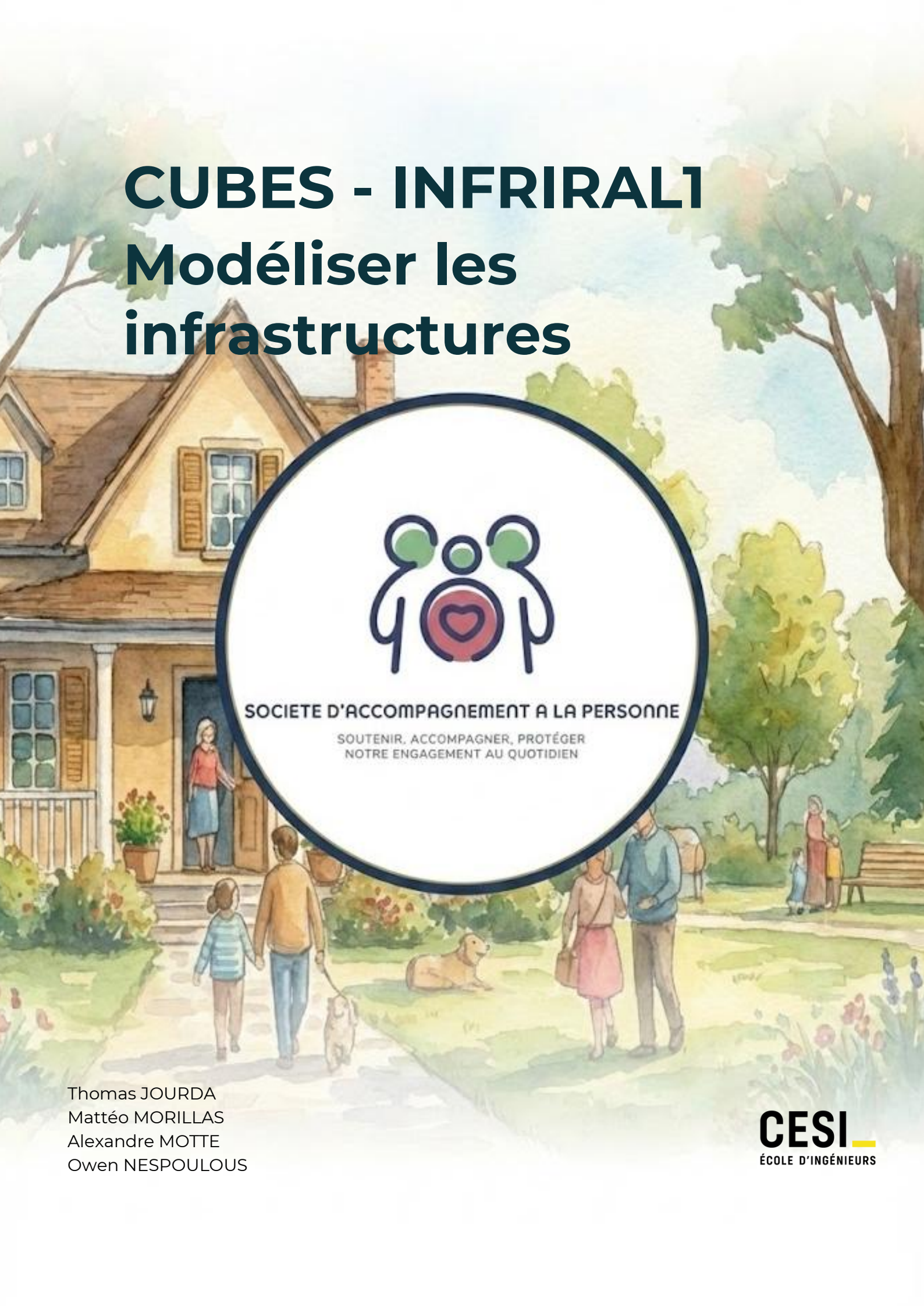
CUBES - INFRIRAL1
Modéliser les infrastructures



Thomas JOURDA
Mattéo MORILLAS
Alexandre MOTTE
Owen NESPOULOUS

CESI
ÉCOLE D'INGÉNIEURS

1 Table des matières

2 Table d’illustration

3 Note de cadrage

3.1 Situation actuelle

SAP (Société d'Accompagnement de la Personne) a un Système d'Informations en place depuis 2015. Ce dernier est devenu obsolète car le parc informatique est vieillissant. Le système actuel n'a pas de solutions collaboratives modernes. Certaines applications sont non intégrées, cela engendre une ressaisie des données par les utilisateurs. Le Système d'Information n'a plus de sécurité suffisante face aux menaces actuelles. L'hébergement en local n'a pas de PRA (Plan de Reprise d'Activité). Ainsi, ce dernier ne respecte plus les normes et réglementations (RGPD, NIS2, ISO 27001 et HDS).

3.2 Situation souhaitée

La situation souhaitée est de renouveler le parc informatique. Par ailleurs, le Système d'Information doit se moderniser en garantissant un accès sécurisé depuis l'extérieur tout en étant optimisé avec de nouveaux outils et sécurisé. Ce dernier doit se conformer aux normes et aux réglementations. Ce nouveau SI doit pouvoir être exploité sur les 5 prochaines années.

3.3 Enjeux

En définissant la situation, les enjeux sont :

- Stratégiques - Transformation digitale et modernisation du SI. La compétitivité dans le secteur médico-social. Pérennité économique sur 5 ans minimum.
- Opérationnels - Continuité de service (haute disponibilité à 99.9%). L'efficacité des équipes avec un SI centralisé et interopérable. La mobilité des professionnels. La sécurité des données sensibles des bénéficiaires.
- Humains & Sociaux - Amélioration des conditions de travail. Qualité de l'accompagnement des bénéficiaires et une coordination multi-sites.
- Techniques - Remplacement de l'infrastructure obsolète. La mise en place d'un PRA et PCA (tolérance d'indisponibilité de 8h45/an). Les applications métiers sont interopérables. Monitoring et supervision proactive du Système d'Information.
- Environnementaux - Démarche GreenIT et performance énergétique. Économie circulaire et recyclage des équipements. Politique RSE et réduction de l'empreinte carbone.
- Financiers - Optimisation du ROI. Maîtrise budgétaire (345-500 K€ lors de la première année). Réduction des coûts opérationnels et un financement validé par la Direction.

3.4 Contraintes

Les contraintes de ce projet sont :

- Temporelle avec une période de 8 mois pour effectuer le renouvellement.
- Réglementaire avec certification HDS, le respect de la norme ISO 27001, de la réglementation NIS2 et de la loi RGPD.
- Technique avec une demande de disponibilité à 99.9%.
- Équipe réduite avec 1 RSI + 1 alternant.
- Démarche éco-responsable

3.5 Hypothèses

Les hypothèses identifiées à ce jour sont :

- Le budget alloué par la Direction
- La collaboration avec les équipes métier
- La formation des utilisateurs
- La disponibilité des ressources internes
- La validation COPIL à chaque étape.

3.6 Périmètre

Le périmètre du projet inclus :

- La modernisation du parc utilisateur
- Le renouvellement des serveurs
- La refonte réseau
- Le déploiement ERP médico-social
- Les outils collaboratifs
- L'implémentation du PCA et PRA
- La sécurisation des données
- La conformité HDS, ISO 27001/22301, RGPD et NIS2
- La supervision et monitoring
- L'accès distant sécurisé.

3.7 Analyse des risques

ID	Risques	Probabilité	Impact avant-	Actions Préventives	Actions Correctives	Probabilité	Impact post-
R01	Dépassement budgétaire	Moyenne	Elevée	• Validation COPIL à chaque phase • Suivi budgétaire hebdomadaire • Réserve de contingence 10%	• Priorisation des lots critiques • Négociation fournisseurs • Étalement sur N+1 si nécessaire	Faible	Moyenne
R02	Retard planning	Moyenne	Elevée	• Diagramme GANTT avec marges • Points d'avancement hebdo • Commandes anticipées	• Mobilisation ressources externes • Parallélisation des tâches • Réduction périmètre non critique	Faible	Moyenne
R03	Indisponibilité SI pendant migration	Faible	Critique	• Migration progressive par site • Tests exhaustifs sur maquette • Fenêtres maintenance planifiées	• Procédure de rollback • Activation PCA • Support H24 pendant migration	Très faible	Elevée
R04	Non-conformité HDS/ISO27001	Faible	Critique	• Audit conformité préalable • Choix solutions certifiées • Accompagnement IT Conseils	• Audit correctif • Plan d'action de mise en conformité • Report certification	Très faible	Critique
R05	Résistance au changement utilistaeurs	Elevée	Moyenne	• Plan de formation des utilisateurs • Accompagnement personnalisé • Communication régulière	• Formation complémentaire • Support utilisateur renforcé • Ajustements fonctionnels	Moyenne	Faible
R06	Défaillance fournisseur (livraison/qualité)	Moyenne	Elevée	• Contrats avec pénalités • Multisourcing si possible • Qualification fournisseurs	• Activation clause pénalités • Fournisseur alternatif • Location temporaire	Faible	Moyenne
R07	Perte/corruption donnés migration	Faible	Critique	• Sauvegardes complètes pré-migration • Tests restauration • Migrations à blanc	• Restauration depuis sauvegarde • Ressaisie partielle si nécessaire • Activation PRA	Très faible	Elevée
R08	Cyberattaque pendant projet	Moyenne	Critique	• Segmentation réseau progressive • EDR/XDR dès début • Sensibilisation équipes	• Isolation segments infectés • Restauration depuis sauvegardes • Analyse forensique MicrosSOC	Faible	Critique
R09	Sous-dimmensionnement équipe	Elevée	Elevée	• Assistance IT Conseils • Prestataires spécialisés • Planning réaliste avec marges	• Renfort temporaire externe • Priorisation stricte • Délai supplémentaire	Moyenne	Moyenne
R10	Obsolescence maquette vs production	Moyenne	Moyenne	• Documentation détaillée • Versioning configuration	• Ajustements post-migration • Tests complémentaires	Moyenne	Moyenne
R11	Dérive objectifs écologiques	Moyenne	Faible	• Choix équipements labellisés • Procédure recyclage formalisée	• Compensation carbone • Renforcement politique RSE N+1	Faible	Faible
R12	Turnover équipe IT pendant projet	Faible	Elevée	• Documentation continue • Transfert de compétences • Conditions travail motivantes	• Recrutement accéléré • Formation intensive remplaçant • Prestataire transitoire	Faible	Moyenne
R13	Problème garantie/SAV constructeurs	Faible	Moyenne	• Contrats garantie 24/7 • Vérification clauses • Stock pièces critiques	• Escalade SAV • Équipement prêt temporaire • Activation clause pénalités	Faible	Faible
R14	Non-disponibilité cloud Azure	Très faible	Elevée	• SLA Microsoft 99.9% • Multi-région (Paris/Marseille)	• Attente rétablissement • Communication utilisateurs • Réclamation Microsoft	Très faible	Elevée

Figure 1 Tableau de l'analyse des risques

3.8 Parties prenantes

NOM	SITE / ENTREPRISE	RÔLE
Directeur Général	SAP	Commanditaire du projet
Directeur Administratif Financier	SAP	Sponsor du projet. Valider le budget. Approvisionne le matériel et les logiciels/licences.
Directeur RH	SAP	Piloter le chargé de Formation. Développement des compétences.
CODIR (Directeurs de sites)	SAP	Validation des orientations.
COPIL (Responsables des Services Centraux)	SAP	Orienter, piloter et valider les grandes étapes Piloter la communication entre le CODIR et le chef de projet
RSI	SAP	Chef de projet Définit la stratégie numérique et les évolutions technologiques. Garantit la cybersécurité et conformité RGPD, HDS, ISO27001 et toutes normes informatiques
Administrateur Réseau & Sécurité	SAP	Équipe projet Configuration réseau et sécurité
Technicien Support Informatique	SAP	Équipe projet Support utilisateurs et déploiement
Développeur et Gestionnaire Applicatif	SAP	Équipe projet Gestion des applications métiers
Chargé(e) de Formation et Développement des Compétences	SAP	Former les Chefs de Service
Chefs de Service	SAP	Former leur Service (Éducateurs et Psychologues)
IT Conseils	IT Conseils	Consultant externe
Fournisseurs		Fournir le matériel et les logiciels/licences
Services (Éducateurs, Psychologues, Centraux)	SAP	

Après avoir créé un registre des parties prenantes, nous avons créé une structure de communication. Ce schéma nous permet de nous rendre compte de la structure de communication des parties prenantes.

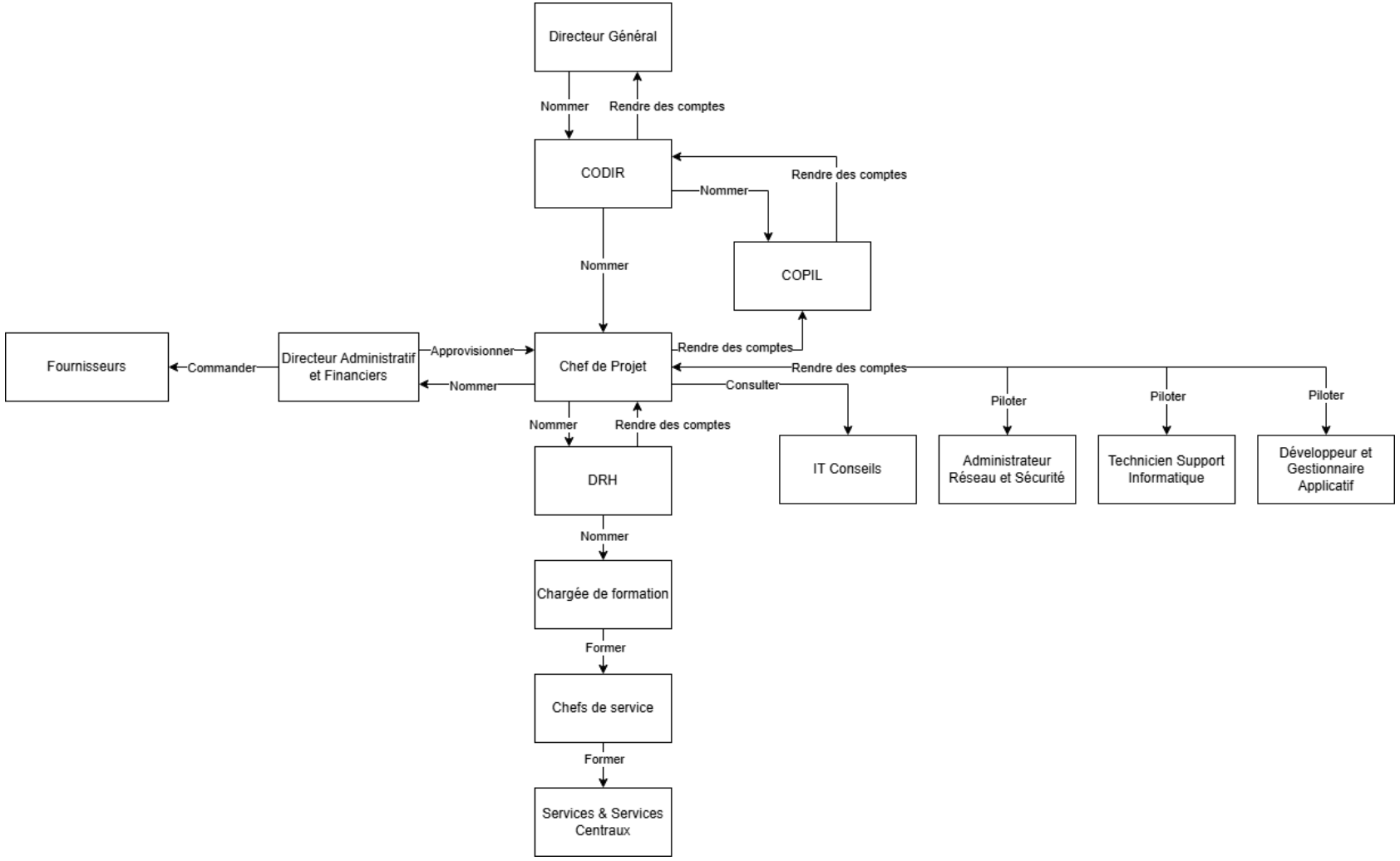


Figure 2 Structure de communication

3.9 Livrables

Phase	Livrable	Planning	Budget
MISSION 1 : Modéliser les infrastructures systèmes et réseaux			
Lot 1	Note de cadrage du projet	Mois 1	Investissement : • Parc utilisateur : 80-120 K€ • Serveurs : 40-60 K€ • Réseau : 30-50 K€ • Logiciels : 50-80 K€ Charges annuelles : • Licences : 20-30 K€ • Maintenance : 15-25 K€ • Hébergement : 10-15 K€ Total estimé : 345-500 K€ (1ère année)
Lot 1	Schémas d'infrastructure (logique et physique)	Mois 1-2	
Lot 1	Analyse des risques et plan d'action	Mois 1	
Lot 1	Récapitulatif des équipements	Mois 2	
Lot 1	Plan de normalisation (équipements, câblage)	Mois 2	
Lot 1	Maquette fonctionnelle de l'infrastructure	Mois 2	
Lot 1	Plan de recyclage des équipements	Mois 2	
MISSION 2 : Déployer les infrastructures systèmes et réseaux			
Lot 2	Configuration serveurs et services	Mois 3-5	Inclus dans budget Mission 1 Charges supplémentaires : • Formation : 10-15 K€ • Support déploiement : 5-10 K€
Lot 2	Plan d'adressage et routage	Mois 3-4	
Lot 2	Documentation technique complète	Mois 5	
Lot 2	Plan de migration et de bascule	Mois 4-5	
MISSION 3 : Maintenir et sécuriser les infrastructures			
Lot 3	Procédures de maintenance préventive/corrective	Mois 6-7	Inclus dans charges annuelles Investissements spécifiques : • Solution supervision : 15-20 K€ • Outils sécurité : 20-30 K€
Lot 3	Plan de continuité et reprise d'activité (PCA/PRA)	Mois 6-7	
Lot 3	Politique de sécurité et bonnes pratiques	Mois 7	
Lot 3	Solution de supervision et monitoring	Mois 7-8	
Lot 3	Plan de formation utilisateurs	Mois 8	

3.10KPI de pilotage et suivi de projet

3.10.1 KPI Budgétaires

KPI	Indicateur	Objectif	Formule de calcul	Fréquence de mesure
Respect du budget global	Ecart budget réel et prévisionnel	345K-500K (la première année)	Budget dépensé / budget prévu *100	Mensuel
ROI (Retour sur investissement) Prévisionnel	ROI à 5 ans	ROI de 130% sur 5 ans	(Gains - coûts)/ coûts *100	Annuel
Coût TCO	Coût total sur 5 ans	Réduction de 15% sur l'ancien SI	TCO nouveau SI / TCO ancien SI *100	Annuel

3.10.2 KPI de Délai

KPI	Indicateur	Objectif	Formule de calcul	Fréquence de mesure
Respect du planning global	Taux d'avancement du projet et planning prévisionnel	< 186 jours ouvrés (marge de 10 jours ouvrés)	Jours réels - Jours prévus	Hebdomadaire
Respect des jalons	% de jalons livrés à temps	100% des jalons respectés	Nb de jalons livrés / Nb total de jalons * 100	Par jalon
Délai de déploiement par site	Temps moyen de déploiement par site	Moins de 3 semaines par site	Date de fin de déploiement - date début de déploiement	Par site déployé
Retard cumulé	Nombre de jours de retard cumulés	0 jour	Date réelle - date prévue par tâches	Somme des écarts entre prévu et effectif

3.10.3 KPI de Qualité / Performance

KPI	Indicateur	Objectif	Formule de calcul	Fréquence de mesure
Disponibilité SI	Temps de fonctionnement / temps total * 100	99,9%	(temps total - temps indisponibilité) / temps total * 100	Mensuel
Fiabilité des processus	Taux d'erreurs (Avant / après ERP)	30% d'erreur en moins	Latence moyenne inter-sites	Audit qualité
Taux de tests réussis	% tests de maquette / PRA réussis	100%	(Nb tests réussis / Nb tests totaux * 100	Par test
Conformité réglementaire	Critères conformes / total critères * 100	90%	Nb équipements / Nb équipements total * 100	Mensuel

4 Tâches & charges

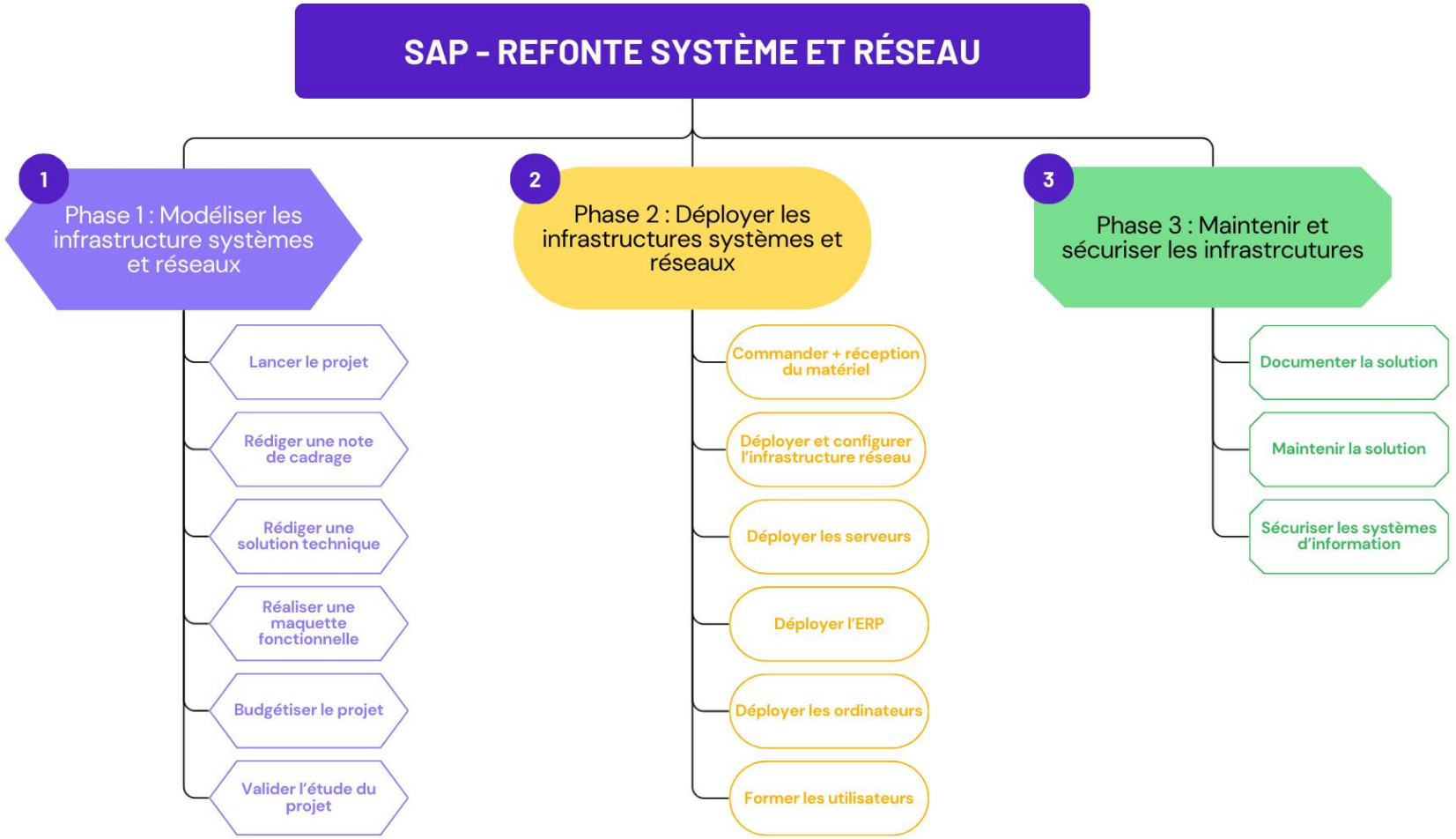


Figure 3 WBS

Phase	Tâches	Sous-tâches	Charge (j/h)	Délai (j)	Marge (j/h)
1 - Modéliser les infrastructures systèmes et réseaux	Lancer le projet		2		3
	Rédiger une note de cadrage		3		4
	Rédiger une solution technique		18		22
	Réaliser une maquette		8		10
	Valider l'étude du projet		3		4
	SOUS-TOTAL		**34**	**0**	**43**
2 - Déployer les infrastructures systèmes et réseaux	Commander + réception du matériel et licences			22	
	Déployer et configurer l'infrastructure réseau		18		22
	Déployer les serveurs		10		12
	Déployer l'ERP		15		19

	Déployer les ordinateurs		30		36
	Former les utilisateurs		30		36
	SOUS-TOTAL		**103**	**22**	**125**
3 - Maintenir et sécuriser les infrastructures	Documenter la solution		8		10
	Sécuriser les systèmes d'informations		18		22
	SOUS-TOTAL		**26**		**32**
	TOTAL		**163**	**22**	**200**
	TOTAL FINAL SANS MARGE			**185**	
	TOTAL FINAL AVEC MARGE			**222**	

PHASES	Tâches	Responsable des Systèmes d'Information	Directeur Général	Directeur Administratif Financier	Directeur RH	CODIR	COPIL	Administrateurs Réseau et Sécurité	Technicien Support Informatique	Développeur et Gestionnaire Applicatif	Chargé(e) de formation et développement des compétences	IT Conseils	Fournisseurs	Chefs de service	Services (Éducateurs, Psychologues, Centraux)
Modéliser les infrastructures systèmes et réseaux	Lancer le projet	R	A	I	I	C	C	I	I	I				I	
	Rédiger une note de cadrage	R	A			C	C					C			
	Rédiger une solution technique	A/R						C/I	C/I	C/I		C			
	Réaliser une maquette fonctionnelle	A/R						C/I	C/I	C/I					
	Validation de l'étude du projet	R	A	C		C	C								
Déployer les infrastructures systèmes et réseaux	Commander + réception du matériel	A		R		C	C	I	I	I			C/I		
	Déployer et configurer	A						R							

	l'infrastructure réseau														
	Déployer les serveurs	A						R							
	Déployer l'ERP	A								R					
	Déployer les ordinateurs	A							R						
	Former les utilisateurs	I			A						R			I	I
Maintenir et sécuriser les infrastructures	Documenter la solution	A/R						C	C	C					
	Maintenir la solution	A/R						C/I	C/I	C/I					

5 Solution cible

Afin de respecter chacune des fonctions techniques et contraintes énoncées dans le cahier de cahier des charges. Une solution a été réfléchie.

Fonction Technique 1 : Pour que tous les utilisateurs puissent accéder aux applications et services, il leur faut un accès distant et Wi-Fi sur tous les sites. Pour se faire, les bâtiments des sites auront des bornes Wi-Fi disposées de manière optimisée avec un roaming transparent. Pour l'accès à distance, les utilisateurs pourront se connecter via un client VPN SSL / TLS. Ils utiliseront leur identifiant AD avec mot de passe robuste et un code OTP pour la MFA. Toutes les connexions seront intégrées dans un journal de connexion du routeur / pare-feu (NGFw). De plus, une segmentation VLAN par service sera mise en place.

Fonction Technique 2 : Afin que tous les utilisateurs soient connectées à Internet et respecter la contrainte de haute disponibilité, nous avons décidé ainsi :

- Lille et Paris auront une FTTO 1 Gb/s garantie + une FTTE 1 Gb/s + un 4G/5G failover avec 50 Mb/s garanti.
- Toulouse aura une FTTO 1 Gb/s + un 4G/5G failover avec 50 Mb/s garanti.
- Lyon et Marseille auront une FTTE 1 Gb/s + un 4G/5G failover avec 50 Mb/s garanti.

1 pare-feu nouvelle génération (NGFw) sera installé et configuré sur chacun des sites. Ce dernier aura une garantie d'échange en moins de 24h et un service 24/7 permettant son remplacement dans la journée. Pour répondre à des contraintes de conformité, ce pare-feu sera certifié / agréé / qualifié par l'ANSSI.
Ce dernier utilisera une fonctionnalité nommée SD-WAN afin que tous les autres sites soient connectés entre eux. Le choix de ce protocole est dû au fait qu'il optimise automatiquement le trafic et le basculement intelligent entre les liens.

Pour les déplacements, les utilisateurs n'ayant pas de téléphone professionnel auront un boîtier 4G/5G mis à disposition le temps du déplacement pour accéder au Système d'Information via VPN de manière sécurisée sans utiliser de connexion publique.

Fonction Technique 3 : Pour permettre aux utilisateurs d'accéder aux stockages de fichiers, voici les solutions que nous mettrons en place sur chacun des sites :

- ***Lille*** : 1 Baie SAN de 24 To de stockage en RAID 6. A cette dernière, 1 hyperviseur sera installé avec 1 serveur virtuel DFS.
- ***Paris*** : 1 Baie SAN de secours de 24 To de stockage en RAID 6. 1 hyperviseur sera installé avec 1 serveur virtuel DFSR permettant la réplication du serveur de fichiers.
- ***Toulouse*** : 1 hyperviseur de backup sera installé. Il prendra le relais si Lille et Paris ne prennent pas le relais.

Chacun des serveurs de fichiers seront cryptés en dehors des heures de production en AES-256 avec l'algorithme de chiffrement SHA-256. Pour la connexion des utilisateurs et le transit des données, le protocole SMB 3.1.1 sera utilisé avec le chiffrement AES-256-GCM.

Pour les données qualifiées HDS (Hébergement de Données de Santé), elles seront stockées en Cloud certifiés HDS et avec 1 sauvegarde réalisée chez Microsoft à Marseille. En plus, la base de données de l'ERP médico-social sera stockée dans le Cloud Microsoft Azure.

Les utilisateurs auront accès à un stockage personnel en local. Un versionning de 30 jours sera mis en place ainsi que des quotas strictes pour les espaces personnelles (cf. FC7) et un archivage automatique des fichiers plus anciens de 2 ans. Ils auront à leur disposition via la suite Office 365, un espace personnel Cloud de 50 Go.

Fonction Technique 4 : Pour permettre aux utilisateurs d'imprimer en couleur ou noir et blanc en fonction de son service, 1 serveur d'impression sera installé sur l'hyperviseur. Afin de respecter une démarche écologique, l'impression sera par défaut en noir et blanc et 1 quota d'impression sera instauré par service. Afin de garantir une traçabilité, toute impression sera enregistrée et des alertes automatiques seront déclenchées lors de la détection d'impression massive.

Le parc imprimante sera géré par un prestataire.

Fonction Technique 5 : L'administrateur aura à sa disposition :

- 1 Serveur de supervision sur le site de Lille permettant la supervision de tout équipement. La base de données du serveur sera redondée sur le site de Paris.
- 1 supervision métrique des serveurs sera mise en place.
- Pour la supervision sécurité, une solution type SOC (Security Of Center). Cette solution doit proposer un EDR, une console XDR et un SIEM qui sera analysé par un prestataire de sécurité.

L'administrateur pourra gérer les utilisateurs, les groupes et les ordinateurs via l'Active Directory. Il pourra attribuer des stratégies de groupes (GPO). Une authentification MFA sera obligatoire pour les administrateurs pour se connecter en local comme sur le Cloud. Un Tiering Model sera mis en place pour cloisonner l'utilisation des utilisateurs ayant la permission administrateur. Chacun des comptes seront nominatifs pour permettre une meilleure traçabilité. Voici une explication du Tiering Model :

- Tier 0 – Administrateur ayant le droit et uniquement le droit de se connecter au serveur AD.
- Tier 1 – Administrateur ayant le droit de se connecter aux serveurs de production (hyperviseur, DFS, Impression…).
- Tier 2 – Administrateur local des posts créé par GPO de groupes restreints.

Fonction Contrainte 1 : Pour assurer la continuité de service du Système d'Informations, l'infrastructure sera la suivante :

- 1 baie SAN à Lille et 1 à Paris. Celle de Lille est la principale, 1 copie asynchrone se fait entre les 2 baies. La perte de données entre les 2 baies SAN lors d'une bascule après interruption de l'une d'entre elles, est de 30 secondes à 15 minutes maximum.
- 1 cluster Hyper-V de 3 nœuds, le nœud A à Lille, le B à Paris et le C à Toulouse (nœud de sauvegarde).
- 1 serveur AD DS et DNS principale sur le site de Lille, 1 réplication à Paris et 1 réplication de sauvegarde à Toulouse.
- Chaque site sera équipé de 2 switchs de niveau 3 en stack permettant une redondance. Les liens pour les équipements vitaux (baie SAN, serveurs) sont redondés.
- 1 maillage inter-sites est mis en place par le biais des routeurs / pare-feu nouvelle génération (NGFw) et le protocole SD-WAN. Chaque site a au moins 1 deuxième connexion Internet permettant la bascule si l'une d'entre elles dysfonctionne.
- 1 PRI (Plan de Reprise Informatique) et PCI (Plan de Continuité Informatique) seront créés.
- Pour le stockage, comme vu lors de la *FT3*, 24 To de stockage en RAID 6 par baie SAN sera configuré et utilisé.

Pour comprendre l'infrastructure système mise en place, vous pouvez retrouver en pièce-jointe les schémas correspondants à chaque site et un global. (Cf. Schéma).

Fonction Contrainte 2 : Comme énoncé lors de la FT5, 1 serveur de supervision sera installé sur l'hyperviseur de Lille. Ce dernier couvre l'ensemble du Système d'Information. Les données collectées seront stockées sur 12 mois glissants.

Fonction Contrainte 3 : Pour permettre à l'administrateur de gérer l'ensemble du SI, les outils suivants seront mit à sa disposition :

- Gestion centralisée des utilisateurs depuis l'Active Directory.
- Gestion du réseau centralisé à l'aide du contrôleur Wi-Fi centralisé, la gestion des switchs via interface web (stack management). Tableau de bord de gestion Cloud pour la gestion des pare-feu multi-sites.
- Gestion des serveurs à l'aide de Windows Admin Center.

Fonction Contrainte 4 : Le système de sauvegarde doit et sera conforme aux recommandations de l'ANSSI. Pour cela :

- Utilisation d'un logiciel de sauvegarde et de réplication avec rapport par mail au SI. Ce dernier doit être chiffré de bout en bout.
- Serveur de sauvegarde physique Windows avec disques durs internes dédiée sur le site de Lille.
- NAS de 50 To en RAID 6 sur le site de Paris.
- Système de sauvegarde 3-2-1-1-0 :
    - 3 copies de données. Production (serveurs de fichiers DFS), Sauvegarde locale sur NAS site Paris et Sauvegarde distante sur serveur de sauvegarde sur site de Lille. Les sauvegardes seront réalisées tous les jours à 4h, 12h et 20h.
    - 2 supports différents (NAS et serveur de sauvegarde).
    - 1 copie des sauvegardes en Cloud chez Azure Blob Storage en France (Marseille). Chiffrement AES-256 activé pour le transfert. Une copie mensuelle des sauvegardes critiques sera réalisée. 12 mois pour les données de santé et 36 mois pour la comptabilité.
    - 1 copie des sauvegardes hors ligne sur des disques externes USB chiffrés sur le site de Toulouse. Sauvegarde mensuelle sur les bandes. Stockage hors site physique dans 1 coffre fort. Test de restauration annuel depuis les bandes.
    - Test mensuel des sauvegardes pour un PRA efficace et garantir 0 erreur. Pour cela, tester 1 VM aléatoire par mois, 1 fichier utilisateur par semaine.

Fonction Contrainte 5 : Afin que les sondes et capteurs de supervision doivent être connectés par Wi-Fi, un VLAN Supervision leur sera dédié. Les équipements récents utilisent du Bluetooth LE (Low Energy). Les anciens seront identifiés par un code barre.

Fonction Contrainte 6 : Tous les équipements et éléments vitaux du SI seront sous garantie. Cette dernière permet d'éviter les frais de réparation non prévus mais aussi de garantir un remplacement, une réparation sur site ou un service client convenable aux attentes HDS. Pour cela, tous les équipements et éléments sous garantie sont les suivants :

- Garantie de 5 ans sur les switchs coeur ;
- Support 24/7, mise à jour firmware, échange express incluses pour Stormshield ;
- Garantie de 5 ans sur SAN/NAS + remplacement disque 4h ouvrée ;
- Contrat de maintenance annuel sur les onduleurs ainsi qu'une garantie de 3 ans est ajoutée ;
- Smartphones professionnels avec garantie + assurance casse/vol et remplacement sous 48h avec téléphone de prêt.

- Pour les serveurs, 1 garantie de 5 ans minimum sera ajoutée ainsi qu'une intervention sur site J+1 ouvrée (ou 4h si critique). Des pièces de rechange seront incluses. Remplacement préventif des disques à 70% durée de vie.

Fonction Contrainte 7 : Afin de rendre disponible et sécurisé les données sur l'ensemble des sites, mais également dans le cadre de la mobilité des utilisateurs, nous mettons en place les solutions suivantes :

- Un serveur DFS avec réplication (DFSR). Le serveur DFS est installé sur le site de Lille avec les données sur la baie SAN et le DFSR est installé sur le site de Paris. Avec le protocole SD-WAN utilisé par les routeurs / pare-feu StormShield, les utilisateurs de n'importe quel site peuvent accéder aux données de manière sécurisée.
- Avec un abonnement Microsoft Office 365 pour tous les utilisateurs, un SharePoint Online sera mis à disposition pour le partage documentaire et le travail collaboratif.
- Les utilisateurs disposent d'un espace de stockage personnel Cloud avec OneDrive de 50 Go. Pour le stockage personnel local, les utilisateurs disposent de 10 Go chacun.
- Grâce au serveur DFS, des dossiers par service seront créés et les utilisateurs appartenant au service auront un lecteur réseau mappé sur leur poste.
- Afin de sécuriser les connexions, des horaires d'accès seront instaurées.

Fonction Contrainte 8 : Pour que l'ensemble des utilisateurs aient accès à la messagerie, Microsoft Outlook dans l'abonnement Microsoft Office 365 sera utilisé.

Fonction Contrainte 9 : La solution de Microsoft Office 365 propose la suite bureautique suivante :

- Microsoft (Word, Excel, PowerPoint…)
- Teams
- SharePoint Online
- MS Project pour les chefs de projet
- Outlook

Afin de s'engager dans une politique RSE et de respecter la DEEE (Déchets d'Équipements Électriques et Électroniques), nous avons mis en place une procédure de recyclage du matériel que nous allons remplacer.

1. Pour les appareils en fin de vie ou qui serait renouvelé, permettre à tout le monde l'accès au numérique en faisant des dons de matériels informatiques obsolètes à des associations ou des particuliers comme de jeunes étudiant n'ayant pas la possibilité de se munir d'un équipement informatique. Les données seraient alors donc effacées et permettraient à l'équipement de bénéficier d'une seconde vie.
2. Remplacer le matériel en fonction de la consommation énergétique ou encore des matériaux qui les composent.
3. Superviser les équipements avec un outil de gestion (GLPI) afin de réduire les coûts inutiles (poste de travail en double, etc).
4. Faire appel à des entreprises spécialisées dans la récupération de Déchets d'équipements électriques et électroniques (DEEE) assurant le recyclage des équipements.

6 Budget

Le budget CAPEX de la solution cible sur la première année (An 1) est estimé à environ 650 000€. Vous pouvez retrouver en annexe, le tableau d'estimation du budget de la solution cible (cf. annexe).

Le budget OPEX pour le maintien et le fonctionnement de la solution est estimé par année à environ 150 000€ / an. De l'An 2 à 5, le budget est estimé à 600 000€. Vous pouvez retrouver en annexe le tableau OPEX (cf. annexe).

L'équipe interne composé d'un RSI (Responsable des Systèmes d'Informations), d'un alternant ASR (Administrateur Systèmes et Réseaux), d'un administrateur réseau, d'un technicien support et un développeur ont coût. De plus, l'équipe du projet est composée d'un DRH (Directeur de Ressources Humaines), d'un chargé de formations, d'un Directeur Administratif Financiers, des Chefs de services, Directeur des sites et Responsable des services centraux. Le budget est estimé à 300 000€.

Les prestations externes telles que les prestataires et IT Conseils, le coût est estimé à 80 000€ sur les 5 ans.

7 Annexes

7.1 Diagramme de GANTT

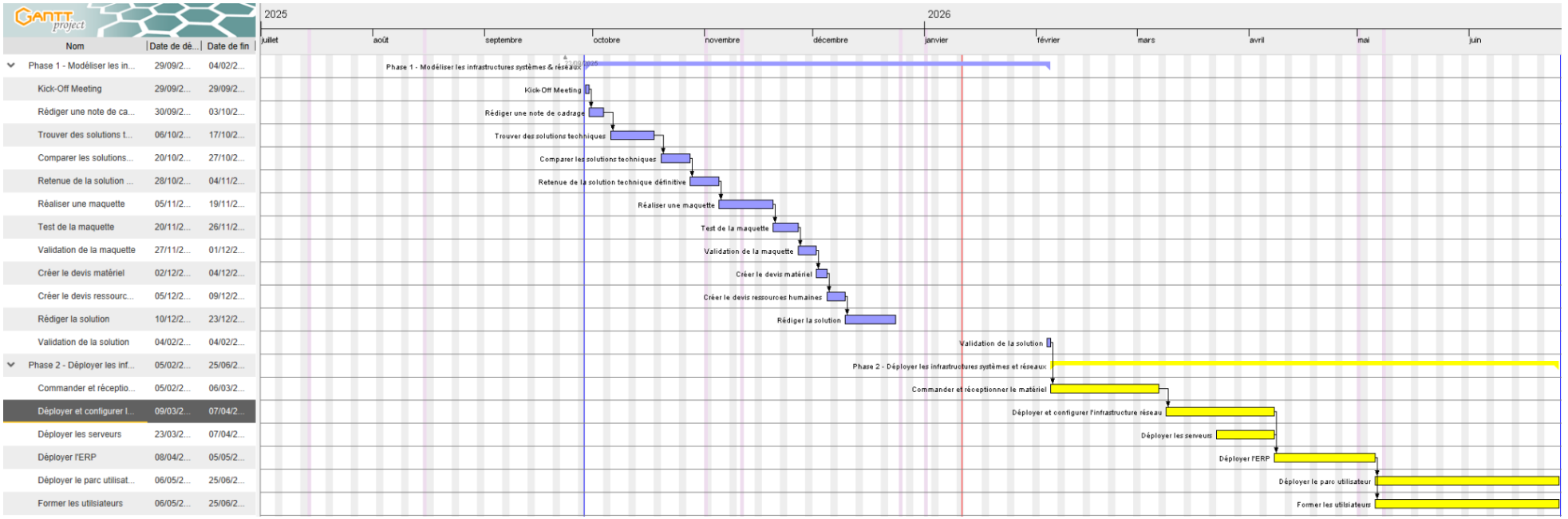


Figure 4 Diagramme de GANTT

7.2 Schéma infrastructure

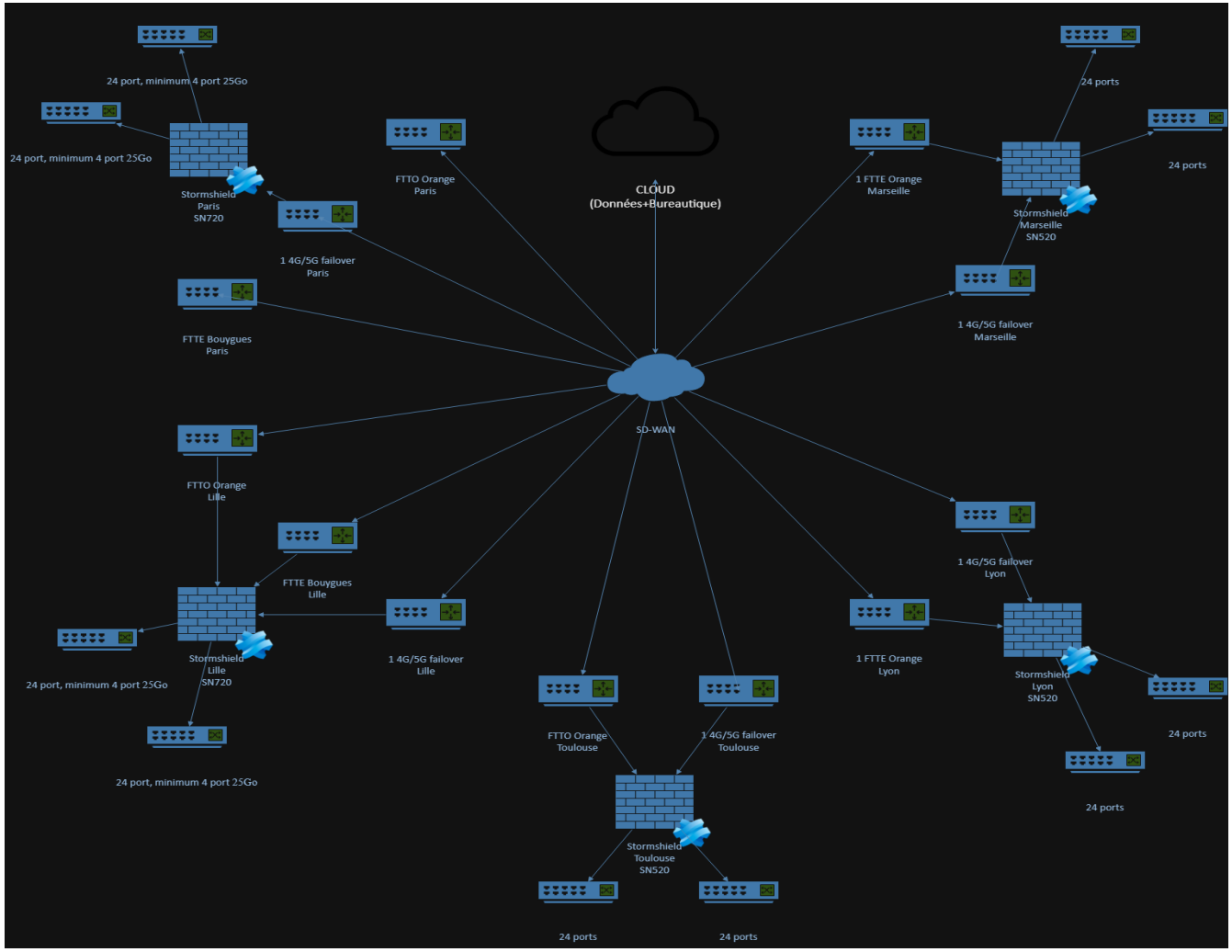


Figure 5 Schéma global de l'infrastructure

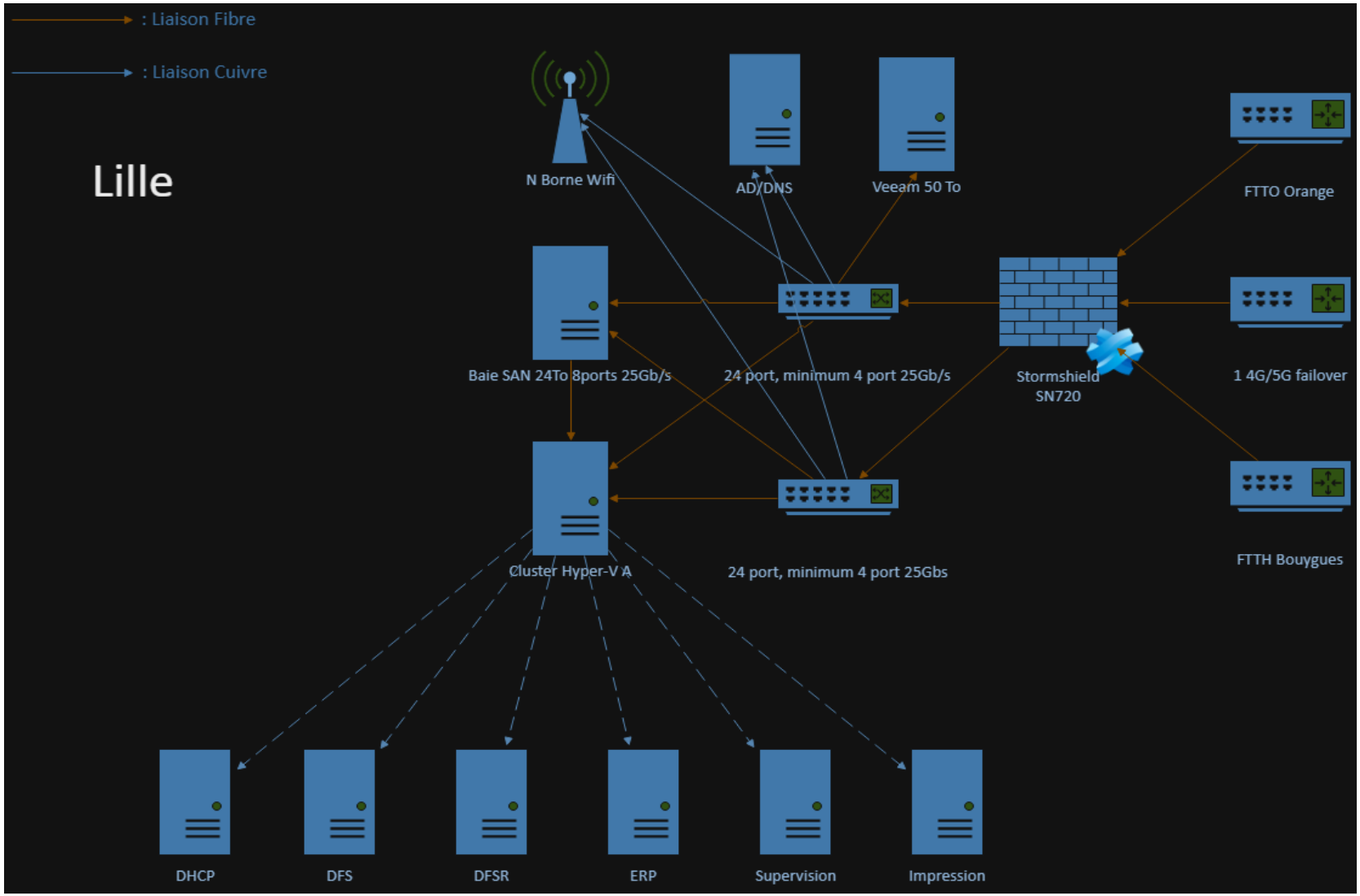


Figure 6 Schéma de l'infrastructure de Lille

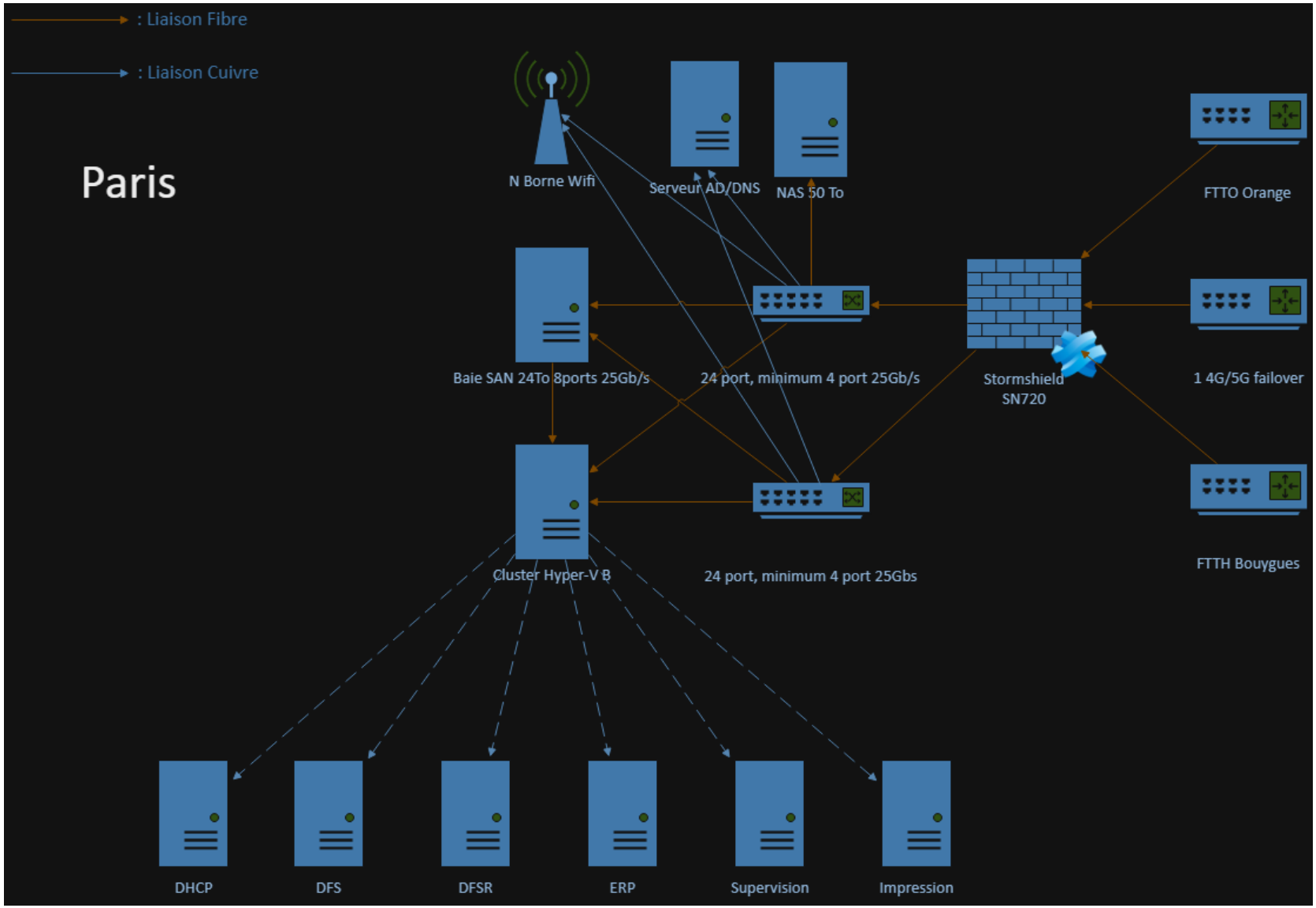


Figure 7 Schéma de l'infrastructure de Paris

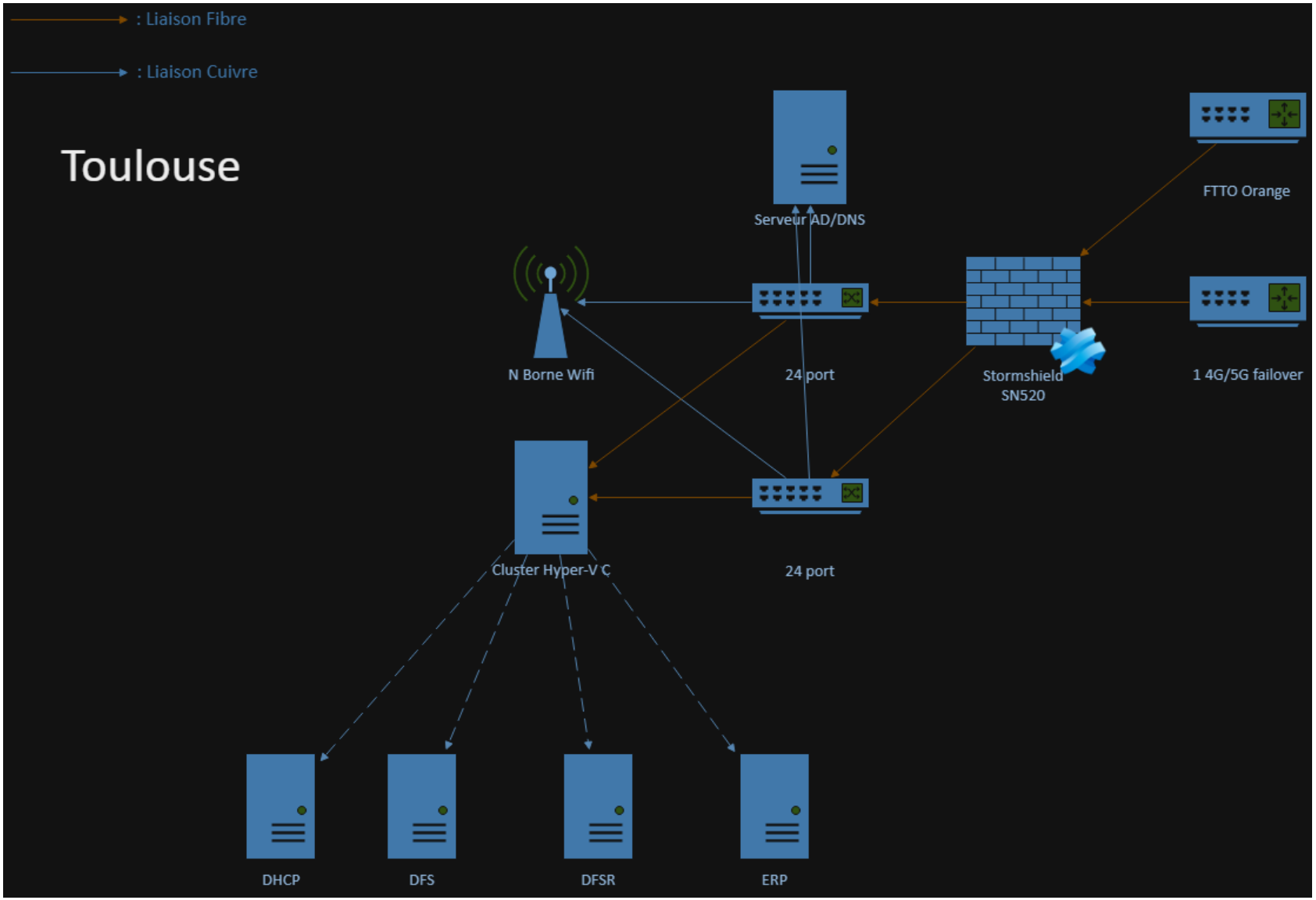


Figure 8 Schéma de l'infrastructure de Toulouse

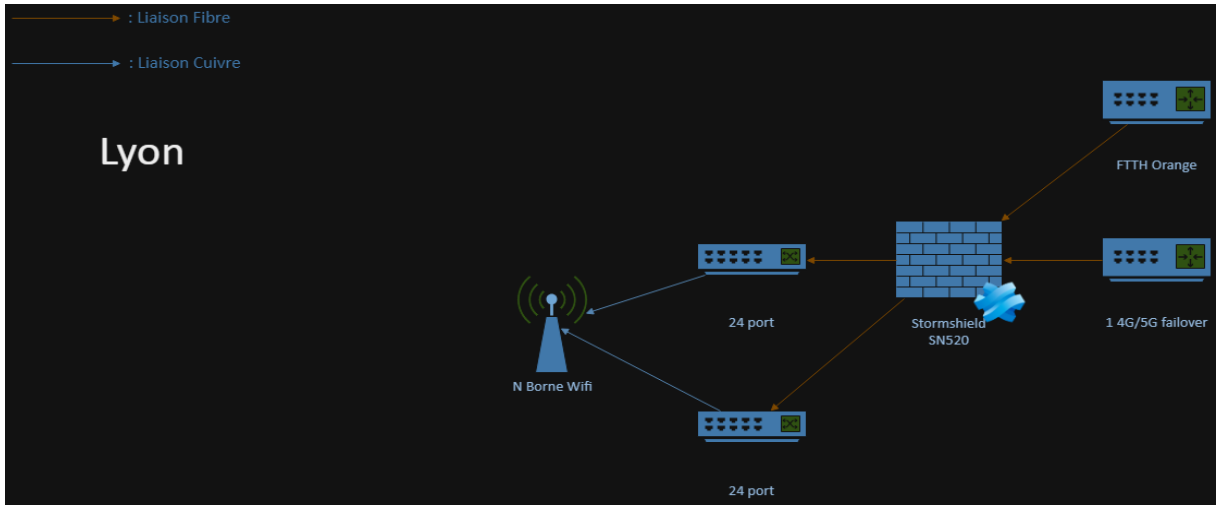


Figure 9 Schéma de l'infrastructure de Lyon

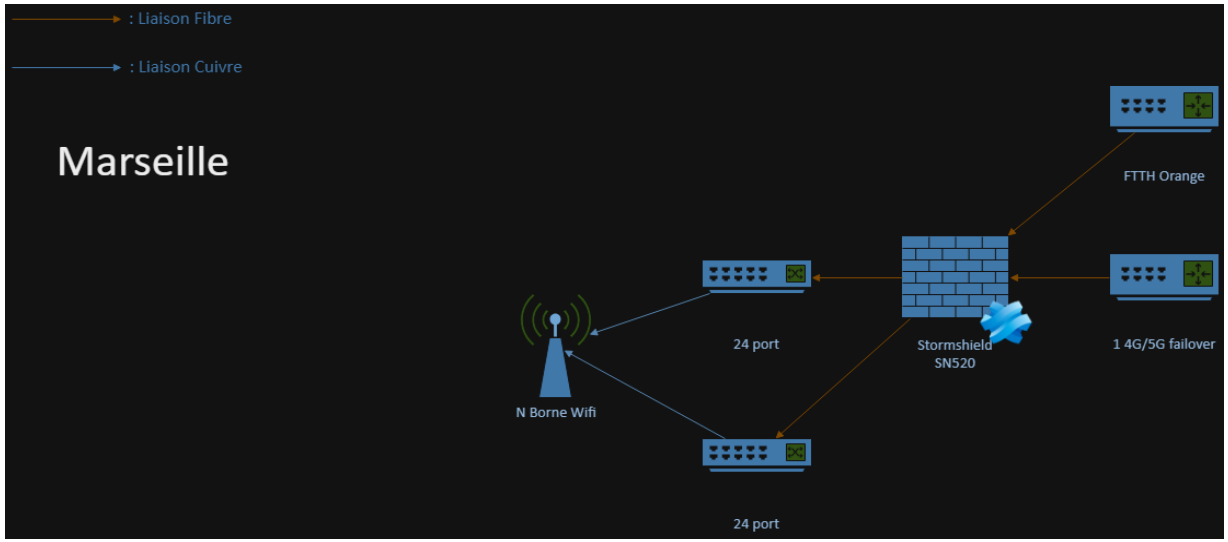


Figure 10 Schéma de l'infrastructure de Marseille

7.3 Budget

Poste budgétaire	Description	Montant HT
1 - Infrastructure serveurs		**99 500,00 €**
Hyperviseurs redondants	3 serveurs physiques haute disponibilité (Lille, Paris et Toulouse) - Capacité : support de virtualisation complète (8-10 VM) - Stockage : 5 SSD RAID 6 pour OS - Garantie : 3 ans avec remplacement à J+1 + extension de garantie de 2 ans	52 500,00 €
Baie SAN	2 baies SAN haute disponibilité (Lille et Paris) - Stockage: Stockage de 24 To en RAID 6 - Garantie : 3 ans avec remplacement à J+1 + extension de garantie de 2 ans	20 000,00 €
Serveur Active Directory	3 serveurs physiques (Lille, Paris et Toulouse) - Capacité : Accueillir un AD/DS et DNS - Stockage : 4 SSD RAID 5 pour OS et 4 To en RAID 6 - Garantie : 3 ans avec remplacement à J+1 + extension de garantie de 2 ans	15 000,00 €
Licences virtualisation	Licences hyperviseur professionnel (type Datacenter) pour les 2 sites - Support de multiples VM - Réplication inter-sites	12 000,00 €
2 - Infrastructure réseau et sécurité		**74 000,00 €**
Pare-feu nouvelle génération (NGFw)	5 pares-feux certifiés/recommandés ANSSI (Tous les sites) - Fonctionnalités : IPS, filtrage applicatif, VPN SSL/TLS - Support MFA intégré - Garantie : 3 ans avec remplacement en moins de 24h	40 000,00 €
Commutateurs de distribution	14 commutateurs niveau accès pour segmentation VLAN - Support PoE pour les bornes Wi-Fi - 48 ports minimum dont 2 SFP +	12 000,00 €
Infrastructure Wi-Fi	20 bornes Wi-Fi professionnelles - Standard Wi-Fi 6 (802.11ax) - Gestion centralisée (contrôleur intégré ou Cloud)	5 000,00 €
Logiciel de supervision et monitoring	Support du logiciel	1 000,00 €

Onduleurs	6 onduleurs professionnels (Lille, Paris et Toulouse) - Autonomie : 15 - 30 min (temps de sauvegarde et arrêt propre) - Garantie : 3 ans avec remplacement à J+1 si défaillance détectée	16 000,00 €
3 - Parc utilisateurs		**343 500,00 €**
Ordinateurs portables	450 postes de travail - Certifications : Energy Star et / ou EPEAT Gold - Configuration : adaptée bureautique + applications métiers. - Garantie : 3 ans sur site	300 000,00 €
Téléphone portables	135 téléphones portables	30 000,00 €
Solution EDR / XDR	Protection Endpoint avec console centralisée - Fonctionnalités : antivirus, anti-ransomware, détection comportementale - Conformité RGPD - 450 licences	13 500,00 €
4 - Stockage et sauvegarde		**28 000,00 €**
Serveur de sauvegarde	Serveur dédié pour les sauvegardes - Stockage haute capacité (>50 To)	10 000,00 €
NAS de sauvegarde	NAS dédié pour les sauvegardes - Stockage haute capcité (>50 To)	6 000,00 €
Disques externes rotatifs	10 disques durs externes haute capcité (12 To minimum) - Rotation journalière + stockage hors site - Débranchables à chaud	8 000,00 €
Logiciel de sauvegarde	Solution professionnelle adaptée à la méthode 3-2-1-1-0 - Fonctionnalités : Chiffrement de bout en bout, réplication, tests automatiques - Conformité ANSSI/RGPD - Licences serveurs	4 000,00 €
5 - Licences et abonnements (1 an)		**98 770,00 €**
Suite bureautique cloud	Microsoft 365 Business Premium (ou équivalent) - 450 licences utilisateurs - Inclus : messagerie, bureautique, stockage cloud (OneDrive), collaboration (Teams, SharePoint) - Conformité RGPD (datacenters UE) - Coût An 1 uniquement (renouvellement en OPEX An 2-5)	9 270,00 €

Microsoft Azure	Microsoft Cloud Azure - Base de données ERP 24 To hébergée à Paris - Sauvegarde hébergée à Marseille - Stockage en ligne de 24 To pour SharePoint Online	8 500,00 €
Abonnements pare-feu	Abonnements 1 an : signatures IPS, filtrage web, licences VPN SSL - Coût An 1 uniquement (renouvellement en OPEX An 2-5)	8 000,00 €
Abonnements Fibre + 4G/5G	Abonnements 1 an : FTTO + FTTE + 4G/5G failover	77 000,00 €
TOTAL CAPEX AN 1		**647 770,00 €**

Poste budgétaire	An 2	An 3	An 4	An 5	Total An 2 - 5
Licences Microsoft 365 (450 utilisateurs + augmentation de la masse salariale de 5%)	9 300,00 €	9 350,00 €	9 400,00 €	9 480,00 €	37 530,00 €
Abonnement Microsoft Azure Cloud	9 000,00 €	9 800,00 €	10 500,00 €	11 000,00 €	40 300,00 €
Abonnements pare-feu	8 000,00 €	8 000,00 €	8 000,00 €	8 000,00 €	32 000,00 €
Licences EDR/XDR (annuel)	13 500,00 €	13 500,00 €	13 500,00 €	13 500,00 €	54 000,00 €
Support logiciel sauvegarde	4 000,00 €	4 000,00 €	4 000,00 €	4 000,00 €	16 000,00 €
Support logiciel journalisation et monitoring	12 900,00 €	12 900,00 €	12 900,00 €	12 900,00 €	51 600,00 €
Formation continue (cybersécurité, ERP, nouveautés…)	3 000,00 €	3 000,00 €	3 000,00 €	3 000,00 €	12 000,00 €
Maintenance matériel	8 000,00 €	8 000,00 €	16 000,00 €	24 000,00 €	56 000,00 €
Abonnements FTTO et FTTE + 4G/5G	77 000,00 €	77 000,00 €	77 000,00 €	77 000,00 €	308 000,00 €
Total OPEX ANNUEL	**144 700,00 €**	**145 550,00 €**	**154 300,00 €**	**162 880,00 €**	**607 430,00 €**