COLLECTION AMRAE
MAÎTRISE DES RISQUES

Les PLANS de Continuité d'Activité

AMRAE
la Maison du risk management

Avant-propos

Version 2.0 – Avril 2026 :

Révision, coordination et cohérence globale :	Benoit Vraie & Elodie Yayer Dunand,
Basé sur la version 1.0 (2013) – Rédaction initiale :	Benoit Vraie & Sophie Huberson
Contributions techniques :	les personnes suivantes ont apporté une contribution technique significative et/ou des retours d'expérience terrain dans leur domaine d'expertise. PCA cyber : Olivier Allaire, Christophe Pelfresne PCA climat : Elodie Yayer Dunand, Santiago Bosio, Christophe Bouvard, Linda Khelid
Relecture :	Jason Crumley (relecture globale et traduction en anglais) Maureen Chagnon (cohérence des mises à jour sur le climat)
Direction artistique :	agence La nageuse

Face à l'intensification des événements climatiques extrêmes, inondations, vagues de chaleur, tempête, feux de forêt, et à l'explosion des intrusions cyber, rançongiciels et sabotages numériques, les organisations doivent composer avec des menaces de plus en plus systémiques. Ni l'adaptation climatique seule, ni le renforcement des défenses informatiques isolément ne suffiront désormais à contenir leurs effets.

Dans ce contexte, la mise en place d'un Plan de Continuité d'Activité (PCA) exige aujourd'hui de dépasser la simple analyse de l'indisponibilité des ressources internes.

Les événements extrêmes récents, canicule de 2022, tempêtes et inondations en Espagne en 2024 (DANA), inondations dans le sud est de la France, feux de forêt en Californie, ou crises cyber majeures, attaques par rançongiciel contre les hôpitaux français en 2023, attaque de La Poste en 2025, rappellent à quel point les organisations sont des systèmes interconnectés. Elles dépendent d'un réseau de partenaires, de fournisseurs, d'infrastructures physiques, de système numériques, de services publics... autant de maillons dont la défaillance peut provoquer des effets domino allant jusqu'à rendre inopérantes les solutions de continuité elles-mêmes.

Par ailleurs, la résilience ne naît pas au moment de la crise, elle se prépare bien en amont et c'est maintenant que les entreprises/organisations doivent faire évoluer leur PCA. De plus, un PCA n'est jamais figé ; une fois élaboré, il doit être régulièrement testé et actualisé pour rester opérationnel. Les exercices de crise constituent à cet égard un levier essentiel. En mettant à l'épreuve des scénarios variés et parfois complexes, les organisations identifient des fragilités jusqu'alors insoupçonnées. Chaque enseignement tiré et chaque amélioration apportée contribuent ainsi à renforcer la capacité collective à maintenir les activités essentielles lorsque la situation se détériore réellement.

C'est pourquoi, actualiser l'ouvrage *« Les Plans de Continuité d'Activité »* publié en 2013, et y intégrer pleinement la dimension climatique et cyber en 2026, apparaissait comme une nécessité. Ce livre propose une lecture renouvelée des PCA, à la lumière des défis climatiques et cybersécurité, pour accompagner les organisations dans leur transition vers une résilience durable.

> Ce n'est pas le plus fort de l'espèce qui survit, ni le plus intelligent, mais celui qui sait s'adapter au changement."
>
> Charles Darwin

Sommaire

Introduction

Quand un sportif se blesse lors d'une compétition, deux questions lui viennent à l'esprit : ma blessure est-elle grave ?

Quand pourrai-je reprendre l'entrainement ? Son coach, ses médecins, ses kinés le connaissent si bien qu'ils vont répondre rapidement à sa question, d'autant qu'ils vont compter sur des éléments déterminants pour tenir les délais de la convalescence : une organisation et une motivation sans faille. Mais pour recouvrer sa pleine forme, encore faut-il bien se connaître et savoir à quel point on peut solliciter tel ou tel fonction de son corps.

Cette métaphore nous permet de saisir l'importance de la parfaite connaissance des Hommes et des process de l'organisation : mettre en place un Plan de Continuité d'Activité (PCA) permet à l'entreprise non seulement de secourir son activité en cas de sinistre mais également (et pour son plus grand bénéfice) de *« mieux se connaitre elle-même »*. En effet, l'élaboration d'un PCA présuppose un travail d'identification des vulnérabilités de l'organisation mais au-delà, nécessite de procéder à un exercice d'introspection, de recensement et de cartographie des processus et des ressources associées. Cette activité d'analyse et de sécurisation de l'activité dépasse donc très largement le cadre de la simple préparation à la crise, mais permet tout autant de revisiter ses cycles fondamentaux sous l'angle critique afin de les optimiser.

Cette introspection est d'autant plus cruciale que le paysage des menaces a radicalement changé. Si la continuité d'activité s'est historiquement construite en réponse à des sinistres accidentels, elle doit aujourd'hui faire face à une nouvelle réalité : celle de l'adversaire délictuel et de la cyber-crise systémique. Comme nous le verrons, la simple préparation à une panne ou à un sinistre physique ne suffit plus face à des attaques délibérées visant le cœur numérique de l'entreprise et son écosystème.

La Continuité d'Activité est donc une philosophie d'entreprise qui consiste à *« préparer la guerre en temps de paix »*[1]. En effet, en proposant d'effectuer a priori[2] un travail d'analyse et de planification de la réaction à apporter face à un événement indésirable, le PCA permet de minimiser les impacts sur l'activité de la survenue d'un sinistre en assurant un fonctionnement en mode dégradé et/ou une reprise graduelle des activités, des plus critiques au moins critiques.

C'est au cours des **années 1970/80** que l'on trouve les premières ébauches de PCA, au niveau de processus industriels et tertiaires, notamment dans des activités qualifiées de *« critiques »* (banques, aéronautiques, défense, agroalimentaire...).
En parallèle, l'importance grandissante des données en jeu et la complexité des architectures de réseau, ont nécessité la mise en place de Plan de Secours Informatique (PSI ou DRP: *« Disaster Recovery Plan »*) qui est l'équivalent d'un PCA dans le domaine informatique.

Les **années 90/2000** ont vu se développer le phénomène de globalisation de l'économie. Celle-ci s'est traduit par une forte concentration des sociétés et le développement exponentiel de la sous-traitance, et donc de la concurrence, provenant des pays émergents, plus particulièrement des pays d'Asie du Sud-Est Ainsi, dans la recherche permanente d'une meilleure rentabilité, les entreprises ont été

(1) in *« Gérer les grandes crises : Sanitaires, écologiques, politiques et économiques »*, L CROCQ and al. Odile JACOB
(2) En amont de toute crise

amenées à faire des choix d'organisation les rendant particulièrement vulnérables aux aspects logistiques (*« supply chain »*). La survenue d'un évènement indésirable, comme un évènement climatique extreme, en un lieu donné peut impacter l'ensemble de la chaîne logistique et par effet domino engendrer des ruptures d'approvisionnements et des arrêts de production dans différentes zones géographiques.

Au cours des deux dernières décennies, la continuité d'activité est passée d'une bonne pratique organisationnelle à une obligation réglementaire structurante dans plusieurs secteurs d'activités considérés comme sensibles ou systémiques. Cette évolution s'est accentuée à la suite de crises majeures, qu'elles soient financières, numériques, sanitaires, énergétiques ou géopolitiques, mettant en évidence la nécessité de garantir la continuité des services essentiels, y compris en situation dégradée.

C'est notamment le cas du secteur bancaire, pour lequel la continuité d'activité constitue désormais un pilier de la résilience opérationnelle. Les établissements financiers sont tenus de garantir leur capacité à assurer la continuité de leurs activités critiques, définie comme l' *« ensemble de mesures visant à assurer, selon divers scénarios de crise, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services ou d'autres tâches opérationnelles essentielles ou importantes, puis la reprise planifiée des activités »*. Cette définition, historiquement fondatrice des politiques de PCA, s'inscrit aujourd'hui dans une approche élargie intégrant la gouvernance, la gestion des risques, les dépendances technologiques et les chaînes de valeur étendues.

Dès le milieu des **années 2000,** cette préoccupation s'est traduite, en France, par des initiatives collectives propres à la Place financière. À ce titre, un groupe de réflexion dénommé *« Groupe de place Robustesse »* a été constitué en 2005 afin de prendre en compte des scénarios de crise susceptibles d'impacter simultanément les acteurs de la place bancaire et boursière de Paris.

Un premier exercice d'envergure a ainsi été organisé le 4 juin 2008, réunissant une quinzaine de grandes banques et institutions de la Place de Paris, ainsi que des représentants de l'État. Cet exercice simulait une crise technique majeure ayant pour point de départ un arrêt prolongé de la distribution d'électricité en Île-de-France, entraînant de nombreuses perturbations pour la Place financière et pour l'économie réelle. Ces travaux préfiguraient les approches actuelles fondées sur des scénarios extrêmes et systémiques.
Parallèlement au secteur bancaire, le secteur des assurances est également soumis à des obligations spécifiques en matière de continuité et de gestion des crises, notamment au travers de la réglementation Solvabilité II, qui impose la mise en place de dispositifs de gouvernance, de gestion des risques et de continuité proportionnée aux activités et aux risques portés par les organismes d'assurance.

Depuis janvier 2025, le cadre réglementaire applicable aux établissements financiers a été substantiellement renforcé par l'entrée en application du règlement (UE) 2022/2554 relatif à la résilience opérationnelle numérique du secteur financier (DORA, Digital Operational Resilience Act). Ce règlement exige que les établissements financiers assujetties mettent en place dans leur cadre de gestion des risques liés aux technologies de l'information et de la communication (TIC) des plans de continuité d'activité (business continuity plans) et des plans de réponse et de reprise après incident, incluant des dispositions documentées, des procédures, des tests périodiques et des mécanismes de reprise pour assurer la continuité des fonctions critiques et la résilience opérationnelle face aux perturbations.

En pratique, cela implique que les entités financières conçoivent, maintiennent, testent périodiquement et révisent leurs plans de continuité et de reprise,

intégrés dans une politique globale de résilience opérationnelle. Ces dispositifs reposent notamment sur des analyses d'impact métier (Business Impact Analysis, BIA), la définition d'objectifs de reprise adaptés (RTO, RPO), la prise en compte des dépendances critiques, y compris vis-à-vis des prestataires tiers, ainsi que la réalisation d'exercices et de tests réguliers afin d'être en mesure de continuer leurs activités essentielles même en cas de défaillance ou d'incident majeur.

Au delà du secteur financier, d'autres activités sont soumises à des obligations réglementaires renforcées en matière de continuité et de résilience, notamment les Secteurs d'Activités d'Importance Vitale (SAIV) définis par le code de la défense et par l'arrêté du 2 juin 2006. Ce dispositif national, toujours en vigueur, s'inscrit désormais dans un cadre élargi et modernisé avec la transposition de la directive européenne sur la résilience des entités critiques (REC).

Les opérateurs d'importance vitale, publics ou privés, exercent des activités indispensables au fonctionnement de la nation et sont, à ce titre, tenus de mettre en œuvre des dispositifs structurés de gestion de crise et de continuité d'activité, couvrant l'ensemble des risques susceptibles d'affecter la fourniture des services essentiels. Ces dispositifs doivent être formalisés, maintenus dans la durée et régulièrement éprouvés au travers d'exercices.

La directive REC renforce cette approche en consacrant une vision globale de la résilience, intégrant les dimensions numériques, physiques, organisationnelles et humaines, et en renforçant la coordination entre acteurs publics et privés. La continuité d'activité s'inscrit ainsi dans une logique de résilience systémique, au cœur de la gouvernance et de la sécurité des organisations critiques.

Alors que, dans les années 2010, les normes et référentiels relatifs aux plans de continuité d'activité se sont multipliés, la norme ISO 22301 s'est imposée comme la référence centrale. Elle définit les exigences permettant de structurer un système de management de la continuité d'activité, depuis l'analyse d'impact métier jusqu'aux plans, aux tests et à l'amélioration continue.
Elle est complétée par d'autres normes de la famille ISO 22300 et par des standards liés à la continuité des systèmes d'information. Dans les secteurs régulés, ces normes s'articulent avec des cadres réglementaires spécifiques, sans s'y substituer.

Notons l'existence du *« Guide pour réaliser un plan de continuité d'activité »* du SGDSN (Secrétariat général de la défense et de la sécurité nationale-2013) accessible gratuitement depuis leur site internet. Ce guide constitue un référentiel méthodologique de référence et de bonnes pratiques, toujours utilisé comme support pédagogique, notamment dans le secteur public et les activités d'importance vitale. Il doit cependant être complété et mis en cohérence avec la norme ISO 22301, ainsi qu'avec les cadres réglementaires et sectoriels en vigueur.

DIRECTIVE REC

Le nouveau pilier de la résilience européenne

La Directive européenne REC (2022/2557) renforce la capacité des entités critiques à assurer la continuité des services essentiels, énergie, eau, santé, transports, infrastructures numériques, face aux crises climatiques, cyber ou géopolitiques.

Elle impose une approche tous risques, incluant l'analyse des menaces, la mise en place de plans de résilience, des mesures de protection, des exercices réguliers et la notification obligatoire des incidents significatifs.

En France, à la date d'édition de cet ouvrage, la transposition est toujours en cours : le projet de loi a été adopté par le Sénat en mars 2025, puis amendé à l'Assemblée nationale en septembre 2025, et attend encore son vote final.

Cette directive marque une évolution majeure : elle fait passer les organisations d'une logique de protection à une véritable culture de résilience opérationnelle, essentielle pour structurer les PCA des secteurs vitaux.

DÉFINITION ET FINALITÉ DU PCA ET DE SON ENVIRONNEMENT

Chapitr

e 1

1.1. DÉFINITIONS ET FINALITÉS DU PCA

1.1.1. Définitions

1.1.1.1. Revue critique des définitions données

Si l'on s'en réfère au Règlement 97-02 du comité de règlementation bancaire, le PCA est l'*« Ensemble de mesures visant à assurer le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services essentielles de l'organisation puis la reprise planifiée des activités »*.

1.1.1.2. Proposition de définition

Le Plan de Continuité d'Activité est l'organisation alternative que l'entreprise met en place en attendant de remédier à l'événement perturbateur qui est à l'origine de l'arrêt des processus.

Le PCA prend la forme d'un document **qui identifie, recense, planifie et ordonnance** les actions de continuité et/ou de reprise d'activité à mettre en place en cas de réalisation d'évènements indésirables, plus ou moins grave.

Il fixe les modalités organisationnelles et techniques du fonctionnement de l'entreprise en mode *« dégradé »*, puis de reprise graduelle des activités, des plus sensibles au moins sensibles.

1.1.2. A quoi sert un PCA ?

Le Plan de Continuité d'Activité assure la pérennité des processus critiques en cas d'indisponibilité d'une ou des ressources de l'environnement de travail. Autrement dit, le PCA sert à amortir les effets d'une crise éventuelle, à minimiser les impacts en cas de sinistre et à garantir la poursuite de l'activité de l'entreprise malgré la survenue d'évènements indésirables. C'est une boite à outil d'aide à la décision pour la cellule de crise.

Ainsi ces objectifs relèvent autant de la performance financière et économique que sociale et environnementale, sans oublier la restauration du *« capital-image »* de l'organisation.

1.1.3. Philosophie du PCA

Le PCA n'est pas un manuel perdu au fond d'une armoire, c'est avant tout un état d'esprit de réalisation des objectifs initialement fixés dans le *business plan*.

« Préparer la guerre en temps de paix » consiste à répondre à des questions en amont de l'évènement, pour s'affranchir des aléas de l'improvisation et de la contrainte des temps de réponse, lorsque

la crise surviendra réellement. Il est donc absolument nécessaire de mettre en place à l'avance, *« à froid »*, l'ensemble des éléments rationnels sur lesquels on pourra s'appuyer *« à chaud »*, dès les premières minutes de la crise. Bien sûr, tout ne peut pas être prévu à l'avance, il sera donc nécessaire de s'adapter constamment aux conditions de la réalité de la crise en les analysant et en tirant les conséquences pour modifier l'ordre de redémarrage des processus, en fonction du contexte (campagne publicitaire de lancement d'un nouveau produit par exemple).

1.1.4. Comment fixer le niveau du maintien des activités ?

L'objectif du PCA ne consiste pas à *« dupliquer »* l'organisation pour permettre une continuité à l'identique, mais d'analyser l'impact de la crise pour chaque métier et chaque processus et de les classer selon une Durée d'Interruption Maximale Admissible (DIMA). Il permet donc un fonctionnement *« dégradé »* des processus de l'organisation et leur reprise graduelle, des plus sensibles au moins sensibles.

En complément, la détermination du niveau de maintien de l'activité est issue de la combinaison de la capacité de respecter les contraintes réglementaires, techniques et sociétales et de la volonté de la Direction Générale de maintenir l'activité de l'entreprise à un niveau donné. L'ensemble se traduit inévitablement par un coût acceptable d'investissement pour préparer le plan et assure le fonctionnement de ce dernier : le PCA devra établir le ratio acceptable entre l'engagement financier et le maintien du niveau des activités.

Ainsi, réduire le PCA à des solutions techniques sans mettre en place une stratégie managériale arbitrée par la Direction Générale peut rendre vains tous les efforts et les investissements consentis.

1.1.5. Plan de continuité d'activité et Plan d'urgence, quelle différence ?

Un plan d'urgence a pour vocation d'organiser la réaction immédiate face à un événement brutal, comme un incendie, une inondation ou toute autre situation mettant en danger les personnes ou la sécurité du site. Il vise avant tout à gérer l'événement sur le moment, à protéger les individus et à stabiliser la situation. Or, dans lesdits plans d'urgence, les solutions de continuité ne sont pas décrites. Il doit être coordonné avec les plans de secours et plans de continuité des activités.

En complément, le Plan de Continuité d'Activité (PCA) intervient une fois l'urgence maîtrisée ou en parallèle de sa gestion, avec pour objectif de maintenir les activités essentielles de l'organisation, même en mode dégradé. Il donne les éléments clés pour gérer les conséquences induites par l'urgence et assurer la continuité des services en cas d'indisponibilité des infrastructures, ressources, systèmes ou parties prenantes clés de la chaine de valeur. Il s'appuie sur une analyse d'impact, la définition des priorités et la mise en place de solutions de repli permettant de poursuivre les opérations malgré la perturbation.

Ainsi, le plan d'urgence et le PCA sont complémentaires : le premier permet de faire face à la crise immédiate, tandis que le second permet d'assurer la continuité du fonctionnement de l'organisation durant et après l'événement.

DE LA LOGIQUE DE « *SCÉNARIO* » À LA LOGIQUE D'« *INDISPONIBILITÉ DES RESSOURCES* »

Chapitr


e 2

2.1. CRITIQUE DE LA MÉTHODOLOGIE/ LOGIQUE DE « *SCÉNARIO* »

La crise se révèle être toujours un film dont le scénario n'est pas écrit.

L'approche de continuité d'activité basée sur les scénarii part du postulat qu'il est nécessaire d'identifier les origines des menaces qui pèsent sur l'organisation avant de mettre en place des solutions de continuité d'activité. Ce principe s'avère dangereux car les scénarii sont des constructions intellectuelles, étayés sur des hypothèses ou au mieux des probabilités qui ne correspondent jamais totalement à la réalité des évènements et des faits.

Par ailleurs, les membres de la cellule de la crise sont soumis à un stress important. Ce stress entame leurs capacités de raisonnement. De ce fait, ils auront tendance à gérer la crise comme si elle s'inscrivait totalement dans le scénario préétabli, et à dupliquer mécaniquement les actions prescrites dans le PCA. C'est une source majeure d'erreurs car la réalité de la crise n'est jamais totalement conforme au scénario.

Cette approche du PCA fondée sur des scénarii précis mais inadéquats (par construction) trouve rapidement ses limites. Une autre approche, plus modulaire, permet de s'adapter plus facilement et plus rapidement à la réalité des faits.

EXEMPLE

Prenons l'exemple de la crue de Seine.

Il apparait délicat de définir un scénario précis de cette « *catastrophe annoncée* ». Les discours véhiculés sur la gravité potentielle d'un tel événement varient en fonction des intérêts des acteurs. Certains protagonistes ont tendance à mettre en avant le fait que des aménagements et travaux ont été réalisés afin de ralentir les délais de montée des eaux et d'écrêter la crue (Bassins de rétention des eaux en amont de Paris) tandis que d'autres soulignent que le Paris d'aujourd'hui n'est plus le Paris de 1910 et que le développement de l'urbanisation et la mise en bitume d'un nombre croissant de surfaces ont pour conséquence directe la diminution des temps de concentration des eaux à l'échelle du bassin versant. Il est donc délicat d'appréhender « *objectivement* » la gravité d'un tel phénomène.

Paris et IDF : la carte des zones inondables

Crédits : ©2025 idé – Le Parisien

EXEMPLE

Prenons l'exemple du plan national de prévention et de lutte « *Pandémie grippale* » du gouvernement français (2006) pour répondre aux problématiques de crise sanitaire.

Ce plan a été structuré en fonction d'hypothèses issues d'études cliniques et épidémiologiques de l'Organisation Mondiale de la Santé et de l'Institut de Veille Sanitaire (InVES). Ainsi la dynamique de la pandémie devait théoriquement être la suivante :

- un développement de la pandémie en vagues successives, chaque vague pouvant s'étendre sur 8 à 12 semaines ;
- un taux d'attaque clinique de 15 à 35% ;
- un taux de décès de 1 à 2%.

- Quant à l'importance de ces deux vagues, deux hypothèses étaient présentes :
  - soit deux vagues identiques (50% chacune) ;
  - soit 1/3 des personnes touchées réparti sur la première vague et 2/3 sur la seconde [3].

Cette approche correspondait à une conceptualisation de la dynamique de crise, à une logique de gradation de la transmission interhumaine et à la diffusion géographique de la maladie, cotée de 1 *« absence de circulation de virus »* à 6 *« pandémie grippale »* ; la phase 7 étant celle du *« retour à la normale »*.

Or, le scénario ne s'est pas déroulé ainsi. Dans les faits, les signes avant-coureurs alarmistes laissant imaginer un développement exponentiel de la crise ont laissé place à une longue phase de stabilisation ne répondant plus à la logique probabiliste définie par les modèles. L'Etat a donc bâti un déroulement chronologique du scénario qui ne s'est pas révélé en adéquation avec la réalité de la dynamique de la crise.

Le taux d'attaques cliniques du scénario évalué entre 15% et 35% se fonde sur la *« Loi des Grands Nombres »* qui ne s'applique que très imparfaitement à petite échelle (quelques personnes ou dizaines de personnes). Ainsi, dans la réalité, il est tout à fait possible qu'une équipe de collaborateurs soit décimée par la grippe et ne puisse travailler, alors qu'une autre ne sera pas affectée. En respectant cette logique statistique de distribution homogène de l'attaque virale, on ne peut résoudre la problématique de continuité d'activité à l'échelle d'une équipe. En effet, la logique de contamination répond ici à une logique de proximité physique et non de distribution statistique.

Ainsi, les PCA structurés en fonction d'un scénario se révèlent être le plus souvent des instruments rigides.

Situations et mesures

Situation 1	Absence de circulation de nouveaux virus aviaires hautement pathogènes chez l'animal et l'homme (pour mémoire).
Situation 2A	Épizootie à l'étranger provoquée par un virus hautement pathogène, sans cas humain (phase 2 OMS).
Situation 2B	Épizootie en France provoquée par un virus hautement pathogène, sans cas humain (phase 2 OMS).
Situation 3A	Cas humains isolés à l'étranger sans transmission interhumaine (phase 3 OMS).
Situation 3B	Cas humains isolés en France sans transmission interhumaine (phase 3 OMS).
Situation 4A	Cas humains groupés à l'étranger, limités et localisés (transmission interhumaine limitée due à un virus mal adapté à l'homme ; phase 4 OMS).
Situation 4B	Cas humains groupés en France, limités et localisés (transmission interhumaine limitée due à un virus mal adapté à l'homme ; phase 4 OMS).
Situation 5A	Larges foyers de cas groupés non maîtrisés à l'étranger (phase 5 OMS)
Situation 5B	Extension des cas humains groupés en France (phase 5 OMS).
Situation 6	Pandémie grippale (phase 6 OMS) : a. Organisation et mesures sanitaires ; b. Maintien des activités.
Situation 7	Fin de vague pandémique.

Source : Plan gouvernemental de prévention et de lutte *« Pandémie grippale »* version 2, 2006.

(3) InVES: Institut national de Veille Sanitaire, *« Estimation de l'impact d'une pandémie grippale et analyse de stratégies »*

2.2. PROPOSITION D'APPROCHE PAR L'INDISPONIBILITÉ DES RESSOURCES

L'approche par scénarii ayant montré ses limites, il est nécessaire d'en adopter une autre : l'approche par indisponibilité des ressources.

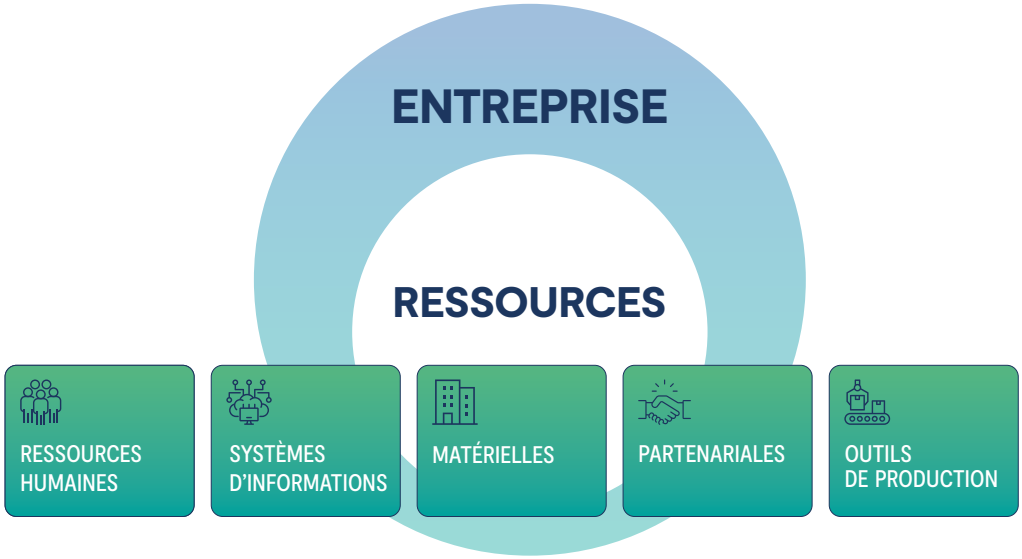
Pour fonctionner correctement une entreprise utilise différentes ressources : les actifs matériels (locaux et outils de production, matières premières, infrastructure informatique, etc.) et les actifs immatériels (main d'œuvre, données, image, etc.).

Ainsi, en cas de dysfonctionnement, d'indisponibilité, de destruction ou de disparition de telle ou telle ressource, le fonctionnement global de l'entreprise est susceptible d'être altéré. Au-delà de la gestion de l'urgence de la crise, le PCA aura pour tâche de diminuer l'impact et la durée de l'indisponibilité de la ou des ressource(s).

Ces ressources peuvent se décrire de la manière suivante :

Nous entendons par « *indisponibilités de ressources* » la conséquence de tout évènement indésirable ou situation qui dépasse les capacités de réponse matérielle et/ou organisationnelle d'un ou de plusieurs Services de l'entreprise. Cette définition n'est pas exclusive, elle peut varier en fonction de l'appétence aux risques de l'entreprise et de la volonté de structurer des réponses de continuité a priori, en cas de survenue d'évènements indésirables.

A la logique de scénarii préétablis, nous substituons la logique d'indisponibilité des ressources. La première étape de la réflexion dans le processus de mise en place d'un PCA est donc de s'interroger sur les conséquences de l'indisponibilité, la destruction ou la disparition de telle ou telle ressource au sein de l'entreprise, quelles que soient les causes et les origines du sinistre et sans considération de probabilités.



La spécificité des crises liées à un évènement climatique extrême est l'indisponibilité simultanée de plusieurs ressources sur une échelle géographique étendue. Si l'environnement peut être impacté comme *« ressource entreprise »*, il faut sécuriser indépendamment le périmètre géographique de l'entreprise.

Critères de rédaction d'un PCA : de la logique *« de scénario »* à la logique « *d'indisponibilité des ressources »*

	Approche par scénarii	Approche par indisponibilité de ressources
Base de raisonnement / logique	Se fonde sur l'origine et la cause de la menace	Se fonde sur l'impact et les conséquences de l'indisponibilité de la ressource
Principe	Construction a priori par hypothèses	Construction a posteriori en fonction de la réalité
Approche	Probabiliste/ statistique	Déterministe (indisponibilité des ressources)
Livrables	Plan de continuité d'activité scénarisé et périmétré	Combinaison de solutions de continuité d'activité thématique & graduelle

2.2.1. Indisponibilité des Ressources Humaines

RESSOURCES HUMAINES

La détermination de la question associée à cette problématique se résume à :

« Votre bâtiment est intact, vos systèmes d'informations fonctionnent correctement mais 30% de votre personnel est absent. Que faites-vous ? »

Avec l'apparition de problématiques sanitaires (on pense au SRAS, et plus récemment, à la COVID-19) mais également avec l'essor de problématiques sociales (mouvements politiques ou sociaux), le champ d'application du PCA s'étend désormais à la problématique de raréfaction ou de disparition temporaire de la ressource Humaine.

2.2.2. Indisponibilité des ressources informatiques : le Plan de Secours Informatique

SYSTÈMES D'INFORMATIONS

La détermination de la question associée à cette problématique se résume à :

« Vos systèmes d'informations ne fonctionnent plus, pouvez-vous continuer de travailler, même en mode dégradé ? »

Le Plan de Secours Informatique (PSI) ou Disaster Recovery Plan (DRP) a pour finalité de pallier tout dysfonctionnement technique au niveau de l'infrastructure et des systèmes d'informations (Panne de serveurs informatiques, perte de réseau...)

A ce titre, la mise en place d'un Plan de Secours Informatique (PSI) nécessite des compétences informatiques poussées et une excellente connaissance des systèmes d'informations de l'entreprise. C'est pourquoi ce projet est généralement sous la responsabilité de la Direction des Systèmes d'Informations (DSI) de l'entreprise.

Notons qu'il convient de distinguer le PSI du PCA. Pour mieux comprendre l'articulation entre ces 2 plans, étudions les 2 cas de figures les plus fréquemment rencontrés.

CAS DE FIGURE **#1**

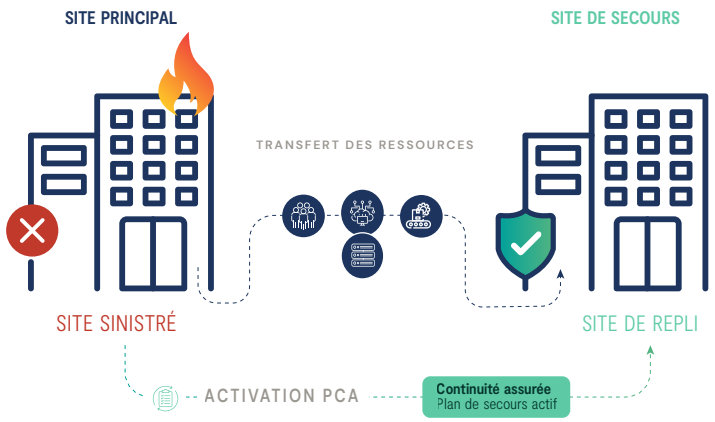
Activation simultanée des 2 plans

Cas où les serveurs informatiques se trouvent dans les locaux des utilisateurs.

Dans ce cas, en cas de destruction des locaux (ex : feu), les serveurs informatiques seront également détruits. De ce fait, il sera nécessaire de déclencher à la fois le PCA et les PSI.

En effet, il sera nécessaire de déplacer les utilisateurs présents dans le bâtiment mais également de « *remonter* » les systèmes d'informations détruits par le sinistre.

Solutions de continuité d'activité :
Transfert de l'ensemble des ressources se trouvant dans le bâtiment



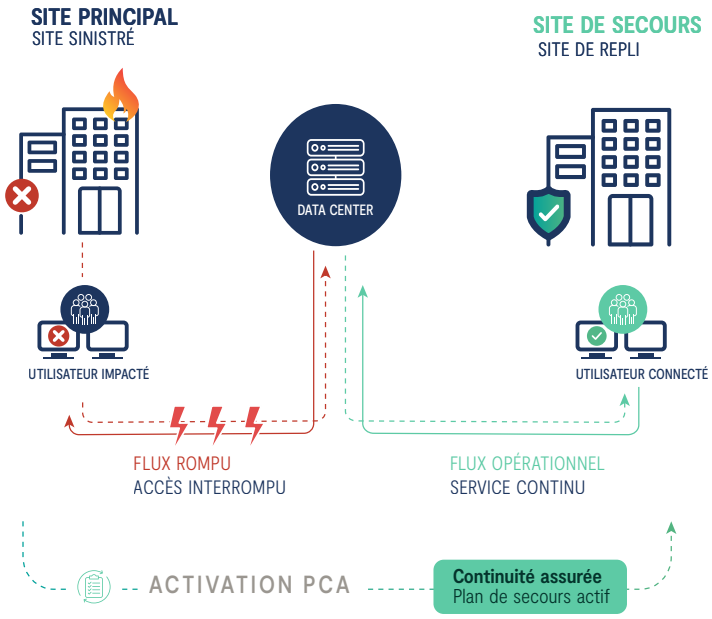
CAS DE FIGURE **#2**

Activation indépendante des 2 plans

Cas où les serveurs se trouvent dans un *« Data center »*, c'est-à-dire dans un lieu disjoint du bâtiment où se trouvent les utilisateurs.

Dans ce cas de figure, les serveurs se trouvent dans un lieu qui leur est réservé, le Data Center. De ce fait, si le bâtiment où se trouvent les utilisateurs est détruit, il est uniquement nécessaire de *« rerouter »* les flux informatiques vers le nouveau lieu d'accueil des utilisateurs. Inversement, si le Data Center dans lequel se trouvent les serveurs informatiques est détruit, le PSI sera déclenché mais non pas le PCA (puisque le bâtiment dans lequel se trouvent les utilisateurs sera épargné par le sinistre).

Solutions de continuité d'activité :
Transfert des ressources constituant l'environnement de travail et reroutage des flux informatiques

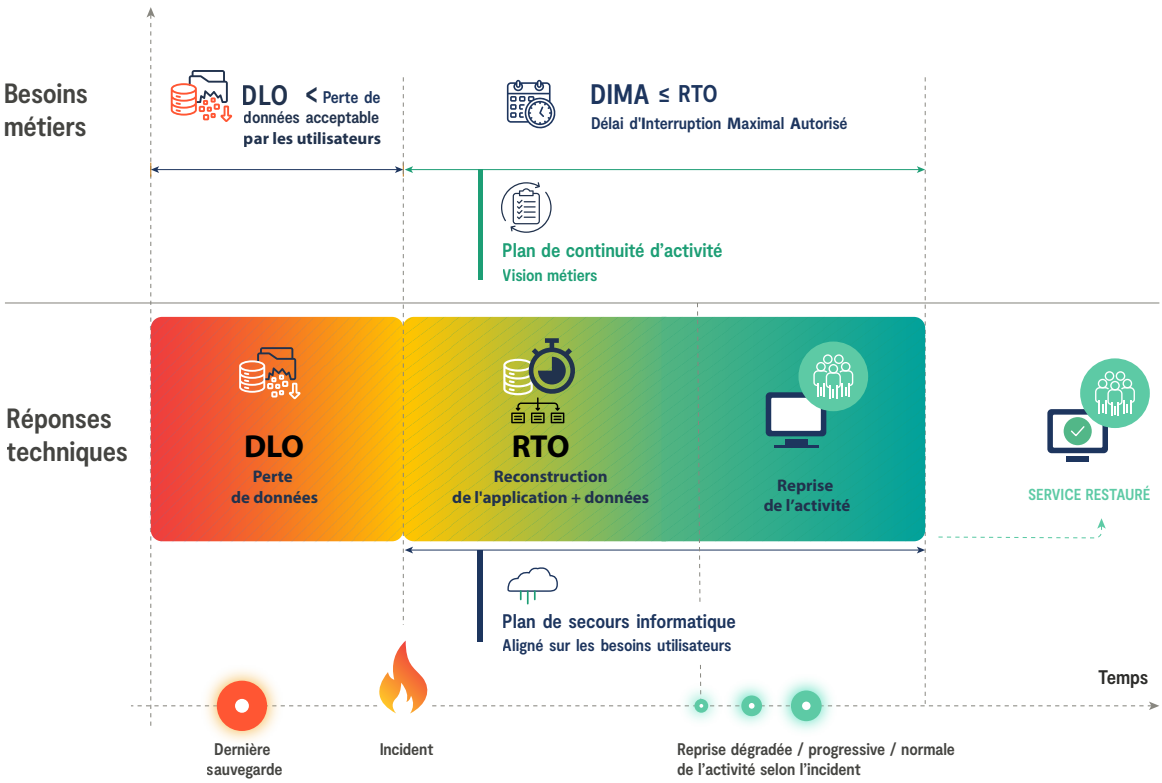


Dans tous les cas de figure (et notamment dans le cas où les serveurs informatiques se trouvent dans les locaux des utilisateurs), il est nécessaire que le Responsable PCA se synchronise avec les équipes informatiques.

→ sur la problématique des délais de redémarrage des applications informatiques que demandent les utilisateurs et qui figurent dans le PCA[4] d'une part et les délais techniques de remise en état des applications et des données associées (*« Recovery Time Objective »*) qui figurent dans le PSI d'autre part.

→ sur la problématique de fréquence de sauvegarde des données informatiques (appelées parfois DLO pour *« Data Loss Objective »* ou RPO pour *« Recovery Point Objective »*). Cet indicateur désigne la durée maximum d'enregistrement des données informatiques qu'il est acceptable pour les utilisateurs de perdre en cas de sinistre.

(4) Généralement appelé *« Durée d'Interruption Maximale Admissible »* (DIMA) des activités: Cf. Chapitre *« Analyse de l'impact de l'arrêt des processus »*



DLO : Data Loss Objective - Perte de données
DIMA : Durée maximale d'interruption admissible
RTO : Recovery Time Objective - Temps de reconstruction de l'application

Autrement dit, si les délais techniques de remise en état des applications et des données associées sont inférieurs à ceux demandés par les utilisateurs, ces derniers pourront utiliser lesdites applications informatiques.

A contrario, si les délais techniques/informatiques de remise en état des applications et des données associées sont supérieurs à ceux demandés par les utilisateurs, ces derniers devront travailler de façon *« dégradée »* c'est-à-dire en l'absence partielle ou totale des outils informatiques mis usuellement à leur disposition.

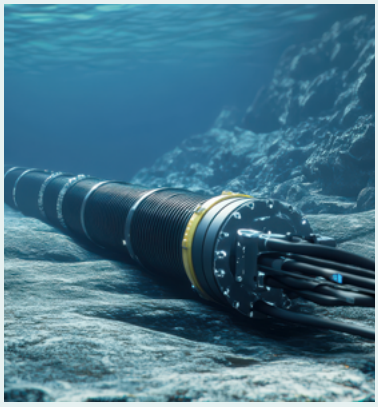
Notons enfin qu'il peut exister deux types d'indisponibilité informatique :

- Indisponibilité de l'*« informatique de gestion »* qui engendre des perturbations au niveau de la gestion des données de l'entreprise d'une part (suspension de l'émission de factures, problème de traitement informatiques de la comptabilité,...) ;
- Indisponibilité de l'*« informatique de production »* pour les entreprises du secteur secondaire qui permet la production industrielle (arrêt de la chaîne de production) d'autre part.

EXEMPLE

Exemple du « *Ping Timeout* » : de la rupture de câbles sous-marin

L'une des perturbations majeures survenues dans le système moderne des télécommunications date de décembre 2006, lorsqu'un séisme de magnitude 7.1 sur l'échelle de Richter a entrainé la rupture de câbles sous-marins entre l'ile de Taïwan et les Philippines, engendrant de facto l'interruption des liaisons de télécommunication entre l'Asie du Sud-Est et le reste du monde. 49 jours de travail ont été nécessaires pour que les connexions, provisoirement réorientées vers d'autres câbles, puissent fonctionner de nouveau. Des incidents similaires ont été constatés en 2008 et en 2013 (rupture de 3 câbles qui ont perturbé l'accès à internet dans une partie du Proche-Orient et de l'Asie).



Plus fréquemment, des entreprises se trouvent privées pour quelques heures ou quelques jours de leurs réseaux informatiques, suite à des accidents divers comme par exemple des arrachements de câbles en proximité des bâtiments lors d'ouverture de tranchées.

Ces exemples, bien que significatifs, illustrent principalement des indisponibilités d'origine accidentelle ou physique qui forment le socle historique du Plan de Secours Informatique (PSI). Cependant, cette approche, bien que nécessaire, ne couvre qu'une partie d'un spectre de risques qui s'est considérablement élargi. Le chapitre 4.1 explorera en détail la nouvelle dimension délictuelle de l'indisponibilité informatique, où la menace n'est plus une défaillance passive mais un adversaire actif et intelligent, redéfinissant en profondeur les exigences de la résilience.

2.2.3. Indisponibilité des ressources matérielles

RESSOURCES MATÉRIELLES

La détermination de la question associée à cette problématique se résume à :

« Votre bâtiment a été détruit cette nuit par un incendie, il est 8h du matin, les salariés arrivent… Que faites-vous ? »

C'est historiquement la disparition ou l'inaccessibilité des bâtiments qui ont poussé à la création des premiers PCA. On a coutume de dire que les premiers PCA en France sont consécutifs à l'incendie du siège du Crédit Lyonnais en 1996 qui a mobilisé 600 pompiers, détruit les deux tiers de l'immeuble et généré plus de 1 milliard de francs de dommages.

2.2.4. Indisponibilité d'un Partenaire

RESSOURCES PARTENARIALES

La détermination de la question associée à cette problématique se résume à :

« Votre fournisseur stratégique est défaillant… Que faites-vous ? »

Dans une recherche permanente de performance, les entreprises sont amenées à faire des choix d'organisation qui les rendent plus vulnérables aux interruptions de process, même mineures. Ainsi, la spécialisation des sites par fonction (mise en place de centre de services partagés sur des processus achat, comptabilité, …), l'externalisation de certaines fonctions, la mutualisation de moyens entre plusieurs entreprises tout comme l'interdépendance plus forte des sites entre eux sont des facteurs aggravants en cas d'arrêt des processus de production. C'est pourquoi les problématiques *« supply chain »*, c'est-à-dire les aspects logistiques et de dépendances aux principaux fournisseurs, doivent être intégrées dans la constitution des PCA.

Au-delà de ces perturbations physiques et logistiques, l'interdépendance avec les partenaires et la chaîne d'approvisionnement (*« supply chain »*) est devenue une surface d'attaque cybernétique de premier plan. Un partenaire peut non seulement être la cible d'une attaque ayant des conséquences indirectes sur l'entreprise, mais également servir de vecteur d'attaque pour l'atteindre. Cette dimension critique, qui lie l'indisponibilité d'un partenaire au risque délictuel informatique, sera approfondie dans le chapitre 4.1.

EXEMPLE

Exemple de la rupture de la « *supply chain* » consécutive aux inondations en Thaïlande

Les inondations en Thaïlande de 2011 furent l'une des catastrophes naturelles les plus coûteuses de ces dernières années : 40 à 50 milliards de dollars de pertes économiques. En effet, elles ont engendré des ruptures de nombreuses chaînes logistiques et d'approvisionnements. Ainsi, ce sont près de 11 000 usines qui ont été inondées entrainant le chômage technique d'un demi-million d'ouvriers. La principale conséquence fut une pénurie massive de composants électroniques à l'échelle mondiale. Elle toucha les principaux fabricants d'ordinateurs et constructeurs automobiles (Toyota et Honda notamment) qui, comme suite à la rupture de leur chaîne logistique, ont subi des baisses significatives de production.

2.2.5. Indisponibilité d'outil de production (machine dans la chaîne de production)

OUTILS DE PRODUCTION

Pour les entreprises du secteur industriel, l'analyse de continuité d'activité doit notamment porter sur les conséquences de l'indisponibilité ou de la destruction de certains outils de production (machines outils, bancs de tests, lignes automatisées, équipements spécifiques). À ce titre, il est essentiel d'identifier les équipements critiques, d'évaluer les possibilités de remplacement ou de réparation, ainsi que les options de déport de production, de mutualisation ou de recours à des modes de production alternatifs.

Dans cette perspective, le PCA constitue également un élément d'attention pour l'assureur dommages aux biens, qui peut en apprécier la robustesse jusqu'au scénario de sinistre majeur voire total, tel que la destruction complète des bâtiments et des équipements à la suite d'un incendie ou d'un événement naturel. La capacité de l'entreprise à limiter les conséquences d'un tel sinistre, à maintenir une activité minimale ou à organiser une reprise structurée constitue alors un facteur clé d'évaluation du risque et de la résilience assurantielle.

Par ailleurs, la continuité d'activité ne se limite pas à la seule gestion de l'indisponibilité des ressources internes. Le PCA doit également intégrer les facteurs aggravants liés à l'environnement de l'entreprise, tels que les contraintes réglementaires ou administratives, les ruptures de chaînes d'approvisionnement, ainsi que les impacts potentiels d'événements naturels, sanitaires ou géopolitiques, susceptibles d'affecter durablement la capacité de production et d'exploitation.

MÉTHODOLOGIE : LA MISE EN PLACE DU PCA EN 5 ÉTAPES

La finalité du présent document est de donner au lecteur les clés de compréhension et de réussite de la mise en place d'un PCA et de l'entretien du dispositif de continuité d'activité afin que ce dernier puisse réaliser de façon autonome son propre dispositif de continuité d'activité.

Chapitr

e 3

Notre méthodologie se structure en 5 phases :

- Phase 1 — Identification des conséquences de l'indisponibilité des ressources
- Phase 2 — Analyse des processus critiques en termes de continuité et identification des besoins en ressources
- Phase 3 — Définition des solutions de continuité d'activité
- Phase 4 — Maintien en conditions opérationnelles du dispositif (dont tests)
- Phase 5 — Communication et sensibilisation (phase transverse)

Chacune de ces *« phases »* est découpée en *« étapes »*. Chaque *« étape »* est découpée en *« action »*.

1 — Identification des conséquences de l'indisponibilités des ressources

Description de l'indisponibilité de la/des ressources et de ses conséquences
- Identifier le périmètre géographique
- Identifier le périmètre fonctionnel
- Identifier le périmètre temporel

2 — Analyse des processus critiques en terme de continuité et identification des besoins en ressources

Identifier les processus et le flux de fonctionnement (en fonction du périmètre de l'étude)
- Identifier et recenser les processus·
- Identifier les dépendances internes entre processus
- Déterminer l'existence de périodes « sensibles »

Analyse de l'impact de l'arrêt des processus
- Etablir une analyse d'impact de l'arrêt des processus et opérer une hierarchisation en fonction de 2 critères :
  – Critère temporel
  – Critère « business »

Identification des besoins en ressources
- Identifier les ressources associées à chaque processus :
  – Hommes, Applications, Données infortmatiques, Utilités...

3 — Définition des solutions de continuité

Identifier les différentes stratégies de continuité d'activités envisageables et attribution d'un ordre de grandeur des coûts associés

Mise en place du PCA et des déclinaisons opérationnelles à l'échelle de chacun des services

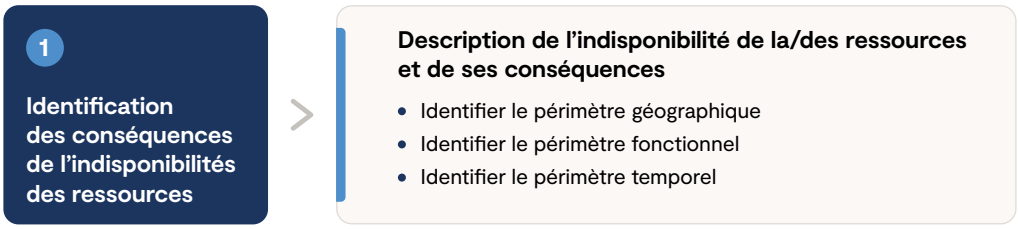
4 — Entretien PCA

Maintien en conditions opérationnelles
- Actualisation du PCA et tests

5 — Communication sur le Projet PCA • Sensibilisation des Dirigeants et des Collaborateurs

Phase 1

3.1. IDENTIFICATION DES CONSÉQUENCES DE L'INDISPONIBILITÉ D'UNE OU DES RESSOURCES



3.1.1. Description de l'indisponibilité de la/des ressources et de ses périmètres

Nous avons vu précédemment que pour fonctionner correctement, une entreprise utilise différentes ressources : les actifs matériels (locaux et outils de production, matières premières, infrastructure informatique, etc.) et les actifs immatériels (main d'œuvre, données, image, etc.). Le dysfonctionnement, l'indisponibilité, la destruction ou la disparition de telle ou telle ressource (Ressources matérielles, Humaines, Systèmes d'informations, ressources partenariales...) est susceptible d'altérer le fonctionnent global de l'entreprise.

La première étape de la réflexion dans le processus de mise en place d'un PCA est donc de s'interroger sur les conséquences de l'indisponibilité, la destruction ou la disparition de telle ou telle ressources au sein de l'entreprise, quelques soient les causes et sans considération de probabilité. C'est donc le critère de l'impact de l'*« indisponibilité de Ressource(s) »* sur le fonctionnement de l'entreprise qui engendre la nécessaire mise en place d'un Plan de Continuité d'Activité.

A ce titre, nous proposons comme définition des évènements nécessitant la mise en place d'un PCA ***« tout évènement indésirable ou situation qui dépasse les capacités de réponse matérielle et/ou organisationnelle d'un ou de plusieurs Services de l'entreprise ».***

Cette définition n'est pas exclusive, elle peut varier en fonction de l'appétence aux risques de l'entreprise et de la volonté de structurer des réponses de continuité a priori, en cas de réalisation d'évènements indésirables.

Pour décrire au mieux chaque type d'indisponibilité et son impact sur les activités de l'entreprise, il est indispensable de déterminer ses périmètres géographique, fonctionnel et temporel.

3.1.1.1. Périmètre géographique

Il s'agit de définir l'étendue géographique de telle ou telle ressource (ou groupe de ressources) c'est-à-dire si l'indisponibilité de la ressource est localisée à l'échelle d'un bâtiment, d'un quartier, ou d'une région. Parfois, un strict périmètre géographique ne peut pas être défini (Cf. supra).

3.1.1.2. Périmètre fonctionnel

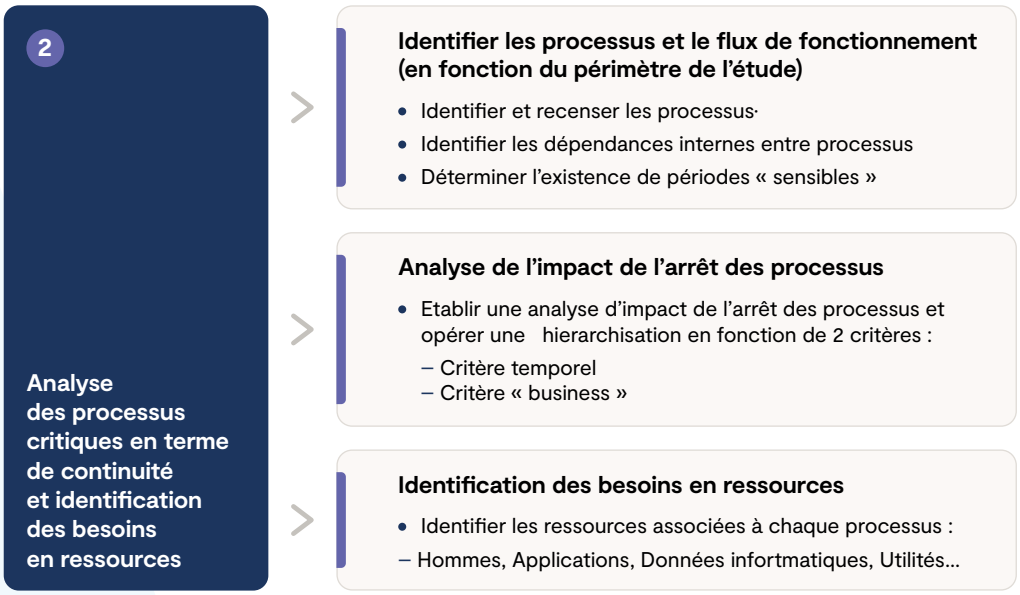
Il s'agit de définir les activités qui seront impactées par l'indisponibilité de la ressource (ou groupe de ressources). Ainsi, l'indisponibilité de la ressource peut perturber de façon homogène toutes les activités de l'entreprise ou a contrario seulement des activités spécifiques. Parfois, un strict périmètre fonctionnel ne peut pas être défini.

3.1.1.3. Périmètre temporel

Il s'agit de définir le laps de temps pendant lequel l'entreprise aura à subir les effets de la réalisation de l'indisponibilité de la ressource. Parfois, un strict périmètre temporel ne peut pas être défini.

Phase 2

3.2. ANALYSE DES PROCESSUS CRITIQUES EN TERMES DE CONTINUITÉ ET IDENTIFICATION DES BESOINS EN RESSOURCES



Rappelons ici les trois actions constitutives de la phase d'analyse des processus en termes de continuité:

- l'identification des processus ;
- l'analyse d'impact de l'arrêt des activités ;
- l'identification des ressources.

L'objectif de continuité ne consiste pas à *« dupliquer »* l'organisation pour permettre une continuité à l'identique, mais d'analyser l'impact de l'arrêt de chacun des processus de l'Organisation et les conséquences associées, d'observer les interactions en interne comme en externe et de procéder à un arbitrage rendu par chaque métier et validé par la Direction Générale [5].

Ainsi, l'analyse de la criticité des activités en termes de continuité et l'identification des besoins en ressources est l'une des phases les plus importantes de la mise en place d'un PCA.

La personne en charge de la collecte desdites données doit planifier des entretiens avec chacun des responsables des Services (que ce soit des lignes Métiers ou des Fonctions support) afin de collecter les informations pertinentes nécessaires à la mise en place d'un PCA.

S'agissant du format et de la durée des entretiens ou des groupes de travail, les choix retenus devront se faire à la lumière de la quantité et de la complexité des données à recueillir d'une part, et en fonction de l'appétence et de la maturité de l'Organisation vis-à-vis des problématiques de gestion des risques d'autre part. Retenons qu'il est nécessaire de trouver le meilleur compromis entre la raisonnable assurance d'avoir recueilli l'exhaustivité des données pertinentes pour le PCA et la durée des entretiens ou des groupes de travail. A titre d'exemple, réaliser une interview trop courte engendre un risque d'oubli ou manque d'informations importantes, réaliser une interview trop longue amputera d'autant le temps de disponibilité de chacun des Chefs de Service lors de la phase opérationnelle de mise en place du PCA.

La méthodologie de recueil d'information, doit être primo connue et partagée à l'échelle de l'équipe projet PCA mais également à l'échelle de chacun des services inclus dans le périmètre du PCA et secundo doit accorder un soin particulier à la collecte, l'implémentation, la centralisation, la formalisation et la compilation des données car c'est à partir des informations recueillies lors de cette phase que seront mises en place les stratégies de continuité d'activité. Pour que ce recueil d'information soit efficace, il convient de formaliser le protocole et de centraliser les propos échangés et les informations collectées au sein d'outils documentaires.

Nous proposons deux outils documentaires pour chacune de ces trois actions (identification des processus et des flux de fonctionnement, analyse de l'impact de l'arret des processus, identification des besoins en ressources) :

- Un protocole d'interview, qui est en fait un *« fil rouge »* d'entretien, un canevas de questions qu'il convient de poser impérativement ;

- Une matrice de recueil d'informations dans laquelle seront formalisées les réponses collectées lors des entretiens.

(5) in *« Gérer les grandes crises : Sanitaires, écologiques, politiques et économiques »*, L CROCQ and al. Odile JACOB, 2009.

3.2.1. L'analyse d'impact de l'arrêt des activités (ou « *Business Impact Analysis* »)

PROTOCOLE D'INTERVIEW EN 5 QUESTIONS CLÉS

L'analyse d'impact de l'arrêt des processus

1 Description des activités : identification des activités

→ « Que faites-vous au quotidien, quelles sont les grandes actions que vous réalisez ? »

2 Durée d'Interruption Maximale Admissible : Evaluation du laps de temps maximal qui peut s'écouler entre l'interruption de l'activité et la reprise totale ou partielle de ladite activité

→ « Combien de temps cette activité pourrait-elle être arrêtée sans générer d'impacts et pourquoi ? »

3 Gravité après DIMA : évaluation de la gravité de l'arrêt de l'activité en fonction de critères et de seuils associés

→ « Quelle est la gravité de l'arrêt de l'activité (après DIMA) ? »

4 Description des interdépendances internes et externes qui permettent le fonctionnement de ladite activité

→ « De quel autre(s) Département(s), autre(s) Services, autre(s) Unités Organisationnelle(s) mais également de quel(s) sous-traitant(s) avez-vous besoin pour réaliser cette activité ? »

5 Identification des périodes critiques

→ « Existe-il une ou des périodes critiques au cours de l'année ? (exemple du closing trimestriel) »

Nota : Le DIMA doit être évalué sur la période la plus critique du processus

FOCUS CYBER

Les critères d'évaluation du BIA doivent être enrichis pour inclure l'impact d'une altération de l'intégrité des données et les effets en cascade sur la chaîne d'approvisionnement (perte de substituabilité, dépendance critique). La cartographie des dépendances tierces (éditeurs, infogérants, fournisseurs cloud, API) doit être formalisée dans le cadre du BIA.

Matrice de recueil d'information *« L'analyse d'impact de l'arrêt des processus »*

→ « Que Faîtes-vous au quotidien, quelles sont les grandes actions que vous réalisez ? »

→ « Combien de temps cette Activité pourrait-elle être arrêtée sans générer d'impacts et pourquoi ? »

→ « Quelle est la gravité de l'arrêt de l'activité (après DIMA) ? »

→ « De quel autre Département(s) ou Unité(s) mais également de quels sous-traitants / prestataires avez-vous besoin pour réaliser cette activité ? »

→ « Existe-t-il une ou des périodes critiques au cours ce l'année ? »

	Description des activités ou processus		DIMA	Impact		Interdépendances		Période(s) critique(s) au cours de l'année							Commentaires
N°	Activités ou Processus	Description/ Observations/	en jours	Business	Image	Dépendance interne (de service à service..)	Dépendance externe (fournisseurs, sous traitants)	Date de début	Durée de la période critique	Autre	Trimestriel	Mensuel	Hebdomadaire	Journalier	
1															
2															
3															
4															
5															
6															
7															

3.2.1.1. Identifier les processus et les flux de fonctionnement

1 Description des activités : identification des activités

→ « Que faites-vous au quotidien, quelles sont les grandes actions que vous réalisez ? »

Définition des termes utilisés

Le vocabulaire utilisé lors de la phase d'identification et de description des processus doit être défini. En effet, une terminologie foisonnante (« *activités* », « *processus* » et autres « *tâches* ») identifie l'ensemble des opérations qui sont réalisées au sein d'une unité organisationnelle. De nombreuses définitions et autant de combinaisons existent : par exemple certains professionnels considèrent qu'une « *activité* » est un ensemble de « *processus* », d'autres proposent de définir un processus comme un ensemble d'activités ou de taches élémentaires.

De ce fait, lors de la mise en place d'un PCA dans une organisation, le chef de projet et le « *Comité PCA* » doivent porter leur effort sur la terminologie employée.

Dans notre propos, nous utilisons indifféremment les termes « *activités* » ou « *processus* ».

Degré de précision dans l'identification et la description des processus

Au-delà de la terminologie, il est nécessaire d'adopter le degré convenable de granularité, c'est-à-dire un niveau de détails des processus qui permette une description exhaustive des opérations présentes dans l'organisation sans que ce travail ne devienne trop chronophage. Ainsi, en moyenne, chaque département gère entre 5 et 15 processus. Un processus peut être défini comme une activité regroupant des ressources humaines, matérielles, informationnelles, qui transforment des éléments entrants en éléments sortants. Chaque « *processus* » devra faire l'objet d'une description lors de l'entretien.

A titre d'exemple et de façon non exhaustive :

Dès lors, comment identifier les processus ?

Les processus RH
- La paie ;
- Le recrutement ;
- La formation ;
- Le droit social ;
- Gestion des frais et avances ;
- Relation avec les instances représentatives du personnel et le comité social et économique (CSE).

Les processus DSI
- Développement / études ;
- Production ;
- Help desk.

Les processus Trésorerie
- Centralisation/optimisation des placements ;
- Relation avec les banques ;
- Réglementation et comptabilisation des flux financiers.

Les processus Comptabilité
- Suivi des comptes ;
- Réception/émissions des factures ;
- Recevoir les factures-fournisseurs, les faire valider pour leur paiement, les comptabiliser et en obtenir le paiement par la Direction de la Trésorerie ;
- Etablir les états financiers ;
- Etablir les déclarations fiscales et assurer le paiement des impôts correspondants.

→ **Cas où l'organisation dispose déjà d'une cartographie/liste des processus**

Il est possible que l'organisation possède déjà une cartographie (ou liste) de ses processus. Ce peut être par le biais d'une certification de type ISO 9000, de la réalisation d'un audit organisationnel ou par l'existence d'une cartographie des risques établie par le prisme des processus (approches généralement utilisées par les Services de Contrôle Permanent, contrôle interne).

→ **Cas où l'organisation ne dispose pas d'une cartographie/liste des processus**

Il sera nécessaire de demander à chacun des responsables la liste des processus de son service. Pour ce faire, la première question à poser lors des entretiens est…

« Que faites-vous au quotidien, quelles sont les actions que vous réalisez ? ».

3.2.1.2. Analyse de l'impact de l'arrêt des processus

2 Durée d'Interruption Maximale Admissible : Evaluation du laps de temps maximal qui peut s'écouler entre l'interruption de l'activité et la reprise totale ou partielle de ladite activité.

→ « Combien de temps cette activité pourrait-elle être arrêtée sans générer d'impacts et pourquoi ? »

3 Gravité après DIMA : évaluation de la gravité de l'arrêt de l'activité en fonction de critères et de seuils associés.

→ « Quelle est la gravité de l'arrêt de l'activité (après DIMA)?»

La finalité de cette étape est d'identifier la sensibilité, en termes de continuité d'activité, des processus présents dans la liste établie lors de l'étape précédente et de hiérarchiser lesdits processus.

Deux critères principaux permettent d'analyser l'impact de l'arrêt des processus :

A / Un critère temporel, la DIMA : évaluation de la *« Durée d'Interruption Maximale Admissible »* (DIMA) des activités.

La *« Durée d'Interruption Maximale Admissible »* (DIMA)[6] d'une activité est la période durant laquelle son interruption n'a pas d'impact, pas de conséquence négative dans la réalisation de l'ensemble des opérations et qui permettent de transformer un *« entrant »* en un *« sortant »*.

Cette DIMA peut être définie en minutes (cas des salles de Marchés), en heures ou en jours, en fonction du secteur d'activité de l'organisation. L'expression de la DIMA se fait généralement en jour(s) calendaire(s).

B / Un critère d'impact, *mesure des impacts consécutifs à l'interruption d'un processus* après DIMA en termes financiers, Humains ou en termes d'image.

Afin de quantifier facilement les impacts de l'arrêt des processus, il est conseillé de créer une échelle de gravité, qui prend la forme d'un tableau à double entrée, dans lequel figurent en abscisse les critères/indicateurs des impacts et en ordonnée les niveaux d'impact (généralement de 1 à 4).

(6) Parfois aussi appelé le *« Délai d'Interruption Maximal Admissible »*

Echelle de gravité

Echelle de gravité			
Seuils	**Gravité financière**	**Gravité image**	**Gravité humaine**
Elevé	> Supérieure à 100 M€	>Médiatisation internationale, dans la presse généraliste et spécialisée, tous supports > Campagne de presse de longue durée, avec suivi de l'événement à moyen/long terme >Perte de crédibilité importante de l'entreprise auprès des actionnaires, des clients, des partenaires financiers, des sous traitants, du personnel et du public, >Baisse importante de la qualité de l'offre, visible par les clients >Impact durable sur la confiance des clients > Impact sur le rating des agences de notation, > Perte partielle ou temporaire d'autorisation d'exercer une activité	> Décès
Intermédiaire	> Entre 10 M€ et 100M€	>Médiatisation nationale , dans la presse généraliste et spécialisée, tous supports >Campagne de presse, d'une durée limitée à quelques jours maximum > Baisse de la qualité de l'offre, visible par les clients > Impact durable sur la confiance des clients > Opportunités manquées de contrats (enjeux importants) sur les activités à l'étranger, du fait notamment de la médiatisation en presse spécialisée	> Blessé grave ou traumatisme nécessitant la mise en place d'une cellule de soutien psychologique
Bas	> Entre 1 M€ et 10M€	> Pas de médiatisation ou très faible, éventuellement limitée aux médias spécialisés >Baisse sensible mais temporaire de la qualité de l'offre de transport, sans impact durable sur la réputation >Opportunités manquées de contrats (enjeux peu importants) sur les activités à l'étranger, du fait notamment de la médiatisation en presse spécialisée	> Blessé léger
Très bas	> Inférieure à 1M€	> Pas de médiatisation	> Pas d'impact

D'un point de vue méthodologique, retenons dans cet exemple que :

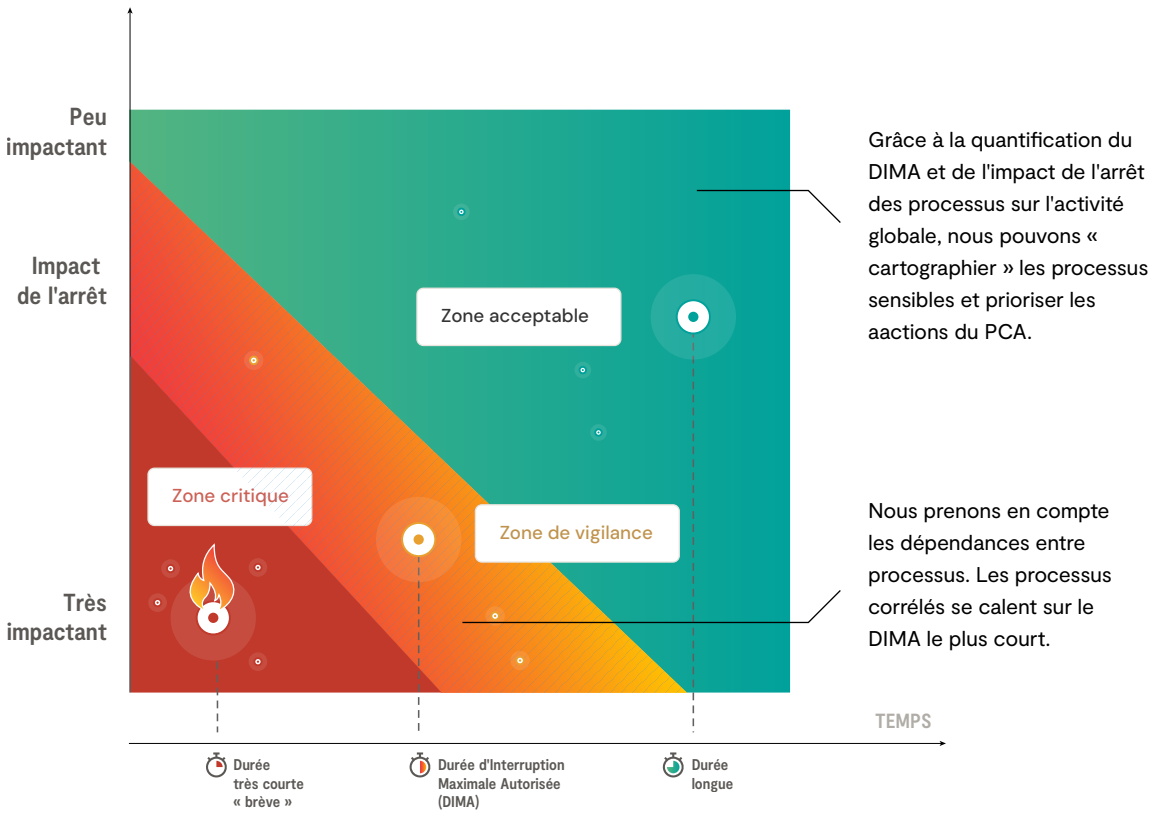
- La mesure de l'impact de l'arrêt des processus est réalisée avec l'hypothèse que le processus ne peut être redémarré pendant un mois complet à compter de la date de l'interruption ;
- La multiplication des critères/indicateurs des impacts engendre une complexification de la matrice. A ce titre, il peut être opportun de se limiter aux critères *« financier »* et *« image »*, les autres critères *« juridique »*,...pouvant être quantifiés financièrement ;
- Les seuils de passage des niveaux d'impacts (généralement de 1 à 4) doivent être mis en perspective avec les résultats financiers de l'organisation ainsi qu'avec ses capacités de trésorerie. A ce titre, cette échelle doit être travaillée et personnalisée selon la surface financière de l'entreprise.

En conclusion, il est bon de rappeler que la finalité de cette étape de l'analyse de l'impact de l'arrêt des processus n'est pas d'obtenir une quantification très *« fine »* des impacts mais plutôt une hiérarchisation de l'impact de l'arrêt des processus, du plus critique au moins critique.

A l'issue de cette analyse il est pertinent de construire une *« cartographie de la criticité des processus en termes de continuité d'activité »* dans laquelle figure en abscisse une échelle des DIMA (des DIMA les plus courtes aux DIMA les plus longues) et en ordonnée les Impacts (Des impacts les plus forts aux impacts les plus faibles).

Cette représentation graphique constitue un support de communication idéal pour sensibiliser un COMEX aux problématiques de continuité d'activité et mettre en perspective les coûts engendrés par la mise en place de stratégie de continuité d'activité.

CARTOGRAPHIE DES PROCESSUS — DIMA & IMPACT DE L'ARRÊT



3.2.1.3. Identifier les processus et les flux de fonctionnement

4 Description des interdépendances internes et externes

→ « De quel autre(s) Département(s), autre(s) Services, autre(s) Unités Organisationnelle(s) mais également de quel(s) sous-traitant(s) avez-vous besoin pour réaliser cette activité ? »

Un processus d'un service peut dépendre d'un autre dans la chaîne de production. La DIMA de l'un doit alors se coordonner avec la DIMA de l'autre. Il est nécessaire d'identifier les interdépendances afin d'arbitrer le choix de la DIMA la plus pertinente.

EXEMPLE

Prenons un exemple : le responsable PCA interroge le Directeur Commercial de sa société, il déclare que l'ensemble des processus dont il est propriétaire peuvent s'interrompre trois jours (DIMA de 3 jours). Il déclare également que l'un de ses processus est dépendant de la validation de la Direction Juridique. Quelques jours plus tard, le RPCA interroge le directeur juridique qui lui annonce que la DIMA la plus courte de son service est de 10 jours.

Un travail de rapprochement des données doit amener le Responsable PCA sur l'inadéquation temporelle de la DIMA du Directeur Commercial (qui fait intervenir la direction juridique et qui est de 3 jours) et la DIMA de la Direction Juridique qui est de 10 jours.

A partir de ce constat, il convient de synchroniser le directeur commercial et le directeur juridique afin qu'ils décident, soit :

- → D'allonger la DIMA du processus 3 de la direction commerciale.
- → De raccourcir la DIMA de la direction Juridique (10 jours → 3 jours).
- → Décider conjointement qu'en cas d'activation, les propositions commerciales ne seront plus relues par la Direction Juridique et seront directement adressées aux clients. Dans ce cas, cette décision doit être avalisée lors d'une session *« Comité PCA »*.

Il convient donc de s'assurer que les *« interdépendances »* aient bien été identifiées, et ce à 2 échelles :

1. INTERDÉPENDANCES INTERNES

- **Echelle intra-Département :**
  Il y a *« interdépendance »* lorsque la bonne réalisation d'une activité *« critique »* nécessite le maintien en condition opérationnelle d'une autre activité au sein du même Service (ou Unité).
- **Échelle inter-Département :**
  Il y a *« interdépendance »* lorsque la bonne réalisation d'une activité *« critique »* nécessite l'intervention d'un autre Service ou Département de l'entreprise.

2. INTERDÉPENDANCES EXTERNES

Il est nécessaire d'identifier les principaux fournisseurs, sous-traitants et prestataires de l'entreprise. Exemple : la Poste et/ou les Société de Coursiers qui acheminent le courrier, le ou les fournisseur(s) d'accès téléphonique....

3.2.1.4. Identifier les périodes critiques au cours de l'année

5 Identification des périodes critiques

→ « Existe-il une ou des périodes critiques au cours de l'année ? (exemple du closing trimestriel) »

Nota : La DIMA doit être évalué sur la période la plus critique du processus

Que ce soit pour préciser les « *clôtures trimestrielles* » (ou « *closing* ») du Service Comptabilité ou pour souligner une période de pic de production ou de vente pour des fonctions Métier (l'impact d'un incendie dans une usine de jouets ne sera pas la même au mois de Novembre qu'au mois de Février), il est nécessaire d'identifier la périodicité des moments critiques (ponctuels, mensuels, trimestriels, semestriels, annuels), la date de début de(s) la période(s) ainsi que sa durée.

3.2.2. Recueil des besoins utilisateurs en termes de Ressources Humaines et matérielles

PROTOCOLE D'INTERVIEW EN 2 QUESTIONS CLÉS

Les besoins utilisateurs en termes de Ressources Humaines et matérielles

3.2.2.1. Recueil des Ressources Humaines

1 Identification des besoins en Ressources Humaines (compétences et volumétrie) : identification jour par jour des besoins Humains et mise en place d'un planning RH de reprise de l'activité

→ « De qui avez-vous besoin et au bout de combien de temps ? »

La matrice *« Identification des besoins en Ressources Humaines en termes de continuité d'activité »* permet d'identifier pour chaque processus :

- → Les personnes qui possèdent des compétences uniques ou des délégations de pouvoir.
- → Le nombre de personnes nécessaires à la reprise de l'activité, et ce jour par jour.

3.2.2.2. Recueil des Ressources Matérielles

2 Identification des besoins matériels : identification jour par jour des besoins matériels

→ « De qui avez-vous besoin et au bout de combien de temps ? »

Nous ne pouvons pas ici établir une liste exhaustive de l'ensemble des moyens matériels nécessaires à la reprise de l'activité. En effet, en fonction de l'activité, les ressources requises varieront (informatique dans le secteur tertiaire, machine-outil pour une chaîne industrielle de montage...).

A ce titre, nous ne représentons pas ici de matrice.

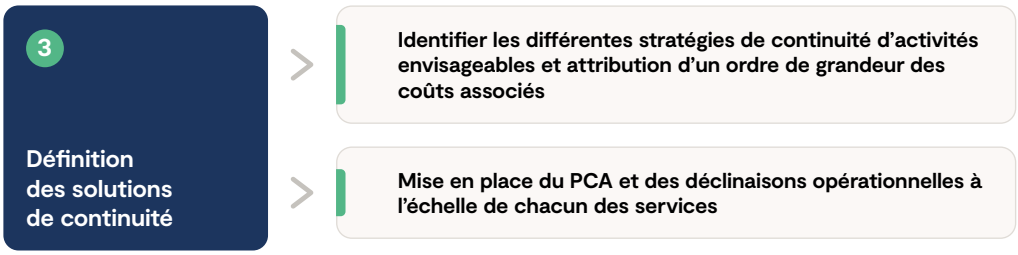
Matrice de recueil d'information « *Identification des besoins en Ressources Humaines en termes de continuité d'activité* »

Nombre total de personnes prenant part à la réalisation des processus listés ci-dessous (en "équivalent Temps plein")	

	Description des activités ou processus		DIMA	Impact		Ressources Humaines	Planning Ressources Humaines de Reprise d'activité *(valeur en "équivalent Temps Plein")*										Commentaire
N°	Activités ou Processus	Description/ Observations/	(in jours)	Business	Image	Compétence Unique ou Délégation de Pouvoir	ASAP	12H	24H ou 1 jour	2 jour	3 jour	5 jour	10 jour	15 jour	20 jours	30 jours	
1			0	0	0												
2			0	0	0												
3			0	0	0												
4			0	0	0												
5			0	0	0												
6			0	0	0												
7			0	0	0												
8			0	0	0												
9			0	0	0												
10			0	0	0												
11			0	0	0												
12			0	0	0												
13			0	0	0												
14			0	0	0												
15			0	0	0												
16			0	0	0												
17			0	0	0												
18			0	0	0												
19			0	0	0												
20			0	0	0												
						TOTAL	0	0	0	0	0	0	0	0	0	0	
						Réserve de personnel	0	0	0	0	0	0	0	0	0	0	

Phase 3

3.3. DÉFINITION DES SOLUTIONS ET DES STRATÉGIES DE CONTINUITÉ D'ACTIVITÉ



3.3.1. La définition des solutions

Le temps de l'analyse est maintenant terminé, les processus critiques et les besoins de continuité d'activité des services sont connus, il est temps de rechercher les différentes stratégies de continuité d'activité qu'il est possible de mettre en œuvre ainsi que d'identifier les coûts associés pour chacune d'entre elles.

Pour ce faire, une recherche tout azimut de solutions de continuité doit être réalisée : appels d'offres auprès de prestataires de services (salles de repli), devis pour achat de matériels (serveurs de back up....). Les résultats de cette recherche sont généralement documentés au sein d'un dossier qui identifient les diverses réponses possibles en termes techniques, matériels et organisationnels. Il présente et explicite les points forts et les points faibles de chacune des différentes stratégies. De ce fait, certaines d'entre elles pourront être abandonnées (pour des raisons de coût notamment) et d'autres pourront être approfondies.

Par ailleurs, ce document constitue le support à la validation définitive de la stratégie de continuité et à l'édification des solutions de continuité.

Veuillez trouver ci-après quelques représentations graphiques (7) qui présentent les principales stratégies de continuité pour chacune des problématiques abordées par le PCA.

(7) Les représentations graphiques ont été réalisées par Chloé Sibilat et Francesca Serio, élèves du master *« Gestion Globale des Risques et des Crises »* Paris 1 Sorbonne.

Problématiques d'indisponibilités de locaux

* Un aléa climatique d'ampleur régionale peut rendre simultanément indisponibles le site principal et le site de repli, soit par exposition directe, soit par indisponibilité des infrastructures et des accès.

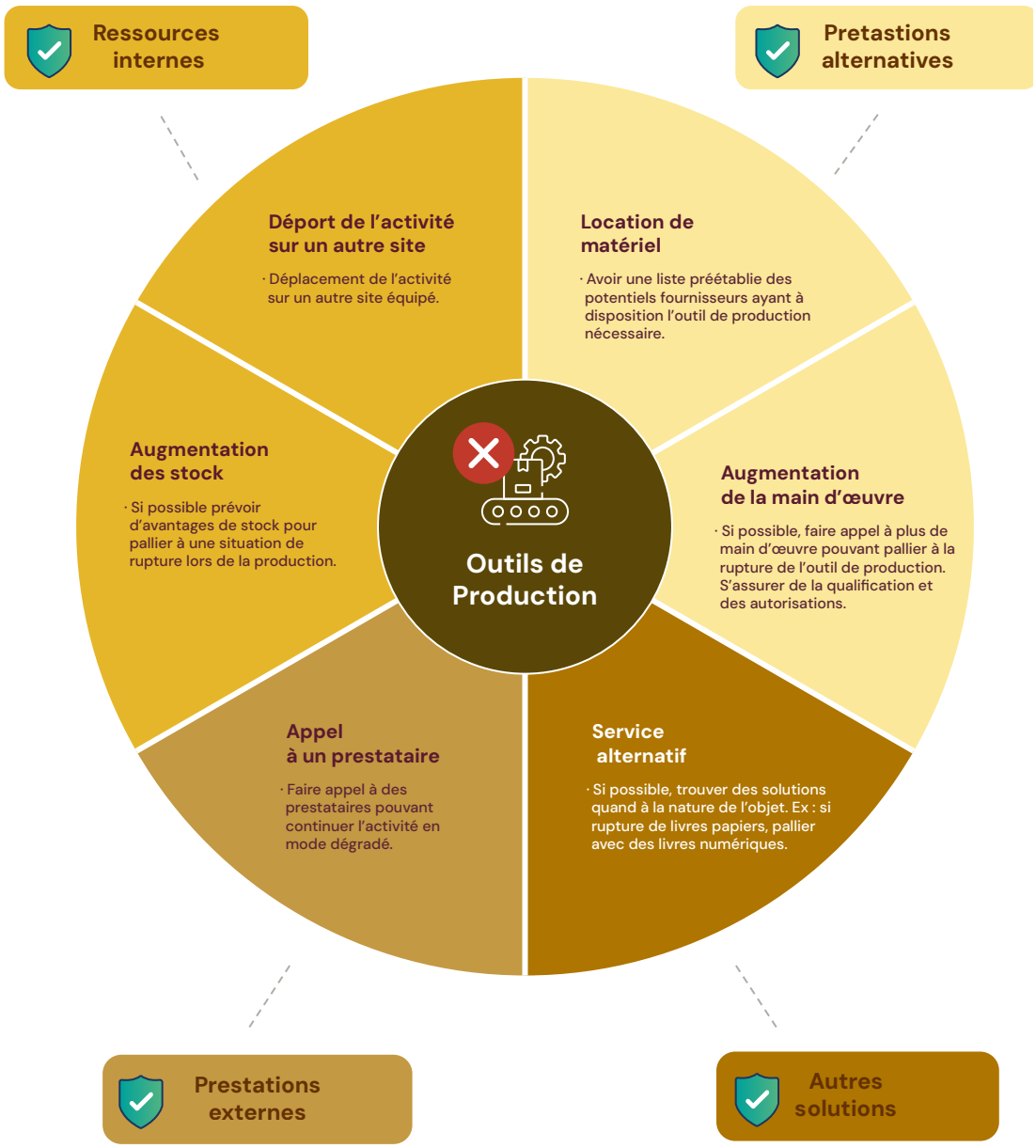
Problématiques d'indisponibilités de Ressources Humaines

* Dans le scenario d'un aléa climatique, les ressources humaines peuvent être simultanément impactées par le même aléa, en raison de difficultés de déplacement, de contraintes personnelles ou de l'indisponibilité des infrastructures de leur lieu de résidence.

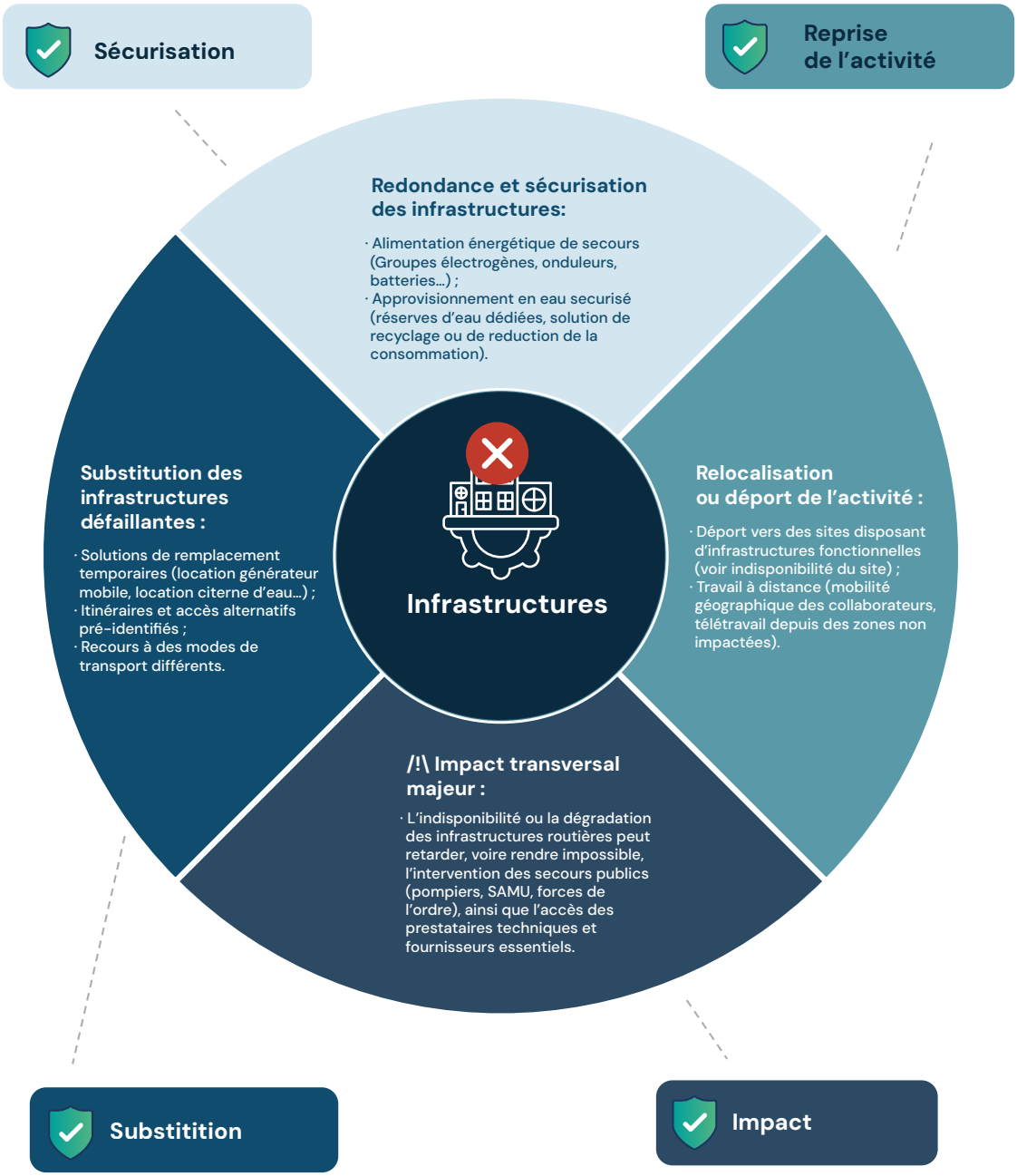
Problématiques d'indisponibilités des Systèmes d'Informations

Problématiques d'indisponibilités de fournisseur(s)

Problématiques d'indisponibilités d'un outil de production



Problématiques d'indisponibilités des infrastructures



3.3.2. Mise en place du PCA

3.3.2.1. La mise en place du *« Plan de Continuité d'Activité »*

Le Plan de Continuité d'Activité prend la forme d'un ensemble de documents formalisés et régulièrement mis à jour, **de planification des actions à mettre en place suite à la survenue d'une catastrophe ou d'un sinistre grave. Il fixe les modalités matérielles, techniques et organisationnelles du fonctionnement en mode *« dégradé »* de l'activité de l'entreprise et de reprise graduelle des activités, des plus sensibles aux moins sensibles.**

A ce titre le Plan de Continuité d'Activité propose donc une organisation alternative que l'entreprise applique, le temps de remédier à l'événement perturbateur à l'origine de l'arrêt des processus et facilite **la reprise graduelle des processus critiques** de l'entreprise (des plus sensibles au moins sensibles) et la mobilisation des ressources associées au regard de la Durée d'Interruption Maximale Admissible (DIMA) et à la gravité de l'arrêt des processus.

Il prend la forme d'un schéma d'ensemble présentant les modalités matérielles, techniques et organisationnelles permettant la reprise de l'activité [8] ainsi que l'ensemble des dispositions de continuité d'activité communes à l'ensemble des services tels que les procédures d'activation des salles de repli, les *« plans de reroutage courrier » et « plans de reroutage téléphonique »* doivent figurer dans ce document. Cet ensemble est complété par des documents de synthèses et graphiques opérationnels : diagramme de Gantt, planning des besoins en ressources humaines sous forme de tableau Excel....

Cet ensemble de documents permet d'acquérir **une visibilité globale et optimale du pilotage opérationnel du PCA** en cas de déclenchement du dispositif.

3.3.2.2. Déclinaison des solutions opérationnelles pour chacun des départements

Le document *« Plan de Continuité d'Activité »* est une synthèse à compléter par des fiches opérationnelles de continuité d'activité à l'échelle de chacun des services (une fiche par service). Ces fiches doivent être simples, claires intégrant si besoin des graphiques et revêtir un formalisme unique et commun à l'ensemble des services.

D'un point de vue méthodologique, le responsable du PCA prendra soin de pré-remplir l'ensemble des fiches avec les informations recueillies lors des phases d'analyse précédentes et de hiérarchiser les processus par ordre de redémarrage, des DIMA les plus courtes aux plus longues. Une application simple de type *« Macro Excel »* permettra d'automatiser la compilation et la concaténation des données en provenance des différentes feuilles.
En complément, un entretien doit être programmé avec chaque responsable de service pour décrire la manière avec laquelle il compte redémarrer chaque processus. Ils feront figurer la liste des actions qui en permettront le redémarrage.

A ce titre, il est nécessaire de sensibiliser les directeurs de services (ou les correspondants PCA) sur leurs responsabilités dans la mise en place de solutions de continuité d'activité et de leur rappeler l'impérieuse nécessité de documenter leur propre politique de continuité d'activité, en cohérence avec le niveau global. Ainsi, la bonne connaissance et la bonne implémentation de la documentation de continuité d'activité par les responsables de service sont des gages d'efficacité dans le pilotage opérationnel de la reprise de l'activité.

(8) Notons également que certains RPCA fractionnent la reprise de l'activité en 3 temps et incluent à ce titre des dispositions d'urgence (fiche actions reflexes), de reprise d'activité (reprise de l'activité sur un site de repli par exemple) et de retour à la normale (retour sur le site nominal après la période de reprise d'activité sur le site de repli).

Phase 4

3.4. MAINTIEN EN CONDITIONS OPÉRATIONNELLES, ACTUALISATION DES PLANS DE CONTINUITÉ D'ACTIVITÉ ET TESTS / SIMULATION

3.4.1. Actualisation des PCA

Le PCA doit être maintenu en conditions opérationnelles. Il doit être actualisé régulièrement afin d'être efficient dès la survenue de la crise. L'actualisation des PCA doit permettre de prendre en compte les changements techniques, fonctionnels, organisationnels de l'entreprise mais également l'évolution des contraintes réglementaires et des choix technologiques de l'entreprise.

La mise à jour du PCA consiste à vérifier l'adéquation des solutions existantes avec les exigences de continuité.

3.4.2. Test / Simulations

A l'instar de la gestion de crise, les bonnes procédures se testent par le biais d'exercice de simulation. Ces exercices permettent d'éprouver la qualité de la documentation, le fonctionnement des équipements techniques mais également la connaissance et la maitrise des personnes qui les utilisent. En mettant en situation les collaborateurs, les responsables PCA peuvent ainsi évaluer le niveau de connaissances, de compétences et le comportement des collaborateurs et procéder à d'éventuels ajustements. Enfin, la fréquence de ces exercices permet de rappeler à l'esprit des parties prenantes que la crise peut survenir et qu'il faut se tenir prêt à l'affronter.

On peut tester le plan de gestion de crise d'un côté et le PCA de l'autre mais également tester la coordination de la mise en œuvre des deux.

EXEMPLE

Exemple de scénario d'exercice de crise qui permet de tester le PCA : une inondation soudaine empêche l'accès au bâtiment A. La cellule de crise est mobilisée dans une salle de crise dite *« secondaire »* à l'extérieur du bâtiment, et décide de déclencher le PCA. Dès lors, les collaborateurs devant se rendre dans la salle de repli (ou *« salle de back-up »*) s'exécutent et s'y présentent selon l'ordre et les modalités opérationnelles décrites dans le document PCA. Un ou des membres dédié(s) de la cellule de crise supervise la dimension logistique et accueille les collaborateurs. Ils se mettent réellement à travailler en salle de repli, le cas échéant en mode *« dégradé »*, et ainsi testent le *« bon »* fonctionnement » du PCA. De leur côté, les membres de la cellule de crise contrôlent la situation et veillent au redémarrage de l'activité tout en répondant également à des sollicitations de journalistes et de parties prenantes de l'entreprise.

Phase 5

3.5. MAINTIEN EN CONDITIONS OPÉRATIONNELLES, ACTUALISATION DES PLANS DE CONTINUITÉ D'ACTIVITÉ ET TESTS/ SIMULATION

5

Communication sur le Projet PCA
- **Sensibilisation des Dirigeants et des Collaborateurs**

Au *« cœur »* de l'organisation, le chef de projet PCA doit être doté de réelles qualités de communication. La dimension transverse de sa mission l'amène à rencontrer des collaborateurs de tous niveaux hiérarchiques : des fonctions support aux unités de production.

3.5.1. Le principe du *KISS*

Il est donc absolument nécessaire de mettre en place, en parallèle du déroulement technique du projet, des actions de communication, de sensibilisation et de formation afin de doter l'entreprise d'une culture de la continuité d'activité. Cette communication peut prendre différentes formes : films, quizz, pastiches de jeux TV (*« money drop »*), etc.

Le leitmotiv étant ici le principe du KISS :
« Keep It Simple and Sexy » (« faisons simple et sexy »)

LES CYBER-ATTAQUES : LES NOUVELLES PROBLÉMATIQUES DU PCA

Chapitr


e 4

4.1. LES RESSOURCES INFORMATIQUES : DE L'ACCIDENTEL AU DÉLICTUELLE

4.1.1. Cyber-Attaque, de quoi parle-t-on ?

Une attaque informatique peut prendre plusieurs formes :

Le défacement de site internet externe	→ Cette menace moins fréquente de nos jours a principalement un impact d'image.
DDOS (indisponibilité de sites institutionnels)	→ De manière identique, il s'agit principalement d'un risque d'image avec peu d'impact opérationnel
DDOS (indisponibilité de sites métiers)	→ Ce type d'attaque est plutôt rare mais a connu un fort retentissement fin 2025 avec l'attaque du groupe la Poste qui a perturbé la distribution des colis et rendu indisponible l'accès à l'application de gestion des comptes de la Banque Postale pour les clients. Ce type d'attaque touche la vitrine numérique d'une entreprise mais ne remet pas en cause l'intégrité de son informatique interne.
Les attaques au « *Président* »	→ Une attaque au président consiste à usurper l'identité ou l'autorité d'un dirigeant afin de tromper des collaborateurs et détourner les fonds d'une entreprise. Avec les nouveaux risques liés à l'IA, cette fraude s'appuie désormais sur des deepfakes vocaux ou vidéo et des messages hyper-personnalisés générés automatiquement, rendant la manipulation plus crédible et difficile à détecter. Il s'agit d'une attaque de type ingénierie sociale (et non pas réellement Cyber).
Les attaques de réputation (fausse attaque informatique)	→ Une attaque par réputation consistant à inventer une fausse cyberattaque vise à faire croire que l'entreprise a subi une faille de sécurité grave, afin de semer le doute sur sa fiabilité. En diffusant de fausses informations ou de faux rapports techniques, les auteurs cherchent à nuire à l'image de marque et à provoquer une perte de confiance des clients et partenaires.
La « *perte* » de données personnelles	→ Les attaques visant à voler les données personnelles des clients consistent à infiltrer les systèmes d'une entreprise pour extraire des informations sensibles comme les identités, adresses ou données bancaires. Les cybercriminels utilisent ensuite ces données pour de la fraude, de l'usurpation d'identité ou les revendre sur des marchés illégaux, causant des dommages importants aux clients comme à la réputation de l'entreprise.

L'accès à des données confidentielles par des tiers	→ Ce type d'attaque consiste à pénétrer ses systèmes pour récupérer des informations stratégiques comme des plans, brevets, procédés internes ou données de R&D. Ces données sensibles sont ensuite exploitées pour obtenir un avantage concurrentiel, affaiblir l'entreprise ou les revendre à des acteurs malveillants ou concurrents.
Intrusion et destruction du système informatique interne (Ransomware, Wiper...)	→ Une attaque de type ransomware chiffre les données de l'entreprise et bloque l'accès à ses systèmes, puis exige une rançon pour rétablir la situation. Un wiper, lui, détruit définitivement les données au lieu de les chiffrer, causant une interruption majeure et souvent irréversible de l'activité. Ces types d'attaques peuvent être complétés par un vol des données de l'entreprise et la menace de les publier si aucune rançon n'est payée, ajoutant une pression supplémentaire et un fort risque de réputation.

Ce dernier type d'attaque se définit par la déstabilisation immédiate et majeure du fonctionnement courant d'une organisation (arrêt des activités, impossibilité de délivrer des services, pertes financières lourdes, perte d'intégrité majeure, etc). C'est donc un évènement à fort impact, qui ne saurait être traité par les processus habituels et dans le cadre du fonctionnement normal de l'organisation.

Repenser les métriques de résilience : du RTO au RIO

L'un des principaux risques mis en évidence par ce chapitre tient à la décorrélation entre les métriques traditionnelles de résilience, historiquement centrées sur les délais de reprise technique (RTO), et la réalité des crises majeures impliquant une perte de confiance dans les données. Dans ce type de situation, la remise en service des systèmes ne suffit pas : tant que l'intégrité et la fiabilité des données ne sont pas établies, la capacité réelle de l'organisation à reprendre ses activités demeure limitée.

Il est dès lors essentiel que les responsables des risques et de la résilience utilisent ces concepts pour faire évoluer le dialogue avec les comités exécutifs et les conseils d'administration. Le reporting ne peut plus se limiter à des indicateurs de type RTO, mais doit intégrer une réflexion plus qualitative autour du RIO (Recovery of Integrity Objective), c'est à dire le temps nécessaire pour restaurer la confiance opérationnelle et décisionnelle dans les données.

Cette approche gagne à s'appuyer sur des scénarios concrets et compréhensibles au niveau de la gouvernance. Par exemple : **quel serait l'impact pour l'entreprise d'une indisponibilité prolongée de son ERP, non pas en raison d'une panne technique, mais du temps requis pour vérifier, réconcilier et certifier l'intégrité des données avant toute reprise effective ?**

4.1.2. Le changement de paradigme et l'obsolescence du Plan de Secours traditionnel

Le Plan de Secours Informatique (PSI), tel que décrit précédemment, constitue le fondement historique de la résilience des systèmes d'information. Conçu pour répondre à des événements accidentels (panne matérielle, rupture de câble, incendie d'un centre de données etc.), son objectif est de restaurer une capacité de fonctionnement dans un délai défini (RTO) avec une perte de données acceptable (RPO). Cette approche reste indispensable, mais elle est devenue fondamentalement inadaptée pour faire face à une nouvelle classe de menaces : l'adversaire délictuel.

Le PSI prépare l'organisation à se remettre d'un événement statique et circonscrit ; il est en revanche mal équipé pour gérer une intrusion dynamique et persistante menée par un acteur intelligent et malveillant. La nature du risque a changé : il ne s'agit plus d'une défaillance passive, mais d'une compromission stratégique active. Par conséquent, la confiance exclusive dans un PSI traditionnel peut engendrer un dangereux sentiment de fausse sécurité. Un PSI suppose que les données à restaurer sont intègres et que le périmètre du sinistre est connu. Or, un acteur malveillant qui obtient un accès administrateur au cœur du système d'information ne cherche pas seulement à provoquer une interruption ; il vise à exfiltrer, voire à altérer subtilement les données. Dans ce contexte, restaurer une sauvegarde récente pourrait signifier réintroduire un système déjà compromis.

Cette situation révèle une défaillance de gouvernance critique. Une organisation qui s'appuie uniquement sur son PSI pourrait estimer son temps de reprise à 48 heures, alors que la réalité, face à une compromission de l'intégrité des données, peut être un arrêt de production d'un mois. Cette dissonance entre la résilience perçue, souvent mesurée par des métriques RTO simplistes, et la réalité de la reprise constitue un angle mort stratégique pour de nombreuses directions.

4.1.3. Anatomie d'une cyber-crise systémique : une étude de cas

Pour illustrer ce changement de paradigme, l'incident survenu en septembre 2025 chez un constructeur automobile mondial de premier plan offre un cas d'étude édifiant. Cet événement n'a pas été un simple incident technique, mais un *« choc systémique »* qui a paralysé l'ensemble de ses opérations mondiales et provoqué des répercussions mesurables sur l'économie nationale.

DU COMPOSANT DÉFAILLANT AU SYSTÈME NÉVRALGIQUE COMPROMIS

La nature systémique de cette crise dépendait moins de la sophistication de l'outil d'attaque que de la criticité de l'actif ciblé. Les attaquants n'ont pas visé un système périphérique, mais le *« cerveau numérique »* de l'entreprise : son progiciel de gestion intégré (ERP) SAP, qui orchestre la production, la finance et la logistique au niveau mondial. Le vecteur d'attaque initial n'était pas une vulnérabilité inconnue de type *« zero-day »*, mais l'exploitation de deux failles critiques publiquement documentées (CVE-2025-31324 et CVE-2025-42999), pour lesquelles des correctifs

étaient disponibles depuis plus de quatre mois. L'incident ne résulte donc pas d'une fatalité technologique, mais d'une défaillance dans les processus fondamentaux d'*« hygiène cyber »* et de gestion des vulnérabilités. Ne pas appliquer un correctif sur un système aussi central, face à une menace aussi clairement identifiée, n'est pas une simple négligence opérationnelle ; c'est un manquement stratégique.

L'ARRÊT STRATÉGIQUE : UN NOUVEAU DÉCLENCHEUR POUR LA CONTINUITÉ D'ACTIVITÉ

L'arrêt complet et mondial de la production pendant un mois n'a pas été le résultat direct de l'attaque, comme un chiffrement par rançongiciel. Il s'agissait d'une *« mesure de confinement défensive délibérée »*, une décision stratégique prise par la cellule de crise de l'entreprise. Cette stratégie de la *« terre brûlée »* a été jugée indispensable pour atteindre deux objectifs vitaux : premièrement, stopper l'exfiltration massive de données (environ 350 Go de propriété intellectuelle) et, deuxièmement, prévenir un risque encore plus grand : le pivot de l'attaquant du réseau informatique (IT) vers l'environnement des technologies opérationnelles (OT). Une compromission des systèmes de contrôle industriel sur les chaînes de montage aurait pu permettre le sabotage physique de la production ou la création d'incidents de sécurité graves.

Cette réalité inverse la logique traditionnelle du PCA. Habituellement, un PCA est activé par un événement externe qui cause une indisponibilité (incendie, inondation). Ici, le déclencheur a été une décision interne, proactive, prise pour prévenir un scénario pire, mais qui n'était à ce stade que potentiel. Le PCA doit donc désormais être conçu non seulement comme un catalogue de réponses à des sinistres avérés, mais aussi comme un plan d'action pour gérer les conséquences d'une décision stratégique de la cellule de crise. Le PCA est activé par la cellule de crise, et non plus seulement pour elle.

LA PRIMAUTÉ DE L'INTÉGRITÉ DES DONNÉES : L'AVÈNEMENT DU RECOVERY INTEGRITY OBJECTIVE (RIO)

La raison pour laquelle la reprise a nécessité un mois entier ne réside pas dans la complexité de la reconstruction des serveurs, mais dans le défi bien plus ardu de la *« validation et de la réconciliation de l'intégrité des données »* au sein de l'ERP compromis. Ayant obtenu un contrôle administratif total, les attaquants auraient pu subtilement altérer des enregistrements critiques : niveaux de stock, ordres de paiement, nomenclatures de produits. Redémarrer la production mondiale avec des données non fiables aurait été un risque commercial inacceptable.

Cet impératif fait émerger un nouveau concept qui supplante les métriques traditionnelles : le **Recovery Integrity Objective (RIO)**, ou Objectif d'Intégrité de la Reprise. Il s'oppose au classique **Recovery Time Objective (RTO)**.

→ Le RTO pose la question : **« En combien de temps pouvons-nous être de nouveau opérationnels ? »**.

→ Le RIO, quant à lui, demande : **« À partir de quel moment pouvons-nous de nouveau faire confiance à nos données et à nos processus ? »**.

Dans le cas d'une compromission systémique, le RIO devient la métrique dominante. Atteindre le RIO transforme la reprise d'une tâche informatique en un audit forensique à grande échelle, nécessitant des compétences différentes (experts en juricomptabilité, analystes de données) de celles d'une équipe de restauration classique. Les organisations doivent donc anticiper cette réalité en incluant dans leur PCA un *« Plan de Validation des Données »* qui identifie à l'avance les sources de confiance externes et les expertises nécessaires.

4.2. L'ÉCOSYSTÈME COMME CHAMP DE BATAILLE : LE DILEMME DE LA CHAÎNE D'APPROVISIONNEMENT

L'impact de la cyberattaque ne s'est pas limité aux frontières de l'entreprise. La chaîne d'approvisionnement a joué un double rôle : celui de victime et celui de vecteur de la menace.

4.2.1. L'effet domino : la chaîne d'approvisionnement comme victime

L'arrêt de la production a mis en péril environ 200 000 emplois au sein de l'écosystème de la chaîne d'approvisionnement. De nombreux fournisseurs, dont l'activité dépendait quasi exclusivement du constructeur, ont été contraints de procéder à des licenciements. La situation a été aggravée par la mise hors ligne des systèmes de paiement, provoquant une crise de liquidité aiguë chez ces partenaires. L'onde de choc a été si violente qu'elle a nécessité une intervention étatique sans précédent : le gouvernement britannique a dû accorder une garantie de prêt de 1,5 milliard de livres sterling pour éviter une vague de faillites en cascade. Cet événement démontre qu'une cyberattaque contre une entité d'importance systémique est une menace pour la sécurité économique nationale.

4.2.2. Le cheval de Troie : la chaîne d'approvisionnement comme vecteur

La chaîne d'approvisionnement est de plus en plus reconnue comme un vecteur de menace majeur, une tendance confirmée par des agences comme l'ENISA et l'ANSSI. Deux principaux scénarios d'attaque émergent :

- **La compromission d'un partenaire** (mouvement latéral) : Les attaquants ciblent un fournisseur ou un prestataire de services, souvent moins bien sécurisé, pour exploiter les accès et les relations de confiance qu'il entretient avec sa cible principale ;
- **La compromission d'un produit ou service** (attaque de la chaîne d'approvisionnement logicielle) : Cette approche consiste à injecter du code malveillant directement dans un produit, un composant ou une mise à jour logicielle fournie par un tiers.

L'hyper-intégration des chaînes d'approvisionnement modernes, optimisées pour une efficacité maximale via des modèles *« juste-à-temps »*, a involontairement créé un vecteur de contagion du risque tout aussi efficace. La résilience de l'écosystème impose donc un changement de paradigme : il ne s'agit plus seulement d'optimiser chaque maillon, mais d'assurer la stabilité de l'ensemble, quitte à sacrifier une part d'efficacité au profit de la robustesse.

4.3. SPÉCIFICITÉ D'UNE CRISE CYBER DE TYPE RANSOMWARE PAR RAPPORT AUX AUTRES INDISPONIBILITÉS CLASSIQUES

En comparaison à d'autres types de crise, les crises cyber de type ransomware ont des caractéristiques propres qu'il est important d'appréhender :

→ **Le diagnostic initial est souvent incertain.**
- Les systèmes touchés sont inaccessibles ou partiellement paralysés, ce qui empêche d'identifier immédiatement l'étendue réelle de l'intrusion. De plus, les attaquants masquent volontairement leurs traces, rendant difficile de savoir si des données ont été exfiltrées, combien de machines sont compromises ou si d'autres menaces dormantes sont encore actives.

→ **Une attaque peut continuer à se propager pendant l'activation du PCA.**
- Soit car l'attaquant est toujours actif et va s'adapter aux mesures de cantonnement mises en place par l'entreprise ;
- Soit car même si un système est sain, l'entreprise peut faire le choix de le couper volontairement afin d'en assurer l'intégrité en attendant d'avoir une meilleure vision sur la situation.

→ **Une absence d'unicité de lieu de réalisation.**
- Potentielle propagation à d'autres organisations en raison de l'interconnexion des SI auxquels sont associés les systèmes d'information de l'organisation et ceux de ses prestataires.

→ **Les outils de gestion de crise peuvent être indisponibles.**
- Que ce soit pour la documentation ;
- Ou les moyens de communication (Messagerie, messagerie instantanée, annuaire…).

→ **Les besoins de collecte de preuve et de communication sont présents avec des délais de déclaration contraints** auprès des différents organismes (Autorités, assureurs…). Cette contrainte existe avec d'autre type de crise mais ce qui est spécifique ici est le manque d'outil et de référentiels disponibles pour le faire (indisponibilité des outils informatiques usuels).

→ **Des temps de rétablissement difficile à estimer.**

→ **La reconstruction du SI** peut être : partielle, progressive et incertaine avec de possibles retours en arrière et une incertitude sur la qualité des données.

→ **Une dépendance forte à des experts techniques** (rares…).

→ **La compromission peut dater de plusieurs mois en arrière** avec la nécessité d'avoir la capacité de reconstruire un système sain sans garantie d'avoir des sauvegardes exploitables (compromises, effacées, non utilisables…).

4.4. VERS UN CADRE INTÉGRÉ DE CYBER-RÉSILIENCE

Le PCA et le PSI, tels que traditionnellement conçus, sont des outils nécessaires mais insuffisants face à un adversaire actif et intelligent. La réponse ne réside pas dans un plan unique, mais dans la décomposition des silos et l'orchestration de trois fonctions distinctes mais interdépendantes : la Gestion d'Incident, la Gestion de Crise et la Continuité d'Activité.

- **La Gestion d'Incident (réponse technique)**

→ Assurée par les équipes techniques (SOC, CERT/CSIRT), son rôle est de détecter, analyser, contenir et éradiquer la menace au niveau des systèmes. C'est le combat tactique, mené sur une échelle de temps de quelques minutes à quelques heures.

- **La Gestion de Crise (pilotage stratégique)**

→ Menée par la cellule de crise (direction, juridique, communication), elle prend les décisions stratégiques à fort impact (ex: *« Faut-il arrêter la production mondiale ? »*) et gère les parties prenantes. Elle opère sur une échelle de temps de quelques heures à quelques jours.

- **La Continuité d'Activité (reprise opérationnelle)**

→ Exécutée par les équipes métier, elle met en œuvre les solutions du PCA pour faire redémarrer les activités critiques, une fois que la cellule de crise a stabilisé la situation. Son échelle de temps s'étend de quelques jours à plusieurs semaines.

Une cyber-crise systémique exige une chorégraphie parfaite de ces trois fonctions, comme l'illustre le tableau suivant. Ce tableau fournit une carte visuelle d'un processus complexe, permettant à différentes équipes de comprendre leur rôle et leurs interdépendances à chaque phase de la crise, passant d'actions en silo à une réponse coordonnée.

Phase de la Crise	Gestion d'Incident Cyber (Objectifs & Actions Clés)	Gestion de Crise (Objectifs & Actions Clés)	Continuité d'Activité (Objectifs & Actions Clés)
1 Préparation	Préparer les outils de détection/réponse (SIEM, EDR). Élaborer des plans de réponse technique (playbooks). Entraîner les équipes.	Constituer et former la cellule de crise. Préparer les plans de communication. Identifier les parties prenantes.	Élaborer et tester les PCA/PSI. Réaliser les BIA. Mettre en place les solutions de secours (sites, données).
2 Détection & Alerte	Détecter l'anomalie. Qualifier l'alerte. Déclencher l'alerte vers la cellule de crise.	Activer la cellule de crise. Évaluer l'impact métier initial. Déclencher la communication interne.	Mettre les équipes de continuité en pré-alerte. Vérifier la disponibilité des ressources de secours.
3 Confinement & Investigation	Isoler les systèmes compromis. Analyser les modes opératoires de l'attaquant. Préserver les preuves numériques.	Suivre l'évolution de l'impact métier. Prendre des décisions de confinement à plus large échelle (ex: couper l'accès internet).	Évaluer l'impact de l'incident sur les stratégies de continuité prévues.
4 Décision Stratégique	Fournir des rapports techniques factuels à la cellule de crise.	Décider des mesures radicales (ex: arrêt de la production). Valider et diffuser la communication externe. Gérer les régulateurs.	Adapter les plans de reprise en fonction des décisions de la cellule de crise.
5 Reprise & Validation	Éradiquer la menace. Reconstruire les systèmes de manière sécurisée. Surveiller le retour à la normale.	Piloter la stratégie de reprise globale. Gérer la communication sur la reprise.	Déclencher le PCA. Migrer les activités sur les solutions de secours. Valider l'intégrité des données (RIO) avant le redémarrage.
6 Post-Crise & REX	Analyser les causes profondes. Produire un rapport forensique détaillé.	Mener un REX stratégique. Gérer les conséquences à long terme (juridiques, réputationnelles).	Mener un REX opérationnel. Mettre à jour les BIA et les PCA sur la base des leçons apprises.

4.5. RECOMMANDATIONS DE MISE EN ŒUVRE : FAIRE ÉVOLUER LA MÉTHODOLOGIE DU PSI*

La PSI doit définir les ressources nécessaires au fonctionnement de l'activité et à une reprise ordonnée et structurée de l'IT

- À la fois au niveau de l'infrastructure, des services support et des applications ;
- Tester sa capacité à restaurer ou/et reconstruire les différentes briques (AD, services techniques, applications...) ;
- Tester sa capacité à disposer de stations de travail non infectés ;
- Confronter les temps de restauration/ reconstruction avec la priorisation faite ;
- Disposer de capacités de communication hors du SI => capacités à utiliser régulièrement sinon elles seront inutilisables le jour J ;
- Concevoir des exercices intégrés : Dépasser les tests de reprise informatique en silo. Concevoir et mener des simulations à grande échelle qui impliquent simultanément l'équipe de réponse technique aux incidents, la cellule de crise stratégique et les équipes de continuité d'activité, en utilisant des scénarios complexes comme une attaque sur l'intégrité des données ;
- Intégrer des tests de *« données compromises » (dirty data)* : Pendant les exercices, tester la capacité des équipes à détecter qu'une sauvegarde restaurée contient des données subtilement altérées, validant ainsi leurs capacités à atteindre le RIO.

→ **La PSI doit garantir une reprise IT testée, cohérente avec les priorités métiers et assurant l'intégrité des données.**

*PSI : Plan de Secours Informatique

4.6. LISTES DES ÉLÉMENTS SUPPLÉMENTAIRES À POSSÉDER À LA FIN DE LA DÉMARCHE DE MISE À JOUR DE SON PCA POUR COUVRIR LE RISQUE CYBER

- Une **liste priorisée des infrastructures et applications à reconstruire**, en prenant en compte les dépendances (applicatives, de données, de version, etc.) nécessaires à la reconstruction.

- Des **fiches réflexes** par métier et par rôle.

- Des **procédures dites *« bouton rouge »***, qui visent à isoler rapidement des segments du SI (en formalisant les impacts opérationnels de ces isolations) et procédures *« bouton vert »* pour mettre en place rapidement l'environnement de réponse à la crise et de continuité.
  - Idéalement, ces procédures peuvent inclure une automatisation dans leur exécution.

- Une **procédure de reconstruction spécifique à chaque application / infrastructure critique** (reconstruction de zéro, copie, restauration de sauvegarde, etc.), en prenant en compte :
  - Les **spécificités technologiques** de la solution à reconstruire ;
  - Les **moyens de récupérer les sauvegardes saines** et les données nécessaires, ainsi que les interconnexions minimales.

- La **stratégie de test unitaire**.

- La stratégie de tests intégrés (simulations à grande échelle qui impliquent simultanément l'équipe de réponse technique aux incidents, la cellule de crise stratégique et les équipes de continuité d'activité).

- Une **stratégie d'acculturation des collaborateurs et de communication du plan de continuité**, notamment sur le cadre normatif, qui précisent les règles en vigueur et les bonnes pratiques à appliquer aux collaborateurs.

FOCUS RISQUES TIERS

La gestion du risque Tiers

La maitrise du risque fournisseur passe par :

1 Identification et classification des fournisseurs

- Cartographier tous les prestataires en fonction de leur rôle, des services qu'ils fournissent et de leur criticité pour l'activité (impact sur la continuité, sécurité, données sensibles) ;
- Prioriser les fournisseurs selon leur importance (ex : fournisseurs critiques vs secondaires).

2 Due diligence avant contractualisation

- Faire des évaluations de risques avant de signer avec un fournisseur : sécurité, conformité, solidité financière, dépendances ;
- Vérifier les certifications, audits de sécurité, posture cyber, continuité d'activité, etc ;
- Ajouter des critères de sécurité et résilience dans les appels d'offres et les choix.

3 Clauses contractuelles robustes

- Inscrire dans les contrats des **clauses d'audit et d'accès aux informations**, des engagements de niveau de service (SLA), des droits de supervision et des KPIs de résilience ;
- Prévoir des **plans de sortie / exit strategies**, des mécanismes de substitution et des obligations en cas de défaillance ;
- Contrôler les droits de sous-traitance et les flux de données sensibles.

4 Surveillance continue en exploitation

- Mettre en place un **monitoring des performances et des risques** tout au long de la relation ;
- Réévaluer régulièrement la criticité et les impacts en cas d'évolution de services ou d'environnement ;
- Intégrer alertes et indicateurs permettant de détecter des dégradations.

5 Plans de continuité et de reprise

- S'assurer que les fournisseurs ont aussi leurs propres plans de continuité cohérents avec les besoins de l'entreprise ;
- Tester la résilience via des scénarios (pannes, incidents majeurs, rupture de service).

6 Information et capitalisation des incidents

- En cas d'incident impliquant un fournisseur, documenter, analyser et reprendre les enseignements pour éviter la récidive dans d'autres relations.

7 Avoir conscience que même si une prestation est externalisée, c'est l'entreprise elle-même qui reste responsable de la conformité globale et de la gestion des risques associés. Ce dernier point est par exemple une exigence formulée dans le règlement DORA.

FOCUS DÉLAI DE RÉTABLISSEMENT

Que faire si le RIO annoncé n'est pas compatible avec les objectifs métiers ?

1

PROPOSER AUX MÉTIERS COMMENT CONTINUER À OPÉRER SANS IT OU SANS IT NOMINAL :

- Procédures manuelles ou semi-manuelles ;
- Outils bureautiques de secours (Excel, formulaires, mails) ;
- Traitements différés avec rattrapage a posteriori ;
- Périmètre fonctionnel réduit (clients prioritaires, opérations essentielles).

→ À formaliser dans un PCA métier, pas seulement IT.

2

PRIORISATION FORTE ET PÉRIMÈTRE RÉDUIT

- Proposer une remise en service partielle (fonctions vitales seulement) ;
- Identifier un socle minimal
- Définir ce qui ne sera pas restauré immédiatement.

Message clé : *« On ne restaure pas tout, mais on restaure l'essentiel plus vite »*.

3

SOLUTIONS DE SECOURS ALTERNATIVES

Selon les cas :

- Applications ou plateformes de secours disponible sur un autre environnement technique (même moins performantes) ;
- Recours temporaire à un prestataire externe,
- Bascule vers un outil tiers ou groupe (si groupe multi-entités) ;
- Duplication de certaines données clés hors SI principal.

FOCUS SAUVEGARDE

La stratégie de sauvegarde, pilier du PSI

Les règles de sauvegardes doivent être construites dans le contexte d'une reconstruction cyber. Les éléments sous-jacents à l'infrastructure (binaires, versions, configuration, etc.) sont notamment **à documenter**, et cette documentation doit être protégée. L'ordonnancement et l'automatisation sont des solutions qui peuvent permettre d'industrialiser ces étapes pour les environnements virtualisées, cela sera plus difficile sur des infrastructures physiques ou propriétaires.

Par ailleurs, l'existence de sauvegarde n'est pas un critère suffisant pour réussir la reconstruction. Il est nécessaire de considérer

- Leur **profondeur** (pour s'assurer de l'existence de sauvegarde suffisamment lointaine pour que l'attaquant n'y soit pas présent) ;
- Leur **protection** (pour éviter la destruction par l'attaquant, par exemple via des mécanismes d'immutabilité ou un stockage out-of-band) ;
- Leur **compatibilité** (notamment le besoin de synchronisation entre différentes systèmes).

Enfin, il est nécessaire de penser à rationaliser les éléments sauvegardés en fonction de la sensibilité et l'importance dans le processus de reconstruction, pour éviter de "polluer" ce dernier avec un surabondance de sauvegardes peu utilisables.

Il faut établir une **cible de systèmes d'information** (au travers de la stratégie de bulle de redémarrage, voir plus bas), pérenne et saine et capable d'être disponible et protégée en cas de crise cyber. Selon les modalités des applications à reconstruire et de l'organisation, un environnement primaire, externalisé voire Cloud peut être considéré.

Une fois la cible définie, il est nécessaire de construire une **stratégie de tests complète**. En effet, une organisation avec des processus et des outils fera face à des problèmes si la reconstruction n'a pas été testée en amont. Cette stratégie doit s'appuyer sur des tests unitaires de chaque brique de l'infrastructure, mais également sur des tests de l'ensemble de la chaine de valeur métier pour assurer que cela fonctionnera au moment de la reconstruction.

FOCUS LA BULLE DE CONFIANCE

Bulle de confiance et/ou bulle de redémarrage ?

C'est un réseau isolé du SI infecté à partir duquel la reconstruction du SI est susceptible d'être réalisée. Cette reconstruction se fait une un socle de confiance, dans lequel ne sont déployer dans un premier temps que les services vitaux à l'organisation.

Selon les stratégies des entreprises, cette bulle de confiance peut être mise en place à partir de systèmes neuf (ex: installation d'un nouvel Active Directory) ou à partir de restauration de sauvegardes non compromises.

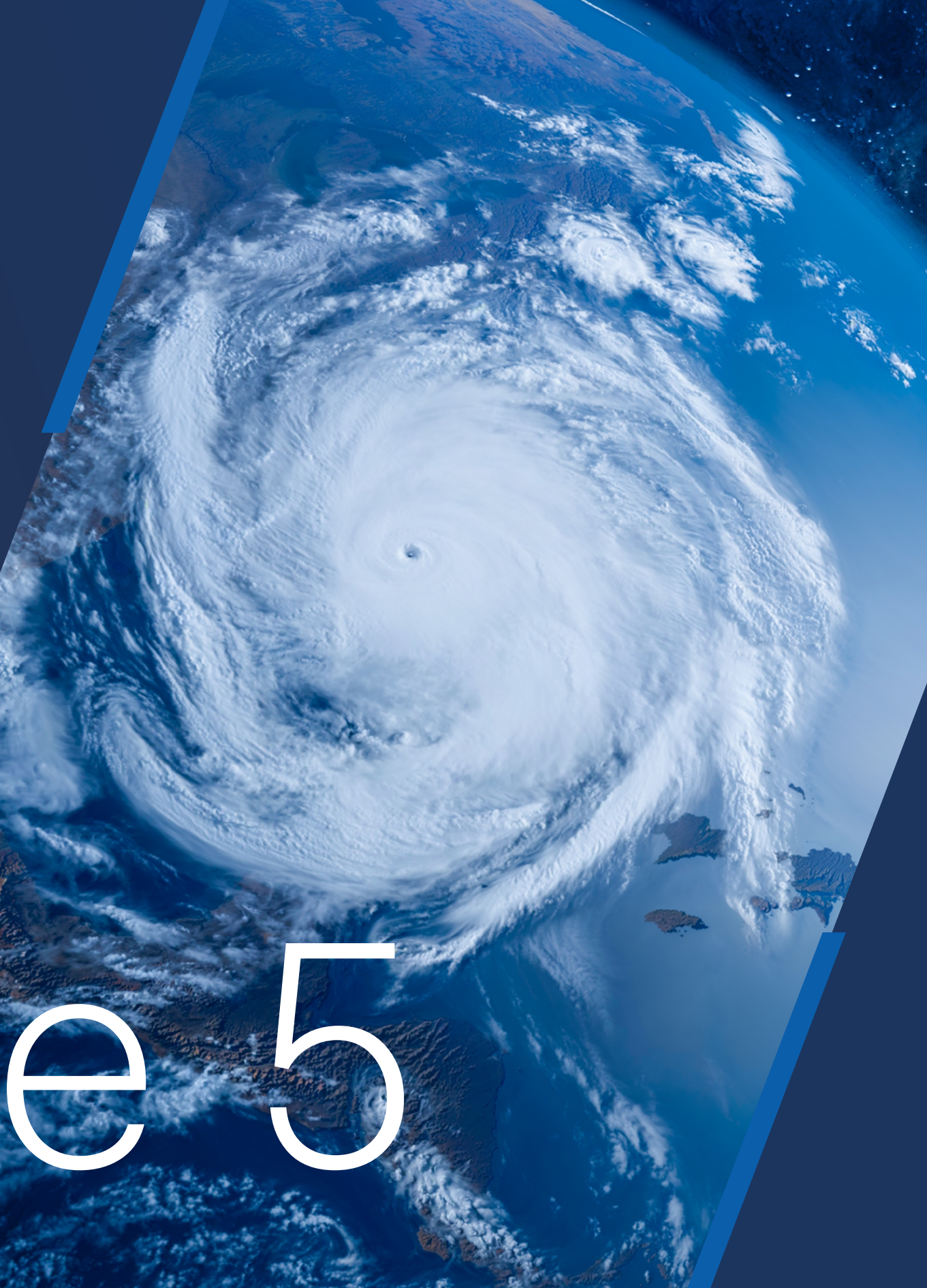
Pour permettre le maintien de la confiance dans ce réseau isolé, il convient de penser à:

- Limiter les éléments déployés au strict minimum du fonctionnement des services vitaux, notamment sur les aspects d'authentification et de réseau ;
- S'assurer du bon niveau de sécurité des éléments déployés, notamment vis-à-vis des vulnérabilités utilisées pour la compromission initiale du SI ;
- Mettre en place une supervision accrue sur le SI pour vérifier du non-retour de l'attaquant.

L'IMPACT DU CHANGEMENT CLIMATIQUE SUR LES PCA : L'URGENCE À PRENDRE EN COMPTE

La montée en fréquence et en intensité des crises climatiques transforme profondément la manière dont les organisations doivent envisager leur continuité d'activité. Les événements récents ont démontré que ces crises dépassent largement les scénarios classiques d'indisponibilité, en touchant simultanément les infrastructures, les ressources humaines, les réseaux et les chaînes d'approvisionnement. Dans ce contexte, le Plan de Continuité d'Activité (PCA) doit évoluer vers une approche systémique, intégrant étroitement l'analyse de risque, la coordination avec les autorités locales et une anticipation renforcée des interdépendances critiques.

Chapitr


e 5

5.1. CRISE CLIMATIQUE : REPENSER SON PCA À TRAVERS UNE APPROCHE SYSTEMIQUE DE L'ENTREPRISE

Les crises climatiques se distinguent fortement des indisponibilités classiques par leur ampleur géographique, leur effet cumulatif et leur capacité à perturber simultanément de multiples ressources critiques.

Les inondations en Allemagne et en Belgique (2021) ont entrainé la destruction simultanée d'infrastructures, coupures prolongées d'électricité, impossibilité d'accès à de larges zones industrielles. Les vagues de chaleur extrême en France et en Angleterre en 2022 ont entrainé la surchauffe des datacenters, ralentissement des chaînes logistiques, et l'indisponibilité du personnel. Ces situations démontrent la nécessité d'une analyse systémique incluant interdépendances, infrastructures locales, énergies disponibles et étendue géographique potentielle de la crise.

Lors de la construction du PCA, il est donc indispensable d'adopter une approche systémique intégrant :

- les chaînes de dépendances critiques ;
- les vulnérabilités locales (infrastructures, énergies, voies d'accès) ;
- la zone géographique potentiellement affectée par l'évènement climatique ;
- les effets domino entre ressources, sites et infrastructures.

Cette analyse est une étape préalable essentielle pour éviter que les stratégies de continuité envisagées ne soient elles-mêmes rendues inopérantes par le même événement climatique.

Ainsi, quelle que soit l'ampleur ou l'étendue géographique de la crise, les processus critiques de l'organisation doivent pouvoir perdurer ou redémarrer dans les délais impartis. Nous utilisons le terme de *« fractale »* pour définir un niveau de résilience homogène, quelle que soit l'échelle géographique retenue. Cette notion implique que la continuité d'activité doit rester robuste, que la perturbation touche un seul site, un ensemble de sites régionaux ou tout un territoire national.

Le niveau de réponse de l'entreprise doit être identique quelle que soit l'échelle géographique de la crise.

- d'un lieu circonscrit : la perte d'un bâtiment dans un incendie ;
- d'une maille géographique : le bassin versant de la Seine en cas de crue de la Seine ;
- d'un pays / état : l'ouragan Katrina qui a frappé l'état de Louisiane ;
- d'une zone : la tempête Boris en septembre 2024 qui a provoqué des inondations dévastatrices dans les pays de l'Est de l'Europe ;
- du monde entier : épisode pandémique à la COVID-19 de 2020.

En conséquence, sécuriser la continuité d'activité de l'entreprise à n'importe quelle échelle géographique » impose de mesurer le niveau d'insertion et de dépendance au territoire, local, départemental, régional, national, afin de comprendre comment les vulnérabilités du territoire peuvent se propager jusqu'aux activités critiques de l'organisation. Cette compréhension conditionne la capacité à concevoir des stratégies réellement résilientes, capables d'absorber ou de contourner les effets d'une crise climatique, quel qu'en soit le périmètre.

5.2. RÉÉVALUER LES STRATÉGIES DE CONTINUITÉ À L'AUNE DU RISQUE CLIMATIQUE

Une crise climatique peut invalider des options de continuité pertinentes dans des situations classiques. Il est donc nécessaire de réexaminer les mesures existantes du PCA, notamment :

→ VALIDATION DE LA DISPONIBILITÉ DES SITES DE REPLI

Un site de secours situé dans la même zone géographique risque d'être affecté par l'événement climatique. Lors de la tempête Xynthia (2010), plusieurs sites côtiers de repli envisagés par des entreprises ont été rendus inaccessibles en raison d'inondations simultanées dans toute la zone littorale.

Il est recommandé de :
- vérifier systématiquement l'exposition climatique du site de repli ;
- prévoir un site alternatif géographiquement dissocié ;
- documenter les critères de sélection (altitude, réseaux, accès, exposition).

→ GESTION DES RESSOURCES HUMAINES EN SITUATION DE CRISE CLIMATIQUE

Les membres de la cellule de crise peuvent être touchés professionnellement et personnellement.

Le passage du cyclone Garance sur l'île de La Réunion, le 28 février 2025, a montré de manière très concrète à quel point les membres d'une cellule de crise peuvent être touchés à la fois professionnellement et personnellement. L'événement a provoqué des vents dépassant les 200 km/h, des pluies exceptionnelles—par endroits plus de 500 mm en quelques heures—ainsi que de lourds dégâts sur les infrastructures essentielles : routes coupées, habitations détruites, centaines de milliers de personnes privées d'eau, d'électricité ou d'Internet. Dans ce contexte, plusieurs professionnels mobilisés pour gérer la crise ont vu leur propre situation personnelle gravement affectée. Certains ont perdu leur maison ou se sont retrouvés dans l'impossibilité de se déplacer en raison des routes effondrées ou inondées. Ainsi, Garance démontre qu'en situation de catastrophe climatique majeure, les membres d'une cellule de crise ne sont pas uniquement des acteurs mobilisés pour la continuité de l'organisation : ils sont aussi des habitants du territoire, exposés et vulnérables, confrontés aux mêmes pertes et traumatismes que le reste de la population. Cette réalité nécessite d'intégrer systématiquement des backups humains, une organisation flexible, ainsi que des scénarios de crise prenant en compte l'indisponibilité soudaine ou prolongée de personnes clés.

Il est indispensable de :
- prévoir des backups opérationnels pour chaque rôle clé de la cellule de crise ;
- organiser une polycompétence minimale sur les fonctions critiques ;
- intégrer l'indisponibilité des membres de la cellule de crise dans le PCA.

L'habitabilité d'un territoire est un point à prendre en compte dans les PCA suite à un évènement extrême comme un séisme, l'ouragan, inondation dévastatrice. Les ressources humaines nécessaires à l'activité n'auront plus de logement, de moyens de transport. Pour assurer la continuité d'activité, l'entreprise pourra prendre la décision de mettre à disposition un service de transport, louer des véhicules ou reloger les salariés et leur famille à proximité de l'activité.

Source : Podcast les coulisses de la Com de crise, Communiquer en pleine tempête : RETEX du Cyclone Garance – 04/12/2025

5.3. ÉVALUER LA RÉSILIENCE DE LA CHAINE D'INTERVENTION

Dans le cadre du BIA (Business Impact Analysis) et de la définition des RTO/RPO, il est nécessaire de prendre en compte les vulnérabilités des fournisseurs critiques et des prestataires impliqués dans la continuité (ex. entreprise de nettoyage, réparation toiture, pompage...),

Prenons le cas des inondations à Valence en Espagne en Octobre 2024 (DANA, Depresion Aislada en Niveles Altos) :

À la fin du mois d'octobre 2024, la région de Valence est frappée par une DANA d'une intensité exceptionnelle. En l'espace de quelques heures, plus de 400 mm de pluie s'abattent sur les provinces de Valence, Alicante et Castellón, provoquant des destructions massives d'infrastructures, l'inondation de quartiers entiers et un bilan humain dépassant les deux cents victimes. Les dégâts matériels, estimés à près de 29 milliards d'euros, témoignent de l'ampleur du sinistre, devenu l'une des catastrophes climatiques les plus graves de l'histoire récente de l'Espagne.

Dans les heures et jours qui suivent, les organisations publiques et privées tentent d'activer leurs plans d'urgence. Cependant, la combinaison d'une zone d'impact très étendue et d'une destruction simultanée des infrastructures essentielles entraîne une saturation rapide des prestataires spécialisés : pompage, assèchement, rétablissement électrique, IT, nettoyage industriel ou logistique lourde. Les entreprises locales ne parviennent plus à répondre à la demande, tandis que plusieurs axes routiers endommagés bloquent l'accès à certaines zones.

Cet épisode fournit un enseignement majeur pour les organisations : lors d'une crise climatique à large périmètre, les prestataires locaux deviennent rapidement indisponibles, même lorsqu'ils sont théoriquement contractuellement engagés à intervenir. Pour les Risk Managers, cette réalité impose de repenser le PCA en intégrant des fournisseurs alternatifs situés hors de la zone d'exposition, en ajustant les RTO pour tenir compte de délais d'intervention fortement allongés et en anticipant l'indisponibilité simultanée de ressources critiques. L'exemple de Valence souligne ainsi la nécessité d'une résilience de chaîne d'intervention, au delà de la résilience interne de l'entreprise.

Dans ce contexte, pour sécuriser davantage la continuité des activités essentielles, il peut etre pertinent d'établir des partenariats avec des spécialistes de l'après sinistre. Cela peut passer par la mise en place de contrats préétablis avec des entreprises expertes dans la remise en état, afin de garantir une intervention rapide en cas de dommages importants. Il est également possible de formaliser des accords de priorité d'intervention, permettant à l'organisation d'être traitée en premier lors d'une crise affectant un grand nombre de clients. Enfin, la réalisation d'audits préalables avec ces prestataires contribue à accélérer leur mobilisation le jour de l'événement, en clarifiant en amont les modalités techniques, les accès aux sites et les besoins spécifiques de l'entreprise.

Structurer un dispositif d'alerte climatique

La mise en place d'un système d'alerte precoce et graduel permet d'anticiper les événements climatiques et de déclencher en amont les mesures du PCA. Cette anticipation réduit les impacts opérationnels en sécurisant les personnes, les actifs et les installations avant la crise. Elle facilite l'activation rapide de solutions de repli et la coordination des équipes. En s'appuyant sur des seuils d'alerte définis et des sources fiables, l'organisation gagne en réactivité. Résultat : un temps de reprise d'activité significativement réduitet une résilience renforcée.

Importance de la coordination avec les autorités locales lors d'une crise climatique

Lors d'une crise climatique, la coordination avec les autorités locales est essentielle, car elles sont les premières à disposer d'une vision opérationnelle de la situation : état des routes, priorités d'évacuation, zones dangereuses, défaillances d'infrastructures critiques ou restrictions d'accès. Elles concentrent également les moyens de secours (pompiers, forces de l'ordre, services techniques) et gèrent la diffusion des alertes à la population. Une entreprise qui ne s'appuie pas sur ces informations risque de mettre en danger ses équipes, de mobiliser inutilement des ressources ou d'aggraver sa propre vulnérabilité.

De plus, les autorités orchestrent la gestion des infrastructures publiques, routes, réseaux électriques, eau, télécoms, qui conditionnent directement la capacité d'une organisation à activer son PCA. Une bonne coordination permet donc d'obtenir des informations fiables, d'anticiper les contraintes logistiques et d'ajuster les priorités de reprise au contexte réel.

5.4. ALLONGEMENT DES TEMPS DE REPRISE D'ACTIVITÉ

Par rapport à une crise classique, une crise climatique entraîne généralement des délais de rétablissement beaucoup plus longs, notamment parce que plusieurs ressources essentielles peuvent être indisponibles simultanément. Elle provoque aussi une dégradation conjointe de multiples infrastructures, qu'il s'agisse de l'eau, des routes, des télécommunications ou de l'électricité, rendant la reprise plus complexe et plus lente. À cela s'ajoute une mobilisation massive des acteurs de secours, souvent dépassés par le volume d'interventions à mener sur un territoire entier.

Face à ces contraintes, le PCA doit intégrer des marges de délai supplémentaires pour chacune des dépendances identifiées. Il devient également indispensable d'ajuster les RTO afin qu'ils reflètent des scénarios climatiques majeurs et non plus de simples incidents isolés. Enfin, une hiérarchisation renforcée des priorités de reprise est nécessaire pour concentrer les ressources limitées sur les activités les plus critiques dès les premières heures de la crise.

FOCUS CRUE DE LA SEINE

Prenons l'exemple de la « *crue de Seine* »

En cas d'inondation, si le fournisseur d'électricité n'est plus en capacité d'alimenter un quartier, les entreprises qui y résident devront se doter de groupes électrogènes pour continuer leurs activités.

De la même manière, les IGH (Immeuble de Grande Hauteur) présentent une vulnérabilité spécifique. En effet, une réglementation particulière impose la présence permanente d'un service de sécurité incendie et d'assistance aux personnes (SSIAP) au sein du PC Sécurité de l'immeuble. Or, la perturbation voire l'interruption des transports en commun et les éventuelles restrictions de circulation pourraient empêcher la nécessaire continuité du service. Ainsi, il est possible que certains IGH deviennent inaccessibles, non par l'impact direct de la crue de Seine (inondation) mais par l'absence des personnels SSIAP qui engendre ipso facto une fermeture administrative de l'immeuble.

Par ailleurs, les entreprises utilisant des « *data centers* », c'est-à-dire des bâtiments dans lesquels sont hébergés tout ou partie des données informatiques, présentent une vulnérabilité particulière. En effet, ils sont généralement localisés en Ile de France, à quelques dizaines de kilomètres des immeubles de bureau.

Dans ce cas de figure, l'immeuble de bureau et le data center sont reliés par un réseau informatique (qui peut transporter des data et/ou de la « *voix* »).

Or, nous savons que ces câbles et fibres « *courent* » dans les tunnels de la RATP et les égouts de Paris. Dans le premier cas, la RATP a prévenu qu'elle ennoierait volontairement aux premiers jours de la crise certains de ces tunnels pour éviter que la pression de l'eau n'endommage les infrastructures. Dans le second cas, l'ensemble des égouts de Paris sera complétement inondé. Même si les câbles sont étanches, il est fort prévisible que certaines parties desdits dispositifs de communication présenteront des vulnérabilités (épissures, répéteurs...) qui pourront engendrer des dysfonctionnements plus ou moins importants sur l'ensemble du réseau. De ce fait, même si l'immeuble de bureau et le data center sont hors de la zone d'inondation géographique de la Seine, il est possible que l'entreprise se trouve fortement affectée par le fait qu'elle ne disposera plus de ses accès au réseau. On peut alors parler de dégâts collatéraux.

Ressources	Vulnérabilité	Impact	Mesure PCA
Alimentation électrique Fournisseur réseau public	**Inondation** quartier < perte alimentation Niveau : élevé	**Arrêt total** des activités bureautique, sécurité, éclairage	**Groupe électrogène** Contrat fournisseur Livraison sous 4h Resp. : Facility Mgr
IGH — SSIAP Service sécurité permanent obligatoire	**Transports bloqués** Agents SSIAP inaccessibles Niveau : critique	**Fermeture** administrative Bâtiment inaccessible sans inondation	**Hébergement sur site** Convention d'astreinte Plan de rotation Resp. : DRH / SSIAP
Data center Localisé en IdF zone exposée	**Inondation** infrastructure ou coupure élec. Niveau : critique	**Perte accès SI** Données inaccessibles Applications arrêtées RTO à définir	**Site de repli / cloud** Réplication données Basculement < RTO Resp. : DSI

5.5. DES RÉPONSES THÉMATIQUES & GRADUELLES

Face à la complexification des problématiques de continuité d'activité, l'approche binaire (mode de fonctionnement usuel/ mode de fonctionnement PCA) ne suffit pas. Il est donc nécessaire d'identifier des actions de reprise d'activité graduelles (des menaces les plus simples aux plus complexes) et d'adopter des réponses proportionnées à un ensemble d'évènements indésirables, plus ou moins perturbants.

Au-delà de leur propre vulnérabilité, les entreprises doivent s'inquiéter des répercussions d'une rupture de la chaine de valeur : la continuité d'un flux tendu avec des fournisseurs, la disponibilité des infrastructures ou même des clients dont ils sont dépendants.

Ainsi, l'approche du *« plan »* unique structurant mais rigide ne convient pas. Il doit laisser place à la constitution d'une *« boîte à outils »* permettant une gradation et une réponse proportionnée dans les actions de continuité d'activité à mettre en œuvre (fiches actions reflexes ou Check List qui présentent les principales actions que chacun des Services doit mettre en œuvre en cas de sinistre, planning de reprise des activités des Ressources Humaines qui présente, jour par jour et service par service, le nombre de collaborateurs devant se présenter sur le site de repli...). Les PCA doivent être conçus pour être flexibles et adaptables, car les crises réelles ne suivent jamais exactement les scénarios anticipés.

La citation *« Le scénario exact ne se produira jamais : il faut se préparer à l'imprévisible »* est encore plus vraie avec les risques climatiques !

Au-delà de leur propre vulnérabilité, les entreprises doivent se préoccuper de la capacité de leurs partenaires ou de leurs prestataires critiques à répondre à leurs obligations de service en cas de sinistre majeur, y compris la capacité de service des moyens de secours. En effet, l'entreprise se situe au cœur des réseaux de dépendances de ses partenaires et sous-traitants (fournisseurs d'eau potable, électricité, réseaux téléphoniques, courrier...). La défaillance de l'un d'entre eux affecte de fait le fonctionnement de l'entreprise.

5.6. LIVRABLES ET COMPLÉMENTS À INTÉGRER DANS LE PCA

À l'issue de la démarche d'actualisation du PCA pour couvrir les indisponibilités liées aux événements climatiques, plusieurs éléments supplémentaires doivent être formalisés :

- Fiches réflexes adaptées aux périls climatiques auxquels le site est exposé (inondation, tempête, chaleur...)
- Cartographie des voies d'accès et routes alternatives. Inclure les routes prioritaires, les routes à risque (crues, glissements de terrain...) et les itinéraires de contingence.
- La localisation des sites de repli et les backups (documenter : le site principal de repli, le site secondaire géographiquement dissocié de l'aléas étudié, vérifier l'autonomie énergétique en cas de coupure prolongée dans la zone...).

ARTICULATION DU PCA ET DES AUTRES OUTILS DE GESTION DES RISQUES

Le Plan de Continuité d'Activité doit être intégré dans un dispositif plus vaste de gestion globale des risques et des crises.

Chapitr

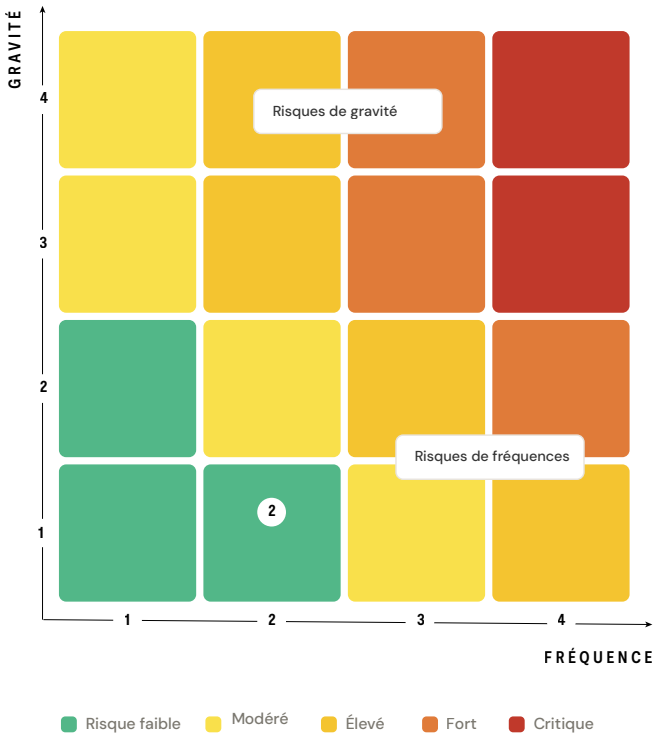

e 6

6.1. PLAN DE CONTINUITÉ D'ACTIVITÉ ET CARTOGRAPHIE DES RISQUES

La cartographie des risques et le Plan de Continuité d'Activité sont étroitement liés : la première identifie et hiérarchise les menaces, tandis que le second organise la réponse opérationnelle visant à en limiter les impacts sur les activités essentielles. Le risque climatique, à l'instar du risque cyber, peut être intégré dans les cartographies des risques selon différentes modalités : en tant que risque autonome, en tant que facteur contributif ou aggravant de risques existants, ou selon une approche hybride, désormais privilégiée car plus représentative des interdépendances et des effets systémiques.

Ces risques présentent des impacts potentiellement critiques sur la continuité d'activité, y compris lorsqu'ils se matérialisent de manière indirecte ou différée. Leur intégration dans les matrices probabilité/impact nécessite en conséquence d'adapter les méthodes d'analyse, afin de mieux prendre en compte des phénomènes à faible fréquence mais à très forte gravité, dont les effets peuvent dépasser les capacités traditionnelles de reprise et de gestion de crise.

6.1.1. Risques de fréquence et risques de gravité



La cartographie des risques est un outil d'identification, de recensement et de quantification des risques. Cette quantification des risques s'opère par une approche statistique. Ainsi, dans cette acception, le *« risque »* est défini comme le produit de *l'ensemble des fréquences d'occurrence* de l'évènement indésirable par les impacts redoutés de la menace que le risque fait peser sur l'organisation.

FOCUS CLIMAT

Risque climatique

L'analyse du risque climatique nécessite une approche approfondie afin d'identifier les menaces liées aux effets physiques du changement climatique, qu'ils soient chroniques (élévation des températures, stress hydrique…) ou aigues (vagues de chaleur, fortes pluies, tempêtes…) ainsi que les risques de non-adaptation.

Elle s'appuie sur trois étapes clés :

- Identifier des aléas climatiques (un événement lié au climat –comme des vagues de chaleurs, des fortes pluies, etc..) ;
- Evaluer l'exposition de l'actif (l'emplacement, les attributs physiques et la valeur des actifs ou des personnes qui pourraient être affectés par un aléa) ;
- Apprécier la vulnérabilité de l'actif (propension ou prédisposition à être affecté négativement par un certain danger et englobe une variété de concepts et d'éléments, y compris la sensibilité ou la susceptibilité aux dommages).

Cette approche par le diptyque *« Probabilité/ Impact »* permet également de déterminer de groupes de risques :

6.1.1.1. Le groupe des risques de fréquence

Il est mesuré par l'indicateur de *« fréquence d'occurrence »*. En effet, même si l'impact unitaire de la réalisation du risque est peu important, le fait qu'il se réalise souvent ou fréquemment engendre ipso facto des conséquences financières importantes pour l'organisation.

EXEMPLE

L'exemple type est celui de la flotte automobile d'entreprise : une population de commerciaux possède des véhicules de fonction. Du fait même que ces personnels réalisent de longs et nombreux parcours professionnels, il est probable qu'ils génèrent ou soient victimes d'accrochages engendrant des destructions matérielles sans conséquences corporelles. Pris unitairement, un accrochage va générer un coût de réparation de quelques milliers d'euros. En revanche, le nombre important de véhicules de fonction va multiplier le risque d'accrochages et donc un volume financier de réparation très important.

Par voie de conséquence, il sera donc opportun de mettre en place des actions de prévention qui auront pour vocation d'abaisser la fréquence d'apparition de l'événement indésirable. Dans l'exemple présent, des cours de conduite *« durable »* sur circuit permettront aux commerciaux de l'entreprise de mieux maîtriser leur véhicule, d'adopter une meilleure conduite et éviter ainsi la survenance d'accrochages : le nombre d'accrochages baissera et donc l'impact financier sera moindre pour l'entreprise.

6.1.1.2. Le groupe des risques de gravité (ou risques de crises)

Il est mesuré par l'indicateur de *« gravité de l'impact »*. Contrairement au risque de fréquence, l'impact unitaire de la réalisation du risque est ici très important, voire vital pour l'entreprise alors que le risque de sa survenance est peu probable. Il conviendra de mettre en place des plans de traitement afin de réduire les impacts associés à la réalisation de l'événement. Ainsi, le plan de gestion de crise et le plan de continuité d'activité font partie des outils de traitement des risques, des outils curatifs, des moyens de protection.

En résumé, au sein du processus global de management des risques, la cartographie des risques constitue l'outil de référence lors de la phase d'identification, de recensement et de hiérarchisation des risques. Elle intervient avant la mise en place d'outils de traitement des risques parmi lesquels le PCA. Ce dernier a pour finalité de réduire les impacts de l'apparition d'un risque de gravité, c'est-à-dire une crise.

Retenons donc que :

1. la cartographie est un outil d'identification et de quantification de l'ensemble des risques de l'organisation.

2. Le PCA est un outil de traitement des risques de gravité (faible probabilité d'occurrence/ forte gravité de l'impact). Sa finalité est opérationnelle.

3. Les méthodologies de cartographies des risques utilisent des approches probabilistes pour quantifier les risques. La méthodologie du PCA utilise une approche déterministe pour assurer la continuité des processus identifiés comme critiques.

4. Contrairement aux autres risques de gravité qui sont généralement ponctuels, une cyberattaque combine plusieurs caractéristiques aggravantes : intentionnalité (l'attaquant s'adapte aux défenses), persistance (la menace reste active), effet systémique (propagation rapide à l'ensemble du SI), et contamination de la confiance (doute sur l'intégrité des données). Ces spécificités nécessitent une approche dédiée détaillée en chapitre 4.

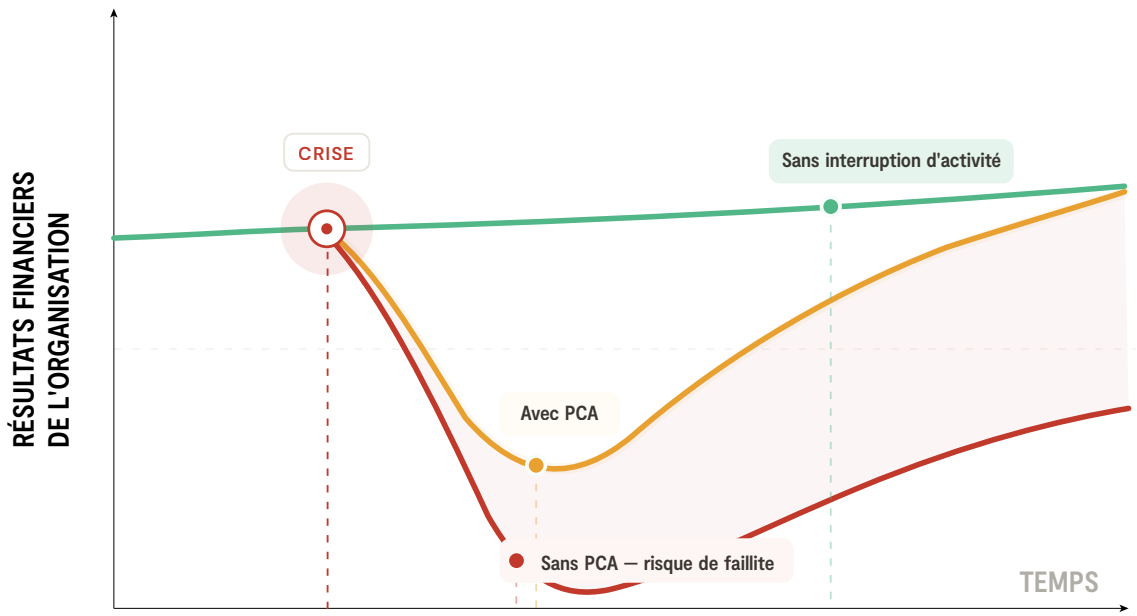
6.2. PLAN DE CONTINUITÉ D'ACTIVITÉ ET RECOURS AUX SYSTÈMES D'ASSURANCE

Le PCA peut constituer un outil d'optimisation des coûts assurantiels : toutes les opérations mises en œuvre pour amortir l'impact financier d'une crise sur les résultats seront autant de facteurs de diminution des dédommagements prévus dans les contrats d'assurances.

Il sera alors plus facile de négocier le montant de la prime d'assurance en prouvant que l'entreprise s'est mise en ordre de marche pour diminuer les impacts de la crise (PCA et plan de gestion de crise actualisés).

Par ailleurs, avec des couvertures d'assurances et notamment la police « *Dommages/ Pertes d'exploitation* », l'entreprise peut se prémunir des frais de déclenchement du PCA (tel que la location de salle de back-up, des frais de re-routage téléphonique et courrier). Il est donc indispensable d'intégrer les interlocuteurs du monde de l'assurance dans l'élaboration du PCA, sans oublier de faire jouer la concurrence.

IMPACT FINANCIER D'UNE CRISE — PCA



FOCUS CLIMAT

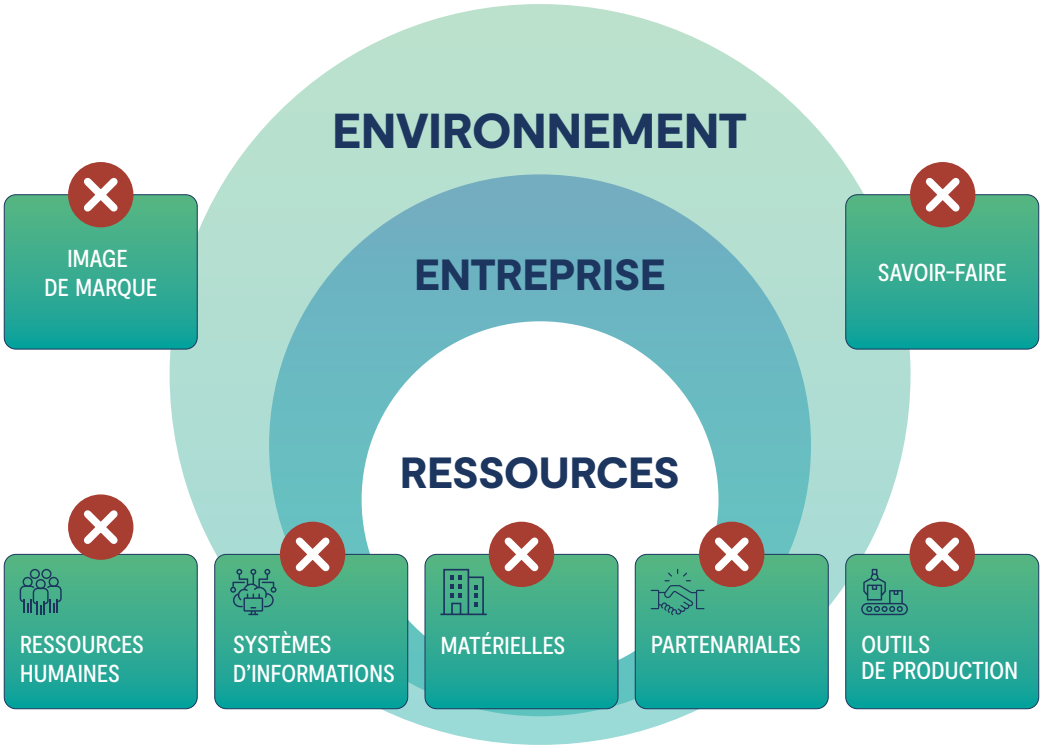
Face aux événements météorologiques extrêmes assurables, tels que les tempêtes, les inondations ou les épisodes de pluies intenses, un Plan de Continuité d'Activité (PCA) robuste permet de démontrer la capacité de l'organisation à limiter les impacts opérationnels et financiers d'un sinistre. À ce titre, le PCA constitue un levier structurant de dialogue et de négociation avec l'assureur dommages aux biens, notamment en matière de pertes d'exploitation, en objectivant les dispositifs de prévention, d'adaptation et de reprise mis en place face aux risques climatiques majeurs. Pour les collectivités territoriales, cet enjeu est particulièrement sensible : elles sont aujourd'hui confrontées à une multiplication des refus de couverture ou à un durcissement des conditions assurantielles liées aux risques climatiques. La capacité à démontrer l'existence d'un PCA robuste, actualisé et éprouvé devient alors un levier essentiel pour sécuriser une couverture assurantielle et renforcer la crédibilité de la collectivité auprès de ses partenaires assureurs.

6.3. L'ARTICULATION DES PROBLÉMATIQUES DE *« GESTION DE CRISE »* ET DE *« CONTINUITÉ D'ACTIVITÉ »*

Un consensus existe sur le fait que les problématiques de *« gestion de crise »* et de *« continuité d'activité »* doivent être articulées. Néanmoins, il n'existe pas de normes sur l'articulation de ces deux concepts. Certains professionnels intègrent la gestion de crise dans les politiques de continuité d'activité alors que d'autres proposent d'insérer le PCA dans des dispositifs plus globaux de gestion de crise. Il convient de clarifier ce point et de proposer une articulation.

Cette articulation est particulièrement mise à l'épreuve lors des cyber-crises modernes. Contrairement à un sinistre physique circonscrit, une intrusion informatique avancée est un événement dynamique qui requiert une chorégraphie parfaite entre la réponse technique (gestion d'incident), la prise de décision stratégique (gestion de crise) et la restauration des opérations (continuité d'activité). Le chapitre 1.3.1 reviendra sur cette convergence indispensable, qui constitue l'une des évolutions majeures de la pensée sur la résilience d'entreprise.

6.3.1. Typologie de crise : *« Crises opérationnelles »* et *« crises de visibilité »*



Nous avons vu précédemment que le fonctionnement normal d'une entreprise nécessite le recours à un ensemble de ressources. En cas de disparition ou d'indisponibilité d'une ou de plusieurs ressources, le déclenchement du Plan de Continuité d'Activité lui permettra de pallier l'indisponibilité autant que faire se peut.

LA CRISE OPÉRATIONNELLE

Ce premier type de crise, portant atteinte aux ressources de l'entreprise et par voie de conséquence nécessitant le déclenchement du PCA, est qualifié de *« crise opérationnelle »*.
Néanmoins, il existe un second type de crise qui porte atteinte au capital de l'entreprise mais qui ne nécessite pas le déclenchement du PCA.

LA CRISE DE VISIBILITÉ

C'est une crise dans laquelle *« notre système de visibilité »* (détection, inventaire, évaluation) est défaillant [9]. En effet, le dénominateur commun de ce type de crise est la mise à l'épreuve de la confiance qu'accorde l'ensemble des acteurs à l'entreprise, ce qui peut se produire dès lors qu'une ou plusieurs parties prenantes de l'entreprise (actionnaires, clients, ONG...) l'interroge voire la mette en cause sur telle ou telle problématique (financière, sociétale, éthique,). Dès lors, si l'organisation ne peut apporter une réponse immédiate qui soit conforme aux représentations, aux aspirations et aux attentes des parties prenantes, elle se trouve en *« crise de visibilité »*.

(9) Le concept de *« Crise de visibilité »* est défini dans l'ouvrage *« Gérer les grandes crises »*, Louis CROCQ, Sophie HUBERSON, Benoit VRAIE, éditions Odile Jacob, 2009.

EXEMPLE

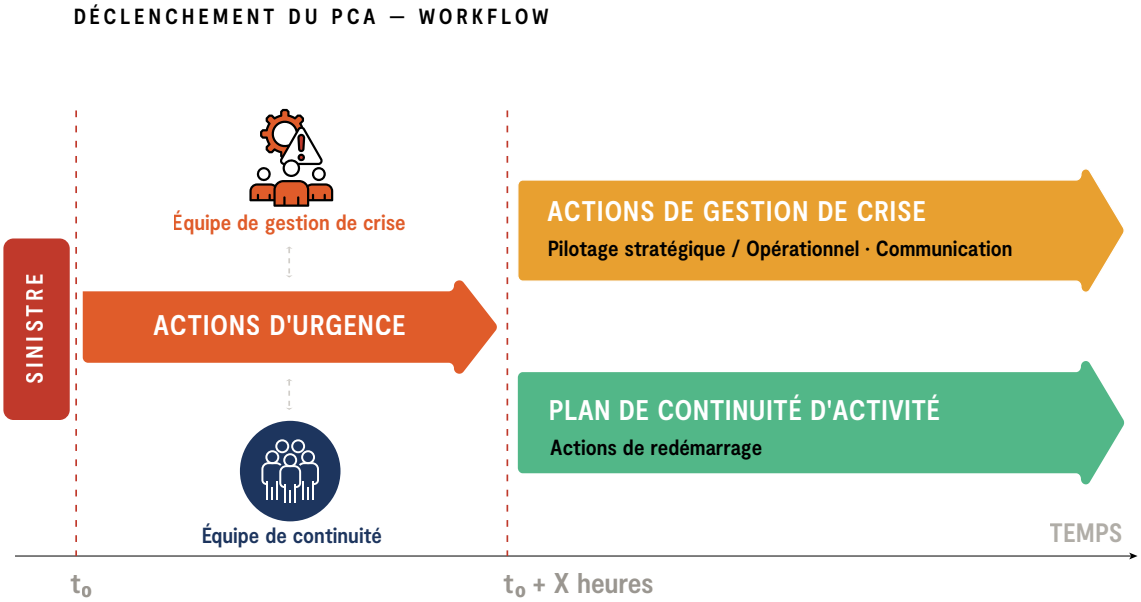
La « *crise de visibilité* » a été traversée par Nike dans les années 1990. Une ONG a révélé que l'entreprise faisait travailler des enfants en Asie du Sud-Est, de surcroît dans des conditions précaires. Devant l'ampleur du scandale, Nike s'est vu contraint de cesser immédiatement cette pratique qui ne correspondait pas aux attentes éthiques de ses clients.

L'épisode de crise pandémique est éloquent. Les experts prévoyaient une extension planétaire du virus H5N1, initialement présent à l'état endémique en Asie du Sud-Est. Mais c'est un autre virus, le virus H1N1 qui est apparu au Mexique et s'est diffusé rapidement. Dès l'origine, les experts ont fourni des avis divergents, tant sur le caractère pandémique que sur la dangerosité du virus. Ainsi, chaque Etat, en fonction de ses propres logiques (contexte, antécédents, sensibilité de la population...) a exercé son principe de précaution à des degrés divers, sans coordination tant à l'échelle internationale qu'à l'échelle européenne ni d'appréciation à sa juste mesure de la perception, des représentations mentales et des réactions de l'opinion publique. Ces différentes prises de position et les divergences exprimées au sein du monde scientifique ont donc très largement contribué à l'apparition d'une crise de visibilité.

Nous voyons donc que ces organisations ont traversé des crises très importantes alors même que l'ensemble des ressources de l'entreprise dans le premier cas, des Etats dans le second cas, étaient toujours disponibles. A ce titre, il n'est pas nécessaire de déclencher le plan de continuité d'activité. En revanche, la restauration de l'image fera l'objet de la mise en œuvre de mesures de communication *« extraordinaires »*.

En complément, notons qu'il est possible qu'une crise soit successivement ou simultanément *« crise opérationnelle »* et *« crise de visibilité »*.

6.3.2. Rôles et responsabilités des équipes de gestion de crise et équipe de continuité d'activité



RÔLES ET RESPONSABILITÉS DES ÉQUIPES DE GESTION DE CRISE

Au sein de l'entreprise, un petit groupe de collaborateurs rassemblés dans les cellules de crise va mettre en place **des actions *« extraordinaires »*** (au sens premier du terme, c'est-à-dire hors du quotidien). Chaque membre de la cellule de crise tiendra une fonction qui peut être différente de celle qu'il exerce habituellement au sein de l'entreprise. Exemple : le directeur financier se retrouve *« coordinateur »* de la cellule de gestion de crise de l'entreprise et de ce fait n'utilise plus son expertise comptable et financière mais plutôt ses talents de coordination en vue d'organiser l'action collective de gestion de crise

RÔLES ET RESPONSABILITÉS DES ÉQUIPES DE CONTINUITÉ D'ACTIVITÉ

Contrairement à la gestion de crise, tout ou partie des salariés (selon la stratégie de continuité adoptée par l'entreprise) continuera de **pratiquer leurs actions *« usuelles »*** au sein de l'entreprise (le comptable continuera de faire la comptabilité, l'agent de maintenance de la maintenance) mais dans **un cadre et avec des modalités qui leur seront *« extraordinaires »*** comme le travail sur un site de repli ou le travail à distance (télétravail).

6.4. PCA & AUTRE MODE DE GESTION DES RISQUES

Comme nous l'avons vu le PCA ne constitue pas une réponse définitive, il est un des différents outils de gestion des risques. Il existe donc des situations où le PCA ne constitue pas une solution idoine/ effective, où l'effort d'investissement doit être réalisé en termes de prévention plutôt qu'en termes de protection.

EXEMPLES

Exemple d'une machine-outil très spécifique (quelques pièces produites à l'échelle mondiale) au sein d'une chaîne de production

En cas de sinistre, il sera très difficile de remplacer la machine-outil. A ce titre, il est préférable de prévenir tout incident susceptible d'altérer l'intégrité de la machine-outil (en mettant en place par exemple un système d'extinction automatique à gaz en cas de début d'incendie) plutôt que de mettre en place un PCA.

Exemple en matière de chaînes d'approvisionnement

Il est conseillé de respecter deux principes de prévention avant même de mettre en place une réflexion PCA *« fournisseurs critiques »*. Primo, ne pas dépendre d'un seul fournisseur mais partager son activité entre plusieurs prestataires et secundo faire appel à des prestataires travaillant sur des zones géographiques distinctes et clairement identifiées.

LE FACTEUR HUMAIN EN SITUATION DE CRISE : LES DIMENSIONS HUMAINES ET SYMBOLIQUES

Chapitr

e 7

7.1. ÉVALUATION DE LA PERCEPTION DE LA GRAVITÉ DES RISQUES PAR LES COLLABORATEURS

À l'instar de la pandémie grippale de 2009, la crise de la COVID 19 a révèlé les difficultés et les leviers associés à la perception du risque par les populations, tout en soulignant l'importance du développement d'une culture du risque et de la crise durablement ancrée dans la conscience collective.

Lors de l'épisode pandémique, la politique de l'Etat en matière de communication de crise s'est enclenchée. Ainsi, le plan de communication a été déroulé de façon automatique sans prendre systématiquement en compte la dimension sensible de l'imaginaire collectif, du stress et des comportements. L'Etat n'a pas réalisé un diagnostic et un suivi suffisants des attentes de la population en termes de communication. Il a sous-estimé la capacité d'adhésion, d'indifférence ou de rejet des citoyens. En d'autres termes, il n'a pas tenu compte du fait que la population pouvait percevoir la menace d'une autre manière et avec une autre intensité que celle qu'il avait prévue.

La prévision des comportements individuels et collectifs en situation de menace ou de réalité pandémique a manqué. Les pouvoirs publics se sont contentés de distiller par voie descendante une communication visant à *« atténuer les craintes et l'anxiété de la population et à éviter le risque de désinformation, de rumeurs, voire de déstabilisation »* (Plan gouvernemental) mais ils n'ont ni exploré ni inventorié les comportements prévisibles de la population.

L'élaboration des PCA tient compte de la prévision de ces comportements individuels et collectifs en situation de menace inhabituelle. Le PCA doit intégrer le facteur humain, individuel et collectif. Il agrège les représentations mentales collectives de la menace et du risque et les comportements individuels ou collectifs aberrants (insouciance, sous-estimation et déni du danger, ou au contraire affolement et panique exacerbés sous l'effet des rumeurs).

En premier lieu, il s'agit de comportements adaptés et responsables. Pour reprendre l'exemple de la pandémie, cela correspond à anticiper le danger, adopter les mesures appropriées, puis s'informer au jour le jour de l'état de la menace, sans s'affoler, ne pas croire aux rumeurs et ne pas les propager, appliquer les mesures de prévention (lavage des mains, port de masques), se faire vacciner si les autorités sanitaires le conseillent, consulter dès les premiers symptômes d'atteinte grippale, se faire soigner, éviter de contaminer ses proches.

En second lieu, il s'agit de comportements d'insouciance, de négligence voire de déni, irresponsables : ne pas croire (par optimisme inconsidéré) à l'éventualité de la crise, ne pas s'informer sur le danger qu'elle présente, ne pas prendre connaissance des mesures de prévention, afficher un scepticisme critique systématique vis-à-vis des informations fournies, ne pas s'informer de la progression de la menace.

En troisième lieu, il s'agit de comportements de crainte exagérée, d'affolement et de panique : état d'inquiétude exagéré à l'annonce de l'éventualité d'une crise, excès dans la recherche de l'information sur ce danger, puis dans l'investigation quotidienne sur sa progression, éprouver une sensibilité exacerbée aux rumeurs, procéder à des achats inconsidérés et excessifs d'équipements...

Ainsi, en fonction de la problématique couverte par tel ou tel PCA, il convient d'identifier les représentations mentales des collaborateurs et d'établir un diagnostic et un suivi suffisants des attentes de la population. C'est donc davantage un travail de pédagogie et d'acculturation de la population à long terme que des réponses ponctuelles, techniques et thématiques à telle ou telle crise.

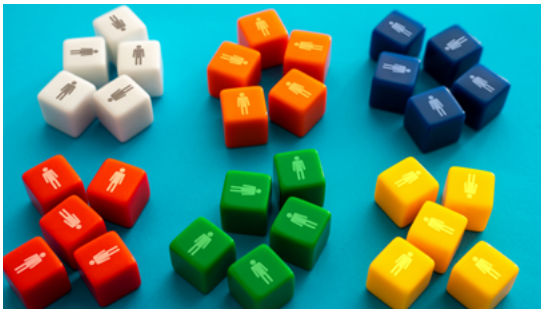
7.2. RESPECTER LES ÉQUILIBRES *« TRAVAIL/REPOS »*

En période de crise, des facteurs physiologiques aggravants sont omniprésents, il est nécessaire de respecter les équilibres *« travail/ repos »*. La fatigue engendrée par la surcharge de travail et la mauvaise ergonomie du poste de travail, la privation de sommeil, la restauration frugale et hâtive peuvent user les énergies individuelles et exacerber les susceptibilités.

Ainsi, au-delà des aspects biologiques, il est indispensable que l'individu respecte les équilibres *« travail/ repos »* et qu'il pratique à échéance régulière des exercices de décontraction. En situation de crise, il convient donc de conserver une hygiène de vie adéquate.

7.3. TUILAGE DES ÉQUIPES DE CONTINUITÉ POUR DURER

La crise peut durer plusieurs jours ou plusieurs semaines. L'Organisation doit prévoir un fonctionnement en binôme et un *« tuilage »* des équipes. Plus qu'un simple briefing lors de la passation de poste, il est important que les deux personnes travaillent ensemble suffisamment longtemps pour que la transmission d'informations soit la plus complète et exacte possible afin d'assurer une véritable continuité malgré le changement.

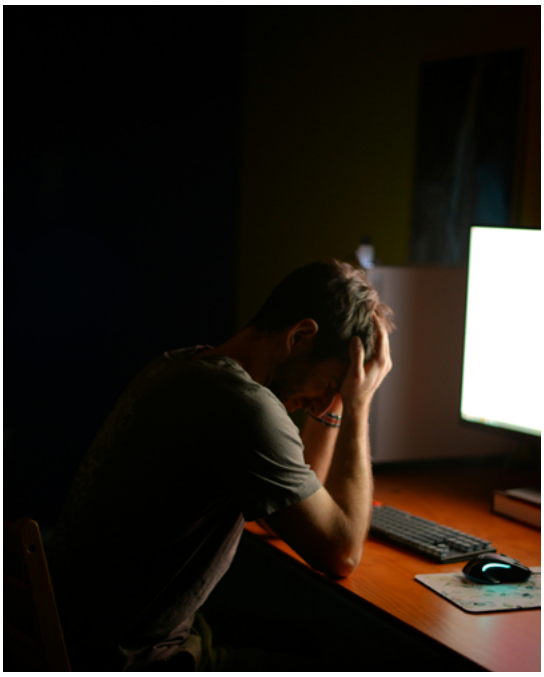


7.4. LE STRESS ET SES IMPACTS

La perception de la crise, du risque et du danger peut devenir un facteur constitutif ou aggravant de la crise elle-même. Le choc émotionnel peut générer une véritable marée *« désorganisante »* dans toutes les capacités cognitives et opérationnelles des individus et des groupes : c'est l'irruption du stress.

En s'inspirant d'une définition proposée par Selye, Louis Crocq a défini (1999) le stress comme : *« la réaction neuro-biologique, physiologique et psychologique d'alarme, de mobilisation et de défense, de l'individu face à une agression ou une menace, menace pour sa vie, son intégrité physique ou son équilibre psychique »*.

Le stress est une réaction utile, adaptative. Grâce à son stress, l'individu échappe au danger ou se trouve en mesure d'y faire face, ce qui correspond au mot anglais *« coping »*.



Crédit ptoho : laram-BpTqCNotBLI-unsplash

On admet que le stress a trois principaux effets psychologiques :

1. **il focalise l'attention sur la situation menaçante, chassant provisoirement de la conscience les autres préoccupations et pensées en cours,**
2. **il mobilise les capacités cognitives (attention, mémorisation, évaluation, raisonnement),**
3. **il incite à la prise de décision et à l'action.**

La contrepartie est que le stress est grevé de symptômes gênants (pâleur, sueur, tachycardie, spasmes viscéraux) et qu'il est coûteux en énergie. Dans sa phase la plus intense on parle alors de stress *« post traumatique »* et on obtient le tableau clinique suivant [10] :

- **la sidération** : l'individu est stupéfait, stuporeux, aboulique, pétrifié ;
- **l'agitation stérile** : le sujet est dans un état d'excitation psychique, verbale et motrice ;
- **la fuite panique** : la personne sous stress est *« lancée »* dans une fuite éperdue, un état d'affolement généralisé ;
- **le comportement d'automate** : l'individu réalise des gestes mécaniques répétés dont il ne se souviendra pas.

(10) Voir à ce sujet les travaux du Médecin Général Louis CROCQ et de Benoit VRAIE

7.5. « PRÉPAREZ-VOUS À ÊTRE PRÊT »[11]

La Croix Rouge propose une campagne de sensibilisation dont le paradigme est l'*« auto-résilience »* c'est à dire la capacité du citoyen à se prendre en charge en cas de crise. *« Prévenir, réfléchir et anticiper pour mieux agir, c'est réduire considérablement les conséquences qui peuvent découler de ces situations d'urgence : chacun peut devenir acteur de sa survie et de celle des autres grâce à des réflexes indispensables qui permettent de réagir aux situations exceptionnelles.»* [12]

Ce principe est transposable aux salariés des entreprises. Dans le cas de la problématique de Crue de Seine, certaines entreprises disposent d'un PCA dans lequel figure le nombre de collaborateurs nécessaires à la reprise de l'activité. Néanmoins, au-delà de la valeur numérique, ces salariés ne seront peut-être pas disponibles pour l'entreprise le jour J. En effet, le phénomène de crue de Seine engendrera d'importantes perturbations aux différents niveaux des services d'Etat, des institutions et de l'ensemble des infrastructures ainsi que des réseaux critiques : eau, électricité, télécommunications, transports, chauffage, ordures ménagères...

Le collaborateur devra donc gérer le fait que sa famille ne dispose plus d'eau potable, d'électricité, d'internet, de téléphonie... A ce titre, il n'est pas certain que ce dernier, s'il n'est pas préparé, réponde présent pour son entreprise. De ce fait, les entreprises, dans leurs réflexions sur les problèmes de continuité d'activité, doivent repositionner *« le collaborateur »* au centre du dispositif et mettre en place, pour les fonctions critiques, des mesures d'accompagnement des collaborateurs. Pour reprendre l'exemple de la crue de Seine, les entreprises doivent sensibiliser les collaborateurs sur l'attitude à adopter afin de les préparer personnellement à ce scénario et les accompagner (financièrement et/ou par des modalités pratiques) dans la mise en sécurité de leur famille.

(11) et (12) Site Internet *« Croix Rouge Française »*

« PRÉPARER LA GUERRE EN TEMPS DE PAIX » COMME PHILOSOPHIE DU PCA

La boîte à outils servant à élaborer les différents types de PCA est bien garnie. Chaque outil détient une fonction spécifique mais ne sera efficace que s'il est bien utilisé par un personnel formé, compétent et motivé.

Chapitr

8.1. LA CULTURE DE CRISE

La culture de crise et la culture de la continuité d'activité vont de pair. L'objectif est de constituer un corpus de valeurs, de convictions et de savoirs partagés au sein de la communauté des collaborateurs qui vise à bien appréhender les situations de crise et à mobiliser les capacités de ces équipes à les dépasser.

Cette posture consiste donc à adopter collectivement une philosophie d'acceptation raisonnée des risques, de vigilance et d'intelligence au monde [13] face à des évènements indésirables. Elle entraine *de facto* une responsabilisation de l'ensemble des personnels détenteurs d'un part de responsabilité dans trois fonctions distinctes :

- fonction de sentinelle, de guetteur dans l'identification des risques ;
- fonction d'alerte dans la détection des signaux faibles, presque-accidents, accident et crises ;
- fonction de gestion dans les modalités de traitement des risques et des crises.

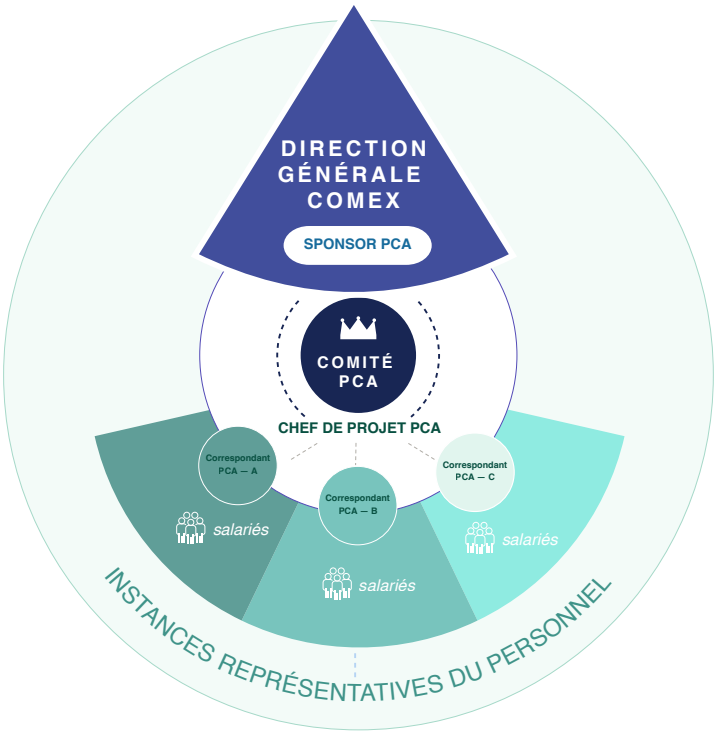
Cette *« culture de crise »* est indispensable mais ne se décrète pas : lorsqu'une population, une organisation, une entreprise est confrontée à une crise à un moment de son histoire, elle est déjà conditionnée par ses habitudes et dépendante de ses propres marqueurs. Ses normes, son cadre de fonctionnement, son *« terreau »* seront propices à générer des comportements spécifiques pour réagir voire pour traiter la crise. Si pour les collaborateurs en poste depuis longtemps, ce corpus a été acquis lors de tests PCA et d'exercices de gestion de crise (ou de gestion de crises en situation réelle), ce dernier doit être transmis aux nouvelles recrues comme autant de manières et d'attitudes à adopter pour faire face aux crises à venir.

Ainsi, la participation active de chaque collaborateur à son niveau aux systèmes de gestion des risques améliore la cohérence et la résilience de l'ensemble du dispositif. Il démultiplie l'efficacité des actions d'ensemble menées par le *« risk manager »*, le *« responsable PCA »* et le *« gestionnaire de crises »* (fonctions qui peuvent également être exercées par une seule et même personne).

En effet, le *« risk manager »* est considéré trop souvent comme l'*« expert maison »* capable de traiter seul l'intégralité des problématiques de gestion des risques. Or il est avant tout, dans sa fonction ERM (Enterprise Risk Management) et Assurances, un coordinateur, un facilitateur, un animateur des acteurs de l'entreprise. Il convient donc à chacun dans l'entreprise de *« penser l'envisageable, l'imprévisible et l'inimaginable »* et de devenir ainsi acteur de la gestion des risques. Pour ce faire, l'implication de la direction des ressources humaines est déterminante.

(13) *« Gérer les grandes crises »*, Crocq, Huberson, Vraie ; 2009.

8.2. LA GOUVERNANCE DU PROJET PCA



8.2.1. Une démarche d'entreprise acceptée par tous et financée par la Direction Générale

Le rôle de la Direction Générale est bien évidemment primordial dans la structuration et l'entretien de la culture de gestion des risques et des crises. Il passe par :

- la clarification des orientations politiques et stratégiques pour donner sens à l'action de restauration des actifs endommagés par la crise ;
- la mise à disposition d'un système de veille et d'information pour anticiper les crises ;
- la mise en place d'une organisation du travail spécifique dans laquelle le paramètre de *« survenue d'une crise »* joue un rôle important : faire savoir, faire comprendre et faire accepter que l'on puisse travailler dans d'autres conditions que celles fixées initialement et ce pour des raisons extraordinaires ;
- la formation des acteurs de l'organisation à la gestion de la crise et au travail en mode dégradé ;
- l'instauration d'un climat de dialogue social propice à accepter des conditions de travail différentes et parfois plus contraignantes qu'à l'état normal.

La Direction Générale de l'Organisation affiche et porte le projet PCA comme un projet fédérateur car il implique et mobilise les différents services, opérationnels ou transverses. Pour ce faire, cette dernière doit être elle-même convaincue de l'utilité du financement des PCA.

Pour un accueil favorable du PCA auprès de la Direction Générale : les arguments à présenter.

Ils se classent en deux ordres :

1 **Un ordre « *quantitatif* » car le PCA permet d'évaluer :**

- les pertes de l'entreprise au cas où l'on ne mettrait pas en œuvre une organisation adéquate de continuité d'activité. (Cf. graphique page 28 sur les résultats de l'entreprise sans l'instauration d'un PCA.) ;
- la diminution de la prime d'assurance en raison de la meilleure protection de l'entreprise : plus le bouclier est solide, moins la compagnie d'assurance n'aura besoin d'indemniser….

2 **Un ordre « *qualitatif* » car le PCA participe à la construction d'une meilleure performance en termes de ressources Humaines :**

- La mobilisation du personnel sur un thème fédérateur : sauvegarder l'entreprise et par là-même l'emploi ;
- Améliorer la qualité dans l'entreprise en procédant à un audit organisationnel, en testant les procédures et en jouant des exercices de crises ;
- Améliorer la circulation de l'information dans l'entreprise en incitant les différents services à travailler ensemble ;
- En démontrant la valeur pédagogique de l'élaboration et de la mise en œuvre d'un PCA : on se préoccupe autant des personnes que des biens. Les communications interne et externe s'en trouvent améliorées.

8.2.1.1. Le sponsor

Trouver un *« sponsor »*, au mieux un commanditaire, au sein de la direction Générale, est un gage de réussite du projet. Ce dernier sera particulièrement convaincu de l'intérêt supérieur de sa mission et en sera autant valorisé. Il sera doté des pouvoirs et de l'autorité nécessaires, bref de la légitimité hiérarchique nécessaire à l'accomplissement de sa mission.

Ce sponsor permet au responsable PCA de bénéficier d'un appui et d'un facilitateur dans le déploiement mais également d'une aide dans la gestion et la résolution des problèmes et des écueils inhérents à la réalisation d'un tel projet.

8.2.1.2. Le chef de projet PCA

Généralement, c'est le *« Risk Manager »* ou le *« Responsable Sécurité »* de l'organisation (sauf pour les organisations de grande taille au sein desquelles la fonction *« Responsable PCA »* est une fonction à part entière). Il est en tout état de cause le porteur du projet PCA. A ce titre, il pilote le projet, en assure le suivi et le bon déroulement, anime le réseau de Correspondants PCA (cet organigramme est à dimensionner en fonction de la taille et de l'exposition aux risques de l'entreprise), préside le Comité *« Plan de continuité d'activité »*, consolide les données et assiste les *« Métiers »* et *« Fonctions-support »* dans l'implémentation des solutions de continuité d'activité. Il est également le garant du maintien en conditions opérationnelles du PCA. A ce titre, il assure les tests.

8.2.1.3. Le Comité *« Plan de continuité d'activité »*

Le Chef de Projet PCA met en place un Comité *« Plan de continuité d'activité »* composé des Directeurs (ou *« Correspondants PCA »*) de l'ensemble des fonctions-supports et des lignes de Métier(s). La composition dudit Comité est validée par la Direction Générale.

La mission de ce comité est de concevoir et de mettre en œuvre le PCA, de valider les différentes étapes et phases du projet qu'il convient de décliner auprès de chaque unité/service de l'entreprise par le biais de *« correspondants PCA »*.

Ce comité aura également pour mission de *« pondérer »* les résultats chiffrés, de ré-étalonner et de comparer les informations fournies par chacun des Services (DIMA, impact sur le business de l'arrêt de tel ou tel processus…) afin de réduire les écarts provenant d'une surévaluation ou d'une sous-évaluation des données. En effet, il est possible qu'apparaissent des distorsions de représentations quant à la gravité de l'arrêt de l'activité de tel ou tel service lors des entretiens individuels avec les collaborateurs de chacun des services concernés.
Ce travail d'homogénéisation des données permet de comparer et de consolider l'ensemble des données fournies par chacun des services. Enfin, ce comité propose des orientations de continuité d'activité à la Direction Générale.

8.2.1.4. Les Correspondants PCA

Dans les organisations de grande taille, il est possible que des relais PCA soient présents à l'échelle de chaque Direction : ce sont les *« Correspondants PCA »*. Leur fonction est de décliner l'ensemble des opérations de mise en place d'un PCA à l'échelle de leur périmètre de responsabilité (collecte d'informations, mise en application de principes et de règles PCA…).

8.2.1.5. Les salariés

Thucydide nous rappelle que *« la sécurité de la cité tient moins à la solidité de ses fortifications qu'à la fermeté d'esprit de ses habitants »*. Cette citation prend tout son sens quand on l'applique au domaine de la gestion des crises et de la continuité d'activité. En effet, si la création d'un corpus documentaire de référence et la mise en place d'outils techniques de gestion et de reporting des risques sont des étapes nécessaires à la mise en place d'un PCA, il est indispensable que l'ensemble des collaborateurs possèdent a minima une culture de gestion des risques et des crises : la sécurité est l'affaire de tous.

CONCLUSION

Une entreprise confrontée à une crise doit avoir mis en place les meilleures conditions pour reprendre au plus vite un niveau d'activité comparable à l'état antérieur et ce aux fins de remplir les objectifs initialement fixés. A ce titre, la stratégie de continuité ne peut plus résider uniquement dans une réponse technique ou un transfert financier du risque vers les assureurs, en raison de l'impact sur l'image de marque et parce que la survie de l'entreprise dépend moins de sa capacité à indemniser des tiers que de son aptitude à réagir efficacement et à communiquer face à une crise.

Chapitr

e 9

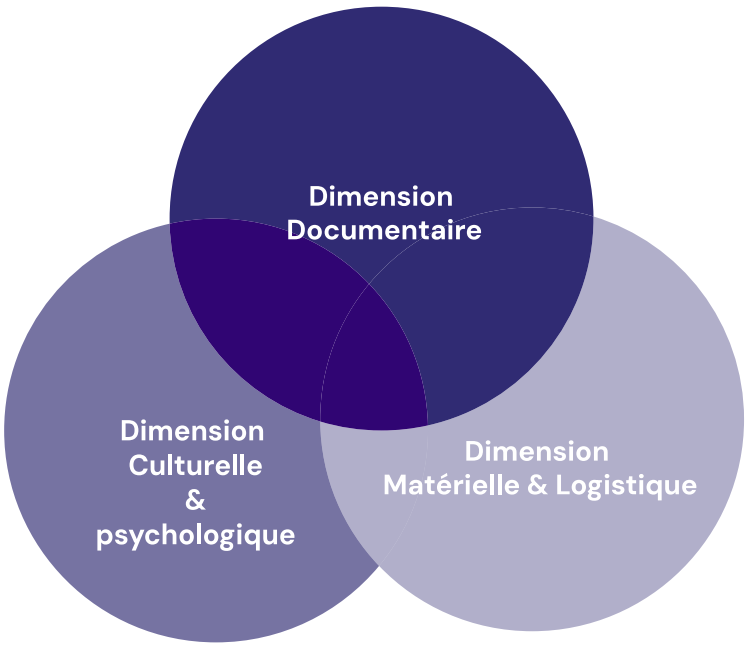
L'efficience des dispositifs de continuité d'activité en cas de crise dépendra directement de la profondeur du questionnement et des investigations préalablement réalisés dans les trois dimensions constitutives de la problématique.

→ Dimension *« documentaire »* tout d'abord qui se concrétise par la rédaction de documents formalisés et régulièrement mis à jour, de planification de la réaction à une catastrophe ou à un sinistre grave.

→ Dimensions *« matérielle et logistique »* qui permettent aux équipes de disposer des équipements et matériels idoines pour répondre à la problématique de destruction de telle ou telle ressources (Bâtiments, problématiques sanitaires, indisponibilités des S.I...).

→ Dimensions *« culturelle et psychologique »* enfin, trop souvent oubliée dans les problématiques de PCA et qui constitue à notre sens la dimension la plus importante. A l'échelle individuelle mais également à l'échelle des équipes des dispositifs de continuité d'activité, il convient de *« Penser l'imprévisible »*, c'est à dire adopter la posture mentale suivante: *« Je dois être prêt à faire face à un événement ou une détérioration de situation que mon savoir, mon expérience et mon intelligence ne peuvent pas imaginer ; je ne sais pas quelle sera la nature de l'agression mais je dois inventorier mes capacités et mes forces pour faire face à l'agression inconnue »*. En complément, au niveau de l'entreprise, il convient d'informer et de former l'ensemble des collaborateurs aux problématiques de continuité d'activité, de gestion de crise mais également aux effets du stress afin de prévenir tout comportement atypique ou pathogène (à l'échelle individuelle et collective), le jour où la crise survient.

Les 3 matériaux de l'efficience du PCA



En synthèse,

Dans un environnement marqué par l'incertitude et la multiplication des crises, le lien entre analyse de risque et PCA devient dès lors fondamental. L'analyse de risque ne se limite plus à un exercice préalable de classement des menaces : elle constitue la colonne vertébrale du PCA, en permettant d'identifier les scénarios majeurs susceptibles d'affecter les activités critiques et de dimensionner des stratégies de continuité réalistes. Sans compréhension fine des vulnérabilités, des interdépendances internes et externes, des points de fragilité humains et techniques, le PCA risque de reposer sur des hypothèses inopérantes au moment de la crise.

Cette exigence est particulièrement manifeste face aux crises climatiques et cyber, qui dépassent largement les schémas traditionnels d'indisponibilité. Les crises climatiques, par leur nature étendue, progressive ou brutale, peuvent provoquer des ruptures simultanées d'infrastructures, d'approvisionnements et de services essentiels, affectant durablement les territoires, les biens et les personnes. Elles remettent en cause les hypothèses usuelles de continuité et imposent de repenser les stratégies de repli, les délais de reprise et les besoins de redondance géographique.

Les crises cyber, quant à elles, illustrent la dépendance critique au numérique des organisations contemporaines. Leur capacité de propagation rapide, leur caractère transversal et leur potentiel d'effet domino sur les systèmes internes et les chaînes d'approvisionnement rendent indispensable une analyse de risque approfondie, centrée sur les actifs critiques, les dépendances technologiques et les scénarios de perte de contrôle ou de confiance dans les données. Sans cette analyse, le PCA ne peut garantir ni la continuité des services numériques essentiels ni un redémarrage maîtrisé des activités. Ainsi, la continuité d'activité doit être appréhendée comme une véritable stratégie d'entreprise, intégrée à la gouvernance et à la gestion globale des risques. Elle constitue un levier majeur de résilience, mais aussi un facteur clé de différenciation et de crédibilité. En renforçant la capacité à faire face aux crises climatiques et cyber, le PCA contribue à sécuriser les trajectoires économiques, à maintenir la confiance des clients, des financeurs et des assureurs, et à renforcer durablement la pérennité des organisations. À l'inverse, celles qui négligent cette approche s'exposent à une fragilisation structurelle dans un contexte où les crises ne sont plus des exceptions, mais des enjeux récurrents.

AD : Active Directory – Service d'annuaire centralisé pour la gestion des identités et accès utilisateurs Windows.
ANSSI : L'Agence nationale de la sécurité des systèmes d'information
API : application programming interface – interface de programmation d'application
BIA : Business Impact Analysis – Analyse d'impact sur l'activité
CERT : Computer Emergency Response Team – Équipe de réaction aux urgences informatiques.
CSE : Comité social et économique
CSIRT : Computer Security Incident Response Team – Équipe de réaction aux incidents de sécurité informatique
CVE : Common Vulnerabilities and Exposures – Les vulnérabilités et expositions courantes
DANA : Depresión Aislada en Niveles Altos – dépression isolée en haute altitude
DDOS : Distributed Denial of Service – Attaque par déni de service distribué
DIMA : Durée d'Interruption Maximale Admissible
DLO : Data Loss Objective – Objectif de perte de données. Volume maximal de données qu'une organisation peut accepter de perdre.
DORA : Digital Operational Resilience Act – règlement européen sur la résilience opérationnelle numérique du secteur financier
DRP : Disaster Recovery Plan – Plan de reprise après sinistre
DSI : Directeur du Systèmes d'Information
EDR : Endpoint detection and response – Détection et réaction aux menaces sur points terminaux
ENISA : Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information
ERP : Entreprise Resource Planing – Progiciel de gestion intégré
IGH : Immeuble de Grande Hauteur
KISS : Keep It Simple and Sexy – "faisons simple et sexy "
KPI : Key Performance Indicator – Indicateur clé de performance
OT : Operational Technology – Technologies opérationnelles
PCA : Plan de Continuité d'Activité
PRA : Plan de Reprise d'Activité
PSI : Plan de Secours Informatique

REC : Résilience des Entités Critiques
REX : Retour d'expérience
RIO : Recovery of Integrity Objective - Objectif de récupération d'intégrité. Délai maximum pour restaurer l'intégrité des données après un incident.
RPCA : Responsable du Plan de Continuité d'Activité
RPO : Recovery Point Objective - Objectif de point de récupération
RTO : Recovery Time Objective - Objectif de temps de rétablissement
SAIV : Secteurs d'Activités d'Importance Vitale
SGDSN : Secrétariat général de la défense et de la sécurité nationale
SIEM : Security Information and Event Management - Gestion d'information et des événements de sécurité.
SLA : Service Level Agreement - Accord de niveau de service.
SOC : Security Operations Center - Centre opérationnel de sécurité
SRAS : Syndrome Respiratoire Aigu Sévère
SSIAP : Service de sécurité incendie et d'assistance aux personnes

À PROPOS DE L'AMRAE

Ancrer la gestion des risques au cœur de la performance et de la résilience des organisations.

L'**Amrae** (Association pour le Management des Risques et des Assurances de l'Entreprise), regroupe les principaux acteurs de la gestion des risques (gestion des risques, contrôle interne et audit, assurance et juridique). À travers ses comités scientifiques, ses publications, ses prises de position et son congrès, elle œuvre pour l'excellence en matière de risk management, qui contribue à sécuriser la stratégie des entreprises et à organiser leur résilience. L'Amrae regroupe environ 2000 membres issus de 850 organisations privées et publiques.

Une gestion des risques éclairée et inscrite dans la durée constitue le socle de la résilience des entreprises. Elle vise à absorber les chocs, à assumer leur responsabilité et à saisir les opportunités, tout en déployant une croissance durable et responsable. Ses bénéfices irriguent les entreprises, leur écosystème et l'ensemble du tissu économique.

L'Amrae a comme missions fondamentales :

→ **CULTURE DU RISQUE**
→ **EXPERTISE**
→ **FORMATION & CONGRÈS**

AMRAE
la Maison du risk management

36 boulevard Sébastopol
75004 Paris
Tél. : 01 42 89 33 16

amrae.fr