Présentation – Gestion parc informatique

I. Quels sont les contours d'une gestion de parc informatique ?

1. Définition générale

Une infrastructure informatique comprend les composants nécessaires au fonctionnement et à la gestion des environnements informatiques d'entreprise. Il est possible de déployer une infrastructure informatique au sein d'un système de cloud computing ou des installations de l'entreprise.

Une infrastructure informatique comprend des composants matériels, logiciels et réseau, un système d'exploitation ainsi qu'un système de stockage des données qui sont utilisés pour fournir des services et solutions informatiques. Ces produits peuvent être des applications logicielles téléchargeables qui s'exécutent sur les ressources informatiques existantes, ou des solutions en ligne proposées par des prestataires de services.

2. Composantes matérielles

Le matériel comprend les serveurs, les datacenters, les ordinateurs, les routeurs, les commutateurs et d'autres équipements.

Les installations qui hébergent, refroidissent et alimentent un datacenter peuvent également être considérées comme des composants matériels de l'infrastructure.

3. Composantes logicielles

Les logiciels font référence aux applications utilisées par l'entreprise, telles que les serveurs web, les systèmes de gestion de contenu et le système d'exploitation, par exemple Linux. Le système d'exploitation est responsable de la gestion des ressources du système et du matériel. C'est lui qui établit les connexions entre tous les logiciels et les ressources physiques requises pour l'exécution des différentes tâches.

Source : Redhat

4. Gestion des utilisateurs

- Tout commence par l'**utilisation d'identifiants uniques et propres à chaque individu**, qu'ils soient utilisateurs de votre application ou collaborateurs dans le développement.
- Veillez à **imposer une authentification** avant tout accès à des données personnelles, conformément aux recommandations de la CNIL.

- Pour vous assurer que chaque personne (utilisateur ou collaborateur) ne puisse accéder qu'**aux données dont il a effectivement besoin**, votre système doit prévoir dès la conception des **politiques de gestion d'accès aux données différenciées** (lecture, écriture, suppression, etc.) suivant les personnes et les besoins. Un mécanisme de gestion des profils utilisateurs global vous permettra de regrouper différents droits en fonction d'un rôle exercé par un groupe d'utilisateurs au sein de l'application.
- La gestion des profils utilisateurs peut s'accompagner d'**un système de journalisation** (c'est-à-dire un enregistrement dans des « fichiers journaux » ou « logs ») **afin de tracer les activités, et détecter toutes anomalies ou évènements liés à la sécurité**, comme les accès frauduleux et les utilisations abusives de données personnelles. L'utilisation de ces dispositifs ne doit en aucun cas servir à d'autres fins que celles de garantir le bon usage du système informatique et les *logs* ne doivent pas être conservés plus longtemps que nécessaire. Ces systèmes de journalisation ne doivent pas amener à stocker des données au-delà de leur durée de conservation. De manière générale, une durée de six mois est adéquate.
- Vous pouvez également prévoir des audits de code ou des tests d'intrusion au sein de votre environnement de développement afin de vous **assurer de la robustesse de votre système de gestion des profils**.

Source : CNIL

5. Maintenance et support

- Inventaire matériel et logiciel

Même sans outils spécialisés, il est essentiel de tenir à jour un **inventaire manuel structuré** :

Objectifs :

- Suivre l'ensemble des équipements (PC, imprimantes, écrans, périphériques…)
- Identifier chaque poste pour savoir à qui il est affecté
- Contrôler les versions logicielles installées pour anticiper les risques de compatibilité ou de sécurité

Bonnes pratiques :

- Créer une **base de données ou un tableau (tableur)** recensant :
  - L'identifiant du matériel (n° de série, modèle, affectation)
  - Le système d'exploitation et les logiciels installés
  - La date d'installation / mise en service
  - La durée de garantie
- Mettre à jour l'inventaire **à chaque modification** (ajout, remplacement, retrait)
- Associer les informations utilisateurs (poste attribué, service, contact)

- Interventions techniques (curatives et préventives)

Interventions curatives :

- Vise à réparer une panne ou résoudre un dysfonctionnement
- Exemples :
    - Réinstallation de logiciel suite à un crash
    - Changement de disque dur défectueux
    - Suppression d'un virus identifié

Interventions préventives :

- Vise à anticiper ou éviter les incidents
- Exemples :
    - Nettoyage interne des postes (poussière, connectique)
    - Vérification régulière des logs système
    - Test de sauvegarde/restauration
    - Contrôle de l'espace disque et de la température

Bonnes pratiques (selon recommandations de l'ANSSI) :

- Documenter chaque intervention (date, nature, matériel concerné, personne en charge)
- Planifier des vérifications trimestrielles ou semestrielles
- Sensibiliser les utilisateurs à signaler les anomalies dès leur apparition

- Mise à jour des outils et correctifs de sécurité

Pourquoi c'est crucial :

- Les failles connues sont la **porte d'entrée principale des cyberattaques**
- Les éditeurs publient des **correctifs de sécurité critiques** que l'on doit appliquer sans attendre

Sans outil dédié, il est recommandé de :

- Paramétrer les postes pour activer les **mises à jour automatiques** (système d'exploitation, navigateur, antivirus, etc.)
- Effectuer un **suivi manuel mensuel** : vérifier les versions installées via les paramètres
- Lire les **bulletins de sécurité officiels** (ANSSI, CERT-FR) pour suivre les vulnérabilités critiques
- Établir un calendrier de contrôle à date fixe (ex. le premier lundi de chaque mois)

En cas d'impossibilité d'appliquer une mise à jour :

- Consigner le poste comme « non conforme » dans l'inventaire
- L'isoler temporairement du réseau si la vulnérabilité est critique
- Chercher une solution alternative (mise à jour partielle, limitation d'accès…)

Source : Fleet, ANSSI, Ami-Gestion, EGSI

6. Cycle de vie des équipements

- **Acquisition** : l'achat ou la location du matériel
- **Déploiement** : l'installation et la configuration de l'équipement
- **Utilisation** : la période d'utilisation active par les collaborateurs
- **Maintenance** : les interventions régulières pour maintenir les performances
- **Fin de vie** : le moment où l'équipement n'est plus adapté aux besoins de l'entreprise

Source : Gost

7. Sécurité du parc

1. Structurer les mesures de sécurité

L'ANSSI recommande d'organiser la sécurité autour de **quatre piliers fondamentaux** :

- **Gouvernance** : stratégie, cartographie des systèmes, gestion des risques, sensibilisation des utilisateurs.
- **Protection** : cloisonnement réseau, gestion des accès, sécurité des données, mises à jour, sécurité physique.
- **Défense** : détection des incidents, supervision, réponse aux attaques.
- **Résilience** : sauvegardes, continuité d'activité, reprise après sinistre.

Objectif : réduire la surface d'attaque et renforcer la capacité de réaction face aux menaces.

Source : Cyber

2. Sécuriser les postes de travail

Les postes de travail sont des **points d'entrée critiques** dans le système d'information. La CNIL recommande :

- **Verrouillage automatique** des sessions après inactivité.
- **Pare-feu logiciel** et limitation des ports ouverts.
- **Antivirus à jour** et **mises à jour de sécurité appliquées rapidement**.
- **Droits utilisateurs limités** au strict nécessaire.
- **Sauvegarde centralisée** des données (éviter le stockage local).
- **Effacement sécurisé** des données avant réaffectation d'un poste.
- **Contrôle des supports amovibles** (désactivation de l'autorun, analyse antivirus).

Source : CNIL

3. Politique de sécurité du système d'information (PSSI)

La PSSI est un **document stratégique** qui encadre la sécurité du parc informatique. Elle définit :

- Les **objectifs de sécurité** : confidentialité, intégrité, disponibilité.
- Les **rôles et responsabilités** (RSSI, DSI, utilisateurs).
- La **gestion des risques** : identification, évaluation, traitement.
- Les **mesures techniques et organisationnelles** : contrôle d'accès, chiffrement, audit, surveillance.
- La **sensibilisation et la formation** des utilisateurs.
- La **conformité réglementaire** (RGPD, ISO 27001…).

Source : Cyber Management

En résumé

La sécurité du parc informatique repose sur :

- Une **vision stratégique claire** (PSSI)
- Une **organisation structurée** (gouvernance, défense, résilience)
- Des **mesures concrètes sur les postes de travail**
- Une **implication humaine** : sensibilisation, formation, responsabilité

Source : Cyber, CNIL, CSM

8. Suivi administratif et financier

1. Budgétisation du renouvellement

Objectif : anticiper les coûts liés au remplacement des équipements obsolètes ou en fin de vie.

Bonnes pratiques :

- Évaluer le **cycle de vie** des matériels (3 à 5 ans en moyenne pour les postes utilisateurs).
- Intégrer les coûts indirects : licences, maintenance, formation.
- Prioriser selon l'usage, la criticité et la vétusté.

Source : CNIL

2. Gestion des stocks

Objectif : assurer une traçabilité complète des équipements et logiciels.

Bonnes pratiques (selon ITIL) :

- Maintenir un **inventaire à jour** (matériel, logiciels, affectations).
- Suivre les mouvements (entrées/sorties, transferts, recyclage).
- Identifier chaque actif par un **numéro unique** (code-barres, QR code).

Source : ITIL, K Inventory (gestion stock ITIL)

3. Suivi des garanties, contrats de maintenance et licences

Objectif : éviter les pertes financières et les risques de non-conformité.

Bonnes pratiques :

- Centraliser les **dates de fin de garantie**, contrats de support, et renouvellements.
- Suivre les **licences logicielles** (quantité, durée, conformité).
- Mettre en place un **calendrier d'alertes** pour les échéances.

Source : Liscience

4. Reporting et tableaux de bord

Objectif : piloter efficacement le parc et appuyer les décisions stratégiques.

Bonnes pratiques :

- Définir des **indicateurs clés (KPI)** : taux de disponibilité, incidents, taux de renouvellement.
- Utiliser des **tableaux de bord dynamiques** pour suivre les performances.
- Réaliser des **reportings périodiques** (mensuels, trimestriels) pour la direction.

Source : Litiliste, Piedalies

9. Outils et méthodes associés

MDM (Mobile Device Management)

Permet de gérer à distance les appareils mobiles (smartphones, tablettes, PC portables) d'une organisation.

Fonctionnalités clés :

- Enrôlement et configuration automatique des appareils
- Application de politiques de sécurité (chiffrement, verrouillage, effacement à distance)

- Gestion des mises à jour et des applications
- Suivi de conformité et géolocalisation

Avantages :

- Sécurité renforcée des terminaux mobiles
- Réduction des risques liés au BYOD (Bring Your Own Device)
- Administration centralisée depuis une console web

Source : IBM

SCCM (System Center Configuration Manager)

Solution Microsoft pour la gestion centralisée des postes de travail, serveurs et logiciels.

Fonctionnalités clés :

- Déploiement automatisé de logiciels et de systèmes d'exploitation
- Gestion des correctifs de sécurité
- Inventaire matériel et logiciel
- Supervision des performances et conformité
- Contrôle à distance

Avantages :

- Administration à grande échelle (centaines à milliers de postes)
- Automatisation des tâches IT répétitives
- Intégration avec Microsoft Endpoint Manager

Source : Bemsp, IT Connect

Méthodes de structuration : ITIL & ISO 27001

ITIL (Information Technology Infrastructure Library)

Cadre de bonnes pratiques pour la gestion des services informatiques (ITSM).

Principes clés :

- Gestion du cycle de vie des services (conception, transition, exploitation)
- Amélioration continue
- Alignement des services IT sur les besoins métiers

ITIL 4 intègre désormais :

- L'agilité, DevOps, cloud computing

- Le concept de **Service Value System (SVS)**

Source : Eternal Network

ISO 27001

Norme internationale pour la mise en place d'un **Système de Management de la Sécurité de l'Information (SMSI)**.

Objectifs :

- Protéger la **confidentialité**, l'**intégrité** et la **disponibilité** des données
- Identifier les risques et mettre en œuvre des mesures de sécurité adaptées
- Structurer les responsabilités, les procédures et les contrôles

Avantages :

- Conformité réglementaire (ex : RGPD)
- Réduction des risques de cyberattaques
- Amélioration continue de la sécurité

Source : DataScientest

II. Que comprend-t-on de la gestion d'un parc informatique ?

1. Inventaire des ressources

1. Recensement des équipements matériels

L'inventaire matériel consiste à **identifier et documenter tous les équipements physiques** utilisés dans l'organisation : ordinateurs, imprimantes, serveurs, routeurs, périphériques, etc.

Un inventaire efficace doit inclure :

- Le type d'équipement (PC, imprimante, scanner…)
- Le numéro de série, la marque, le modèle
- L'utilisateur affecté et l'emplacement
- L'état du matériel et la date d'achat

Objectifs :

- Optimiser l'utilisation des ressources
- Planifier les remplacements
- Réduire les coûts liés aux doublons ou à l'obsolescence

Source : AMI - Gestion

2. Inventaire des logiciels installés, versions et licences

Il s'agit de **recenser tous les logiciels installés** sur les postes et serveurs, ainsi que leurs **versions et modalités de licence**.

Cela permet de :

- Suivre la conformité des licences (éviter les sanctions)
- Identifier les logiciels obsolètes ou non utilisés
- Planifier les mises à jour et rationaliser les coûts

Données à collecter :

- Nom du logiciel, version, éditeur
- Clé de licence, date d'achat, date d'expiration
- Nombre d'installations autorisées vs utilisées

Source : Manage Engine

3. Mise à jour régulière pour fiabiliser les données

Une base d'inventaire n'est utile que si elle est **tenue à jour**.

Cela implique :

- La suppression des doublons
- La correction des erreurs (ex. : affectation incorrecte)
- L'actualisation des données obsolètes (ex. : matériel remplacé)

Bonnes pratiques :

- Planifier des audits réguliers
- Mettre en place des alertes sur les dates de fin de garantie ou de licence
- Associer chaque ressource à un identifiant unique (code-barres, QR code)

Source : Echo Solution

2. Maintenance et support technique

1. Interventions curatives et préventives

Objectif : assurer le bon fonctionnement des équipements et limiter les interruptions de service.

Maintenance curative

- **Définition** : intervention après une panne ou un dysfonctionnement constaté.
- **Exemples** : remplacement de disque dur, réinstallation de logiciel, suppression de virus.
- **Avantage** : rétablir rapidement l'activité en cas d'incident.

Source : Nomadia, RS Online

Maintenance préventive

- **Définition** : actions planifiées pour éviter les pannes (nettoyage, vérification, test).
- **Exemples** : nettoyage interne, contrôle des logs, test de sauvegarde.
- **Avantage** : prolonge la durée de vie des équipements et réduit les coûts à long terme.

Source : Mainsim

2. Suivi des tickets d'incidents

Objectif : tracer, prioriser et résoudre les incidents signalés par les utilisateurs.

- Chaque incident est enregistré sous forme de **ticket** avec un identifiant unique.
- Le ticket suit un **cycle de vie** : ouverture → diagnostic → résolution → clôture.
- Permet une **traçabilité complète**, une meilleure réactivité et un suivi des performances (SLA).

Source : Efalia, InvGate

3. Garantie de disponibilité et continuité de service

Objectif : assurer que les services informatiques restent accessibles même en cas d'incident majeur.

- **Disponibilité** : capacité à fournir un service sans interruption (ex. : 99,9 % de disponibilité annuelle).
- **Continuité** : mise en place de plans de secours (PRA/PCA) pour maintenir l'activité en cas de sinistre.
- **Bonnes pratiques ITIL** : surveillance proactive, redondance, sauvegardes, tests réguliers.

Source : CeRFI, Exaegis

3. Sécurité des équipements et des données

1. Mise à jour des systèmes d'exploitation et antivirus

Les mises à jour régulières sont essentielles pour corriger les failles de sécurité exploitées par les cyberattaques.

- **Systèmes d'exploitation** : activer les mises à jour automatiques pour Windows, macOS, Linux, etc.
- **Antivirus** : maintenir à jour les bases de signatures (ex. : Microsoft Defender, Avast, Bitdefender…)
- **Microsoft recommande** de maintenir Defender à jour via les mises à jour de sécurité et de plateforme.
- Ces mises à jour incluent des correctifs critiques contre les malwares, ransomwares et exploits récents.

Source : Microsoft Learn

2. Sauvegarde régulière des données

Une sauvegarde efficace protège contre la perte de données due à une panne, un vol ou une attaque (ex. : ransomware).

- **CNIL** recommande la règle du **3-2-1** : 3 copies, sur 2 supports différents, dont 1 hors ligne.
- **ANSSI** insiste sur la nécessité de tester régulièrement les sauvegardes pour garantir leur restauration.
- Les sauvegardes doivent être **chiffrées**, **géographiquement séparées** et **déconnectées du réseau** après usage.

Source : CNIL, ANSSI

3. Contrôle des accès, verrouillage et chiffrement

Ces mesures protègent les données contre les accès non autorisés, internes ou externes.

- **Contrôle des accès** : gestion des droits selon les rôles (principe du moindre privilège)
- **Verrouillage automatique** des sessions après inactivité (recommandé par la CNIL)
- **Chiffrement des données sensibles** : sur les disques, les sauvegardes et les échanges réseau
- **France Num** rappelle que le chiffrement est une barrière efficace contre le vol ou la fuite de données

Source : France Num, ANSSI

4. Conformité réglementaire

RGPD : Confidentialité des données utilisateurs

Le **Règlement Général sur la Protection des Données (RGPD)** encadre le traitement des données personnelles au sein de l'Union européenne.

Principes clés :

- **Licéité, loyauté, transparence** : informer clairement les utilisateurs
- **Minimisation des données** : ne collecter que ce qui est strictement nécessaire
- **Sécurité** : garantir la confidentialité, l'intégrité et la disponibilité des données
- **Droits des personnes** : accès, rectification, effacement, portabilité

Source : CNIL, Leto Legal

Durée de conservation des logs & droit d'accès

Les **logs** (ou fichiers de journalisation) permettent de tracer les accès et actions sur les systèmes informatiques. Ils sont considérés comme des **données personnelles** lorsqu'ils identifient un utilisateur.

Recommandations CNIL :

- **Durée de conservation limitée** : en général **6 mois à 1 an**, jusqu'à **3 ans** si justifié
- **Finalité claire** : uniquement pour la sécurité, pas pour surveiller les employés
- **Droit d'accès** : les personnes concernées peuvent demander à consulter les données les concernant

Source : CNIL, CIO Online

ISO 27001 et autres référentiels

La norme **ISO/IEC 27001** est un **cadre international** pour la mise en place d'un **Système de Management de la Sécurité de l'Information (SMSI)**.

Objectifs :

- Identifier les **risques liés à la sécurité de l'information**
- Définir des **mesures de protection** (contrôles techniques, organisationnels, physiques)
- Assurer la **conformité réglementaire** (RGPD, NIS2, etc.)
- Améliorer la **résilience** face aux cybermenaces

Source : Microsoft Learn, MakeItSafe, June Factory

Résumé très synthétique

I. Quels sont les contours d'une gestion de parc informatique ?

1. Définition & infrastructure

- Environnement technique regroupant **matériel, logiciel, réseau, stockage et OS**
- Hébergé localement ou dans le cloud (RedHat)

2. Composants essentiels

- **Matériel** : serveurs, postes, périphériques, datacenters
- **Logiciel** : systèmes d'exploitation, outils métier, CMS…

3. Gestion des utilisateurs (CNIL)

- Comptes uniques, droits différenciés
- Authentification obligatoire
- Journalisation des accès et contrôles de sécurité

4. Maintenance & support (ANSSI)

- **Inventaire structuré** (matériel et logiciel)
- **Interventions curatives** (pannes) et **préventives** (vérifications, nettoyages)
- Suivi régulier, documentation, sensibilisation

5. Mises à jour & sécurité

- Mises à jour automatiques
- Veille sur vulnérabilités (CERT-FR, ANSSI)
- Isoler les postes non conformes si nécessaire

6. Cycle de vie des équipements (Gost)

1. **Acquisition** → Achat/location
2. **Déploiement** → Installation, configuration
3. **Utilisation** → Affectation à un collaborateur
4. **Maintenance** → Suivi & réparation
5. **Fin de vie** → Recyclage ou remplacement

7. Sécurité du parc

- **Structure ANSSI** : gouvernance, protection, défense, résilience
- **Postes** : verrouillage, antivirus, sauvegardes, droits limités (CNIL)
- **PSSI** : cadre stratégique avec rôles, conformité RGPD (Cyber)

8. Suivi administratif et financier

- **Budget** : anticiper renouvellement, formations
- **Stocks** : traçabilité, affectation
- **Garanties & licences** : alertes de fin, conformité
- **Reporting** : indicateurs (KPI), tableaux de bord direction

9. Outils & méthodes

- **MDM** : gestion centralisée des terminaux mobiles
- **SCCM** : déploiement d'OS, correctifs, inventaire poste à distance
- **ITIL** : gestion IT orientée service
- **ISO 27001** : sécurité structurée, gestion des risques (SMSI)

II. Que comprend-t-on de la gestion d'un parc informatique ?

1. Inventaire des ressources

- Recensement des matériels (type, modèle, utilisateur, état)
- Suivi des logiciels (versions, licences, conformité)
- Actualisation régulière : audit, identifiants uniques

2. Maintenance & support

- **Curatif** : pannes, réinstallations, réparation
- **Préventif** : nettoyage, sauvegardes, logs
- Suivi via tickets → traçabilité + SLA
- Garantir disponibilité & continuité (PCA/PRA)

3. Sécurité des équipements & données

- Mises à jour OS/antivirus systématiques
- Sauvegardes 3-2-1 testées et sécurisées (CNIL/ANSSI)
- Contrôle des accès, verrouillage, chiffrement

4. Conformité réglementaire

- **RGPD** : transparence, droits, sécurité
- **Logs** : conservation limitée, finalité claire
- **ISO 27001** : cadre structurant & gestion des risques