

MODÈLE

Plan de continuité d'activité (PCA/PRA) simplifié

Un modèle prêt à remplir pour garder votre PME opérationnelle face à un rançongiciel, une panne ou un sinistre — du BIA aux procédures de reprise.

Sedona Radar — audit de sécurité externe automatisé

Sedona AI Lecture ~12 min Édition 2026 sedona-ai.com

Un plan de continuité (PCA) et un plan de reprise (PRA) transforment une crise — rançongiciel, panne, sinistre — en incident maîtrisé plutôt qu'en arrêt fatal. Ce modèle vous guide pas à pas : cartographier vos activités critiques (BIA), fixer un RTO et un RPO par système, préparer les scénarios et écrire les procédures de bascule et de reprise. Remplissez les champs entre crochets et vous obtenez un plan concret, testable et proportionné à une PME, sans jargon superflu.

À retenir

- Le PCA maintient vos activités métier essentielles pendant la crise (y compris en mode dégradé sans informatique) ; le PRA remet en service l'infrastructure IT. Ce sont deux volets complémentaires, pas un seul document.
- Tout commence par le BIA (analyse d'impact) : sans hiérarchisation de vos activités critiques, impossible de fixer des priorités de reprise réalistes.
- Le RTO répond à « combien de temps sans ce système ? » et le RPO à « combien de données peut-on perdre ? ». Ces deux curseurs dictent votre stratégie de sauvegarde et de secours.
- Le scénario rançongiciel est à part : il peut chiffrer aussi vos sauvegardes si elles sont connectées. Des sauvegardes déconnectées ou immuables sont la condition d'un RPO réel.
- En 2025, 48 % des victimes de rançongiciels traitées par l'ANSSI étaient des TPE, PME et ETI (contre 37 % en 2024) : les petites structures sont désormais des cibles de premier plan.
- Un plan n'existe que s'il est testé et maintenu. Planifiez un exercice au moins une fois par an et après tout changement majeur du système d'information.

01 Comment utiliser ce modèle

Ce document est une trame à remplir. Chaque champ [entre crochets] est une zone à compléter avec vos propres données. Parcourez les sections dans l'ordre : le BIA (section 3) alimente les RTO/RPO (section 4), qui conditionnent les scénarios (section 5) puis les procédures (section 6). Comptez une demi-journée d'atelier avec les responsables métier et le référent informatique pour une première version exploitable.

1. Renseignez l'en-tête

Organisation : [nom]. Périmètre couvert : [sites / entités / activités]. Version : [v1.0]. Date : [JJ/MM/AAAA]. Responsable du plan (RACI) : [nom, fonction]. Prochaine revue prévue : [date].

2. Complétez chaque tableau

Remplacez tous les [placeholders] par vos valeurs. Ne laissez aucune cellule vide : « non applicable » est une réponse valable et traçable.

3. Faites valider et testez

Faites relire par la direction, puis planifiez un exercice de simulation. Un plan non testé est une hypothèse, pas une garantie.

Ce modèle n'est pas une certification

Il vous aide à structurer votre démarche. La norme de référence, ISO 22301:2019, exige un système de management complet (gouvernance, tests, amélioration continue) qui va bien au-delà de ce document. Utilisez cette trame comme point de départ, pas comme preuve de conformité.

02 PCA, PRA, réponse à incident : ne pas confondre

Trois dispositifs se complètent sans se substituer. Les distinguer clairement évite les angles morts le jour J. Le PCA relève du métier, le PRA de l'informatique, et le plan de réponse à incident (PRI) de la sécurité technique.

Dispositif	Objectif	Question centrale
PCA — Plan de continuité d'activité	Maintenir les activités métier essentielles pendant la perturbation, y compris en mode dégradé (sans SI)	Comment continue-t-on à servir les clients malgré la crise ?
PRA — Plan de reprise d'activité	Remettre en service l'infrastructure informatique après l'incident	Comment relance-t-on les systèmes et restaure-t-on les données ?
PRI — Plan de réponse à incident	Détecter, qualifier, contenir et éradiquer techniquement l'attaque	Comment arrête-t-on et élimine-t-on l'incident de sécurité ?

Recommandation ANSSI

Dans sa doctrine de préparation aux crises cyber, l'ANSSI recommande de disposer à la fois d'un PCA « robuste aux cyberattaques » et d'un PRA. La distinction PCA (métier) / PRA (IT) présentée ici est la convention usuelle du secteur ; l'ANSSI insiste surtout sur l'existence des deux volets.

03 Étape 1 — BIA : identifier vos activités critiques

L'analyse d'impact sur l'activité (Business Impact Analysis) est le socle de tout PCA/PRA. Elle consiste à lister vos activités, évaluer l'impact d'une interruption dans le temps (financier, opérationnel, réglementaire, réputationnel) et en déduire des priorités de reprise. C'est ce travail qui rendra vos RTO/RPO crédibles plutôt qu'arbitraires.

Activité / processus	Impact d'une interruption	Durée max tolérable	Priorité de reprise
[ex. Prise de commande client]	[perte de CA, clients bloqués, pénalités]	[ex. 4 h]	[1 — Vitale]
[ex. Paie / comptabilité]	[retard salaires, sanction, tension sociale]	[ex. 3 jours]	[2 — Importante]
[ex. Site web vitrine]	[image, faible impact opérationnel]	[ex. 1 semaine]	[3 — Différable]
[activité 4]	[impact]	[durée]	[priorité]

Astuce de priorisation

Classez sur 3 niveaux (Vitale / Importante / Différable) plutôt que sur une échelle fine. En PME, la simplicité de la grille garantit qu'elle sera réellement utilisée et tenue à jour.

04 Étape 2 — Fixer les RTO et RPO

Le RTO (Recovery Time Objective) est la durée maximale d'indisponibilité tolérable avant que l'impact ne devienne inacceptable. Le RPO (Recovery Point Objective) est la quantité de données, mesurée en temps, que vous acceptez de perdre entre la dernière sauvegarde valide et l'incident. Ces définitions sont issues du standard de référence NIST SP 800-34. Le RPO dicte la fréquence de sauvegarde ; le RTO dicte les moyens de bascule.

Système / donnée	RTO (indispo. max)	RPO (perte de données max)	Stratégie de sauvegarde / secours
[ex. ERP / base clients]	[ex. 4 h]	[ex. 1 h]	[réplication + sauvegarde horaire déconnectée]
[ex. Messagerie]	[ex. 8 h]	[ex. 24 h]	[sauvegarde quotidienne cloud UE]
[ex. Serveur de fichiers]	[ex. 2 jours]	[ex. 24 h]	[sauvegarde quotidienne + copie hors ligne]
[système 4]	[RTO]	[RPO]	[stratégie]

RTO/RPO ne sont pas des obligations légales françaises

Ce sont des concepts d'ingénierie (standardisés par le NIST, largement repris en France), pas des exigences réglementaires. Ils vous servent à dimensionner vos moyens, pas à cocher une case de conformité. Fixez-les selon votre tolérance réelle au risque.

05 Étape 3 — Scénarios : rançongiciel, panne, sinistre

Un plan se prépare par scénario. Trois familles couvrent l'essentiel des perturbations d'une PME. Pour chacune, décrivez la réponse de continuité (comment tenir en mode dégradé) puis la bascule et la reprise (comment revenir à la normale).

Scénario	Déclencheur	Réponse continuité (mode dégradé)	Bascule / reprise
Rançongiciel	[chiffrement des postes/serveurs, demande de rançon]	[isolement réseau, procédures papier, cellule de crise]	[restauration depuis sauvegarde déconnectée/immuable après éradication]
Panne matérielle ou cloud	[serveur HS, indisponibilité fournisseur]	[report sur système de secours, dégradation temporaire]	[réparation/remplacement, restauration selon RTO/RPO]
Sinistre physique	[incendie, dégât des eaux, coupure prolongée]	[repli sur site/télétravail, matériel de substitution]	[réinstallation locaux, remontée de l'infrastructure]

48 %

des victimes de rançongiciels traitées par l'ANSSI en 2025 étaient des TPE, PME et ETI (contre 37 % en 2024)

ANSSI, Panorama de la cybermenace 2025

Le rançongiciel s'attaque aussi à vos sauvegardes

Contrairement à une panne, un rançongiciel peut chiffrer ou exfiltrer les sauvegardes si elles restent connectées au réseau. Sans copie déconnectée ou immuable, votre RPO théorique s'effondre. C'est le point le plus souvent négligé, et le plus déterminant pour survivre à l'attaque.

06 Étape 4 — Procédures de bascule et de reprise

Décrivez qui fait quoi, dans quel ordre, avec quels moyens. Les procédures doivent être exécutables par une personne sous stress, éventuellement sans accès aux systèmes habituels. Conservez une version hors ligne (papier ou support déconnecté).

1 Alerter et déclencher

Qui déclenche le plan : [nom / fonction]. Cellule de crise : [membres]. Canal de communication de secours (hors SI compromis) : [ex. numéros mobiles, messagerie externe].

2 Contenir et isoler

Actions immédiates : [isolement réseau, coupure des accès, préservation des preuves]. Ne jamais restaurer avant d'avoir confirmé l'éradication avec le référent sécurité : [nom].

3 Basculer en mode dégradé

Procédures métier de secours par activité vitale : [décrire]. Systèmes de secours à activer : [listier].

4 Restaurer et vérifier

Ordre de restauration selon priorités du BIA : [1, 2, 3...]. Sauvegarde utilisée : [source déconnectée/immuable]. Test d'intégrité avant remise en production : [oui/non, responsable].

5 Revenir à la normale et informer

Critères de retour nominal : [définir]. Communication clients / autorités : [notification CNIL sous 72 h si violation de données personnelles (RGPD art. 33), dépôt de plainte, information des clients concernés].

☐ Sauvegardes déconnectées ou immuables testées et restaurables

☐ Annuaire de crise à jour (internes, prestataires, assurance, autorités)

☐ Copie hors ligne du plan accessible sans le SI

☐ Contrat d'assurance cyber et coordonnées du prestataire de réponse à incident identifiés

☐ Contacts utiles notés : ANSSI, CERT-FR, cybermalveillance.gouv.fr, dépôt de plainte

07 Étape 5 — Tester, maintenir, améliorer

Un PCA/PRA n'a de valeur que testé. La logique d'amélioration continue (Planifier-Déployer-Contrôler-Agir, le cycle PDCA) portée par ISO 22301:2019 s'applique à toute taille d'organisation. Programmez des exercices, tirez-en des enseignements, mettez le plan à jour.

- Exercice de simulation : au moins [1 fois par an] et après tout changement majeur du SI
- Test de restauration réelle des sauvegardes : [fréquence] — vérifier le RPO effectif, pas seulement l'existence des sauvegardes
- Revue du plan : responsable [nom], échéance [date], à chaque évolution d'activité, d'infrastructure ou d'équipe
- Journal des versions et des exercices : [conserver la traçabilité des tests et des corrections]

ISO 22301, un cap et non une case à cocher

ISO 22301:2019 (« Sécurité et résilience — Systèmes de management de la continuité d'activité — Exigences ») est un système de management certifiable, comme ISO 27001. Ce modèle vous met sur la trajectoire ; la certification, elle, suppose une démarche organisationnelle complète.

08 Anticiper avec Sedona

Un PCA/PRA robuste suppose de connaître ce qui est exposé et vulnérable. Sedona Radar analyse ce que votre domaine expose sur Internet et classe les vulnérabilités par gravité : de quoi nourrir vos scénarios d'attaque externe avec des faits, pas des suppositions. Il ne remplace pas l'analyse d'impact (BIA), qui porte sur vos activités.

Radar évalue, il ne certifie pas

Radar vous donne un rapport daté de votre exposition externe. Il ne certifie rien : il n'existe aucune certification NIS2. C'est un complément amont d'un plan de réponse à incident et d'un PCA/PRA.

Besoin d'un regard humain ? Nos audits OSINT (à partir de 1 900 € HT) et audits de surface manuels (à partir de 4 500 € HT) approfondissent la cartographie. Le PCA/PRA gère la continuité métier ; le plan de réponse à incident traite l'attaque : les deux se préparent, idéalement avant la crise.

§ Sources

1. ISO 22301:2019 — Sécurité et résilience, Systèmes de management de la continuité d'activité, Exigences — <https://www.iso.org/standard/75106.html>
2. ANSSI — cyber.gouv.fr, Anticiper et gérer une crise cyber — <https://cyber.gouv.fr/securisation/gestion-de-crise/anticiper-gerer-une-crise-cyber/>
3. ANSSI — Panorama de la cybermenace 2025 — <https://cyber.gouv.fr/nous-connaître/publications/panoramas-de-la-cybermenace/panorama-de-la-cybermenace-2025/>
4. CERT-FR — Panorama de la cybermenace 2025 (CERTFR-2026-CTI-002) — <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2026-CTI-002.pdf>
5. NIST SP 800-34 Rev. 1 — Contingency Planning Guide for Federal Information Systems — <https://csrc.nist.gov/publications/sp/800/34/r1/final>
6. Cybermalveillance.gouv.fr — Rapport d'activité 2025 — https://www.cybermalveillance.gouv.fr/medias/2026/03/RA_2025_Cybermalveillance_gouv_fr.pdf
7. SGDSN — Guide de la continuité d'activité (portail officiel) — <https://guide-continuite-activite.sgdsn.gouv.fr/>

Cartographiez ce qui est exposé avant la crise

Sedona Radar analyse ce que votre domaine expose sur Internet : de quoi nourrir vos scénarios d'attaque externe. Le plan Discovery est gratuit : un scan pour voir ce qu'un attaquant voit.

Lancer mon scan gratuit

sedona-ai.com/scan-gratuit