Compte Rendu Détaillé du Projet : Audit et Sécurisation du Parc Informatique

Date de rendu : 04/04/2025

Durée du projet

**1. Contexte et Objectifs**

Objectif principal : Réaliser un audit complet du parc informatique, sécuriser les ressources, et garantir la conformité aux normes RGPD et ISO 27001, tout en mettant en place des mécanismes de sauvegarde et de continuité d’activité.

Livrables attendus :

- Inventaire détaillé du matériel, logiciels, et services cloud.

- Rapport de conformité RGPD/ISO 27001 avec plan d’action correctif.

- Matrice des habilitations (AD/LDAP) pour la gestion des accès.

- Plan de sauvegarde automatisé (Veeam/Bacula) et documentation des procédures de continuité.

Contraintes :

- Respect des délais légaux pour la conformité RGPD.

- Minimisation des interruptions de service pendant l’audit.

**2. Méthodologie et Organisation**

- Rôles de l’équipe :

- Auditeur en chef : Pilotage de l’audit, coordination des équipes.

- Responsable conformité : Vérification des normes RGPD/ISO 27001.

- Administrateur système : Gestion AD/LDAP, déploiement des sauvegardes.

- Documentaliste : Rédaction des procédures et rapports finaux.

Outils utilisés :

- Lansweeper/GLPI : Inventaire automatisé des actifs matériels et logiciels.

- Microsoft Excel : Matrice des habilitations et suivi des corrections.

- Veeam Backup & Replication : Sauvegardes automatisées et chiffrées.

- ISO 27001 Toolkit : Checklist pour l’audit de sécurité.

**3. Phases du Projet**

Phase 1 : Recensement des ressources (2 semaines)

- Inventaire matériel :

- Scan réseau via Lansweeper pour identifier serveurs, postes clients, imprimantes.

- Liste des équipements obsolètes (ex: Windows 7, matériel hors garantie).

- Inventaire logiciel :

- Détection des logiciels non licenciés ou non conformes (ex: versions piratées).

- Cartographie des services cloud (Microsoft 365, AWS, Google Workspace).

- Résultats :

- 150 postes clients, 20 serveurs, 5 services cloud recensés.

- 12 logiciels non licenciés identifiés.

Phase 2 : Mise en conformité RGPD/ISO 27001 (3 semaines)

- Audit RGPD :

- Identification des données personnelles stockées (ex: fichiers RH, clients).

- Vérification des clauses de consentement et des politiques de confidentialité.

- Audit ISO 27001 :

- Évaluation des contrôles de sécurité (ex: contrôle d’accès physique, chiffrement).

- Écart détecté : Absence de politique de mot de passe complexe.

- Actions correctives :

- Suppression des données inutiles (20 Go de données obsolètes nettoyés).

- Mise en place d’une politique de mot de passe (12 caractères, changement tous les 90 jours).

Phase 3 : Création de la matrice des habilitations (1 semaine)

- Structuration AD/LDAP :

- Création de groupes hiérarchisés (ex: \*GRH\_AccèsComplet\*, \*IT\_LectureSeule\*).

- Attribution des droits via GPO (ex: interdiction d’accès au Registre pour les utilisateurs standard).

- Matrice Excel :

| Ressource | Groupe AD | Droits | Responsable |

|---------------------|------------------------|--------------------------|-----------------|

| Dossier RH | GRH\_AccèsComplet | Lecture/Écriture | Responsable RH |

| Serveur SQL | IT\_Admin | Plein accès | Admin système |

Phase 4 : Plan de sauvegarde automatisé (2 semaines)

- Configuration de Veeam :

- Sauvegardes incrémentielles quotidiennes (20h-22h).

- Chiffrement AES-256 et stockage hors site (Amazon S3).

- Tests de restauration :

- Temps moyen de restauration : 2h pour un serveur virtuel.

- Validation des sauvegardes SQL (0 erreur détectée).

Phase 5 : Documentation de la continuité de service (1 semaine)

- Procédures clés :

- Procédure de reprise après incident : Étapes pour restaurer les services critiques en cas de panne.

- Plan de communication de crise : Contacts urgents (hébergeur, équipe IT, DPO).

- Support de formation :

- Guide utilisateur pour accéder aux sauvegardes en self-service.

- Atelier de formation pour les administrateurs sur Veeam.

4. Résultats et Livrables

Inventaire finalisé :

- Base de données centralisée avec 100 % des ressources recensées.

- 100 % des logiciels conformes aux licences.

Conformité validée :

- 95 % des exigences RGPD/ISO 27001 respectées.

- 5 actions correctives planifiées (ex: audit annuel des habilitations).

Sauvegarde opérationnelle :

- 30 To de données sauvegardées quotidiennement.

- RPO (Recovery Point Objective) : 24h.

**5. Défis Rencontrés et Solutions**

Problème 1 : Données personnelles non chiffrées dans le cloud

- Solution : Activation du chiffrement natif (BitLocker pour Azure, AWS KMS pour S3).

Problème 2 : Conflits de groupes AD

- Solution : Utilisation de l’outil ADManager Plus pour auditer les droits existants.

Problème 3 : Sauvegardes lentes en raison de la bande passante

- Solution : Compression des données et limitation des sauvegardes aux heures creuses.

**6. Bilan et Perspectives**

Points forts :

- Centralisation des ressources et des habilitations.

- Réduction de 70 % des risques de perte de données.

Améliorations futures :

- Automatiser l’audit des habilitations via des scripts PowerShell.

- Migrer vers un SOC (Security Operations Center) pour une surveillance 24/7.

**Annexes**

Annexe 1 : Extrait de la matrice des habilitations

Ressource : Serveur de fichiers

- Groupe AD : IT\_Admin

- Droits : Plein accès

- Responsable : Jean Dupont

Annexe 2 : Plan de sauvegarde Veeam

- Fréquence : Quotidienne (20h-22h)

- Rétention : 30 jours

- Stockage : Amazon S3 + NAS local

Annexe 3 : Procédure de continuité (exemple)

1. Identifier les systèmes critiques (ERP, base de données).

2. Restaurer les sauvegardes via Veeam.

3. Tester l’intégrité des données avant réouverture.

Équipe Projet

- Auditeur en chef : Axel

- Responsable conformité : Axel

- Administrateur système : Axel

- Documentaliste : Axel