

BLOC – INFRIR2 – Modéliser les infrastructures – KERNELAC



1 Table des matières

| | | |
|-------|---|----|
| 1 | Table des matières | 2 |
| 2 | Table des illustrations | 4 |
| 3 | Contexte | 5 |
| 3.1 | Présentation de la Mairie de KERNELAC | 5 |
| 3.2 | Enjeux et objectifs du projet | 5 |
| 3.2.1 | Enjeux du projet | 5 |
| 3.2.2 | Objectifs du projet | 5 |
| 3.3 | Organisation du projet | 6 |
| 3.3.1 | Parties prenantes | 6 |
| 3.3.2 | Gouvernance du projet | 7 |
| 3.3.3 | Structure de communication | 7 |
| 3.4 | Matrice RACI | 8 |
| 4 | Analyse de l'existant | 9 |
| 4.1 | Situation actuelle | 9 |
| 4.2 | Audit de conformité | 9 |
| 4.2.1 | Non-conformités réglementaires | 9 |
| 4.2.2 | Obsolescence technique | 10 |
| 4.2.3 | Vulnérabilités de sécurité | 11 |
| 5 | Cahier des charges | 12 |
| 5.1 | Périmètre du projet | 12 |
| 5.1.1 | Périmètre fonctionnel | 12 |
| 5.1.2 | Périmètre géographique | 12 |
| 5.2 | Hypothèses | 12 |
| 5.3 | Besoins fonctionnels | 13 |
| 5.3.1 | Fonctions Techniques | 13 |
| 5.3.2 | Fonctions Contraintes | 13 |
| 5.4 | Exigences du projet | 14 |
| 5.4.1 | Contraintes | 14 |
| 5.5 | Livrables attendus | 14 |
| 6 | Solution proposée | 16 |
| 6.1 | Architecture cible | 16 |
| 6.1.1 | Infrastructure serveur | 16 |
| 6.1.2 | Solution de sauvegarde | 16 |
| 6.1.3 | Architecture réseau | 16 |

| | | |
|-------|--|----|
| 6.1.4 | Postes utilisateurs..... | 17 |
| 6.2 | Justification des choix techniques | 18 |
| 6.3 | Schéma d'infrastructure..... | 21 |
| 7 | Analyse de risques | 22 |
| 7.1 | Méthodologie d'analyse | 22 |
| 7.1.1 | Matrice de criticité | 22 |
| 7.2 | Risques techniques | 22 |
| 7.3 | Risques organisationnels | 23 |
| 7.4 | Risques financiers | 24 |
| 7.5 | Risques planning | 24 |
| 7.6 | Risques réglementaires..... | 25 |
| 8 | Pilotage du projet | 26 |
| 8.1 | Planning prévisionnel..... | 26 |
| 8.2 | Budget détaillé..... | 28 |
| 8.2.1 | Principes du budget | 28 |
| 8.2.2 | Répartition du budget CAPEX..... | 29 |
| 8.2.3 | Répartition du budget OPEX | 31 |
| 8.3 | Indicateurs clés de performances..... | 31 |

2 Table des illustrations

| | |
|--|----|
| Figure 1 Structure de communication du projet | 7 |
| Figure 2 Matrice RACI..... | 8 |
| Figure 3 Schéma logique de Kernelac | 9 |
| Figure 4 Schéma de l'infrastructure cible | 21 |
| Figure 5 Matrice de criticité | 22 |
| Figure 6 WBS | 26 |
| Figure 7 Planning prévisionnel - Diagramme de GANTT..... | 27 |

3 Contexte

3.1 Présentation de la Mairie de KERNELAC

KERNELAC est une commune française de 4 000 habitants située en Bretagne. La Mairie emploie 79 salariés répartis sur 12 sites municipaux et dispose d'un budget de fonctionnement annuel de 5,57 M€ avec un excédent de 320 000 €.

L'organisation s'articule autour d'une Direction Générale des Services (DGS) dirigée par M. Simon JESECK et de trois pôles opérationnels : Petite Enfance/Jeunesse, Technique, et Attractivité & Dynamique Sociale.

La mission du BLOC 1 consiste à :

- Auditer l'existant : cartographier l'infrastructure actuelle (serveurs, réseau, stockage, applications métiers)
- Recueillir les besoins : identifier les attentes des 3 pôles métiers et de la DGS à partir de l'analyse fonctionnelle
- Concevoir la solution cible : proposer une architecture moderne avec redondance, segmentation VLAN, solution de sauvegarde, supervision centralisée
- Rédiger le cahier des charges : spécifications techniques, planning sur 8 mois, budget prévisionnel (investissement + charges sur 5 ans), analyse des risques et indicateurs de pilotage

3.2 Enjeux et objectifs du projet

3.2.1 Enjeux du projet

Le projet de refonte Système et Réseau de la Mairie de KERNELAC répond à des enjeux identifiés lors de l'audit de IT Conseils :

- Mobilité – Permettre l'accès au SI de manière sécurisée en télétravail ou en déplacements. Choisir des solutions adaptées aux déplacements.
- Sécurité – Conformité RGPD, NIS2, ANSSI et ISO27001/22301 pour la mairie de KERNELAC. Mettre à jour le parc informatique physique et logiciel.
- Résilience – Garantir une disponibilité de 99.9%. Implémenter un PCA/PRA opérationnel.
- Efficience – Optimiser les ressources du Système d'Information.
- Écoresponsabilité – Intégrer une démarche éco-responsable et RSE avec ISO14001 et la DEEE.

3.2.2 Objectifs du projet

Face aux enjeux identifiés, des objectifs S.M.A.R.T (Spécifiques, Mesurables, Atteignables, Réalistes, Temporels) ont été fixés. Voici la liste :

- Se mettre en conformité réglementaire :
 - o Conformité NIS2 en respectant 100% des mesures essentielles ;
 - o Conformité RGPD en créant un registre et en désignant un DPO ;
 - o Conformité ANSSI en appliquant les 40 règles d'hygiène de base.

- Garantir la disponibilité du Système d'Information :
 - o Disponibilité visée de 99,9% (maximum 8h45/an) ;
 - o Redondance pour tous les équipements informatiques critiques
 - o Mettre en place un PCA (Plan de Continuité d'Activité) et PRA (Plan de Reprise d'Activité) avec un RTO inférieur à 4 heures et un RPO inférieur à 1 heure ;
 - o Mise en place de sauvegardes opérationnels avec la méthode 3-2-1-0.
- Moderniser l'infrastructure, en y apportant :
 - o Un nouveau parc serveur ;
 - o Une nouvelle infrastructure réseau ;
 - o Un renouvellement du parc utilisateur (ordinateurs et téléphones professionnels).
- Améliorer l'efficacité opérationnelle :
 - o Obtenir une mobilité de 100% pour les salariés en télétravail ;
 - o Une supervision claire du SI ;
 - o Une réduction de 50% du temps de résolution des incidents au sein du support informatique.
- Intégrer une démarche éco-responsable :
 - o Green IT avec du matériel certifié Energy Star et / ou EPEAT Gold ;
 - o Respect de la réglementation DEEE (Déchets d'Équipements Électriques et Électroniques) en proposant une solution de recyclage de 100% du matériel remplacé ;
 - o Réduire de 30% la consommation électrique des équipements informatique ;
 - o Respect de la norme ISO 14001 avec une conformité de la gestion environnemental.

3.3 Organisation du projet

3.3.1 Parties prenantes

Les parties prenantes sont composées :

- Maire (M. BAILLY)
- Directeur Général des Services (M. JESECK)
- Responsable Informatique. Il jouera un rôle de chef de projet.
- Assistante de la Direction Générale des Services (Mme. MINNE)
- Assistantes administratives des pôles :
 - o Petite enfance, jeunesse (Mme. BOURSAULT)
 - o Technique (Mme. LEFEBVRE)
 - o Attractivité et dynamique sociale (Mme. KEYFISER)
- IT Conseils
- Technicien informatique
- Alternant ASR
- Intégrateurs/Fournisseurs retenu après un appel d'offre sur le marché public.

3.3.2 Gouvernance du projet

Pour la gouvernance du projet, un comité de Pilotage (COPIL) est nécessaire. Ce dernier sera composé de :

- Maire
- DGS
- Le Responsable Informatique
- Assistantes administratives des pôles

3.3.3 Structure de communication

Après avoir identifié les parties prenantes, j'ai créé une structure de communication.

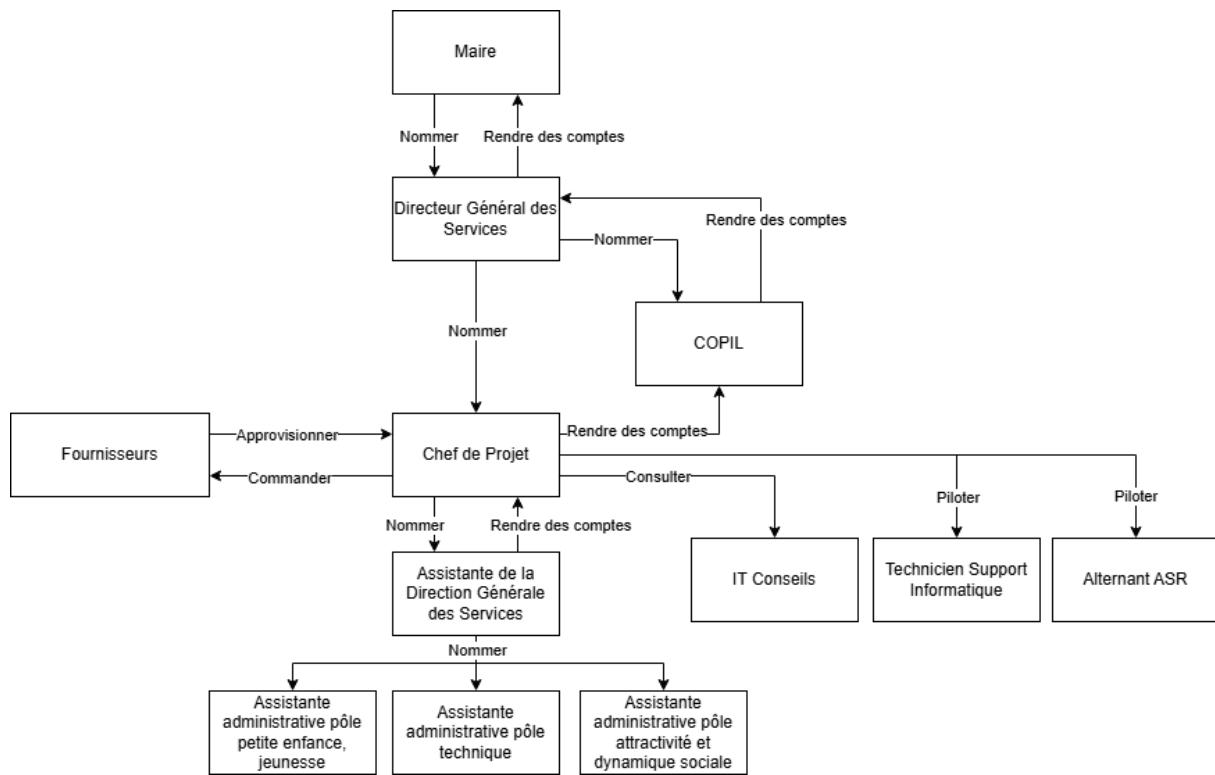


Figure 1 Structure de communication du projet

3.4 Matrice RACI

| PHASES | Tâches | Chef de projet | Maire | Directeur Général des Services | COPIL | Alternant ASR | IT Conseils | Fournisseurs | Assistante de la DGS | Assistantes administratives des pôles | Pôles |
|---|--|----------------|-------|--------------------------------|-------|---------------|-------------|--------------|----------------------|---------------------------------------|-------|
| Modéliser les infrastructures systèmes et réseaux | Lancer le projet | R | A | I | I | | | | I | | |
| | Rédiger une note de cadrage | R | | A | C | | | | | | |
| | Rédiger une solution technique | A/R | | | | C/I | C | | | | |
| | Rédiger un cahier des charges techniques | A/R | | | | | C | | | | |
| | Budgétiser le projet | | | | | | | | | | |
| | Validation de l'étude du projet | R | A | | C | | | | | | |
| Déployer les infrastructures systèmes et réseaux | Commander + réception du matériel | A/R | | | C | I | | C/I | | | |
| | Déployer et configurer l'infrastructure réseau | A | | | | R | | | | | |
| | Déployer les serveurs | A | | | | R | | | | | |
| | Déployer le parc utilisateur | A | | | | R | | | | | |
| | Former les utilisateurs | A | | I | | | | | I | R | I |
| | Documenter la solution | A | | | | R | | | | | |
| Maintenir et sécuriser les infrastructures | Maintenir la solution | A/R | | | | C/I | | | | | |
| | Sécuriser les systèmes d'information | A/R | | | | C/I | | | | | |

Figure 2 Matrice RACI

4 Analyse de l'existant

4.1 Situation actuelle

La mairie de KERNELAC a un parc informatique vieillissant. Ce dernier est composé de :

- 8 serveurs situés à la Mairie dont :
 - o 5 machines virtuelles sous Windows Server 2012 R2
 - o 2 Hyperviseurs de la marque Dell sous Windows Server 2012 R2
 - o 1 serveur de la marque Dell sous Windows Server 2008 R2.
- 104 ordinateurs portables de la marque Dell situés à la Mairie.
- 6 imprimantes réseau.
- 1 réseau local équipé de la marque D-Link pour les routeurs, commutateurs et pare-feu.

Ci-dessous, une représentation de la cartographie actuelle du parc informatique.

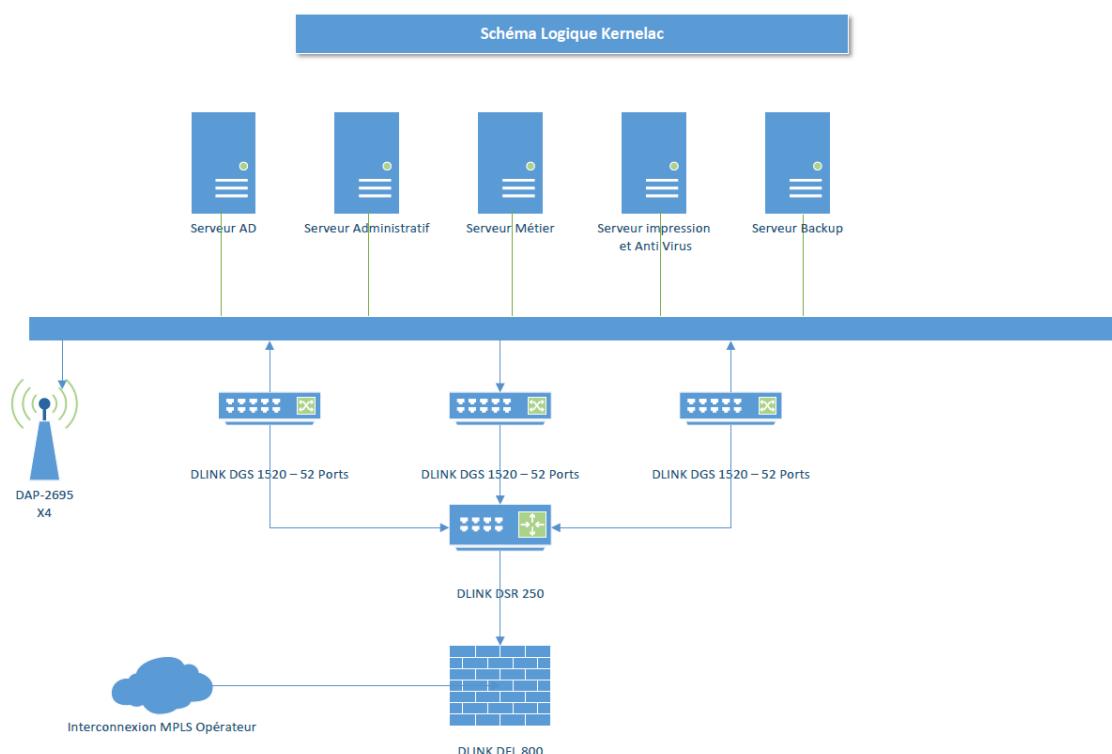


Figure 3 Schéma logique de Kernelac

4.2 Audit de conformité

4.2.1 Non-conformités réglementaires

L'audit réalisé par le consultant externe IT Conseils a démontré des écarts d'un point de vue réglementaire du secteur public. Les écarts identifiés sont :

- Conformité RGPD (Règlement Général de la Protection des Données) qui comporte :
 - o Une absence de registre des traitements de données (Article 30) ;
 - o Aucun Délégué à la Protection des Données a été désigné (Article 37) ;
 - o Aucune analyse d'impacts (PIA).

- Conformité NIS2 (Network & Information Security) qui comporte :
 - o Une absence de cartographie des services critiques ;
 - o Aucune procédure de gestion des incidents cyber ;
 - o Une formation à la cybersécurité non réalisée ;
 - o Une absence de surveillance et de journalisation ;
 - o Un plan de continuité et de reprise d'activité (PCA / PRA) inexistant.
- Conformité ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) qui comporte :
 - o Une absence de politique de mot de passe robuste ;
 - o Aucune centralisation et analyse de la journalisation des accès ;
 - o Windows 7 encore utilisé ;
 - o Aucune segmentation VLAN ;
 - o Aucune authentification multi-facteurs (MFA) mise en place pour l'accès VPN. Seul un mot de passe est requis ;
 - o Une documentation interne de la politique de sécurité non à jour ;
 - o Un inventaire du SI non à jour.

4.2.2 Obsolescence technique

Comme vu dans l'inventaire, le parc informatique est obsolète. Cette obsolescence met à risque la sécurité des données ainsi que la continuité de service. Les systèmes obsolètes sont :

- Windows Server 2008 R2 installé sur 1 serveur. Ce système d'exploitation n'a plus de support et de mise à jour de sécurité depuis le 14 janvier 2020 ;
- Windows Server 2012 R2 installé sur 5 machines virtuelles et 2 hyperviseurs (Hyper-V). Ce dernier n'a plus de support et de mise à jour de sécurité depuis le 10 octobre 2023.
- Windows 10 installé sur 104 ordinateurs portable. Le support de Windows 10 s'est arrêté le 14 octobre 2025.
- Office 2016 Standard installé sur tous les ordinateurs. Le support de cette suite bureautique s'est arrêté le 14 octobre 2025.

L'impact d'avoir des systèmes d'exploitation n'ayant plus de support et de mise à jour de sécurité :

- Des CVE critiques non corrigées qui peut engendrer une exploitation ;
- Une incompatibilité avec des nouvelles solutions ;
- Une impossibilité de mettre à jour les applications métiers ;
- Une productivité réduite.

De plus, le matériel informatique n'est plus sous garantie. L'impact de ne plus avoir d'équipements sous garantie est :

- Une panne majeure peut prolonger les services ;
- Le coût des interventions urgentes sont élevées.

4.2.3 Vulnérabilités de sécurité

De plus, l'audit de IT Conseils révèle des failles de sécurité majeures. Ces dernières sont :

- Une architecture réseau non sécurisée par :
 - o L'absence de segmentation réseau (VLAN) ;
 - o Le réseau Wi-Fi invité non isoler du réseau administratif ;
 - o Pare-feu D-Link grand public (box opérateur + NAT).
- Une gestion des accès insuffisante par :
 - o Un VPN utilisé uniquement par la Direction Générale des Services, sans authentification multi-facteurs (MFA). Un simple mot de passe est requis ;
 - o Une absence de politique de mots de passe robuste ;
 - o Aucune gestion centralisée des droits.
- Des sauvegardes non fiables par :
 - o Des sauvegardes locales sur NAS uniquement ;
 - o Une externalisation hebdomadaire via disque USB ;
 - o Aucun test régulier de restauration ;
 - o Une absence de PCA/PRA.
- Une supervision et détection absente par :
 - o Aucune solution de journalisation centralisée (SIEM) ;
 - o Aucun monitoring des ressources ;
 - o Aucune protection EDR sur les ordinateurs.

5 Cahier des charges

5.1 Périmètre du projet

5.1.1 *Périmètre fonctionnel*

Le périmètre fonctionnel inclus :

- Infrastructure des serveurs
- Architecture réseau
- Parc informatique des utilisateurs
- Solution de sauvegarde et PCA / PRA
- Supervision
- Sécurité du Système d'Information
- Conformité réglementaire

5.1.2 *Périmètre géographique*

Le périmètre géographique inclus :

- Les établissements et locaux municipaux appartenant à la Mairie de KERNELAC :
 - o Mairie
 - o Ateliers municipaux
 - o Espace PERCEVAL
 - o Espace Social Père BLAISE : Secours Catholique
 - o Salle LEODAGAN
 - o Espace Multi Accueil de la Dame du LAC
 - o Jardin d'enfant Dame SELI
 - o Espaces sportifs LANCELOT
 - o Espace culturel du Roi BURGONDE
 - o Salle des fêtes du Roi ARTHUR
 - o Halle des sports du Maître d'armes
 - o Espace Vert
 - o Stade de football Excalibur

5.2 Hypothèses

Ce projet repose sur des hypothèses. Les hypothèses identifiées sont :

- Disponibilité des parties prenantes :
 - o COPIL disponible pour les réunions
 - o Responsable SI disponible 80% du projet
- Accompagnement au changement :
 - o Formation des 79 agents
 - o Support technique disponible
- Continuité des services pendant le renouvellement :
 - o Les interventions hors heures ouvrées seront-elles possibles ?
 - o Les bascules critiques pourront-elles être faites le week-end ?
 - o Les services publics sont-ils maintenus pendant la bascule ?

- Infrastructures existantes :
 - o Les locaux techniques sont-ils conformes ?
 - o L'alimentation électrique est-elle stable ?
 - o Les abonnements fibres sont-ils adaptés ?

5.3 Besoins fonctionnels

5.3.1 Fonctions Techniques

FT1 – Tout utilisateur accède aux applications et services. Pour cela, chacun doit pouvoir accéder à distance aux ressources et avoir un accès Wi-Fi disponible dans l'ensemble des sites.

FT2 – Tout utilisateur est connecté à Internet. Ils doivent pouvoir accéder à Internet peu importe le site et dans leur déplacement.

FT3 – Tout utilisateur accède au stockage de fichiers. Le stockage doit être centralisé. Il doit avoir au minimum un niveau RAID 5. De plus, la baie de stockage à une capacité de X go.

FT4 – Tout utilisateur est connecté aux imprimantes. Ils doivent pouvoir imprimer en couleur ou en N/B en fonction de la politique attribuée à chacun de leurs services. L'impression en noir et blanc doit être priorisée.

FT5 – L'administrateur SR monitore et gère le SI. La gestion et le monitoring doit être accessible depuis une console en place sur les postes de contrôle. Cela doit être accessible à partir des desktops des techniciens ou des administrateurs. L'administrateur donne les droits d'accès aux périphériques, applications et données, soumis à l'accord de la Direction.

5.3.2 Fonctions Contraintes

FC1 – Le système doit assurer la continuité de service. Il doit y avoir une redondance DNS, AD, DHCP, des services, des commutateurs cœur de réseau, des lignes Internet, des moyens d'interconnexion et d'un stockage à haut niveau de disponibilité.

FC2 – L'application de supervision doit couvrir l'ensemble du SI. La solution doit être intégrée sur le serveur central. Les données historiques de ce dernier doivent être hébergées sur le serveur.

FC3 – L'administrateur doit pouvoir manager l'ensemble du SI. Ce dernier doit pouvoir paramétrier le réseau afin d'optimiser les flux. Il doit pouvoir surveiller depuis une console les charges réseau, l'état des serveurs et déployer les stations à distance.

FC4 – Les données doivent faire l'objet d'une sauvegarde. Un système doit être présent pour assurer la sauvegarde des données.

FC5 – Les sondes et capteurs de supervision doivent être connectables par Wi-Fi. Elles doivent permettre la connexion d'IOT. Les équipements récents sont compatibles Bluetooth. Pour les anciens, ils sont identifiés à partir d'un code barre.

FC6 – Tous les éléments vitaux du SI doivent faire l'objet d'une garantie. Les serveurs, routeurs, commutateurs, firewall, stockages de données sont concernés. Ils doivent et peuvent être remplacés en 24H.

FC7 – Les données doivent être disponible et sécurisé sur l'ensemble des sites, mais également dans le cadre de la mobilité des utilisateurs. Les données doivent être accessibles depuis le SI et les autres sites. Elles doivent être accessible depuis des technologies ou moyens de type Cloud. Les utilisateurs disposeront d'un espace personnel de X Go. Ils doivent avoir accès à un lecteur réseau correspondant au domaine d'activité de leur service. De plus, les horaires d'accès sont en conformité avec le tableau communiqué.

FC8 – L'ensemble des utilisateurs ont accès à la messagerie. L'accès est disponible au sein du SI mais également en dehors. Les horaires d'accès sont en conformité avec le tableau communiqué.

FC9 – L'ensemble des utilisateurs doit disposer de la suite bureautique. Suite bureautique Microsoft, Messagerie Outlook, Collaboratif SharePoint et Teams et de Planification MS Project pour les chefs de service.

5.4 Exigences du projet

5.4.1 Contraintes

Les contraintes sont :

- Apporter une architecture redondante
- La durée de 8 mois pour réaliser le projet
- La part du budget de 200 000€
- La disponibilité du SI à 99.9%
- Les obligations réglementaires du RGPD, NIS2 et ISO27001.

5.5 Livrables attendus

Le projet est structuré en 3 missions avec des livrables spécifiques.

La première mission consiste à modéliser l'infrastructure. Les livrables attendus sont :

- Inventaire, audit et cartographie de l'infrastructure existante ;
- Analyse des besoins ;
- Solution système, réseau et sécurité souhaitée ;
- Schéma de l'infrastructure souhaitée ;
- Analyse de risques ;
- Budget prévisionnel et planning.

La deuxième mission consiste à déployer le parc informatique. Les livrables attendus seront :

- Configuration réseau de la nouvelle architecture ;
- Déploiement de la nouvelle infrastructure serveur ;
- Déploiement du parc utilisateur ;
- Mise en place de la solution de sauvegarde ;
- Documentation de la solution.

La troisième mission consiste à sécuriser le parc informatique. Les livrables attendus sont :

- Création d'un PCA / PRA
- Mise en place d'une solution de supervision et de journalisation ;
- Validation de conformité envers les réglementations et normes suivantes : RGPD, NIS2, ISO27001 et ISO22301 ;
- Formation des agents.

6 Solution proposée

6.1 Architecture cible

6.1.1 *Infrastructure serveur*

Premièrement, l'infrastructure serveur. Cette dernière aura 1 hyperviseur sur le site de la Mairie et 1 hyperviseur sur le site des ateliers municipaux. L'hyperviseur de la Mairie aura les rôles suivants installés :

- AD/DS DNS ;
- DHCP ;
- Serveur d'impression ;
- DFS ;
- Supervision installée.

Pour l'hyperviseur situé dans les ateliers municipaux, les rôles installés sont :

- Réplication AD/DS et DNS ;
- Réplication DHCP ;
- DFSR.

Ces hyperviseurs auront une capacité de stockage suffisante de 5 To en RAID 6. La redondance sera assurée pour une continuité de service optimale. Les hyperviseurs et machines virtuelles disposeront des dernières mises à jour de système d'exploitation.

6.1.2 *Solution de sauvegarde*

Pour assurer un PCA/PRA opérationnel, une solution de sauvegardes doit être apportée. En s'appuyant sur le guide de l'ANSSI, le système de sauvegarde 3-2-1-1-0 est à implanté. Pour se faire, 1 serveur de sauvegarde sera installé à la mairie, 1 NAS sera installé dans les ateliers municipaux. Des disques durs journaliers débranchables à chaud et stocker hors site seront mis en place à la mairie. Les données sauvegardées seront :

- Les disques durs des machines virtuelles
- Les dossiers et fichiers de production.

Ces données seront sauvegardées tous les jours 7h et 18h. Des tests de restauration des sauvegardes seront effectués tous les mois afin d'avoir aucune erreur.

La solution logicielle doit :

- Cryptage et algorithme de chiffrage de bout en bout ;
- Possibilité de réplication des sauvegardes vers d'autres systèmes ;
- En conformité avec le RGPD et recommandé par l'ANSSI.

6.1.3 *Architecture réseau*

Pour la partie réseau, à la Mairie et aux ateliers municipaux, des pare-feu nouvelle génération seront installés. Ces derniers doivent être du matériel recommandé et / ou certifié par l'ANSSI. Une garantie de changement de matériel en cas d'incident dans un délai de 24 heures sera incluse.

En réseau local, 2 commutateurs d'agrégation redondé seront situés derrière le pare-feu. Puis, des commutateurs de niveau 2 afin de pouvoir créer des VLANs. Le découpage de ces deniers sera :

- VLAN Serveur ;
- VLAN Direction ;
- VLAN Production ;
- VLAN IoT ;
- VLAN Supervision.

La Mairie et les ateliers municipaux pourront communiquer via SD-WAN. Ils sortiront vers Internet avec :

- 1 FTTE
- 1 4G/5G failover.

Pour les autres sites, une box 4G/5G sera installée. Les agents se connecteront dessus. Pour accéder au système d'information de manière sécurisée, ils utiliseront un VPN SSL/TLS avec authentification via utilisateur de l'AD et mot de passe robuste en plus d'une MFA.

6.1.4 Postes utilisateurs

Tous les ordinateurs des utilisateurs seront remplacés.

Les postes seront dotés d'une solution d'antivirus EDR. Cet EDR doit avoir une console XDR pour permettre aux administrateurs de superviser la sécurité du parc utilisateur et serveur. Cette solution doit être en conformité avec le RGPD et hébergée sur le territoire de l'U.E.

Les Fonctions Contraintes 8 et 9 décrivent une solution de messagerie et bureautique (Microsoft Office). Pour cela, la suite Microsoft Office 365 sera installée pour leur permettre :

- Un accès à leurs mails en situation de nomadisme ou en présentiel ;
- Un accès à la suite bureautique de Microsoft ;
- Une possibilité pour les administrateurs de créer et / ou gérer des règles de chiffrement et de filtrage sur la messagerie ;
- Un travail collaboratif à l'aide de SharePoint Online et Microsoft Teams pour les agents ;
- Un stockage personnel sécurisé dans le Cloud via OneDrive ;
- Des outils de planification pour les chefs de service.

Pour permettre un accès à distance et sécurisé au système d'information, une solution VPN SSL/TLS avec authentification via utilisateur de l'AD et mot de passe robuste en plus d'une MFA sera installée et configurée.

6.2 Justification des choix techniques

| Critère | HPE ProLiant | Dell PowerEdge | Lenovo ThinkSystem |
|------------------------|---------------|----------------|--------------------|
| Fiabilité (MTBF) | 1,2M heures | 1,1M heures | 1M heures |
| Garantie et support | J+1 sur site | J+1 sur site | J+2 région |
| Compatibilité Hyper-V | Certifié SVVP | Certifié | Certifié |
| Gestion à distance | iLO (inclus) | iDRAC (payant) | XClarity |
| Rapport Qualité / Prix | 17500€/unité | 19 000 € | 16 500 € |

Le choix retenu est HPE ProLiant pour les raisons suivantes :

- Fiabilité éprouvée
- iLo inclus
- Support local
- Écosystème Hyper-V
- Évolutivité

| Critère | Hyper-V Cluster | Vmware vSphere | Proxmox VE |
|-------------------------|--------------------|----------------------|-------------------------|
| Coût licences (2 hôtes) | 12 000 € | 25 000 € | 0 € |
| Réplication inter-sites | Natif | Natif | Module payant |
| Haute disponibilité | Failover Cluster | vSphere HA | Moins mature |
| Intégration AD/DNS | Natif Windows | Via LDAP | Via LDAP |
| Complexité | Familier équipe IT | Courbe apprentissage | Expertise Linux requise |
| Support professionnel | Microsoft Premier | Vmware Support | Communauté |

Le choix retenu sera Hyper-V Cluster pour les raisons suivantes :

- Coût
- Intégration native
- Compétences internes
- Failover automatique
- Réplication Hyper-V Replica
- Conformité NIS2 grâce à une journalisation native.

| Critère | Stormshield | Fortinet Fortigate | Cisco |
|----------------------|------------------------|-----------------------|-----------------|
| Qualification ANSSI | Standard | Aucune | Aucune |
| Interface française | Oui (éditeur français) | Anglais majoritaire | Anglais |
| Support français | 24/7 français | 24/7 anglais/français | 8h-18h français |
| Prix (2 unités) | 16 000 € | 13 000 € | 22 000 € |
| Journalisation ANSSI | Conforme RGS v2,0 | Conforme | Conforme |

Le choix retenu sera Stormshield pour les raisons suivantes :

- Qualification ANSSI
- Souveraineté numérique
- Interface en français
- Support 24/7 francophone
- VPN SSL/TLS natif
- MFA intégré
- Journalisation native en conformité avec le RGPD et les bonnes pratiques ANSSI.

| Critère | Ubiquiti UniFi | Cisco Catalyst | HPE Aruba |
|---------------------|----------------------------|--------------------|------------------------|
| Prix (parc) | 19 000 € | 45 000 € | 38 000 € |
| Gestion centralisée | UniFi Controller (gratuit) | Cisco DNA (payant) | Aruba Central (payant) |
| Wi-Fi 6 (802.11ax) | Oui | Oui | Oui |
| PoE+ | Oui | Oui | Oui |
| Support VLAN | Oui | Oui | Oui |
| Interface | Web moderne | CLI complexe | CLI + Web |
| Garantie | 2 ans (extensible 5 ans) | 3 ans (NBD) | 3 ans (NBD) |

Le choix retenu sera Ubiquiti UniFi pour les raisons suivantes :

- Le rapport qualité / prix
- La gestion unifiée gratuite et native
- Interface de gestion intuitive
- Écosystème homogène
- Performance suffisante

| Critère | HP ProBook | Dell Latitude | Lenovo ThinkPad |
|------------------|--------------------------|----------------|-----------------|
| Prix (/unité) | 700 € | 1 050 € | 1 100 € |
| Écocertification | EPEAT Gold + Energy Star | EPEAT Gold | EPEAT Gold |
| Garantie | 3 ans sur site | 3 ans sur site | 3 ans dépôt |
| Réparabilité | 8,5/10 | 08/10 | 7,5/10 |
| Support local | SAV Brest | SAV Brest | SAV Paris |

Le choix retenu sera HP ProBook pour les raisons suivantes :

- L'économie possible grâce à un coût moindre
- Éco-responsabilité
- Support local

| Critère | Veeam Backup & Replication | Windows Server Backup |
|-------------------------|----------------------------|------------------------|
| Prix | 2000€/an | Inclus Windows Server |
| Support Hyper-V | Natif (CBT) | Natif |
| Réplication inter-sites | Oui (WAN Accelerator) | Non |
| Chiffrement | AES-256 bout en bout | BitLocker uniquement |
| Tests automatiques | SureBackup | Manuel |
| Restore granulaire | Fichiers/AD/Exchange | VM complète uniquement |
| Conformité ANSSI | Recommandé (3-2-1-1-0) | Partiel |
| Support professionnel | 24/7 français | Microsoft (payant) |

Le choix retenu sera Veeam Backup & Replication pour les raisons suivantes :

- Utilisation et normalisation dans la quasi-totalité des entreprises du monde
- Conformité ANSSI
- Chiffrement de bout en bout
- Réplication optimisée
- Restauration rapide
- Granularité par le choix des fichiers à restaurer.

| Critère | FTTE | FTTO |
|---------------------|-----------------------------------|----------------------|
| Débit symétrique | 1 Gbps download / 500 Mbps upload | 1 Gbps symétrique |
| Latence | 5-10 ans | < 2 ms |
| SLA (disponibilité) | 99,5% (GTR 4h) | 99,9% (GTR 2h) |
| Prix mensuel | 500€/mois | 1200€/mois |
| Coût sur 5 ans | | 9 000 € |
| Installation | 2 semaines | 2-3 mois |
| Propriété fibre | Opérateur | Propriété municipale |

Le choix retenu sera FTTE pour les raisons suivantes :

- Rapport coût / performance
- Besoins réels adaptés
- SLA acceptable
- Délai de déploiement acceptable
- Pas de travaux civils

6.3 Schéma d'infrastructure

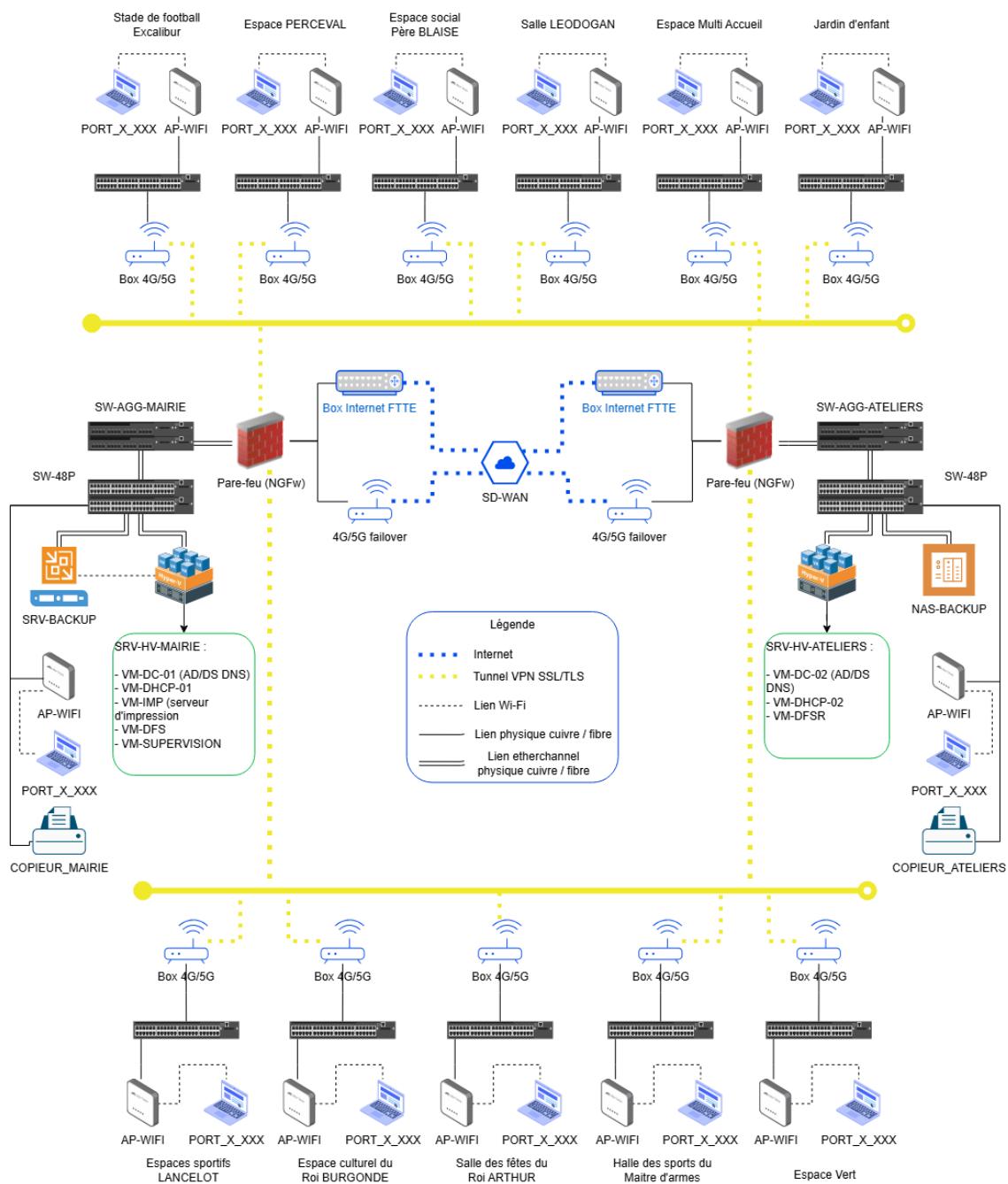


Figure 4 Schéma de l'infrastructure cible

7 Analyse de risques

7.1 Méthodologie d'analyse

7.1.1 Matrice de criticité

Afin de procéder à une analyse de risques conformes, une matrice doit être établie. En voici le résultat.

| | | | | | | |
|----------------|-------------|--------------------|------------|----------|----------|---------------|
| Gravité | Très élevée | 5,00 | 10,00 | 15,00 | 20,00 | 25,00 |
| | Élevée | 4,00 | 8,00 | 12,00 | 16,00 | 20,00 |
| | Moyenne | 3,00 | 6,00 | 8,00 | 12,00 | 15,00 |
| | Faible | 2,00 | 4,00 | 6,00 | 8,00 | 10,00 |
| | Très faible | 1,00 | 2,00 | 3,00 | 4,00 | 5,00 |
| | | Impossible | Improbable | Possible | Probable | Très probable |
| | | Probabilité | | | | |

Figure 5 Matrice de criticité

7.2 Risques techniques

RT-01 : Incompatibilité des applications métiers avec la nouvelle infrastructure

| Élément | Détail |
|--------------------|---|
| Description | Les logiciels métiers (état civil, finances, urbanisme, cantine) ne fonctionnent pas sur Windows Server 2022 ou avec Office 365 |
| Cause | Applications développées pour Windows Server 2008/2012, éditeurs disparus ou versions non maintenues |
| Gravité | ÉLEVÉE - Blocage des services municipaux essentiels (état civil, comptabilité) |
| Probabilité | POSSIBLE - Applications anciennes mais pas toutes testées |
| Criticité | 12 |

RT-02 : Défaillance matérielle pendant la migration

| Élément | Détail |
|--------------------|--|
| Description | Panne d'un hyperviseur, commutateur ou du système de stockage pendant la phase de migration |
| Cause | Matériel ancien encore en place, surtension, surchauffe, défaut de fabrication du nouveau matériel |
| Gravité | TRES ÉLEVÉE - Interruption totale des services (état civil, accueil, applications métiers) |
| Probabilité | IMPROBABLE - Nouveau matériel sous garantie |
| Criticité | 10 |

RT-03 : Perte de données lors de la migration

| Élément | Détail |
|--------------------|--|
| Description | Corruption ou perte de données pendant le transfert depuis les anciens serveurs (2008R2/2012R2) |
| Cause | Erreur de manipulation, corruption fichiers, script de migration défectueux, interruption pendant transfert |
| Gravité | TRES ÉLEVÉE - Perte de documents administratifs, données RH, finances (obligation légale de conservation) |
| Probabilité | IMPROBABLE - Mais impact catastrophique |
| Criticité | 10 |

RT-04 : Saturation de la bande passante Internet/MPLS

| Élément | Détail |
|--------------------|--|
| Description | Les connexions Internet et MPLS actuelles ne supportent pas la charge Office 365 (79 utilisateurs) + VPN + supervision cloud |
| Cause | Sous-dimensionnement des liens, trafic Office 365 (OneDrive, Teams, SharePoint) non anticipé |
| Gravité | MOYENNE - Lenteurs, timeouts, impossibilité de travailler pour les utilisateurs distants |
| Probabilité | POSSIBLE - Office 365 consomme beaucoup de bande passante |
| Criticité | 8 |

7.3 Risques organisationnels

RO-01 : Résistance au changement des agents

| Élément | Détail |
|--------------------|--|
| Description | Les 79 agents refusent ou peinent à adopter les nouveaux outils (Office 365, VPN avec OTP, nouvelles procédures) |
| Cause | Peur du changement, habitudes ancrées, manque de formation, âge moyen élevé, fracture numérique |
| Gravité | MOYENNE - Perte de productivité temporaire, erreurs utilisateurs, tickets support massifs |
| Probabilité | PROBABLE - Changement majeur pour une mairie de 4000 hab |
| Criticité | 12 |

RO-02 : Indisponibilité des parties prenantes clés

| Élément | Détail |
|--------------------|---|
| Description | Le Maire, le DGS, le Responsable Informatique ou les assistantes administratives sont absents lors de décisions critiques |
| Cause | Maladie, congés, obligations électorales, surcharge de travail, réunions conseil municipal |
| Gravité | MOYENNE - Retard dans les validations, blocage des jalons, dérive du planning |
| Probabilité | POSSIBLE - Élus et cadres très sollicités |
| Criticité | 8 |

RO-03 : Manque de ressources internes (Responsable Informatique surchargé)

| Élément | Détail |
|--------------------|---|
| Description | Le Responsable Informatique (80% du projet) et l'alternant ASR (100%) ne suffisent pas à gérer le projet + le support courant |
| Cause | Sous-estimation de la charge, incidents sur l'existant, support utilisateurs pendant migration |
| Gravité | ÉLEVÉE - Retard projet, qualité dégradée, burnout des ressources |
| Probabilité | PROBABLE - Équipe IT réduite pour un projet d'envergure |
| Criticité | 16 |

7.4 Risques financiers

RF-01 : Le budget n'est pas validé

| Élément | Détail |
|--------------------|---|
| Description | Le COPIL ne valide pas la part du budget. |
| Cause | Trop coûteux |
| Gravité | ÉLEVÉE - Décalage de tout le planning (effet domino), dépassement des 8 mois |
| Probabilité | POSSIBLE - Pénurie semiconducteurs récurrente |
| Criticité | 12 |

RF-01 : Dépassement de la part du budget initial

| Élément | Détail |
|--------------------|--|
| Description | Les coûts réels (matériel, licences, prestations) dépassent le budget voté. |
| Cause | Hausse des prix fournisseurs, besoins additionnels non prévus, réserve de contingence insuffisante, change € si matériel importé |
| Gravité | ÉLEVÉE - Blocage projet, nécessité d'un vote complémentaire du Conseil Municipal (délai 2-3 mois) |
| Probabilité | PROBABLE - Marché volatil, inflation |
| Criticité | 16 |

7.5 Risques planning

RP-01 : Retard de livraison du matériel

| Élément | Détail |
|--------------------|---|
| Description | Les fournisseurs ne livrent pas les équipements informatiques dans les délais. |
| Cause | Rupture de stock, problème de supply chain mondiale, douanes, grève transporteurs |
| Gravité | ÉLEVÉE - Décalage de tout le planning (effet domino), dépassement des 8 mois |
| Probabilité | POSSIBLE - Pénurie semiconducteurs récurrente |
| Criticité | 12 |

RP-02 : Interventions impossibles pendant heures ouvrées

| Élément | Détail |
|--------------------|--|
| Description | Les coupures nécessaires (migration serveurs, réseau) ne peuvent pas être faites en journée sans impacter les services publics (état civil, accueil) |
| Cause | Obligation de continuité du service public, pas d'interruption possible 8h-17h |
| Gravité | MOYENNE - Nécessité de travailler hors heures (soirs/week-ends), fatigue équipe, coûts supplémentaires prestataires |
| Probabilité | TRES PROBABLE - Services publics prioritaires |
| Criticité | 15 |

7.6 Risques réglementaires

RR-01 : Non-atteinte de la conformité RGPD/NIS2 dans les délais

| Élément | Détail |
|--------------------|---|
| Description | À la fin du projet, la mairie n'est toujours pas conforme RGPD (registre, DPO) ou NIS2 (gestion des incidents, PCA/PRA) |
| Cause | Sous-estimation de la charge administrative, complexité réglementaire, manque d'expertise juridique/sécurité |
| Gravité | TRES ÉLEVÉE - Sanctions CNIL (jusqu'à 20M€ ou 4% budget), mise en demeure, audit ANSSI négatif |
| Probabilité | POSSIBLE - Réglementations complexes |
| Criticité | 15 |

8 Pilotage du projet

8.1 Planning prévisionnel

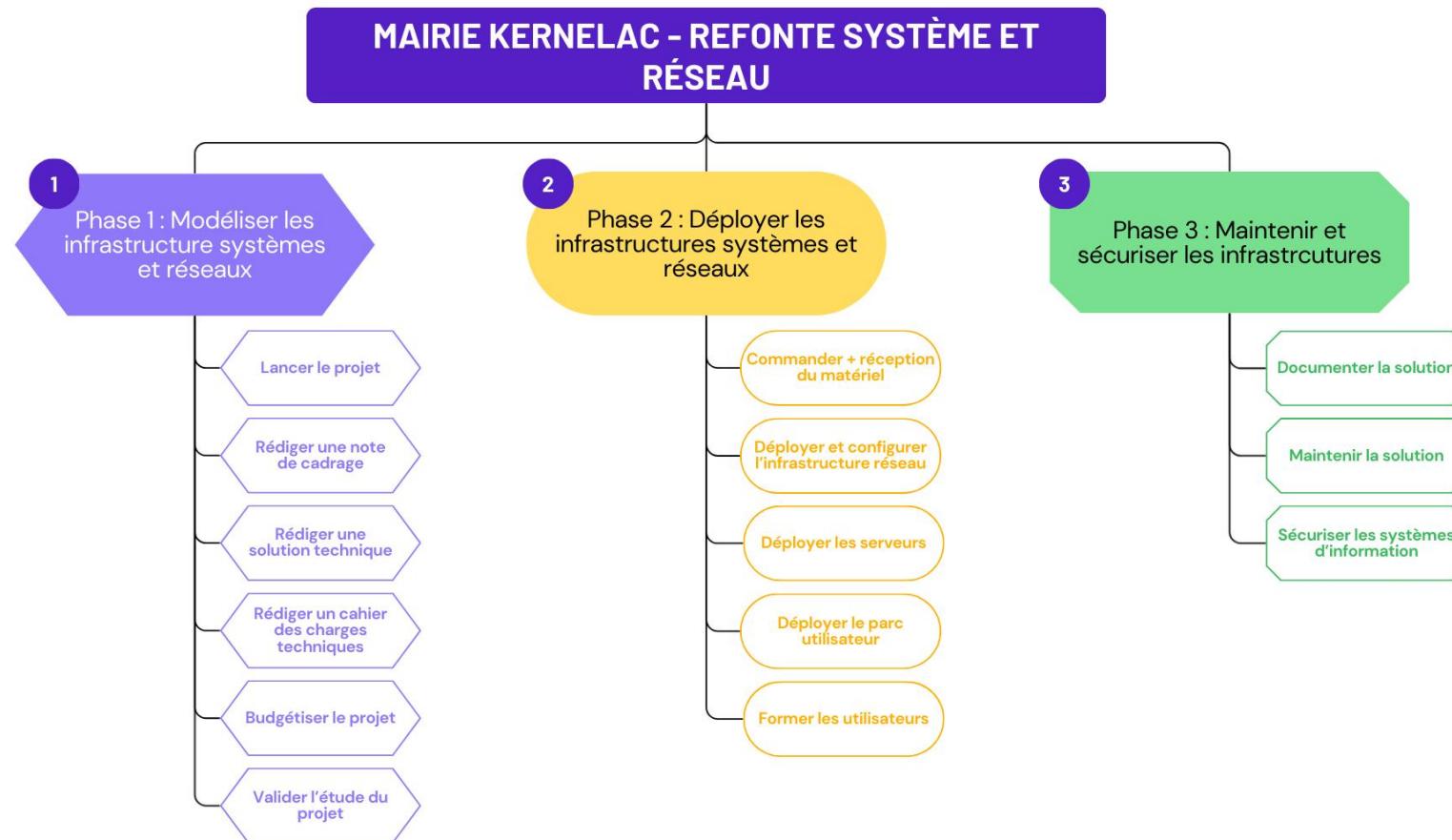


Figure 6 WBS

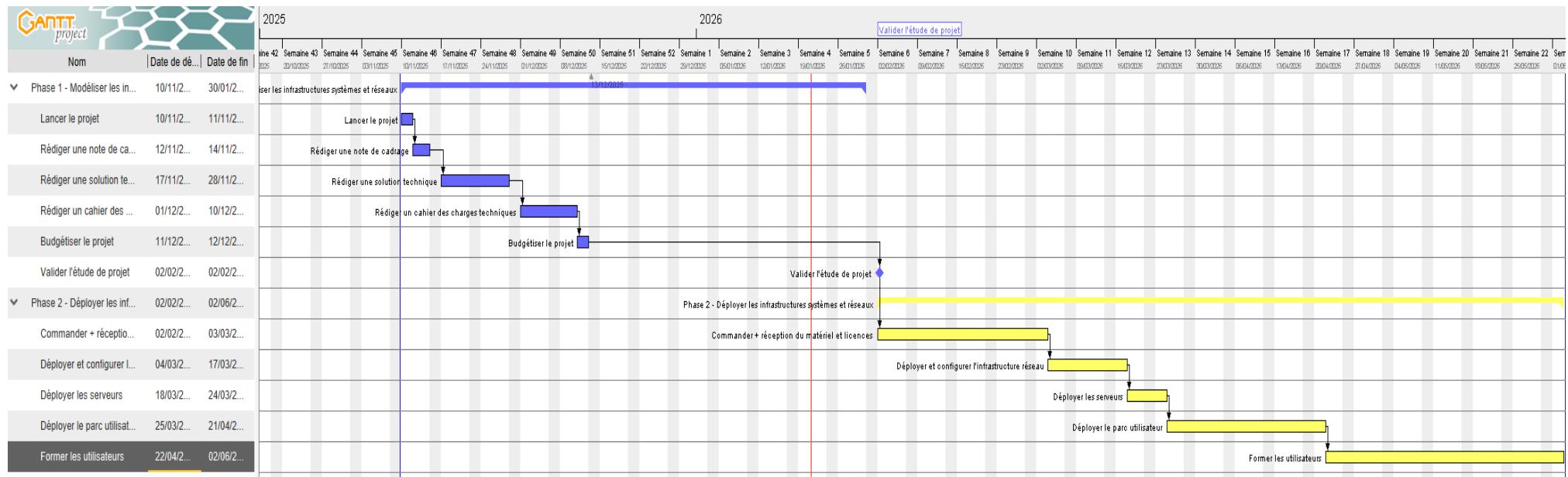


Figure 7 Planning prévisionnel - Diagramme de GANTT

| Phase | 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 | 10 | | 12 |
| | Rédiger un cahier des charges techniques | 8 | | 10 |
| | Budgétiser le projet | 2 | | 3 |
| | Valider l'étude du projet | 3 | | 4 |
| | SOUS-TOTAL | 28 | 0 | 36 |
| 2 - Déployer les infrastructures systèmes et réseaux | Commander + réception du matériel et licences | | 22 | |
| | Déployer et configurer l'infrastructure réseau | 10 | | 12 |
| | Déployer les serveurs | 5 | | 6 |
| | Déployer le parc utilisateur | 20 | | 24 |
| | Former les utilisateurs | 30 | | 36 |
| | SOUS-TOTAL | 65 | 22 | 78 |
| 3 - Maintenir et sécuriser les infrastructures | Documenter la solution | 8 | | 10 |
| | Sécuriser les systèmes d'informations | 18 | | 22 |
| | SOUS-TOTAL | 26 | 0 | 32 |
| | TOTAL | 119 | 22 | 146 |
| | TOTAL FINAL SANS MARGE | | | 141 |
| | TOTAL FINAL AVEC MARGE | | | 168 |

8.2 Budget détaillé

8.2.1 Principes du budget

Le budget du projet s'articule autour d'une logique CAPEX et OPEX. L'investissement CAPEX est un investissement sur la 1^{ère} année. L'OPEX, c'est le budget de fonctionnement nécessaire après la 1^{ère} année jusqu'à la 5^{ème} année.

L'année 1, le CAPEX est de 200 000€. C'est l'investissement initial nécessaire à la refonte du système et réseau de la mairie de KERNELAC.

Les années 2 à 5, l'OPEX est estimé à environ 30 000€/an. Ce qui donne un budget nécessaire au fonctionnement de 120 000€.

Le budget estimé sur 5 ans est de 320 000€. Ce budget peut être amené à évoluer au fur et à mesure du projet.

L'équipe interne composé d'un RSI (Responsable des Systèmes d'Informations) et d'un alternant ASR (Administrateur Systèmes et Réseaux) ont un coût. Le coût est estimé à 58 000€.

Les prestations externes tels que IT Conseils ou d'autres prestataires démarchés dans le futur ont un coût estimé à 45 000€.

8.2.2 Répartition du budget CAPEX

| Poste budgétaire | Description | Montant HT |
|--|--|--------------------|
| 1 - Infrastructure serveurs | | 47 000,00 € |
| Hyperviseurs redondants | 2 serveurs physiques haute disponibilité (Maire + Ateliers) - Capacité : support de virtualisation complète (8-10 VM) - Stockage : 4 SSD RAID 5 pour OS, Stockage de 5 To en RAID 6 - Garantie : 3 ans avec remplacement à J+1 + extension de garantie de 2 ans | 35 000,00 € |
| 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 | | 40 000,00 € |
| Pare-feu nouvelle génération (NGFw) | 2 pares-feux certifiés/recommandés ANSSI (Mairie + Ateliers) - Fonctionnalités : IPS, filtrage applicatif, VPN SSL/TLS - Support MFA intégré - Garantie : 3 ans avec remplacement en moins de 24h | 16 000,00 € |
| Commutateurs d'agrégation | 4 commutateurs cœur de réseau avec redondance - Support VLAN, QoS, PoE+ - Empilage (stacking) pour haute disponibilité | 5 000,00 € |
| 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 | 18 bornes Wi-Fi professionnelles - Standard Wi-Fi 6 (802.11ax) - Gestion centralisée (contrôleur intégré ou Cloud) | 2 000,00 € |
| Onduleurs | 2 onduleurs professionnels (sites principaux) - Autonomie : 15 - 30 min (temps de sauvegarde et arrêt propre) - Garantie : 3 ans avec remplacement à J+1 si défaillance détectée | 5 000,00 € |
| 3 - Postes utilisateurs | | 63 000,00 € |
| Ordinateurs portables | 79 postes de travail - Certifications : Energy Star et / ou EPEAT Gold - Configuration : adaptée bureautique + applications métiers. - Garantie : 3 ans sur site | 60 000,00 € |
| Solution EDR / XDR | Protection endpoint avec console centralisée - Fonctionnalités : antivirus, anti-ransomware, détection comportementale - Conformité RGPD - 79 licences | 3 000,00 € |

| 4 - Stockage et sauvegarde | | 14 000,00 € |
|---|--|---------------------|
| Serveur de sauvegarde | Serveur dédié pour les sauvegardes - Stockage haute capacité (>12 To) | 5 000,00 € |
| NAS de sauvegarde | NAS dédié pour les sauvegardes - Stockage haute capacité (>12 To) | 3 000,00 € |
| Disques externes rotatifs | 10 disques durs externes haute capacité (4 To minimum) - Rotation journalière + stockage hors site - Débranchables à chaud | 4 000,00 € |
| 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 | 2 000,00 € |
| 5 - Licences et abonnements (1 an) | | 36 000,00 € |
| Suite bureautique cloud | Microsoft 365 Business Premium (ou équivalent) - 79 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) | 12 000,00 € |
| Abonnements pare-feu | Abonnements 1 an : signatures IPS, filtrage web, licences VPN SSL - Coût An 1 uniquement (renouvellement en OPEX An 2-5) | 4 000,00 € |
| Abonnements Fibre + 4G/5G | Abonnement annuel : FTTE + 4G/5G failover Abonnements téléphoniques 4G/5G | 20 000,00 € |
| TOTAL CAPEX AN 1 | | 200 000,00 € |

8.2.3 Répartition du budget OPEX

| Poste budgétaire | An 2 | An 3 | An 4 | An 5 | Total An 2 - 5 |
|---|--------------------|--------------------|--------------------|--------------------|---------------------|
| Licences Microsoft 365 (79 users) | 12 000,00 € | 12 000,00 € | 12 000,00 € | 12 000,00 € | 48 000,00 € |
| Abonnements pare-feu | 4 000,00 € | 4 000,00 € | 4 000,00 € | 4 000,00 € | 16 000,00 € |
| Licences EDR/XDR (annuel) | 3 000,00 € | 3 000,00 € | 3 000,00 € | 3 000,00 € | 12 000,00 € |
| Support logiciel sauvegarde | 2 000,00 € | 2 000,00 € | 2 000,00 € | 2 000,00 € | 8 000,00 € |
| Support logiciel journalisation et monitoring | 1 000,00 € | 1 000,00 € | 1 000,00 € | 1 000,00 € | 4 000,00 € |
| Formation continue (cybersécurité, nouveautés...) | 3 000,00 € | 3 000,00 € | 3 000,00 € | 3 000,00 € | 12 000,00 € |
| Maintenance matériel | 2 000,00 € | 2 000,00 € | 4 000,00 € | 6 000,00 € | 14 000,00 € |
| Total OPEX ANNUEL | 27 000,00 € | 27 000,00 € | 29 000,00 € | 31 000,00 € | 114 000,00 € |

8.3 Indicateurs clés de performances

| Catégorie | Indicateur | Formule de calcul | Seuil d'alerte | Cible | Fréquence |
|---|---|--|----------------|------------|------------|
| Taux d'avancement global | Nombre de tâches terminées / Total tâches planifiées * 100 | (Tâches OK / Total) * 100 | < 80% attendu | >95% | Hebdo |
| Respect du planning | Écart entre date réelle et date prévue (en jours) | Date réelle - Date planifiée | > +7 jours | < +3 jours | Hebdo |
| Taux de réalisation | Nombre de jalons validés / Total jalons prévus * 100 | (Jalons OK / Total) * 100 | < 90% | 100% | Mensuel |
| Disponibilité du SI | Temps de fonctionnement / Temps total * 100 | (Uptime / Total) * 100 | < 95% | > 99,9% | Mensuel |
| Taux de restauration réussie | Tests de sauvegarde réussis / Total tests * 100 | (Tests OK / Total) * 100 | < 95% | 100% | Mensuel |
| Conformité réglementaire | Critères conformes / Total critères * 100 (RGPD, NIS2, ANSSI) | (Critères OK / Total) * 100 | < 80% | 100% à M8 | Mensuel |
| Satisfaction utilisateurs | Note moyenne satisfaction (enquête post-formation) | Moyenne sur 5 | < 3/5 | > 4/5 | Fin projet |
| Temps moyen résolution incidents | Moyenne du temps de résolution tickets support | Σ (temps résolution) / Nb tickets | < 3/5 | > 4/5 | Hebdo |
| Taux de consommation budget | Budget dépensé / Budget total * 100 | (Dépenses / 200K€) * 100 | > 95% avant M7 | < 100% | Mensuel |
| Écart budgétaire | Budget réel - Budget prévisionnel | Réel - Prévisionnel | > +10 000€ | < +5 000€ | Mensuel |
| Réserve de contingence | Montant restant / Réserve initiale * 100 | (Restant / 10K€) * 100 | < 30% | > 50% à M6 | Mensuel |