

Comment gérer votre système d'information

Reprendre le contrôle de votre informatique
sans devenir informaticien

MANAGE · PROTECT · TRANSFORM · DECIDE

Édition 2026

Oakteam.
L'informatique est un sujet de décision

Avertissement au lecteur

Ce livret ne contient pas de secret. Il contient méthode, ordre de priorité et bon sens — c'est-à-dire exactement ce qui manque à la plupart des PME quand elles parlent d'informatique.

Vous pouvez appliquer seul l'intégralité de ce qui suit. Certains le feront, et ils auront raison. D'autres constateront en le lisant qu'ils n'ont ni le temps, ni les compétences internes, ni l'envie de porter ce chantier — et c'est une conclusion tout aussi légitime. Dans les deux cas, vous saurez de quoi vous parlez, ce qui est déjà l'essentiel.

Les chiffres et repères réglementaires cités sont sourcés en fin de document. Les ordres de grandeur budgétaires restent indicatifs : ils doivent être adaptés à l'activité, à la taille, aux dépendances et au niveau de risque de chaque entreprise.

Sommaire

Partie I — Comprendre

- 1 — Ce qu'est vraiment votre système d'information
- 2 — Les six symptômes d'un SI mal géré
- 3 — Qui pilote, qui décide, qui exécute

Partie II — Cartographier

- 4 — L'inventaire : on ne protège que ce que l'on connaît
- 5 — Évaluer la criticité : la matrice à quatre cases
- 6 — La dette technique : la mesurer avant qu'elle ne vous mesure

Partie III — Construire le socle

- 7 — Les postes de travail
- 8 — Le réseau et les accès distants
- 9 — Serveurs, cloud et hébergement : arbitrer sans dogme
- 10 — Les identités et les droits d'accès
- 11 — Sauvegarde et reprise d'activité

Partie IV — Sécuriser

- 12 — Les douze mesures qui bloquent l'essentiel des attaques
- 13 — Le facteur humain : sensibiliser sans infantiliser
- 14 — Données personnelles, RGPD et NIS2 : ce qui vous concerne réellement
- 15 — Gérer une crise cyber : les 72 premières heures

Partie V — Piloter

- 16 — Le budget informatique : construire, arbitrer, défendre
- 17 — Contrats et prestataires : lire un contrat d'infogérance
- 18 — Les indicateurs qui comptent
- 19 — Votre feuille de route : 30 / 90 / 365 jours

Annexes

- A — Checklist d'audit express (60 questions)
- B — Modèle de registre des actifs
- C — Modèle de charte informatique
- D — Fiche réflexe « incident en cours »
- E — Glossaire
- F — Sources et ressources gratuites

PARTIE I — COMPRENDRE

1. Ce qu'est vraiment votre système d'information

La plupart des dirigeants pensent « informatique » et visualisent des ordinateurs. C'est une erreur de cadrage qui coûte cher, parce qu'elle conduit à traiter comme un poste de dépense ce qui est en réalité un actif d'exploitation.

Votre système d'information, c'est l'ensemble des moyens qui permettent à votre entreprise de produire, stocker, transmettre et exploiter de l'information. Il comprend quatre couches :

La couche « matérielle ». Postes de travail, serveurs, téléphones, imprimantes, équipements réseau, périphériques métier (terminaux de caisse, lecteurs de codes-barres, automates, capteurs). C'est la couche visible, celle qu'on achète et qu'on amortit.

La couche « logicielle ». Systèmes d'exploitation, logiciels métier, ERP, CRM, suite bureautique, outils de communication, applications SaaS. C'est la couche qui structure réellement vos processus — et celle que vous maîtrisez le moins, parce qu'elle s'achète souvent par abonnement, service par service, sans vision d'ensemble.

La couche « données ». Fichiers clients, contrats, comptabilité, plans, historiques de production, e-mails, sauvegardes. C'est la seule couche irremplaçable. Un serveur se rachète en 48 heures ; dix ans d'historique commercial, non.

La couche « humaine et organisationnelle ». Qui a le droit de faire quoi, qui appelle qui en cas de panne, comment un nouvel arrivant est équipé, comment un départ est traité. C'est la couche la plus souvent absente des discussions — et celle qui détermine si les trois autres tiennent debout.

À retenir. Un SI n'est pas une somme d'équipements. C'est une chaîne. Sa solidité est celle de son maillon le plus faible, et ce maillon est rarement technique.

Le SI comme chaîne de valeur

Faites l'exercice suivant. Prenez votre processus le plus critique — celui sans lequel vous ne facturez plus — et listez chaque étape en notant, pour chacune, l'outil informatique mobilisé.

Exemple pour une PME de négoce :

Étape	Outil	Sans cet outil, on fait quoi ?
Réception commande client	Messagerie + ERP	Téléphone, saisie manuelle
Vérification stock	ERP	Comptage physique
Bon de préparation	ERP + imprimante	Papier, erreurs
Expédition	Portail transporteur	Appel transporteur
Facturation	ERP + logiciel compta	Blocage total
Encaissement	Banque en ligne	Retard, tension de trésorerie

Cet exercice, mené sur trois ou quatre processus, produit en une demi-journée une vision plus utile que la plupart des audits. Il révèle vos points de rupture réels, indépendamment de la valeur comptable des équipements.

La question qui structure tout

Une seule question doit guider vos arbitrages informatiques : **combien de temps mon entreprise peut-elle fonctionner sans tel élément, et que coûte chaque heure d'arrêt ?**

Cette question a un nom technique : la **DMIA** (durée maximale d'interruption admissible, ou RTO en anglais). Elle se double d'une seconde : **quelle quantité de données puis-je me permettre de perdre ?** (la **PDMA**, ou RPO).

Un exemple concret. Une PME industrielle de 60 salariés estime qu'une journée d'arrêt de production coûte 18 000 € de marge perdue. Sa DMIA sur l'ERP de production est donc de quelques heures, pas de trois jours. Cela justifie un investissement en redondance que la même entreprise refuserait pour son serveur d'impression, dont l'arrêt coûte de l'agacement et rien d'autre.

Sans ces deux chiffres, toute discussion sur la sauvegarde ou la haute disponibilité est une discussion de croyances.

2. Les six symptômes d'un SI mal géré

Un SI ne tombe pas en panne brutalement. Il se dégrade, et il envoie des signaux. Voici les six plus fiables.

Symptôme 1 — Personne ne sait exactement ce que vous possédez. Si vous ne pouvez pas produire en cinq minutes la liste de vos postes, serveurs, licences et abonnements, vous ne gérez pas votre SI : vous le subissez. C'est le symptôme le plus répandu et le plus facile à corriger.

Symptôme 2 — Les mots de passe circulent. Un compte partagé entre trois personnes, un mot de passe administrateur écrit dans un fichier Excel, un accès d'un ancien salarié toujours actif. Ce sont des symptômes d'absence de gestion des identités, qui est le premier vecteur d'incident réel.

Symptôme 3 — La sauvegarde n'a jamais été restaurée. Une sauvegarde qui n'a pas été testée n'est pas une sauvegarde : c'est une hypothèse. Le taux d'échec de restauration lors du premier test réel est notoirement élevé, et il se découvre toujours au pire moment.

Symptôme 4 — Les dépenses informatiques sont invisibles. Elles existent, mais sont éparpillées : un abonnement sur la carte bancaire du dirigeant, un autre en note de frais, une licence renouvelée automatiquement pour un outil peu ou plus utilisé. La consolidation révèle fréquemment des doublons, des abonnements dormants et des contrats devenus inadaptés.

Symptôme 5 — Tout repose sur une personne. « Il n'y a que Marc qui sait faire ça. » Marc est une excellente personne. Marc est aussi un point de défaillance unique, qu'il soit salarié, prestataire ou beau-frère du dirigeant.

Symptôme 6 — On appelle quand ça casse. Le mode pompier paraît économique tant que rien ne bloque, mais chaque urgence mobilise davantage de temps, perturbe l'activité et laisse peu de place à l'analyse des causes. La prévention transforme ces dépenses imprévisibles en décisions planifiées.

Auto-diagnostic rapide. Comptez vos symptômes. 0 à 1 : votre SI est piloté. 2 à 3 : vous avez une dette de gestion, rattrapable en un trimestre. 4 et plus : vous êtes en risque opérationnel, et statistiquement, l'incident est devant vous.

3. Qui pilote, qui décide, qui exécute

C'est le chapitre le plus court et le plus déterminant.

Dans une PME de 10 à 100 salariés, il n'y a généralement pas de DSI. Il y a, dans le meilleur des cas, un « référent informatique » : un salarié plus à l'aise que les autres, souvent au contrôle de gestion ou aux services généraux, qui gère l'informatique sur 10 % de son temps sans mandat clair ni budget propre.

Cette configuration produit systématiquement les mêmes effets : décisions repoussées, arbitrages faits par défaut, prestataire choisi sur la relation plutôt que sur le besoin.

Les trois rôles à distinguer

Le sponsor — c'est vous, dirigeant. Vous ne décidez pas des choix techniques. Vous décidez du niveau de risque acceptable et du budget. Ces deux décisions ne sont pas déléguables, parce qu'elles engagent l'entreprise.

Le pilote — il traduit les besoins métier en exigences, suit les prestataires, tient l'inventaire, prépare les arbitrages. Ce rôle peut être interne (à condition d'être formalisé : fiche de poste, temps alloué, budget) ou externalisé (DSI à temps partagé, généralement 1 à 4 jours par mois pour une PME de cette taille).

L'exécutant — il installe, configure, dépanne. C'est un rôle technique, très majoritairement externalisé en PME.

L'erreur la plus fréquente est de confondre pilote et exécutant, c'est-à-dire de demander à son prestataire de dépannage de définir sa stratégie informatique. Ce n'est pas malhonnête de sa part, mais c'est structurellement biaisé : on ne demande pas à son garagiste de décider quelle voiture acheter.

Formaliser en une page

Un document d'une page suffit à professionnaliser la gouvernance :

- Qui est sponsor, pilote, exécutant (nom, société, coordonnées)
- Le budget annuel validé et sa répartition
- Les seuils de décision (en dessous de X €, le pilote décide seul ; au-dessus, arbitrage du sponsor)
- La fréquence du point de pilotage (mensuel ou trimestriel)
- Les trois indicateurs suivis

Ce document existe rarement. Quand il existe, la qualité des décisions change en un trimestre.

PARTIE II — CARTOGRAPHIER

4. L'inventaire : on ne protège que ce que l'on connaît

L'inventaire est la fondation. Toutes les démarches qui suivent — sécurité, budget, conformité, contractualisation — en dépendent. C'est aussi la tâche la moins gratifiante, ce qui explique qu'elle soit si souvent absente.

Ce qu'il faut inventorier

Le matériel. Pour chaque équipement : type, marque et modèle, numéro de série, date d'achat, utilisateur ou emplacement, date de fin de garantie, système d'exploitation et version, statut (en service, stock, à réformer).

Les logiciels et abonnements. Nom, éditeur, type de licence (perpétuelle ou abonnement), nombre de postes couverts, coût annuel, date d'échéance, mode de renouvellement (tacite ou non), interlocuteur commercial, criticité.

Les données. Nature (clients, RH, comptable, technique), volume approximatif, localisation (serveur local, cloud, poste utilisateur), présence de données personnelles, niveau de confidentialité, sauvegarde associée.

Les accès et comptes. Comptes administrateurs, comptes de service, accès distants, comptes sur services externes (banque, URSSAF, plateformes clients, réseaux sociaux, nom de domaine, hébergement web).

Les contrats. Prestataire, périmètre, durée, préavis de résiliation, engagements de niveau de service, coût.

La règle du 80/20

Ne visez pas l'exhaustivité au premier tour. Un inventaire à 80 %, tenu à jour, vaut infiniment mieux qu'un inventaire parfait abandonné au bout de six mois.

Méthode pragmatique, réalisable en deux jours pour une PME de 50 personnes :

1. **Jour 1, matin** — Exportez ce qui existe déjà : liste des immobilisations comptables, relevés bancaires filtrés sur les prestataires informatiques des 12 derniers mois, annuaire des utilisateurs.
2. **Jour 1, après-midi** — Tour physique des locaux, avec un téléphone pour photographier les étiquettes de numéros de série.
3. **Jour 2, matin** — Entretiens de 15 minutes avec chaque responsable de service : quels outils utilisez-vous réellement, lequel vous bloque s'il tombe.
4. **Jour 2, après-midi** — Consolidation dans un tableur unique, identification des trous.

Le tour des relevés bancaires réserve presque toujours des surprises. C'est là que se trouvent les abonnements oubliés, les doublons fonctionnels (deux outils de visioconférence, trois espaces de stockage) et le « shadow IT » — ces outils souscrits par un service sans en informer personne.

Point de vigilance : le « shadow » IT. Un commercial qui stocke son fichier prospects sur un cloud personnel, un chef de projet qui utilise un outil gratuit non validé, un service qui souscrit une IA générative avec un compte personnel. Ce n'est ni de la malveillance ni de la bêtise : c'est le signe que l'outil officiel ne répond pas au besoin. Traitez la cause, pas seulement le symptôme.

Tenir l'inventaire à jour

Un inventaire se périmé en six mois s'il n'y a pas de rituel. Trois déclencheurs suffisent :

- **Toute entrée ou sortie de salarié** déclenche une mise à jour (matériel attribué ou restitué, comptes créés ou désactivés).
- **Tout achat supérieur à un seuil** défini passe par le pilote et est enregistré.
- **Une revue trimestrielle** de 30 minutes vérifie les échéances de contrats et de garanties à venir.

5. Évaluer la criticité : la matrice à quatre cases

Tout ne se protège pas au même niveau. Vouloir tout sécuriser au maximum est le meilleur moyen de ne rien sécuriser correctement, faute de budget et d'attention.

Classez chaque élément de votre inventaire selon deux axes : **l'impact d'une indisponibilité** et **l'impact d'une fuite ou d'une altération**.

	Impact indisponibilité faible	Impact indisponibilité fort
Impact fuite faible	Standard — Traitement courant, sauvegarde simple, remplacement sur incident. <i>Ex. : imprimante bureau, poste d'appoint.</i>	Disponibilité — Redondance, pièces de rechange, procédure de contournement écrite. <i>Ex. : serveur de production, connexion Internet.</i>
Impact fuite fort	Confidentialité — Chiffrement, accès restreint, traçabilité. <i>Ex. : archives RH, dossiers juridiques.</i>	Critique — Tout le dispositif : redondance, chiffrement, sauvegarde renforcée, contrôle d'accès strict, tests réguliers. <i>Ex. : ERP, base clients, comptabilité.</i>

En pratique, dans une PME, la case « Critique » contient rarement plus de cinq à huit éléments. C'est là que doit se concentrer 70 % de votre effort et de votre budget de protection.

Le calcul du coût d'arrêt

Pour objectiver les arbitrages, chiffrez une heure d'arrêt de vos éléments critiques :

Coût horaire d'arrêt ≈ (Masse salariale des personnes bloquées + Marge horaire perdue + Coûts de rattrapage) × Facteur d'aggravation

Le facteur d'aggravation (généralement 1,2 à 2) couvre les effets indirects : pénalités de retard, perte de confiance client, heures supplémentaires de rattrapage.

Exemple pour un cabinet de 25 personnes dont 20 sont bloquées par une panne d'ERP :

- Masse salariale bloquée : $20 \times 35 \text{ €/h} = 700 \text{ €/h}$
- Marge non produite : environ 900 €/h
- Sous-total : 1 600 €/h, soit environ 12 800 € par jour ouvré
- Avec facteur 1,4 : **environ 18 000 € par jour**

Ce chiffre change immédiatement la nature des discussions budgétaires. Une solution de reprise à 6 000 € par an cesse d'être une dépense pour devenir une assurance dont la prime représente un tiers de journée d'arrêt.

6. La dette technique : la mesurer avant qu'elle ne vous mesure

La dette technique, c'est l'écart accumulé entre l'état actuel de votre SI et l'état où il devrait être. Comme la dette financière, elle porte intérêts : chaque année de retard rend le rattrapage plus coûteux.

Les cinq formes de dette technique en PME

Dette matérielle. Postes de plus de cinq ans, serveurs hors garantie, équipements réseau obsolètes. Symptôme : lenteurs, pannes répétées, incompatibilités.

Dette logicielle. Systèmes d'exploitation ou logiciels métier qui ne reçoivent plus de mises à jour de sécurité. C'est la forme la plus dangereuse, parce qu'elle est invisible tant qu'elle n'est pas exploitée.

Dette de configuration. Paramétrages par défaut jamais revus, règles de pare-feu empilées depuis dix ans, droits d'accès accordés ponctuellement et jamais retirés.

Dette documentaire. Aucune procédure écrite, aucun schéma réseau, mots de passe dans la tête d'une personne. Elle ne provoque pas d'incident, mais elle multiplie par cinq le temps de résolution de tous les autres.

Dette contractuelle. Contrats reconduits tacitement, conditions jamais renégociées, périmètre devenu inadapté.

La mesurer simplement

Pour chaque ligne de votre inventaire, attribuez un statut :

- **Vert** — supporté, à jour, sous garantie ou contrat actif
- **Orange** — fin de support ou fin de garantie dans moins de 12 mois
- **Rouge** — hors support, hors garantie, ou obsolète

Le ratio de rouge sur le total, pondéré par la criticité, donne votre indicateur de dette. Un objectif raisonnable : **zéro rouge sur les éléments critiques**, moins de 20 % de rouge sur l'ensemble.

Le piège du renouvellement par vagues

Beaucoup de PME renouvellent leur parc en une fois : 40 postes achetés la même année, remplacés cinq ans plus tard en un seul chèque. C'est un pic budgétaire douloureux qui pousse à repousser, donc à accumuler de la dette.

L'alternative est le **renouvellement glissant** : remplacer chaque année un cinquième du parc (pour une durée de vie cible de cinq ans). Le budget devient prévisible et lissé, la dette ne s'accumule jamais, et vous conservez une capacité d'arbitrage annuelle.

PARTIE III — CONSTRUIRE LE SOCLE

7. Les postes de travail

Le poste de travail est le point d'entrée de la grande majorité des incidents, et le principal poste de dépense visible. Il mérite une politique, pas des décisions au coup par coup.

Standardiser

La standardisation est le levier d'économie le plus sous-estimé en PME. Définissez deux ou trois profils de poste, pas douze :

Profil	Usage	Caractéristiques indicatives	Budget indicatif
Standard	Bureautique, messagerie, applications web	16 Go RAM, SSD 512 Go, processeur milieu de gamme	700 – 950 €
Mobile	Commerciaux, dirigeants, itinérants	Ultraportable, autonomie, station d'accueil	1 000 – 1 500 €
Puissance	CAO, montage, calcul, développement	32 Go RAM et plus, carte graphique dédiée	1 800 – 3 500 €

Les bénéfices de la standardisation sont concrets : achats groupés donc remises, image de déploiement unique, pièces de rechange mutualisées, support simplifié, prévisibilité budgétaire.

La durée de vie réelle

La durée d'amortissement comptable (souvent trois ans) n'est pas la durée de vie économique. En pratique :

- **Postes fixes bureautiques** : 5 à 6 ans
- **Portables** : 4 à 5 ans (usure mécanique, batterie)
- **Postes de puissance** : 3 à 4 ans (obsolescence fonctionnelle)

Au-delà, le coût de possession repart à la hausse : pannes, temps perdu, incompatibilités, risque de sécurité si le système n'est plus supporté.

Acheter, louer ou reconditionné ?

Achat. Le plus simple, propriété immédiate, coût de possession le plus bas sur la durée de vie complète. Inconvénient : pic de trésorerie et tendance à conserver trop longtemps.

Location ou leasing. Lisse la trésorerie, inclut souvent le renouvellement et parfois le support. Coût total supérieur de 10 à 25 % sur la durée. Pertinent si la trésorerie est tendue ou si la discipline de renouvellement fait défaut.

Reconditionné. Économie de 30 à 50 %, empreinte environnementale réduite, garantie généralement de 12 à 36 mois. Adapté aux profils standards et aux postes non critiques. À éviter pour les usages intensifs et les profils puissance.

Une combinaison fonctionne bien : neuf pour les profils critiques et mobiles, reconditionné pour les postes standards et d'appoint.

Le socle de configuration

Chaque poste livré doit sortir avec le même socle, sans exception :

- Système d'exploitation à jour, mises à jour automatiques activées
- Chiffrement du disque activé (BitLocker sous Windows, FileVault sous macOS)
- Solution de protection déployée et supervisée
- Compte utilisateur **sans droits administrateur**
- Session verrouillée automatiquement après 10 minutes d'inactivité
- Sauvegarde des dossiers de travail configurée
- Inventaire mis à jour

Le point sur les droits « administrateur » est le plus discuté et le plus important. Un utilisateur sans droits administrateur ne peut pas installer de logiciel — c'est contraignant, et c'est précisément l'objectif : la majorité des compromissions de poste exploitent des droits élevés inutiles. Prévoyez en contrepartie un processus de demande d'installation rapide, faute de quoi les utilisateurs contourneront.

8. Le réseau et les accès distants

Les fondamentaux

La connexion Internet. Elle est devenue aussi critique que l'électricité. Deux questions : quel débit réel avez-vous besoin (comptez 5 à 10 Mbit/s symétriques par utilisateur simultané en usage cloud intensif), et que se passe-t-il si elle tombe ?

Pour toute entreprise dont l'activité s'arrête sans Internet, un **lien de secours** est indispensable : seconde ligne d'un opérateur différent, ou secours 4G/5G avec bascule automatique. Le surcoût est de l'ordre de 40 à 150 € par mois. Comparez-le à votre coût horaire d'arrêt.

Le pare-feu. Équipement qui filtre les échanges entre votre réseau et l'extérieur. Une box opérateur n'en est pas un au sens professionnel. Un pare-feu d'entreprise pour une PME représente 800 à 3 000 € d'investissement, plus un abonnement annuel de mise à jour des signatures. Sans cet abonnement, il perd l'essentiel de son intérêt au bout d'un an.

Le Wi-Fi. Trois règles simples : un réseau invités strictement séparé du réseau interne, un chiffrement WPA3 (ou WPA2 au minimum), et un mot de passe interne différent du mot de passe invités — ce dernier étant à changer périodiquement.

La segmentation. Séparer logiquement les usages : postes bureautiques, serveurs, équipements de production, caméras et objets connectés, invités. Un objet connecté compromis ne doit pas pouvoir atteindre votre serveur comptable. C'est une mesure peu coûteuse et très efficace, souvent négligée.

Le télétravail et les accès distants

Le sujet a été traité dans l'urgence en 2020 et rarement repris depuis. C'est aujourd'hui une source majeure de vulnérabilité.

Ce qu'il faut proscrire : l'ouverture directe d'un accès bureau à distance sur Internet (le fameux RDP exposé). C'est l'une des portes d'entrée les plus exploitées par les rançongiciels. Si vous avez un doute, faites vérifier ce point en priorité absolue.

Ce qui fonctionne :

- Un **VPN** d'entreprise, systématiquement couplé à une authentification à deux facteurs
- Ou une solution d'accès applicatif moderne de type « zero trust », qui n'expose que l'application et non le réseau
- Un poste **fourni et maîtrisé par l'entreprise**, plutôt que l'ordinateur personnel du salarié
- Une charte de télétravail écrite précisant les usages autorisés

Quand faire appel à un prestataire. L'architecture réseau et les accès distants sont le domaine où l'auto-formation atteint le plus vite ses limites. Une erreur de configuration de pare-feu ne se voit pas : elle se découvre le jour de l'incident. Si vous n'avez pas de compétence réseau interne, c'est le premier périmètre à confier à un professionnel — et à faire auditer périodiquement par quelqu'un d'autre que celui qui l'a installé.

9. Serveurs, cloud et hébergement : arbitrer sans dogme

Le débat « cloud ou pas cloud » est mal posé. La bonne question est : **pour chaque usage, où l'hébergement est-il le plus pertinent ?** La réponse est presque toujours hybride.

Grille de décision

Critère	Plutôt local (on-premise)	Plutôt cloud
Volume de données très important	■	
Besoin de latence très faible (production, CAO)	■	
Contrainte réglementaire de localisation forte	■	Selon l'offre
Équipe technique interne disponible	■	
Effectif variable, croissance rapide		■
Télétravail ou multisites		■
Trésorerie tendue, préférence pour l'OPEX		■
Besoin de reprise d'activité rapide sans investir		■
Application métier éditée uniquement en SaaS		■

Le coût réel du cloud

Le cloud est souvent présenté comme moins cher. Sur trois à cinq ans, ce n'est pas systématique. Ce qu'il faut intégrer dans la comparaison :

- Le coût des licences en mode abonnement, qui augmente avec l'effectif
- Les frais de sortie de données, parfois substantiels

- Le coût de la bande passante et du lien de secours
- L'absence de valeur résiduelle (vous ne possédez rien)
- Mais aussi : l'absence de renouvellement matériel, de maintenance, de climatisation, d'onduleur, et la mutualisation de compétences que vous n'avez pas

Le cloud transforme une dépense d'investissement irrégulière en charge récurrente prévisible. C'est souvent son principal intérêt pour une PME — davantage que l'économie brute.

Trois points de vigilance contractuelle

La réversibilité. Comment récupérez-vous vos données si vous changez de fournisseur ? Sous quel format ? À quel coût ? Faites inscrire la réponse au contrat. C'est la clause la plus souvent omise et la plus coûteuse à découvrir tardivement.

La localisation. Où sont physiquement stockées vos données ? Un hébergement en Union européenne est préférable pour les données personnelles. Pour certains secteurs (santé notamment), des certifications spécifiques sont obligatoires — l'hébergement de données de santé requiert une certification HDS.

La responsabilité de la sauvegarde. Point crucial et massivement mal compris : **la plupart des fournisseurs SaaS ne sauvegardent pas vos données au sens où vous l'entendez.** Ils assurent la disponibilité de leur infrastructure, pas la récupération d'un fichier que vous auriez supprimé il y a trois semaines, ni la restauration après un chiffrement par rançongiciel de vos espaces cloud. Vérifiez le modèle de responsabilité partagée de chaque service, et prévoyez une sauvegarde tierce pour vos données critiques hébergées en SaaS.

10. Les identités et les droits d'accès

Si vous ne deviez traiter qu'un seul chapitre de ce livret, ce serait celui-ci. La gestion des identités est le domaine où l'effort est le plus faible et le gain de sécurité le plus élevé.

Les mots de passe : ce qui a changé

Les recommandations ont évolué. Ce qui est aujourd'hui admis :

- **La longueur prime sur la complexité.** Une phrase de passe de 20 caractères est plus robuste et plus mémorisable qu'un mot de 8 caractères truffé de symboles.
- **Le changement périodique obligatoire est contre-productif.** Imposer un changement tous les 90 jours conduit les utilisateurs à des variations prévisibles (Ete2026!, Automne2026!). On ne change un mot de passe que s'il y a suspicion de compromission.
- **L'unicité est non négociable.** Un mot de passe réutilisé entre un service professionnel et un service personnel compromis expose l'entreprise entière.
- **Le gestionnaire de mots de passe est indispensable.** Il est déraisonnable de demander à un salarié de mémoriser 40 identifiants uniques. Un gestionnaire d'entreprise coûte 3 à 6 € par utilisateur et par mois, et résout le problème structurellement — y compris le partage sécurisé d'accès entre collègues et la reprise des accès au départ d'un salarié.

L'authentification à deux facteurs (MFA)

C'est la mesure au meilleur rapport efficacité/coût de toute la sécurité informatique. Elle neutralise l'immense majorité des attaques par vol d'identifiants.

Priorité de déploiement :

1. Comptes administrateurs — sans exception, immédiatement

2. Messagerie professionnelle — c'est la clé de tout le reste (elle sert à réinitialiser les autres mots de passe)
3. Accès bancaires et financiers
4. Accès distants et VPN
5. Applications métier critiques
6. Tous les autres services

Sur les méthodes : une application d'authentification ou une clé physique sont nettement préférables au SMS, vulnérable à l'échange de carte SIM. La clé physique reste la référence pour les comptes les plus sensibles.

Le principe du moindre privilège

Chaque personne ne doit disposer que des droits strictement nécessaires à son travail. Ce principe est simple à énoncer et exigeant à tenir, car les droits s'accumulent naturellement au fil des mutations internes.

En pratique :

- **Comptes nominatifs uniquement.** Aucun compte partagé, jamais. Sans compte nominatif, aucune traçabilité n'est possible.
- **Séparation des comptes administrateurs.** L'administrateur travaille au quotidien avec un compte standard et n'utilise son compte à privilèges que pour les tâches qui l'exigent.
- **Revue semestrielle des droits.** Chaque responsable valide la liste des accès de son équipe. L'exercice prend une heure et révèle systématiquement des droits obsolètes.
- **Procédure d'arrivée et de départ formalisée.** Voir ci-dessous.

Les processus d'arrivée et de départ

Le départ d'un salarié est le moment de vérité de votre gestion des identités. Une checklist écrite, déclenchée automatiquement par les RH :

À l'arrivée (J-2)

- ☐ Création du compte nominatif avec les droits du profil défini
- ☐ Attribution du matériel, enregistrement à l'inventaire
- ☐ Remise et signature de la charte informatique
- ☐ Inscription au module de sensibilisation
- ☐ Configuration du gestionnaire de mots de passe et du MFA

Au départ (J du départ, avant la fin de journée)

- ☐ Désactivation immédiate de tous les comptes (pas suppression : désactivation, pour préserver les données)
- ☐ Redirection ou transfert de la messagerie vers le responsable
- ☐ Récupération du matériel, effacement sécurisé, retour à l'inventaire
- ☐ Changement des mots de passe partagés auxquels la personne avait accès
- ☐ Retrait des accès aux services externes (banque, plateformes, réseaux sociaux)
- ☐ Révocation des accès physiques (badges) et distants

Le point le plus souvent oublié est le troisième : les accès aux services externes, qui ne passent pas par l'annuaire d'entreprise et restent actifs des années.

11. Sauvegarde et reprise d'activité

La règle 3-2-1-1-0

C'est le standard actuel, et il mérite d'être compris ligne à ligne :

- **3** copies de vos données (l'originale et deux sauvegardes)
- **2** supports de nature différente (par exemple disque local et cloud)
- **1** copie hors site (protection contre incendie, dégât des eaux, vol)
- **1** copie **hors ligne ou immuable** — c'est-à-dire inaccessible depuis le réseau, ou non modifiable même par un administrateur. Cet ajout récent répond directement aux rançongiciels, qui cherchent systématiquement à chiffrer les sauvegardes avant les données de production.
- **0** erreur lors des tests de restauration

Le dernier point est celui que personne ne fait, et c'est celui qui compte.

Ce qu'il faut sauvegarder — et ce qu'on oublie

La liste habituelle (serveurs de fichiers, bases de données, comptabilité) est généralement couverte. Les oublis récurrents :

- **Les postes de travail.** Les commerciaux et les dirigeants stockent des données critiques localement.
- **Les boîtes mail.** Y compris et surtout en environnement cloud.
- **Les données SaaS.** CRM, outils de gestion de projet, espaces de stockage en ligne.
- **Les configurations.** Pare-feu, serveurs, équipements réseau. Restaurer des données sur une infrastructure qu'il faut reconfigurer de zéro double le temps de reprise.
- **Le site web et la base associée.**
- **Les certificats et clés de chiffrement.** Une sauvegarde chiffrée dont la clé a été perdue est une sauvegarde perdue.

Tester, vraiment

Une restauration doit être testée selon trois niveaux, avec des fréquences distinctes :

Niveau	Contenu	Fréquence	Durée
1 — Fichier	Restaurer un fichier au hasard et vérifier son intégrité	Mensuelle	15 min
2 — Système	Restaurer un serveur complet sur un environnement de test	Semestrielle	2 à 4 h
3 — Exercice de crise	Simuler une perte totale, dérouler la procédure complète avec les équipes	Annuelle	1 journée

Le niveau 3 est celui que les PME sautent, et c'est le seul qui révèle les vrais problèmes : documentation introuvable, mot de passe détenu par une personne en congé, délai de commande de matériel non anticipé, ordre de redémarrage des applications inconnu.

Le plan de reprise d'activité

Un PRA n'a pas besoin d'être un document de 80 pages. Pour une PME, cinq pages bien faites suffisent et doivent contenir :

1. **Les scénarios couverts** — panne serveur, rançongiciel, sinistre des locaux, indisponibilité du prestataire, perte d'un service cloud
2. **Les objectifs par application** — DMIA et PDMA pour chaque élément critique
3. **La chaîne d'alerte** — qui appelle qui, dans quel ordre, avec les numéros à jour
4. **Les procédures de bascule** — étape par étape, rédigées pour être exécutables par quelqu'un qui n'a pas écrit le document
5. **Les modes dégradés** — comment continuer à travailler sans le SI pendant la reprise (bons de commande papier, liste de contacts imprimée, procédure de facturation de secours)

Impératif : ce document doit exister sous forme **papier** et en copie hors ligne. Un PRA stocké uniquement sur le serveur chiffré par le rançongiciel n'a jamais aidé personne.

PARTIE IV — SÉCURISER

12. Les douze mesures qui bloquent l'essentiel des attaques

La sécurité informatique souffre d'un problème de présentation : elle est décrite comme un domaine infini et technique, ce qui décourage. En réalité, un petit nombre de mesures bien appliquées bloque la très grande majorité des attaques réellement rencontrées par une PME.

Voici ces mesures, classées par rapport efficacité/effort.

1. Activer l'authentification à deux facteurs partout où c'est possible. Effort : faible. Impact : majeur. Commencez par la messagerie et les comptes administrateurs.

2. Appliquer les mises à jour de sécurité sous 30 jours (7 jours pour les failles critiques exposées). La majorité des intrusions exploitent des failles connues et corrigées depuis des mois. Activez les mises à jour automatiques sur les postes ; planifiez une fenêtre mensuelle pour les serveurs et équipements réseau.

3. Supprimer les droits « administrateur » des comptes utilisateurs. Effort : faible techniquement, moyen politiquement. Impact : très élevé sur la propagation.

4. Mettre en place une sauvegarde conforme au 3-2-1-1-0 et la tester. C'est votre dernière ligne de défense. Elle doit tenir.

5. Déployer une protection moderne sur les postes et serveurs (EDR). L'antivirus traditionnel détecte des signatures connues ; un EDR détecte des comportements anormaux. Comptez 3 à 8 € par poste et par mois. La supervision est aussi importante que l'outil : un EDR qui alerte dans une console que personne ne consulte ne sert à rien.

6. Filtrer la messagerie. La messagerie reste le vecteur d'entrée dominant. Un filtrage anti-hameçonnage, l'authentification des expéditeurs (SPF, DKIM, DMARC) et une bannière signalant les mails externes réduisent fortement l'exposition. Ces trois enregistrements DNS sont gratuits à mettre en place et protègent aussi votre réputation : sans eux, n'importe qui peut usurper votre nom de domaine pour écrire à vos clients.

7. Segmenter le réseau. Empêcher qu'une compromission d'un poste donne accès à tout.

8. Chiffrer les postes mobiles et les supports amovibles. Un portable volé chiffré est une perte matérielle. Non chiffré, c'est potentiellement une violation de données à notifier.

9. Sécuriser les accès distants. Aucun accès bureau à distance directement exposé sur Internet. VPN avec MFA, ou solution d'accès applicatif.

10. Journaliser et conserver les traces. Sans journaux, un incident ne peut être ni compris, ni prouvé, ni notifié correctement. Conservez au minimum six mois de journaux pour les éléments critiques.

11. Formaliser une charte informatique signée. Elle a une valeur juridique en cas de litige et une valeur pédagogique au quotidien. Modèle en annexe C.

12. Sensibiliser les équipes, régulièrement et brièvement. Voir chapitre suivant.

Repère de maturité. Dans le baromètre national 2025 de Cybermalveillance.gouv.fr, trois TPE-PME sur quatre déclaraient consacrer moins de 2 000 € par an à la cybersécurité et 80 % se disaient non préparées à une attaque ou incapables d'évaluer leur préparation. Ce constat n'est pas une recommandation budgétaire : le bon niveau d'investissement dépend de vos risques, de vos dépendances et du coût acceptable d'une interruption.

Ce que vous n'avez probablement pas besoin d'acheter

Par honnêteté, quelques dépenses souvent proposées et rarement justifiées à ce stade de maturité :

- Un **SOC** (centre de supervision 24/7) tant que les douze mesures ci-dessus ne sont pas en place. C'est mettre une alarme sur une maison sans serrure.
- Des **outils de sécurité redondants** : trois solutions qui font la même chose se gênent mutuellement et consomment votre budget.
- Une **certification** (ISO 27001 par exemple) si aucun client ne l'exige contractuellement. La démarche est utile, mais coûteuse et prématurée pour la plupart des PME.
- Une **cyber-assurance** souscrite avant d'avoir mis en place les mesures de base : les contrats comportent des exclusions et des exigences minimales, et un sinistre peut ne pas être couvert si vous n'avez pas respecté vos propres déclarations.

13. Le facteur humain : sensibiliser sans infantiliser

L'expression « le maillon faible, c'est l'humain » est à la fois banale et fautive dans sa formulation. Un salarié qui clique sur un lien piégé n'est pas négligent : il fait son travail, vite, dans un environnement qui rend l'erreur facile.

La bonne approche consiste donc à agir sur deux plans : réduire les occasions d'erreur (les mesures techniques du chapitre précédent) et augmenter la capacité de détection (la sensibilisation).

Ce qui ne fonctionne pas

- La formation annuelle de deux heures en amphithéâtre. Le taux de rétention à trois mois est proche de zéro.
- Les campagnes de faux hameçonnage utilisées comme outil de sanction. Elles produisent de la peur, donc du silence — c'est-à-dire l'inverse de l'objectif, puisqu'un incident non signalé est un incident non traité.
- Les documents de 40 pages que personne ne lit.

Ce qui fonctionne

Des sessions courtes et fréquentes. 15 à 20 minutes par trimestre, sur un thème unique et concret. Mieux vaut quatre fois vingt minutes qu'une fois deux heures.

Des exemples issus de votre secteur. Une fausse facture fournisseur parle davantage à un comptable qu'une explication générique sur le hameçonnage.

Des simulations bienveillantes. Une campagne de faux hameçonnage est utile si elle est annoncée dans son principe (pas dans sa date), si les résultats sont communiqués de manière agrégée et anonyme, et si celui qui clique reçoit une explication et non un blâme.

Une culture du signalement. L'indicateur qui compte n'est pas le nombre de personnes qui cliquent, mais le **délai entre le clic et le signalement**. Communiquez-le. Félicitez publiquement le premier qui signale

une tentative. Un salarié qui appelle en disant « je crois que j'ai fait une bêtise » dans les cinq minutes vous fait économiser une crise.

Les quatre scénarios à couvrir en priorité

L'hameçonnage. Les signaux d'alerte : urgence inhabituelle, demande de confidentialité, lien dont l'adresse réelle diffère du texte affiché, pièce jointe inattendue, expéditeur dont le domaine comporte une variation subtile.

La fraude au président et au faux fournisseur. C'est la menace la plus coûteuse pour une PME, et elle est purement organisationnelle. La parade est une procédure, pas un outil : **tout changement de coordonnées bancaires fournisseur, et tout virement dépassant un seuil défini, fait l'objet d'une vérification par un canal différent** — un appel sur le numéro connu du fournisseur, pas sur celui indiqué dans le mail. Cette règle unique, appliquée sans exception y compris quand c'est le dirigeant qui demande, neutralise l'essentiel du risque.

Les supports amovibles et les usages personnels. Clé USB trouvée, chargement d'un téléphone personnel sur un poste, transfert d'un fichier professionnel vers une messagerie personnelle.

L'usage des IA génératives. Sujet nouveau et déjà massif. Vos salariés utilisent ces outils, avec ou sans votre accord. Plutôt que d'interdire — ce qui pousse vers le shadow IT — définissez un cadre : quels outils sont autorisés, quelles catégories d'informations ne doivent jamais y être saisies (données personnelles, données clients identifiantes, secrets industriels, code source propriétaire), et quelle vérification humaine s'applique avant utilisation d'un résultat.

14. Données personnelles, RGPD et NIS2 : ce qui vous concerne réellement

Ce chapitre est volontairement factuel. La conformité est un sujet où l'anxiété commerciale a beaucoup circulé ; l'objectif ici est de vous permettre de distinguer vos obligations réelles du reste.

RGPD : le socle applicable à toutes les entreprises

Le RGPD s'applique dès que vous traitez des données personnelles — ce qui est le cas de toute entreprise ayant des salariés et des clients. Quatre obligations structurent l'essentiel.

Le registre des traitements. Obligatoire dans la quasi-totalité des cas. Il liste, pour chaque traitement (paie, recrutement, prospection, gestion clients, vidéosurveillance...) : la finalité, la base légale, les catégories de données et de personnes concernées, les destinataires, la durée de conservation, les mesures de sécurité. La CNIL met à disposition un modèle gratuit adapté aux petites structures.

L'information des personnes. Mentions d'information sur vos formulaires, votre site, vos contrats de travail. Elles doivent être claires et accessibles.

Le respect des droits. Accès, rectification, effacement, opposition, portabilité. Vous devez pouvoir répondre à une demande sous un mois. En pratique, cela suppose de savoir où sont vos données — d'où l'importance du chapitre 4.

La notification des violations. En cas de violation de données personnelles présentant un risque, notification à la CNIL **sous 72 heures**. Si le risque est élevé pour les personnes, information des personnes concernées également. Ce délai est court : il suppose d'avoir anticipé qui rédige, qui valide, et sur quelle base factuelle.

Le **DPO** (délégué à la protection des données) n'est obligatoire que dans trois cas : organisme public, suivi régulier et systématique à grande échelle, ou traitement à grande échelle de données sensibles. La plupart des PME ne sont pas concernées, mais désigner un référent interne reste une bonne pratique.

Sur les durées de conservation, quelques repères usuels en France : double des bulletins de paie 5 ans au titre du Code du travail (une conservation plus longue est fréquente en pratique, et la dématérialisation impose des obligations de mise à disposition spécifiques), pièces comptables 10 ans, CV de candidats non retenus 2 ans maximum après le dernier contact, données de prospection commerciale 3 ans après le dernier contact, journaux de connexion 6 mois à 1 an. Vérifiez les durées applicables à votre secteur.

NIS2 : êtes-vous concerné ?

La directive européenne NIS2 élargit le nombre d'organisations soumises à des obligations de cybersécurité. À la date de cette édition, sa transposition en droit français est toujours en cours. Les textes définitifs et leurs modalités d'application doivent donc être vérifiés sur les services officiels de l'ANSSI.

L'assujettissement dépend principalement de trois éléments :

1. Le secteur d'activité. La directive vise notamment l'énergie, les transports, la santé, l'eau, certaines infrastructures numériques, l'administration publique, la gestion des déchets, l'industrie, l'agroalimentaire, certains fournisseurs numériques et la recherche.
2. La taille de l'organisation. Les seuils d'effectif et les seuils financiers entrent dans l'analyse, avec des exceptions et des règles particulières selon les activités.

Le rôle réel de l'entreprise. Certaines organisations peuvent être concernées indépendamment de leur taille ou du fait de services essentiels qu'elles rendent. Utilisez MonEspaceNIS2 et, si nécessaire, un conseil juridique pour qualifier votre situation.

Deux points méritent votre attention même si vous n'êtes pas assujetti :

- **L'effet de ruissellement contractuel.** Les entités assujetties doivent sécuriser leur chaîne d'approvisionnement. Si vous êtes fournisseur d'un grand compte ou d'une entité concernée, vous recevrez des exigences contractuelles de sécurité. C'est déjà le cas dans l'industrie.
- **La responsabilité des dirigeants.** La directive engage explicitement la responsabilité des organes de direction, qui doivent approuver les mesures et suivre des formations. C'est un changement de nature : la cybersécurité devient un sujet de gouvernance, pas de service technique.

L'ANSSI publie le Référentiel Cyber France ReCyF et des fiches pratiques pour aider les organisations à structurer leurs mesures de sécurité. Ces ressources constituent également un cadre utile pour les entreprises qui ne sont pas directement assujetties.

Autres cadres possiblement applicables

Selon votre activité : hébergement de données de santé (certification HDS), secteur financier (règlement DORA), sous-traitance pour la défense, ou exigences sectorielles portées par vos donneurs d'ordre. Vérifiez ce point avec votre conseil juridique plutôt qu'avec votre prestataire informatique.

15. Gérer une crise cyber : les 72 premières heures

Une crise cyber ne se gère pas en improvisant. Voici la trame à préparer **avant**, et à appliquer le jour venu.

Heure 0 à 1 — Détecter et isoler

Ne pas éteindre les machines. C'est le réflexe le plus courant et le plus dommageable : l'extinction détruit des éléments de preuve présents en mémoire vive et peut, sur certains rançongiciels, déclencher des mécanismes supplémentaires.

Isoler du réseau. Débrancher le câble réseau, désactiver le Wi-Fi. Isoler physiquement, pas électriquement.

Alerter la chaîne définie. Dirigeant, pilote informatique, prestataire, assureur cyber le cas échéant.

Ouvrir un journal de crise. Sur papier ou sur un support non compromis : heure, constat, action, décideur. Ce document sera indispensable pour la notification, l'assurance et le dépôt de plainte.

Heure 1 à 6 — Qualifier et contenir

- Déterminer le périmètre : quels systèmes, quelles données, depuis quand
- Vérifier l'intégrité et l'isolement des sauvegardes **avant** toute tentative de restauration
- Couper les accès distants et changer les mots de passe administrateurs depuis un poste sain
- Décider du mode dégradé : quelles activités continuent, comment, avec quels moyens

Heure 6 à 24 — Décider et communiquer

Sur le paiement d'une rançon. La position des autorités françaises est constante : le paiement est déconseillé. Il ne garantit ni la restitution des données, ni l'absence de publication, ni l'absence de nouvelle attaque, et il finance l'écosystème criminel. Prévenez immédiatement votre assureur et déposez plainte dans les délais prévus par le contrat et les textes applicables.

Communication interne. Les salariés savent qu'il se passe quelque chose. Un message factuel, même incomplet, vaut mieux que le silence, qui génère rumeurs et initiatives individuelles hasardeuses.

Communication externe. Préparez un message court pour les clients et fournisseurs affectés. La transparence maîtrisée limite les dégâts réputationnels ; la découverte par un tiers les aggrave.

Heure 24 à 72 — Notifier et engager les recours

- **Plainte** auprès de la police ou de la gendarmerie. Nécessaire pour l'assurance et pour les suites judiciaires.
- **Notification CNIL sous 72 heures** si des données personnelles sont concernées et que la violation présente un risque.
- **Déclaration à l'assureur** dans les délais du contrat.
- **Signalement** sur la plateforme publique [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr), qui oriente et référence des prestataires de réponse à incident.
- Pour les entités assujetties à NIS2 : appliquez les obligations et délais de notification prévus par les textes en vigueur et les instructions de l'ANSSI.

Après — La reprise et le retour d'expérience

La tentation est de restaurer vite et de tourner la page. C'est une erreur : restaurer sur une infrastructure encore compromise conduit à une seconde attaque, souvent plus destructrice.

Séquence correcte : identifier le point d'entrée, le corriger, reconstruire sur une base saine, restaurer les données, surveiller de manière renforcée pendant plusieurs semaines, puis conduire un retour d'expérience écrit débouchant sur un plan d'action daté.

À préparer dès aujourd'hui — 30 minutes. Une fiche papier, affichée et distribuée : les numéros du dirigeant, du pilote informatique, du prestataire, de l'assureur, du référent juridique. Les quatre premières actions (ne pas éteindre / isoler / alerter / journaliser). L'adresse de [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr). C'est le meilleur retour sur temps investi de tout ce livret.

PARTIE V — PILOTER

16. Le budget informatique : construire, arbitrer, défendre

Les ordres de grandeur

Le budget informatique d'une PME française se situe généralement entre **3 % et 6 % du chiffre d'affaires**, avec des écarts sectoriels marqués : plutôt 2 à 4 % dans l'industrie et le BTP, plutôt 5 à 6 % dans les services intellectuels et le conseil, davantage encore dans les activités nativement numériques.

Ces pourcentages sont des repères de cadrage, pas des objectifs. Un budget de 2 % dans une entreprise dont l'informatique est peu structurante peut être parfaitement sain ; un budget de 6 % mal alloué reste mal alloué.

Une seconde lecture, souvent plus parlante, est le **coût par utilisateur et par an**, toutes charges comprises (matériel amorti, licences, infogérance, connectivité, sécurité). Pour une PME correctement équipée, l'ordre de grandeur se situe fréquemment entre **1 500 et 3 000 € par utilisateur et par an**. En dessous de 1 000 €, il est probable que de la dette s'accumule quelque part.

La structure d'un budget lisible

Poste	Part indicative	Nature
Matériel (renouvellement glissant)	15 – 25 %	Investissement
Licences et abonnements logiciels	25 – 35 %	Récurrent
Infogérance et support	20 – 30 %	Récurrent
Connectivité et hébergement	8 – 15 %	Récurrent
Sécurité (outils et services dédiés)	8 – 15 %	Récurrent
Projets et évolutions	10 – 20 %	Variable
Provision imprévus	5 – 10 %	Réserve

La provision pour imprévus est la ligne que tout le monde supprime et que tout le monde regrette. Sans elle, le moindre incident se finance en annulant un projet.

Les trois erreurs budgétaires classiques

Confondre coût d'achat et coût de possession. Un serveur à 8 000 € coûte, sur cinq ans, entre 20 000 et 30 000 € en incluant licences, maintenance, électricité, sauvegarde et temps d'administration. Raisonniez toujours en TCO sur la durée de vie.

Sous-estimer la charge de conduite du changement. Sur un projet applicatif, la formation, la reprise de données et l'accompagnement représentent couramment 30 à 50 % du coût total. Un projet budgété uniquement sur les licences échouera ou dérapera.

Traiter la sécurité comme une ligne optionnelle. Elle est arbitrée en dernier et coupée en premier, alors qu'elle relève de la même logique qu'une assurance ou qu'une norme incendie.

Défendre le budget

Trois arguments fonctionnent en comité de direction, et un seul est technique :

1. **Le coût d'arrêt** (chapitre 5). Chiffré, il rend toute discussion de disponibilité tangible.
2. **Le coût de la non-conformité**. Sanctions, mais surtout perte de marchés : les clauses de sécurité dans les appels d'offres sont devenues éliminatoires dans de nombreux secteurs.
3. **Le coût de l'inefficacité**. Dix minutes perdues par jour et par salarié à cause d'outils lents ou mal intégrés représentent, pour 50 personnes, l'équivalent d'environ un poste et demi à temps plein sur l'année.

17. Contrats et prestataires : lire un contrat d'infogérance

L'externalisation est le mode d'organisation dominant en PME, et c'est un choix rationnel. Encore faut-il contractualiser correctement, car un contrat d'infogérance mal cadré transforme un partenaire en source de blocage.

Les modèles d'offre

L'assistance à la demande (régie). Vous payez à l'intervention ou par lot d'heures. Souple, adapté aux très petites structures ou aux besoins ponctuels. Inconvénient majeur : le modèle économique du prestataire est aligné sur le volume d'incidents, pas sur leur absence.

Le forfait par poste ou par utilisateur. Un montant mensuel fixe couvre un périmètre défini. C'est le modèle le plus courant et généralement le plus sain : le prestataire a intérêt à ce que ça fonctionne. Comptez, selon le périmètre et le niveau de service, **40 à 120 € par utilisateur et par mois** pour une infogérance incluant support, supervision et administration courante.

Le DSI à temps partagé. Ce n'est pas de l'infogérance mais du pilotage : quelques jours par mois pour tenir la stratégie, arbitrer, piloter les prestataires et préparer les décisions. Souvent complémentaire d'une infogérance technique.

Les clauses à examiner en priorité

Le périmètre exact. Ce qui est inclus, et surtout ce qui ne l'est pas. Les exclusions classiques : les logiciels métier (« nous ne supportons pas votre ERP »), les déplacements, les interventions hors heures ouvrées, les projets, la sécurité au-delà de l'antivirus.

Les engagements de service (SLA). Deux notions à ne pas confondre : le **délai de prise en charge** (quelqu'un s'occupe de vous) et le **délai de résolution** (le problème est réglé). Beaucoup de contrats n'engagent que le premier. Exigez une grille par niveau de gravité, et vérifiez ce qui se passe en cas de non-respect — des pénalités symboliques ne sont pas des engagements.

La réversibilité. Que se passe-t-il si vous changez de prestataire ? Restitution de la documentation, des mots de passe, des configurations, des données ; accompagnement de transition ; délai et coût. **C'est la clause la plus importante et la plus souvent absente**. Un prestataire qui refuse de la formaliser vous indique quelque chose.

La propriété. Les licences sont-elles à votre nom ou au sien ? Le nom de domaine ? Les certificats ? Les comptes chez les fournisseurs cloud ? Des PME découvrent au moment de partir que leur nom de domaine appartient à leur prestataire.

La documentation. Exigez contractuellement un dossier d'exploitation à jour : schéma réseau, inventaire, procédures, coordonnées des fournisseurs. Et exigez d'en détenir une copie.

Les accès administrateurs. Vous devez disposer, en coffre-fort scellé si nécessaire, des accès administrateurs de votre propre système. Ne jamais en être dépossédé.

La durée et le préavis. Un an renouvelable est un bon équilibre. Méfiez-vous des engagements de trois ans à reconduction tacite avec préavis de six mois.

Piloter la relation

Un contrat ne suffit pas ; la relation se pilote.

- **Un point mensuel ou trimestriel** avec un compte rendu écrit : incidents du mois, tendances, actions correctives, sujets à venir.
- **Un tableau de bord partagé** : nombre d'incidents, délais respectés, état des sauvegardes et des tests, état des mises à jour, dette technique.
- **Une revue annuelle** du contrat et des tarifs.
- **Un audit externe périodique** — tous les deux ou trois ans — par un tiers indépendant. Ce n'est pas une marque de défiance : c'est une pratique de bonne gestion, et un bon prestataire l'accueille favorablement.

Quand faire appel à un prestataire — et lequel. Distinguez trois besoins qui ne se confondent pas : le pilotage (définir la stratégie, arbitrer, contrôler), l'exploitation (faire fonctionner au quotidien) et le contrôle (vérifier). Confier les trois au même acteur revient à supprimer tout contre-pouvoir. La combinaison la plus saine en PME associe un exploitant sous contrat, un pilotage interne ou à temps partagé, et un contrôle externe périodique.

18. Les indicateurs qui comptent

Un tableau de bord informatique de PME tient en une page et se lit en cinq minutes. Voici les indicateurs qui produisent réellement des décisions.

Disponibilité et incidents

Indicateur	Définition	Cible indicative
Taux de disponibilité des services critiques	% de temps de fonctionnement sur la période	> 99,5 %
Nombre d'incidents bloquants	Incidents arrêtant tout ou partie de l'activité	Tendance décroissante
Délai moyen de résolution	Du signalement au rétablissement	Selon SLA
Taux d'incidents récurrents	Part des incidents déjà survenus	< 15 %

Le dernier est le plus révélateur : un taux élevé signifie que l'on traite les symptômes et jamais les causes.

Sécurité

Indicateur	Cible indicative
Postes et serveurs à jour des correctifs de sécurité	> 95 %
Comptes protégés par MFA	100 % des comptes à privilèges, > 90 % au global
Sauvegardes réussies sur la période	100 %
Tests de restauration réalisés vs planifiés	100 %
Comptes actifs sans utilisateur identifié	0
Délai moyen de signalement d'un mail suspect	< 1 h

Économie et dette

Indicateur	Usage
Coût informatique par utilisateur et par an	Comparaison dans le temps et avec le secteur
Part du budget en récurrent vs projet	Un récurrent supérieur à 85 % signale une absence d'investissement
Nombre d'éléments critiques en statut « rouge »	Cible : 0
Écart budget réalisé / budget prévu	Qualité du pilotage
Nombre d'abonnements non utilisés identifiés	Gisement d'économies

La règle de la page unique

Résistez à la tentation d'un tableau de bord exhaustif. Cinq à huit indicateurs suivis mensuellement produisent plus d'effet que trente indicateurs consultés une fois par an. Si un indicateur n'a jamais déclenché de décision en douze mois, supprimez-le.

19. Votre feuille de route : 30 / 90 / 365 jours

Voici une séquence testée, ordonnée par rapport impact/effort. Elle suppose un dirigeant impliqué et un référent identifié.

Les 30 premiers jours — Voir clair

Effort : 3 à 5 jours cumulés. Coût : proche de zéro.

- ☐ Désigner formellement le pilote et lui allouer du temps
- ☐ Réaliser l'inventaire (matériel, logiciels, abonnements, contrats, accès)
- ☐ Passer en revue 12 mois de dépenses informatiques et identifier les doublons
- ☐ Identifier les 5 à 8 éléments critiques et chiffrer le coût horaire d'arrêt
- ☐ Vérifier que la sauvegarde fonctionne et **restaurer un fichier au hasard**
- ☐ Activer le MFA sur la messagerie et tous les comptes administrateurs
- ☐ Lister les comptes actifs et désactiver ceux des personnes parties

- ☐ Rédiger et afficher la fiche réflexe « incident en cours »

Ces huit actions ne coûtent presque rien et éliminent une part importante du risque immédiat.

Les 90 premiers jours — Sécuriser le socle

Effort : 8 à 15 jours cumulés. Coût : premiers investissements.

- ☐ Supprimer les droits administrateur des comptes utilisateurs
- ☐ Mettre en place ou reprendre la sauvegarde selon le principe 3-2-1-1-0
- ☐ Réaliser une restauration complète de test sur un serveur
- ☐ Vérifier et sécuriser les accès distants (aucun RDP exposé)
- ☐ Déployer un gestionnaire de mots de passe
- ☐ Déployer une protection moderne (EDR) supervisée
- ☐ Mettre en place SPF, DKIM et DMARC sur votre domaine
- ☐ Rédiger et faire signer la charte informatique
- ☐ Formaliser les procédures d'arrivée et de départ
- ☐ Établir le registre RGPD des traitements
- ☐ Construire le budget informatique de l'année à venir
- ☐ Relire le contrat du prestataire principal (réversibilité, SLA, propriété)

Les 12 mois — Structurer et pérenniser

Effort : rythme de croisière.

- ☐ Rédiger le plan de reprise d'activité et le tester en conditions réelles
- ☐ Mettre en place le renouvellement glissant du parc
- ☐ Segmenter le réseau
- ☐ Instaurer le programme de sensibilisation trimestriel
- ☐ Mettre en place le tableau de bord mensuel
- ☐ Conduire la première revue semestrielle des droits d'accès
- ☐ Réaliser un audit externe indépendant
- ☐ Définir le cadre d'usage des IA génératives
- ☐ Évaluer l'assujettissement NIS2 et, le cas échéant, engager la mise en conformité
- ☐ Formaliser le document de gouvernance en une page
- ☐ Établir le plan pluriannuel à trois ans

La règle des trois chantiers

N'ouvrez jamais plus de trois chantiers simultanés. Une PME n'a pas la capacité d'absorption d'un grand groupe, et un chantier abandonné coûte plus cher qu'un chantier différé : il consomme du budget, épuise la crédibilité de la démarche et laisse une configuration à moitié faite, parfois moins sûre que la situation initiale.

ANNEXES

Annexe A — Checklist d'audit express

Répondez par oui, non ou partiellement. Chaque « non » sur une question marquée ★ mérite une action dans le trimestre.

Gouvernance

1. ★ Une personne est-elle formellement responsable de l'informatique ?
2. Un budget informatique annuel est-il défini et suivi ?
3. Un point de pilotage régulier a-t-il lieu ?
4. Les seuils de décision et d'engagement sont-ils écrits ?
5. Existe-t-il un plan à 12 mois ?

Inventaire

6. ★ Disposez-vous d'un inventaire à jour du matériel ?
7. ★ Disposez-vous de la liste complète des logiciels et abonnements ?
8. Connaissez-vous les dates d'échéance de vos contrats ?
9. Savez-vous où sont stockées vos données ?
10. Les éléments critiques sont-ils identifiés ?

Postes de travail

11. Les postes sont-ils standardisés sur deux ou trois profils ?
12. ★ Les mises à jour de sécurité sont-elles appliquées automatiquement ?
13. ★ Les utilisateurs travaillent-ils sans droits administrateur ?
14. Les disques des portables sont-ils chiffrés ?
15. Les sessions se verrouillent-elles automatiquement ?
16. Existe-t-il un plan de renouvellement ?

Réseau

17. Disposez-vous d'un pare-feu professionnel avec abonnement actif ?
18. Le Wi-Fi invités est-il séparé du réseau interne ?
19. Le réseau est-il segmenté par usage ?
20. ★ Existe-t-il un accès distant exposé directement sur Internet ?
21. Disposez-vous d'un lien Internet de secours ?
22. Les équipements réseau sont-ils sous support constructeur ?

Identités et accès

23. ★ Le MFA est-il actif sur la messagerie ?
24. ★ Le MFA est-il actif sur tous les comptes administrateurs ?
25. ★ Les comptes partagés ont-ils été éliminés ?
26. Un gestionnaire de mots de passe est-il déployé ?
27. Les administrateurs utilisent-ils un compte séparé au quotidien ?
28. Les droits sont-ils revus au moins une fois par an ?

- 29. ★ Les comptes des personnes parties sont-ils tous désactivés ?
- 30. Une procédure d'arrivée et de départ est-elle écrite ?

Sauvegarde

- 31. ★ Les données critiques sont-elles sauvegardées quotidiennement ?
- 32. ★ Une copie est-elle stockée hors site ?
- 33. ★ Une copie est-elle hors ligne ou immuable ?
- 34. ★ Une restauration a-t-elle été testée dans les 6 derniers mois ?
- 35. Les postes de travail sont-ils inclus dans la sauvegarde ?
- 36. Les données SaaS sont-elles sauvegardées indépendamment ?
- 37. Les configurations d'équipements sont-elles sauvegardées ?
- 38. Les DMIA et PDMA sont-elles définies par application ?

Sécurité

- 39. Une protection moderne est-elle déployée sur tous les postes et serveurs ?
- 40. Les alertes de sécurité sont-elles supervisées par quelqu'un ?
- 41. Un filtrage anti-hameçonnage est-il en place ?
- 42. SPF, DKIM et DMARC sont-ils configurés ?
- 43. Les journaux sont-ils conservés au moins 6 mois ?
- 44. Un audit de sécurité a-t-il eu lieu dans les 24 derniers mois ?
- 45. Une cyber-assurance est-elle souscrite, et ses exigences respectées ?

Humain

- 46. Une charte informatique est-elle signée par tous ?
- 47. Une sensibilisation a-t-elle eu lieu dans les 12 derniers mois ?
- 48. ★ Une procédure de vérification des changements de RIB fournisseurs existe-t-elle ?
- 49. Les salariés savent-ils qui alerter et comment ?
- 50. Un cadre d'usage des IA génératives est-il défini ?

Continuité

- 51. ★ Un plan de reprise d'activité écrit existe-t-il ?
- 52. Est-il disponible sous forme papier et hors ligne ?
- 53. A-t-il été testé dans les 12 derniers mois ?
- 54. Les modes dégradés sont-ils décrits ?
- 55. La chaîne d'alerte est-elle à jour ?

Conformité et prestataires

- 56. Le registre RGPD des traitements est-il tenu à jour ?
- 57. Les durées de conservation sont-elles définies et appliquées ?
- 58. ★ Détenez-vous vos propres accès administrateurs ?
- 59. ★ Une clause de réversibilité figure-t-elle au contrat ?
- 60. La documentation d'exploitation est-elle en votre possession ?

Interprétation. Moins de 10 « non » : votre SI est correctement tenu. De 10 à 25 : situation courante, avec des priorités identifiables. Plus de 25 : reprise structurée nécessaire — commencez par les questions étoilées, dans l'ordre.

Annexe B — Modèle de registre des actifs

Colonnes minimales pour un tableur exploitable :

Feuille « Matériel » ID · Type · Marque/Modèle · N° de série · Date d'achat · Prix · Fin de garantie · Utilisateur/Emplacement · Système et version · Criticité (1-4) · Statut · Commentaire

Feuille « Logiciels et abonnements » Nom · Éditeur · Type de licence · Nb de postes · Coût annuel · Date d'échéance · Reconduction tacite (O/N) · Préavis · Contact commercial · Criticité · Utilisé réellement (O/N)

Feuille « Données » Catégorie · Emplacement · Volume · Données personnelles (O/N) · Base légale · Durée de conservation · Sauvegardée (O/N) · Fréquence · Confidentialité

Feuille « Accès et comptes » Service · Type de compte · Titulaire · MFA actif (O/N) · Dernière revue · Criticité

Feuille « Contrats » Prestataire · Objet · Date de début · Durée · Préavis · SLA · Coût annuel · Contact · Clause de réversibilité (O/N)

Annexe C — Trame de charte informatique

Structure type, à adapter et à faire valider par votre conseil juridique et vos représentants du personnel avant diffusion.

1. **Objet et champ d'application** — Qui est concerné (salariés, intérimaires, stagiaires, prestataires), quels équipements.
2. **Moyens mis à disposition** — Matériel, comptes, services ; règles d'attribution et de restitution.
3. **Règles d'usage** — Usage professionnel ; tolérance d'un usage personnel raisonnable ; usages interdits.
4. **Sécurité** — Mots de passe, verrouillage de session, supports amovibles, installation de logiciels, signalement des incidents.
5. **Mobilité et télétravail** — Équipements hors des locaux, connexions publiques, confidentialité en espace partagé.
6. **Messagerie et Internet** — Règles d'usage, statut des messages personnels (à identifier comme tels), archivage.
7. **Données personnelles et confidentialité** — Obligations des salariés, secret professionnel.
8. **Usage des IA génératives** — Outils autorisés, informations proscrites, vérification des résultats.
9. **Contrôles et journalisation** — Nature des contrôles, finalités, durée de conservation, information des personnes.
10. **Sanctions** — Rappel du régime disciplinaire.
11. **Entrée en vigueur, modification, signature.**

Points d'attention juridiques : la charte doit être portée à la connaissance des salariés (annexion au règlement intérieur ou remise contre décharge), le comité social et économique doit être consulté lorsqu'il existe, et les dispositifs de contrôle doivent être proportionnés et déclarés au registre RGPD.

Annexe D — Fiche réflexe « incident en cours »

À imprimer, afficher près des postes clés et conserver en copie papier hors du système d'information.

SI VOUS SUSPECTEZ UN INCIDENT DE SÉCURITÉ

1. N'ÉTEIGNEZ PAS l'ordinateur.

2. ISOLEZ-LE du réseau — débranchez le câble réseau, coupez le Wi-Fi.

3. ALERTEZ immédiatement :

- Référent informatique interne :
- Prestataire informatique (astreinte) :
- Direction :
- Assureur cyber / n° de police :

4. NOTEZ sur papier : l'heure, ce que vous avez vu, ce que vous veniez de faire, les messages affichés (photographiez l'écran).

5. NE TENTEZ RIEN d'autre. Ne supprimez rien, ne redémarrez pas, ne réinstallez pas, ne payez rien.

Ressources publiques

- [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) — assistance et mise en relation
- Police ou gendarmerie — dépôt de plainte
- CNIL — notification sous 72 h si données personnelles concernées

Signaux d'alerte à connaître : fichiers renommés ou illisibles, message de rançon, lenteur générale inexplicable, comptes verrouillés, activité en dehors des heures ouvrées, alertes de connexion depuis l'étranger, mail sortant envoyé à votre insu.

Annexe E — Glossaire

BYOD — Usage d'équipements personnels à des fins professionnelles. DMIA (RTO) — Durée maximale d'interruption admissible : combien de temps un service peut rester indisponible. PDMA (RPO) — Perte de données maximale admissible : quelle quantité de données récentes peut être perdue. EDR — Solution de détection et réponse sur les postes et serveurs, successeur de l'antivirus classique. Hameçonnage (phishing) — Message frauduleux visant à obtenir des informations ou à faire exécuter une action. Infogérance — Externalisation de tout ou partie de l'exploitation du système d'information. MFA / 2FA — Authentification à plusieurs facteurs : mot de passe complété par un second élément. NIS2 — Directive européenne de cybersécurité élargissant les obligations à de nombreux secteurs. PCA / PRA — Plan de continuité (fonctionner pendant) et plan de reprise (redémarrer après). PSSI — Politique de sécurité du système d'information : document cadre définissant les règles. Rançongiciel (ransomware) — Logiciel malveillant chiffrant les données contre rançon. Réversibilité — Capacité contractuelle à récupérer données et services pour changer de fournisseur. RGPD — Règlement européen sur la protection des données personnelles. SaaS — Logiciel utilisé en ligne par abonnement, hébergé par l'éditeur. Shadow IT — Outils utilisés dans l'entreprise sans validation ni connaissance de la direction. SLA — Engagement contractuel de niveau de service (délais de prise en charge et de résolution). SOC — Centre de supervision de sécurité assurant une surveillance continue. TCO — Coût total de possession sur la durée de vie complète d'un actif. VPN — Tunnel chiffré permettant un accès distant sécurisé au réseau de l'entreprise. Zero trust — Approche de sécurité ne présupant aucune confiance implicite, vérifiant chaque accès.

Annexe F — Ressources gratuites et sources

Ressources publiques françaises

- ANSSI et MesServicesCyber — Guides d'hygiène informatique, Référentiel Cyber France ReCyF, fiches pratiques et services d'accompagnement. Documentation gratuite et régulièrement mise à jour.
- [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) — Assistance aux victimes, kits de sensibilisation prêts à l'emploi, annuaire de prestataires labellisés ExpertCyber.

- **CNIL** (cnil.fr) — Modèle de registre des traitements pour petites structures, guide de la sécurité des données personnelles, référentiels sectoriels.
- **Bpifrance** — Diagnostics et dispositifs d'accompagnement à la cybersécurité des PME.
- **France Num** — Ressources et aides à la transformation numérique des TPE-PME.

Sources des données citées

Les repères réglementaires et les chiffres de maturité cyber ont été vérifiés à partir de publications institutionnelles disponibles en octobre 2026. Les principales sources sont les suivantes :

- ANSSI et MesServicesCyber — Référentiel Cyber France ReCyF v2.5, fiches pratiques ReCyF, portail NIS2 et informations sur l'avancement de la transposition française.
- Cybermalveillance.gouv.fr — Baromètre national 2025 de la maturité cyber des TPE-PME : enquête OpinionWay menée auprès de 588 entreprises françaises de moins de 250 salariés.
- CNIL — Guide de la sécurité des données personnelles 2026, checklist de sécurité et recommandations relatives à la charte informatique.
- Directive UE 2022/2555 dite NIS2 et informations officielles publiées par l'ANSSI sur sa transposition et sa mise en œuvre en France.
- Règlement UE 2016/679 dit RGPD et doctrine publiée par la CNIL.

Les chiffres du marché varient sensiblement selon les méthodologies et les périmètres. Ils sont donnés ici comme repères d'ordre de grandeur pour l'arbitrage, non comme valeurs de référence.

Et maintenant ?

Vous disposez désormais d'une méthode complète. En appliquant la feuille de route du chapitre 19, vous pouvez reprendre progressivement le contrôle de votre système d'information et rendre vos décisions plus prévisibles.

Trois questions déterminent la suite :

Avez-vous le temps ? L'inventaire et les 30 premiers jours représentent environ une semaine de travail cumulée. Les 90 jours, deux à trois semaines. C'est du temps qui ne se prend pas sur les activités commerciales ou de production.

Avez-vous les compétences ? Une partie de ce livret s'applique sans compétence technique particulière : gouvernance, inventaire, budget, contrats, procédures. Une autre partie — réseau, sauvegarde, sécurisation des accès distants — suppose une expertise réelle, et les erreurs y sont invisibles jusqu'à l'incident.

Avez-vous le recul ? Le point le plus difficile à obtenir seul est le regard extérieur : ce que l'on ne voit plus parce qu'on y est habitué.

Si vous souhaitez un regard extérieur, choisissez un interlocuteur qui commence par écouter et cartographier, distingue le pilotage de l'exploitation, inscrit la réversibilité dans ses engagements et vous laisse détenir vos propres accès.

OAKTEAM Europe

Comprendre d'abord. Décider ensuite.

OAKTEAM Score — Obtenez gratuitement une première lecture structurée de votre situation. [Commencer le Score](#)

Décodage SI — Faites analyser votre système d'information, vos risques et vos priorités dans un cadre documenté. [Découvrir Décodage SI](#) · [Contacter OAKTEAM](#)

Ce guide est diffusé à titre informatif. Il ne constitue ni un conseil juridique, ni un conseil en assurance, ni une garantie de conformité réglementaire. Les obligations applicables dépendent de votre secteur, de votre taille, de votre activité et des textes en vigueur. Faites qualifier votre situation lorsque l'enjeu le justifie.

OAKTEAM Europe — Édition octobre 2026 — Reproduction interdite sans autorisation.