Politique de Sécurité du Système d'Information (PSSI)

Escaliers Dubois

1. Introduction et Contexte

La PSSI définit les règles de sécurisation de l'infrastructure multisites (Lille, Dax, Annecy, Brest, Mâcon) modernisée via virtualisation, VLANs, VPN IPsec/WireGuard et outils open-source (Zabbix, GLPI). Elle répond aux points critiques identifiés : serveurs obsolètes Windows Server 2003, absence de PRA/PCA et sauvegardes non testées.

2. Objectifs de Sécurité

- Assurer confidentialité, intégrité et disponibilité (CID) des services critiques (AD/DNS/DHCP, ERP, messagerie, fichiers).
- Respecter GTI 1h, GTR 4h, RTO 4h, RPO 1 jour (classique)/1h (sensibles).
- Intégrer IDS/IPS, pare-feux pfSense et authentification centralisée AD.

3. Mesures Techniques

- Réseau : VLANs segmentés (admin, prod, users, serveurs) ; VPN site-à-site chiffré ; redondance fibre/4G-5G.
- Systèmes : Virtualisation Proxmox/VMware avec snapshots ; mises à jour automatisées ; principe de moindre privilège.
- Accès : MFA pour accès distants (commerciaux itinérants) ; zero-trust model.
- Sauvegarde : 3-2-1 (3 copies, 2 médias, 1 offsite) externalisée, testée mensuellement.

4. Organisation et Responsabilités

Rôle	Responsabilités
RSSI (Responsable SSI)	Pilotage PSSI, audits annuels, incidents majeurs.
Équipe IT multisites	Supervision Zabbix/GLPI, application règles quotidiennes.
Direction	Validation budget sécurité, approbation PRA/PCA.

5. Gestion des Incidents et PRA/PCA

- Détection via Zabbix/Centreon ; ticketing GLPI.
- Plan de réponse : alerte <5min, confinement, restauration selon RTO/RPO.
- Tests PRA trimestriels ; exercices simulés annuels.

6. Conformité et Suivi

Audits internes semestriels ; indicateurs KPI (temps résolution, faux positifs). Mise à jour PSSI annuelle ou post-incident majeur.