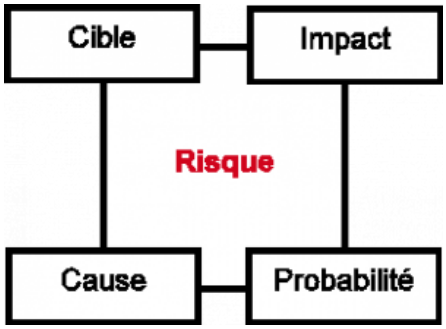
# Évaluer le besoin de sécurité pour mes données

***Une donnée, au sens informatique, est une représentation de l'information. Sa valeur provient à la fois de son coût d'acquisition (interviews, campagnes de mesure…) et de la plus-value qu'elle apporte en terme de connaissance. Sa divulgation, sa perte ou sa corruption peuvent entraîner des dommages financiers, des pertes d'image, des engagements de la responsabilité de l'Institut, voire des désorganisations ou des retards dans le travail des équipes. Mettre en place un système d'informations induit un risque, qui doit être maîtrisé.***

## Le risque informatique

### Qu'est-ce que le risque ?




Le risque peut être défini comme la conjonction entre :

- une cause, une menace, un événement ;
- une occurrence, une probabilité ou une vraisemblance ;
- une cible ;
- un impact, une gravité ou une conséquence.

### Comment estimer le risque ?

#### *La cible*

C'est le système d'informations considéré, par exemple un jeu de données, ou une application et ses données associées. Le plan de gestion de données permet de la définir précisément.

#### *L'impact*

Il s'évalue pour trois critères :

- la confidentialité : qui peut accéder à l'information ?
- L'intégrité : l'information peut-elle être perdue ou modifiée sans dommage ?
- La disponibilité : le système d'informations peut-il ne pas être opérationnel pendant un certain délai ?

Ces critères sont notés selon une échelle :

**En savoir plus**

Homologation

Les systèmes d'informations doivent être homologués avant leur mise en route opérationnelle. Le Comité de Sécurité des Systèmes d'Information (CSSI) valide l'étude de sécurité et les mesures de protection mises en place. Les informaticiens des centres peuvent vous aider à mener cette démarche.

Recommandations

Au démarrage d'un projet, élaborez un plan de gestion des données, et réalisez en même temps une étude de sécurité (les formulaires sont disponibles dans le référentiel documentaire d'Irstea).
Faites-vous aider par les informaticiens du Centre. Ils disposent des connaissances techniques nécessaires pour répondre aux interrogations que vous pourriez vous poser. Ils vous aideront également à déposer votre projet pour qu'il puisse être instruit par le responsable de la sécurité des systèmes d'information (RSSI) et validé par le CSSI.

Guide pratique pour la gestion des données de la recherche

| Critère/niveau | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| Confidentialité | Public : accès à tous | Limité : accessible au personnel et aux partenaires | Réservé : accessible uniquement aux personnes impliquées | Privé : accessible uniquement aux personnes identifiées |
| Intégrité | Altérable : l'information peut être reconstituée facilement (calculs, p.e.) | Détectable : il est possible de revenir à une solution saine à partir d'une sauvegarde | Maîtrisé : l'information ne peut être perdue, des mécanismes de réplication temps réel sont nécessaires | Intègre : l'information est signée par un mécanisme de chiffrement |
| Disponibilité | Faible : indisponibilité possible > 72 heures | Importante : disponible dans les 3 jours | Critique : disponible dans les 24 heures | Vitale : disponible dans les 4 heures |

En cas de défaillance, l'impact va être évalué selon 4 axes :

- le fonctionnement interne : désorganisation, retard…
- le coût financier, soit direct, soit indirect (frais judiciaires, communication, perte de contrats de recherche…) ;
- la responsabilité (plaintes d'usagers, civile, pénale…) ;
- l'atteinte à l'image.

Là encore, une échelle à 4 niveaux a été élaborée :

| Nature/impact | 1. Limité | 2. Important | 3. Grave | 4. Critique |
|---|---|---|---|---|
| Fonctionnement interne | Perturbation limitée | Perturbation significative | Désorganisation très importante | Désorganisation durable |
| Pertes financières | Non significatif | Pertes < 50 K€ | Pertes < 200 K€ | Pertes > 200 K€ |
| Responsabilité | Plaintes d'usager pour dysfonctionnement | Recours pouvant annuler une procédure | Plainte au civil | Plainte au pénal |
| Atteinte à l'image | Impact limité | Altération significative | Altération très importante | Altération définitive |

### *Les menaces*

En informatique, elles sont très variées et évoluent très vite. Les informaticiens s'appuient en général sur des référentiels de bonnes pratiques pour sécuriser les systèmes.

### *La probabilité*

Pour les attaques informatiques, la probabilité s'évalue très mal, et uniquement en fonction de la valeur des informations. Ainsi, on distingue trois types d'attaques :

- les attaques menées au hasard ;
- les attaques ciblées ;
- les attaques concertées, qui nécessitent un travail de préparation important, et qui visent des informations à haute valeur ajoutée.

Dans le cadre de l'établissement des plans de continuité d'activités, d'autres incidents sont évalués : incendie, inondation, mouvements sociaux… Ils sont réalisés site par site et prennent en compte en général 2 facteurs :

- la durée maximale d'indisponibilité admissible, c'est à dire le temps maximum de remise en état du système d'informations concerné avant que l'impact atteigne le niveau 2 ;
- la perte de données maximale admissible, c'est à dire les informations qu'il est possible de perdre avant que l'impact s'en fasse sentir (ressaisie à partir d'une sauvegarde, par exemple).

## Comment traiter le risque ?

L'objectif est de rendre le risque acceptable pour Irstea. 4 approches sont en général proposées :

- l'acceptation, quand l'impact est négligeable ou la probabilité nulle ;
- la diminution, en prenant des mesures adaptées (sauvegardes, renforcement des protections...) ;
- le transfert, par exemple en externalisant un site web critique ;
- le refus, en abandonnant le projet au vu des risques qu'il fait prendre.