



CHECKLIST

# Sauvegardes 3-2-1 : votre assurance anti-ransomware

La checklist pour bâtir une stratégie de sauvegarde qui survit à un rançongiciel : copies multiples, hors ligne, immuables, chiffrées et surtout testées.

---

Sedona Radar — audit de sécurité externe automatisé

Sedona AI   Lecture ~11 min   Édition 2026   [sedona-ai.com](https://sedona-ai.com)

**F**ace à un rançongiciel, une sauvegarde saine et restaurable est ce qui sépare une reprise en quelques jours d'un arrêt d'activité prolongé. La règle 3-2-1, recommandée par l'ANSSI, en pose le socle : trois copies de vos données, sur deux supports, dont une hors ligne. Mais elle ne suffit plus si vos sauvegardes sont chiffrées par l'attaquant ou, pire, illisibles le jour J. Cette checklist va au bout de la logique : hors ligne, immuable, chiffré, testé.

### À retenir

- Appliquez la règle 3-2-1 (recommandation R11 de l'ANSSI) : 3 copies distinctes, sur 2 supports différents, dont 1 copie hors ligne totalement déconnectée.
- Une copie hors ligne est jugée « indispensable » par l'ANSSI (R12) : c'est la seule qu'un attaquant présent dans votre réseau ne peut ni chiffrer ni effacer.
- Complétez par l'immuabilité (WORM) pour le stockage en ligne, mais gardez en tête qu'une copie hors ligne déconnectée reste plus robuste.
- Une sauvegarde jamais testée n'est pas une sauvegarde : l'ANSSI (R22) recommande une procédure de restauration écrite et régulièrement rejouée.
- Les PME/TPE/ETI sont désormais la cible n°1 des rançongiciels : 48 % des victimes signalées à l'ANSSI en 2025, contre 37 % en 2024.
- Protégez l'infrastructure de sauvegarde elle-même : chiffrement des flux, isolement d'urgence (« bouton rouge »), et reconstruction saine après incident.

## 01 Pourquoi la sauvegarde est votre dernière ligne de défense

Un rançongiciel chiffre vos données pour vous rendre votre propre système inutilisable, puis exige une rançon. Aucune protection périmétrique n'est infaillible : le jour où un attaquant passe, seule une sauvegarde saine et restaurable vous permet de repartir sans payer. Encore faut-il qu'elle soit hors de portée de l'attaquant et réellement exploitable — deux conditions que la plupart des organisations découvrent trop tard.

# 48 %

des victimes de rançongiciel signalées à l'ANSSI en 2025 sont des PME/TPE/ETI (contre 37 % en 2024)  
ANSSI, Panorama de la cybermenace 2025 (CERT-FR)

### La menace se déplace, elle ne recule pas

L'ANSSI a recensé 128 compromissions par rançongiciel en 2025, en légère baisse. Mais les incidents d'exfiltration de données (avec ou sans chiffrement) bondissent de plus de 50 % : 196 en 2025 contre 130 en 2024. Les attaquants font désormais aussi de l'extorsion sans chiffrer. Une bonne sauvegarde reste indispensable, mais ne protège pas d'une fuite de données : les deux volets sont à traiter.

## 02 La règle 3-2-1 expliquée

La règle 3-2-1 est le fondement recommandé par l'ANSSI (recommandation R11 du guide ANSSI-BP-100). Elle tient en trois chiffres, faciles à mémoriser et à auditer.

| Chiffre      | Ce qu'il signifie                                           | Exemple concret                                               |
|--------------|-------------------------------------------------------------|---------------------------------------------------------------|
| 3 copies     | Vos données de production + 2 sauvegardes distinctes        | Le serveur de fichiers, une sauvegarde sur NAS, une sur bande |
| 2 supports   | Les sauvegardes reposent sur 2 types de supports différents | Disque (NAS/SAN) et bande magnétique, ou disque et cloud      |
| 1 hors ligne | Au moins une copie totalement déconnectée de tout système   | Bande stockée dans un coffre, disque débranché après copie    |

### Pourquoi le « hors ligne » change tout

L'ANSSI signale qu'un attaquant tente fréquemment de chiffrer, d'effacer ou de rendre indisponible l'infrastructure de sauvegarde pour maximiser ses chances d'obtenir la rançon. Une copie hors ligne — déconnectée de tout SI — est la seule qu'il ne peut pas atteindre depuis votre réseau. Selon l'ANSSI, la bande magnétique reste le moyen le plus efficace pour cet usage.

## 03 Au-delà du 3-2-1 : hors ligne, immuable, testé

Dans la profession, on complète souvent la règle par une déclinaison « 3-2-1-1-0 » : le second « 1 » désigne une copie hors ligne ou immuable, et le « 0 » signifie zéro erreur de restauration prouvée par des tests. Ce libellé exact n'apparaît pas tel quel dans le guide ANSSI 2025, mais il est cohérent avec ses principes, que l'Agence formule via des recommandations distinctes.

- Copie hors ligne (R12) : jugée « indispensable » par l'ANSSI, même si sa fréquence est plus faible que les sauvegardes locales régulières.
- Immuabilité / WORM (§3.5) : pour le stockage en ligne externalisé, envisager une solution WORM (Write Once Read Many) qui empêche toute modification. L'ANSSI note toutefois qu'une copie hors ligne déconnectée reste plus robuste qu'un WORM en ligne.
- Tests de restauration (R22) : une procédure de restauration écrite et régulièrement rejouée — c'est le « 0 » de la formule.
- Localisation (externalisation) : garder les sauvegardes sur le territoire de l'Union européenne et les chiffrer avec un moyen propre à l'entité avant tout envoi chez un hébergeur.

## 04 La checklist de mise en place

Passez chaque point en revue. Un seul « non » est un angle mort exploitable par un rançongiciel.

☐ Vous disposez d'au moins 3 copies : la production + 2 sauvegardes distinctes.

- ☐ Ces sauvegardes reposent sur 2 supports de nature différente (ex. disque + bande).
- ☐ Au moins une copie est hors ligne, totalement déconnectée du réseau.
- ☐ Pour le stockage en ligne, une solution immuable (WORM) est en place.
- ☐ Les sauvegardes externalisées restent hébergées dans l'Union européenne.
- ☐ La fréquence des sauvegardes correspond à votre perte de données tolérable (RPO).
- ☐ Les comptes qui gèrent les sauvegardes sont distincts des comptes d'administration courants.
- ☐ Les utilisateurs finaux ne peuvent pas déclencher eux-mêmes des restaurations sur le SI (R18).
- ☐ Un contrôle régulier détecte tout comportement inhabituel : volumes incohérents, lenteurs, changement de politique (R21).

## 05 Chiffrer et protéger l'infrastructure de sauvegarde

Vos sauvegardes concentrent vos données les plus sensibles : elles doivent être au moins aussi bien protégées que la production. L'ANSSI cadre précisément ce volet.

- Chiffrer les flux de sauvegarde en transit : chiffrement et authentification mutuelle client-serveur à l'état de l'art, avec TLS par exemple (R28).
- Aligner la robustesse du chiffrement des sauvegardes sur celle des données en production (R29).
- Chiffrer systématiquement les supports si la sécurité physique du site de sauvegarde est insuffisante (R31).
- Sauvegarder l'infrastructure de sauvegarde elle-même : binaires, procédures d'import, catalogue et clés de chiffrement, pour pouvoir reconstruire sur un site de secours (R26).

### Deux guides ANSSI à ne pas confondre

Le guide technique ANSSI-BP-100 « Sauvegarde des systèmes d'information : les fondamentaux » (v1.1, 27/11/2025) détaille les recommandations R11 à R31. Le guide « Attaques par rançongiciels, tous concernés » est plus généraliste et orienté dirigeants. Les deux sont utiles et complémentaires.

## 06 Tester les restaurations : le point que tout le monde néglige

Une sauvegarde qui n'a jamais été restaurée est une hypothèse, pas une garantie. Le jour d'une attaque n'est pas le moment de découvrir qu'une bande est illisible ou qu'il manque une clé de chiffrement. Formalisez et rejouez régulièrement le scénario complet.

## 1 Rédiger la procédure

Documentez pas à pas la restauration du SI (ordre des systèmes, dépendances, comptes, clés). C'est la recommandation R22 de l'ANSSI.

## 2 Planifier des tests réguliers

Programmez des restaurations de test sur un environnement isolé, à intervalle défini, pas seulement une fois à l'installation.

## 3 Mesurer le temps de reprise réel

Chronométrez la restauration pour valider que votre RTO (durée d'indisponibilité tolérable) est réaliste, et corriger si besoin.

## 4 Consigner et corriger

Notez chaque échec ou lenteur et traitez-le. L'objectif est zéro erreur de restauration le jour J.

# 07 Réagir sans recontaminer : le « bouton rouge »

En cas d'incident, deux réflexes conditionnent la survie de vos sauvegardes et la propreté de la reconstruction.

1. Isoler immédiatement l'infrastructure de sauvegarde du reste du SI (R24), via un mode « bouton rouge » préparé à l'avance : script automatisé ou déconnexion physique d'un commutateur.
2. Reconstruire proprement (R27) : partez du principe que les sauvegardes peuvent déjà contenir un implant de l'attaquant. Reconstituez de façon granulaire — images officielles, binaires signés, analyse antivirus avant toute réimportation.

### Le coût de l'inaction

Selon le rapport IBM Cost of a Data Breach 2025, un incident d'extorsion ou de rançongiciel coûte en moyenne 5,08 M\$ à l'échelle mondiale lorsqu'il est révélé par l'attaquant. Une stratégie de sauvegarde résiliente reste l'un des investissements de sécurité au meilleur rapport coût/protection.

# 08 Où Sedona Radar intervient

Une bonne sauvegarde protège vos données ; encore faut-il ne pas laisser grande ouverte la porte par laquelle le rançongiciel entre. Sedona Radar analyse ce que votre domaine expose sur Internet, classe les vulnérabilités exposées par gravité et donne des indicateurs de maturité au regard de référentiels comme NIS2 et l'ANSSI Hygiène.

### Radar évalue, il ne certifie pas

Radar mesure votre exposition pour vous aider à combler les failles avant qu'elles ne soient exploitées. Ses indicateurs de maturité ne sont pas une certification : il n'existe aucune certification NIS2. Vos données sont stockées dans l'Union européenne.

1. ANSSI-BP-100 — Sauvegarde des systèmes d'information : les fondamentaux (v1.1, 27/11/2025) — [https://messervices.cyber.gouv.fr/documents-guides/anssi\\_fondamentaux\\_sauvegarde\\_systemes\\_dinformation\\_v1.1.pdf](https://messervices.cyber.gouv.fr/documents-guides/anssi_fondamentaux_sauvegarde_systemes_dinformation_v1.1.pdf)
2. ANSSI — Panorama de la cybermenace 2025 (PDF officiel CERT-FR) — <https://www.cert.ssi.gouv.fr/uploads/CERT-FR-2026-CTI-002.pdf>
3. cyber.gouv.fr — Actualité : Panorama de la cybermenace 2025 — <https://cyber.gouv.fr/actualites/panorama-de-la-cybermenace-2025/>
4. ANSSI — Attaques par rançongiciels, tous concernés : comment les anticiper et réagir — [https://messervices.cyber.gouv.fr/documents-guides/anssi-guide-attaques\\_par\\_rancongiels\\_tous\\_concernes-v1.0.pdf](https://messervices.cyber.gouv.fr/documents-guides/anssi-guide-attaques_par_rancongiels_tous_concernes-v1.0.pdf)
5. IBM — Cost of a Data Breach Report 2025 : The AI Oversight Gap — <https://www.ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai>
6. IBM — Rapport complet PDF Cost of a Data Breach 2025 — <https://www-api.ibm.com/adobe/assets/urn:aaid:aem:607b9590-38e0-4c91-b433-aa8a17f5b5e8/original/as/cost-of-a-data-breach-2025-full-report.pdf>

### Fermez la porte avant de compter sur la sauvegarde

Les sauvegardes sont votre filet de sécurité, mais mieux vaut ne pas avoir à l'utiliser. Lancez un scan gratuit avec Sedona Radar pour voir ce que votre domaine expose avant qu'un rançongiciel ne le trouve.

**Lancer mon scan gratuit**

[sedona-ai.com/scan-gratuit](https://sedona-ai.com/scan-gratuit)