Sécurité, Maintenance

Plan de reprise après incident Le minimum vital pour une PME

Une sauvegarde ne suffit pas si personne ne sait quoi faire le jour de l’incident. Un plan de reprise aide une PME à identifier les priorités, les responsabilités, les accès critiques, les délais acceptables et les premières décisions à prendre pour remettre un site, une messagerie ou un service numérique en fonctionnement.

Publié le 9 juin 2026

Un plan court, utile et disponible avant l’incident

Un plan de reprise après incident n’est pas réservé aux grandes entreprises. Pour une PME, il peut tenir en quelques pages, à condition de répondre aux bonnes questions : qui décide, qui intervient, quels services doivent repartir en priorité, où sont les sauvegardes, quels accès sont nécessaires, qui prévenir, et dans quel délai ?

Le dossier sur les sauvegardes répondait à la question : avons-nous de quoi restaurer ? Ce dossier répond à la question suivante : sommes-nous capables de reprendre l’activité de manière organisée ?

Un incident peut être technique, humain ou cyber : mise à jour qui casse le site, panne serveur, suppression accidentelle, compromission WordPress, messagerie bloquée, fuite de données, rançongiciel, perte d’accès à un prestataire, nom de domaine expiré ou erreur DNS. Dans tous les cas, l’urgence crée souvent le même risque : improviser.

Le plan de reprise sert précisément à éviter cette improvisation. Il ne remplace ni la sécurité, ni les sauvegardes, ni l’assistance d’un prestataire. Il donne un cadre de décision : isoler, préserver, diagnostiquer, prioriser, restaurer, vérifier, communiquer, documenter.

Pour les incidents impliquant des données personnelles, la CNIL rappelle que le responsable de traitement doit documenter les violations. Si la violation présente un risque pour les droits et libertés des personnes, l’article 33 du RGPD impose une notification à l’autorité compétente dans les meilleurs délais et, si possible, dans les 72 heures après en avoir pris connaissance. Si la notification intervient au-delà de 72 heures, le retard doit être motivé.[1]

Le vrai problème n’est pas seulement la panne, c’est l’improvisation

Lorsqu’un site devient indisponible, qu’une messagerie ne reçoit plus les emails ou qu’un outil métier est bloqué, la première réaction est souvent de chercher “qui peut réparer”. C’est normal, mais insuffisant.

Dans une PME, la difficulté vient rarement d’un manque total de solutions. Il existe parfois une sauvegarde, un prestataire, un accès hébergeur, un compte administrateur, une facture avec un support, une console DNS, un plugin de sécurité. Le problème est que ces éléments sont dispersés, détenus par plusieurs personnes, mal documentés ou connus d’un seul interlocuteur.

Le jour de l’incident, cette dispersion coûte du temps. On ne sait pas qui décide. On ne sait pas si l’on peut couper le site. On ne sait pas quelle sauvegarde utiliser. On ne sait pas si le prestataire détient tous les accès. On ne sait pas si les clients doivent être prévenus. On ne sait pas si l’incident touche des données personnelles. On ne sait pas si la restauration risque de supprimer des commandes récentes.

Un plan de reprise n’a pas besoin d’être complexe. Il doit surtout être disponible, à jour, compréhensible et testé.

Plan de reprise, plan de continuité, gestion de crise : clarifier sans compliquer

Il n’est pas nécessaire de transformer une PME en grande direction informatique pour structurer la reprise. Mais trois notions doivent être distinguées.

?Plan de reprise

Il décrit comment remettre en service un système après un incident : site web, messagerie, e-commerce, application métier, base de données, serveur ou domaine.

?Plan de continuité

Il décrit comment l’entreprise continue à fonctionner en mode dégradé : téléphone, email alternatif, page d’information, prise de commande manuelle.

?Gestion de crise

Elle coordonne les décisions, priorités, obligations légales, prestataires, assureur, communication et relation client.

L’ANSSI propose des ressources dédiées à la gestion de crise d’origine cyber.[2] Pour une PME, le minimum viable est souvent un document unique qui combine ces trois dimensions : reprise technique, continuité métier et décisions de crise.

Les incidents à prévoir : pas seulement la cyberattaque

Un bon plan ne doit pas être écrit uniquement pour le scénario spectaculaire du rançongiciel. Les incidents les plus fréquents peuvent être beaucoup plus simples.

Type d’incident	Exemple	Risque principal
Incident de mise à jour	WordPress, WooCommerce ou Elementor casse le site	Site indisponible ou tunnel de commande bloqué
Incident hébergement	Panne serveur, quota disque, erreur PHP, base inaccessible	Indisponibilité totale ou partielle
Incident DNS / domaine	Domaine expiré, DNS modifié, mauvais enregistrement	Site ou emails inaccessibles
Incident messagerie	Emails bloqués, compte compromis, SPF/DKIM/DMARC mal configurés	Perte de demandes clients ou usurpation
Incident de sécurité	Piratage WordPress, backdoor, spam SEO, malware	Réputation, données, référencement
Incident humain	Suppression de contenu, mauvais accès, erreur de manipulation	Perte de données ou mauvaise restauration
Incident prestataire	Relation rompue, accès non transmis, indisponibilité	Blocage opérationnel

Incident données personnelles | Fuite, accès non autorisé, perte de disponibilité | Documentation interne et notification légale si risque

La valeur du plan vient de sa capacité à traiter les cas courants, pas seulement les scénarios extrêmes.

Définir les services prioritaires

Tout ne doit pas repartir en même temps. C'est une erreur fréquente : vouloir restaurer "tout le site" sans hiérarchiser.

Visuel de contenu à créer : image-plan-reprise-incident-pme-priorites.webp

Schéma recommandé : ordre de reprise des services, du nom de domaine jusqu'aux outils tiers.

Priorité | Service | Pourquoi
1 | Nom de domaine et DNS | Sans domaine fonctionnel, site et emails peuvent être affectés.
2 | Messagerie professionnelle | C'est souvent le canal principal avec clients, fournisseurs et prestataires.
3 | Site vitrine ou landing page temporaire | Il faut maintenir une présence et informer.
4 | Formulaires de contact / demandes de devis | Le flux commercial doit reprendre rapidement.
5 | WooCommerce / tunnel de commande | Pour un e-commerce, c'est le cœur de l'activité.
6 | Back-office WordPress | Nécessaire pour piloter, publier, vérifier, corriger.
7 | Outils tiers | CRM, newsletter, facturation, paiement, support client.

Le plan doit indiquer ce qui est critique, ce qui est important, et ce qui peut attendre.

RPO et RTO : reprendre avec des délais réalistes

Comme pour les sauvegardes, deux repères structurent le plan de reprise. Le NIST SP 800-34 est une référence de fond complémentaire sur la planification de continuité et les priorités de reprise, même s'il vise d'abord les systèmes fédéraux américains.[4]

?RPO : perte de données maximale

Le RPO indique la quantité maximale de données que l'entreprise accepte de perdre : aucune commande perdue, maximum une journée de contenu ou maximum une heure de formulaires.

?RTO : délai de reprise maximal

Le RTO indique le délai maximal acceptable avant remise en service : page temporaire en moins d'une heure, messagerie restaurée dans la demi-journée, boutique restaurée sous 24 heures.

Service | RPO acceptable | RTO acceptable

Site vitrine	24 h à 7 jours selon fréquence de mise à jour	4 h à 24 h
Formulaire de contact	24 h ou moins	2 h à 8 h
WooCommerce	Quelques minutes à quelques heures	2 h à 24 h
Messagerie	Idéalement très faible	1 h à 8 h
Application métier	À définir selon impact métier	À définir selon criticité

Ces valeurs sont des exemples à ajuster selon le contexte métier, les contrats, les moyens techniques et les exigences de l'entreprise.

Les rôles : qui décide, qui agit, qui communique ?

Un plan de reprise doit éviter une situation fréquente : tout le monde appelle tout le monde, mais personne ne sait qui arbitre.

Rôle	Responsabilité
Décideur métier	Arbitre les priorités, valide l'arrêt ou la remise en ligne.
Référent technique	Coordonne le diagnostic et la reprise.
Prestataire web / hébergeur	Intervient sur serveur, WordPress, DNS et sauvegardes.
Référent communication	Prépare les messages clients, internes ou publics.
Référent RGPD / direction	Évalue l'impact sur les données personnelles.
Support / accueil	Répond aux clients avec un message cohérent.
Comptabilité / administratif	Gère contrats, assurances, factures et preuves.

Dans une petite structure, une même personne peut tenir plusieurs rôles. L'important est de le savoir avant l'incident.

Les accès critiques à documenter

Un plan de reprise sans accès est inutilisable. La PME doit savoir où se trouvent les accès suivants, même si elle ne les utilise pas tous au quotidien.

Accès	Pourquoi c'est critique
Registre du nom de domaine	Renouvellement, DNS, transfert, propriété.
DNS / zone Cloudflare ou équivalent	Site, emails, SPF/DKIM/DMARC, redirections.
Hébergement / Plesk / cPanel / console serveur	Fichiers, base de données, logs, sauvegardes.

WordPress administrateur | Diagnostic, maintenance, désactivation de plugins.
Base de données | Export, restauration, contrôle d’intégrité.
Stockage des sauvegardes | Choix du point de restauration.
Messagerie admin | Réinitialisation de comptes, alertes, notifications.
Google Search Console | Contrôle indexation, spam SEO, alertes sécurité.
Outils paiement | Stripe, PayPal, banque, rapprochement commandes.
Outils tiers | CRM, newsletter, facturation, analytics, support.
Comptes prestataires | Assistance, tickets, contrats, garanties.

À prévoir hors ligne

Ces accès doivent être protégés, mais pas détenus par une seule personne. Un gestionnaire de mots de passe partagé, avec droits limités et authentification forte, permet d’éviter la dépendance à un seul interlocuteur.

Les premières heures : la procédure minimale

Le plan doit prévoir une procédure simple, utilisable sous stress.

Visuel de contenu à créer : image-plan-reprise-incident-pme-premieres-heures.webp

Schéma recommandé : qualifier, isoler, prévenir, stabiliser, mode dégradé, restaurer, vérifier, documenter.

1. 1Qualifier l’incidentQue constate-t-on ? Site inaccessible, erreur serveur, redirection suspecte, commande impossible, compte compromis, alerte Google, malware, données supprimées ?
2. 2Isoler sans détruire les preuvesCouper certains accès, mettre le site en maintenance, isoler un serveur ou bloquer un compte. Attention : éviter de supprimer trop vite les traces utiles, notamment logs, fichiers suspects, emails et captures.
3. 3Prévenir les bonnes personnesDirection, prestataire, hébergeur, référent RGPD, support client, personne en charge du domaine ou de la messagerie.
4. 4StabiliserL’objectif immédiat n’est pas toujours de réparer, mais d’empêcher l’aggravation : stopper la propagation, figer les sauvegardes, éviter les commandes perdues.
5. 5Décider du mode dégradéPage temporaire, prise de commande manuelle, email alternatif, suspension claire d’un service ou canal de contact de secours.
6. 6Restaurer ou reconstruireLa restauration ne doit intervenir qu’après choix d’un point sain et correction de la cause probable. Restaurer trop vite peut remettre en ligne la faille.
7. 7Vérifier avant réouvertureLe site s’affiche-t-il ? Les formulaires et commandes fonctionnent-ils ? Les emails transactionnels arrivent-ils ? Les accès ont-ils été réinitialisés ?
8. 8DocumenterHeure de début, symptômes, décisions, actions, sauvegardes utilisées, prestataires contactés, personnes informées, mesures correctives.

Le mode dégradé : continuer sans l’outil principal

La reprise ne signifie pas toujours “réparer immédiatement le système complet”. Parfois, le plus utile est de maintenir une activité minimale.

Situation	Mode dégradé possible
Site vitrine indisponible	Page temporaire avec coordonnées et message sobre.
Formulaire cassé	Email direct ou numéro de téléphone visible.
E-commerce indisponible	Prise de commande manuelle ou suspension claire des ventes.
Messagerie principale bloquée	Adresse de secours sur domaine alternatif.
Back-office inaccessible	Gel des publications et passage par prestataire.
Paiement en ligne bloqué	Devis manuel, virement ou autre canal validé.
CRM indisponible	Export local récent ou fichier de suivi temporaire.

Ce mode dégradé doit être prévu à l’avance. En crise, improviser une adresse email ou une page temporaire peut créer de nouvelles erreurs.

Dire assez, sans dire trop

La communication de crise est souvent sous-estimée. Pourtant, elle protège la confiance. Elle doit être sobre, factuelle, cohérente, non accusatoire, actualisée si nécessaire et validée par la direction ou le référent désigné.

Nous rencontrons actuellement un incident technique affectant l’accès à certains services. Nos équipes et prestataires sont mobilisés. Les demandes urgentes peuvent être adressées à [canal de secours]. Une mise à jour sera communiquée dès que la situation sera stabilisée.

Il faut éviter les formulations trop définitives tant que le diagnostic n’est pas terminé : “aucune donnée n’est concernée”, “tout est sécurisé”, “simple panne”, “incident sans impact”. Ces phrases peuvent devenir problématiques si l’analyse montre ensuite autre chose.

La recherche sur la communication après incident cyber souligne qu’un incident peut devenir une crise réputationnelle, d’où l’intérêt de préparer la communication avant l’événement.[5]

Documenter et décider vite

Si l’incident touche des données personnelles, il faut traiter le sujet dès le début, pas après la restauration. La CNIL définit une violation comme une perte de disponibilité, d’intégrité ou de confidentialité de données personnelles, de manière accidentelle ou illicite.[1]

Question	Pourquoi
Quelles données sont concernées ?	Contacts, clients, commandes, comptes, emails, mots de passe.
Combien de personnes peuvent être concernées ?	Estimation initiale, puis complément lorsque les informations sont consolidées.
Les données ont-elles été consultées, copiées, supprimées ou altérées ?	Qualification du risque et choix des mesures correctives.
L’incident présente-t-il un risque pour les personnes ?	Décision de notification à la CNIL.
Le risque est-il élevé ?	Possible information directe des personnes concernées.
Quelles mesures correctives sont prises ?	Réduction du risque et documentation interne.

Rappel juridique à formuler avec précision

En cas de violation présentant un risque pour les droits et libertés des personnes, la notification à la CNIL doit être faite sans délai injustifié et, si possible, dans les 72 heures après en avoir pris connaissance. Une notification tardive doit être accompagnée des motifs du retard.

Clarifier les responsabilités avant l’incident

Dans beaucoup de PME, le site est géré par un prestataire web, l’hébergement par un autre acteur, les emails par Microsoft ou Google, le nom de domaine par un registrar, le DNS par Cloudflare, et la maintenance par une agence. En situation normale, cette organisation fonctionne. En crise, elle peut devenir un labyrinthe.

Question	Risque si ce n’est pas clair
Qui a la main sur le domaine ?	Impossible de modifier les DNS ou de renouveler le domaine.
Qui peut restaurer le site ?	Perte de temps critique.
Qui a accès aux sauvegardes ?	Dépendance prestataire.
Qui peut ouvrir un ticket hébergeur ?	Blocage administratif.
Qui décide de couper le site ?	Hésitation ou action contradictoire.
Qui vérifie WooCommerce après reprise ?	Reprise partielle ou commandes perdues.
Qui communique aux clients ?	Messages incohérents.

Un contrat de maintenance sérieux devrait préciser au minimum : périmètre, délais d’intervention, sauvegardes, restauration, responsabilités, accès, astreinte éventuelle, limites de garantie et procédure d’escalade.

Le plan de reprise PME en dix fiches

Le plan peut tenir en dix pages ou moins. L’important est qu’il soit exploitable.

1Contacts d’urgence

Direction, prestataire web, hébergeur, registrar, messagerie, paiement, assureur, référent RGPD, support client.

2Cartographie des services

Site, domaine, DNS, hébergement, WordPress, WooCommerce, messagerie, CRM, newsletter, facturation, paiement.

3Priorités de reprise

Ce qui doit repartir immédiatement, ce qui peut attendre, ce qui peut fonctionner en mode dégradé.

4Accès critiques

Où sont les accès, qui les détient, comment les récupérer et quelles protections sont en place.

5Sauvegardes

Fréquence, emplacement, rétention, dernier test, durée estimée de restauration, responsable.

6Premières heures

Qualifier, isoler, prévenir, stabiliser, mode dégradé, restaurer, vérifier, documenter.

7Communication

Messages types internes, clients, fournisseurs, page temporaire, support.

8Données personnelles

Grille de qualification, documentation interne, notification CNIL éventuelle, information des personnes si nécessaire.

9Retour à la normale

Tests fonctionnels, surveillance, réinitialisation des mots de passe, fermeture des accès temporaires, rapport d’incident.

10Retour d’expérience

Ce qui a fonctionné, ce qui a manqué, ce qu’il faut corriger dans les sauvegardes, les contrats, les accès ou la sécurité.

Tester le plan : l’exercice vaut mieux que le document

Un plan non testé reste théorique. Il n’est pas nécessaire d’organiser une simulation lourde. Une PME peut commencer par un exercice court, sur table.

Scénario simple

Le site WooCommerce est indisponible depuis 8 h 30. Des clients appellent. Le prestataire habituel ne répond pas. La dernière sauvegarde connue date de la veille. Qui fait quoi ?

Les contacts sont-ils à jour ?

Les accès sont-ils disponibles ?

Les sauvegardes sont-elles identifiées ?

Les priorités sont-elles claires ?

Le message client est-il prêt ?

Le mode dégradé est-il réaliste ?

La décision RGPD peut-elle être prise ?

Le temps de reprise estimé est-il crédible ?

Ce qui bloque souvent une reprise

Erreur	Conséquence
Penser que la sauvegarde suffit	Personne ne sait quoi restaurer, ni dans quel ordre.
Ne pas connaître les accès critiques	Perte de temps ou blocage complet.
Restaurer sans diagnostic	Réinfection ou retour de la faille.
Ne pas prévoir de mode dégradé	L’activité s’arrête totalement.
Ne pas documenter l’incident	Difficulté RGPD, assurance, plainte, retour d’expérience.
Confondre panne technique et incident de sécurité	Mauvaises décisions dans les premières heures.
Dépendre d’un seul prestataire	Blocage si la personne est indisponible.
Communiquer trop vite avec certitude	Risque de contradiction si le diagnostic évolue.
Oublier les emails et le DNS	Site restauré mais demandes clients toujours perdues.
Ne jamais tester le plan	Découverte des failles au moment critique.

Les questions à poser avant l’incident

Visuel de contenu à créer : image-plan-reprise-incident-pme-checklist.webp

Checklist visuelle avec trois colonnes : décisions, accès, délais.

Question	Si la réponse est floue
Qui décide en cas d’incident ?	Les actions risquent d’être contradictoires.
Qui a accès au domaine et au DNS ?	Site et emails peuvent rester bloqués.
Où sont les sauvegardes ?	La restauration peut être impossible.
Quand la dernière restauration a-t-elle été testée ?	Le délai réel de reprise est inconnu.
Quels services doivent repartir en premier ?	Les équipes peuvent perdre du temps sur le secondaire.
Quel mode dégradé est prévu ?	L’activité peut s’arrêter totalement.
Qui contacte le prestataire et l’hébergeur ?	Les demandes peuvent se disperser.
Qui rédige le message client ?	Communication incohérente ou trop risquée.
Que faire si des données personnelles sont concernées ?	Risque de non-documentation ou de notification tardive.
Le plan est-il accessible hors ligne ?	Il peut être inutilisable si les emails ou le cloud sont indisponibles.

Ce que les lecteurs demandent souvent

Un plan de reprise est-il nécessaire pour un simple site vitrine ?

Oui, mais il peut être très simple. Le minimum est de savoir où sont le domaine, l’hébergement, les sauvegardes, les accès WordPress, le prestataire à contacter et le message temporaire à publier.

Quelle différence avec une sauvegarde ?

La sauvegarde est une ressource. Le plan de reprise est la méthode pour l’utiliser correctement. Sans plan, une sauvegarde peut rester inaccessible, mal choisie ou restaurée trop tard.

Faut-il un document juridique ?

Pas forcément. Il faut surtout un document opérationnel. Les aspects contractuels viennent ensuite : responsabilités prestataires, délais, sauvegardes, assurance, protection des données.

Le plan doit-il être imprimé ?

Oui, au moins en version synthétique. Si l’incident touche les emails, le cloud ou le poste principal, un plan uniquement stocké en ligne peut devenir inaccessible.

Qui doit tenir le plan à jour ?

Une personne doit être responsable de sa mise à jour, mais plusieurs doivent le connaître. Le plan doit être revu après chaque changement important : nouvel hébergeur, nouveau prestataire, nouvelle messagerie, nouveau module WooCommerce, nouvelle solution de sauvegarde.

Faut-il prévenir les clients dès le début ?

Pas toujours. Cela dépend de l'impact. En revanche, si le service est visiblement indisponible ou si les clients sont directement touchés, un message sobre et factuel vaut mieux que le silence.

Faut-il déposer plainte en cas de cyberattaque ?

En cas de cyberattaque avérée, le dépôt de plainte est fortement recommandé. Il peut être utile pour les démarches d'assurance, la documentation de l'incident et les obligations éventuelles auprès de la CNIL. Certains contrats d'assurance peuvent aussi le demander selon les garanties souscrites. Avant toute restauration ou nettoyage, il faut préserver les preuves disponibles : logs, fichiers suspects, emails, captures, dates, comptes concernés et sauvegardes utilisées.

Que faire avec 17Cyber ?

17Cyber, lancé en décembre 2024, est le guichet national d'assistance en ligne pour les victimes de cybermalveillance. Il s'appuie sur Cybermalveillance.gouv.fr et fonctionne en lien avec les forces de l'ordre pour orienter les victimes, poser un premier diagnostic et faciliter les démarches utiles.[3]

Un bon plan de reprise est court, connu et utilisable

Une PME n'a pas besoin d'un classeur de crise de 200 pages. Elle a besoin d'un plan clair, à jour et accessible : contacts, accès, priorités, sauvegardes, mode dégradé, procédure des premières heures, communication, données personnelles et retour à la normale.

Le plan de reprise ne supprime pas le risque. Il réduit le désordre. Il permet de gagner du temps, d'éviter les décisions dangereuses, de protéger les données, de rassurer les clients et de mieux piloter les prestataires.

La vraie question n'est donc pas seulement : avons-nous une sauvegarde ?La vraie question est : sommes-nous capables de décider et d'agir dans le bon ordre le jour où quelque chose se passe ?

Sources

- CNIL, Notifier une violation de données personnelles. Référence sur la définition d'une violation, la documentation interne et la notification à la CNIL lorsque le risque le justifie. cnil.fr
- ANSSI, Gestion de crise cyber et ressources rançongiciels. Source française de référence sur les réflexes de crise, la préservation des preuves et l'organisation de la réponse. cyber.gouv.fr
- 17Cyber / Cybermalveillance.gouv.fr. Guichet national d'assistance aux victimes de cybermalveillance, en lien avec les dispositifs d'orientation et les forces de l'ordre. 17cyber.gouv.fr · cybermalveillance.gouv.fr

• NIST, SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems. Référence de fond complémentaire sur la planification de continuité, les exigences et priorités de reprise. csrc.nist.gov

• Knight & Nurse, A framework for effective corporate communication after cyber security incidents. Recherche complémentaire sur la communication après incident cyber et le risque réputationnel. arxiv.org