



# Management de la sécurité dans un contexte d'infogérance

J-François MAHE  
Gie GIPS

## Mise en place d'une convention de service

Traitant les points suivants :

- L'organisation de la sécurité du SI
- La gestion des biens
- La gestion des communications et de l'exploitation
- La gestion des incidents
- La gestion des accès logiques
- L'acquisition, le développement et la maintenance des systèmes d'information
- La gestion du Plan de Reprise d'Activité Informatique

## L'organisation de la sécurité du SI

- Création d'une instance de pilotage
- Définition des rôles et responsabilités
- Traitement des risques liés aux relations avec les tiers
- Protection des accès physiques aux zones d'exploitation des serveurs
- Tableaux de bord

# La gestion des biens

- Un inventaire de toutes les ressources du système d'information est réalisé comprenant :
  - numéro de série
  - Description du bien
  - Localisation
  - Liste des composants
  - Version
  - Date de mise en service
  - Propriétaire
  - Pour les progiciels : nom de l'éditeur et le nombre de licences

## La gestion des communications et de l'exploitation

- L'administration des systèmes
  - Les droits d'administration
  - Les comptes administrateurs
- Les mises en production
- Les évolution du SI
- La veille technologique
- Les sauvegardes – les restaurations – l'archivage
- La traçabilité des systèmes

## La gestion des incidents

- Établissement d'une typologie
- MEO d'une procédure d'escalade
- Définition des responsabilités
- Engagement de délais pour la résolution des incidents

## La gestion des accès logiques

- La gestion des habilitations
  - Définition des délais des demandes (création, déblocage, modification, blocage, suppression)
  - Traçage des opérations réalisées
- La sécurité des mots de passe
  - Définition de règles pour assurer la sécurité des mots de passe

# Acquisition, développement et maintenance des SI

- Mise en place de Plan d'assurance sécurité
  - Couvrant l'ensemble des mesures et dispositifs de sécurité relatifs à un projet (pour les phases d'étude, de développement et la phase d'exploitation)
  - Traçage des opérations réalisées
- MEO de procédures de développement
  - Pour la séparation des tâches entre spécifications détaillées, conception, test unitaires et intégration
- MEO de procédures de gestion et de maintenance
  - Permettant de garantir la sécurité des programmes (modification)
- MEO de procédures de maintenance à chaud en environnement de production

# Gestion du Plan de Reprise d'Activité Informatique

- Mise en place d'une solution de secours
  - Testée au moins deux fois par an
  - Avec la participation des métiers
  - Compte rendu établi et diffusé au COMEX

# Sécurité des données

Selon quatre axes :

- Logique
- Physique
- Protection virale
- Réseau

## Sécurité logique

Concerne la sauvegarde des données stockées sur les serveurs, à l'exclusion des postes de travail sous la responsabilité des utilisateurs

- L'organisation des sauvegardes permet d'assurer des rotations selon des cycles quotidiens, hebdomadaires ou mensuels avec stockage hors site.
- Les demandes de restauration de données s'effectuent par une demande au SVP Informatique

## Sécurité physique

La sécurité physique est assurée par des mesures de prévention et l'application d'un plan de secours sous la responsabilité du responsable sécurité;

### Mesures de prévention

- Un contrôle des accès aux zones sensibles
- Des détections incendies et intrusions
- Le plan de secours est testé au moins deux fois par an

## Sécurité « protection virale »

Les risques viraux sont importants. Un ensemble de moyens a été mis en oeuvre pour détecter les virus s'introduisant dans le système d'information.

Une protection antivirale permanente est active sur les postes de travail, les serveurs et les messages en provenance d'Internet (Firewall).

Une gestion préventive des risques permet également de minimiser les risques de contamination (sensibilisation des utilisateurs, mise à jour des failles de sécurité, surveillance des sites d'alerte, ...).

## Sécurité réseau

L'accès au réseau est restreint par l'utilisation d'outils de contrôle d'accès, d'analyse du trafic et d'identification forte des utilisateurs nomades.

Un outil de filtrage des accès Internet est en place pour réduire les risques potentiels et interdire l'accès aux sites reprehensible par la loi.

## Les tableaux de bord

Des tableaux de bord ont été mis en place avec deux niveaux d'indicateurs

- Les indicateurs stratégiques
- Les indicateurs opérationnels pour le pilotage de la sécurité au quotidien

## Les indicateurs stratégiques

- Suivi du pourcentage de mise en oeuvre du règlement minimum sécurité des fédérations AGIRC/ARRCO
- Audit de conformité
- Continuité – fréquence de réussite des tests du PRAI
- Taux de personnes sensibilisées à sécurité
- Taux de prestataires externes sur les postes sensibles
- Nombre de composants matériels ou applicatifs non conformes, non maintenus
- Tenue des Comités Permanents Sécurité

## Les indicateurs opérationnels

- Nombre de vols et pertes – PC fixes
- Nombre de vols et pertes – terminaux mobiles
- Perte de mots de passe
- Pourcentage d'accès non autorisés sur les applications sensibles
- Continuité – taux de vulnérabilité
- Attaques en environnement de messagerie
- Attaques en environnement Intranet
- Attaques en environnement Internet
- Disponibilité des applications critiques
- Mise à jour des anti-virus et patches
- Inventaire et évolution du nombre d'identifiant génériques
- Pourcentage des application en production ayant un dossier sécurité formalisé
- Tenue des réunions du comité de sécurité opérationnel
- Nombre de correspondants SSI

# Fréquence des collectes

Indicateurs stratégiques : annuelle

Indicateurs opérationnels : trimestrielle