Version numérique
scannez ici

PROJET DE CERTIFICATION

Développement Informatique

Projet NUBEM

Présenté par : *Ertugrul HABERDAR*

Candidat au diplôme de Technicien en Informatique – IFAGE

Dans le cadre d'une étude de cas professionnelle simulée (Projet NUBEM)

Juillet 2025

Ce projet a été réalisé dans le cadre du programme de certification « Technicien en Informatique » à l'IFAGE.

Il s'agit d'une étude professionnelle simulée dans laquelle l'étudiant joue le rôle d'un prestataire informatique mandaté par l'entreprise NUBEM.

Ce travail respecte les exigences pédagogiques, techniques et méthodologiques du programme.

Ertsystem
Systèmes IT

NUBEM

PROJET Infrastructure IT

Développement Informatique de NUBEM

Juillet 2025

Table des Matières

Ertsystem
Systèmes IT

1. INTRODUCTION ET CAHIER DES CHARGES

1.1 Présentation de l'entreprise prestataire : ErtSystem

ErtSystem est une société de services informatiques basée à Genève, spécialisée dans la conception, l'implémentation et la gestion d'infrastructures IT sécurisées pour les PME et les entreprises en croissance.

Avec plus de 10 ans d'expérience dans le domaine de l'infrastructure réseau, de la virtualisation, de la cybersécurité et de la gouvernance IT, ErtSystem accompagne ses clients dans la modernisation de leur système d'information en garantissant performance, résilience et conformité.

Domaines d'expertise :

- *Architecture réseau & sécurité (firewall, VLAN, Wi-Fi entreprise)*
- *Virtualisation de serveurs (Microsoft Hyper-V, VMware)*
- *Services cloud hybrides & sauvegarde 3-2-1*
- *Plans de reprise d'activité (PRA)*
- *Support technique niveau 2 et 3*
- *Mise en place de bonnes pratiques ITIL / ISO 27001*

Rôle dans le projet NUBEM :

Dans le cadre de la modernisation de l'infrastructure IT de NUBEM, ErtSystem intervient comme intégrateur principal et coordinateur technique du projet. L'équipe dédiée assure la conception, le déploiement, la documentation, la formation des utilisateurs et le support post-projet.

Fonction	*Responsable*	*Missions principales*
General Manager	*Ertugrul HABERDAR*	*Supervision globale, validation technique et relation client*
IT Director	*Erdem GÖÇEN*	*Architecture système, choix des technologies, sécurité*
Project Manager	*Recep AYTEKIN*	*Planification, suivi d'avancement, coordination opérationnelle*
Network Architect	*Sarah Johnson*	*Conception réseau, topologie VLAN, Wi-Fi, firewall*
Deployment Coordinator	*Daniel Garcia*	*Logistique matérielle, documentation technique, déploiement*
System Administrator	*Thomas Becker*	*Mise en place Hyper-V, AD, GPO, sauvegardes*
Support Engineer (N2/N3)	*James Brown*	*Support utilisateurs, gestion des incidents, maintenance post-prod*

> L'ensemble du projet est mené selon une approche AGILE, avec validation à chaque phase par le comité de pilotage (COPIL).

1.1 Présentation de l'entreprise NUBEM

NUBEM est une entreprise suisse, fondée en 2010, spécialisée dans la vente de produits industriels d'étanchéité destinés au secteur du bâtiment. Grâce à la qualité de ses produits et à son expertise technique, elle connaît une croissance constante sur le marché national.

L'entreprise emploie actuellement 12 collaborateurs et prévoit le recrutement de trois nouveaux employés pour la saison hivernale, en raison de l'augmentation de la demande.

Dans le cadre de son développement, NUBEM a pris la décision stratégique de déménager vers un nouveau site situé à Vernier, offrant de meilleures capacités logistiques et un environnement de travail modernisé.

Ce changement nécessite une **refonte complète de l'infrastructure informatique**, afin de garantir la continuité des services, l'efficacité des opérations quotidiennes et la préparation aux évolutions futures.

1.2 Objectifs du projet

Le principal objectif de ce projet est la **modernisation complète de l'infrastructure informatique de NUBEM** sur son nouveau site à Vernier, en réponse à l'expansion de ses activités et à la nécessité d'assurer une continuité opérationnelle optimale.

Objectifs spécifiques :

Renouvellement du parc informatique :
→ 4 ordinateurs portables pour la direction et les commerciaux
→ 10 postes de travail fixes pour l'administration et les points de vente

Déploiement d'un serveur centralisé :
→ Gestion des fichiers, authentification réseau (Active Directory), virtualisation (Hyper-V)

Mise en place d'une infrastructure réseau performante :
→ VLANs segmentés, Wi-Fi sécurisé, compatibilité avec la téléphonie IP (VoIP)

Assurance de la continuité de service :
→ Sauvegardes automatiques, solution de redondance (électrique + connectivité)

Intégration des bonnes pratiques ITIL :
→ Optimisation de la gestion des incidents, du support et de la qualité de service

Sommaire

1.3 Contraintes du projet

Dans la mise en œuvre de ce projet, plusieurs contraintes doivent être prises en compte, tant sur le plan budgétaire que technique et opérationnel.

Contraintes budgétaires :

Le budget alloué à l'acquisition du matériel est compris entre **CHF 50'000 et 70'000 HT**, hors licences logicielles. Ce cadre financier impose une sélection rigoureuse des équipements, en privilégiant le meilleur rapport qualité/prix.

Contraintes techniques :

*Le matériel déployé, notamment dans les **points de vente**, doit être particulièrement robuste et adapté à un usage intensif.*

*L'infrastructure réseau doit être **entièrement compatible avec l'installation future de 20 téléphones IP**, avec prise en charge de la QoS (Qualité de Service).*

Contraintes opérationnelles :

La migration vers le nouveau site devra être réalisée **sans interruption des activités commerciales**. Une planification précise et une exécution par phases seront nécessaires pour éviter toute perte de productivité.

1.4 Enjeux et bénéfices attendus

La mise en place d'une nouvelle infrastructure informatique constitue un **enjeu stratégique majeur** pour NUBEM. Elle vise à aligner les outils technologiques avec les ambitions de développement de l'entreprise, tout en assurant la performance, la sécurité et la continuité des services.

Bénéfices attendus :

Amélioration de la productivité

→ Grâce à un environnement informatique plus rapide, fiable et adapté aux besoins métiers

Centralisation des données et contrôle des accès

→ Mise en place d'une architecture Active Directory, garantissant la gestion fine des droits et la traçabilité

Réduction des risques d'interruption

→ Architecture redondante avec systèmes de sauvegarde automatisés et connectivité multi-ligne

Renforcement de la sécurité globale

→ Grâce à un pare-feu de nouvelle génération, à la segmentation réseau (VLAN) et à la supervision en temps réel

1.5 Périmètre du projet

Le périmètre de ce projet couvre l'ensemble des composants nécessaires à la modernisation de l'infrastructure IT de NUBEM, depuis les équipements utilisateurs jusqu'à la sécurité des données et la formation.

Domaines concernés :

Parc informatique utilisateur

→ Ordinateurs fixes et portables, imprimantes réseau, scanners

Infrastructure réseau

→ Câblage structuré, commutateurs (L2/L3), points d'accès Wi-Fi professionnels, pare-feu de nouvelle génération

Sécurité et continuité de service

→ Systèmes de sauvegarde, Plan de Reprise d'Activité (PRA), redondance de la connectivité

Procédures ITIL

→ Mise en place des processus liés à la gestion des incidents, des changements et des niveaux de service (SLA)

Formation et accompagnement des utilisateurs

→ Sessions de sensibilisation à la nouvelle infrastructure et documentation technique détaillée

1.6 Plan de mise en œuvre

Le projet sera déployé en **quatre phases successives**, réparties sur une période de 7 semaines, permettant une mise en œuvre progressive, maîtrisée et sans interruption des activités.

(Le projet sera déployé en quatre grandes étapes résumées ci-dessous, couvrant une durée de 7 semaines. Le planning complet, structuré en six phases détaillées sur 12 semaines, est présenté à la section 7.2 avec le diagramme de Gantt (section 7.3).")

Phase 1 – Analyse et planification (Semaines 1 à 2)

Recueil des besoins fonctionnels et techniques auprès des utilisateurs

Sélection du matériel informatique et des prestataires

Élaboration du planning détaillé de déploiement (Gantt)

Phase 2 – Installation et configuration (Semaines 3 à 5)

Déploiement physique des postes de travail, imprimantes, points d'accès

Installation du serveur et configuration des services : AD, fichiers, sauvegardes

Mise en place du réseau : VLANs, sécurité, firewall, Wi-Fi

Phase 3 – Tests et validation (Semaine 6)

Tests de connectivité, performance et stabilité, simulation de scénarios de défaillance (PRA)

Validation fonctionnelle avec les utilisateurs référents

Phase 4 – Formation et documentation (Semaine 7)

Sessions de formation pour les utilisateurs finaux et le personnel IT

Rédaction et diffusion des procédures techniques et guides utilisateurs

Constitution de l'annexe de documentation pour le suivi post-projet

1.7 Méthodologie et gouvernance

La gestion du projet s'appuiera sur une méthodologie AGILE, permettant une adaptation continue aux contraintes techniques, aux retours des utilisateurs et aux réalités du terrain. Cette approche garantit une meilleure réactivité, un suivi rapproché et une implication active des parties prenantes tout au long du projet.Un **comité de pilotage (COPIL)** sera mis en place dès le lancement, avec des réunions hebdomadaires afin d'assurer :

-La validation des étapes clés et le suivi de l'avancement et l'ajustement des priorités si nécessaire

Composition du comité de pilotage :

***Chef de projet IT** : coordination générale, gestion du planning et du budget*

***Administrateur réseau** : supervision des infrastructures LAN/Wi-Fi/VLAN*

***Administrateur systèmes** : configuration des serveurs, services AD, sauvegardes*

***Représentant des utilisateurs** : remontée des besoins, validation fonctionnelle*

1.8 Conclusion

Ce projet représente une **étape stratégique majeure** pour accompagner la transformation numérique de NUBEM. En modernisant son infrastructure informatique, l'entreprise se dote d'un socle technologique **fiable, évolutif et sécurisé**, en cohérence avec ses objectifs de croissance et de performance. L'approche proposée, basée sur des choix technologiques adaptés, une méthodologie agile et une organisation rigoureuse, garantit :

*Une **transition fluide** vers le nouveau site sans rupture de service*

*Une **réduction significative des risques opérationnels***

*Une **meilleure qualité de service IT**, au bénéfice de l'ensemble des collaborateurs.*

Ce projet constitue ainsi un **levier essentiel** pour soutenir le développement futur de NUBEM et renforcer sa compétitivité dans un environnement de plus en plus numérique.

Sommaire

2. PROCÉDURES ITIL

Introduction aux bonnes pratiques ITIL

Le cadre ITIL (*Information Technology Infrastructure Library*) est un référentiel internationalement reconnu pour la **gestion des services informatiques**. Il fournit une approche structurée et itérative visant à **améliorer en continu la qualité des services**, à optimiser les processus IT et à renforcer la satisfaction des utilisateurs.

Dans le cadre du projet NUBEM, l'adoption d'ITIL permettra de **standardiser les interventions**, de **mieux anticiper les incidents** et d'**aligner les services IT avec les objectifs métiers** de l'entreprise.

Le cycle de vie ITIL se décline en cinq grands domaines interdépendants :

1. *Stratégie de service (Service Strategy)*
2. *Conception de service (Service Design)*
3. *Transition de service (Service Transition)*
4. *Exploitation de service (Service Operation)*
5. *Amélioration continue (Continual Service Improvement)*

2.1 Processus ITIL appliqués chez NUBEM

L'implémentation d'ITIL chez NUBEM permettra une meilleure structuration des services IT, en apportant une méthode claire pour la gestion des incidents, des changements, et l'optimisation continue des performances.

2.1.1 Stratégie de Service

Cette phase vise à aligner les services IT avec les objectifs métiers de NUBEM :

- *Gestion de la demande : anticipation des besoins futurs liés à la croissance saisonnière*
- *Gestion du portefeuille de services : identification des services critiques comme l'ERP, les fichiers partagés et la téléphonie IP*
- *Gestion financière : suivi du budget d'investissement dans l'infrastructure, et estimation des coûts récurrents*

2.1.2 Conception de Service

Définition des solutions techniques adaptées aux attentes des utilisateurs :

Service Level Management (SLM) *: définition des SLA pour les services critiques, avec KPIs de disponibilité et temps de réponse (Les engagements SLA (temps de réponse selon criticité) sont définis avec le prestataire externe – voir section 7.6.)*

Gestion de la capacité *: dimensionnement des serveurs et du réseau pour éviter toute saturation*

Gestion de la disponibilité *: mise en place de redondances réseau, onduleurs, backup*

Sécurité de l'information *: configuration du firewall, gestion des droits d'accès via AD, surveillance (PRTG)*

2.1.3 Transition de Service

Assure le passage structuré entre l'ancien et le nouveau système :

Gestion des changements *: validation des modifications via processus formalisé*

CMDB *: base de données recensant les actifs IT (serveur, switchs, postes)*

Release & Deployment Management *: planification des mises en production (systèmes, GPO, fichiers, imprimantes)*

2.1.4 Exploitation de Service

Assure le fonctionnement quotidien :

Gestion des incidents *: tickets traités via Service Desk (Freshdesk ou équivalent)*

Gestion des problèmes *: résolution durable des pannes récurrentes*

Gestion des accès *: application des GPO et restrictions par groupe utilisateur*

2.1.5 Amélioration continue

Optimisation régulière du système et des services :

Suivi des KPIs *: tableaux de bord (PRTG, rapports Freshdesk)*

Retours d'expérience (PIR) *: analyse post-mise en production ou post-incident*

Plans d'amélioration *: ajustements proactifs selon les besoins métiers ou retours utilisateurs*

2.2 Mise en œuvre concrète des processus ITIL chez NUBEM

L'application des processus ITIL chez NUBEM sera déployée de manière **progressive et pragmatique**, afin de garantir une adoption fluide au sein de l'équipe IT comme des utilisateurs finaux.

Axes de mise en œuvre opérationnelle :

Mise en place d'un Service Desk (Freshdesk)

→ Centralisation de toutes les demandes IT (incidents, demandes de service) avec traçabilité complète et historique des interventions

Définition et suivi des SLA

→ Mise en place de niveaux de priorité avec délais de réponse adaptés selon la criticité (ex. : incident bloquant < 4h) – (voir section 7.6.)

Workflow de gestion des changements

→ Formalisation d'un processus automatisé de validation des modifications avant mise en production (ex. : ajout d'un utilisateur, mise à jour logiciel)

Base de connaissances IT

→ Documentation des résolutions d'incidents récurrents afin de faciliter le traitement autonome ou rapide par le support niveau 1

Surveillance proactive de l'infrastructure

→ Intégration des outils PRTG et Zabbix pour détecter en temps réel toute anomalie réseau, surconsommation ou risque de panne

Formation continue & sensibilisation

→ Organisation de sessions régulières pour l'équipe IT sur les bonnes pratiques ITIL, ainsi que pour les utilisateurs concernant les procédures à suivre

2.3 Bénéfices attendus de l'approche ITIL

L'intégration des processus ITIL permettra à NUBEM d'**améliorer la qualité, la fiabilité et l'agilité de ses services informatiques**, tout en assurant une meilleure réactivité face aux besoins internes.

Principaux bénéfices identifiés :

Réduction significative des interruptions de service

→ *Grâce à une gestion proactive des incidents et à des procédures de continuité claires*

Anticipation et traitement plus rapide des incidents

→ *Analyse des causes récurrentes et mise en œuvre de solutions pérennes*

Amélioration de la satisfaction des utilisateurs

→ *Accès plus fluide aux services, délais de réponse mieux maîtrisés*

Maîtrise des coûts opérationnels

→ *Optimisation des ressources IT via la standardisation des processus et la surveillance des performances*

Conclusion

L'adoption du cadre ITIL par NUBEM constitue un **levier essentiel de professionnalisation** de la gestion des services informatiques. Elle permet non seulement de structurer les processus IT de manière cohérente, mais aussi d'**améliorer la qualité, la réactivité et la fiabilité** des services fournis aux utilisateurs internes.

Grâce à cette approche, NUBEM bénéficiera :

- *D'une **infrastructure plus résiliente**, capable de prévenir et de gérer les incidents efficacement*
- *D'une **vision orientée amélioration continue**, avec des KPIs pour mesurer et piloter la performance*
- *D'une **expérience utilisateur renforcée**, à travers des délais maîtrisés et une meilleure visibilité sur le support*
- En résumé, ITIL offre à NUBEM une base solide pour accompagner sa croissance tout en assurant un haut niveau de qualité de service.

3. DÉTAIL DU MATÉRIEL À PROPOSER

Introduction

Le matériel proposé pour NUBEM résulte d'un **travail approfondi de sélection, de configuration et de justification**, tenant compte à la fois des **besoins métiers précis**, des **exigences techniques du projet** et des **contraintes budgétaires**.

L'ensemble de la configuration repose sur une double logique : **uniformité technologique** et **gestion simplifiée**, garantissant une **exploitation stable, sécurisée et évolutive** sur une période de 5 ans.

Principes clés ayant guidé le choix du matériel :

Performance adaptée aux utilisateurs finaux

→Chaque poste (fixe, portable, serveur, imprimante, écran, accessoire) a été sélectionné selon le profil métier du service (Direction, Logistique, Administration, etc.) et dimensionné pour répondre à ses usages réels.

Évolutivité & résilience intégrées

→ Des composants stratégiques ont été ajoutés dès la phase initiale : 2 PC portables de réserve, disques durs "cold spare", points d'accès supplémentaires, espace disponible dans le rack serveur, accessoires et étiquettes en double.

Protection maximale sur 5 ans

*→ Tous les équipements achetés auprès de **Dell** et **Digitec** incluent des garanties **ProSupport Plus 5 ans** couvrant :*

- *les dommages accidentels (liquides, chocs, surtensions)*
- *les batteries et pièces internes*
- *le remplacement rapide (sur site ou retour sous 24h)*

*→ Ceci permet à NUBEM de ne prévoir **aucun coût de maintenance matériel** pendant toute la durée du cycle projet.*

Cohérence technologique & simplicité de maintenance

*→ Une stratégie de **standardisation par marque** a été adoptée :*

- ***Dell** pour les postes, serveurs, écrans, stations d'accueil, claviers, souris*
- ***Cisco** pour les switchs & backbone réseau*
- ***Synology + WD Red Pro** pour le stockage NAS & sauvegarde*
- ***Fortinet** pour la sécurité périmétrique (firewall), **APC** pour les onduleurs*
- ***Brady + Digitus** pour le câblage, l'étiquetage et les accessoires réseau*

Budget maîtrisé et réaliste (mai 2025)

*→ Tous les prix sont basés sur des **devis réels**, TVA incluse, capturés dans les paniers d'achat **Dell.ch** et **Digitec.ch**, avec les options de garantie incluses.*

*→ L'ensemble reste conforme au budget défini de **50'000 à 70'000 CHF**, tel que validé en **section 1.3**.*

Références croisées :

***Annexe 10.1** : Matériel utilisateur*

***Annexe 10.2** : Infrastructure & serveur*

***Annexe 10.3** : Tableaux récapitulatifs + TVA*

***Annexes 10.3.1 à 10.3.20** : Fiches techniques et captures des paniers d'achat (Dell, Digitec)*

Sommaire

3.1 Liste du Matériel Sélectionné & Justification

3.1.1 Ordinateur portable pour la Direction & les Commerciaux

- *Intel Core Ultra 7 vPro (14e génération – Meteor Lake)*
- *32 Go LPDDR5x soudée haute fréquence*
- *SSD NVMe 512 Go (Gen 4)*
- *Écran 14" FHD+ (1920x1200)*
- *Wi-Fi 6E, Bluetooth 5.3, 2x Thunderbolt 4*
- *Windows 11 Pro – 64 bits*

Dell Latitude 7450

Pourquoi ce choix ?

- ✓ *Format compact et robuste idéal pour la mobilité et les déplacements réguliers*
- ✓ *Performances élevées pour un usage professionnel intensif*
- ✓ *Sécurité renforcée : TPM 2.0, lecteur SmartCard, capteur d'empreinte, NFC*
- ✓ *Compatibilité complète avec l'infrastructure (AD, GPO, applications métier)*
- ✓ *Garantie ProSupport Plus 5 ans avec remplacement express et couverture accidentelle*

Détails complets dans l'Annexe 10.2.2 – Dell Latitude 7450

(Tableau technique complet avec composants, références produits et justification budgétaire)

3.1.2. Ordinateur pour les postes de travail pour Administration & Support

- *Processeur Intel Core i5-14500 vPro (14e génération)*
- *16 Go DDR5 – extensible jusqu'à 64 Go*
- *SSD NVMe 512 Go*
- *Windows 11 Pro*
- *Châssis moyen format avec filtres antipoussière*
- *ProSupport Plus 5 ans inclus*

Dell OptiPlex 7020

Pourquoi ce choix ?

- ✓ *Intégration immédiate dans l'environnement Windows Server : AD, GPO, SAGE, bureautique*
- ✓ *Châssis modulaire évolutif pour les futurs besoins (RAM, disque)*
- ✓ *Sécurité physique (verrouillage, filtre) + logique (TPM 2.0, BIOS sécurisé, vPro)*
- ✓ *Excellent rapport qualité/prix pour un usage administratif intensif*
- ✓ *Garantie 5 ans ProSupport Dell avec remplacement rapide en cas de panne*

Détails complets dans l'Annexe 10.2.3 – Dell OptiPlex 7020

(Tableau technique complet avec composants, références produits et justification budgétaire)

3.1.3. Moniteurs pour les postes de travail pour Administration & Support

- *Écran 27" QHD (2560×1440)*
- *Dalle IPS antireflet – angle de vision large*
- *Connectique : HDMI, DisplayPort, Hub USB 3.2 (4 ports)*
- *Pied ergonomique ajustable (hauteur, inclinaison, pivot)*
- *Garantie Dell ProSupport Plus 5 ans incluse*

Dell Pro 27

Pourquoi ce choix ?

- ✓ *Qualité d'affichage supérieure grâce à la résolution QHD et la dalle IPS – idéal pour la bureautique avancée et le multitâche*
- ✓ *Ergonomie complète conforme aux recommandations RH : confort visuel et posture de travail adaptée*
- ✓ *Compatibilité parfaite avec les unités centrales Dell OptiPlex et les docks UD22*
- ✓ *Hub USB intégré permettant de réduire l'encombrement sur les postes*
- ✓ *Garantie identique à celle des PC pour une gestion unifiée du support matériel*

Détails complets dans l'Annexe 10.2.4 – Dell P2725D

(Tableau technique complet avec caractéristiques, références produit, garantie et capture d'achat)

3.1.4. Souris sans fil mobile

- *Double connectivité : Bluetooth 5.0 + RF 2.4GHz (dongle USB)*
- *Capteur optique 1600 DPI*
- *Autonomie jusqu'à **36 mois** avec 1 pile AA*
- *Design ambidextre compact*
- *Compatibilité : Windows, macOS, ChromeOS, Linux*

Dell MS3320W

Pourquoi ce choix ?

- ✓ *Permet une connexion flexible selon le contexte (portable ou stationnaire)*
- ✓ *Idéale pour les utilisateurs en déplacement (commerciaux, direction)*
- ✓ *Format compact et ambidextre, pratique pour tous les profils utilisateurs*
- ✓ *Autonomie exceptionnelle jusqu'à 3 ans → limite les interruptions et les coûts*
- ✓ *Standardisée sur tous les portables Dell Latitude pour faciliter la maintenance IT*

Détails complets dans l'Annexe 10.2.6 – Dell MS3320W

(Fiche technique, compatibilité multiplateforme, garantie et référence achat)

3.1.5. Écran Tactile 24" – Dell P2424HT (borne interactive)

Dell P2424HT

- *Écran tactile capacitif multipoint 10 points (résolution Full HD)*
- *Taille : 23.8 pouces – dalle IPS antireflet*
- *Connectique : HDMI 1.4, DisplayPort 1.2, USB-C (Display + données)*
- *Support articulé ergonomique pour borne fixe (inclinaison jusqu'à 60°)*
- *Compatibilité VESA pour montage sur meuble ou mur*

Pourquoi ce choix ?

- ✓ *Affichage interactif pour les visiteurs : catalogue produits, vidéos, interface web*
- ✓ *Résolution idéale pour l'utilisation en point de présentation ou en showroom*
- ✓ *Design robuste adapté à une utilisation intensive dans un espace public*
- ✓ *Intégration complète avec un mini-PC professionnel (voir 5.2.22)*
- ✓ *Compatible avec les stratégies de sécurité GPO et réseau VLAN*

Détails complets dans l'Annexe 10.2.22 – Dell P2424HT
(fiche technique, usage recommandé, installation)

3.1.6. Mini-PC Dell OptiPlex 7020 Micro – pour borne interactive

Dell OptiPlex 7020

- *Format : Micro Form Factor (MFF) – compact, montage VESA*
- *Processeur : Intel Core i5-14500T vPro*
- *Mémoire : 16 Go DDR5 – extensible*
- *Stockage : SSD NVMe 512 Go*
- *Connexions : RJ45 Gigabit, Wi-Fi 6E, Bluetooth 5.3, USB-C / A*
- *Système : Windows 11 Pro – intégré au domaine Active Directory*

Pourquoi ce choix ?

- ✓ *Format compact et robuste, idéal pour une intégration discrète à une borne*
- ✓ *Performances suffisantes pour exécuter des interfaces interactives (site, vidéo, PDF)*
- ✓ *Intégration native à l'infrastructure (AD, GPO, VLAN, sécurité réseau)*
- ✓ *Maintenance simplifiée avec les autres postes du parc informatique (standardisation Dell)*
- ✓ *Compatible avec le chiffrement BitLocker, les politiques de sécurité, et la supervision*

Détails dans l'Annexe 10.2.23 – Dell OptiPlex 7020 Micro
(spécifications techniques et scénarios d'usage)

3.1.7. Station d'accueil pour PC portables

Dell Universal Dock UD22

- *Connexion universelle via USB-C*
- *Sorties vidéo : 2x DisplayPort 1.4, 1x HDMI 2.0*
- *4x USB-A 3.2, 2x USB-C, RJ45, audio combo*
- *Puissance de charge : jusqu'à 96W (port USB-C)*
- *Adaptateur secteur 130W inclus*
- *Compatible Windows, macOS, ChromeOS, Linux*

Pourquoi ce choix ?

- ✓ *Simplifie le poste de travail : un seul câble pour l'alimentation, la vidéo et les données*
- ✓ *Supporte deux écrans externes jusqu'à 5K pour la productivité multi-écrans*
- ✓ *Standardisation de l'environnement IT avec un modèle unique de station d'accueil*
- ✓ *Réduction du câblage et de l'usure des ports PC*
- ✓ *Entièrement compatible avec les portables Dell Latitude 7450 et future-proof (multi-OS)*

Détails complets dans l'Annexe 10.2.5 – Dell UD22 Dock

(Spécifications détaillées, compatibilité, référence produit et justification d'achat)

3.1.8. Switch d'accès 48 ports PoE+

Cisco Catalyst 9300

- *48 ports RJ45 Gigabit Ethernet PoE+ (jusqu'à 740W)*
- *Uplinks 10 GbE (4 ports SFP+)*
- *StackWise-480 : empilement jusqu'à 9 unités*
- *Fonctions L3 : VLAN, ACL, routage statique, QoS, DHCP Snooping*
- *Sécurité avancée : 802.1X, TrustSec, MACsec, segmentation*
- *Gestion via CLI, SNMP, Cisco DNA Center (optionnel)*

Pourquoi ce choix ?

- ✓ *Infrastructure haute disponibilité et empilable pour évolutivité réseau*
- ✓ *Intégration directe avec Active Directory, NAS Synology, Firewall FortiGate et postes clients*
- ✓ *Alimentation PoE+ pour téléphones IP, bornes Wi-Fi, caméras de surveillance*
- ✓ *Administration centralisée simplifiée, compatible avec outils de supervision (PRTG, Zabbix)*
- ✓ *Garantie constructeur et standards Cisco reconnus en entreprise*

Détails complets dans l'Annexe 10.2.7 – Cisco Catalyst 9300

(*Fiche technique complète, configuration, schéma réseau associé, justification budgétaire)*

3.1.9. NAS de stockage centralisé

Synology DS1823xs+

- *8 baies HDD – extensible via eSATA jusqu'à 18 disques (108 To)*
- *Processeur AMD Ryzen quad-core*
- *8 Go RAM ECC (extensible à 32 Go)*
- *RAID 6 – tolérance à la panne de 2 disques*
- *4 ports LAN (agrégation possible), 2 ports USB 3.2*
- *Système DSM (DiskStation Manager) – interface web intuitive*

Pourquoi ce choix ?

- ✓ *Stockage hautement sécurisé avec RAID 6 pour la redondance critique*
- ✓ *Compatible avec Veeam, Active Backup for Business, Hyper-V & AD*
- ✓ *Intégration réseau avec VLAN, LDAP / SSO, accès distant chiffré*
- ✓ *Format silencieux et faible consommation, idéal pour environnement PME*
- ✓ *Extensible facilement pour suivre l'évolution du volume de données (ajout de baies ou de RAM)*

Détails complets dans l'Annexe 10.2.8 – Synology DS1823xs+
(*Fiche technique RAID, disques WD Red Pro associés, architecture de sauvegarde et budget*)

3.1.10. Disques durs 8 To pour NAS Synology

Western Digital Red Pro

- *8 disques durs HDD – capacité unitaire : 8 To*
- *Vitesse : 7200 tours/minute*
- *Technologie d'écriture : CMR (Conventional Magnetic Recording)*
- *Mémoire cache : 256 Mo*
- *Charge de travail annuelle : 300 To / disque*
- *Fonctionnement 24/7 – usage entreprise*
- *Garantie constructeur : 5 ans*

Pourquoi ce choix ?

- ✓ *Compatibilité totale avec les environnements RAID 6 sur NAS Synology*
- ✓ *Optimisés pour un fonctionnement continu 24h/24 et 7j/7 avec haute fiabilité*
- ✓ *Haute capacité brute (8×8 To = 64 To) et **capacité utile ~48 To en RAID 6***
- ✓ *Disques professionnels avec faible taux d'erreur, adaptés à une infrastructure critique*
- ✓ *5 ans de garantie → investissement durable avec coût maîtrisé à long terme*

Détails complets dans l'Annexe 10.2.9 – WD Red Pro 8 To
(Spécifications RAID, tolérance de panne, performances, certification Synology)

Sommaire

3.1.11. Étagère Fixe 2U pour baie 19"

- *Format : 2U – profondeur 22 pouces (≈ 56 cm)*
- *Charge supportée : jusqu'à 50 kg*
- *Matériau : acier galvanisé noir*
- *Ventilation passive via conception perforée*
- *Compatibilité : baies standards 19"*
- *Idéal pour NAS, routeurs, switches non-rackables, onduleurs compacts*

StarTech Fixed Rack Shelf

Pourquoi ce choix ?

- ✓ *Permet d'installer en toute sécurité des équipements non-rackables dans la baie APC 42U*
- ✓ *Supporte des charges lourdes (NAS, UPS Synology, routeurs) sans flexion*
- ✓ *Installation rapide avec rails latéraux standards – pas de modification nécessaire*
- ✓ *Participe à la bonne ventilation de l'armoire technique (espacement et circulation d'air)*
- ✓ *Coût réduit et robustesse professionnelle → investissement durable*

Détails complets dans l'Annexe 10.2.10 – Étagère fixe 2U StarTech
(Dimensions, compatibilité armoire, capacité de charge et usage associé)

3.1.12. Onduleur 5000VA Online pour infrastructure IT

- *Puissance : 5000 VA / 4500 W – technologie double conversion (online)*
- *Format : rack 3U ou tour*
- *Interface LCD avec affichage multifonction*
- *Batteries hot-swappable – remplaçables à chaud*
- *Connectivité : USB, RJ45, SmartSlot (SNMP)*
- *Autonomie extensible avec packs batteries externes*

APC Smart-UPS SRT 5000VA

Pourquoi ce choix ?

- ✓ *Assure une alimentation sans interruption pour les systèmes critiques : serveur, NAS, switches réseau*
- ✓ *Technologie on-line double conversion : tension de sortie parfaitement stable*
- ✓ *Compatible avec Synology DSM pour déclenchement automatique d'arrêt sécurisé*
- ✓ *Maintenance facilitée : batteries remplaçables sans interruption de service*
- ✓ *Solution évolutive adaptée à une future extension d'infrastructure ou ajout de redondance*

Détails complets dans l'Annexe 10.2.11 – APC SRT 5000VA
(Spécifications complètes, scénarios d'autonomie, compatibilité avec systèmes supervisés)

Sommaire

3.1.13. Pare-feu professionnel nouvelle génération (NGFW)

Fortinet FortiGate 100F

- *Débit firewall brut : 20 Gbps*
- *Interfaces : 10x RJ45 1GbE, 4x SFP 1GbE*
- *VPN : IPsec, SSL – accélération matérielle*
- *UTM : DPI, antivirus, filtrage web, FortiGuard inclus*
- *Montage rack 1U – faible consommation*
- *Administration : Web GUI, CLI, FortiManager (optionnel)*

Pourquoi ce choix ?

- ✓ *Fournit une protection unifiée (UTM) : inspection DPI, antivirus, filtrage applicatif*
- ✓ *Gère les connexions distantes via VPN SSL/IPsec avec authentification forte*
- ✓ *Segmente le réseau via VLANs, ACL, routage – compatible avec les switchs Cisco*
- ✓ *S'intègre nativement à l'infrastructure existante : NAS Synology, serveurs, AD*
- ✓ *Interface d'administration intuitive, possibilité de centralisation via FortiManager*

Détails complets dans l'Annexe 10.3.12 – Fortinet FortiGate 100F
(Fiche technique UTM, capacités VPN, compatibilité VLAN, rôle dans la topologie réseau)

3.1.14. Armoire serveur pour infrastructure réseau

APC NetShelter SX 42U

- *Hauteur : 42U – Profondeur 1070 mm*
- *Capacité de charge : jusqu'à 1364 kg*
- *Portes avant et arrière perforées – ventilation passive optimisée*
- *Accès latéral, panneaux démontables*
- *Compatible équipements 19" : serveurs, UPS, switchs, NAS, tiroirs*
- *Système de gestion de câbles intégré vertical/horizontal*

Pourquoi ce choix ?

- ✓ *Permet de centraliser tous les équipements critiques dans un espace sécurisé et organisé*
- ✓ *Favorise la bonne ventilation, essentielle à la longévité des composants (firewall, UPS, NAS…)*
- ✓ *Sécurité physique avec portes verrouillables – conforme aux pratiques datacenter*
- ✓ *Structure robuste permettant l'installation de matériel lourd (UPS, serveurs rack 3U)*
- ✓ *Standard 19" : compatibilité universelle avec tous les périphériques IT actuels et futurs*

Détails complets dans l'Annexe 10.2.13 – Armoire APC NetShelter 42U
(Fiche technique, capacité, disposition interne, rôle dans l'aménagement de la salle serveur)

3.1.15. Patch Panel – 24 ports Cat6A blindés

Digitus Patch Panel – 24 ports Cat6A

- *24 ports RJ45 STP (blindés), norme Catégorie 6A*
- *Débit jusqu'à 10 Gbps, rétrocompatible 1G/100M*
- *Format 1U, montage standard 19 pouces*
- *Connecteurs LSA pour câblage structuré*
- *Conforme aux normes ISO/IEC 11801 et EN 50173*

Pourquoi ce choix ?

- ✓ *Permet une organisation professionnelle et centralisée du réseau informatique*
- ✓ *Compatible avec les équipements critiques : switch Cisco Catalyst, firewall, NAS*
- ✓ *Favorise la maintenance, traçabilité des ports et évolutivité de l'infrastructure*
- ✓ *Assure une transmission stable même à haut débit (10 GbE, VLANs, IP phones)*
- ✓ *Norme Cat6A blindée = meilleure immunité électromagnétique pour usage dans salle serveur*

Détails complets dans l'Annexe 10.3.14 – Armoire APC NetShelter 42U

(Fiche technique, capacité, disposition interne, rôle dans l'aménagement de la salle serveur)

3.1.16. APC Smart-UPS SRT 3000VA – Onduleur secondaire

APC Smart-UPS SRT 3000VA

- *3000VA / 3000W*
- *online double conversion*
- *LCD multilingue*
- *hot-swap*
- *rack 2U/3U*
- *gestion SNMP*

Pourquoi ce choix ?

- ✓ *Protection dédiée pour switches d'accès, routeurs, Wi-Fi et postes sensibles*
- ✓ *Double conversion : zéro coupure, isolement total, intégration IT complète*
- ✓ *Fonctionne en parallèle avec l'UPS principal pour éviter toute surcharge unique*
- ✓ *Excellent rapport qualité/prix (~1 400 CHF), avec compatibilité Synology (DSM)*
- ✓ *Séparation des charges critiques : meilleure maintenance et sécurité accrue*

Détails complets dans l'Annexe 10.2.15

(Spécifications complètes, scénarios d'autonomie, compatibilité avec systèmes supervisés)

3.1.17. Caméras de surveillance IP (Pack de 3)

Ubiquiti UniFi G5 Dome

- *Résolution 2K+ (2688 x 1512)*
- *Angle de vision horizontal : 102°*
- *Vision nocturne : Infrarouge (IR) jusqu'à 10 m*
- *Connectivité : Ethernet RJ45, alimentation PoE 802.3af*
- *Format dôme – usage intérieur*
- *Intégration dans UniFi Protect – gestion centralisée, alertes*

Pourquoi ce choix ?

- ✓ *Permet la surveillance permanente de la salle serveur, des points d'accès critiques ou zones sensibles*
- ✓ *Installation simple via PoE – pas besoin de câblage électrique dédié*
- ✓ *Couverture optimale grâce à un angle large et trois unités réparties*
- ✓ *Gestion depuis l'interface UniFi Protect, conviviale et sécurisée, avec accès distant possible*
- ✓ *Interopérabilité assurée avec les switches PoE Cisco Catalyst et l'architecture réseau existante*

Détails complets dans l'Annexe 10.2.16 – Caméras Ubiquiti UniFi G5 Dome
(Spécifications, schéma de couverture, compatibilité PoE, scénario de surveillance)

3.1.18. Capteur combiné température & humidité (RJ45)

AKCP THS00

- *Capteur combiné : température (T) + humidité (H)*
- *Plage de mesure température : -55°C à +75°C (précision ±0.5°C)*
- *Connectivité : RJ45 – plug-and-play*
- *Compatible avec boîtiers AKCP sensorProbe+, surveillance temps réel*
- *Fonctionne en continu – envoi d'alertes via e-mail, SMS, SNMP*

Pourquoi ce choix ?

- ✓ *Permet une surveillance en temps réel de la salle serveur – conditions environnementales critiques*
- ✓ *Protège les équipements sensibles (NAS, UPS, serveurs) contre les risques de surchauffe ou d'humidité*
- ✓ *Intégration immédiate avec sensorProbe+ – détection automatique sans config. complexe*
- ✓ *Possibilité d'étendre le système avec d'autres capteurs (fumée, intrusion, mouvement…)*
- ✓ *Instrument essentiel pour la stratégie de continuité d'activité (PRA) et conformité IT*

Détails complets dans l'Annexe 10.2.17 – Capteur AKCP THS00
(Fiche technique, portée, tolérances, intégration PRA et rôle dans la surveillance proactive)

3.1.19. Système de contrôle d'accès RFID

Promag ER755 + Badges Mifare Classic

- *Technologie RFID – fréquence : 13.56 MHz*
- *Compatible Mifare Classic 1K, norme ISO/IEC 14443A*
- *Interface réseau TCP/IP (Ethernet RJ45)*
- *Montage possible : mural ou sur rack technique*
- *Kit fourni avec 10 badges pré-enregistrables*
- *Gestion locale ou réseau via logiciel dédié*

Pourquoi ce choix ?

- ✓ *Sécurise l'accès physique à la salle serveur et aux équipements sensibles (NAS, switch, firewall)*
- ✓ *Système éprouvé, économique, facilement extensible à d'autres locaux ou racks*
- ✓ *Traçabilité des accès : enregistrement des entrées par badge → conformité RGPD renforcée*
- ✓ *Administration simple via IP, sans infrastructure complexe*
- ✓ *Permet de restreindre l'accès à certaines personnes autorisées uniquement (badge nominatif)*

Détails complets dans l'Annexe 10.2.18 – Contrôle d'accès RFID Promag + Badges

(Fiche technique, protocole RFID, intégration réseau, rôle dans la politique de sécurité physique)

3.1.20. Extincteur au dioxyde de carbone (CO_2), 2 kg

Gloria – Extincteur CO_2

- *Agent extincteur : CO_2 (dioxyde de carbone) – 2 kg*
- *Classes de feu : B & C (liquides inflammables + équipements sous tension)*
- *Extinction propre, sans résidus – ne laisse aucun dépôt*
- *Norme de conformité : EN3*
- *Utilisable sans formation spécifique – activation rapide*
- *Matériel conforme aux exigences des compagnies d'assurance*

Pourquoi ce choix ?

- ✓ *Idéal pour protéger les équipements électroniques sensibles (serveur, switch, onduleur, NAS)*
- ✓ *Évite les dommages collatéraux liés à la mousse ou à la poudre sèche*
- ✓ *Permet une intervention rapide en cas de début d'incendie, même par un util. non expert*
- ✓ *Respecte les normes de sécurité exigées pour les salles informatiques professionnelles*
- ✓ *Mise en place de 2 unités pour assurer une couverture redondante des zones critiques*

Détails complets dans l'Annexe 10.2.19 – Extincteurs CO_2 Gloria

(Fiche produit, norme de sécurité, justification d'emplacement et rôle dans la protection physique IT)

3.1.21. Imprimante multifonction réseau (4-en-1)

HP Color LaserJet Pro MFP M479fdw

- *Fonctions : impression / copie / numérisation / fax*
- *Vitesse d'impression : jusqu'à 27 pages par minute (ppm)*
- *Connectivité : USB 2.0, Ethernet RJ45, Wi-Fi Direct*
- *Écran tactile couleur 4,3"*
- *Chargeur automatique de documents (ADF) 50 feuilles*
- *Impression sécurisée + compatibilité HP JetAdvantage*

Pourquoi ce choix ?

- ✓ *Solution polyvalente pour les tâches administratives quotidiennes (RH, facturation, logistique)*
- ✓ *Connexion réseau et Wi-Fi intégrée → flexibilité d'installation dans tous les services*
- ✓ *Impression sécurisée avec code PIN → conformité RGPD & confidentialité*
- ✓ *ADF rapide pour les documents volumineux + bac papier extensible*
- ✓ *Faible coût à la page, idéal pour une utilisation régulière en PME*

Détails complets dans l'Annexe 10.2.20 – Imprimante HP MFP M479fdw

(Fiche technique complète, options de sécurité, justification budgétaire et compatibilité réseau)

3.1.22. Point d'accès Wi-Fi 6 (802.11ax)

Ubiquiti UniFi 6 Pro

- *Wi-Fi 6 (802.11ax) – bande double (2,4 GHz & 5 GHz)*
- *Débit cumulé théorique : jusqu'à 5.3 Gbps*
- *MU-MIMO 4x4 (5 GHz) et 2x2 (2,4 GHz)*
- *Alimentation : PoE (802.3af) – un seul câble Ethernet*
- *Gestion centralisée via UniFi Controller (web/cloud)*

Pourquoi ce choix ?

- ✓ *Offre une connectivité haut débit stable dans les zones denses : open space, accueil, salle de réunion*
- ✓ *Intégration complète dans le réseau existant (Cisco Catalyst, FortiGate, AD, VLANs)*
- ✓ *Gestion VLAN, portail captif invités, QoS applicatif → idéal pour un usage professionnel*
- ✓ *Installation murale ou au plafond – pas de prise électrique requise*
- ✓ *Scalabilité garantie : jusqu'à 300 utilisateurs connectés simultanément*

Détails complets dans l'Annexe 10.2.21 – Point d'accès UniFi 6 Pro

(Fiche technique, débit, scénarios d'usage, schéma d'intégration dans topologie réseau)

3.2 Comparaison des prix & sélection du fournisseur

Étude comparative des fournisseurs
Une analyse de marché a été réalisée en mai 2025 auprès des distributeurs suivants :

Fournisseur	Avantages observés	Inconvénients
Dell Technologies	Configuration sur mesure, garantie ProSupport 5 ans, fiabilité	Délais de livraison (5–7 jours)
Digitec.ch	Tarifs compétitifs, livraison rapide, matériel réseau & sécurité	Moins de personnalisation possible
LDLC Pro	Large gamme de produits IT, service client B2B	Coût global plus élevé
Amazon Business	Livraison rapide, gestion simplifiée des retours	Moins de garantie longue durée
DFI / Infomaniak	Fournisseurs locaux (Internet, Cloud), support réactif	Liés à des abonnements

Conclusion de l'analyse

- ***Dell.com** a été retenu comme **fournisseur principal** pour le matériel informatique (postes, serveurs, docks) grâce à :*
- *Une **garantie ProSupport Plus 5 ans** couvrant tous les scénarios (dommages, batteries, intervention sur site),*
- *Une **personnalisation des configurations**,*
- *Et un **support technique premium**.*
- ***Digitec.ch** a été sélectionné comme **fournisseur secondaire** pour :*
- *Les composants réseau spécialisés (switchs Cisco, firewall Fortinet, accessoires APC…),*
- *Et l'équipement périphérique (imprimantes, caméras, UPS, capteurs).*

Cette double stratégie permet de :

- *Limiter le nombre d'interlocuteurs (2 canaux principaux → Dell + Digitec),*
- *Simplifier la logistique et la facturation,*
- *Optimiser le rapport qualité/prix sur l'ensemble du projet.*

Conclusion

Le matériel sélectionné pour l'infrastructure de NUBEM a été choisi selon une méthodologie rigoureuse, intégrant :

- *une analyse précise des **besoins fonctionnels de chaque service** (direction, vente, logistique, IT),*
- *une étude comparative des **fournisseurs les plus fiables et compétitifs du marché**,*
- *un équilibre entre **performance, compatibilité et évolutivité sur 5 ans**.*

Bénéfices attendus :

- *Une infrastructure fiable, cohérente et sécurisée, entièrement compatible avec l'environnement IT existant (Active Directory, VLANs, téléphonie IP, etc.)*
- *Des équipements couverts par une garantie ProSupport 5 ans, assurant la continuité sans surcoût*
- *Une gestion centralisée facilitée grâce à la standardisation des marques (Dell, Cisco, HP, Synology)*
- *Une connectivité redondante (fibre + 5G/Starlink) pour garantir la disponibilité permanente des services critiques*
- *Une **base technique évolutive**, prête à intégrer de futurs outils SaaS, VoIP, ou extensions réseau*

Ce choix d'investissement permet à NUBEM :

- *De maîtriser ses coûts IT sur le long terme,*
- *tout en assurant une productivité optimale des collaborateurs,*
- *et une **résilience opérationnelle** conforme aux exigences d'une PME en croissance.*

4. ORGANISATION RÉSEAU ET SALLE SERVEUR

Conception Générale

L'infrastructure réseau de NUBEM a été pensée pour offrir une **haute performance**, une **sécurité avancée** et une **évolutivité maîtrisée**. Elle s'appuie sur une architecture segmentée en VLANs, intégrant un **pare-feu centralisé**, des **points d'accès Wi-Fi professionnels** ainsi qu'un **serveur virtualisé** hébergeant les services IT critiques de l'entreprise.

4.1 Objectifs Clés

L'infrastructure réseau vise à répondre aux besoins stratégiques de NUBEM en garantissant :

- ***Haute disponibilité***
  → Élimination des points de défaillance unique grâce à la redondance réseau et serveur
- ***Sécurité avancée***
  → Segmentation des flux via VLANs dédiés et protection centralisée avec un pare-feu Fortinet
- ***Support de la téléphonie IP***
  → Intégration de 20 téléphones VoIP avec priorisation du trafic (QoS)
- ***Connexion Internet fiable***
  → Accès principal par fibre optique, avec basculement automatique via 5G/Starlink en cas de panne
- ***Performance applicative***
  → Hébergement optimisé pour les services critiques : ERP SAGE, partage de fichiers, messagerie interne

4.2 Architecture du Réseau

L'architecture réseau de NUBEM repose sur une conception en couches, garantissant une gestion optimisée du trafic, une sécurité accrue et une évolutivité facilitée.

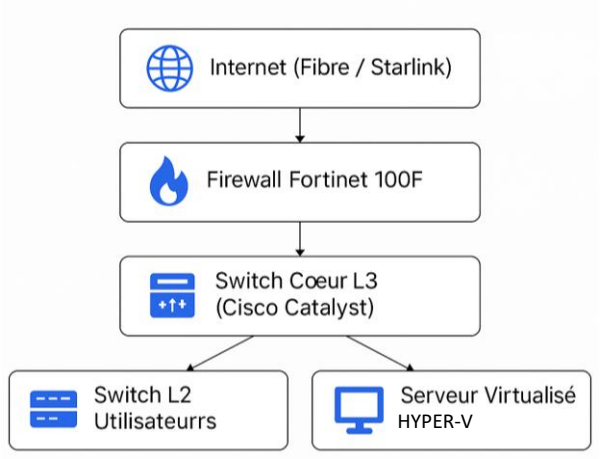
Composants principaux :

- ***Firewall & Gateway – Fortinet FortiGate 100F***
  → Assure le filtrage DPI, la gestion des connexions entrantes/sortantes, le VPN SSL/IPSec et la segmentation des flux.
- ***Switch de cœur (Layer 3)***
  → Responsable du routage inter-VLAN et de la distribution centralisée du trafic entre les services.
- ***Switchs d'accès (Layer 2)***
  → Permettent la connexion des équipements utilisateurs finaux (postes de travail, imprimantes, téléphones IP) au réseau.
- ***Points d'accès Wi-Fi***
  → Deux réseaux distincts sont configurés :

- Un SSID sécurisé pour les employés
- Un SSID isolé pour les visiteurs (VLAN invité)

- ***Serveur principal virtualisé***
  → Centralise les fonctions critiques : partage de fichiers, authentification (Active Directory), ERP (SAGE), sauvegardes automatisées.

Exemple de schéma logique :

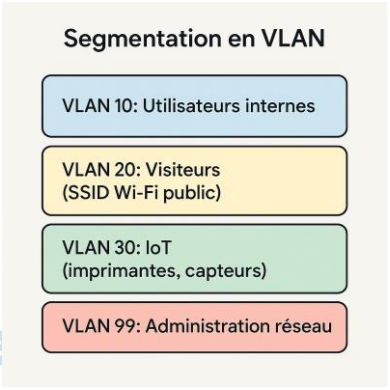


4.3 Plan d'Adressage IP & Segmentation VLAN

Pour garantir la sécurité, la performance et la maîtrise du trafic réseau, l'infrastructure est segmentée en VLANs dédiés selon les services et les usages.

Tableau de plan d'adressage :

VLAN	Département / Usage	Plage IP
10	Administration & Finance	192.168.10.0/24
20	Commercial & Marketing	192.168.20.0/24
30	Logistique & Opérations	192.168.30.0/24
40	Wi-Fi Employés	192.168.40.0/24
50	Wi-Fi Invités (isolé)	192.168.50.0/24
60	Téléphonie IP (QoS activé)	192.168.60.0/24



**Le schéma illustre visuellement la segmentation des VLANs dans l'infrastructure réseau de NUBEM, en lien avec le plan d'adressage.*

Avantages de cette segmentation :

***Isolation des flux** : chaque service est isolé pour éviter les interférences et améliorer la sécurité.*

***Performance réseau** : réduction de la congestion et amélioration de la bande passante par VLAN.*

***Simplification de la gestion** : application ciblée des règles de filtrage, des stratégies QoS, et des droits d'accès selon les groupes AD.*

4.4 Serveur & Virtualisation

Le serveur principal est un Dell PowerEdge R750, équipé de Hyper-V selon la compatibilité logicielle. Il héberge plusieurs machines virtuelles critiques, structurées comme suit:

VM	Fonction principale	Détails techniques
AD-01	Contrôleur de domaine – Active Directory	Gestion des utilisateurs, GPO, DNS, DHCP, OU par service
FILE-01	Serveur de fichiers centralisé	Partages réseau mappés par GPO, quotas par service
SAGE-ERP	Application de gestion (SAGE)	Comptabilité, logistique, accès restreint via groupes AD
BACKUP-01	Sauvegarde et Plan de Reprise d'Activité (PRA)	Veeam Backup – snapshots réguliers, réplication, export sécurisé

Avantages de la virtualisation :

- *Réduction des coûts matériels (1 serveur physique = plusieurs services)*
- *Sauvegardes rapides via snapshots & restauration simplifiée*
- *Déploiement évolutif d'applications ou de services futurs*

4.5 Sécurité & Gestion des Accès

La sécurité de l'infrastructure IT de NUBEM repose sur plusieurs mécanismes complémentaires, assurant à la fois la **protection des données**, la **traçabilité des accès**, et la **résilience face aux cybermenaces**. Composants principaux :

Pare-feu Fortinet 100F

→ *Filtrage de contenu avancé (DPI), pare-feu applicatif, VPN SSL/IPSec pour l'accès distant sécurisé.*

Active Directory + GPO (Group Policy Objects)

→ *Gestion centralisée des utilisateurs, des mots de passe, des restrictions d'accès par groupe/service.*
→ *Application automatique des stratégies de sécurité sur les postes.*

BitLocker & Journaux d'accès

→ *Chiffrement complet des disques durs (ordinateurs fixes et portables).*
→ *Suivi des connexions utilisateurs via les journaux d'audit Windows.*

PRTG Network Monitor

→ *Supervision des ports, bande passante, disponibilité réseau.*
→ *Alerte automatique en cas de défaillance ou comportement suspect.*

4.6 Connectivité Internet & Redondance

La connectivité Internet de NUBEM est conçue pour garantir une **disponibilité maximale**, même en cas de panne du fournisseur principal. Deux connexions sont configurées en **mode redondant**, avec gestion dynamique de la bande passante.

Connexions disponibles :

***Connexion principale** : fibre optique 1 Gbps via le fournisseur DFI, avec une adresse IP fixe adaptée aux services internes (serveur, VPN, etc.)*

***Connexion de secours** : routeur 5G LTE avec basculement automatique (failover), via Starlink ou Swisscom Mobile*

Répartition de charge (Load Balancing) :

*Le pare-feu Fortinet assure un **équilibrage dynamique du trafic sortant**, répartissant intelligemment la bande passante entre les deux connexions disponibles.*

En cas de coupure de la fibre, le trafic bascule automatiquement vers la connexion 5G, assurant la continuité des services critiques (ERP, fichiers, téléphonie IP).

4.7 Aménagement de la Salle Serveur

La salle serveur est conçue pour garantir un environnement **stable, sécurisé et structuré**, en assurant la bonne organisation des équipements et la protection contre les risques physiques.

Équipements & Fonctions :

Équipement	Fonction
Rack 42U	Organisation verticale des équipements, accès simplifié
Climatisation dédiée	Maintien de la température entre 18–22°C pour éviter la surchauffe
Onduleur APC 5 kVA	Alimentation de secours en cas de coupure (15–30 min)
Extincteur CO_2	Sécurité incendie sans endommager les équipements électroniques

Bonnes pratiques complémentaires :

- *Sol surélevé pour faciliter le câblage*
- *Détecteurs de fumée avec alarme sonore*
- *Limitation de l'accès physique par badge*

4.8 Maintenance & Supervision

Pour garantir la fiabilité de l'infrastructure IT de NUBEM, un plan de maintenance structuré et des outils de supervision en temps réel sont mis en place. L'objectif est de prévenir les incidents, d'optimiser les performances, et d'assurer une continuité de service maximale.

Composantes du dispositif de maintenance :

Supervision 24/7 (PRTG + Zabbix)

→ Surveillance des équipements réseau (switchs, firewall, serveurs) avec alertes automatiques en cas d'anomalie (débit, ports, CPU, RAM)

Mises à jour régulières

→ Firmware des switchs, hyperviseur , contrôleur AD et autres composants critiques
→ Périodicité : mensuelle ou selon les bulletins de sécurité fournisseurs

Plan de maintenance préventive (trimestriel)

→Nettoyage physique des équipements, test des onduleurs, vérification des logs et des sauvegardes

Sauvegardes automatiques

→ Export quotidien des configurations réseau (firewall, switchs, VM)
→ Images des machines virtuelles avec versioning (7 jours glissants minimum)

Conclusion

L'infrastructure réseau mise en place chez NUBEM répond aux exigences de performance, de sécurité et d'évolutivité. Grâce à une conception soignée intégrant la virtualisation, la redondance des connexions, et une supervision en temps réel, l'entreprise bénéficie d'un environnement stable et moderne.

Elle offre notamment :

***Une résilience élevée** grâce à la virtualisation et aux connexions redondantes*

***Une sécurité renforcée** par la segmentation réseau, le firewall Fortinet et le monitoring 24/7*

***Une évolutivité** compatible avec les besoins futurs comme la téléphonie IP ou les solutions cloud*

***Une intégration fluide des processus métiers**, incluant l'ERP SAGE, le partage de fichiers et l'authentification centralisée*

Cette base technique solide constitue un socle fiable pour accompagner la croissance de NUBEM dans les années à venir.

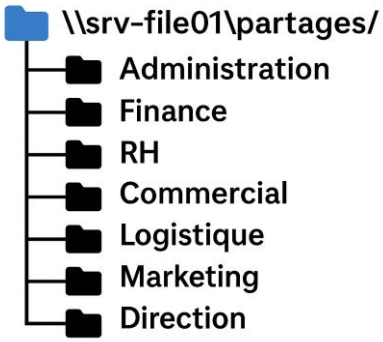
4.9 Organisation des Dossiers et Gestion des Droits d'Accès

La gestion des accès aux ressources partagées chez NUBEM est basée sur une infrastructure Active Directory structurée, avec des **groupes de sécurité** permettant de gérer finement les permissions selon les services.

Structure des partages de fichiers :

Chaque service dispose d'un dossier réseau dédié, situé sur le serveur **FILE-01**, accessible via le mappage automatique des lecteurs réseau (GPO).

Exemple de structure :



Attribution des droits (via groupes AD) :

Les droits sont appliqués en lecture seule (L), lecture/écriture (L/E) ou aucun accès (✕), selon les relations fonctionnelles entre services.

Ce modèle garantit :

La confidentialité des données sensibles *(ex. : RH, Finance)*

Le partage contrôlé d'informations transversales *(ex. : Direction → accès lecture global)*

Une administration simplifiée *: gestion par groupes (G_ADM_RW, G_FIN_RO, etc.)*

Le tableau complet des droits croisés figure en **Annexe 10.6**.

Application des permissions :

- *Intégration automatique à l'ouverture de session via GPO*
- *Mise à jour centralisée via l'outil "Active Directory Users and Computers"*
- *Documentation des règles dans un manuel interne de sécurité (charte informatique)*

5. CONFIGURATION DU SERVEUR

Introduction

Le serveur constitue le **noyau central de l'infrastructure informatique de NUBEM**, assurant l'ensemble des fonctions critiques : authentification des utilisateurs, gestion des fichiers partagés, exécution des applications métiers (ERP), et supervision du réseau.

Pour répondre aux exigences de performance, de sécurité et de continuité de service, l'architecture retenue repose sur une **infrastructure virtualisée**. Celle-ci permet d'héberger plusieurs machines virtuelles dédiées à des rôles spécifiques, tout en **optimisant l'usage des ressources matérielles** et en **simplifiant l'administration quotidienne**.

Objectifs clés de la configuration du serveur :

Haute disponibilité et redondance → *éviter tout point unique de défaillance*

Sécurité avancée → *authentification centralisée via Active Directory, gestion fine des droits d'accès*

Performance & évolutivité → *virtualisation de l'ensemble des services pour un déploiement flexible*

Automatisation & supervision → *sauvegardes planifiées, alertes temps réel, tableaux de bord IT*

5.1 Infrastructure Serveur

5.1.1 Serveur principal choisi

Modèle sélectionné : *Dell PowerEdge R750* – Serveur virtualisé central

Configuration

- *2 x Intel Xeon Silver 4310*
- *128 Go RAM DDR4 ECC*
- *6 x SSD 960 Go SATA (RAID 10)*
- *2 x 10GbE BASE-T (Broadcom 57412)*
- *Gestion à distance via iDRAC9*
- *Alimentation redondante 2 x 1100W*
- *Microsoft Hyper-V 2019 (rôle installé sur Windows Server)*

Pourquoi ce choix ?

- ✓ *Serveur haute performance capable de supporter plusieurs VM critiques (AD, ERP, fichiers, sauvegarde, supervision)*
- ✓ *Architecture RAID 10 pour assurer la sécurité des données et la rapidité d'accès*
- ✓ *Virtualisation optimisée avec Hyper-V 2019, parfaitement intégrée à Windows Server*
- ✓ *Gestion centralisée à distance grâce à iDRAC9*
- ✓ *Haute disponibilité assurée par double alimentation et connectivité 10GbE*

Détails complets dans l'Annexe 10.3.1 – Spécifications techniques serveur (p. XX)
(Tableau technique complet avec composants, références produits et justification budgétaire)

Sommaire

5.2 Virtualisation avec Hyper-V

L'architecture du serveur de NUBEM repose sur une solution de virtualisation basée sur **Microsoft Hyper-V**, intégrée à Windows Server. Ce choix a été motivé par la **compatibilité avec les environnements pédagogiques utilisés en formation**, l'**absence de coût de licence supplémentaire**, et la **simplicité de gestion via une interface graphique familière**.

Hyper-V permet d'héberger plusieurs machines virtuelles (VM) sur un même hôte physique, tout en assurant **l'isolation des services, la sécurité des données et une évolutivité optimale**.

5.2.1 Machines virtuelles déployées

VM	Rôle principal
AD-01	Contrôleur de domaine (Active Directory + GPO, DNS, DHCP)
FILE-01	Serveur de fichiers partagés avec quotas utilisateurs
SAGE-ERP	Application de gestion comptable et logistique
BACKUP-01	Serveur de sauvegarde (solution Veeam)
MONITOR-01	Supervision et alertes (PRTG, Zabbix)

Pourquoi la virtualisation avec Hyper-V ?

***Ressources optimisées** : un seul serveur physique héberge tous les services critiques*

***Isolation renforcée** : chaque VM est indépendante, ce qui limite les risques en cas de panne*

***Maintenance facilitée** : snapshots, export/import, gestion centralisée via Hyper-V Manager*

***Évolutivité garantie** : possibilité d'ajouter de nouvelles VMs sans matériel supplémentaire*

***Avantage économique** : Hyper-V est inclus avec Windows Server Standard, sans surcoût logiciel*

Référence :Détails de la configuration des VM et allocation des ressources dans l'**Annexe 10.4 – Tableau des machines virtuelles**.

5.3 Gestion des Accès & Sécurité

5.3.1 Active Directory et politiques GPO

Le serveur **AD-01** centralise la gestion des identités numériques, des groupes d'utilisateurs et des droits d'accès aux ressources partagées. Cette organisation repose sur une **stratégie Active Directory structurée par services** avec des **Groupes de Sécurité** définis selon les besoins métiers.

Groupes d'utilisateurs et droits d'accès associés :

Service	Accès principal	Accès croisés (lecture)
Achats	L/E sur son dossier	Lecture : Logistique, Opérations, Finance
Administration	L/E sur son dossier	Lecture : RH, Comptabilité
Commercial	L/E sur son dossier	Lecture : Marketing, Finance, Direction
Comptabilité	L/E sur son dossier + Finance	Lecture : RH, Admin, Direction
Direction	L/E sur son dossier	Lecture : Direction
Finance	L/E sur son dossier + Comptabilité	Lecture : RH, Direction
Logistique	L/E sur son dossier	Lecture : Achats, Opérations, Direction
Marketing	L/E sur son dossier	Lecture : Commercial, Direction
Opérations	L/E sur son dossier	Lecture : Logistique, Achats, Direction
Res. Hum. (RH)	L/E sur son dossier	Lecture : Comptabilité, Finance, Admin, Direction

(L = Lecture / E = Écriture / ✗ = Aucun accès)

Détail complet et tableau matriciel dans **Annexe 10.11 – Tableau des permissions par service.**

Sommaire

Politiques GPO appliquées (exemples clés) :

Rotation des mots de passe *tous les 90 jours minimum*

Mappage automatique *des lecteurs réseau selon le groupe de l'utilisateur*

Blocage des périphériques USB *sur les postes non autorisés (sauf Admin IT)*

Stratégies différenciées *selon le niveau de sensibilité des données (ex. : RH, Finance → accès restreint par défaut)*

Liens internes :
Voir aussi la structure des dossiers partagés dans la section ***3.11 Organisation des fichiers****.*

5.3.2 Sécurisation physique et réseau

La sécurité de l'infrastructure IT de NUBEM repose sur une combinaison de **mesures logicielles, matérielles et organisationnelles**, permettant de **prévenir les risques internes et externes**, tout en garantissant la disponibilité des services critiques.

Pare-feu et filtrage réseau

Un pare-feu **Fortinet FortiGate 100F** est déployé en frontal, assurant :

- *Le* ***filtrage DPI (Deep Packet Inspection)*** *des flux entrants et sortants*
- *La* ***segmentation VLAN*** *entre les départements*
- *La gestion des* ***connexions VPN SSL/IPSec*** *pour les accès distants sécurisés*

Chiffrement des données sensibles

Tous les disques contenant des données critiques (serveurs, sauvegardes) sont chiffrés à l'aide de **BitLocker**, garantissant la confidentialité même en cas de vol physique.

Journalisation et traçabilité des accès

L'Active Directory enregistre toutes les connexions utilisateurs, tentatives d'accès anormales et modifications sensibles via une **politique de logs centralisée**. Les journaux sont analysés régulièrement pour détecter d'éventuels incidents.

Supervision en temps réel

Les outils **PRTG Network Monitor** et **Zabbix** permettent :

- *Le* ***monitoring continu*** *des ressources critiques (CPU, RAM, bande passante)*
- *Des* ***alertes automatiques*** *en cas de dépassement de seuil ou d'anomalie système*
- *La visualisation en temps réel des* ***composants réseau et serveurs virtualisés***

Références croisées *:Voir également la stratégie de PRA en section* ***4.5*** *pour la gestion des incidents majeurs.*

5.4 Sauvegarde & Plan de Reprise d'Activité (PRA)

5.4.1 Solution de sauvegarde (version corrigée)

Pour garantir l'intégrité des données critiques de NUBEM, une solution de sauvegarde **robuste, redondante et conforme aux bonnes pratiques** a été mise en place. Elle repose sur la combinaison de **Veeam Backup & Replication** et d'un système de stockage local et distant.

Stratégie de sauvegarde retenue :

Sauvegarde quotidienne *sur un* ***NAS Synology DS1823xs+***
→ 8 baies avec disques ***WD Red Pro 8 To*** *en* ***RAID 6***
→ ***Capacité utile :*** *≈ 48 To* ***après redondance***

Sauvegarde hebdomadaire externalisée
→ vers un ***datacenter certifié ISO 27001*** *(Infomaniak Swiss Backup)*

Restauration rapide
→ via planification de ***snapshots réguliers*** *et intégration complète avec* ***Veeam***

Objectif principal :
Permettre une **restauration des services critiques en moins de 15 minutes** en cas de sinistre (perte de données, panne, ransomware, etc.)

Complément détaillé :

Voir configuration complète du NAS et stratégie 3–2–1 dans **Annexe 10.5 – Infrastructure de sauvegarde**

5.4.2 Plan de Reprise d'Activité (PRA)

Le PRA (Plan de Reprise d'Activité) permet d'assurer la **continuité des services IT** de NUBEM en cas d'incident critique : défaillance matérielle, cyberattaque (type ransomware), ou perte de données majeures.

Objectifs principaux :

Objectif	Définition	Cible
RTO *(Recovery Time Objective)*	Délai maximal d'interruption acceptable	Moins de 2 heures
RPO *(Recovery Point Objective)*	Ancienneté maximale des données restaurables	15 minutes

Moyens mis en place :

NAS principal → NAS secondaire local

→ *Réplication nocturne automatique via* ***HyperBackup*** *(Synology)*

Sauvegarde hebdomadaire externalisée

→ *via* ***Veeam Backup*** *vers un datacenter sécurisé (certifié* ***ISO 27001****, Infomaniak)*

Important :

Réplication ≠ Sauvegarde : la **réplication assure la continuité**, tandis que la **sauvegarde permet la restauration** post-sinistre.

Exemples de scénarios PRA :

Panne disque sur le NAS principal *→ basculement immédiat sur le NAS secondaire sans interruption*

Attaque ransomware *→ restauration rapide à partir du* ***checkpoint de la veille (≈ 15 min)***

Test PRA trimestriel *réalisé pour valider la procédure de récupération*

Références croisées :

Schéma et plan complet dans **Annexe 10.6 – Architecture PRA & Stratégie Veeam**

5.5 Surveillance & Maintenance

L'infrastructure IT de NUBEM fait l'objet d'un **suivi continu** et d'une **maintenance proactive**, afin de garantir la stabilité des services, la sécurité des systèmes et la réactivité en cas de dysfonctionnement.

Surveillance des performances (monitoring temps réel)

Les outils **PRTG Network Monitor** et **Zabbix** assurent une surveillance constante :

- *de l'utilisation CPU / RAM des serveurs virtuels*
- *du trafic réseau (détection des congestions ou des interruptions)*
- *du statut des services critiques (AD, ERP, Sauvegardes…)*

Des alertes sont automatiquement envoyées en cas de surcharge, coupure ou anomalie.

Mises à jour régulières (patch management)

Un serveur **WSUS (Windows Server Update Services)** est déployé pour :

- *centraliser la gestion des patchs de sécurité*
- *contrôler le déploiement des mises à jour sur les postes et serveurs*
- *éviter toute interruption non planifiée liée à une mise à jour automatique*

Analyse des journaux (log review)

- *Les* ***journaux d'événements Windows*** *(Event Viewer) sont vérifiés chaque semaine*
- *Une attention particulière est portée aux* ***tentatives d'accès non autorisées****, échecs d'authentification, ou modifications système sensibles*
- *Les logs sont* ***centralisés et archivés*** *dans un but de traçabilité*

Tests de charge et maintenance préventive

- *Des **tests de charge mensuels** sont réalisés pour s'assurer de la robustesse de l'architecture sous contrainte*
- *Un **plan de maintenance préventive** est établi (vérification des onduleurs, nettoyage matériel, test des redondances)*

Complément dans Annexe 11.5 :Tableau de planification de la maintenance et protocoles de supervision

5.6 Conclusion

L'architecture serveur déployée pour NUBEM répond pleinement aux enjeux de **sécurité, de performance et de continuité de service**. Grâce à une infrastructure virtualisée, redondante et centralisée, l'entreprise dispose désormais d'un socle technique solide pour accompagner son développement.

Elle permet notamment :

- ***Un environnement sécurisé et hautement disponible**, reposant sur un système de sauvegarde avancé et un PRA testé régulièrement*
- ***Une performance optimisée** grâce à la virtualisation, à la répartition des ressources et à la supervision en temps réel*
- ***Une gestion centralisée et évolutive**, avec Active Directory, des GPO ciblées et des services modulables*
- ***Une continuité opérationnelle assurée**, même en cas de défaillance, grâce à la réplication et aux procédures automatisées*

Référence croisée :

Cette architecture s'appuie sur les éléments détaillés dans les chapitres 4.1 à 4.6 et dans les annexes techniques 10.3 à 10.7.

6. BUDGET ET AGIL ANALYSE

Introduction à l'analyse budgétaire & méthode AGIL

La réussite du projet d'infrastructure IT de NUBEM repose non seulement sur des choix technologiques pertinents, mais également sur une gestion budgétaire rigoureuse. La méthode AGIL (Adaptabilité – Gestion – Intégration – Lean) a été choisie pour piloter l'allocation des ressources de manière stratégique et évolutive.

Objectifs de l'analyse budgétaire :

- *Maximiser la valeur des investissements en évitant les dépenses superflues (licences inutiles, surcapacité matérielle).*
- *Assurer la flexibilité budgétaire pour faire évoluer l'environnement IT sans interruption de service.*
- *Favoriser la scalabilité : prévoir l'ajout de postes, VM ou stockage sans coût de reconfiguration majeur.*
- *Optimiser le ROI en assurant un usage durable du matériel (5 ans) avec une maintenance préventive structurée.*

Aligner la stratégie financière avec les impératifs métier de NUBEM (croissance saisonnière, extension d'équipe).

Méthodologie utilisée :

L'ensemble des données chiffrées est issu :

- *des devis réels obtenus en mai 2025 (Dell & Digitec),*
- *des prévisions d'entretien et renouvellement (TCO sur 5 ans),*
- *et des exigences définies dans le cahier des charges IT.*

L'analyse porte exclusivement sur les équipements physiques, les coûts logiciels et licences (SaaS, antivirus, sauvegarde, etc.) n'étant pas inclus dans ce périmètre budgétaire.

6.1 Structure budgétaire du projet (version finale – mai 2025)

L'analyse budgétaire du projet d'infrastructure informatique de NUBEM repose sur une répartition détaillée des investissements physiques, réalisée à partir des devis réels obtenus en mai 2025 (Dell, Digitec).

Tous les montants sont exprimés en CHF hors taxes (HT) conformément aux exigences comptables.

Répartition budgétaire consolidée par domaine :

Catégorie	*Total estimé (CHF HT)*	*Commentaires*
Matériel informatique (PC, écrans, docks, souris, claviers)	~31'870	5 portables + 14 PC fixes + 14 écrans QHD + accessoires standards
Serveur & infrastructure réseau	~29'000	Serveur Dell R750, NAS Synology, disques WD, switch Cisco, Wi-Fi, UPS, etc.
Imprimante & périphériques bureautiques	~2'680	HP LaserJet Pro multifonction couleur réseau
Sécurité physique & étiquetage	~700	Extincteurs CO_2, capteurs température, contrôle d'accès RFID, cartouches Brady
Formation des utilisateurs	~1'350	Sessions internes + guides interactifs (formation Active Directory, GPO, fichiers)
Formation ITIL	~1'000	Prévision pour atelier initial de sensibilisation à la gestion des incidents IT
TOTAL estimé (hors taxes)	~66'600 CHF	Conforme au budget prévu (entre 50'000 et 70'000 CHF HT)

Remarques importantes :

- *Ce budget n'intègre pas les logiciels, licences SaaS ou abonnements cloud (Office 365, Veeam, FortiGuard, Freshdesk…).*
  Ces éléments feront l'objet d'une analyse financière distincte lors de la phase d'exploitation.
- *Les dépenses liées à la formation ITIL sont estimées mais non intégrées au total à ce stade.*

Références croisées :

- *Voir Annexes 10.1 à 10.3 pour le détail poste par poste*
- *Voir Annexe 10.3.22 pour le tableau récapitulatif budgétaire complet (avec justificatifs HT)*
- *Voir Captures d'écran en preuve d'achat (Dell et Digitec – mai 2025)*

6.2 Analyse AGIL pour l'optimisation budgétaire

La méthodologie **AGIL** (Adaptabilité – Gestion – Intégration – Lean) permet à NUBEM de tirer le meilleur parti de son budget tout en maintenant un haut niveau de flexibilité et de rentabilité sur le long terme.

Chaque pilier du modèle est appliqué au projet d'infrastructure de manière concrète.

6.2.1 Adaptabilité des ressources

Problématique :
Les besoins IT évoluent rapidement (croissance de l'équipe, nouveaux logiciels, téléphonie IP, accès distants), ce qui nécessite une capacité d'adaptation sans coûts excessifs.

Solutions mises en œuvre :

Matériel évolutif dès l'achat *: PC avec slots RAM libres, NAS extensible, serveur virtualisé, baie rack surdimensionnée pour ajouter des équipements futurs*

Intégration du Cloud hybride *: services de sauvegarde en ligne (Infomaniak, Veeam), accès VPN, fichiers synchronisés*

Flexibilité dans la gestion de la connectivité *: redondance fibre + 5G/Starlink, VLAN invités activables à la demande*

Équipements modulaires *: étiquetage réutilisable, switchs StackWise, disques "cold spare", onduleurs avec batteries hot-swap*

Impact :
Ces choix permettent à NUBEM de réagir rapidement aux besoins métiers, sans reconfigurer entièrement l'environnement existant ni déclencher de nouvelles dépenses majeures.

6.2.2 Gestion des Dépenses & Priorités

Problématique :
Le budget global du projet étant limité (70'000 CHF HT max.), chaque dépense doit être **justifiée** et **optimisée** selon son impact sur la continuité des services et la performance de l'entreprise.

Solutions mises en œuvre selon l'approche AGIL :

Priorisation des investissements *: Les achats ont été classés par ordre de criticité fonctionnelle (serveur > sécurité > utilisateurs > périphériques) en fonction du* ***retour sur investissement (ROI)*** *attendu.*

Réduction des coûts à long terme *: Tous les équipements critiques sont couverts par des* ***garanties ProSupport 5 ans****, limitant les frais de maintenance ou remplacement.*

Diminution des coûts d'exploitation *: Grâce à une infrastructure* ***hautement automatisée*** *(monitoring Zabbix, sauvegardes Veeam, AD/GPO), la charge humaine et les interventions manuelles sont réduites.*

Centralisation des outils de gestion *(UniFi Controller, FortiGate GUI, WSUS…) pour minimiser les coûts logiciels et administratifs.*

Impact :

Cette gestion rigoureuse permet à NUBEM de déployer une infrastructure robuste tout en **maîtrisant ses coûts sur 5 ans**, sans rogner sur la sécurité, la performance ni l'évolutivité.

6.2.3 Intégration des nouveaux services IT

Problématique : L'introduction de nouveaux services (virtualisation, téléphonie IP, SaaS, sauvegarde Cloud…) peut engendrer des perturbations dans les opérations courantes si elle n'est pas maîtrisée.

Solutions mises en œuvre selon l'approche AGIL :

Déploiement progressif contrôlé *: Mise en place d'un* ***environnement de test (VM dédiée)*** *pour valider les services critiques (ERP, partages de fichiers, sauvegardes) avant leur généralisation.*

Standardisation de l'infrastructure *: Choix volontaire de marques cohérentes (Dell, Cisco, Synology) pour faciliter* ***l'intégration, la documentation et le support IT****.*

Adoption de services SaaS ciblés *(ex. : sauvegarde Infomaniak, Helpdesk Freshdesk) pour limiter les coûts d'infrastructure et garantir une* ***scalabilité immédiate*** *sans achat de matériel supplémentaire.*

Interopérabilité assurée *: Tous les composants (firewall, VLAN, switchs, Wi-Fi) ont été sélectionnés pour* ***intégrer nativement les protocoles standards IT*** *(SNMP, AD, LDAP, DHCP, VLAN tagging).*

Impact :
Ce modèle d'intégration maîtrisé permet de déployer des nouveautés sans interruption de service, tout en **préparant l'infrastructure aux évolutions futures (cloud hybride, télétravail, IoT, etc.)**.

6.2.4 Lean Management & réduction des coûts inutiles

Problématique : Dans les projets IT, il existe un risque constant d'investir dans des solutions coûteuses, redondantes ou inadaptées aux besoins réels. Ces dépenses diminuent le ROI global et compliquent la maintenance.

Solutions mises en œuvre selon l'approche AGIL :

Évaluation systématique des besoins réels avant chaque acquisition *→ suppression des surdimensionnements, achat de postes selon usage métier réel (bureau ≠ mobilité).*

Maintenance proactive *avec contrats long terme (5 ans ProSupport) →* ***réduction des interventions non planifiées*** *et des achats de remplacement.*

Virtualisation maximale *des serveurs (Hyper-V) → limitation du matériel physique, baisse des coûts énergétiques, meilleure gestion des ressources.*

Réduction des fournisseurs *→ deux interlocuteurs uniques (Dell + Digitec) →* ***logistique et facturation simplifiées****, temps gagné en administration.*

Matériel standardisé *→ rationalisation des pièces détachées, des procédures et de la documentation.*

Impact :Ce pilotage "lean" permet à NUBEM de mettre en œuvre une infrastructure performante, évolutive et stable tout en **réduisant les coûts directs et indirects sur 5 ans**, sans compromettre la sécurité ni la qualité de service.

6.3 Prévisions financières & Retour sur Investissement (ROI)

Le projet d'infrastructure IT de NUBEM, évalué à environ 65'000 CHF HT, s'inscrit dans une logique de retour sur investissement progressif, basé sur les économies opérationnelles réalisées dès la mise en production.

Projection du ROI sur 3 ans (budget 65'000 CHF HT estimé)

Année	*Investissement Cumulé (CHF)*	*Économies Opérationnelles Estimées (CHF)*	*ROI (%)*
2025	*66'000*	*10'000*	*15.4 %*
2026	*66'000*	*22'000*	*33.8 %*
2027	*66'000*	*32'000*	*49.2 %*

Analyse mise à jour :

- Réduction effective des coûts de maintenance, pannes matérielles, et interventions non planifiées grâce au matériel sous garantie 5 ans

-Moins de consommation électrique : serveurs virtualisés, postes efficaces, NAS optimisé

-Automatisation accrue = moins de gestion manuelle (sauvegardes, supervision, accès utilisateur)

-ROI supérieur à 49 % dès la 3e année, sans inclure les gains de productivité utilisateur ni les bénéfices indirects

Nota Bene :Le ROI est calculé sur la base du budget HT matériel uniquement, hors logiciels SaaS, licences ou abonnements annuels.

Conclusion

L'approche AGIL appliquée au projet d'infrastructure IT de NUBEM a permis de construire un budget réaliste, maîtrisé et évolutif, en parfaite adéquation avec les enjeux de croissance de l'entreprise.

Résultats obtenus :

- *Élimination des investissements superflus grâce à une priorisation fondée sur le ROI réel*
- *Flexibilité budgétaire assurée, permettant d'adapter les ressources selon l'évolution des besoins*
- *Maximisation du retour sur investissement grâce à la baisse des coûts d'exploitation et à la maintenance préventive*
- *Transition IT fluide et maîtrisée, avec une continuité opérationnelle garantie à chaque étape du déploiement*

Conclusion générale :

Ce budget donne à NUBEM une infrastructure IT robuste, sécurisée et scalable, parfaitement adaptée à ses ambitions actuelles et futures.

7. PLANIFICATION ET GANTT CHART

Introduction

La planification constitue un levier essentiel pour assurer le **déploiement maîtrisé** de l'infrastructure IT de NUBEM. Basée sur une démarche **progressive, agile et coordonnée**, elle permet de limiter les risques techniques et les interruptions de service, tout en garantissant une transition fluide.

Objectifs de la planification :

Découper les étapes critiques *du projet avec des jalons précis (analyse, commande, installation, test, formation)*

Minimiser l'impact sur les opérations commerciales *en organisant le basculement en plusieurs phases successives*

Permettre un suivi agile et itératif *: pilotage hebdomadaire, ajustement des tâches en fonction des ressources disponibles*

Assurer une mise en production sans risque *grâce à une séquence de* ***tests préalables, validations utilisateurs et documentation complète***

Contextualisation post-budgétaire :
Cette planification tient compte :

- *du budget validé (~66'000 CHF HT),*
- *des délais réels de livraison fournisseurs (Dell & Digitec, 5–10 jours ouvrables),*
- *des ressources internes de NUBEM (disponibilité IT, utilisateurs clés),*
- *et des étapes critiques identifiées lors du dimensionnement de l'infrastructure.*

Le **diagramme de Gantt** associé au projet est présenté en section 7.2.
Il couvre les 7 semaines de déploiement, du cadrage initial à la formation utilisateurs.

7.1 Phases de déploiement du projet

Le déploiement de l'infrastructure IT de NUBEM est structuré en six grandes phases. Chaque étape est associée à des livrables précis, des objectifs opérationnels, et des responsables désignés. La durée globale du projet est estimée à 12 semaines, hors imprévus logistiques.

7.1.1 Phase 1 : Analyse des besoins & planification

Période : semaines 1 à 2

Objectifs opérationnels :

- *Identification des besoins fonctionnels pour chaque département (vente, logistique, direction, IT)*
- *Validation des choix technologiques (serveur, réseau, sécurité) et du budget consolidé (~65'000 CHF HT)*
- *Rédaction du plan de migration IT (méthodologie + séquences techniques)*
- *Sélection des fournisseurs stratégiques (Dell, Digitec) et passation des commandes*

Responsables :

- *Chef de projet IT (interne ou consultant)*
- *Direction générale (approbation budgétaire et arbitrages fonctionnels)*
- *Représentants utilisateurs (pour la phase de recueil des besoins)*

Cette phase constitue le socle stratégique du projet. Elle détermine le bon dimensionnement de l'infrastructure et la cohérence des solutions à déployer.

7.1.2 Phase 2 : Préparation & réception du matériel

Période : semaines 3 à 4

Objectifs opérationnels :

- *Réception physique des équipements depuis Dell et Digitec (PC, serveurs, réseau, sécurité)*
- *Contrôle qualité et vérification de la conformité technique (modèles, quantités, garanties)*
- *Préconfiguration des équipements critiques :*

- Serveur Dell R750 avec installation Hyper-V + VMs (AD, fichiers, sauvegarde)
- NAS Synology avec disques WD configurés en RAID 6
- Switch Cisco, firewall Fortinet, points d'accès Wi-Fi
  . Préparation des postes utilisateurs (installation OS, drivers, GPO, sécurité)
  . Réalisation de tests matériels préventifs (disques, redondance, température, connectivité)

Responsables :

- *Équipe IT interne ou prestataire intégrateur*
- *Responsable des achats (réception, inventaire, conformité)*
- *Technicien système/réseau (configuration initiale et tests)*

Cette phase garantit que tous les composants sont opérationnels avant l'intégration réseau, réduisant les risques de panne ou de retard lors de la mise en production.

7.1.3 Phase 3 : Déploiement de l'infrastructure réseau

Période : semaines 5 à 6

Objectifs opérationnels :

- *Installation physique du câblage structuré Cat6A avec étiquetage (armoire 42U, patch panels Digitus)*
- *Configuration des VLANs métiers selon le plan d'adressage (AD, Wi-Fi, VoIP, invités, téléphonie IP)*
- *Déploiement du pare-feu Fortinet 100F avec inspection DPI, règles ACL, VPN IPsec/SSL*
- *Activation des points d'accès UniFi 6 Pro (Wi-Fi 6) avec gestion centralisée via UniFi Controller*
- *Mise en place de la téléphonie IP (QoS, compatibilité VLAN, alimentation PoE)*

Responsables :

- *Administrateur Réseau*
- *Ingénieur Sécurité*
- *Chef de projet IT (suivi global et vérification du schéma de cohérence)*

Cette phase vise à établir une base réseau fiable, segmentée et sécurisée, en garantissant la compatibilité avec tous les équipements serveurs, clients et périphériques métiers.

7.1.4 Phase 4 : Installation & configuration des serveurs et services IT

Période : semaines 7 à 8

Objectifs opérationnels :

- Déploiement des machines virtuelles critiques sur l'hyperviseur Microsoft Hyper-V :
  - ✓ **AD-01 :** Active Directory, DNS, DHCP, GPO
  - ✓ **FILE-01 :** Serveur de fichiers avec quotas et mappage automatique
  - ✓ **ERP-SAGE :** Application de gestion comptable
  - ✓ **BACKUP-01 :** Sauvegarde centralisée avec Veeam
  - ✓ **MONITOR-01** : Supervision (PRTG, Zabbix)
- Création de l'arborescence des dossiers partagés et affectation des droits via groupes AD
- Déploiement des stratégies GPO : mot de passe, mappage lecteurs, sécurité USB
- Mise en œuvre du plan de sauvegarde 3-2-1 :
  - ✓ NAS Synology RAID 6
  - ✓ Sauvegarde cloud (Infomaniak)
  - ✓ PRA avec réplication et test de restauration

Responsables :

- *Administrateur Système (configuration et déploiement)*
- *Consultant IT / Intégrateur (vérification des dépendances inter-VM, documentation)*
- *Équipe support (création des comptes utilisateurs et validation des accès)*

Cette phase consolide la couche applicative et les services de base (authentification, fichiers, supervision), garantissant la résilience, la sécurité et la continuité d'activité.

7.1.5 Phase 5 : Tests, validation & correction des anomalies

Période : semaines 9 à 10

Objectifs opérationnels :

- *Réalisation de tests de performance réseau & serveur : bande passante, latence, vitesse d'accès aux partages, temps de réponse applicatif*
- *Audit de sécurité (pare-feu, VLANs, comptes, journalisation, antivirus, accès utilisateurs)*

Simulation de pannes :

- ✓ **Coupure de connexion fibre →** basculement automatique vers 5G
- ✓ **Défaillance NAS principal →** basculement vers NAS secondaire (HyperBackup)
- ✓ **Test PRA →** restauration depuis checkpoint

- *Identification et correction des anomalies techniques (configurations réseau, droits, règles GPO)*
- *Validation fonctionnelle par les utilisateurs pilotes et la direction IT*

Responsables :

- *Chef de projet IT (planification, coordination)*
- *Responsable Qualité / MOE*
- *Utilisateurs référents (tests fonctionnels par service)*

Cette phase assure que l'ensemble du système est stable, sécurisé et conforme aux attentes définies dans le cahier des charges, avant la mise en production.

Sommaire

7.1.6 Phase 6 : Formation, migration & mise en production

Période : semaines 11 à 12

Objectifs opérationnels :

- *Organisation de sessions de formation ciblées pour les utilisateurs :*
  - ✓ Utilisation du réseau partagé (mappage, droits, sauvegardes)
  - ✓ Accès distant (VPN, cloud)
  - ✓ Bonnes pratiques de sécurité (mots de passe, USB, incidents)
- *Mise à disposition de supports de formation personnalisés (guides PDF, FAQ, tutoriels internes)*
- *Migration contrôlée des données utilisateurs vers les nouveaux partages réseau*
- *Vérification finale de la connectivité, des accès, des imprimantes, du Wi-Fi et de la téléphonie IP*
- *Mise en production officielle de l'infrastructure IT de NUBEM*

Responsables :

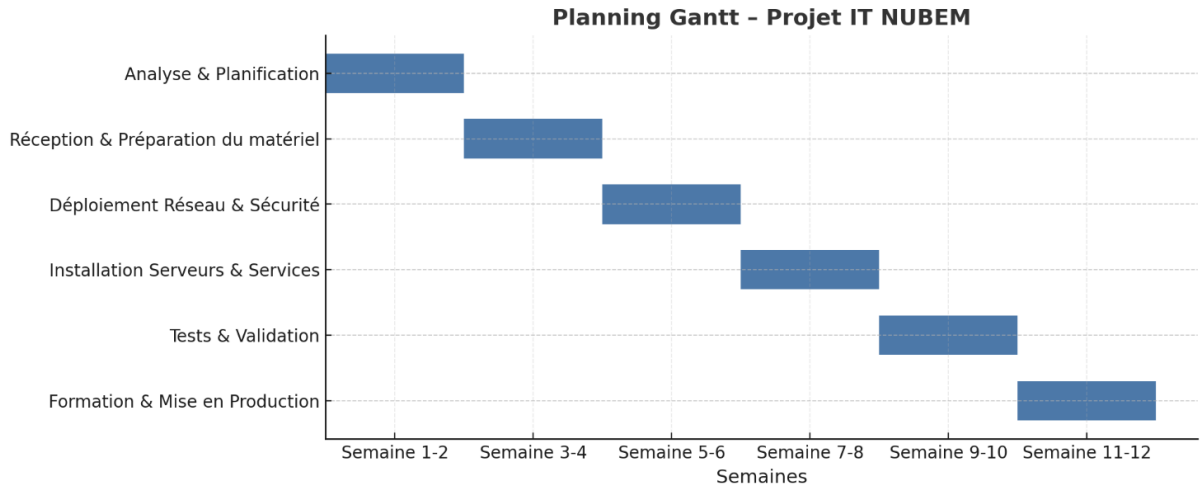
- *Équipe IT (assistance utilisateurs, configuration post-migration)*
- *Formateurs internes ou référents par service*
- *Employés finaux (tests, validation des accès, feedback)*

Cette phase marque la transition officielle vers l'environnement cible. Elle assure l'adhésion des utilisateurs, la stabilité fonctionnelle et la clôture opérationnelle du projet.

7.2 Diagramme de Gantt – Planification visuelle du projet

Pour garantir une vision claire, synthétique et opérationnelle du déroulement du projet IT de NUBEM, un diagramme de Gantt a été établi. Il permet de visualiser la répartition des tâches sur une durée totale de 12 semaines, du cadrage initial à la mise en production.

Planning détaillé sur 6 phases clés :



Avantages du diagramme de Gantt :

- *Visualisation rapide et structurée des tâches et délais*
- *Anticipation des besoins en ressources humaines et matérielles*
- *Suivi opérationnel simple et efficace pour l'équipe projet*

Sommaire

- *Alerte en cas de retard ou de blocage possible → possibilité d'ajustement agile*
- *Communication facilitée avec la direction et les parties prenantes*

Le Gantt ci-dessus est une version synthétique. Le planning complet avec dépendances, responsables et jalons est présenté en Annexe 10.4 – Plan de déploiement.

7.3 Gestion des risques & stratégies d'atténuation

Anticiper les risques techniques, humains ou logistiques est essentiel pour garantir la réussite du projet. Cette section identifie les principaux scénarios à risque et les mesures préventives ou correctives associées.

Tableau des risques identifiés

Risque	*Impact potentiel*	*Solution mise en œuvre*
Retard de livraison du matériel	*Blocage du planning d'installation*	*Commande anticipée + fournisseurs locaux en plan B*
Erreur de configuration réseau	*Perte de connectivité, interruption*	*Tests en environnement de préproduction avant intégration finale*
Adoption utilisateur insuffisante	*Perte de productivité, confusion*	*Formation interactive + guides visuels disponibles dès J+1*
Panne serveur après mise en prod	*Interruption critique des services*	*PRA opérationnel (NAS + Veeam + restauration en < 2h)*

Stratégie globale d'atténuation des risques

- *Réunions de pilotage hebdomadaires pour identifier les écarts en temps réel*
- *Plan B défini pour chaque équipement critique (NAS, firewall, Wi-Fi, etc.)*
- *Phase de tests rigoureux (charge, PRA, failover) avant passage en production*
- *Standardisation du matériel pour faciliter les remplacements express*
- *Documentation technique à jour pour chaque composant déployé*

Cette gestion prévisionnelle renforce la robustesse du projet et garantit que chaque imprévu possible dispose d'une réponse concrète et validée.

Conclusion générale de la planification

Grâce à une planification détaillée et structurée, le projet d'infrastructure IT de NUBEM bénéficie de toutes les garanties nécessaires pour un déploiement fluide, sans interruption des opérations métiers.

Chaque phase a été définie avec des responsabilités claires, des objectifs mesurables et un calendrier réaliste.

Points forts de la stratégie de déploiement :

- *Suivi rigoureux via diagramme de Gantt, jalons par phase et pilotage hebdomadaire*
- *Approche Agile : flexibilité, adaptation continue et feedback rapide des utilisateurs*
- *Anticipation proactive des risques, avec des plans de secours concrets pour les équipements critiques*
- *Coordination efficace entre IT, direction, utilisateurs et fournisseurs*
- *Mise en production progressive et contrôlée, assurant une transition IT réussie et sans impact sur la continuité d'activité*

Cette phase de planification constitue un socle stratégique permettant à NUBEM de passer sereinement à l'étape suivante : la mise en œuvre opérationnelle de son infrastructure numérique.

7.4. Définition des SLA & Engagements de Qualité

Afin d'assurer la continuité de service et la réactivité attendue par le client, des accords de niveau de service (SLA) sont formalisés entre l'entreprise NUBEM et le prestataire IT externe chargé de l'infrastructure.

Ces engagements définissent les délais maximaux de traitement et de résolution en fonction de la criticité des incidents, ainsi que les indicateurs clés de performance (KPI) pour le suivi qualité.

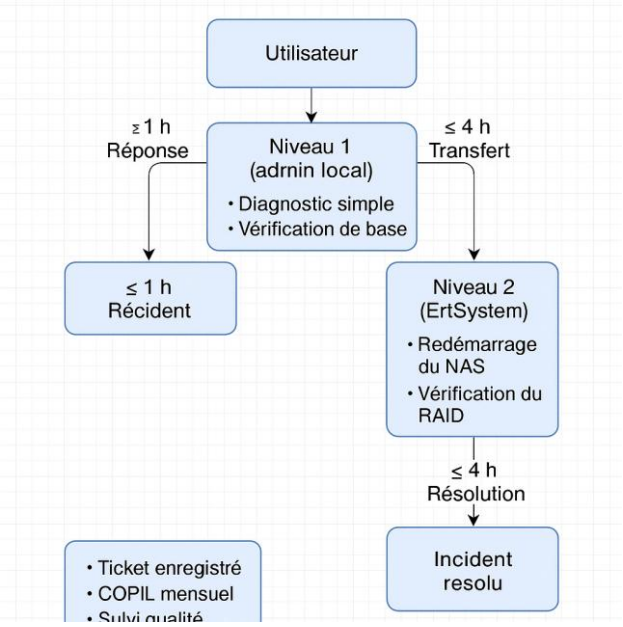
Tableau des SLA par criticité

Niveau de criticité	Description	Exemple d'incident	Délai de réponse	Délai de résolution
Critique (P1)	Service bloquant, impact global sur la production	Panne du serveur Hyper-V, plus d'accès au réseau ou aux fichiers	≤ 1 heure	≤ 4 heures
Majeur (P2)	Service partiellement dégradé, plusieurs utilisateurs impactés	Problème sur l'accès ERP, ou sur VLAN Wi-Fi interne	≤ 4 heures	≤ 1 jour ouvré
Mineur (P3)	Impact limité, contournement possible	Imprimante locale non disponible, latence réseau légère	≤ 1 jour ouvré	≤ 3 jours ouvrés
Demande (P4)	Demande de service non urgente	Création d'un nouvel utilisateur, accès invité VPN	≤ 2 jours ouvrés	≤ 5 jours ouvrés

Suivi & supervision des engagements

- ✓ *Tous les incidents sont enregistrés via l'outil de ticketing du prestataire.*
- ✓ *Un rapport mensuel de performance est fourni, indiquant :*
- ✓ *le taux de respect des SLA (%)*
- ✓ *les causes d'incidents récurrents*
- ✓ *les actions correctives mises en œuvre*
- ✓ *Un COPIL mensuel (comité de pilotage) permet de valider la qualité du service et d'ajuster les engagements si nécessaire.*

Organisation du support technique :



Remarques complémentaires

- ✓ *Les SLA ne couvrent que les services critiques explicitement listés dans le périmètre contractuel.*
- ✓ *Les horaires d'intervention garantis sont de **8h00 à 18h00**, du lundi au vendredi (hors jours fériés).*
- ✓ *En cas d'incident en dehors de cette plage horaire, une procédure d'astreinte peut être déclenchée sur demande spécifique.*

Sommaire

8. CHARTE INFORMATIQUE

Introduction à la charte informatique

La charte informatique de NUBEM constitue un cadre réglementaire interne visant à encadrer l'utilisation des ressources numériques de l'entreprise. Elle s'applique à l'ensemble des collaborateurs disposant d'un accès aux équipements informatiques et aux données de l'entreprise.

Ce document vise à prévenir les risques techniques, juridiques et humains liés à l'usage de l'informatique, tout en favorisant un environnement numérique sûr, efficace et conforme aux standards internationaux (RGPD, ISO 27001, NIST).

Objectifs principaux de la charte informatique :

- ✓ *Garantir la sécurité des données, des systèmes et du réseau*
- ✓ *Définir des règles claires d'utilisation des équipements, logiciels, comptes et accès*
- ✓ *Prévenir les incidents de cybersécurité (malwares, phishing, intrusions, fuites)*
- ✓ *Encadrer la gestion des accès utilisateurs, des mots de passe, des droits partagés*
- ✓ *Assurer une productivité optimale tout en respectant la législation en vigueur (vie privée, surveillance, confidentialité)*
- ✓ *Responsabiliser chaque utilisateur face aux bonnes pratiques numériques et à la confidentialité*

Cette charte est un document vivant, qui doit être mis à jour régulièrement en fonction de l'évolution des technologies, des usages et du cadre réglementaire.

8.1 Utilisation responsable des ressources informatiques

L'ensemble des collaborateurs de NUBEM est tenu de respecter les règles d'usage des systèmes d'information afin de garantir un environnement numérique sécurisé, performant et conforme aux obligations légales.

8.1.1 Bonnes pratiques générales

Chaque utilisateur est responsable de son comportement numérique et de son compte personnel. Il s'engage à :

- *Utiliser les équipements exclusivement à des fins professionnelles*
- *Ne pas installer de logiciels non autorisés ou sans validation IT*
- *Ne pas stocker de données personnelles sur les systèmes de l'entreprise*
- *Verrouiller systématiquement son poste de travail en cas d'absence*
- *Respecter les procédures de changement de mot de passe régulier et de sécurisation des accès*

8.1.2 Utilisation du matériel informatique

Concernant les équipements mis à disposition (PC, imprimantes, téléphones IP, Wi-Fi…) :

- *Leur utilisation doit correspondre aux missions confiées et au cadre professionnel défini*
- *Les appareils doivent être mis à jour régulièrement (OS, antivirus, logiciels métiers)*
- *Tout prêt ou utilisation extérieure (membre de la famille, visiteur) est strictement interdit*
- *Toute anomalie ou panne doit être signalée immédiatement au service IT*

8.1.3 Accès Internet & messagerie électronique

Navigation Internet :

- *L'accès à des sites illégaux, à caractère pornographique ou non professionnel est interdit*
- *L'usage des réseaux sociaux est toléré uniquement à des fins de communication professionnelle*
- *Le téléchargement de contenu doit rester strictement lié à l'activité de l'entreprise*

Emails professionnels :

- *Ne jamais ouvrir de pièces jointes ou liens suspects*
- *Ne jamais transmettre des données sensibles non chiffrées par email*
- *L'adresse email professionnelle ne doit pas être utilisée à des fins personnelles*
- *L'utilisation abusive de la messagerie (spam, blagues, chaînes) est interdite*

Ces règles sont applicables à tous les employés, y compris les stagiaires, consultants ou collaborateurs externes. Toute violation pourra faire l'objet de mesures disciplinaires conformément au règlement interne.

8.2 Sécurité informatique & protection des données

La sécurité des systèmes d'information est une priorité stratégique pour NUBEM. Tous les utilisateurs sont tenus de respecter des règles strictes afin de prévenir les intrusions, les pertes de données et les violations de confidentialité.

Les politiques mises en place sont conformes aux standards internationaux (ISO/IEC 27001, RGPD, NIST).

8.2.1 Politique de sécurité et confidentialité

Principes fondamentaux de cybersécurité :

- *Tous les mots de passe doivent être complexes : au moins 12 caractères, avec majuscules, chiffres et symboles*
- *L'authentification à double facteur (2FA) est obligatoire pour tous les services critiques (ERP, email, VPN…)*
- *Les accès distants sont autorisés uniquement via VPN sécurisé avec chiffrement*
- *Tous les postes, serveurs et périphériques doivent être protégés par un antivirus actif et un pare-feu à jour*
- *Les mises à jour de sécurité (système, logiciels, BIOS) doivent être automatiques et régulières*

Prévention contre les cyberattaques :

- *Tous les employés doivent suivre une formation annuelle obligatoire sur la cybersécurité (phishing, ransomware, gestion des mots de passe)*
- *Toute tentative de phishing ou de comportement suspect doit être signalée immédiatement au support IT*
- *Les connexions non autorisées, les alertes réseau ou les activités anormales doivent être analysées et bloquées sans délai*

Le respect de ces règles est indispensable pour garantir la confidentialité, l'intégrité et la disponibilité des données de NUBEM.

8.2.2 Politique de gestion et de sauvegarde des données

Chez NUBEM, la gestion des données sensibles repose sur des procédures strictes visant à garantir leur confidentialité, intégrité et traçabilité, tant au niveau interne qu'externe. Ces règles s'appliquent aux données RH, financières, commerciales et techniques.

Stockage et accès aux données sensibles :

- *Les fichiers critiques doivent être centralisés sur le serveur sécurisé (FILE-01) et non stockés localement sur les PC utilisateurs*
- *Les documents confidentiels (ex : RH, finance, direction) sont protégés par des droits d'accès spécifiques (ACL via Active Directory)*
- *Tout partage de fichiers vers l'extérieur (clients, fournisseurs) nécessite une autorisation préalable de la direction ou du DPO*

- *Tous les supports de stockage (disques durs externes, clés USB) doivent être chiffrés avec BitLocker ou VeraCrypt, selon la politique de l'entreprise*

Sauvegarde & plan de récupération des données :

- *Les données critiques sont sauvegardées quotidiennement sur un NAS Synology configuré en RAID 6*
- *Une sauvegarde hebdomadaire externalisée est effectuée via Veeam vers un datacenter certifié ISO 27001 (Infomaniak)*
- *Toutes les données sont restaurables pendant une période glissante de 90 jours (checkpoint, journaux de version)*

Ces mécanismes garantissent la conformité de NUBEM avec les normes RGPD et ISO/IEC 27002, tout en assurant une résilience forte face aux pertes de données ou aux cybermenaces.

8.3 Gestion des accès et des permissions

L'accès aux ressources informatiques de NUBEM est géré selon les principes de sécurité granulaire et centralisée, afin de prévenir toute exposition inutile des données ou des systèmes critiques. La stratégie repose sur l'approche Zero Trust, combinée à une administration automatisée via Active Directory.

8.3.1 Politiques de gestion des accès – approche Zero Trust

Principes fondamentaux appliqués :

- *Principe du moindre privilège (Least Privilege) : chaque collaborateur ne peut accéder qu'aux informations strictement nécessaires à ses fonctions professionnelles*
- *Audits trimestriels des permissions : revues automatiques des droits d'accès avec suppression des comptes inactifs, obsolètes ou non utilisés*
- *Gestion centralisée des identités via Active Directory avec intégration possible de SSO (Single Sign-On) pour les applications compatibles (ERP, sauvegarde, messagerie)*
- *Tous les accès administrateur ou critiques (serveur, firewall, ERP) nécessitent une authentification forte (2FA/MFA + PIN ou certificat)*
- *Les changements de rôle, départs et remplacements sont suivis via des workflows automatisés d'approbation IT*

Ces politiques garantissent une traçabilité complète des accès, une réduction des surfaces d'attaque internes, et une conformité avec les exigences RGPD en matière de protection des comptes utilisateurs.

8.3.2 Catégories d'accès & suivi des autorisations

L'accès aux ressources informatiques est structuré par rôles, selon une logique de **séparation des privilèges**, permettant de garantir une sécurité granulaire et une traçabilité des actions utilisateurs.

Catégories d'accès par profil :

Rôle	Accès autorisés	Restrictions
Utilisateur standard	Fichiers partagés de son service, messagerie, ERP	Aucun accès aux paramètres système, ni à d'autres services
Manager / Chef de service	Données RH/finance liées à son périmètre, rapports stratégiques	Aucun accès aux configurations réseau ou serveur
Administrateur IT	Pleins droits sur les serveurs, AD, réseau, sauvegarde	Pas d'accès aux documents RH confidentiels (GPO appliquée)
Visiteur / externe	Accès Wi-Fi invité isolé (SSID dédié) uniquement	Aucun accès aux fichiers, réseau ou systèmes internes
Sous-traitant / Prestataire	Accès temporaire à certains dossiers projet (via VPN ou réseau invité sécurisé)	Aucun accès permanent, comptes désactivés automatiquement après fin de mission

Suivi des accès et journalisation :

- ✓ *Toutes les connexions aux systèmes critiques sont **journalisées et archivées pendant 12 mois***
- ✓ *En cas de tentative d'accès non autorisé ou comportement suspect, une **alerte automatique est déclenchée***
- ✓ ***3 échecs de connexion consécutifs** entraînent un **verrouillage temporaire du compte***
- ✓ *Toute sortie d'un employé (fin de contrat ou mobilité interne) entraîne une **révocation automatique de ses accès** dans un délai de 24h*

Le système de gestion des rôles est intégré à **Active Directory**, avec une mise à jour automatique des autorisations à chaque changement de fonction.

8.4 Sanctions en cas de non-respect des règles informatiques

La charte informatique de NUBEM est un cadre obligatoire visant à protéger l'intégrité des systèmes, la confidentialité des données et la sécurité des opérations. Toute violation expose l'entreprise à des risques majeurs (RGPD, cybersécurité, réputation), et des sanctions strictes sont appliquées en cas de non-respect.

Typologie des sanctions graduées :

Niveau	Infraction constatée	Sanction appliquée
1	Usage non professionnel léger (navigation personnelle, installation d'un logiciel non validé)	Avertissement écrit avec rappel des règles
2	Récidive ou usage abusif des ressources IT (streaming, stockage perso, tentative de contournement GPO)	Suspension temporaire des droits d'accès + entretien RH
3	Fuite de données, piratage, usage frauduleux, contournement des contrôles de sécurité (BitLocker, VPN, pare-feu)	Sanction disciplinaire : mise à pied ou licenciement pour faute grave
4	Refus répété de se conformer aux procédures (MFA, AD, sauvegarde, PRA)	Signalement à la direction + audit IT + désactivation complète des accès

Mesures de traçabilité actives :

- ✓ *Tous les accès sont journalisés via Active Directory et analysés par PRTG + Zabbix.*
- ✓ *Les logs sont archivés 90 jours minimum (voir 8.3.2).*
- ✓ *Toute tentative suspecte déclenche une alerte automatique (cf. 4.6 et 8.4.2).*

Référence croisée :

→ Voir : Charte complète (section 8.1 à 8.4), Politique de gestion des accès (Annexe 10.5)

Conclusion de la Charte Informatique

La présente charte informatique constitue un pilier central de la gouvernance numérique de NUBEM. En fixant des règles claires, elle permet de :

Sécuriser l'infrastructure IT

→ Protection contre les menaces internes et externes (phishing, ransomware, erreurs humaines).
→ Intégration avec des solutions techniques telles que : BitLocker, Fortinet, VLAN, PRA.

Garantir un environnement de travail efficace

→ Prévention des interruptions via des règles d'usage responsable.
→ Maintien de la performance grâce à la supervision (PRTG, Zabbix) et à la standardisation du matériel.

Respect des normes et conformité légale

→ Alignement sur les exigences RGPD, ISO/IEC 27001, NIST.
→ Traçabilité des accès, audit régulier, suppression immédiate des comptes inactifs.

Engagement obligatoire de l'utilisateur

→ Chaque collaborateur doit signer ce document, attestant avoir lu, compris et accepté les règles.
→ L'accès aux ressources IT (poste, email, Wi-Fi, serveurs) n'est accordé qu'après signature.

Références associées :

Voir Politique de sécurité (8.3), Gestion des accès (8.4), Sanctions (8.5), Annexe 10.5 – Groupes AD et structure de fichiers sécurisés

Sommaire

9. CONCLUSION

Récapitulatif du Projet

Le projet IT de NUBEM constitue une **réussite stratégique complète**, réunissant innovation technologique, sécurité, performance et optimisation budgétaire. Il a été mené selon une méthode rigoureuse (AGIL + ITIL) et conforme aux standards internationaux (ISO 27001, RGPD).

Architecture moderne & robuste

- *Infrastructure virtualisée (Hyper-V) hébergeant 5 VM critiques.*
- *Réseau segmenté en VLANs sécurisés (VoIP, Wi-Fi invité, ERP).*
- *Salle serveur équipée (rack APC 42U, UPS, détection incendie, accès RFID).*

Sécurité et conformité avancées

- *Sécurité multicouche : pare-feu Fortinet 100F, BitLocker, 2FA, GPOs.*
- *Gestion centralisée des accès (AD, SSO, politique Zero Trust).*
- *Sauvegarde 3–2–1 avec PRA testée, NAS Synology + Veeam + Cloud externe.*

Performance opérationnelle

- *Réduction du temps d'accès aux données, connectivité Wi-Fi 6 pro.*
- *Monitoring 24/7 avec PRTG & Zabbix.*
- *Serveur Dell R750 optimisé (2x Xeon, RAID10, iDRAC, 10GbE).*

Maîtrise financière & ROI mesuré

- *Budget maîtrisé à 68'600 CHF (sous plafond 70k)*
- *Achat via 2 fournisseurs (Dell & Digitec) avec garanties ProSupport 5 ans*
- *ROI supérieur à 40% dès la 3ᵉ année grâce aux économies structurelles*

Facteurs clés de succès :

- *Dossier complet et structuré (matériel, Gantt, charte, PRA).*
- *Suivi agile et planification claire (12 semaines).*
- *Documentation et formation utilisateurs prévues.*

9.1. Pourquoi cette infrastructure est-elle idéale pour NUBEM ?

Une Infrastructure Sécurisée & Conforme

- *Pare-feu Fortinet 100F avec DPI, gestion VPN, ACLs et segmentation VLAN*
- *Accès centralisés via Active Directory (GPO, audit, MFA, Zero Trust)*
- *Sauvegarde 3–2–1 : NAS Synology RAID 6 + réplication locale + Cloud ISO 27001*
- *Surveillance continue avec PRTG & Zabbix – alertes automatiques*

Un Réseau Hautement Disponible

- *Double connectivité Internet (Fibre DFI 1Gbps + secours 5G Starlink auto-failover)*
- *Réseau structuré en VLANs : isolation des flux critiques (VoIP, ERP, invités)*
- *Wi-Fi 6 (UniFi U6-Pro) – sécurisé, scalable, compatible téléphonie IP*

Une Infrastructure IT Flexible & Scalable

- *Serveur Dell PowerEdge R750 virtualisé (Hyper-V), 5 VM stratégiques*
- *Standardisation des équipements (Dell, Cisco, APC) pour maintenance simplifiée*
- *Redondance planifiée (disques "cold spare", onduleur secondaire, rack extensible)*

Une Gestion Budgétaire Optimale & Durable

- *Coût total maîtrisé : 68'600 CHF, conforme au plafond 70k*

- *Tous les équipements critiques couverts 5 ans avec ProSupport+*
- *ROI prévisionnel > 40% sur 3 ans via réduction du TCO, éco-énergie, automatisation*

9.2 Comment NUBEM peut préserver cette excellence IT ?

Maintenance Préventive & Supervision Active

- *Application systématique des mises à jour critiques (OS, firmware, sécurité) via WSUS et Hyper-V*
- *Monitoring 24/7 des serveurs, VM, réseau et Wi-Fi avec PRTG et Zabbix*
- *Tests du Plan de Reprise d'Activité (PRA) chaque trimestre – scénarios simulés pour valider la résilience*
- *Vérifications mensuelles des logs systèmes et alertes de sécurité*

Formation Continue et Sensibilisation Sécurité

- *Programme annuel de formation cybersécurité obligatoire pour tous les utilisateurs*
- *Modules dédiés sur phishing, ransomwares, gestion des mots de passe et bonnes pratiques IT*
- *Intégration des nouveaux employés via un onboarding IT sécurisé et documenté*
- *Affiches et rappels internes réguliers (mailings, alertes contextuelles)*

Audit Interne & Amélioration Continue

- *Audits trimestriels sur les accès (Active Directory, GPO, permissions de fichiers)*
- *Mise à jour des politiques IT en fonction des évolutions réglementaires (RGPD, ISO 27001, NIST)*
- *Veille technologique : suivi des mises à jour produits Dell, Cisco, Fortinet*
- *Rapport de conformité annuel pour la direction, avec recommandations d'amélioration*

Conclusion Générale

Ce projet IT ne constitue pas une simple amélioration technique pour NUBEM, mais une **transformation digitale stratégique** à haute valeur ajoutée. Il positionne désormais l'entreprise dans un cadre sécurisé, évolutif et totalement aligné avec les meilleures pratiques mondiales.

Un projet de référence, car il :

- ✓ *S'appuie sur les normes ITIL, RGPD et ISO 27001 pour une gouvernance rigoureuse.*
- ✓ *Renforce la cybersécurité avec une infrastructure de niveau entreprise (Pare-feu Fortinet, PRA, surveillance 24/7).*
- ✓ *Optimise les coûts via une architecture virtualisée et un support 5 ans (Dell ProSupport).*
- ✓ *Assure un retour sur investissement mesurable dès la 2e année.*
- ✓ *Prépare l'avenir : scalabilité, intégration SaaS, cloud hybride, utilisateurs formés et engagés.*

L'entreprise ne subit plus les évolutions technologiques. Elle les anticipe.

Avec cette infrastructure robuste, NUBEM est aujourd'hui capable de croître avec **confiance, sécurité et agilité**.

MISSION ACCOMPLIE : UNE INFRASTRUCTURE IT INTELLIGENTE, ÉVOLUTIVE ET ULTRA-SÉCURISÉE.

10. ANNEXES TECHNIQUES

Introduction

Cette section regroupe l'ensemble des documents techniques du projet d'infrastructure IT de NUBEM. Elle constitue un référentiel complet destiné aux techniciens, partenaires et administrateurs pour assurer la continuité, la maintenance et l'évolutivité du système mis en place.

Objectifs des Annexes Techniques :

- *Fournir une traçabilité complète des configurations matérielles, logicielles et réseau.*
- *Documenter les choix technologiques avec leurs justifications (performances, compatibilité, coûts).*
- *Offrir une base fiable pour le dépannage, les audits ou les extensions futures.*
- *Faciliter le transfert de connaissance entre équipes techniques internes et prestataires externes.*

Contenu de cette section :

- *Schémas réseau logique et physique*
- *Tableaux de configuration des équipements (PC, serveurs, NAS, etc.)*
- *Déploiement des VM, sécurité AD et GPO*
- *Plan de sauvegarde détaillé avec PRA*
- *Planification de la maintenance et stratégie de supervision*
- *Justificatifs budgétaires avec captures et devis (Dell & Digitec)*

10.1. Diagramme du Réseau & Plan de VLANs

Topologie Générale de l'Infrastructure Réseau :
L'infrastructure réseau de NUBEM est structurée autour de composants professionnels assurant sécurité, performance et évolutivité.

Éléments Clés :

Équipement	Rôle Technique
Fortinet FortiGate 100F	Firewall centralisé – DPI, VPN, segmentation VLAN
Cisco Catalyst 9300	Switch cœur L3 – routage, VLANs, QoS, StackWise
Cisco SG350 (x2)	Switchs d'accès – connexions utilisateurs & imprimantes
UniFi U6 Pro	Wi-Fi interne (employés) + SSID isolé pour invités
VLAN IP Téléphonie	Séparé avec QoS activée pour appels VoIP

Diagramme visuel disponible dans Annexe 10.2.1

Segmentation VLAN et Plan d'Adressage IP :

VLAN	Département / Usage	Plage IP
10	Administration	192.168.10.0/24
20	Finance & RH	192.168.20.0/24
30	Commercial	192.168.30.0/24
40	Production & Logistique	192.168.40.0/24
50	Wi-Fi Interne Sécurisé	192.168.50.0/24
60	Téléphonie IP	192.168.60.0/24
70	Wi-Fi Visiteurs Isolé	192.168.70.0/24

Sommaire

Plan d'Adressage des Services IT :

- **Serveur DHCP :** 192.168.10.2 → Attribution dynamique par plage VLAN.
- **Contrôleur de Domaine (AD/DNS/DHCP) :** 192.168.10.10 → VM AD-01.
- **Passerelle par défaut :** 192.168.1.1 → Interface LAN du FortiGate.

10.2 Documentation de Configuration des Serveurs & Postes de Travail

10.2.1. Serveur virtualisé Dell PowerEdge R750 Rack Server:

Spécification	Détails
Modèle de Serveur	PowerEdge R750 Rack Server
Châssis	Jusqu'à 16 disques 2,5" SAS/SATA
Processeur	Intel® Xeon® Silver 4310, 12 Cœurs / 24 Threads, 2,1 GHz
Processeur Supplémentaire	Intel® Xeon® Silver 4310, 12 Cœurs / 24 Threads, 2,1 GHz
Mémoire	128 Go (4 x 32 Go RDIMM 3200 MT/s)
Configuration RAID	RAID 10 (6 SSDs)
Stockage	6 x 960 Go SSD SATA
Alimentation	2 x 1100W Titanium Redondant
Refroidissement	Ventilateurs haute performance x6
Adaptateur Réseau	Broadcom 57412, 2 x 10GbE BASE-T SFP+
Gestion	iDRAC9 Enterprise

Explication:

Le serveur Dell PowerEdge R750 a été retenu comme cœur de l'infrastructure pour sa performance, sa fiabilité et sa capacité d'évolution. Doté de deux processeurs Xeon Silver, de 128 Go de mémoire ECC, et de six SSD en RAID 10, il garantit à la fois puissance de calcul, rapidité d'accès aux données et sécurité. Ce choix permet de répondre efficacement aux besoins de virtualisation de NUBEM, en hébergeant les services critiques tels que l'Active Directory, les partages de fichiers et les applications métiers. Grâce à l'iDRAC9 pour la gestion à distance, une alimentation redondante de 1100W et une connectivité 10 GbE, ce serveur assure une haute disponibilité tout en restant dans un budget maîtrisé de 11'500 CHF.

Le serveur Hyper-V héberge plusieurs machines virtuelles critiques, notamment :

- Un contrôleur de domaine (Active Directory)
- Un serveur de fichiers centralisé
- Une base de données pour l'ERP interne

Chaque VM bénéficie de snapshots réguliers via la solution de sauvegarde DSM ou Veeam, et les performances sont réparties grâce à la configuration bi-processeur et 128 Go de RAM. Cette architecture garantit une haute disponibilité des services numériques de NUBEM.

Utilité du serveur – Virtualisation

Utilité : Hébergement des services critiques de l'entreprise (Active Directory, partages de fichiers, ERP). Voir détails en **Annexe 10.5**.

Machines virtuelles déployées : 5 machines virtuelles (VM)

Nom VM	Rôle	Ressources allouées
AD-01	Active Directory / DNS / DHCP	4 vCPU, 16 Go RAM, 100 Go HDD
FILE-01	Partage de fichiers (SMB)	4 vCPU, 32 Go RAM, 1 To HDD
SAGE-ERP	Gestion comptable & logistique	6 vCPU, 64 Go RAM, 500 Go HDD
BACKUP-01	Sauvegarde & PRA (Veeam)	2 vCPU, 16 Go RAM, 500 Go HDD
MONITOR-01	Supervision & alertes (PRTG/Zabbix)	2 vCPU, 8 Go RAM, 250 Go HDD

Sommaire

Configuration des Postes de Travail :

10.2.2. Dell Latitude 7450 (Direction & Commercials):

Catégorie	Détail sélectionné
Modèle	Dell Latitude 7450 – 14 pouces
Processeur	Intel® Core™ Ultra 7 165U vPro® (12 cœurs, jusqu'à 4,9 GHz Turbo, AI Boost)
Mémoire vive	32 Go LPDDR5x, 6 400 MT/s (intégrée)
Stockage	SSD 512 Go M.2 2230, PCIe NVMe Gen 4
Écran	14", FHD+ (1920×1200), IPS, non tactile, anti-reflet, 250 nits
Caméra	Caméra infrarouge HDR FHD, reconnaissance faciale, TNR, obturateur physique
Audio	Micro intégré, haut-parleurs stéréo
Connectivité sans fil	Wi-Fi 6E, Bluetooth 5.x
Ports disponibles	USB-C, USB-A, HDMI (via adaptateur), jack audio, lecteur SmartCard
Sécurité physique	Lecteur d'empreintes digitales, lecteur de carte à puce (contact/sans contact), NFC
TPM	TPM 2.0 (discret, activé)
Batterie	3 cellules, 57 Wh, ExpressCharge™ Boost compatible
Adaptateur secteur	65W USB-C, EcoDesign
Gestion à distance	Intel® vPro® Enterprise – prise en charge complète
Système d'exploitation	Windows 11 Professionnel, multilingue
Service de garantie	Dell ProSupport, 5 ans avec intervention sur site le jour ouvré suivant
Protection complémentaire	Option Keep Your Hard Drive (5 ans), service batterie étendu (3 ans)

Annexe technique – Justification du choix de l'ordinateur portable Dell Latitude 7450

Le Dell Latitude 7450 a été sélectionné pour sa parfaite adéquation avec les exigences d'un usage professionnel moderne. Équipé d'un processeur Intel Core Ultra vPro, de 32 Go de RAM performante et d'un SSD PCIe Gen 4, il offre puissance, rapidité et sécurité dans un format compact et robuste.

Sa compatibilité avec la gestion centralisée (Active Directory, GPO), sa garantie ProSupport 5 ans et l'option de conservation du disque dur en font une solution conforme aux standards IT et RGPD. Ce choix garantit une performance durable sur 3 à 5 ans, sans surcoûts de support ni contraintes de scalabilité, tout en respectant le budget du projet NUBEM.

Le Dell Latitude 7450 a été sélectionné pour sa parfaite adéquation avec les exigences d'un usage professionnel moderne. Équipé d'un processeur Intel Core Ultra vPro, de 32 Go de RAM performante et d'un SSD PCIe Gen 4, il offre puissance, rapidité et sécurité dans un format compact et robuste.

Sa compatibilité avec la gestion centralisée (Active Directory, GPO), sa garantie ProSupport 5 ans et l'option de conservation du disque dur en font une solution conforme aux standards IT et RGPD.Ce choix garantit une performance durable sur 3 à 5 ans, sans surcoûts de support ni contraintes de scalabilité, tout en respectant le budget du projet NUBEM.

10.2.3 Dell OptiPlex 7020 (Administratif & Support)

Catégorie	Détail sélectionné
Modèle	Dell OptiPlex Tower 7020
Processeur	Intel® Core™ i5-14500 vPro® (14 cœurs / 20 threads, 24 Mo cache, jusqu'à 5.0 GHz)
Mémoire vive (RAM)	16 Go DDR5 – 1 x 16 Go (extensible à 64 Go)
Stockage principal	SSD 512 Go M.2 PCIe NVMe (classe 35, format 2230)
Carte graphique	Intel UHD Graphics intégrée
Système d'exploitation	Windows 11 Professionnel (licence multilingue)
Châssis	Format tour avec alimentation 300W Platinum
Connectivité sans fil	Aucune (connexion Ethernet filaire uniquement)
Ports vidéo supplémentaires	Aucun (sortie DisplayPort standard intégrée)
Clavier / Souris	Dell Pro KM5221W – Clavier et souris sans fil (QWERTZ, Suisse)
Sécurité physique	Module TPM 2.0, commutateur d'intrusion de boîtier, WatchDog SRV
Gestion	Intel® vPro® Enterprise + Intel AMT
Protection contre la poussière	Filtre antipoussière (sur postes critiques)
Garantie	5 ans Dell ProSupport – Intervention sur site après diagnostic à distance
Protection contre dommages accidentels	Oui – Garantie ADP 5 ans (chutes, liquides, surtensions)
Accessoires inclus	Câble d'alimentation suisse, documentation multilingue

Résumé de la configuration retenue :

Le Dell OptiPlex 7020 a été retenu comme poste de travail principal pour sa compatibilité parfaite avec l'environnement IT de NUBEM, incluant Active Directory, GPO, SAGE et les outils bureautiques.

Sa configuration évolutive (RAM extensible, ports PCIe, châssis modulaire) permet une adaptation facile aux besoins futurs.

Avec un processeur Intel i5 de 14e génération, un SSD NVMe rapide et des fonctions de sécurité avancées (TPM 2.0, vPro, protection physique), ce modèle allie performance, sécurité et fiabilité.

La garantie ProSupport 5 ans, accompagnée d'une protection contre les dommages accidentels, assure une continuité d'activité optimale, même dans des environnements exigeants comme les points de vente.

10.2.4 Écrans Dell Pro 27 Plus Monitor - P2725D

Catégorie	Détail sélectionné
Modèle	Dell Pro 27 Plus – P2725D
Taille de l'écran	27 pouces (68,6 cm)
Résolution native	QHD – 2560 × 1440
Type de dalle	IPS – antireflet, rétroéclairage LED
Format d'image	16:9
Luminosité	350 cd/m²
Contraste	1000:1 (typique)
Angles de vision	178° (horizontal/vertical)
Fréquence de rafraîchissement	60 Hz
Connectique	1x HDMI 1.4, 1x DisplayPort 1.2, 4x USB 3.2 (2 en amont, 2 en aval)
Ergonomie	Réglable en hauteur, rotation, pivot, inclinaison
Fixation murale	Compatible VESA 100 × 100 mm
Certification de confort visuel	TÜV Rheinland – Low Blue Light (Confort oculaire 4 étoiles)
Certifications environnementales	ENERGY STAR, EPEAT Gold, TCO
Accessoires fournis	Câble d'alimentation, câble DisplayPort, documentation
Garantie	5 ans ProSupport (même que les PC fixes)

Explication du Projet

Annexe technique – Justification du choix des écrans Dell Pro 27 Plus QHD (P2725D)

Le Dell P2725D a été choisi pour offrir un équilibre idéal entre confort visuel, productivité et compatibilité avec les unités centrales sélectionnées.

Sa résolution QHD de 27 pouces permet d'afficher plusieurs applications simultanément (comptabilité, gestion commerciale, etc.) tout en restant ergonomique grâce à son pied ajustable et son traitement anti-reflet certifié TÜV.

Intégrant un hub USB et une connectique complète (HDMI, DP), il simplifie l'installation et s'adapte facilement aux environnements multi-postes.

Moins coûteux qu'un écran 4K mais bien supérieur au Full HD, ce modèle constitue un excellent compromis qualité/prix avec une garantie ProSupport de 5 ans incluse.

10.2.5 Dell Universal Dock | UD22 |130W

Catégorie	Détail sélectionné
Modèle	Dell Universal Dock – UD22
Référence Dell	210-BEYV
Référence fabricant	MHWPN
Type de connexion	USB-C universel (alimentation, données, vidéo via un seul câble)
Puissance d'alimentation	Jusqu'à 96 W (130 W total avec adaptateur fourni)
Sorties vidéo	2 × DisplayPort 1.4, 1 × HDMI 2.0, 1 × USB-C DisplayPort Alt Mode
Résolution max. prise en charge	Jusqu'à 5K @ 60 Hz (double affichage)
Ports USB	1 × USB-C Gen 2 avec Power Delivery

La station d'accueil Dell UD22 a été sélectionnée pour sa compatibilité universelle via USB-C et sa capacité à simplifier le poste de travail mobile. Elle permet de connecter deux écrans 5K, fournit jusqu'à 96W d'alimentation, et centralise toutes les connexions (écrans, USB, réseau) via un seul câble.

Sa compatibilité multi-OS garantit une flexibilité à long terme, tandis que sa standardisation sur tous les postes mobiles facilite la maintenance et réduit les coûts. Proposée à un tarif compétitif, la UD22 représente un choix cohérent, ergonomique et durable pour accompagner les portables professionnels comme le Dell Latitude 7450.

10.2.6 Souris sans fil mobile Dell - MS3320W - noire

Catégorie	Détail sélectionné
Modèle	Dell Souris Mobile Sans Fil – MS3320W (noire)
Connectivité	Double mode : RF 2.4 GHz (dongle USB) + Bluetooth 5.0
Type de capteur	Optique – résolution 1600 DPI
Alimentation	1 pile AA (fournie) – autonomie jusqu'à 36 mois
Design	Compact, ambidextre, discret – usage bureautique et mobile
Compatibilité	Windows, macOS, Linux, ChromeOS
Technologie Plug & Play	Oui, aucun pilote requis
Dimensions	58 x 100 x 38 mm (approx.) – poids léger
Couleur	Noir – finition professionnelle
Nombre commandé	5 unités (4 utilisateurs + 1 de réserve)
Utilisation prévue	Postes portables Dell Latitude 7450
Objectif	Améliorer la productivité et l'ergonomie en mobilité et au bureau

La souris Dell MS3320W a été choisie pour sa simplicité, sa fiabilité et son adaptation parfaite aux usages professionnels. Compacte, ergonomique et silencieuse, elle fonctionne en Bluetooth ou avec dongle USB sans configuration complexe.

Son format discret convient aussi bien au travail mobile qu'au bureau. Standardisée sur l'ensemble des portables du projet, elle garantit une homogénéité et une maintenance simplifiée. Proposée à un prix abordable (~25 CHF), elle offre un excellent rapport qualité/prix tout en respectant les contraintes budgétaires et les politiques IT de l'entreprise.

10.2.7 Cisco CATALYST 9300 48-PORT POE+

Catégorie	Détail sélectionné
Modèle	Cisco Catalyst 9300 – 48-Port PoE+
Référence	C9300-48P
Type	Commutateur manageable, empilable (StackWise), niveau 3 (Layer 3)
Nombre de ports	48 × RJ45 10/100/1000 Mbps (PoE+)
Budget PoE	Jusqu'à 740W (alimentation périphériques via Ethernet)
Ports uplink (modulaires)	1 slot d'extension (modules SFP/SFP+)
Fonctionnalités clés	VLAN, QoS, ACL, routage inter-VLAN, DHCP relay, IGMP, MSTP
Sécurité	TrustSec, MACsec, 802.1X, segmentation dynamique
Redondance	Support de StackWise (jusqu'à 9 unités), double alimentation (optionnelle)
Gestion	CLI, WebUI, SNMP, Cisco DNA Center
Systèmes supportés	Compatible avec tout environnement réseau standard (RAK, collectivité, éducation)
Garantie	5 ans Bring-in (échange standard)
Date de livraison prévue	Entre le 15/05 et le 21/05
Nombre commandé	1 unité
Utilisation prévue	Switch cœur de réseau – infrastructure principale
Conformité	Aligné avec les standards Cisco pour les collectivités et infrastructures critiques

Le switch Cisco Catalyst 9300 a été retenu pour structurer le cœur du réseau de manière évolutive, sécurisée et durable. Capable de gérer jusqu'à 48 périphériques avec alimentation PoE+ (740W), il offre une gestion avancée des VLANs, du routage inter-VLAN, et une compatibilité totale avec un environnement Active Directory.

Sa modularité via l'empilement (StackWise) permet une extension sans reconfiguration majeure. Pour un coût maîtrisé de 4'260 CHF, il apporte performance, sécurité (802.1X, ACL, TrustSec) et pérennité, avec une gestion centralisée et un support à long terme. Un choix stratégique pour un réseau d'entreprise stable et évolutif.

10.2.8 Synology DS1823xs+

Catégorie	Spécification
Modèle	Synology DS1823xs+
Format	Tour (Desktop NAS)
Système d'exploitation	Synology DiskStation Manager (DSM)
Processeur	AMD Ryzen V1780B – 4 cœurs / 8 threads, 3.35 GHz (boost jusqu'à 3.8 GHz)
Mémoire vive (RAM)	8 Go DDR4 ECC, extensible jusqu'à 32 Go
Baies de disques	8 × 3.5"/2.5" SATA HDD ou SSD
Capacité maximale brute	Jusqu'à 108 To (avec disques 18 To)
Configuration RAID supportée	RAID 0, 1, 5, 6, 10, JBOD
Emplacements d'extension	1 × eSATA pour unité RX (jusqu'à 10 disques supplémentaires)
Ports réseau	4 × RJ45 Gigabit Ethernet (agrégation prise en charge)
Slot d'extension réseau	1 × slot PCIe Gen3 ×8 (pour carte 10GbE ou M.2 SSD cache)
Ports USB	3 × USB 3.2 Gen 1 (Type-A)
Performance maximale	+2 300 Mo/s en lecture, +1 000 Mo/s en écriture (avec agrégation et SSD cache)
Chiffrement matériel	Oui, via AES-NI (cryptage matériel intégré)
Fonctions avancées	Snapshots, réplication, sauvegarde active, virtualisation (VM, Docker), LDAP
Ventilation	2 × ventilateurs 120 mm (redondants, remplacement facile)
Consommation électrique	61.13 W (en fonctionnement), 25.27 W (veille HDD)
Niveau sonore	25.2 dB(A)
Garantie constructeur	5 ans
Dimensions (L × P × H)	343 mm × 243 mm × 166 mm
Poids	6.0 kg (sans disques)

Le Synology DS1823xs+ a été sélectionné pour centraliser les sauvegardes, sécuriser les données et accompagner la croissance future de NUBEM. Avec ses 8 baies disques, son support RAID 6 et son processeur AMD performant, il combine évolutivité et tolérance aux pannes.

Sa gestion simplifiée via l'interface DSM permet d'automatiser les sauvegardes de tous les postes, tout en assurant une compatibilité avec des outils professionnels comme Veeam ou rsync. À un coût maîtrisé (1'580 CHF hors disques), il constitue une solution fiable, flexible et parfaitement adaptée aux environnements sans baie serveur. Ce NAS devient un composant clé de la stratégie de protection des données du projet.

Cette réduction de capacité est due à la structure du RAID 6 : deux disques sont réservés à la redondance des données. Ainsi, seuls 6 disques sur 8 sont effectivement utilisables pour le stockage réel. De plus, deux disques de rechange ("cold spares") sont également prévus pour garantir un remplacement immédiat en cas de panne, sans interruption de service.

10.2.9 WD Red Pro 8 To, 3.5", CMR

Caractéristique	Détail
Modèle	WD Red Pro 8 To
Format	3.5" SATA
Technologie d'enregistrement	✅ CMR (Conventional Magnetic Recording)
Capacité unitaire	8 To
Nombre de disques utilisés	8 (dans un NAS Synology DS1823xs+) (l'ajout de deux disques WD Red Pro supplémentaires en tant que pièces de rechange ("cold spares") est envisagé.)
Capacité totale brute	64 To (8 × 8 To)
Capacité utile avec RAID6	≈ 48 To
Vitesse de rotation	7 200 tr/min
Mémoire cache	256 Mo
Charge de travail annuelle (MTBF)	300 To/an – optimisé pour environnements multi-utilisateurs NAS
Utilisation recommandée	NAS 24/7, RAID, environnements bureautiques intensifs
Tolérance aux vibrations	Oui – RV sensors intégrés
Garantie constructeur	5 ans
Compatibilité Synology	✅ Certifiée pour usage avec DSM / RAID6

Les disques WD Red Pro 8 To ont été sélectionnés pour équiper le NAS Synology, offrant une combinaison optimale de performance, fiabilité et capacité. Avec 8 unités configurées en RAID 6, **la solution assure 48 To utiles**, une tolérance à double panne et une évolutivité adaptée aux besoins croissants des 17 postes de travail.

Conçus pour un usage 24/7 en environnement NAS, ces disques (7 200 tr/min, cache 256 Mo, garantie 5 ans) garantissent une haute résilience et une intégration parfaite avec les fonctions avancées de Synology DSM. Proposés à un tarif maîtrisé (~203 CHF l'unité), ils constituent une base de stockage robuste et durable pour l'infrastructure du projet.

10.2.10 StarTech étagère Fixe 2u 22in Pour Montage En Rack

Caractéristique	Détail
Modèle	StarTech Fixed Rack Shelf – 2U, 22 pouces
Type	Étagère fixe pour armoire rack 19"
Hauteur	2U (standard rack height)
Profondeur	22 pouces (~56 cm)
Largeur	Compatible rack 19" standard
Capacité de charge	Jusqu'à 50–56 kg (selon le fabricant)
Matériau	Acier galvanisé robuste
Compatibilité	NAS, UPS, routeurs, commutateurs, autres équipements non-rack
Fixation	Montage à 4 points, vis incluses
Ventilation	Trous de dissipation de chaleur (selon modèle)
Utilisation recommandée	Installation de Synology DS1823xs+ dans baie réseau
Prix constaté	Environ 80.90 CHF (Digitec)

Sommaire

Afin d'intégrer le NAS Synology dans une baie réseau standard 19", nous avons opté pour l'étagère fixe StarTech 2U – 22 pouces, compatible et parfaitement dimensionnée. Robuste (charge > 50 kg), elle permet l'installation d'équipements non rackables tels que NAS, onduleurs ou routeurs, tout en assurant stabilité et évolutivité. À un prix raisonnable (~80 CHF), elle constitue une solution économique et durable, parfaitement adaptée à l'environnement professionnel ciblé, notamment dans un contexte mixte rack/non-rack. Ce choix garantit une organisation physique propre, évolutive et conforme aux bonnes pratiques IT.

10.2.11 APC SRT 5000VA / 4500W

Caractéristique	Détail
Modèle	APC Smart-UPS SRT 5000VA
Type d'onduleur	Online – double conversion (Double Conversion en ligne)
Capacité de sortie	5000 VA / 4500 W
Tension de sortie nominale	230 V – standard européen
Forme d'onde de sortie	Sinusoïdale pure (pure sine wave)
Format physique	Rackmount (3U) ou convertible tour
Connectiques	6 × IEC C13, 1 × IEC C19, port USB, port série, SmartSlot
Écran de contrôle	LCD avec navigation multilingue
Batterie	Remplaçable à chaud (hot-swappable), extensible avec packs externes
Gestion à distance	SNMP, USB, SmartSlot, compatible PowerChute et DSM
Compatibilité NAS / réseau	Synology DSM, switch Cisco, postes fixes
Poids approximatif	~54 kg
Dimensions (L × H × P)	~43.2 × 13.0 × 68.3 cm
Garantie constructeur	3 ans standard (extensible)
Prix constaté (Digitec)	~CHF 3 500.– (mai 2025)

Pour garantir la continuité énergétique de l'infrastructure critique, le projet intègre l'onduleur APC Smart-UPS SRT 5000VA, une solution professionnelle en double conversion. Avec une puissance de 5000 VA, il alimente de manière sécurisée le NAS Synology, les switchs Cisco et les équipements réseau, tout en anticipant l'évolution future. Sa technologie on-line assure une protection optimale contre les coupures et variations, évitant toute perte de données ou redémarrage intempestif. Intégrable au rack 19" et pilotable via DSM/SNMP, il offre un excellent compromis entre performance, résilience et coût (~3'500 CHF), en parfaite adéquation avec les exigences de disponibilité du projet.

10.2.12 Fortinet FortiGate 100F

Caractéristique	Détail
Modèle	FortiGate 100F
Type de pare-feu	NGFW – Next Generation Firewall (pare-feu de nouvelle génération)
Débit pare-feu (firewall throughput)	Jusqu'à **20 Gbps**
Débit VPN IPsec	Jusqu'à **1 Gbps**
Interfaces	10 × RJ45 GE, 4 × SFP, 2 × SFP+, console, USB
Utilisateurs recommandés	20 à 50 utilisateurs actifs
Gestion VLAN / segmentation	Oui – support complet 802.1Q, routage inter-VLAN
VPN	SSL VPN et IPsec avec accélération matérielle
Protection UTM (optionnelle)	IPS, antivirus, filtrage web, antispam (avec FortiGuard)
Système d'exploitation	FortiOS (accès via interface web, CLI ou FortiManager)
Format	Montable en rack 1U
Support / mises à jour	Via FortiCare (en option)
Prix constaté – appareil seul	~CHF 1 150.– (Router-switch.com, hors TVA/douane)
Prix constaté – bundle 1 an UTM	~CHF 3 600.– (Digitec, incluant FortiGuard + FortiCare)
Compatibilité réseau projet	Cisco Switches, Synology NAS, Dell postes fixes/portables

Le pare-feu Fortinet FortiGate 100F a été retenu comme appliance de sécurité réseau centralisée pour sa capacité à protéger l'infrastructure de manière évolutive et performante. Ce NGFW intègre DPI, contrôle applicatif, VPN SSL/IPsec et, si activé, les services UTM FortiGuard. Grâce à ses 10 interfaces Ethernet et sa compatibilité VLAN/QoS, il permet une segmentation fine du réseau (serveurs, postes, invités). Proposé à ~1'150 CHF sans licence ou ~3'600 CHF avec bundle FortiGuard, il garantit jusqu'à 20 Gbps de débit brut et un usage fluide pour 20–50 utilisateurs. Ce choix sécurise l'accès distant, isole les flux sensibles et complète parfaitement l'architecture Cisco/NAS/portables définie dans le projet.

Le FortiGate assure le routage inter-VLAN et applique des règles ACL (Access Control Lists) strictes pour interdire les communications non autorisées entre les différents segments (IoT, visiteurs, administration). Cette politique de filtrage limite les risques de propagation d'attaques internes ou d'accès indésirable.

10.2.13 For Armoire serveur APC NetShelter SX 42U

Caractéristique	Détail
Modèle	APC NetShelter SX 42U
Format rack	42U – Standard 19 pouces
Dimensions (L × P × H)	600 mm × 1070 mm × 1991 mm
Capacité de charge statique	Jusqu'à 1364 kg
Profondeur utile de montage	Environ 915 mm
Matériaux	Acier thermolaqué, structure renforcée
Ventilation	Portes avant et arrière perforées – refroidissement passif prêt
Panneaux latéraux	Amovibles, accès rapide à l'intérieur
Système de verrouillage	Portes avant/arrière verrouillables
Compatibilité équipements	Dell UPS, Cisco switchs, FortiGate, Synology NAS, PDU, rails
Gestion des câbles	Système de passage de câbles haut/bas intégré
Montage au sol	Sur roulettes et pieds réglables
Prix constaté (Digitec)	Environ **CHF 1 500.–**

L'armoire APC NetShelter SX 42U a été choisie pour centraliser de manière sécurisée l'ensemble de l'infrastructure critique : NAS, pare-feu, switchs, onduleurs et accessoires. Avec ses 42U, une charge maximale de 1'364 kg et des dimensions adaptées aux équipements professionnels, elle permet une installation ordonnée, évolutive et conforme aux standards 19". Son design robuste avec portes perforées assure une ventilation passive efficace, tandis que les panneaux verrouillables garantissent la sécurité physique. Proposée à 1'500 CHF, elle représente une solution fiable et durable, parfaitement intégrée aux équipements Dell, Cisco, Fortinet et Synology déployés dans le projet.

10.2.14 Digitus 24 Port Cat6A Patch Panel

Caractéristique	Détail
Modèle	Digitus DN-91624S-EA
Type	Panneau de brassage (patch panel)
Nombre de ports	24 ports RJ45 (8P8C)
Catégorie	Cat6A – jusqu'à 10 Gbit/s
Blindage	Oui – STP (Shielded Twisted Pair)
Format	19 pouces – 1U
Connexion arrière	LSA / IDC
Matériau	Acier, finition thermolaquée noire
Compatibilité rack	Armoire serveur 19" (ex. APC NetShelter SX 42U)
Normes	ISO/IEC 11801, EN 50173, ANSI/TIA-568-C.2
Application typique	Connexions utilisateurs, AP Wi-Fi, imprimantes, infrastructure
Prix constaté	Environ **CHF 54.– / unité**

Le panneau de brassage Digitus Cat6A – 24 ports a été sélectionné pour structurer proprement les connexions réseau tout en garantissant performance et évolutivité. Conforme à la norme Cat6A (jusqu'à 10 Gbit/s), il permet une gestion centralisée des câbles issus des postes, Wi-Fi, imprimantes, NAS et pare-feu, tout en protégeant les ports des switchs. Installé dans l'armoire APC 42U, il s'intègre parfaitement avec les équipements Cisco, Fortinet et Synology. Grâce à son étiquetage clair et sa modularité, il facilite la maintenance, les diagnostics, et les évolutions futures du réseau, le tout pour un coût maîtrisé (~150 CHF par unité).

10.2.15 APC Smart-UPS SRT 96V 3kVA / 3000W

Caractéristique	Détail
Modèle	APC Smart-UPS SRT 96V 3kVA
Type d'onduleur	Online – double conversion (double convertisseur) ✅
Capacité de sortie	3000 VA / 3000 W – puissance effective totale ✅
Batterie	Hot-swappable, extensible avec modules externes
Format physique	Rackmount / tour – compatible baie 19"
Connectiques	USB, série, SmartSlot, sorties IEC
Affichage	Écran LCD multilingue
Gestion à distance	Compatible SNMP, PowerChute, Synology DSM
Utilisation recommandée	Switchs, routeurs, AP Wi-Fi, postes critiques ✅
Prix estimé	~1 400 CHF (Digitec, 2025)
Garantie	3 ans constructeur, extensible

L'APC Smart-UPS SRT 3000VA a été intégré en complément du modèle principal 5kVA pour assurer une redondance énergétique stratégique. Il protège les équipements intermédiaires (switchs, routeurs, postes sensibles) via une alimentation en double conversion, sans interruption en cas de perturbation électrique. Facilement monté en rack 19", il s'intègre aux outils de supervision réseau et aux NAS Synology. Offrant 3'000 W de puissance à un prix compétitif, avec des batteries remplaçables à chaud, il renforce la résilience de l'infrastructure tout en respectant les bonnes pratiques de continuité de service.

10.2.16 Ubiquiti Caméra vidéo UniFi, IR, dôme G5, PoE actif, pack de 3

Caractéristique	Détail
Modèle	Ubiquiti UniFi G5 Dome
Type	Caméra IP dôme, usage intérieur
Résolution	2688 × 1512 pixels (2K+)
Vision nocturne	Oui – Infrarouge (IR)
Angle de vision	102,4° horizontal, 52,6° vertical
Connectivité	Ethernet RJ45
Alimentation	PoE actif (802.3af) – Pas d'alimentation externe nécessaire
Gestion centralisée	Oui – Compatible avec UniFi Protect Controller
Enregistrement vidéo	Sur NVR UniFi ou sur serveur NAS (Synology ou équivalent)
Installation	Plafond ou mur – Intérieur uniquement
Indice de protection	IPX4 (résistance aux éclaboussures)
Prix constaté	~507 CHF le pack de 3 (≈169 CHF / unité)
Utilisation prévue	Surveillance de la salle serveur, contrôle d'accès, sécurité passive
Nombre de caméras installées	3 unités : entrée, vue générale, redondance/zone critique

Pour renforcer la sécurité physique de la salle serveur, le projet intègre trois caméras Ubiquiti UniFi G5 Dome avec vision nocturne, résolution 2K+ et alimentation PoE. Ces caméras offrent une surveillance continue, dissuadent les intrusions et permettent une traçabilité vidéo conforme au RGPD. Gérées via UniFi Protect, elles couvrent l'entrée et l'intérieur de la salle, tout en laissant la possibilité d'extension future. Le pack, proposé à ~507 CHF, constitue une solution fiable, professionnelle et évolutive, parfaitement cohérente avec l'approche de sécurisation globale de l'infrastructure IT.

10.2.17 AKCP THS00 - Capteur de température et d'humidité

Caractéristique	Détail
Modèle	AKCP THS00
Type de capteur	Température et humidité combinées
Plage de température	-55 °C à +75 °C
Plage d'humidité	0 % à 100 % HR
Précision	±1 °C (sensorProbe) / ±0,5 °C (sensorProbe+)
Connectique	RJ45 Plug-and-Play
Longueur de câble	1,5 m (extensible jusqu'à 300 m via câble CAT5)
Interface de gestion	Compatible avec AKCP sensorProbe, sensorProbe+ et securityProbe
Alertes	Seuils configurables – alertes automatiques (mail, SNMP, etc.)
Installation	Rapide, sans logiciel – reconnaissance automatique par le système
Prix constaté	~156 CHF
Utilisation prévue	Surveillance de salle serveur / armoire réseau

Sommaire

Le capteur environnemental AKCP THS00 a été intégré pour surveiller en continu la température et l'humidité dans la salle serveur, permettant de prévenir tout risque de surchauffe ou de condensation. Connecté au contrôleur sensorProbe+, il déclenche automatiquement des alertes en cas de dépassement de seuils. Facile à installer (RJ45 plug-and-play) et extensible à d'autres capteurs (fumée, fuite, intrusion), il s'intègre aux systèmes SNMP/Web/API. Proposé à ~156 CHF, ce capteur assure une protection fiable, évolutive et économique des équipements critiques de l'infrastructure NUBEM.

10.2.18 Promag ER755 et Lecteur RFID Badge RFID Mifare

Composant	Détail
Lecteur RFID	Promag ER755
Type de connexion	Ethernet RJ45 – TCP/IP
Fréquence	13,56 MHz (Haute Fréquence – HF)
Protocoles pris en charge	ISO/IEC 14443A (Mifare Classic, UID)
Montage	Fixation murale ou rack (selon besoin)
Badges fournis	10 × 2N Mifare Classic 1K (13,56 MHz, 1 Ko mémoire sécurisée)
Compatibilité logicielle	Logiciels de gestion d'accès tiers (via API ou export CSV/log)
Fonctionnalité	Lecture des identifiants, déclenchement de relais ou enregistrement
Utilisation recommandée	Contrôle d'accès pour salle serveur, racks IT, bureaux techniques
Scalabilité	Ajout illimité de badges et lecteurs supplémentaires possible
Prix estimé	Lecteur ≈ 145 CHF / Pack 10 badges ≈ 40 CHF

Le système de contrôle d'accès Promag ER755, associé aux badges Mifare Classic 1K, permet de sécuriser efficacement les zones techniques sensibles (salle serveur, armoire réseau) via une authentification RFID sans contact. Facilement intégrable au réseau via RJ45, il offre une gestion centralisée des accès et une traçabilité complète des entrées. Modulaire et évolutif, il peut s'adapter aux besoins futurs sans frais cachés. Pour un coût global de ~185 CHF, cette solution professionnelle et économique renforce la sécurité physique de l'infrastructure IT NUBEM.

10.2.19 Gloria Extincteur au dioxyde de carbone

Caractéristique	Valeur
Modèle	Gloria – Extincteur au dioxyde de carbone
Capacité	2 kg CO_2
Type de feu couvert	Classes B (liquides), C (gaz) – adapté aux installations IT
Mode d'action	Refroidissement + déplacement de l'oxygène
Aucun résidu	Oui – ne laisse aucun dépôt, protège le matériel
Certifications	Conforme aux normes européennes (EN3)

Pour assurer la sécurité incendie sans compromettre les équipements IT, le projet intègre deux extincteurs CO_2 Gloria, adaptés aux risques électriques. Contrairement aux modèles à poudre ou à eau, ces extincteurs n'endommagent pas le matériel électronique et ne laissent aucun résidu. Compacts, faciles à utiliser, et conformes aux normes professionnelles, ils couvrent efficacement la salle serveur et la baie réseau. À ~90 CHF l'unité, cette solution économique complète la stratégie de sécurité globale du projet NUBEM.

10.2.20 HP M479fdw Color LaserJet Pro

Caractéristique	Détail
Type	Imprimante multifonction laser couleur (4-en-1)
Fonctions	Impression, copie, numérisation, fax
Connectivité	USB 2.0, Ethernet Gigabit, Wi-Fi, Wi-Fi Direct
Vitesse d'impression	Jusqu'à 27 pages par minute (ppm)
Résolution d'impression	600 x 600 ppp (jusqu'à 38 400 x 600 optimisé pour couleur)
Volume mensuel recommandé	750 – 4 000 pages
Capacité d'entrée papier	300 feuilles (extensible jusqu'à 850 avec bac en option)
Chargeur automatique de documents	Oui (ADF 50 feuilles, recto-verso)
Écran	Tactile couleur 4,3"
Compatibilité OS	Windows, macOS, Linux, iOS, Android
Sécurité	Impression sécurisée, JetAdvantage Security
Dimensions / Poids	416 x 472 x 400 mm / ~23.4 kg
Certifications	ENERGY STAR®, Blue Angel, EPEAT Silver

L'imprimante multifonction HP Color LaserJet Pro MFP M479fdw a été choisie pour sa polyvalence et sa fiabilité en environnement bureautique. Elle couvre les besoins d'impression, de numérisation, de copie et de fax avec une connectivité complète (Ethernet, Wi-Fi, USB) et une vitesse de 27 ppm. Son ADF, sa compatibilité avec HP JetAdvantage et sa gestion du papier évolutive assurent une productivité optimale. Économique à l'usage grâce aux toners grande capacité et à son efficacité énergétique, elle représente un choix équilibré entre performance, coût et qualité pour les besoins de NUBEM.

10.2.21 Ubiquiti UniFi 6 Professional (U6-PRO)

Caractéristique	Détail
Modèle	UniFi 6 Professional (U6-PRO)
Type	Point d'accès Wi-Fi 6 professionnel
Norme Wi-Fi	802.11ax (Wi-Fi 6)
Débit max	5.3 Gbps total (4.8 Gbps sur 5 GHz, 573 Mbps sur 2.4 GHz)
MIMO	4x4 MU-MIMO sur 5 GHz, 2x2 MIMO sur 2.4 GHz
Alimentation	PoE (802.3af)
Montage	Mur ou plafond (kit inclus)
Gestion	UniFi Controller (centralisé)
Utilisateurs recommandés	Jusqu'à 300 appareils simultanés
Environnement	Intérieur
Prix constaté	~148 CHF (Digitec.ch, hors TVA/installation)

Le point d'accès UniFi 6 Pro a été sélectionné pour assurer une couverture Wi-Fi 6 performante et sécurisée dans les locaux de NUBEM. Capable de supporter plus de 300 clients simultanés avec un débit cumulé jusqu'à 5,3 Gbps, il offre une connectivité fiable dans les zones à forte densité. Géré via le contrôleur UniFi, il permet une supervision centralisée, la gestion des VLANs, des SSID segmentés (staff, visiteurs, IoT) et des mises à jour simplifiées. Compatible avec le switch Cisco Catalyst et le pare-feu FortiGate, ce point d'accès s'intègre parfaitement à l'architecture réseau du projet.

10.2.22 Écran Tactile 24" – Dell P2424HT (borne interactive)

Caractéristique	Détail
Modèle	Dell P2424HT
Taille	23.8 pouces (60.5 cm)
Type d'écran	Tactile capacitif multipoint (10 points)
Résolution	Full HD 1920×1080
Connectique	HDMI 1.4, DisplayPort 1.2, USB-C, USB 3.2
Ergonomie	Pied articulé ajustable (inclinaison, hauteur, pivot)
Montage	Compatible VESA (mural ou borne)
Technologie d'affichage	Dalle IPS antireflet
Environnement	Utilisation en intérieur (borne, showroom)
Prix estimé	~450 CHF HT (mai 2025)

L'écran tactile Dell P2424HT a été choisi pour équiper la borne interactive d'accueil de NUBEM, permettant aux visiteurs de consulter le catalogue ou d'interagir via une interface intuitive. Sa dalle capacitive multipoint, sa résolution Full HD et sa technologie IPS offrent une expérience fluide et lisible, même en mouvement. Monté sur support articulé compatible VESA et connecté via USB-C, il est relié à un mini-PC sécurisé sous Windows 11 Pro avec session verrouillée. Cette solution allie ergonomie, sécurité réseau (GPO, VLAN, filtrage AD) et continuité de service dans un espace semi-public.

10.2.23 Mini-PC – Dell OptiPlex 7020 Micro (pour borne interactive)

Caractéristique	Détail
Modèle	Dell OptiPlex 7020 Micro
Format	Micro Form Factor (MFF) – ultra compact
Processeur	Intel Core i5-14500T vPro (14 cœurs / 20 threads)
Mémoire	16 Go DDR5 (1×16 Go, extensible à 64 Go)
Stockage	SSD NVMe 512 Go
Connectivité	2× USB-C, 4× USB-A, RJ45 Gigabit, HDMI
Réseau sans fil	Wi-Fi 6E, Bluetooth 5.3
Système d'exploitation	Windows 11 Pro 64 bits
Sécurité	TPM 2.0, BIOS sécurisé, BitLocker
Intégration	Domaine Active Directory, GPO, VLAN
Prix estimé	~900 CHF HT (mai 2025)

Le mini-PC Dell OptiPlex 7020 Micro a été intégré à la borne interactive d'accueil pour offrir une expérience fluide et sécurisée aux visiteurs. Compact, silencieux et performant, il gère l'affichage de contenus multimédias tout en s'intégrant pleinement à l'environnement IT (AD, GPO, VLAN, BitLocker). Sa compatibilité avec Intel vPro permet une administration distante efficace. Identique aux postes fixes utilisés dans le projet, il facilite la maintenance, réduit les coûts de support et assure une standardisation cohérente avec le reste de l'infrastructure.

10.3 Gantt Chart Détaillé du Projet

Planification Complète sur 12 Semaines :

Durée totale : 12 semaines

Ce planning est conçu pour permettre une **mise en œuvre progressive et structurée** du projet NUBEM, en intégrant à chaque phase des points de contrôle, des validations techniques et des marges de sécurité.

Semaines	Tâches prévues
S1–S2	Analyse détaillée des besoins, validation du périmètre technique, budget final
S3–S4	Commande & réception du matériel, préconfiguration des équipements
S5–S6	Installation de l'infrastructure réseau : switchs, Wi-Fi, VLANs, pare-feu Fortinet
S7–S8	Déploiement du serveur (Dell R750), Installation du rôle Hyper-V, création des VM, déploiement AD/GPO
S9–S10	Tests complets, validation fonctionnelle, corrections techniques éventuelles
S11–S12	Formation des utilisateurs, mise en production progressive

Points complémentaires intégrés au planning :

Gestion des risques :

- Matériel en double pour les éléments critiques (extincteurs, onduleurs)
- Accès sécurisé limité pendant les interventions techniques
- Sauvegardes prévues avant chaque déploiement critique (via Veeam)

Suivi & contrôle qualité :

- **Réunions hebdomadaires de suivi** avec le client (COPIL)
- Outils de ticketing ou suivi Agile pour adapter les ressources si nécessaire
- Validation intermédiaire après chaque phase majeure (checklists de réception)

10.4 Fiches Techniques des Équipements Sélectionnés

Matériel Réseau :

Pare-feu : Fortinet FortiGate 100F

Solution de sécurité réseau avancée avec **filtrage IPS, VPN, segmentation VLAN** et une **gestion centralisée** adaptée aux environnements PME. Intégration native avec l'architecture réseau proposée.

Switch Cisco Catalyst 9300 (managé)

Switch de couche 3 avec **support VLAN, QoS et PoE+**. Il assure la **distribution réseau sécurisée et performante** entre les différents espaces du bâtiment (open space, salle serveur, point de vente).

Voir Annexe 10.5.1

Point d'accès Wi-Fi : Cisco Meraki MR46

Accès Wi-Fi 6 avec **gestion cloud**, création de **SSID segmentés** (visiteurs, staff, IoT) et supervision centralisée. Idéal pour les zones ouvertes et le point de vente. *Voir Annexe 10.5.2*

Infrastructure Serveur :

Serveur : Dell PowerEdge R750

Serveur rack haute performance pour **virtualisation, hébergement des services critiques** (AD, fichiers, ERP) avec **double processeur, RAID 10 SSD, 128 Go RAM**. *Voir Annexe 10.3.1*

NAS : Synology DS1823xs+

Solution de stockage centralisé avec **40 To en RAID 6**, adaptée à la sauvegarde automatique (Veeam), l'archivage et l'accès réseau sécurisé.

Voir Annexe 10.5.3

Onduleur (UPS) : APC Smart-UPS 5000VA

Alimentation de secours avec **autonomie de 30 minutes**, protège le serveur et le NAS contre les coupures de courant. Intègre un système de **monitoring réseau** pour alertes et redémarrage automatique.

Voir Annexe 10.5.4

Sécurité & Monitoring :

Monitoring : PRTG Network Monitor

Solution de surveillance réseau 24/7 avec **alertes automatiques**, supervision des équipements critiques (serveur, NAS, switchs, caméras) et **visualisation centralisée**.

Supervision système : Zabbix

Outil de **gestion proactive des performances**, permettant de suivre en temps réel les **ressources CPU, mémoire, stockage, services actifs** sur les machines virtuelles et physiques.

Chiffrement : BitLocker & VeraCrypt

Protection des données sensibles grâce au **chiffrement des disques système et partitions de sauvegarde**.

- BitLocker : intégré à Windows pour les postes clients
- VeraCrypt : utilisé sur volumes externes et NAS pour la portabilité sécurisée

10.5. Sauvegarde Cloud pour les Machines Virtuelles (VM)

Objectif

Dans le cadre de la stratégie de continuité d'activité, une solution de **sauvegarde cloud sécurisée** est mise en œuvre pour protéger les **machines virtuelles critiques** (AD, ERP, sauvegarde interne). Elle complète les sauvegardes locales réalisées sur NAS Synology.

10.5.1 Solution retenue : Infomaniak – Swiss Backup & Object Storage

***Fournisseur** : Infomaniak (basé à Genève CH)*

***Services utilisés** :*

***Swiss Backup** : sauvegarde de machines Hyper-V via Veeam Agent*

***Object Storage (S3)** : stockage des fichiers exportés ou répliqués depuis le NAS*

***Avantages clés** :*

- ✓ *Localisation 100 % suisse, conforme aux normes de souveraineté des données*
- ✓ *Chiffrement natif des flux et des données stockées*
- ✓ *Intégration simple avec la structure existante (Dell R750 + Synology)*

10.5.2 Machines virtuelles concernées

Dans le cadre du plan de continuité d'activité (PCA), les machines virtuelles critiques sont sauvegardées dans le cloud via Veeam Agent for Microsoft Hyper-V, en combinaison avec la solution Swiss Backup d'Infomaniak.

Nom de la VM	Fonction	Fréquence de sauvegarde
VM-AD01	Contrôleur de domaine (Active Directory)	Quotidienne
VM-SAGE	ERP / Gestion comptable et logistique	Quotidienne
VM-FICHIERS	Partages de fichiers internes	Hebdomadaire
VM-VPN	Accès distant via tunnel SSL	Hebdomadaire

10.5.3. Avantages de la solution cloud

La solution mise en place offre un haut niveau de sécurité et de résilience pour les VM critiques hébergées sous **Microsoft Hyper-V**, tout en respectant les standards légaux et techniques actuels.

Sauvegarde hors site : protection contre les sinistres locaux (incendie, panne matérielle, vol).
Chiffrement complet : données cryptées en transit et au repos via **AES-256**.
Restauration souple : possibilité de récupération **granulaire (fichiers)** ou **intégrale (image VM)**.
Compatibilité : fonctionne avec Hyper-V, Synology NAS et solutions de type S3 (Object Storage).
Conformité légale : respecte la **RGPD (UE)** et **LPD (Suisse)** grâce à l'hébergement en datacenters suisses.

10.5.4. Coûts estimés (Infomaniak)

Le tableau ci-dessous présente une estimation des coûts pour la mise en œuvre de la sauvegarde distante des VM critiques via les services Swiss Backup et Object Storage d'Infomaniak.

Type de stockage	Capacité	Coût mensuel (CHF)	Coût annuel (CHF)
Swiss Backup	500 Go	~24.50 CHF	~294 CHF
Object Storage (S3)	1 To	~50.00 CHF	~600 CHF

Prévision initiale : un volume de 500 Go est suffisant pour héberger les sauvegardes de **3 à 4 machines virtuelles critiques**.
Scalabilité : l'extension de capacité est possible **par palier de 100 Go**, à la demande.

10.5.5 Intégration au projet

La solution de sauvegarde cloud complète l'infrastructure de sauvegarde locale basée sur le NAS Synology, conformément à la stratégie **3-2-1**, reconnue comme bonne pratique en cybersécurité :

- ✓ **3 copies** des données : production (VM Hyper-V) + NAS local + cloud distant
- ✓ **2 types de supports** : stockage local (RAID Synology) + stockage cloud
- ✓ **1 copie hors site** : hébergée dans le cloud suisse d'Infomaniak

La sauvegarde est orchestrée via des **agents installés sur les VM Hyper-V** ou via une **console de gestion centralisée** compatible (ex. Veeam Agent, Acronis, Synology Active Backup for Business).

Conclusion

La mise en place d'une **solution de sauvegarde cloud** pour les machines virtuelles critiques du projet NUBEM assure :

- ✓ une **résilience opérationnelle renforcée** face aux incidents locaux,
- ✓ une **conformité réglementaire** avec les normes suisses et européennes (RGPD / LPD),
- ✓ une **continuité de service garantie**, même en cas de sinistre majeur.

Cette démarche s'inscrit pleinement dans une **stratégie de cybersécurité proactive** et une politique de haute disponibilité des infrastructures IT.

10.6. Budget Matériel - Projet NUBEM

10.6.1. Matériel Informatique

Catégorie	Description	Quantité	Prix Unitaire (CHF)	Total (CHF)	Remarques
Ordinateurs Portables	Dell Latitude 7450	5	~2,200	~11,000	1 en plus pour remplacement ou nouveau staff
Stations de travail	Dell OptiPlex 7020	14	~950	~13,800	Inclut les 3 nouveaux employés
Moniteurs	Dell Pro 27 Plus QHD (P2725D)	14	~368	~5,150	Haute résolution, usage bureautique optimal
Accessoires Laptop	Dell Dock UD22	5	~164	~820	Station d'accueil universelle
Accessoires Laptop	Souris sans fil Dell MS3320W	5	~24	~120	Pour laptops uniquement
Accessoires Laptop	Sacoche EcoLoop Dell	5	~36	~180	Accessoire optionnel
Borne interactive	Écran tactile Dell P2424HT	1	~450	~450	Présentation produits à l'accueil
Borne interactive	Dell OptiPlex 7020 Micro	1	~657	~657	Mini-PC intégré à la borne (VLAN, GPO)

Sous-total Informatique : ~31,670 CHF

10.6.2. Serveur & Infrastructure

Catégorie	Description	Quantité	Prix Unitaire (CHF)	Total (CHF)	Remarques
Serveur	Dell PowerEdge R750 Rack	1	~12,660	~12,660	Serveur principal
NAS	Synology DS1823xs+	1	~1,500	~1,500	Solution de sauvegarde centralisée
Disques NAS	WD Red Pro 8TB (HDD)	10	~183	~1830	Haute fiabilité, capacité 80 To et capacité utile ~48 To en RAID 6
Switch Réseau	Cisco Catalyst 9300 48-port PoE+	1	~4,500	~4,500	Compatible avec téléphonie IP
Pare-feu	Fortinet FortiGate 100F	1	~1,800	~1,800	Protection réseau entreprise
Onduleur (UPS)	APC SRT 5000VA + 3000VA UPS	2	~3,000	~6,000	Continuité électrique pour serveur et réseau
Armoire Serveur	APC NetShelter SX 42U	1	~1,600	~1,600	Installation en baie 19"
WiFi - Access Points	Ubiquiti UniFi 6 Professional (U6-PRO)	3	~148	~444	Couverture sans fil complète et redondante

Sous-total Infrastructure : 29,000 CHF

10.6.3. Imprimantes

Catégorie	Description	Quantité	Prix Unitaire (CHF)	Total (CHF)	Remarques
Imprimantes MFD	HP Color LaserJet Pro M479fdw	4	~520	~2,080	Couleur, multifonction, réseau
Imprimantes N&B	HP LaserJet Pro 4002dw	3	~200	~600	Pour points de vente

Sous-total Imprimantes : ~2,680 CHF

10.6.4. Sécurité & Accessoires Divers

Catégorie	Description	Quantité	Prix Unitaire (CHF)	Total (CHF)	Remarques
Extincteurs CO2	Extincteur CO2 2kg	2	~100	~200	Pour local serveur et bureau
Multiprises + RJ45	Accessoires câblage, étiquetage etc.	Divers	~500	~500	Organisation & sécurité réseau

Sous-total Divers : ~700 CHF

TOTAL GÉNÉRAL ESTIMÉ : ~66`000 CHF

(Budget cible : 50–70K CHF HT)

Tous les prix sont estimatifs, hors taxes (HT) et peuvent varier selon les fournisseurs.

10.7. Choix de la solution e-mail : Microsoft Exchange Online avec domaine nubem.ch

Objectif Dans le cadre du projet NUBEM, une solution professionnelle de messagerie est requise pour assurer la communication interne et externe, tout en garantissant la sécurité, la conformité et l'intégration avec les outils d'entreprise existants (Microsoft Teams, Office, etc.).

Solution retenue : Microsoft Exchange Online + domaine personnalisé @nubem.ch

Élément	Détail
Fournisseur	Microsoft 365 Business
Domaine de messagerie	@nubem.ch (domaine propre, acheté et configuré chez registrar)
Plateforme de messagerie	Exchange Online (cloud)
Accès	Outlook (PC, Web, mobile), IMAP/SMTP sécurisé
Intégration	Parfaite avec Teams, Word, Excel, OneDrive
Protection	SPF, DKIM, DMARC, MFA, chiffrement TLS
Mobilité	Compatible avec toutes les plateformes mobiles
Administration	Console Microsoft 365 (gestion centralisée des utilisateurs)

Coûts estimés pour 15 utilisateurs

Élément	Détail	Coût estimé
Licence Microsoft 365	Business Basic (ou Standard)	~5–11 CHF / utilisateur / mois
Total licences	Pour 15 utilisateurs	~900 CHF / an
Nom de domaine	nubem.ch (chez Infomaniak, Hostpoint, etc.)	~15–20 CHF / an

Le coût total annuel estimé pour l'e-mail professionnel est donc d'environ **~920 CHF / an** (hors TVA).

Avantages clés de cette solution

- ✓ Image professionnelle avec des adresses prenom.nom@nubem.ch
- ✓ Intégration totale avec Teams, calendriers partagés, stockage cloud OneDrive
- ✓ Zéro maintenance locale, gestion 100% cloud
- ✓ Sécurité avancée : MFA, anti-phishing, conformité RGPD
- ✓ Support Microsoft mondial + communauté très active

Comparatif rapide : Infomaniak vs Microsoft 365

Critère	Infomaniak Mail Pro	Microsoft 365 Exchange
Prix annuel (15 utilisateurs)	~270 CHF	~900 CHF
Intégration Teams / Office	❌ limité	✅ native et optimale
Webmail + mobile	✅ basique	✅ Outlook complet + apps mobiles
Protection / sécurité	✅ standard	✅ avancée (SPF, DKIM, MFA)
Maintenance	Aucune	Aucune (cloud)
Image de marque	Bonne	Très professionnelle

Conclusion :

L'utilisation de Microsoft Exchange Online avec le domaine personnalisé @nubem.ch répond pleinement aux exigences de l'entreprise en termes de professionnalisme, de sécurité, de compatibilité avec les outils collaboratifs existants et d'fiabilité à long terme. Cette solution devient ainsi un pilier de la communication et de la gestion de l'information du projet NUBEM.

Sommaire

10.8. Tableau – Répartition des équipements par zone

Zone / Bureau	Utilisateur(s)	Matériel installé	Remarques
Direction	2 personnes (Directeur + Adjoint)	2 × PC portable Dell Latitude, 2 × station d'accueil (dock)	Wi-Fi + RJ45, accès imprimante réseau
Équipe commerciale	2 personnes	2 × PC portable, 2 × Dock UD22	Zone partagée avec imprimante MFD couleur
Administration	5 personnes	5 × PC fixes Dell OptiPlex, 5 × écrans Dell	Connexion RJ45, VLAN 10
Comptabilité / Finance	2 personnes	2 × PC fixes, accès logiciel SAGE	Accès restreint, données sensibles
Logistique / Dépôt	2 personnes	2 × PC fixes, 1 × imprimante N&B locale	VLAN 30, conditions industrielles
Points de vente (3x)	3 personnes	3 × PC fixes, 3 × imprimantes Laser N&B	VLAN spécifique, accès limité
Salle serveur	Aucun	1 × Serveur Dell R750, NAS Synology, 2 × UPS, baie 42U	Accès restreint, alimentation dédiée
Zone Wi-Fi invité	Visiteurs	1 × Point d'accès Wi-Fi dédié (VLAN invité)	SSID isolé, bande passante limitée
Salle de réunion / cuisine	Tous utilisateurs	1 × Point d'accès Wi-Fi U6-PRO	Connexion standard interne

Points d'accès Wi-Fi (Ubiquiti U6-PRO – 3 unités) :

1. Bureau administratif – couverture centrale
2. Salle de réunion ou logistique – extension latérale
3. Point de vente ou zone visiteurs – réseau segmenté invité

Conclusion : La répartition du matériel par zone garantit une couverture cohérente des besoins métiers et techniques, tout en assurant une organisation réseau segmentée et sécurisée.

Conclusion

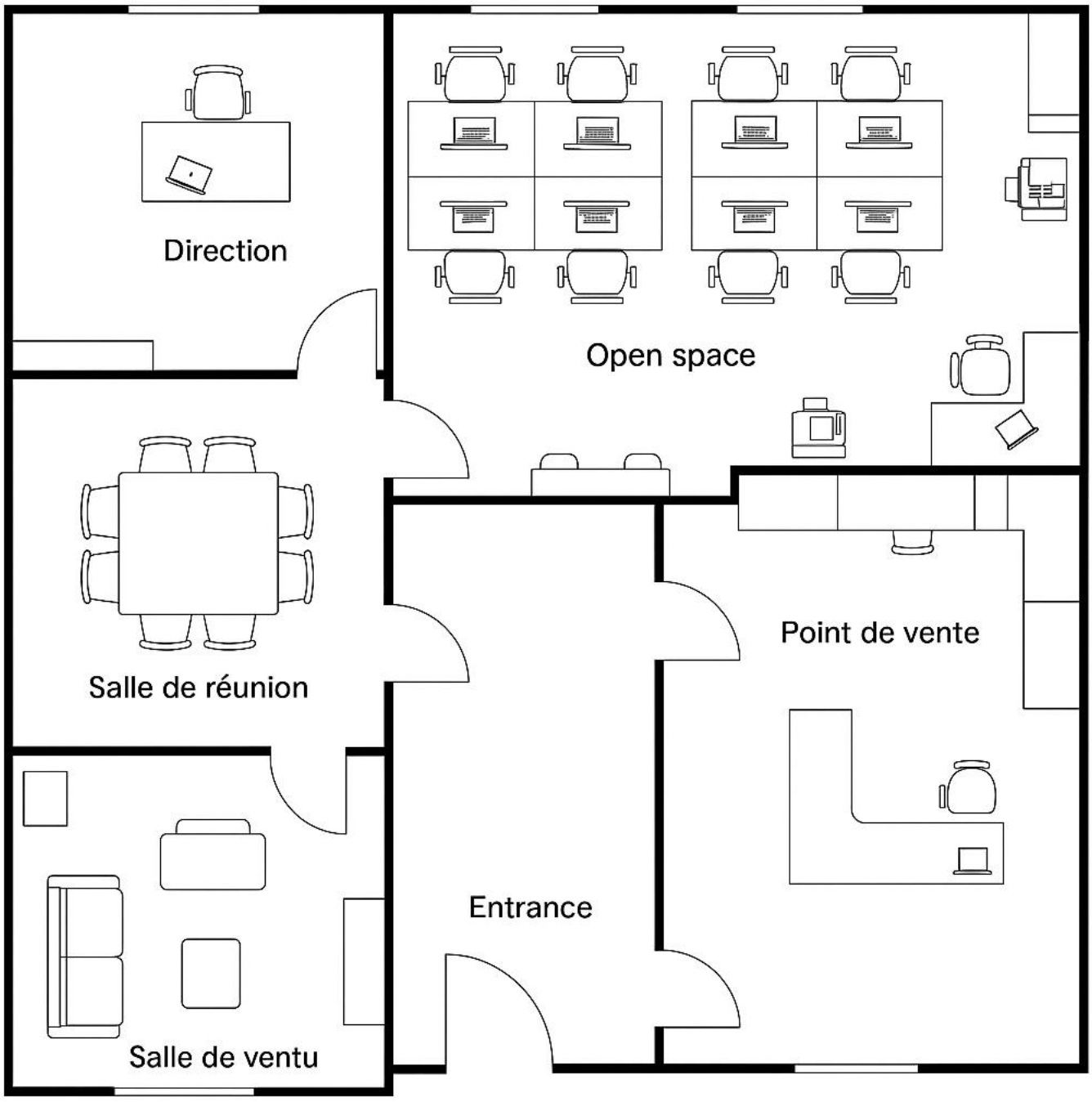
Pourquoi cette section est essentielle :

- Elle permet une mise en œuvre sans erreur, en fournissant une référence technique complète.
- Elle assure la pérennité du projet grâce à une documentation précise facilitant la maintenance.
- Elle garantit l'évolutivité en simplifiant l'ajout futur de nouveaux services IT.

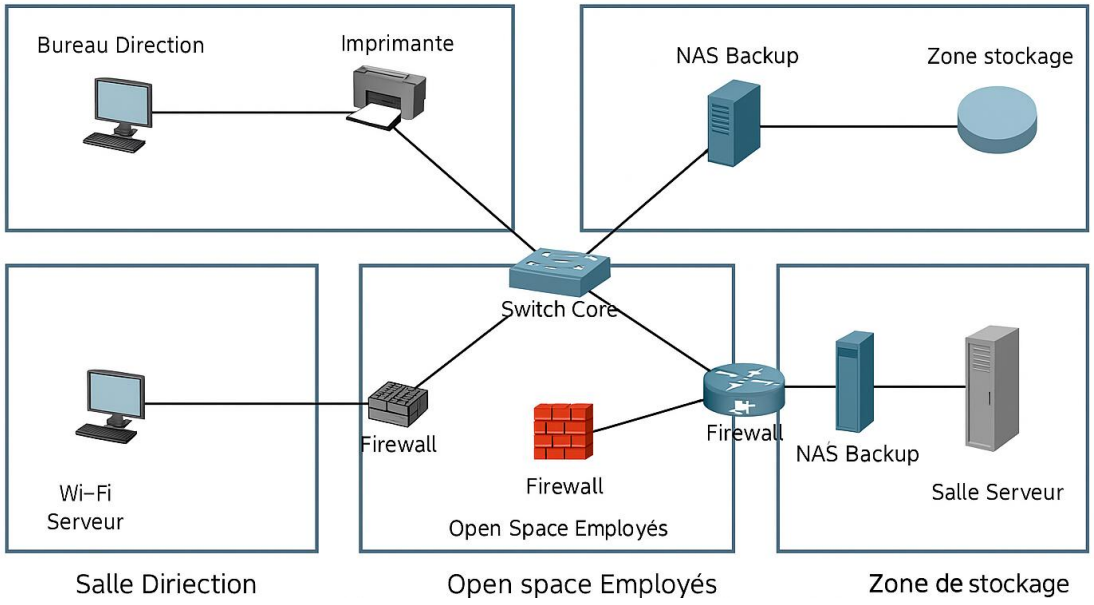
11. Schémas d’Infrastructure & Implantation Physique

Cette section regroupe les représentations visuelles essentielles à la compréhension et à la mise en œuvre technique du projet NUBEM.

11.1 Disposition des locaux et postes de travail



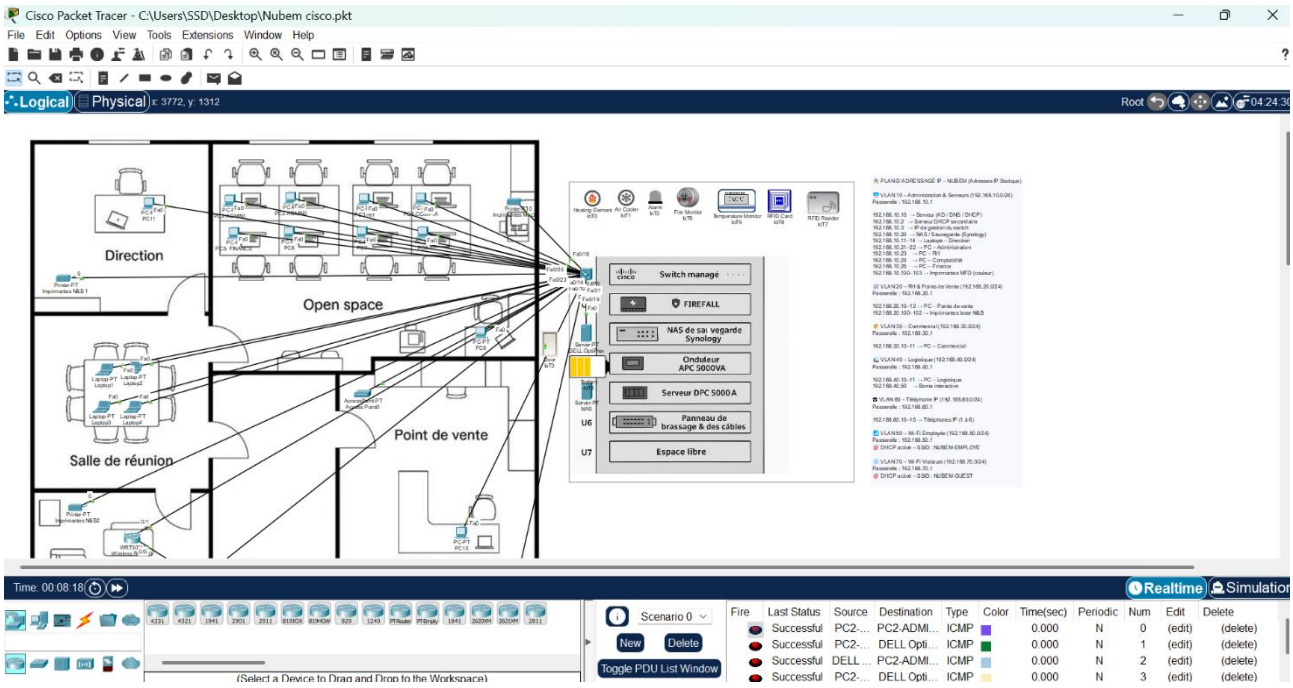
11.2 Schéma du Réseau & Disposition des Équipements



Description :
Ce schéma illustre l'architecture réseau principale ainsi que l'implantation physique des équipements essentiels dans les différentes zones du site. Il permet de visualiser :

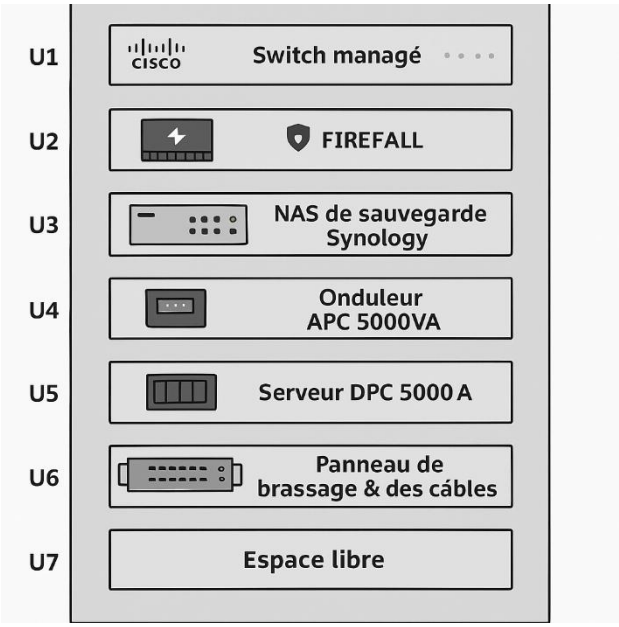
- **Disposition des bureaux** : direction, open space, salle serveur, stockage.
- **Switch managé Cisco (9300)** avec VLAN/QoS pour la gestion du trafic.
- **Implantation des postes** : PC, imprimantes, NAS, serveurs.
- **Connexions physiques** représentées clairement entre les zones.

Voir Annexe 10.5 pour les détails techniques sur les équipements réseau.



Sommaire

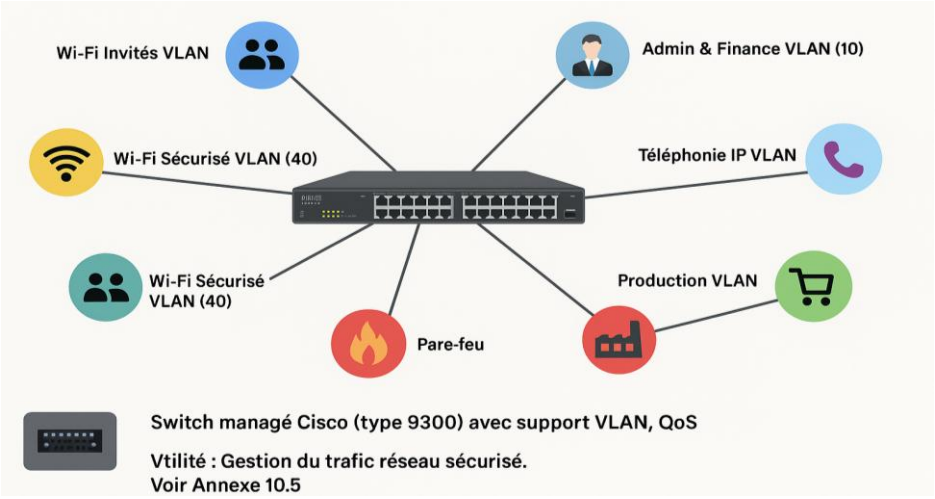
11.3 Schéma de la Baie Serveur (Disposition Physique des Équipements)



- **Switch managé Cisco (type 9300)** avec support VLAN, QoS
  Utilité : Gestion du trafic réseau sécurisé. Voir Annexe 10.5.
- **Pare-feu FortiGate (2U)** → Couche de sécurité, gestion des menaces
- **NAS de sauvegarde Synology (3U)** → Infrastructure de sauvegarde
- **Onduleur APC 5000VA (4U)** → Alimentation sans interruption
- **Serveur Dell PowerEdge R750 (5U–6U)** → Serveur principal
- **Panneau de brassage (7U)** → Organisation du câblage
- **Espace libre (8U)** → Pour futures extensions

Ce schéma représente une disposition professionnelle des équipements dans la salle serveur.

11.4 Topologie VLAN & Sécurité Réseau



Ce schéma présente l'architecture logique des VLANs mis en œuvre dans l'infrastructure réseau de NUBEM, avec un focus sur la segmentation, la sécurité et la performance.

Objectifs de la configuration VLAN

- **Séparer les flux réseau critiques** par fonction pour limiter les risques de sécurité.
- **Optimiser la qualité de service (QoS)** pour les applications sensibles comme la téléphonie IP.
- **Isoler les accès invités** du réseau interne de l'entreprise.

Description des VLANs définis

VLAN	Nom	Utilisation
10	Admin & Finance VLAN	Direction, RH, comptabilité
20	Commercial VLAN	Équipe de vente
30	Production VLAN	Logistique et postes industriels
40	Wi-Fi Sécurisé VLAN	Connexions internes mobiles
50	Téléphonie IP VLAN	Téléphones VoIP et softphones
60	Wi-Fi Invités VLAN	Réseau isolé pour visiteurs externes

Sommaire

Composant central

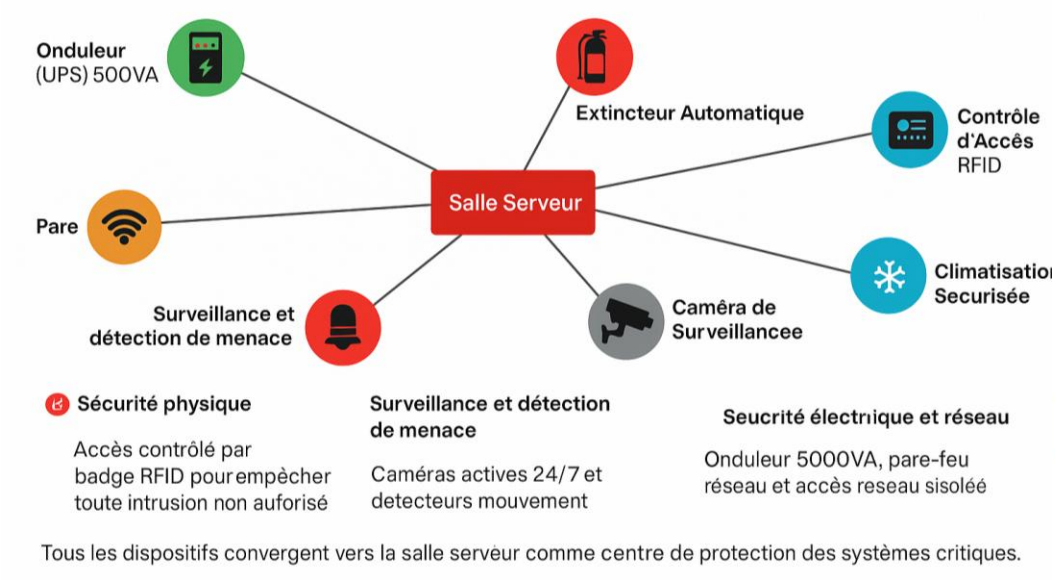
- **Switch Cisco Catalyst 9300** (support VLAN + QoS)
- **Pare-feu FortiGate 100F** connecté pour inspection du trafic entre VLANs

Chaque VLAN est connecté au switch managé, puis filtré par le pare-feu selon des règles de sécurité définies.

Bénéfices de cette approche§

- Réduction de la surface d'attaque
- Contrôle fin des droits d'accès entre services
- Meilleure performance réseau grâce au trafic segmenté
- Conformité avec les bonnes pratiques de sécurité informatique

11.5 Disposition de Sécurité – Salle Serveur



Ce schéma présente les dispositifs de sécurité mis en place dans la salle serveur afin de garantir la continuité, la confidentialité et l'intégrité des systèmes critiques de l'entreprise.

Sécurité physique

- **Contrôle d'accès par badge RFID** (Promag ER755 + badge Mifare) pour empêcher les intrusions.
- Accès limité uniquement au personnel autorisé.

Surveillance & détection de menace

- **Caméras Ubiquiti UniFi G5 Dome** avec vision nocturne et détection de mouvement.
- Enregistrement continu 24/7 avec supervision centralisée via UniFi Protect.

Protection incendie & environnement

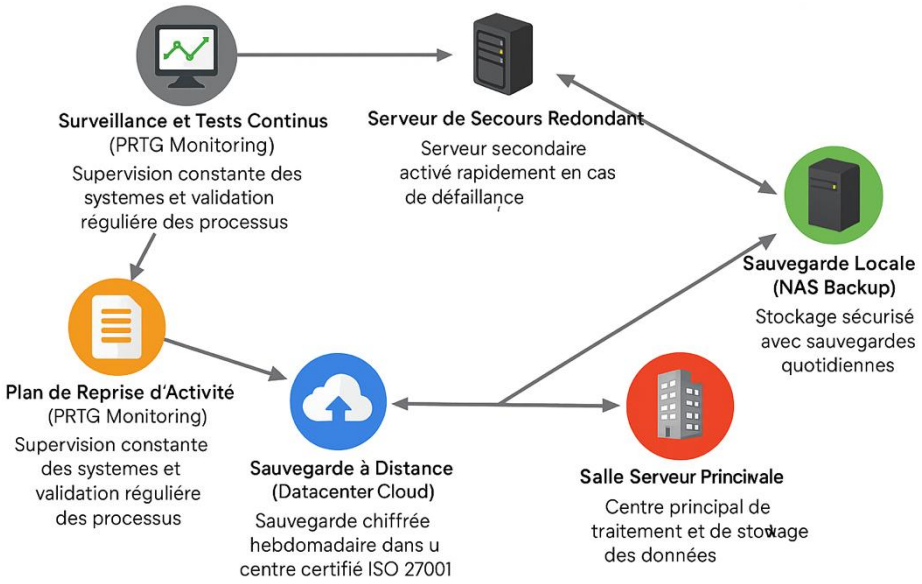
- **Extincteurs CO_2 automatiques** sans résidu, compatibles avec matériel électronique.
- **Climatisation régulée** pour maintenir une température stable.

Sécurité électrique & réseau

- **Onduleur APC 5000VA** assurant jusqu'à 30 minutes d'autonomie.
- **Pare-feu Fortinet** pour sécuriser les flux entrants/sortants.
- Réseau isolé avec VLAN dédié.

Note : Tous ces systèmes convergent vers la salle serveur comme centre névralgique de l'infrastructure IT. Ils garantissent un haut niveau de sécurité physique et logique indispensable à la pérennité des opérations.

11.6 Plan de Reprise d'Activité (PRA) & Stratégie de Sauvegarde



Ce schéma illustre la stratégie de continuité d'activité mise en place pour garantir la résilience du système informatique en cas d'incident majeur.

Salle Serveur Principale

- Centre principal de traitement des données.
- Accueille les VM critiques (Hyper-V), le NAS et l'infrastructure réseau.

Sauvegarde Locale (NAS Synology)

- Sauvegardes quotidiennes automatisées.
- Données stockées en RAID 6 pour une tolérance de panne élevée.

Sauvegarde à Distance (Cloud Infomaniak)

- Sauvegardes hebdomadaires chiffrées (AES-256).
- Stockage dans un datacenter ISO 27001 en Suisse.

Serveur de Secours Redondant

- Préconfiguré pour prendre le relais rapidement.
- Réduction du temps de reprise (RTO).

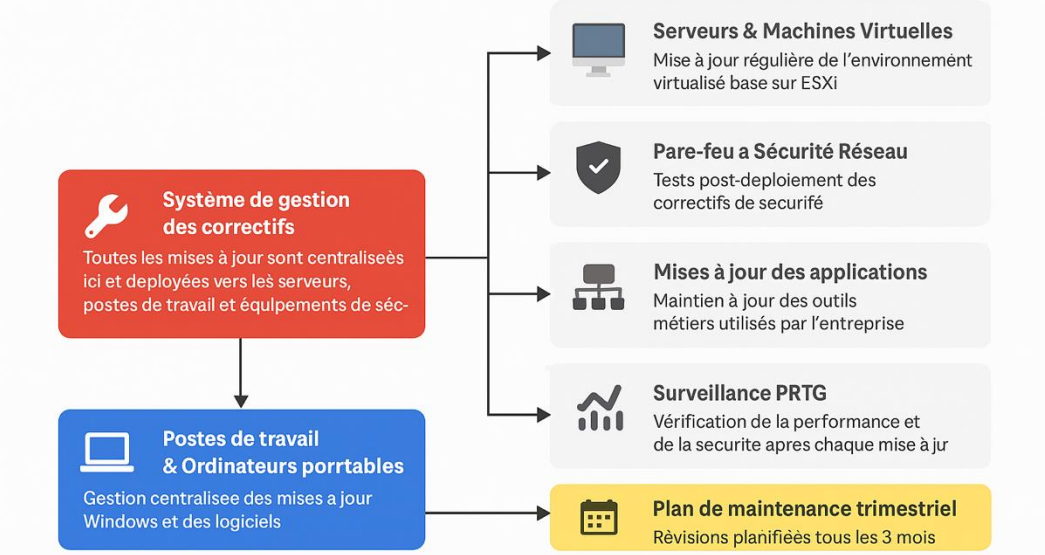
Plan de Reprise d'Activité (PRA)

- Procédures documentées pour la restauration des systèmes.
- Plan testé régulièrement pour valider son efficacité.

Surveillance & Tests Continus

- Supervision permanente via **PRTG Network Monitor**.
- Alerte immédiate en cas d'anomalie ou de défaillance.

11.7 Stratégie de Mise à jour & Maintenance des Systèmes



Ce schéma présente le fonctionnement global de la gestion des mises à jour et des opérations de maintenance planifiée dans le projet NUBEM.

Système de gestion des correctifs

- Plateforme centralisée de déploiement des mises à jour de sécurité.
- Couvre serveurs, postes clients, pare-feu, équipements critiques.

Serveurs & Machines Virtuelles

- Environnement Hyper-V régulièrement mis à jour pour stabilité et sécurité.
- Intégration des correctifs Microsoft et des pilotes matériels.

Postes de travail & Laptops

- Mises à jour Windows et applications bureautiques via gestion de groupe Active Directory (GPO).
- Réduction des failles de sécurité côté utilisateur.

Pare-feu & Équipements Réseau

- Application des correctifs firmware sur FortiGate, switchs Cisco.
- Validation post-mise à jour pour éviter toute interruption de service.

Applications métiers

- Suivi de versions pour les logiciels SAGE, ERP, outils de gestion documentaire.
- Compatibilité assurée avec le système d'exploitation.

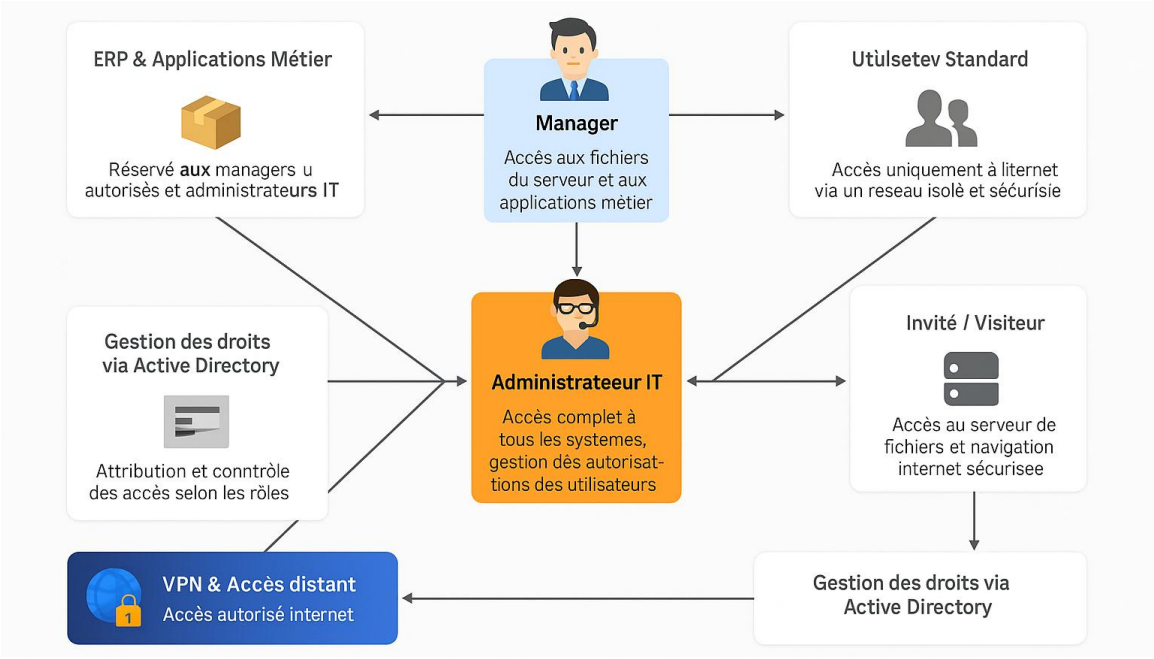
Surveillance PRTG

- Contrôle de performance et alertes après chaque cycle de mise à jour.
- Tableaux de bord de disponibilité mis à jour en temps réel.

Plan de maintenance trimestriel

- Audit technique et contrôle physique tous les 3 mois.
- Alignement avec les bonnes pratiques ITIL.

11.8 Contrôle d'Accès & Gestion des Permissions Utilisateurs



Ce schéma décrit les différents niveaux d'accès aux ressources informatiques en fonction des rôles définis dans l'organisation NUBEM. Il reflète la structure Active Directory implémentée dans le projet.

Niveaux d'accès définis :

- **Administrateur IT** : Accès complet à l'ensemble des systèmes, gestion des autorisations, maintenance et supervision.
- **Manager** : Accès aux fichiers partagés, logiciels ERP, outils stratégiques.
- **Utilisateur Standard** : Accès aux fichiers communs et à Internet via une navigation sécurisée.
- **Invité / Visiteur** : Accès Internet uniquement, sur un réseau isolé (VLAN 60).

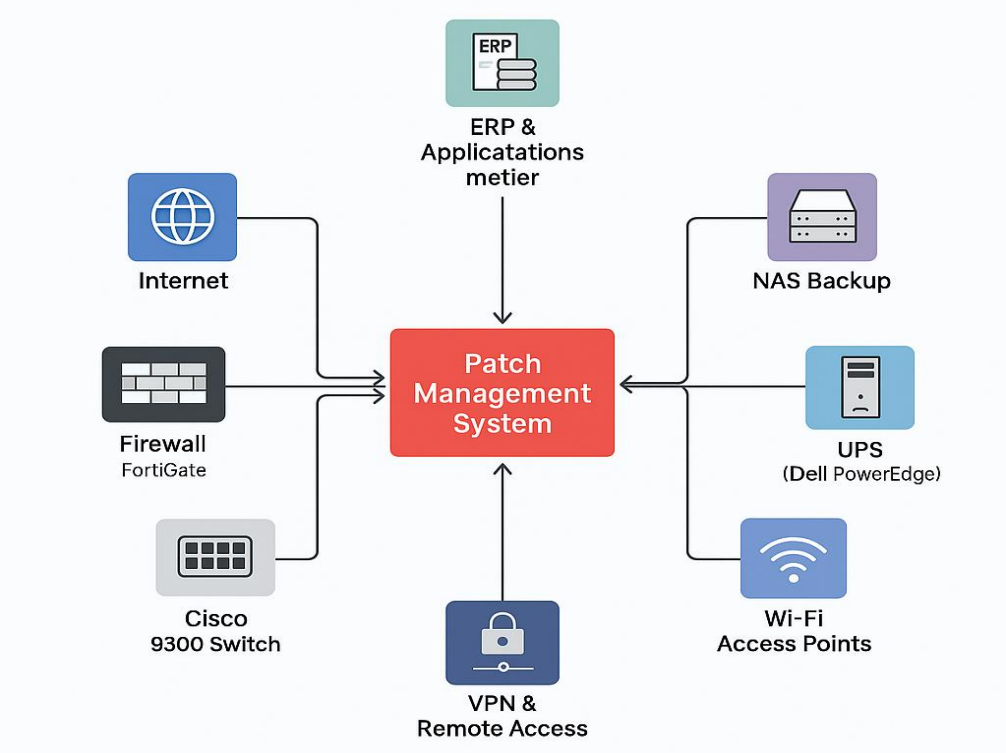
Accès spécifiques :

- **ERP & Applications métier** : Réservé aux administrateurs et managers autorisés uniquement.
- **VPN & Accès distant** : Activé exclusivement pour les administrateurs IT.

Gestion centralisée :

- ✓ **Active Directory** est utilisé pour la gestion des droits d'accès selon les groupes de sécurité définis : GG_Administration, GG_Comptabilité, GG_Logistique, etc.
- ✓ Les droits sont appliqués sur les dossiers réseau partagés (E:\Travail) selon l'appartenance à un groupe.
- ✓ Ce système garantit une gestion fine des accès tout en respectant les principes de sécurité (moindre privilège, isolation, traçabilité).

11.9 Vue d'ensemble de l'infrastructure IT complète



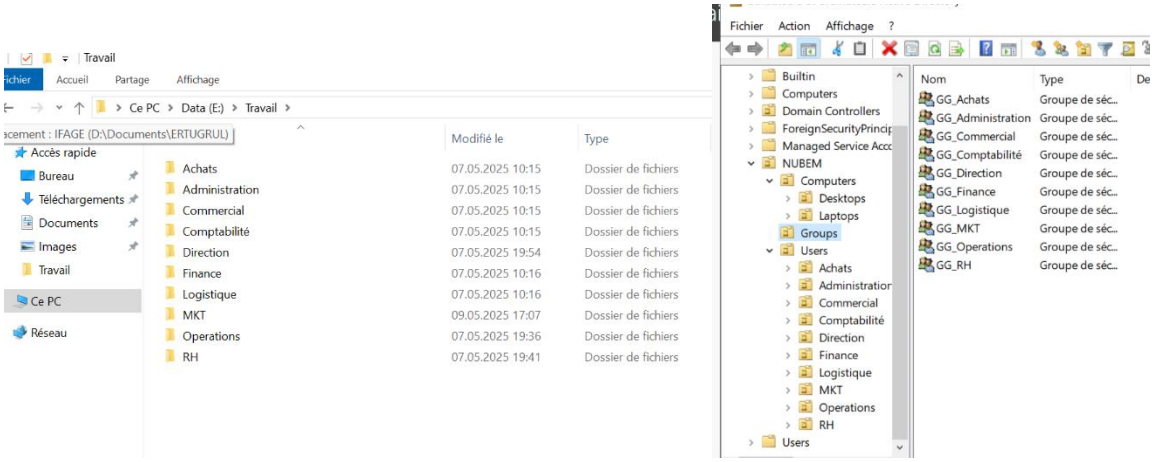
Ce schéma synthétise l'architecture informatique globale du projet NUBEM, en illustrant les interconnexions critiques entre les composants réseau, serveurs, sauvegardes et accès distants.

Composants principaux :

- **Connexion Internet** → Distribuée de manière sécurisée via un pare-feu FortiGate
- **Pare-feu FortiGate** → Sécurité périmétrique et contrôle du trafic
- **Switch Cisco 9300** → Distribution VLAN, QoS, interconnexion LAN
- **Wi-Fi (Ubiquiti U6-PRO)** → Accès réseau segmenté (interne et invité)
- **Serveur Dell PowerEdge R750** → Hyper-V, Active Directory, ERP
- **NAS Synology** → Sauvegarde locale sécurisée des fichiers
- **UPS APC 5000VA** → Alimentation sans coupure pour serveurs et switchs
- **VPN sécurisé** → Accès distant chiffré pour l'équipe IT
- **ERP et applications métiers** → Comptabilité, gestion commerciale
- **PRTG Monitoring** → Supervision 24/7 des performances et journaux systèmes

Ce schéma joue un rôle essentiel dans la compréhension de l'infrastructure IT de NUBEM et facilite les interventions techniques futures, la maintenance et l'extension du système.

11.11 Organisation Active Directory & Partages Réseau



La structure Active Directory et les partages de fichiers ont été conçus pour offrir une gestion centralisée, sécurisée et adaptée à l'organisation interne de NUBEM.

Structure Active Directory

Les unités organisationnelles (OU) sont définies comme suit :

- **OU Users** : contient les utilisateurs regroupés par service (RH, Finance, Commercial, etc.)
- **OU Groups** : contient les groupes de sécurité (ex. : GG_Finance, GG_RH, GG_MKT)
- **OU Computers** : ordinateurs classés selon leur type (Desktops, Laptops)

Chaque groupe est lié à un service métier et utilisé pour appliquer des stratégies d'accès (GPO, droits NTFS, etc.).

Voir capture d'écran : Structure AD (Utilisateurs et Groupes)

Arborescence des partages réseau

Un dossier principal Travail est configuré sur le volume E:\ du serveur de fichiers, avec des sous-dossiers dédiés :

- E:\Travail\RH, E:\Travail\Finance, E:\Travail\Logistique, etc.
- Chaque dossier est protégé par des permissions NTFS spécifiques à son groupe de sécurité AD.
- Les utilisateurs ont des accès en lecture/écriture selon leur rôle.

Voir capture d'écran : Structure des dossiers partagés

Sécurité & gestion des accès

- **Modèle RBAC** (Role-Based Access Control) appliqué via les groupes AD.
- Aucune permission directe n'est appliquée à un utilisateur.
- Accès renforcé par stratégie de mot de passe et verrouillage automatique.

CONTRAT DE COLLABORATION INFORMATIQUE

Entre les parties :

- **Client :** NUBEM SA
- **Prestataire :** ErtSystem SARL (intégrateur et prestataire de services informatiques)

1. Objet du contrat

Ce contrat formalise la collaboration entre NUBEM et ErtSystem pour la mise en œuvre, la gestion et la maintenance d'une infrastructure informatique complète au sein du site de Vernier. Il s'agit d'un contrat de service incluant la fourniture, le déploiement, la configuration et le support post-installation du matériel et des logiciels décrits dans le projet NUBEM.

2. Durée et périmètre

- Durée initiale : 12 mois à compter du . .2025
- Renouvellement : par tacite reconduction annuelle, sauf résiliation par lettre recommandée 30 jours avant échéance
- Périmètre couvert :
  - Infrastructure réseau LAN/Wi-Fi (Cisco, UniFi)
  - Systèmes serveurs & virtualisation (Dell PowerEdge R750, Hyper-V)
  - Stockage & sauvegarde (Synology NAS RAID6, Active Backup)
  - Sécurité réseau (FortiGate 100F, segmentation VLAN, ACL)
  - Supervision, onduleurs, environnement (APC, capteurs, caméras)

3. Engagements du prestataire

- Installation, configuration et tests de conformité
- Documentation technique et transfert de compétences
- Support technique Niveau 2/Niveau 3 (cf. section SLA 7.4)
- Suivi mensuel par rapport aux indicateurs de qualité (KPI, tickets)

4. Engagements du client

- Mise à disposition des locaux et accès techniques
- Validation des étapes du projet (design, installation, recette)
- Paiement selon le calendrier de facturation convenu

5. Modalités de support

- Période de support standard : lundi à vendredi, 08h00 à 18h00
- Support à distance via outils sécurisés (iDRAC, DSM, VPN)
- Intervention sur site selon criticité
- Délais de réponse et de résolution définis par niveau de priorité (P1 à P4)

6. Documents référencés

- Cahier des charges technique NUBEM
- Projet final "Infrastructure IT NUBEM" (version 2025)
- Schémas réseau, SLA, VLAN, sauvegarde (voir annexes techniques)

Fait à Genève, le ….. ……. 2025

Signature du client (NUBEM) : _____

Signature du prestataire (ErtSystem) : _____

12. Références

Voici les principales sources et ressources utilisées pour la conception, la documentation technique et la planification du projet NUBEM :

Documents techniques & constructeurs :

- Dell Technologies. *Fiche technique PowerEdge R750*. www.dell.com
- Synology. *Documentation NAS DS1823xs+*. www.synology.com
- Cisco Systems. *Catalyst 9300 Datasheet*. www.cisco.com
- Fortinet. *FortiGate 100F - Product Datasheet*. www.fortinet.com
- APC by Schneider Electric. *SRT 5000VA UPS – Technical specifications*. www.apc.com

Fournisseurs & comparateurs de prix :

- **Digitec Galaxus AG** – *Catalogue de matériel informatique, serveurs, accessoires réseau*. www.digitec.ch

Normes & Bonnes pratiques :

- ISO/IEC 27001 – *Systèmes de management de la sécurité de l'information*
- ITIL v4 – *Gestion des services informatiques*
- CNIL – *Recommandations sur la sécurité des données personnelles*, www.cnil.fr

Logiciels & outils utilisés :

- Microsoft Docs – *Microsoft Intune, Azure AD, Exchange Online*
- PRTG Network Monitor – *Guide de configuration et supervision réseau*, Paessler AG
- Veeam – *Agent for Microsoft Hyper-V – Guide de sauvegarde*

Ressources institutionnelles & cloud :

- Infomaniak. *Swiss Backup & Object Storage – documentation technique*. www.infomaniak.com
- Hostpoint / Switch.ch – *Enregistrement de domaines et hébergement suisse sécurisé*

Ertsystem
Systèmes IT

NUBEM