

Gestion du risque

Identification des
risques et définition
des mesures de
sécurité

CONFIDENTIAL
Sylvain DENIS

Sommaire

- Concepts et définitions
- Gestion de la sécurité de l'information
- Évaluation des risques

Buts

- Être en conformité avec la Commission de la Vie Privée



- Être en conformité avec l'utilisation des logiciels en relation avec SIEL

Concepts et définition 1/6

- Actif : tout élément du système d'information, ayant de la valeur pour l'organisation
 - Exemples :
 - Locaux et installations techniques
 - Matériel informatique
 - Infrastructure télécom
 - Logiciels
 - Base de données
 - Documentation
 - Personnel

Concepts et définition 2/6

- Attributs de sécurité
 - **Disponibilité** : actifs utilisables et accessibles
 - **Intégrité** : informations transmises / traitées / conservées sans erreur
 - **Confidentialité** : informations accessibles seulement aux personnes autorisées

Concepts et définition 3/6

- Autres attributs de sécurité

Authenticité / Traçabilité / Irrévocabilité / Fiabilité

Concepts et définition 4/6

- Menace

- Cause pouvant affecter la sécurité d'un actif
- Caractéristiques :

- Origine :

- Naturelle : incendie, inondation, ...
 - Humaine :
Accidentelle : erreurs (saisie, bug,...)
Délibérée : fraude, virus, intrusion,...



Probabilité

Opportunité,
Motivation,
Faisabilité

- Impact sur l'organisation

Concepts et définition 5/6

- Vulnérabilité
 - Point faible permettant à une menace de porter atteinte à la sécurité d'un actif

- Exemple :

Détection/extinction d'incendie absente ou inefficace

Test insuffisant des logiciels

Personnel insuffisamment formé

Antivirus non mis à jour

Copies de sauvegarde absentes ou non testées

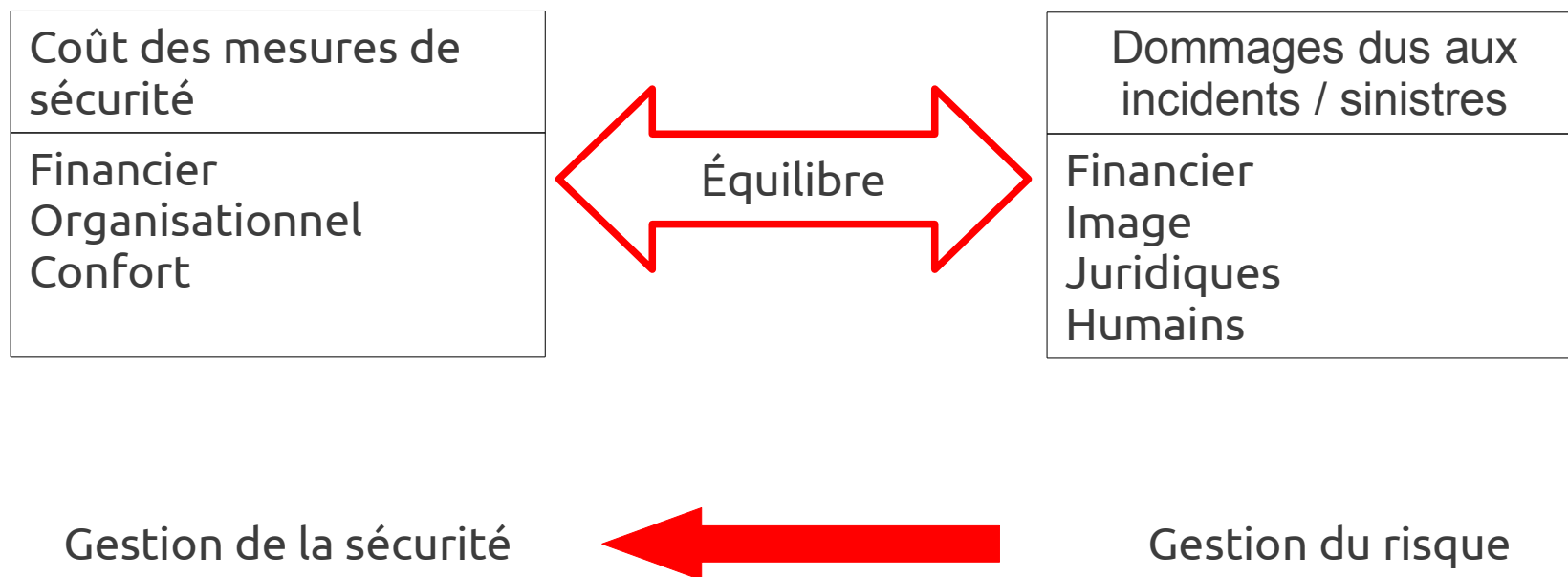
Plan « catastrophe » absent ou non testé

Concepts et définition 6/6

- Risque
 - Probabilité qu'une menace exploite une vulnérabilité pour affecter un actif du système d'information
 - Impact sur les actifs : disponibilité, intégrité, confidentialité, ...
 - sur l'organisation : perte financière, image, ...
 - Probabilité / fréquence / opportunité

Gestion de la sécurité de l'information 1/3

- Objectif fondamental



Gestion de la sécurité de l'information 2/3

- Processus continu ———▶ roue de Deming

« PDCA »

4 - *[Act]*
Rectifier
Améliorer

1 - *[Plan]*
Identifier / évaluer
- risques
- actions adéquates

3 - *[Check]*
Mesurer / évaluer
les résultats

2 - *[Do]*
Réaliser les actions
Informer / éduquer



Gestion de la sécurité de l'information 3/3

- Facteurs critiques de succès
 - Support de la direction
 - Stratégie : définition centrale / mise en œuvre locale
 - Impacts des risques pour l'organisation
 - Sensibilisation / formation (personnel, ...)
 - Méthodes
 - Outils

Évaluation des risques 1/4

- Méthode EBIOS :

*Expression des **B**esoins et **I**dentification des **O**bjectifs de **S**écurité*

- Simple
- Adaptée au contexte d'une école
- Autant qualitative que quantitative

Évaluation des risques 2/4

- Étapes :
 - Déterminer la métrique
 - Identifier les actifs
 - Évaluation des risques actif par actif
 - Identifier les risques les plus importants
 - Déterminer les mesures de sécurité
 - Ré-évaluation des risques après mesures

Évaluation des risques 3/4

- Déterminer la métrique

GRAVITÉ	Nature des conséquences			
	Perte Financière (F)	Juridique Judiciaire (J)	Image (I)	Social et humain (S)
1	< 1000 €	Avertissements	Plaintes occasionnelles	Divulgarion de données personnelles
2	1000 – 10 000 €	Sanctions internes	Critiques occasionnelles dans les médias	Divulgations de données personnelles sensibles
3	10 000 – 100 000 €	Action en justice	Critiques graves dans les médias	Atteinte sérieuse à l'intégrité ou à la réputation
4	> 100 000 €	Condamnation de l'entité	Altération définitive	Perte de vie humaine Atteinte grave à la réputation

Évaluation des risques 4/4

- Identifier les actifs :
 - Hardware (serveur et réseau local)
 - Hardware PC
 - Software – Proeco (autre)
 - Software – Web-service
 - DB données élèves
 - Documents papier
 - Personnel
 - Locaux

Sylvain DENIS - 0499 219 802

sylvain.denis@felsi.eu

