RAPPORT DE DIAGNOSTIC

# Cybersécurité PME

Identifiant du diagnostic : **CD-F93CF-B88CD-5D560**

14 octobre 2026
Rapport confidentiel

SCORE DE MATURITÉ CYBERSÉCURITÉ

**55**

/100

**Niveau moyen — des améliorations importantes sont nécessaires**

## Résumé pour la direction

Votre entreprise obtient un score de 55/100, ce qui correspond à un niveau de protection moyen. Deux risques majeurs nécessitent votre attention immédiate : l'absence totale de plan de gestion de crise en cas d'attaque informatique (vous pourriez perdre plusieurs semaines d'activité sans savoir comment réagir), et des manquements aux obligations légales sur la protection des données personnelles (risque d'amende pouvant atteindre 4% de votre chiffre d'affaires). La bonne nouvelle : vos équipes sont déjà sensibilisées aux risques et vos accès informatiques sont bien gérés. Avec quelques actions ciblées dans les prochaines semaines, vous pouvez significativement renforcer votre protection.

**Points positifs identifiés**

- Vos collaborateurs sont formés et sensibilisés aux risques informatiques, ce qui réduit fortement le risque d'erreur humaine comme cliquer sur un email frauduleux
- La gestion des mots de passe et des accès aux systèmes est bien maîtrisée, limitant les risques d'intrusion par des comptes compromis

## Résultats par domaine

| | |
|---|---|
| Gouvernance | 44/100 |
| Accès & identités | 75/100 |
| Infrastructure | 56/100 |
| Données & RGPD | 42/100 |
| Sensibilisation | 75/100 |
| Incidents | 25/100 |
| Analyse risque | 63/100 |

## Analyse des risques identifiés

CRITIQUE **Aucun plan de secours si votre informatique tombe en panne**

Vous n'avez pas de procédure écrite pour continuer à travailler si vos ordinateurs ou logiciels deviennent inaccessibles. En cas d'attaque par rançongiciel (logiciel qui bloque tous vos fichiers), une PME met en moyenne 23 jours à reprendre une activité normale, avec un coût moyen de 50 000 à 200 000 euros entre perte de chiffre d'affaires et frais de remise en route.

CRITIQUE **Non-conformité aux obligations légales sur les données personnelles**

Vous collectez probablement des données clients ou salariés sans respecter certaines obligations légales obligatoires. En cas de contrôle ou de plainte d'un client, vous risquez une amende pouvant aller jusqu'à 4% de votre chiffre d'affaires annuel, plus l'atteinte à votre réputation.

ÉLEVÉ **Absence de règles écrites sur la sécurité informatique**

Sans politique de sécurité formalisée, chaque employé applique ses propres règles. Un collaborateur pourrait par exemple utiliser une clé USB personnelle infectée ou partager des fichiers sensibles sur un service non sécurisé, ouvrant une porte aux pirates.

ÉLEVÉ **Pas de procédure quand un employé quitte l'entreprise**

Sans processus de départ formalisé, un ancien salarié peut conserver ses accès aux emails, fichiers ou logiciels pendant des semaines. Un ex-employé mécontent pourrait supprimer des données ou les transmettre à un concurrent.

ÉLEVÉ **Équipements informatiques potentiellement vulnérables**

Certains de vos ordinateurs ou logiciels ne sont pas protégés de manière optimale contre les attaques connues. Une faille non corrigée peut permettre à un pirate d'entrer dans votre réseau en quelques minutes, comme laisser une fenêtre ouverte dans votre local.

MODÉRÉ **Aucune analyse des risques spécifiques à votre activité**

Vous n'avez jamais identifié quelles sont VOS données les plus sensibles et VOS points faibles. Sans cette vision, vous investissez peut-être dans des protections inutiles tout en laissant des failles béantes sur ce qui compte vraiment pour votre business.

## Plan d'action priorisé

| Priorité | Action | Comment faire | Effort |
|---|---|---|---|
| 🔴 Immédiat | **Créer une fiche réflexe en cas d'attaque informatique** | Rédigez un document d'une page avec les numéros à appeler en urgence (prestataire informatique, assurance, police via le 17) et les 5 premiers gestes à faire (débrancher internet, ne pas éteindre les machines, prévenir la direction). Affichez-le près de chaque poste de travail. | quelques heures |
| 🔴 Immédiat | **Vérifier que vos sauvegardes** | Demandez à votre prestataire informatique ou à la personne qui gère vos sauvegardes de restaurer un fichier | 30 minutes |

| Priorité | Action | Comment faire | Effort |
|---|---|---|---|
| | **fonctionnent vraiment** | datant d'une semaine devant vous. Si personne ne sait le faire ou si ça échoue, vous avez identifié votre urgence numéro 1. | |
| 🔴 Immédiat | **Désigner un responsable des données personnelles** | Nommez officiellement une personne (vous-même ou un collaborateur de confiance) comme référent pour les questions de données personnelles. Cette personne n'a pas besoin d'être experte, juste identifiée comme point de contact. Notifiez ce nom à votre équipe par email. | 30 minutes |
| 🟡 Court terme (1 mois) | **Créer une checklist de départ des employés** | Listez tous les accès à couper quand quelqu'un part : email, logiciels métier, accès aux locaux, récupération du matériel. Ajoutez cette checklist à votre processus RH existant. Un modèle simple en 10 points suffit pour commencer. | quelques heures |
| 🟡 Court terme (1 mois) | **Rédiger 5 règles de sécurité essentielles pour tous** | Écrivez un document d'une page maximum avec 5 règles simples : ne jamais partager son mot de passe, signaler tout email suspect, verrouiller son poste en partant, ne pas brancher de clé USB inconnue, ne pas installer de logiciel sans autorisation. Faites-le signer à chaque employé. | quelques heures |
| 🟡 Court terme (1 mois) | **Faire un audit de sécurité de votre site web et de vos postes** | Demandez à votre prestataire informatique un rapport écrit sur l'état de vos mises à jour (Windows, antivirus, logiciels) et la sécurité de votre site internet. S'il ne peut pas le fournir, c'est un signal d'alerte sur ses compétences en sécurité. | 1-2 jours |
| 🟢 Moyen terme (3 mois) | **Lister vos 10 données les plus précieuses** | Prenez 2 heures avec vos responsables de service pour identifier les 10 informations dont la perte ou le vol serait catastrophique : fichier clients, secrets de fabrication, contrats, données bancaires. Pour chacune, notez où elle est stockée et qui y a accès. | quelques heures |
| 🟢 Moyen terme (3 mois) | **Rédiger un plan de continuité simplifié** | Décrivez sur 2-3 pages comment votre entreprise continuerait à fonctionner pendant 1 semaine sans informatique : qui contacter, quelles tâches prioritaires, quels documents papier conserver, comment communiquer avec les clients. Testez-le mentalement avec votre équipe. | 1-2 jours |

**Votre action prioritaire cette semaine**

Dès demain, appelez votre prestataire informatique et demandez-lui de vous montrer comment restaurer un fichier sauvegardé il y a 7 jours, cette simple vérification de 15 minutes vous dira si vous êtes vraiment protégé en cas de catastrophe.

## Nos recommandations de prestataires en cybersécurité

Ces recommandations sont établies à partir des points à renforcer identifiés par votre diagnostic. Chaque entreprise présentée figure dans au moins une source officielle (Cybermalveillance.gouv.fr · ANSSI — prestataires en cours de qualification · Catalogue ANSSI · Catalogue France Cybersecurity) ; son statut exact et la date de vérification sont indiqués.

### DOCAPOSTE

Le Pack Cyber est une solution de cybersécurité couvrant l'ensemble des besoins essentiels des TPE, PME, ETI et collectivités territoriales. Cette offre unifiée est construite à partir des services et produits des meilleurs acteurs du marché français, choisis et assemblés par Docaposte, qui assure le déploiement et le support.

**Risque concerné :** Gouvernance, analyse de risques et conformité

**Action corrective :** Structurer la politique de sécurité, l'analyse de risques et la conformité RGPD.

**Pourquoi ce prestataire :** Votre diagnostic révèle 4 point(s) à renforcer sur « Gouvernance, analyse de risques et conformité ». Statut : labellisé (Catalogue France Cybersecurity).

**Services :** Le Pack Cyber est une solution de cybersécurité couvrant l'ensemble des besoins essentiels des TPE, PME, ETI et collectivités territoriales. Cette offre unifiée est construite à partir des services et produits des meilleurs acteurs du marché français, choisis et assemblés par Docaposte, qui assure le déploiement et le support.

**Statut vérifié :** Labellisé — Offre « PACK CYBER » labellisée France Cybersecurity (catalogue 2026) — le label porte sur l'offre, pas sur l'ensemble de l'entreprise

**Source :** Catalogue France Cybersecurity · informations vérifiées le 14/10/2026

**Avis clients :** non vérifiés à ce jour

https://www.docaposte.com/

### INSPEERE

DATIS : stockage souverain et résilient, sans cloud centralisé. Données chiffrées, fragmentées et redondantes, récupérables même après une cyberattaque ou un sinistre. Moins 32 % d'énergie, 100 % indépendant. La solution pour DSI et acteurs publics qui refusent les risques du cloud traditionnel.

**Risque concerné :** Sauvegardes et reprise après incident

**Action corrective :** Mettre en place des sauvegardes testées, dont une copie isolée du réseau.

**Pourquoi ce prestataire :** Votre diagnostic révèle 2 point(s) à renforcer sur « Sauvegardes et reprise après incident ». Statut : labellisé (Catalogue France Cybersecurity).

**Services :** DATIS : stockage souverain et résilient, sans cloud centralisé. Données chiffrées, fragmentées et redondantes, récupérables même après une cyberattaque ou un sinistre. Moins 32 % d'énergie, 100 % indépendant. La solution pour DSI et acteurs publics qui refusent les risques du cloud traditionnel.

**Statut vérifié :** Labellisé — Offre « DATIS STOCKAGE DE SAUVEGARDE RÉSILIENT, DISTRIBUÉ ET SOUVERAIN » labellisée France Cybersecurity (catalogue 2026) — le label porte sur l'offre, pas sur l'ensemble de l'entreprise

**Source :** Catalogue France Cybersecurity · informations vérifiées le 14/10/2026

**Avis clients :** non vérifiés à ce jour

https://www.inspeere.com/

### LINKT

SOC 6e Sens est une offre de service de SOC managé 24x7, 100% souveraine à destination des entreprises et collectivités territoriales. Nous apportons une couverture 360° de l'infrastructure on-premise ou Cloud et un service SOC allant de la prévention à la réponse aux incidents et gestion de crises cyber.

**Risque concerné :** Réponse aux incidents (PRIS)

**Action corrective :** Formaliser et tester un plan de réponse aux incidents.

**Pourquoi ce prestataire :** Votre diagnostic révèle 2 point(s) à renforcer sur « Réponse aux incidents (PRIS) ». Statut : labellisé (Catalogue France Cybersecurity).

**Services :** SOC 6e Sens est une offre de service de SOC managé 24x7, 100% souveraine à destination des entreprises et collectivités territoriales. Nous apportons une couverture 360° de l'infrastructure on-premise ou Cloud et un service SOC allant de la prévention à la réponse aux incidents et gestion de crises cyber.

**Statut vérifié :** Labellisé — Offre « SOC 6E SENS » labellisée France Cybersecurity (catalogue 2026) — le label porte sur l'offre, pas sur l'ensemble de l'entreprise

**Source :** Catalogue France Cybersecurity · informations vérifiées le 14/10/2026

**Avis clients :** non vérifiés à ce jour

https://www.linkt.fr/

### DIGITALBERRY

BerryCert est une solution de gestion du cycle de vie des certificats (CLM) offrant un inventaire centralisé pour superviser en continu tous vos certificats numériques, dans une vue unifiée. Supervisez l'ensemble de vos certificats. Renouvelez en 1 clic et évitez les arrêts de service. Automatisez les tâches manuelles et économisez 50% du temps passé.

**Risque concerné :** Gestion des accès et authentification multifacteur

**Action corrective :** Déployer l'authentification multifacteur et revoir les droits d'accès.

**Pourquoi ce prestataire :** Votre diagnostic révèle 1 point(s) à renforcer sur « Gestion des accès et authentification multifacteur ». Statut : labellisé (Catalogue France Cybersecurity).

**Services :** BerryCert est une solution de gestion du cycle de vie des certificats (CLM) offrant un inventaire centralisé pour superviser en continu tous vos certificats numériques, dans une vue unifiée. Supervisez l'ensemble de vos certificats. Renouvelez en 1 clic et évitez les arrêts de service. Automatisez les tâches manuelles et économisez 50% du temps passé.

**Statut vérifié :** Labellisé — Offre « BERRYCERT » labellisée France Cybersecurity (catalogue 2026) — le label porte sur l'offre, pas sur l'ensemble de l'entreprise

**Source :** Catalogue France Cybersecurity · informations vérifiées le 14/10/2026

**Avis clients :** non vérifiés à ce jour

https://www.digitalberry.fr/

Un référencement, un label, une certification et une qualification ne sont pas équivalents. Ces informations ne constituent pas une garantie de qualité : comparez plusieurs offres et demandez des références avant de vous engager. Aucune de vos données n'est transmise à ces entreprises.