

Sauvegardes web Pourquoi une sauvegarde n'est utile que si elle est restaurable

Une sauvegarde ne protège réellement une entreprise que si elle est complète, récente, isolée et restaurable. Beaucoup de sites disposent de sauvegardes automatiques, mais personne ne sait dire quand elles ont été testées, ce qu'elles contiennent ni combien de temps prendrait une restauration.

Publié le 2 juin 2026

Ce document reproduit le contenu publié à l'adresse indiquée en pied de page, dans sa version disponible à la date de sa génération. Il est fourni à titre exclusivement informatif et ne constitue ni un conseil juridique, réglementaire, fiscal ou professionnel, ni une garantie d'exhaustivité, d'exactitude ou d'actualité. Les textes officiels et la situation propre du lecteur doivent être vérifiés avant toute décision. Dans les limites permises par la loi applicable, Nasteo n'assume aucune responsabilité au titre des décisions prises ou des conséquences résultant de l'utilisation de ce document.

Ce qu'il faut retenir de ce dossier

Une sauvegarde web n'est pas une simple copie de fichiers. Pour un site professionnel, elle doit permettre de remettre en service un site complet, avec ses contenus, sa base de données, ses médias, ses comptes utilisateurs, ses commandes, ses formulaires, ses réglages et ses configurations techniques.

Le point clé est simple : une sauvegarde non testée n'est qu'une hypothèse de sécurité. Elle peut être incomplète, corrompue, trop ancienne, stockée au mauvais endroit, inaccessible au moment critique ou inutilisable avec la version actuelle du site.

Pour un site WordPress, la documentation officielle rappelle que les fichiers et la base de données sont deux ensembles distincts : télécharger le répertoire WordPress ne sauvegarde généralement pas la base MySQL/MariaDB, alors que celle-ci contient les contenus et de nombreuses données générées par le site.

Deux notions permettent de cadrer la décision : le RPO, c'est-à-dire la quantité maximale de données que l'entreprise accepte de perdre, et le RTO, c'est-à-dire le délai maximal acceptable avant remise en service. Le bon objectif n'est donc pas "avoir une sauvegarde", mais pouvoir répondre clairement à quatre questions : que sauvegarde-t-on, où est-ce stocké, quand a-t-on testé la restauration, et combien de temps faut-il pour redémarrer ?

Une sauvegarde existe peut-être, mais est-elle réellement exploitable ?

Beaucoup d'entreprises pensent être protégées parce que leur hébergeur, leur plugin WordPress ou leur prestataire indique que des sauvegardes sont réalisées automatiquement. C'est rassurant, mais insuffisant.

Une sauvegarde automatique peut très bien exister sans être utile le jour où l'entreprise en a besoin. Elle peut ne couvrir que les fichiers et pas la base de données. Elle peut être stockée sur le même serveur que le site. Elle peut être écrasée trop rapidement. Elle peut dater d'après l'incident et contenir déjà le problème. Elle peut aussi être techniquement restaurable, mais trop lente à remettre en ligne pour l'activité de l'entreprise.

La question utile n'est pas "avons-nous une sauvegarde ?"

La vraie question est : pouvons-nous restaurer notre site correctement, dans un délai connu, avec une perte de données acceptable ?

Trois questions pour commencer

- Qui peut lancer une restauration si le site tombe aujourd'hui ?
- Quelle est la date du dernier test de restauration réussi ?
- Que perdrait l'entreprise si elle devait restaurer la sauvegarde de cette nuit ?

Pourquoi une sauvegarde peut échouer le jour où elle devient indispensable

Une sauvegarde échoue rarement parce qu'elle n'existe pas du tout. Elle échoue souvent parce qu'elle n'a jamais été vérifiée dans des conditions réalistes.

?Sauvegarde incomplète

Un site dynamique ne se limite pas à des fichiers. La base de données, les médias, les réglages et les tables de plugins doivent aussi être couverts.

?Sauvegarde trop ancienne

Une sauvegarde hebdomadaire peut suffire pour un site vitrine, mais pas pour un e-commerce qui reçoit des commandes chaque jour.

?Stockage au mauvais endroit

Une copie conservée uniquement sur le serveur de production peut disparaître avec le site en cas de panne ou de compromission.

?Sauvegarde déjà contaminée

Après une attaque, les sauvegardes récentes peuvent déjà contenir la porte dérobée ou les fichiers malveillants.

?Sauvegarde inaccessible

Un compte prestataire fermé, une double authentification attachée à une personne absente ou un accès perdu peuvent bloquer la reprise.

?Restauration trop lente

Une restauration peut fonctionner techniquement tout en prenant trop de temps pour l'activité de l'entreprise.

Ce qu'il faut sauvegarder sur un site WordPress

Un site WordPress doit être sauvegardé comme un système complet. La documentation WordPress distingue clairement les fichiers du site, cœur WordPress, thèmes, extensions, médias, fichiers de configuration, et la base de données, généralement MySQL ou MariaDB, qui vit séparément du répertoire WordPress.

Élément Pourquoi c'est important
Fichiers WordPress Cœur du CMS, thèmes, extensions et fichiers techniques.
Base de données Pages, articles, menus, réglages, utilisateurs, formulaires, commandes et contenus dynamiques.

Dossier wp-content/uploads Images, PDF, documents et médias publiés.
Thème actif et thème enfant Personnalisations graphiques ou fonctionnelles parfois critiques.
Extensions Formulaires, SEO, cache, sécurité, e-commerce, paiement, langues, import/export.
wp-config.php Paramètres essentiels de connexion et de configuration.
Règles serveur .htaccess, configuration Nginx, redirections, règles de sécurité ou cache.
Données spécifiques de plugins Certaines extensions utilisent des tables dédiées : formulaires, abonnements, langues, champs personnalisés, imports ou données e-commerce.

Point souvent oublié

Certains plugins stockent leurs données dans des tables spécifiques. Une sauvegarde qui n'inclut pas toutes les tables de la base peut produire une restauration partielle sans erreur visible au premier chargement.

Le cas particulier de WooCommerce et des sites qui enregistrent des données chaque jour

Un site WooCommerce n'a pas les mêmes exigences qu'un site vitrine. Chaque commande crée de nouvelles données : client, adresse, produit, paiement, statut, stock, email transactionnel, facture éventuelle, note de commande.

Si la sauvegarde est trop espacée, une restauration peut provoquer des incohérences : commandes perdues, stocks incorrects, paiements enregistrés chez le prestataire mais absents du site, clients sans accès à leur compte, emails de confirmation manquants, factures ou exports comptables incomplets.

Un e-commerce se raisonne en perte de données acceptable

Une sauvegarde quotidienne peut être insuffisante si l'activité est soutenue. Certains contextes nécessitent des sauvegardes plus fréquentes de la base, des exports de commandes ou des mécanismes complémentaires de journalisation.

RPO et RTO : les deux questions qui changent tout

Deux notions permettent de sortir du flou. Elles sont utilisées dans les démarches de continuité et de reprise d'activité pour déterminer les exigences et priorités de restauration.

Visuel de contenu à créer : image-sauvegardes-web-restaurable-rpo-rto.webp

Schéma recommandé : deux curseurs simples, "données perdues acceptables" pour le RPO et "délai de remise en service" pour le RTO.

?RPO : combien de données peut-on perdre ?

Le RPO correspond à la perte maximale de données acceptable. Si vous restaurez la sauvegarde de cette nuit, que perdez-vous depuis cette sauvegarde ?

?RTO : combien de temps peut-on rester hors ligne ?

Le RTO correspond au délai maximal acceptable pour remettre le service en ligne. Combien de temps votre activité peut-elle fonctionner sans ce site ?

Type de site RPO indicatif RTO indicatif
Site vitrine peu modifié Perte acceptable souvent faible mais non critique Quelques heures peuvent être acceptables selon l'activité
Site éditorial actif Articles, médias et modifications récentes à préserver Retour rapide utile pour éviter la perte d'audience
WooCommerce Commandes, paiements, comptes clients et stocks à protéger Retour rapide fortement recommandé
Application métier Perte de données souvent très limitée voire quasi nulle Délai de reprise à cadrer formellement

Où stocker les sauvegardes ?

Le stockage est aussi important que la sauvegarde elle-même. Une bonne stratégie évite que le site et ses sauvegardes disparaissent en même temps.

?Même serveur

Pratique pour une restauration rapide après petite erreur, mais insuffisant si le serveur est compromis ou indisponible.

?Stockage distant

Réduit le risque de perte simultanée du site et des sauvegardes. L'accès doit être sécurisé et séparé de la production.

?Espace isolé

Limite les dégâts si un attaquant obtient un accès WordPress ou serveur. Il ne doit pas pouvoir supprimer toutes les copies.

La rétention doit aussi être cadrée. Conserver uniquement la dernière sauvegarde est risqué : si l'incident date de plusieurs jours, la dernière copie peut déjà contenir le problème. Il faut souvent conserver plusieurs points de restauration, par exemple quotidiens, hebdomadaires et mensuels selon le niveau de criticité.

La règle 3-2-1, et son évolution 3-2-1-1-0

La règle 3-2-1 est un repère courant en sauvegarde : trois copies des données, deux supports ou emplacements différents, une copie hors site. Pour un site web, cela peut correspondre à la production, une sauvegarde locale rapide et une sauvegarde distante.

Visuel de contenu à créer : image-sauvegardes-web-restaurable-32110.webp

Infographie recommandée : 3 copies, 2 emplacements, 1 hors site, 1 copie isolée ou immuable, 0 erreur au test de restauration.

Principe Application web
3 copies Production + sauvegarde rapide + sauvegarde distante.
2 supports ou emplacements Serveur de production + stockage externe indépendant.
1 copie hors site Copie située hors de l'infrastructure principale.
1 copie isolée ou immuable Copie hors ligne, air-gapped ou non modifiable directement par un attaquant.
0 erreur Restauration testée ou intégrité vérifiée, sans erreur bloquante.

Pourquoi cette évolution compte

Dans un contexte de rançongiciel, les sauvegardes sont une cible. Ajouter une copie isolée ou immuable et vérifier qu'il n'y a pas d'erreur lors des tests rend la stratégie beaucoup plus robuste qu'une simple copie automatique.

Tester la restauration : le point que beaucoup oublient

Le test de restauration est la preuve que le dispositif fonctionne. Il ne s'agit pas forcément de restaurer le site en production : on peut restaurer sur un environnement de test, un sous-domaine, une préproduction ou un espace isolé.

- 1Restaurer fichiers et base ensembleLes deux éléments doivent correspondre à un même point de restauration pour éviter les incohérences.
- 2Vérifier l'affichage et les médiasPages principales, menus, images, documents, thème et modèles doivent être contrôlés.
- 3Tester les fonctions critiquesFormulaires, comptes utilisateurs, panier WooCommerce, paiement, emails transactionnels et exports si besoin.
- 4Mesurer le temps réelLe test doit donner un délai de reprise connu, pas seulement confirmer qu'une copie existe.
- 5Documenter le résultatDate, personne responsable, durée, problème rencontré, correctif appliqué et prochain test prévu.

Sauvegarde et rançongiciel : attention aux fausses sécurités

Les sauvegardes sont un élément essentiel de résilience face aux cyberattaques, mais elles sont elles-mêmes une cible. Dans certaines attaques, l'objectif de l'attaquant est de supprimer, chiffrer ou rendre inutilisables les sauvegardes avant de chiffrer le site ou les données.

Après une cyberattaque, il faut éviter deux réflexes dangereux : restaurer immédiatement la dernière sauvegarde sans comprendre l'origine de l'incident, ou supprimer trop vite les traces nécessaires au diagnostic.

Processus recommandé :

isoler le site, préserver les traces, diagnostiquer l'origine, choisir un point de restauration sain, corriger la faille, restaurer, vérifier puis surveiller. Une restauration trop rapide peut remettre en ligne la même porte d'entrée.

Sauvegarde, RGPD et registre des traitements

Un site professionnel peut contenir des données personnelles : formulaires de contact, comptes utilisateurs, commandes, adresses, emails, historiques de messages, demandes de devis. Les sauvegardes qui contiennent ces données doivent donc être protégées avec les mêmes exigences de sécurité que les données de production.

La CNIL rappelle que le registre des activités de traitement, prévu par l'article 30 du RGPD, permet de recenser les traitements de données personnelles et de documenter notamment les catégories de données, les destinataires, les durées de conservation et les mesures de sécurité. Si les sauvegardes contiennent des données personnelles, elles doivent être cohérentes avec cette documentation.

Point RGPD Application aux sauvegardes
Accès limité Seules les personnes ou prestataires autorisés doivent pouvoir consulter ou restaurer les sauvegardes.
Durée de conservation La rétention doit être justifiée et cohérente avec les finalités du traitement.
Sécurité Chiffrement, séparation des accès, authentification forte et journalisation si nécessaire.
Sous-traitance Les prestataires qui hébergent ou manipulent les sauvegardes doivent être identifiés et encadrés.
Registre Les traitements non occasionnels ou sensibles doivent être documentés ; en cas de doute, la CNIL recommande de les intégrer au registre.

Les erreurs les plus fréquentes

- ?Sauvegarde uniquement sur le serveur de productionLe site et les sauvegardes peuvent disparaître ensemble en cas d'incident serveur.
- ?Sauvegarde uniquement des fichiersLe site peut être inutilisable si la base de données est absente.
- ?Sauvegarde uniquement de la baseLes médias, thèmes, extensions et fichiers de configuration peuvent manquer.

- ?Une seule sauvegarde conservéeImpossible de revenir avant un incident ancien.
- ?Aucun test de restaurationLes problèmes sont découverts au pire moment.
- ?Accès détenu par un seul prestataireBlocage possible si la relation se termine ou si le prestataire est indisponible.
- ?Restauration sans diagnostic après piratageRisque de réinfection ou de remise en ligne d'une faille encore présente.

Les questions à poser dès maintenant

Visuel de contenu à créer : image-sauvegardes-web-restaurable-checklist.webp

Checklist visuelle recommandée : questions dirigeant + conséquences si la réponse est floue.

Question Si la réponse est floue ou négative
Que sauvegardons-nous exactement ? Le site peut être restauré partiellement seulement.
La base de données est-elle sauvegardée ? Les contenus dynamiques, commandes et réglages peuvent être perdus.
Les fichiers et médias sont-ils sauvegardés ? Images, documents, thèmes et extensions peuvent manquer.
Où sont stockées les sauvegardes ? Elles peuvent disparaître avec le serveur.
Combien de versions sont conservées ? Impossible de revenir avant une attaque ancienne.
Quand la dernière restauration a-t-elle été testée ? La sauvegarde reste théorique.
Combien de temps faut-il pour restaurer ? Le délai réel d'interruption est inconnu.
Quelle quantité de données peut-on perdre ? Le rythme de sauvegarde peut être inadapté.
Qui a accès aux sauvegardes ? Risque de dépendance ou d'accès non maîtrisé.
Les sauvegardes contiennent-elles des données personnelles ? Il faut encadrer sécurité, conservation et confidentialité.

Méthode simple pour auditer ses sauvegardes

- 1Inventorier les données critiquesSite, base, médias, commandes, formulaires, comptes, documents, emails transactionnels, configurations serveur.
- 2Identifier les sauvegardes existantesHébergeur, plugin, prestataire, outil externe, export manuel ou stockage distant.
- 3Vérifier les emplacementsServeur, espace hébergeur, cloud, coffre distant, espace prestataire.
- 4Contrôler la rétentionNombre de versions conservées, durée de conservation, capacité à revenir avant un incident ancien.
- 5Tester une restaurationRestaurer sur un environnement de test et vérifier le fonctionnement réel.

- 6 Documenter le résultat Date, sauvegarde utilisée, durée, problèmes, corrections, personne responsable.
- 7 Planifier le prochain test Le site évolue : nouvelles extensions, nouveau PHP, nouvelles pages, nouvelle boutique, nouveaux formulaires.

Adapter la stratégie au type de site

?Site vitrine

Une sauvegarde quotidienne ou hebdomadaire peut suffire selon la fréquence de mise à jour. Le point important est de conserver plusieurs versions et de tester la restauration.

?Site éditorial

Les contenus et médias publiés régulièrement doivent être protégés. La base de données doit être sauvegardée plus souvent si l'activité éditoriale est soutenue.

?WooCommerce

Commandes, clients, paiements et stocks évoluent en continu. Le rythme de sauvegarde doit être beaucoup plus fin qu'un simple export hebdomadaire.

?Site Elementor

Les modèles, réglages globaux, CSS générés et médias sont souvent essentiels. Une restauration partielle peut casser la mise en page.

?Application métier

Les objectifs de reprise doivent être plus stricts : RPO, RTO, personnes responsables et procédures documentées.

?Site géré par un prestataire

Il faut savoir qui détient les accès aux sauvegardes, ce qui se passe si la relation se termine, et comment l'entreprise récupère ses fichiers, sa base et ses copies de restauration.

Sauvegarde, restauration, archivage : trois notions à ne pas confondre

La sauvegarde consiste à copier des données ou un système pour pouvoir les récupérer en cas de problème. La restauration est l'opération inverse : elle remet en place ce qui a été sauvegardé et prouve que la copie est exploitable. L'archivage vise plutôt la conservation longue durée d'une information dans un état donné : documents légaux, factures, preuves, contrats. Il ne remplace pas une sauvegarde opérationnelle.

Ce que les lecteurs demandent souvent

Une sauvegarde hébergeur suffit-elle ?

Et sur un hébergement mutualisé ?

Faut-il aussi utiliser un plugin de sauvegarde WordPress ?

Quelle fréquence de sauvegarde choisir ?

Faut-il sauvegarder avant chaque mise à jour ?

Une sauvegarde protège-t-elle contre le piratage ?

Qui doit avoir accès aux sauvegardes ?

Conclusion

La vraie question n'est pas "avons-nous une sauvegarde ?". La vraie question est : pouvons-nous restaurer notre site correctement, dans un délai connu, avec une perte de données acceptable ?

Une sauvegarde utile est complète, récente, isolée, protégée et testée. Elle couvre les fichiers, la base de données, les médias, les configurations et les données métier importantes. Elle est stockée dans un emplacement distinct, avec plusieurs versions, et sa restauration a déjà été vérifiée.

Pour une PME, ce sujet n'est pas seulement technique. Il touche la continuité commerciale, la confiance client, la conformité, la relation avec les prestataires et la capacité à réagir en cas d'incident.

Sources

- ANSSI, Attaques par rançongiciels, tous concernés : recommandations de prévention, de réaction et d'organisation face aux attaques par rançongiciel.
- Cybermalveillance.gouv.fr : ressources de prévention et d'assistance liées aux risques de perte de données et aux cybermalveillances.
- WordPress.org, Backups : distinction entre fichiers WordPress et base de données, contenu à sauvegarder, recommandations de sauvegarde et de restauration.
- CNIL, Le registre des activités de traitement : article 30 du RGPD, documentation des traitements, durées de conservation et mesures de sécurité.

- Veeam, 3-2-1-1-0 Golden Backup Rule : formulation sectorielle de la règle 3-2-1-1-0, incluant copie isolée ou immuable et zéro erreur lors des tests.
- NIST, SP 800-34 Rev. 1 : référence de fond complémentaire sur la planification de continuité, les priorités de reprise et les exigences de restauration des systèmes d'information.