

Bien choisir son prestataire informatique

Infogérance, maintenance, sécurité : les questions qui séparent un vrai partenaire d'une future mauvaise surprise.

9 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/choisir-prestataire-it

Pour une TPE/PME sans équipe informatique, le prestataire IT est de fait le gardien du système : il détient les accès administrateurs, les sauvegardes, la réponse aux incidents. Bien choisi, c'est un multiplicateur de sérénité ; mal choisi, c'est un risque de plus — et des situations de dépendance douloureuses. Voici la grille d'évaluation, côté client.

1. Les questions qui révèlent le sérieux

- « Comment gérez-vous VOS accès à notre système ? » — comptes nominatifs, MFA, journalisation : un prestataire qui se connecte en admin partagé sans MFA est disqualifié
- « Que se passe-t-il si nous sommes attaqués un samedi soir ? » — astreinte réelle, délais d'intervention contractuels, procédure écrite
- « Comment testez-vous nos sauvegardes ? » — la réponse doit inclure des restaurations régulières documentées, pas « elles tournent »
- « Que nous remettez-vous si nous partons ? » — documentation, mots de passe, exports : la réversibilité se juge avant de signer
- « Qui sont vos clients comparables à nous ? » — des références vérifiables dans votre taille et votre secteur

2. Lire le contrat comme il faut

- Le périmètre précis : quels équipements, quels logiciels, qu'est-ce qui est inclus et hors forfait — le flou d'aujourd'hui est la facture surprise de demain
- Les engagements chiffrés (SLA) : délais de prise en compte ET de résolution, plages horaires, pénalités
- La propriété : les comptes (domaine, hébergement, licences, admin cloud) sont au nom de VOTRE entreprise, jamais à celui du prestataire
- La réversibilité : restitution de la documentation et des accès en fin de contrat, avec délais et sans frais dissuasifs
- La sécurité du prestataire lui-même : assurance cyber, engagement de confidentialité, clauses RGPD (article 28)

ATTENTION

Le signal d'alarme absolu : le prestataire qui garde les mots de passe « pour vous simplifier la vie » — domaine à son nom, admin cloud sur son email, documentation « dans sa tête ». Le jour d'un désaccord commercial, votre système devient son otage. Tout doit être au nom de l'entreprise, documenté, et accessible à un tiers en cas de besoin.

3. Les modèles de prestation

L'intervention à la demande

On appelle quand ça casse. Adapté aux très petites structures peu dépendantes de l'informatique — mais personne ne surveille rien entre deux pannes : ni sauvegardes, ni mises à jour, ni alertes. Le mode « pompier » coûte souvent plus cher au final que la prévention.

L'infogérance (forfait mensuel)

Supervision continue, maintenance préventive, support aux utilisateurs, gestion des sauvegardes et mises à jour. C'est le modèle pertinent dès que l'informatique conditionne l'activité. Le prix se compare à périmètre égal : nombre de postes et serveurs, plages d'astreinte, inclusions sécurité (EDR supervisé, sensibilisation).

Les services de sécurité managés

Au-delà de l'infogérance classique : EDR supervisé 24/7 (MDR), audits réguliers, exercices de phishing, accompagnement conformité. Selon la sensibilité de votre activité, ces briques s'ajoutent chez le même prestataire ou chez un spécialiste.

4. Piloter la relation dans la durée

- Un point périodique (trimestriel par exemple) avec indicateurs : incidents, délais tenus, état des sauvegardes et mises à jour, recommandations
- Un interlocuteur désigné de chaque côté — les demandes qui partent dans le vide sont le premier motif d'insatisfaction
- Exiger la documentation à jour de VOTRE système, consultable par vous, hébergée hors de ce système (utile le jour où il est chiffré)
- Rester décideur : le prestataire recommande, l'entreprise arbitre — notamment sur les investissements de sécurité, avec des risques expliqués en langage métier

L'essentiel à retenir

01 Vérifier la sécurité des accès du prestataire (MFA, comptes nominatifs)

02 Exiger des SLA chiffrés et une astreinte adaptée à votre activité

03 Garder tous les comptes au nom de l'entreprise

04 Négocier la réversibilité avant de signer

05 Vérifier assurance, clauses RGPD et références comparables

06 Instaurer un point de pilotage périodique avec indicateurs

Questions fréquentes

Quel budget prévoir pour l'infogérance d'une TPE/PME ?

Les forfaits se chiffrent généralement par poste et par mois (ordre de grandeur : quelques dizaines d'euros par poste, serveurs et options sécurité en sus). Méfiez-vous des écarts extrêmes : le forfait deux fois moins cher exclut souvent l'essentiel (interventions plafonnées, sécurité en option, astreinte facturée). Comparez à périmètre écrit égal.

Faut-il tout confier au même prestataire ?

Un interlocuteur unique simplifie le quotidien et évite les renvois de responsabilité. La séparation garde du sens pour le contrôle : faire auditer la sécurité par un tiers indépendant de celui qui l'opère évite d'être juge et partie. Beaucoup de PME combinent : un infogérant au quotidien, un audit externe périodique.

Comment changer de prestataire sans catastrophe ?

La transition se prépare : inventaire des accès et comptes à transférer, période de recouvrement où l'ancien documente et le nouveau reprend, changement de tous les mots de passe administrateurs à la bascule, et vérification des sauvegardes sous contrôle du nouveau. Si le contrat prévoyait la réversibilité, tout cela est fluide — c'est maintenant qu'on mesure l'importance de l'avoir négociée.

Notre « informaticien », c'est le neveu du dirigeant. C'est grave ?

Le problème n'est pas la personne, c'est la structure : pas de contrat, pas d'astreinte, pas de documentation, pas d'assurance, et tout repose sur une disponibilité bénévole. Pour une activité qui dépend de son informatique, il faut au minimum formaliser (documentation, sauvegardes vérifiées, accès au nom de l'entreprise) — et souvent basculer vers un professionnel, le neveu restant un excellent relais local.

Pour aller plus loin

Cybermalveillance.gouv.fr — annuaire des prestataires labellisés ExpertCyber — www.cybermalveillance.gouv.fr/cherche-prestataire

ANSSI — prestataires qualifiés — cyber.gouv.fr/produits-services-qualifies

Structurer sans vous noyer dans la paperasse ?

Audit, mise en conformité, chartes et sensibilisation des équipes : un accompagnement à la taille de votre entreprise.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr