Juillet 2015

Ce kit est destiné aux entrepreneurs, dirigeants de TPE et PME, artisans, commerçants et professions libérales pour leur permettre d'assurer la continuité de leur activité, en cas d'événement perturbateur lors d'une crise majeure d'origine naturelle, accidentelle ou malveillante.

KIT PCA à l'usage du chef d'entreprise en cas de crise majeure

Dirigeants de TPE-PME, artisans, commerçants, professions libérales, comment faire face à une crise majeure: les démarches propres de l'entreprise, les interfaces avec les dispositifs publics

Comment réaliser un plan de continuité d'activité (PCA)
en situation de crise majeure,
et pistes pour se préparer en amont.

DGE
DIRECTION GÉNÉRALE DES ENTREPRISES

CGPME

*

* *

Ce kit contient

Pour plus d'informations

- Guide d' « hygiène informatique » de l'ANSSI
- Guide ANSSI-CPME des bonnes pratiques de l'informatique
- Guide ENISA sur le "*cloud*" pour les PME (*Cloud Security Guide for SMEs - ENISA*)

... et encore davantage :

- Guide du SGDSN sur les plans de continuité d'activité
- Norme ISO 22301 sur la continuité d'activité
- Norme ISO 27000 sur le management du risque

Questions en cas d'événements redoutés survenant lors d'une crise majeure

Face à des événements redoutés occasionnés par une crise majeure, quelles sont les questions à se poser ?

Evénements perturbateurs

De nombreux événements – externes ou internes - sont susceptibles de perturber plus ou moins gravement l'activité d'une PME – TPE, comme :

- des accidents du travail, des maladies
- la disparition d'une personne clé,
- des produits défectueux,
- un incendie destructeur, un bris de machine,
- des vols, des sabotages,
- une défaillance de fournisseur,
- une coupure électrique, des problèmes de transport
- une défaillance de clients
- la dégradation d'un risque pays
- une défaillance informatique
- une attaque informatique
- une attaque terroriste
- une campagne de désinformation, un vol de patrimoine immatériel, une attaque financière…

Crises[1] majeures

Certains de ces événements peuvent survenir lors d'une crise majeure, c'est-à-dire d'ampleur massive et justifiant l'intervention des pouvoirs publics pour une gestion collective.

Différents risques majeurs d'origine naturelle, accidentelle ou malveillante sont susceptibles de se produire sur tout ou partie du territoire national, en particulier :

- des catastrophes naturelles ou sanitaires : intempéries (épisode neige-verglas, tempête…), des inondations (à déroulement rapide ou lent), des séismes (tremblements de terre…), des pandémies (grippe ou autre)

[1] Rappel succinct de ce qui caractérise une situation de crise (interne ou externe) :
- Soudaineté du phénomène et urgence des mesures à prendre
- Complexité de la situation due à l'accumulation erratique d'informations
- Irrationalité due à la désagrégation du système ou de l'organisation, et à la perte de références.

On appelle crise tantôt la situation ainsi caractérisée qu'on veut remettre sous contrôle, tantôt une situation qu'on gère en mode «crise» pour éviter qu'elle ne dégénère ainsi.
Ceci justifie d'encourager une PME/TPE à faire appel aux pouvoirs publics, comme l'explique le guide.

- des accidents majeurs : coupures électriques prolongées, interruptions de transport, accidents de toute nature
- des cyberattaques, des actions malveillantes (dont terrorisme)
- de tels évènements ou des « risques politiques » survenant à l'étranger qui peuvent avoir des conséquences sur le territoire national.

Les questions à se poser

A/ interrogations préalables

- l'entreprise est-elle vulnérable ?
- faut-il choisir entre se mettre à l'abri et continuer son activité ?
- à quels types de situation faire face ?
- à quel moment faire appel à un soutien externe ?

B/comment procéder en urgence ?

S'organiser

- comment l'entreprise est-elle informée ?
- peut-elle réunir une cellule de crise et assurer sa communication ?
- dispose-t-elle de relais pour faciliter son action ?

Agir

- comment protéger le personnel et l'outil de travail ?
- passer en mode dégradé pour maintenir tout ou partie de son activité ?
- recourir à un dispositif de repli si le site de l'entreprise est inutilisable ?
- rétablir une activité normale dans les meilleurs délais ?

C/ Gérer de multiples aspects

La gestion d'une crise majeure présente de multiples composantes (production, RH, informatique, relations avec les clients et fournisseurs, communication …) pour construire une réponse efficace. Une réponse élaborée en urgence a nécessairement des limites, qu'une préparation en amont permet de dépasser.

A/ interrogations préalables

Quels impacts sur l'activité de l'entreprise ?

Outre les dommages possibles, l'activité de l'entreprise peut être impactée de différentes manières :

- directement : le personnel, l'outil de travail sont touchés ou affectés,
- indirectement : des fournisseurs, des clients, les transports, des services publics essentiels sont touchés ; par ailleurs, les mesures prises par les pouvoirs publics peuvent générer des contraintes (confinement, évacuation massive, définition de priorités …).

NB : Selon les cas, c'est la capacité de l'entreprise à produire ou délivrer le produit ou celle de la clientèle à l'absorber qui sont atteintes.

Quelle attitude générale adopter ?

En cas d'impact négatif ou de menace sur l'entreprise, il y a deux attitudes à adopter, plus complémentaires que contradictoires :

- se « mettre à l'abri » pour éviter ou limiter les dégâts, quitte à suspendre son activité, voire à fermer temporairement l'entreprise si c'est nécessaire : il s'agit de préserver ses actifs et ceux des tiers (données détenues …) en prenant des mesures conservatoires ou de repli, en évitant l'aggravation de la situation et le sur-accident ;
- dans la mesure du possible, maintenir ou reprendre une activité minimale afin de garder sa place sur le marché, quitte à passer en mode dégradé avec des moyens réduits ; en toute hypothèse, rétablir son activité le plus tôt possible, avec les moyens disponibles.

Le cas particulier des entreprises « contributives »

Certaines entreprises peuvent être appelées à fournir des prestations supplémentaires en cas de crise, qu'elles y soient tenues - contractuellement (ex : prestataire informatique) ou réglementairement (réquisition) - ou sollicitées par leurs clients (pour compenser la défaillance d'un autre fournisseur) ou encore par les pouvoirs publics.

Les entreprises juridiquement engagées doivent avoir pris les dispositions nécessaires (pratiques ou juridiques, décrites de préférence dans un PCA formalisé, voire certifié). Pour celles sollicitées à titre facultatif, ce peut être une opportunité.

Ex : fourniture de groupe électrogène, *back-up* de systèmes d'information, mobilisation d'engins de travaux publics.

Trois situations types

Pour apprécier la situation concrète et préparer la réponse, on distingue trois grands types de situations, qui appellent des modes de réponse adaptés :

1) un épisode bref et brutal

Ex : tempête, neige et verglas, inondation de type méditerranéen.

Il convient de se mettre à l'abri, pour protéger son personnel et ses installations, quitte à suspendre l'activité en attendant la fin de l'épisode.

2) un épisode prolongé

Ex : pandémie, collaborateurs touchés, dégradation de la situation d'un pays, attaque informatique majeure.

Outre les mesures 1, il est souhaitable de maintenir ou reprendre les activités prioritaires dans un délai rapide.

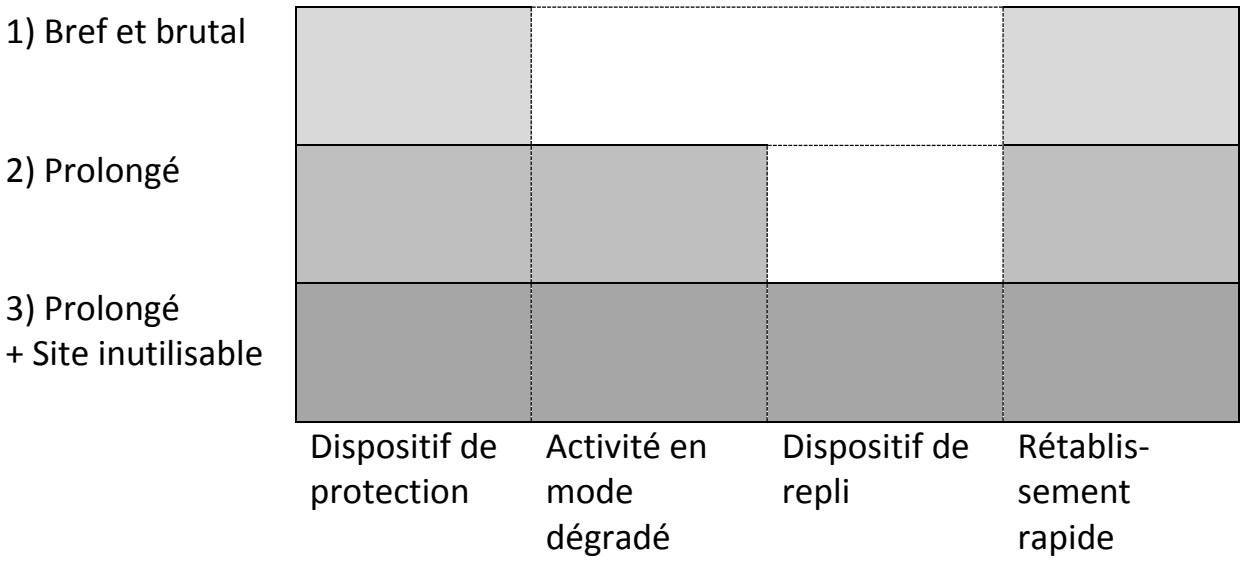
3) un épisode prolongé avec site de l'entreprise inutilisable (indisponible ou inaccessible)

Ex : inondation longue, séisme, incendie majeur.

Outre les mesures 1 et 2, il s'agit de mettre en œuvre, de surcroit, un dispositif de repli pour la partie de l'entreprise « repliable ».

Réponse (entreprise impactée)

Situation type selon l'épisode



B/ Comment procéder en urgence (règles de base) ?

Les situations vécues varient considérablement selon les circonstances, mais il y a des règles de base pour la conduite à tenir en cas d'événement avéré.

S'organiser

1) **Se tenir informé de la situation**
   - recevoir les alertes,
   - récupérer les consignes et informations données par les autorités publiques.

   Principaux moyens : radio (toujours) et :
   - dispositifs d'alerte publics : le système d'alerte et d'information des populations (SAIP)[2]
   - sites dédiés :
     - sites permanents dédiés à un risque

     Ex: Vigicrues, Sytadin pour la connaissance du trafic routier en Ile-de-France, plan Pandémie...
     - sites temporaires dédiés à une crise (sites Internet dédiés par les administrations en charge de la gestion de crise, avec accès plus ou moins ouvert aux entreprises intéressées).

     Ex : projet de site d'informations opérationnelles à l'étude pour le risque inondation en Île-de-France.

     Ex: cellule de crise du ministère des affaires étrangères pour la recherche et le rapatriement des citoyens français pris dans une crise à l'étranger.

2) **Se mettre en mode «crise»**
   - évaluer la gravité et la cinétique de la crise,
   - constituer une cellule de crise [3],
   - communiquer : en interne (personnel) sur la situation de l'entreprise et les mesures prises ; en externe (clients, fournisseurs, partenaires, médias) pour échanger des informations, se coordonner, défendre son image.

Principaux moyens : téléphone portable et Internet, salle de réunion organisée en cellule de crise.

[2] en cours de mise en place par le ministère de l'intérieur
[3] éventuellement avec l'aide d'un organisme d'assistance

3) identifier des organismes relais

- relais officiels :
  Préfectures : directions de la sécurité publique
  Site Internet de la DGE[4] pour l'orientation et la fourniture de liens
  Services territoriaux de l'Etat (en fonction du secteur économique)
  Collectivités territoriales
- relais institutionnels :
  Organisations patronales interprofessionnelles (dont la CGPME)
  Organisations professionnelles
  Comités territoriaux
  Unions territoriales (CGPME territoriales)
  Chambres consulaires (Vigipirate ...)
- prestataires et partenaires :
  Organismes de conseil, plateformes de veille et de formation
  Organismes d'assurance, organismes d'assistance
  Groupements d'entreprises (GIE, association …).

Note : les modes de relations avec ces organismes peuvent varier considérablement suivant les lieux et les circonstances.

Agir

4) **Se protéger** :

L'objectif est d'éviter des dommages inutiles et permettre une reprise rapide.

- protéger son personnel et l'outil de travail (lieu de travail ; équipements ; système d'information, données et dossiers) :
  - GRH : ajuster l'organisation et les modalités de travail (horaires …), recourir au travail à distance (en mode «crise»)[5], prendre des mesures d'hygiène, distribuer des équipements de protection individuelle ; mesures Vigipirate (pour les ERP) ; apporter si possible un soutien au personnel victime …

[4] http://www.entreprises.gouv.fr/

[5] En période de crise majeure, l'employeur peut imposer le travail à distance pour une durée limitée aux personnels à qui il est demandé de ne pas se rendre sur leur lieu de travail. Principales modalités : identifier les personnels concernés, recueillir si possible leurs coordonnées téléphoniques et adresses courriel, recenser les matériels informatiques disponibles ou mis à disposition, prévoir les modalités de communication entre le service et le domicile, identifier les tâches à mener.

- système d'information : sauvegarder les données (*back-up* par le prestataire informatique, utilisation du « *cloud* ») ; assurer le traitement informatique en cas de cyber-menace,
- installations : assurer la protection physique des sites et des matériels ; si nécessaire assurer l'arrêt de l'outil « en sécurité » ; assurer le gardiennage des sites fermés,

- suspendre tout ou partie de l'activité si nécessaire.

5) Maintenir une activité minimale en passant en mode dégradé

L'objectif est de s'assurer d'un flux d'activité minimal.

- identifier les activités prioritaires et vérifier les moyens mobilisables :
  - identifier les activités prioritaires en fonction des besoins des clients essentiels (délais[6] …) et définir ses priorités en conséquence,
  - vérifier l'état des fonctions vitales de l'entreprise nécessaires à ces activités (processus métiers et supports : ex : production, délivrance des produits, relations fournisseurs, comptabilité…),
  - vérifier la disponibilité des ressources minimales pour fonctionner (effectifs « prioritaires », système d'information, locaux, fournisseurs) ;

- fonctionner en mode dégradé :
  - choisir entre abaissement général du service et tri des bénéficiaires,
  - activer toutes solutions palliatives utiles,
  - assurer un traitement métier pendant une indisponibilité informatique (ex : passage en mode manuel),
  - demander, s'il y a lieu, un accès prioritaire aux "réseaux" (énergie, eau, communications électroniques) via le dispositif ORSEC Rétap réseaux[7].

[6] notion de délai maximal d'interruption acceptable (DMIA)

[7] Le guide ORSEC Rétap réseaux (mars 2015) prescrit le processus de hiérarchisation des priorités en cas de rupture d'alimentation en matière de fluides. Il prévoit d'établir des listes départementales d' « usagers sensibles » sélectionnés en fonction de leur sensibilité aux ruptures d'alimentation et classés selon différents enjeux, dont un enjeu « économie » (usagers dont la rupture d'alimentation entraîne une perturbation importante et durable dans l'économie du département, de la région ou de la nation). Les listes, nominatives, sont pré-établies et servent, en cas de crise, de fondement aux décisions prises en fonction de la situation réelle du moment. Les préfets sont chargés d'établir ces listes sur proposition des communes et de les exploiter à chaud pour définir les « vraies » priorités.
Les entreprises souhaitant savoir si elles peuvent bénéficier de ces dispositions sont invitées à se rapprocher de la préfecture du ressort du site concerné pour obtenir les précisions nécessaires.
Le guide est accessible par les liens suivants :
http://www.economie.gouv.fr/hfds/service-secretaire-general-haut-fonctionnaire-defense-et-securite
http://www.interieur.gouv.fr/Le-ministere/Securite-civile/Documentation-technique/Planification-et-exercices-de-Securite-civile

6) **Se délocaliser en cas de site inutilisable** (indisponible ou inaccessible)

Trois volets :

- le transfert des données et des applications sur un dispositif de secours lui-même sécurisé (*back-up*, *cloud*…) (structure amie ou prestataire de confiance),
- le transfert physique – de ce qui peut être transféré - sur un site de repli sécurisé (implantation « sœur », structure amie, prestataire privé, site public d'accueil temporaire) : savoir où aller, transférer ce qui est transférable ; protéger ce qui doit rester sur place,
- le travail à distance pour le personnel maintenu à domicile.

De façon générale, il est nécessaire de privilégier les moyens nomades (micro portables, clés USB, téléphones portables …).

7) Rétablir l'activité le plus tôt possible

C'est généralement un impératif vital pour l'entreprise.

- Assurer le retour à la normale :
  - organiser la montée en puissance du retour à la normale (priorités, étapes), si celui-ci ne peut être immédiat après la phase d'urgence,
  - réaliser diagnostics et travaux sur les installations touchées (électricité …),
  - développer sans attendre des solutions pragmatiques provisoires pour une reprise d'activité progressive.
- Engager le moment venu des demandes d'indemnisation s'il y a lieu :
  - chômage technique,
  - assurance dommages ou pertes d'exploitation,
  - responsabilité civile de l'auteur de l'accident,
  - fonds d'indemnisation le cas échéant.

C/ Pistes pour se préparer en amont

La réactivité et le pragmatisme sont nécessaires pour faire face à une crise en urgence, mais il est préférable de se préparer également en amont, en particulier face aux cyber-menaces.

Eléments d'expérience

Se préparer à l'avance permet, en vue de mieux absorber les impacts d'une crise majeure :

- de disposer de mesures plus efficaces et de listes prédéfinies

Certaines mesures ne sont efficaces pour se protéger que si elles sont prises en amont (l'exemple typique est celui du rançonnage qui est sans effet si les données ont été correctement sauvegardées mais qu'il est très difficile de contrer à défaut). L'expérience montre également que les « *check-lists* » d'actions à réaliser permettent d'éviter les omissions qui se produisent fréquemment dans l'urgence (en particulier en termes de communication).

- de mieux identifier les cibles à protéger, les activités à maintenir, les délais disponibles, les relais à utiliser le cas échéant

Il est fondamental d'identifier son patrimoine essentiel (patrimoine propre et données détenues concernant des tiers), ses activités prioritaires en fonction notamment des besoins de ses clients critiques, les délais acceptables en cas d'interruption d'activité, les relais sur lesquels s'appuyer si nécessaire. Pour bien faire, l'identification devrait se faire plutôt en amont et non pendant l'émergence d'une crise.

- d'améliorer la perception de l'entreprise par les parties intéressées

Un minimum de préparation est de nature à accroître la confiance de ses partenaires économiques (donneurs d'ordre, clients …) dans sa capacité à maintenir son activité, à répondre à leurs besoins essentiels et à renforcer sa résilience. Une gestion défectueuse en période d'urgence peut au contraire détériorer l'image de l'entreprise.

Consistance d'un PCA et coût

Le PCA est un dispositif qui prend racine dans une démarche amont de management du risque. Il offre la possibilité de gérer des incertitudes et aléas, associés à des événements indésirables identifiés a priori. Le PCA a pour vocation de « repousser » le moment où on bascule dans une situation de crise. Il sert à mieux anticiper et gérer une situation de crise majeure.

a. Mettre en place une démarche de management du risque formalisée par un PCA

- Identifier le patrimoine essentiel (humain, matériel, immatériel) et les activités prioritaires à préserver ou protéger,
- Identifier les scénarios d'événements indésirables à prendre en compte *a priori* dans le dispositif de management du risque et de gestion de crise,
- Définir les mesures de prévention et de protection prédéterminées à mettre en place en cas d'occurrence de ces scénarios,
- Définir le processus de gestion de crise, définir les rôles et interfaces,
- Formaliser tous ces éléments dans un PCA comportant en particulier un volet continuité informatique, un volet dispositif de repli des utilisateurs et un volet gestion de crise.

b. Se préparer à la gestion des événements en cas d'occurrence

- Sensibiliser les personnels,
- Procéder à des exercices de crise pour tester le dispositif et les mesures (exercices spécifiques à l'entreprise ou collectifs).

c. Coût de réalisation

La notion de continuité d'activité est plus ou moins intense selon les activités (ex : très forte intensité dans certaines activités financières et informatiques).
La tendance générale est à une élévation progressive des souhaits et préoccupations des donneurs d'ordre et des régulateurs.
Pour les PME, la question se pose du coût en termes de budget, de temps et d'énergie pour l'élaboration d'un PCA. Un PCA est nécessairement tributaire de données externes et soumis à des économies d'échelle, ce qui est plus favorable aux grandes entreprises.
La production d'outils standards adaptés aux PME et les regroupements d'entreprises (secteur ou profession, territoire, partenaire structurant …) pour réduire et partager les coûts et accélérer les retours d'investissement à en attendre sont des voies à explorer.

Annexe - Fiche cyber-continuité et cyber-sécurité

Cyber-continuité

Actions en prévention

- Déterminer une politique sécurisée de sauvegarde redondante (locale et externe) des données.
- Définir un dispositif de secours pour les applications vitales, par exemple par transfert dans un *cloud* sécurisé[8].
- S'assurer que le ou les prestataires informatiques à activer en cas de menace sont eux-mêmes en capacité de continuer leur activité dans une telle situation et placent l'entreprise parmi leurs clients essentiels à soutenir en cas de besoin.

Actions à mener en cas de menace effective

- Transférer les données récentes et les applications vitales sur des dispositifs de sauvegarde et de secours (dispositifs nomades – ex : micros portables, disques durs externes, clés – ou fixes sécurisés – ex : serveur délocalisé, *cloud* sécurisé …).
- Activer son ou ses prestataires informatiques.
- Utiliser tous les moyens palliatifs afin de maintenir l'activité économique (ex : passer en mode manuel, continuer la relation clientèle par téléphone, etc.).

Cyber-sécurité

Actions à mener en prévention (hygiène numérique)

- Précaution matérielle et logicielle :
  - Cartographier les installations critiques permettant la continuité de l'activité économique et commerciale (lister les serveurs ou postes de travail).
  - Pratiquer une séparation ou une isolation des réseaux afin de contenir une éventuelle contamination.
  - S'équiper de logiciels antivirus et mettre en place des règles de pare-feu.
  - Installer sans attendre les mises à jour en provenance directe de l'éditeur du logiciel ; ne pas installer des logiciels non demandés.
  - Déterminer une politique sécurisée de sauvegarde redondante (locale et externe) des données.
  - Favoriser les canaux chiffrés en cas de transmission de données (sites en https, connexions ftp via une « tunnelisation » ssh, serveur de messagerie disposant d'un protocole chiffré activé, etc.).

[8] Se renseigner auprès de l'ANSSI

- Précautions humaines :
    - Identifier clairement les responsables des systèmes d'information.
    - Tenir à jour une liste constituée d'un vivier de spécialistes en informatique.
    - Sensibiliser et responsabiliser le personnel régulièrement.
    - Ne pas ouvrir les pièces jointes en provenance d'expéditeurs inconnus, ou ayant un caractère distractif ou non professionnel à partir d'un poste professionnel.
    - Eviter de cliquer sur les liens contenus dans des courriels, en particulier en présence d'un environnement douteux ou d'urgence.
    - Utiliser des mots de passe composés de lettres, chiffres et caractères spéciaux autant sur les applications internes que sur les sites externes.

Actions à mener en cas d'intrusion effective ou de suspicion d'intrusion

- Détecter l'intrusion (mauvais fonctionnement, réactions aberrantes …).
- Contacter immédiatement le responsable ou prestataire de confiance du système d'information, afin qu'il prenne en charge le traitement informatique.
- Utiliser tous les moyens palliatifs afin de maintenir l'activité économique (ex : passer en mode manuel, continuer la relation clientèle par téléphone, etc.).