Modèle d’Audit Technique – Tercium (Version enrichie)

# I. Informations Générales

|  |  |
| --- | --- |
| Élément | Description à renseigner |
| Nom de l'entité | Exemple : Agence Web Alpha |
| Responsable présent | Nom + rôle |
| Date de l’audit | AAAA-MM-JJ |
| Auditeur | Nom / rôle |
| Lieu | Adresse physique / réseau logique |
| Nombre de postes | Ex : 3 postes utilisateurs + 1 NAS |
| Connexion Internet | Fibre / ADSL / 4G / Autre (préciser) |

# II. Matériel & Configuration Réseau

Identifie : système d’exploitation, IP fixe/dynamique, usage (bureautique, dev...), type de connectivité, VLAN éventuel.

Ajout : Plan d’adressage IP connu ? Segmentation (VLAN/DMZ) ?

# III. Comptes, Authentification & Accès

Présence de comptes admin/root, SSH, mots de passe faibles/non expirables, accès distant exposé.

# IV. Sauvegardes & PCA

Fréquence, type de sauvegarde, emplacement (local/cloud), vérification/restauration testée, existence d’un PRA formel.

# V. Sécurité et Mises à Jour

Firewall local actif ? Services exposés ? Politique de mises à jour ? Authentification forte ? Certificats SSL installés ?

# VI. Services critiques hébergés en local

Service | Présent ? | Type | Hébergement (PC/NAS/VM/etc.)

# VII. Procédure d’incident ou rollback

Existe-t-il une procédure de bascule ? Quelles sont les conditions de déclenchement ? Documentée ou orale ?

# VIII. Gouvernance IT locale

Existe-t-il un référent technique ? Une délégation de responsabilité ?

# IX. Projets d’évolution ou de migration envisagés

Des projets à court/moyen terme sont-ils prévus (matériel, cloud, services) ?

# X. Intégration Cloud

Instance / service, provider, objectif, IP/domaine, sécurité déployée, certificats SSL, ports ouverts, security-groups.

# XI. Observations / Anomalies / Recommandations

Bloc libre à remplir sur site : matériel obsolète, services inutiles, manque de sauvegarde, absence PRA, etc.