Sécurisez votre infrastructure : les 10 critères pour choisir votre partenaire d'infogérance

Sécurité et conformité réglementaire

• Vérifier la certification ISO/IEC 27001 pour garantir un système de management de la sécurité de l'information (SMSI) conforme aux standards internationaux.

• S'assurer de la localisation des centres de données au sein de l'Union européenne et de la stricte conformité au RGPD pour le stockage des données personnelles.

• Auditer le processus de gestion des accès via l'utilisation de solutions PAM (Privileged Access Management) et l'authentification multifacteur (MFA) obligatoire pour les techniciens.

Expertise et garanties contractuelles

• Confirmer la détention du label 'Expert Cyber' délivré par l'ANSSI, gage d'une expertise reconnue en cybersécurité.

• Exiger une preuve d'assurance responsabilité civile professionnelle spécifiquement adaptée aux risques IT et aux dommages immatériels (perte de données, interruption d'activité).

• Valider l'inclusion d'une clause de réversibilité opérationnelle détaillée pour sécuriser la reprise des données et le transfert de compétences en fin de contrat.

Pilotage et performance opérationnelle

• Exiger un contrat incluant un SLA (Service Level Agreement) avec des temps de rétablissement (GTR) et des temps d'intervention (GTI) chiffrés.

• Évaluer la capacité du prestataire à fournir un reporting mensuel complet (disponibilité, incidents, temps de réponse, état des correctifs).

• Vérifier l'existence d'une procédure de gestion des mises à jour (patch management) automatisée et documentée pour limiter les vulnérabilités.

Continuité d'activité

• S'assurer de la mise en place d'une sauvegarde externalisée géographiquement distincte du site principal.

• Confirmer la réalisation régulière d'exercices de restauration complets pour garantir l'intégrité et la disponibilité des données en cas de sinistre.