RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

DONNÉES ET TRAITEMENTS SENSIBLES

Des données ou des traitements sont dits sensibles si leur compromission, leur perte ou leur altération peut sérieusement entraver la capacité de l'entité à atteindre ses objectifs, voire à exister. L'identification de ces éléments sensibles est indispensable pour orienter la stratégie de sécurité de l'information, et donc les protéger efficacement.

Ce document fournit une méthode d'évaluation simple et applicable à tout type d'entité, petite entreprise, multinationale, organisation gouvernementale ou association pour protéger ses données au juste niveau.

Il est à noter que les mesures de sécurisation spécifiques aux informations classifiées (Secret et Très secret) au sens de l'IGI 1300 ne sont pas couvertes dans les recommandations.

1/ DÉFINIR DES NIVEAUX DE SENSIBILITÉ

→ **Établir une échelle d'impact homogène pour toute l'entité,** permettant d'évaluer les conséquences possibles d'une compromission des données. Cette échelle peut s'inspirer du modèle ci-dessous, ou se baser sur les besoins de sécurité (disponibilité, intégrité, confidentialité…) – cette alternative est cependant moins intuitive pour les métiers.

→ **Définir des niveaux de sensibilité des données**, par exemple :

> non sensible (niveau 1) : impacts mineurs uniquement ;

> sensible : au moins un impact significatif (niveau 2) ou grave (niveau 3) ;

> très sensible : pouvant avoir un impact critique (niveau 4). Ce niveau comprend notamment les informations protégées par la mention Diffusion Restreinte (DR).

Impact	Humain	Financier	Juridique	Opérationnel	Image
Mineur	Atteinte physique ou psychique mineure	Pas de perte	Avertissement	Pas de perturbation	Couverture médiatique locale limitée
Significatif	Atteinte physique ou psychique modérée	Perte inférieure à X	Règlement à l'amiable	Perturbation inférieure à T heures/jours	Couverture médiatique régionale, impact sur la réputation locale
Grave	Atteinte physique ou psychique grave mais réversible	Perte entre X et Y	Responsabilité civile de l'entité	Perturbation entre T et U heures/jours	Couverture médiatique nationale, perte de confiance des parties prenantes
Critique	Atteinte physique ou psychique irréversible pouvant aller jusqu'au décès	Perte supérieure à Y	Responsabilité pénale individuelle d'un dirigeant de l'entité	Perturbation supérieure à U heures/jours	Couverture médiatique internationale, perte majeure de parts de marché

V1.0 (03/25)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

2/ IDENTIFIER ET CATÉGORISER

→ **Réaliser un inventaire macroscopique des données et des traitements de l'entité, sans se limiter aux éléments sensibles.**

→ **Catégoriser les données et traitements sensibles par division/direction et par contexte d'utilisation** (test, production, contrôle interne réglementaire, etc.), par exemple :

> données financières ;

> données commerciales et propriété intellectuelle ;

> données soumises à des réglementations ;

> données liées au fonctionnement du système d'information (journaux, adressage IP, schémas d'architecture).

→ **Identifier la/les source(s) et le(s) responsable(s)** de chaque catégorie de données et de traitements.

→ **Évaluer le niveau de sensibilité des catégories de données :**

> le RSSI doit questionner les besoins exprimés par le métier afin d'éviter une sous-évaluation ou une surévaluation ;

> l'évaluation doit être validée par les décideurs ;

> cette évaluation par catégorie est préférable à une évaluation par donnée en raison des contraintes de temps et de disponibilité des décideurs.

→ **Élever, si nécessaire, le niveau de sensibilité lors d'accumulation ou d'agrégation de données** (ex : un dépôt contenant de nombreuses données de niveau 2 pourra être réévalué au niveau 3).

→ **Inclure des revues régulières dans le processus d'évaluation**, la sensibilité évoluant dans le temps et en fonction des contextes.

3/ ANTICIPER ET PROTÉGER

→ **Définir les exigences de sécurité à appliquer aux SI**, en fonction du niveau de sensibilité des données qu'ils traitent :

> pour chaque catégorie et niveau, identifier les besoins de sécurité (disponibilité, intégrité, confidentialité…) dont les défaillances sont les plus susceptibles d'être à l'origine des impacts redoutés. Par exemple, si un impact opérationnel critique est surtout causé par l'indisponibilité d'une catégorie de SI, le besoin de disponibilité est prépondérant ;

> en fonction des besoins de sécurité ainsi définis, appliquer des mesures *ad hoc*. Pour répondre à un besoin de disponibilité, on pourra par exemple exiger un plan de continuité d'activité (PCA) ;

> pour certains niveaux (ex. : les données DR), des exigences réglementaires peuvent s'appliquer.

→ **Cadrer les conditions d'interconnexion entre les niveaux de sensibilité**, dont le non sensible.

→ **Prioriser les travaux de sécurisation en fonction de critères simples** tels que l'exposition, évaluée selon :

> le nombre et le type de personnes (interne, prestataire, partenaire, public) pouvant accéder à la donnée ;

> le nombre et le niveau de maitrise des interfaces permettant d'accéder à la donnée (accès physique, accès logique, réseau tiers).