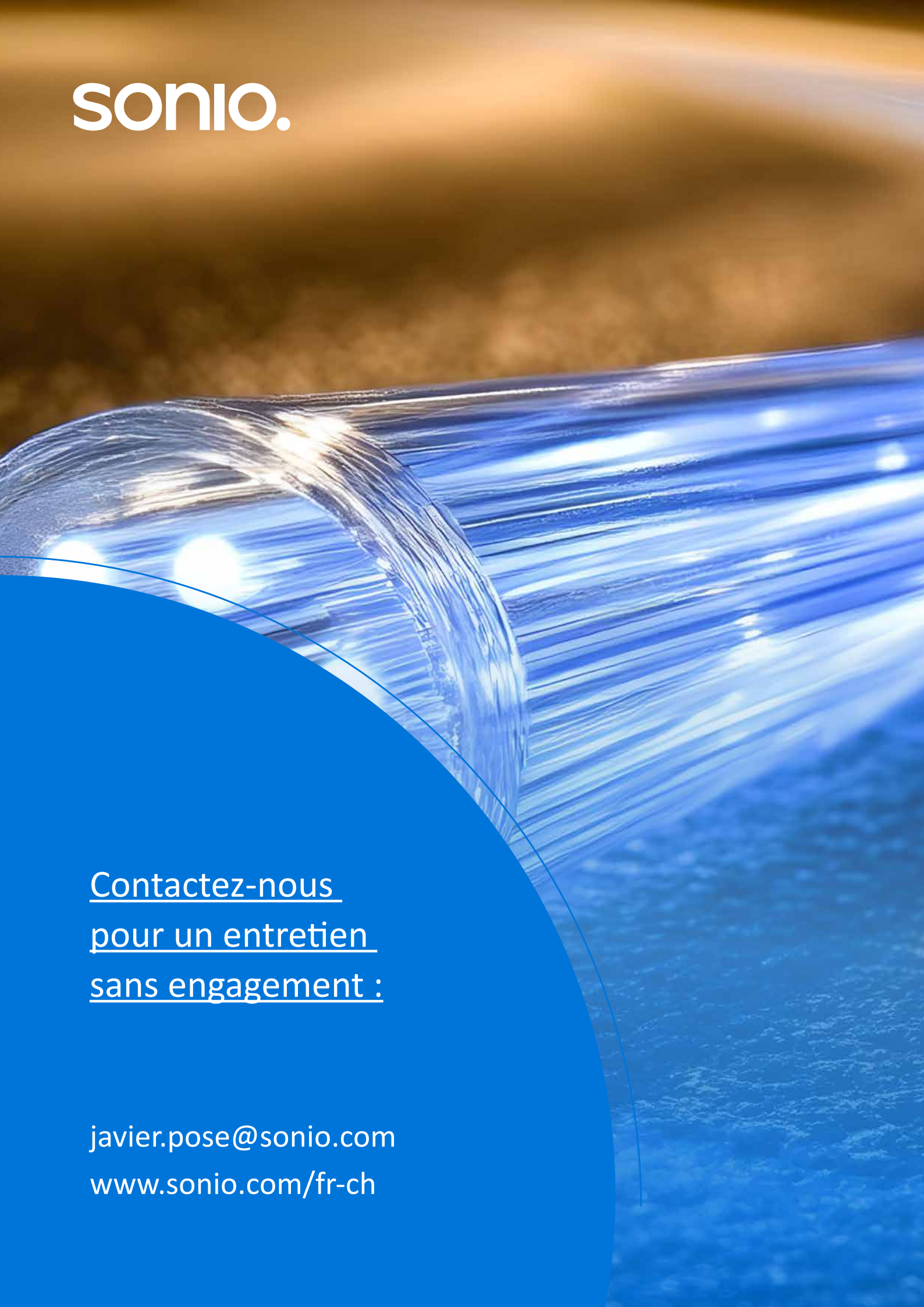
Nous vous proposons un premier entretien gratuit et sans engagement. Pas de discours commercial, mais une analyse structurée de votre situation actuelle.

Ce que vous saurez après l'entretien :

✓ Où se situent vos principales lacunes
✓ Quelles mesures ont un effet immédiat
✓ Ce qu'implique une solution BC complète pour votre entreprise

Prenez rendez-vous dès maintenant pour un entretien de conseil personnalisé :
www.sonio.com/fr-ch/business-continuity

Sources : ce livre blanc s'appuie sur les sources suivantes : Discussion interne avec les parties prenantes : Sasa Gržinić, Lars Kündig, Markus Fischer, Mario Stich – avril 2026. Article de blog : Lars Kündig, « Business Continuity : les bons atouts pour les urgences informatiques », avril 2026, Sonio AG. Livre blanc : Ralph Budil, « La réussite commerciale grâce à une gestion moderne des données avec SONIO », avril 2026, Sonio AG. BACS (Office fédéral de la cybersécurité), rapports annuels sur les ransomwares, Suisse. Inside IT : « Les inondations ont paralysé les serveurs de 30 communes », juillet 2024. DAMA DMBOK – Data Management Body of Knowledge. Cadre de cybersécurité NIST 2.0 ; Cadre de gestion des risques liés à l'IA du NIST. Gartner, points de vue actuels des analystes sur la protection des données et la résilience, 2025/2026. Sonio AG, page d'accueil Continuité des activités, www.sonio.com/fr-ch/business-continuity



Contactez-nous
pour un entretien
sans engagement :

javier.pose@sonio.com
www.sonio.com/fr-ch