Synthèse et repères pour la PME:

Sécuriser et fiabiliser vos données

Par Catherine Torsy,
DSI à temps partagé pour PME

Les aspects à considérer:

1. **Confidentialité**
2. **Qualité et intégrité**
3. **Conformité**
4. **Sécurité des infrastructures et applications**
5. **Sensibilisation des salariés et partenaires**
6. **Disponibilité et résilience des systèmes**

Confidentialité

Objectif : **Limiter l’accès aux données sensibles et prévenir les fuites**
Responsable : IT (technique), Métiers (règles d’accès), Direction (politique)

🔍 Définir

- Identifier et classifier les informations: données publiques / sensibles / personnelles / confidentielles…
- Définir qui peut accéder à quoi, dans quel contexte, et pourquoi

🔧 Mettre en place

- Gestion des accès basée sur l’authentification des utilisateurs et la notion de rôle
- Accès limité au strict nécessaire (principe du moindre privilège)
- Désactivation rapide des comptes lors des départs
- Chiffrement des données au repos et en transit

Qualité et intégrité

Objectif : **Garantir des données fiables, cohérentes, non altérées**
Responsables : IT (contrôles techniques) + Métiers (règles de gestion)

🔍 Définir

- Règles de collecte, de validation et de mise à jour
- Principes de cohérence métier : formats, valeurs, relations entre données
- Stratégies d'historisation, sauvegarde et suppression

🔧 Exemples de mise en œuvre

- Validation de l'information saisie dans les interfaces utilisateurs (format, valeur, cohérence)
- Contrôle d'intégrité automatique dans les bases de données : ex. vérifier qu'une facture a un client valide

La qualité est essentielle pour ensuite valoriser les données:

- ✓ **Approfondir sa connaissance client et identifier de nouvelles opportunités**
- ✓ **Analyser et piloter l'activité commerciale**
- ✓ **Améliorer l'efficacité opérationnelle, réduire les coûts et augmenter la productivité**
- ✓ **…**

Conformité

Objectif : **Respecter les obligations légales (RGPD, données de santé, exigences sectorielles)**
Responsables : Métiers + DPO (cadre légal) + IT (implémentation technique)

📌 Principes fondamentaux du RGPD:

- **Collecte licite et transparente** : informer clairement les personnes
- **Minimisation** : ne collecter que ce qui est nécessaire
- **Limitation des finalités** : utiliser les données uniquement pour l'objectif prévu
- **Durée limitée** : supprimer quand ce n'est plus utile
- **Sécurité & confidentialité** : protéger contre les accès non autorisés
- **Responsabilité** : être capable de prouver la conformité

Sécurité des infrastructures et applications

Objectif : **Protéger les données à toutes les étapes : stockage, utilisation, circulation**
Responsables : IT + RSSI (définition de la politique de sécurité)

🔐 Sécurisation du stockage

But : protéger les données "au repos"
Risques couverts : vol, copie, accès non autorisé, perte
Exemples de mise en place :

- Chiffrement des bases et fichiers sensibles
- Droits d'accès stricts (principe du moindre privilège)
- Stockage isolé pour les données critiques

⚙️ Sécurisation des traitements

But : s'assurer que seuls les traitements autorisés peuvent être effectués
Risques couverts : fraude, accès détourné, manipulation illégitime
Exemples de mise en place :

- Contrôles d'accès applicatifs (permissions, rôles)
- Traçabilité via des logs (conserver des preuves, comprendre un incident)

🌐 Protection des données en transit

But : empêcher l'interception et le vol de données
Exemples de mise en place :

- Chiffrement systématique (TLS/HTTPS)
- VPN pour l'accès distant ou le télétravail

🖧 Séparation & segmentation des environnements

But : limiter la propagation d'une attaque et cloisonner les usages
Exemples de mise en place :

- Réseaux séparés et Environnements isolés
- Pare-feu et règles de filtrage

Implication des salariés et partenaires

Sensibiliser les employés

- Aux bonnes pratiques : mots de passe, phishing, manipulation de données
- Aux risques : perte de matériel, partage inapproprié

Encadrer les prestataires

- Par un accord de confidentialité
- Par une clause de conformité au RGPD dans le contrat
- En s'assurant d’un niveau de sécurité adapté
- En limitant les accès accordés (uniquement ceux nécessaires à la mission)

Disponibilité et résilience

Objectif : **Garder les données et systèmes accessibles. Permet à l'entreprise de fonctionner même en crise**
Responsable : Informatique (IT)

Mesures courantes :

Redondance

- Serveurs doublés, liens internet multiples, stockage dupliqué
- Si un composant tombe, un autre prend le relais automatiquement

Sauvegardes fiables

- Sauvegardes régulières, chiffrées, hors ligne
- Test de restauration obligatoire

Segmentation et isolation

- Un problème dans une zone du réseau ne doit pas contaminer tout le reste

Monitoring et alertes

- Détecter les anomalies assez tôt pour agir avant que la situation n'empire

PCA / PRA

- **PCA (Plan de Continuité d'Activité) :** maintenir l'activité malgré l'incident
- **PRA (Plan de Reprise d'Activité) :** reconstruire et redémarrer le SI après un sinistre

Gestion de crise

- Organisation prête à réagir : rôles définis, communication, processus

Des interrogations? Un projet à l’étude?

👉 Parlons-en!

Nous vous proposons une **consultation gratuite et sans engagement**, pour comprendre et évaluer votre besoin en accompagnement

Pour nous contacter:

contact@torsyconseil.fr

09.53.28.42.87

https://torsyconseil.fr/