Cahier des charges pour la conception de la nouvelle infrastructure informatique de l'Hôpital Public Belfort Montbéliard

2 oct. 2024

PLOUFTECH

Pays de Montbéliard AGGLOMÉRATION

1. Présentation générale

1. Présentation du Client

Le client est l'Hôpital Public Belfort-Montbéliard, qui souhaite simuler la mise en place en urgence d'un hôpital de campagne. Le projet de création de l'HPBM est porté par Pays de Montbéliard Agglomération et par les Territoires de Belfort.

2. Contexte du projet

L'Hôpital Public Belfort-Montbéliard souhaite mettre en place un système informatique afin d'utiliser des outils informatiques pour automatiser les processus, la communication, stocker et sécuriser les données médicales. Aussi, permettre ou assurer un accès plus rapide à l'information.

2. Présentation du projet

1. Objectifs

Ce projet a pour objectif de créer sur le site de l'HPBM à Montbéliard l'infrastructure informatique du nouvel Hôpital Public Belfort Montbéliard.

Cette infrastructure sera totalement nouvelle et ne s'appuiera sur aucune infrastructure informatique existante.

A cet effet, la mise en place du réseau sur le site de l'HPBM doit permettre :

- Le partage de ressources matérielles (Imprimantes, disques durs etc…)
- Le partage de ressources logicielles (fichiers, applications…)
- L'accès à un espace commun de partage
- L'accès à des services de communication de type intranet et extranet.
- L'amélioration de la gestion des patients et des dossiers médicaux, des services fournis aux patients (prescriptions, la prise de rendez-vous en ligne, le suivi post-traitement, etc.) ;
- L'optimisation de la communication interne (entre les services médicaux, infirmiers et administratifs, ainsi qu'avec les centres médicaux externes) ;
- La sécurisation des données médicales (en respectant le RGPD) ;
- Le contrôle des accès physiques aux salles

2. Périmètre de couverture

L'infrastructure informatique devra être en mesure de pouvoir évoluer vers une mise en connexion de plusieurs bâtiments. On appelle "bâtiment" dans ce projet un ensemble d'une vingtaine de tentes réunies.

A ce jour, un seul bâtiment est prévu et rentre dans le périmètre du projet avec cependant une liaison à prévoir avec la Clinique Saint Plouf située à Belfort dans le cadre de la coopération inter-hôpital des communes de Montbéliard et de Belfort.

3. Utilisation du réseau

La méthode de connexion à l'extranet pour les personnels soignants ainsi que pour les services administratifs se fera par un portail captif. Des accès invités seront mis en place pour une durée déterminée pour les patients lors de leur premier rendez-vous.

Un accès devra être mis en place pour permettre le télétravail des personnels administratifs.

4. Les acteurs du projet

Les principaux acteurs du projet sont :

- **Pays Montbéliard Agglomération (PMA)**

PMA est responsable de la coordination générale du projet sur son territoire, ainsi que de la mise à disposition des ressources nécessaires pour assurer son bon déroulement. Ils s'engagent également à superviser l'intégration du projet dans les politiques locales de développement numérique et d'innovation territoriale.

- **Hôpital Public Belfort Montbéliard (HPBM)**

L'Hôpital Public Belfort Montbéliard est le principal bénéficiaire des infrastructures informatiques qui seront mises en place dans le cadre de ce projet. Il s'engage à fournir des spécifications claires concernant les besoins spécifiques en matière de santé et de gestion des données médicales. L'hôpital sera également impliqué dans la phase de validation et de test des solutions déployées, en particulier en ce qui concerne la sécurité et la conformité aux normes médicales.

- **ESN PloufTech Solutions**

PloufTech Solutions, en tant qu'entreprise de services du numérique (ESN), est chargée de la conception, de la mise en place et de la gestion de l'infrastructure informatique nécessaire à la réalisation du projet. PloufTech s’engage à :

  - Concevoir une infrastructure informatique sécurisée, performante et évolutive, adaptée aux besoins des différents acteurs.
  - Gérer l’installation, la configuration et le support technique des solutions déployées.
  - Assurer la maintenance et la supervision des systèmes pour garantir leur disponibilité et leur bon fonctionnement sur le long terme.
  - Former les utilisateurs et l’équipe technique interne à l’utilisation des nouvelles infrastructures.
  - Respecter les délais, les coûts et les objectifs définis dans le cahier des charges.

- **Les utilisateurs finaux**

- **Personnel de l'Hôpital Public Belfort Montbéliard** : Ils sont les utilisateurs finaux des systèmes informatiques mis en place. Ils contribueront à tester l'interface et à signaler d'éventuelles améliorations pour adapter l'infrastructure aux besoins du personnel médical et administratif.

3. Environnement informatique à mettre en place

1. Cahier de charges fonctionnel

Dans le CDC fonctionnel , on indique l'ensemble des services que nous souhaitons informatiser. Cela va de pair avec les objectifs que nous avons susmentionnés mais en détaillant un peu plus. Il s'agirait de citer les différentes fonctionnalités qu'apportent ces services.

a) Gestion des dossiers patients

- Création, mise à jour et consultation des dossiers patients ;
- Historique des consultations, traitements, prescriptions et diagnostics ;
- Accès sécurisé avec authentification multi-facteur pour les professionnels de santé ;
- Respect des normes de confidentialité (chiffrement des données) ;
- Mise en place d'un formulaire PHP d'ajout d'utilisateur : Lorsqu'un nouvel employé arrive, l'équipe administrative remplit un formulaire contenant toutes les informations nécessaires à la configuration de son environnement de travail informatique, qui sera ensuite transmis au service informatique.

b) Gestion des rendez-vous

- Système de prise de rendez-vous en ligne et en clinique ;
- Notifications automatiques par SMS ou email pour rappeler des rendez-vous.

c) Prescriptions électroniques

- Prescriptions directement envoyées à la pharmacie interne par exemple ou à d'autres médecins ;
- Intégration avec des bases de données de médicaments pour vérifier les interactions médicamenteuses.

d) Communication interne

- Messagerie interne sécurisée entre les services médicaux et administratifs. Peut-être l'agrandir au niveau d'autres structures ;
- Tableau de bord des tâches et affectations pour les médecins et infirmières ;
- Lignes téléphoniques privées et directes ;
- Logiciel de chat instantané (Teams etc…).

e) Suivi post-consultation

- Plateforme de téléconsultation pour le suivi à distance (via un portail patient) ;
- Accès sécurisé aux comptes rendus et résultats d'examens via un espace en ligne pour les patients.

f) Infrastructure connectée

- Mise en place de capteurs de porte
- Mise en place d'une armoire connectée.

2. Cahier des charges technique

On met ce qui est indispensable à notre travail. On va essayer de répondre aux besoins techniques du CDC fonctionnel.

a) Infrastructure réseau

Voici l'infrastructure informatique qui devra être mise en place pour l'Hôpital Public de Belfort Montbéliard.

1. Serveur Central

- **Fonction** : C'est le cœur de l'infrastructure. Il héberge les différentes applications de gestion hospitalière, les bases de données des dossiers patients, et les autres applications critiques.
- **Matériel recommandé** : Dell PowerEdge ou HP ProLiant.
- **Système d'exploitation** : Windows Server ou Linux (Debian, CentOS).
- **Logiciels** : HIS (OpenMRS ou Odoo Healthcare pour la gestion hospitalière).

2. Serveur de Base de Données

- **Fonction** : Stocke toutes les données médicales, y compris les dossiers patients, les rendez-vous, les prescriptions, etc.
- **Système de gestion de bases de données (SGBD)** : MySQL ou PostgreSQL.
- **Sécurité** : chiffrement AES-256, accès restreint, authentification multi-facteur.

3. Serveur de Téléphonie VoIP

- **Fonction** : Gère la téléphonie interne pour permettre des communications efficaces entre les services médicaux et administratifs.
- **Logiciel** : FreePBX.
- **Matériel recommandé** : Serveur Linux compatible VoIP.

4. Serveur de Messagerie

- **Fonction** : Gestion des emails internes pour le personnel soignant et administratif.
- **Logiciel** : Postfix/Dovecot.
- **Système d'exploitation** : Linux.

5. Serveur RADIUS (Serveur d'accès et d'authentification)

- **Fonction** : Gestion de l'authentification sécurisée des utilisateurs pour l'accès au réseau Wi-Fi, VPN, et autres services.
- **Logiciel** : FreeRADIUS.
- **Système d'exploitation** : Linux (Debian recommandé).

6. Serveur de Stockage (NAS - Network Attached Storage)

- **Fonction** : Stockage centralisé de fichiers et de données avec accès pour les différents services.
- **Matériel** : Synology, QNAP ou Dell EMC.
- **Logiciel** : Serveur NAS intégré ou Nextcloud pour la gestion des fichiers.

7. Serveur de Sauvegarde

- **Fonction** : Sauvegarde régulière des données et applications critiques pour éviter toute perte en cas d'incident.
- **Logiciel** : Veeam Backup & Replication ou Bacula.
- **Matériel recommandé** : Serveur HP ProLiant ou Dell PowerEdge dédié à la sauvegarde.

8. Serveur de Virtualisation

- **Fonction** : Héberger plusieurs serveurs virtuels pour optimiser l'utilisation des ressources matérielles.
- **Logiciel** : VMware ESXi ou Proxmox VE.
- **Matériel** : Dell ou HP avec de la redondance pour la haute disponibilité.

9. Serveur VPN

- **Fonction** : Permet l'accès sécurisé à distance pour le télétravail des administratifs et la téléconsultation des médecins.
- **Logiciel** : OpenVPN ou WireGuard.
- **Système d'exploitation** : Linux (Debian, CentOS).

10. Serveur d'Application Web

- **Fonction** : Hébergement des applications web (portail patient, prise de rendez-vous en ligne, formulaire PHP pour la gestion des utilisateurs).
- **Logiciel** : Apache, Nginx.
- **Système d'exploitation** : Linux (Debian).

11. Serveur de Monitoring & IDS/IPS

- **Fonctio**n : Surveiller l'infrastructure réseau et détecter les intrusions ou comportements suspects.
- **Logiciel** : Nagios ou Zabbix pour la supervision ; Snort pour IDS/IPS.
- **Système d'exploitation** : Linux.

12. Réseau et Sécurité

- **Switches et Routeurs** : Cisco, Juniper, Ubiquiti pour la connectivité et segmentation du réseau.
- **Firewall** : pfSense ou Fortinet pour filtrer les connexions et protéger l'infrastructure.
- **VLAN** : Segmentation du réseau avec différents VLANs pour le médical, les invités, la téléconsultation, etc.
- **Plan d'adressage IP** : Classe C privée (192.168.X.Y).

13. Sécurité des Données

- Chiffrement des données : TLS (Transport Layer Security) pour les communications, AES-256 pour le stockage des données sensibles.
- Antivirus et anti-malware : À déployer sur les postes clients et serveurs

b) Le nombre des postes

- 2 postes pour les IT ;
- 12 postes de travail pour le personnel médical ;
- 3 stations mobiles pour les infirmiers et consultations à distance ;
- 2 stations pour la réception à l'accueil (prise de rdv et gestion administrative) ;
- 1 poste libre service ;
- Le nombre d'objets connectés qui feront office de terminaux.

c) Le type de réseau à déployer

- *Réseau filaire et sans fil*

Un réseau Wi-Fi pour le personnel médical sera déployé, un autre réseau Wi-Fi pour les objets connectés sera également déployé. Un réseau filaire pour les postes critiques (serveur, réception) sera mis en place et une séparation des flux réseau de chaque service sera crée grâce à des VLANs et autres technologies (VWLANs, Tunnels TLS, MPLS, et même PPPOE).

- *Le plan d'adressage IP*

Le plan d'adressage IP devra être défini par la société PloufNTech Solution ainsi que les VLANs. Voici les VLANs qui devront être mis en place :

- VLAN 10 - Administration & Infrastructure Critique : AD, Central, Monitoring, Sauvegarde, NAS, RADIUS
- VLAN 20 - Services Médicaux : BDD, Applications, Téléconsultation, Broker MQTT (dispositifs médicaux)
- VLAN 30 - Téléphonie & Communication : ToIP, Mail
- VLAN 40 - Réseau Personnel Médical : RADIUS (Wi-Fi personnel médical)
- VLAN 50 - Objets Connectés (IoT) : Broker MQTT (IoT), Serveur d'accès IoT
- VLAN 60 - Patients & Invités : Aucun serveur, accès Internet uniquement
- VLAN 70 - Accès Distants (VPN) : VPN

Chaque sous-réseau aura une passerelle vers le routeur principal pour permettre l'accès à Internet pour les services externes, mais avec des restrictions de sécurité (Filtrage par Firewall).

d) La sauvegarde des données

- Solutions Cloud ;
- Sauvegarde grâce à des sites physiques distants ;
- Serveur de sauvegarde : Veeam ou Bacula
- Virtualisation des serveurs

e) Sécurité réseau et données

- Firewall : configurer pour bloquer les connexions non autorisées ;
- Mise en place d'un IDS/IPS (Snort) : surveille les tentatives d'intrusion ;
- VPN : sécurise les accès distants et permet la téléconsultation pour les médecins et patients ;
- Antivirus/Anti Malwares : à déployer sur tous les postes pour prévenir les cyberattaques ;
- Onduleurs pour dépanner d'une coupure électrique.

f) Système de gestion hospitalière

Un système de gestion hospitalière HIS (OpenMRS) sera mis en place. Ce système permettra de gérer la clinique, les dossiers médicaux, la gestion des prescription ainsi que d'autres fonctionnalités qui pourront être installées si le besoin s'avère nécessaire.

4. Infrastructure IoT Sécurisée pour le Contrôle d'Accès et l'Identification

1. Composants IoT Intégrés

- Caméras de Sécurité :
  - Caméras IP haute définition avec vision nocturne.
  - Connexion au réseau via PoE (Power over Ethernet) pour réduire les câbles et améliorer la sécurité.
  - Accès à distance sécurisé pour le personnel autorisé via un portail sécurisé avec authentification multi-facteurs.
- Capteurs de Présence et de Luminosité :
  - Utiliser des capteurs PIR (infra-rouge passif) pour détecter les mouvements et surveiller les accès non autorisés.
  - Capteurs de luminosité pour ajuster l'éclairage dans les zones sensibles, améliorer l'efficacité énergétique, et activer des mesures de sécurité lorsque l'éclairage est insuffisant.
- Lumières Connectées :
  - Lumières LED intelligentes contrôlées via le réseau pour ajuster automatiquement l'éclairage en fonction de la présence ou de la luminosité ambiante.
  - Intégration avec des scénarios d'alerte en cas de détection de mouvements non autorisés la nuit.
- Armoires Connectées :
  - Armoires sécurisées avec serrures électroniques contrôlées par un système d'ouverture par badge RFID/NFC.
  - Détection d'état (ouvert/fermé) des armoires, avec enregistrement des événements d'ouverture pour savoir quand et par qui l'armoire a été ouverte.
- Lecteur et Graveur de Badges :
  - Installation de lecteurs RFID sur les armoires pour autoriser l'accès via badge.
  - Un graveur de badges permettant de programmer et attribuer des badges aux membres du personnel selon les rôles (accès restreint pour les médicaments, accès complet pour le matériel informatique).
  - Gestion des droits d'accès via une application centrale, permettant d'ajuster ou de révoquer les autorisations à distance.

2. Surveillance et Protection des Matériels

- Ordinateurs Portables et Téléphones de Service :
- Utilisation de capteurs d'ouverture sur les postes de travail et les espaces de stockage d'équipement sensible.
- Badges d'accès nécessaires pour débloquer les ordinateurs portables et les téléphones de service.
- Connexion à un système central de gestion des droits d'accès pour permettre l'activation/désactivation à distance.

3. Sécurité des Données et du Réseau

- Chiffrement des communications entre les capteurs, les caméras, et le serveur central via àTLS pour empêcher l'interception des données.
- Séparation des flux IoT sur un VLAN dédié pour les objets connectés (ex : VLAN 6 pour les objets connectés dans votre architecture réseau).
- Firewall et contrôle d'accès pour surveiller et restreindre les connexions entrantes et sortantes des dispositifs IoT.

4. Supervision et Maintenance

- Tableau de bord centralisé pour surveiller l'état des caméras, des capteurs et des armoires en temps réel.
- Notifications automatiques par email/SMS en cas de tentative d'accès non autorisé ou de problème technique (comme une armoire laissée ouverte).
- Sauvegarde des données de sécurité (images, événements de badge) dans un serveur sécurisé avec redondance pour garantir que les logs sont conservés.

5. Conformité et Respect des Normes

- Respect des normes GDPR pour la gestion des accès et la protection des données personnelles, notamment celles des badges et des logs d'accès.

- Audit des accès avec un historique détaillé des événements liés à l'utilisation des badges (ex. qui a accédé aux médicaments ou aux ordinateurs portables).

- Cette infrastructure vous permettra de sécuriser l'accès aux zones sensibles de l'hôpital et de garantir un suivi précis des accès, tout en intégrant une gestion avancée des objets connectés.

5. Gestion du projet et planification

Afin d'assurer la livraison du produit dans les temps, une méthode dite Agile avec un outil de gestion de projet comme Trello sera mise en place. Différentes phases seront définies : Phase de conception, Phase de développement, Phase de test, Phase de formation et déploiement, Phase de maintenance et de suivi.

1. Phase de conception

- Durée approximative de 1,5 jours
- Analyse des besoins spécifiques de l'hôpital;
- Validation du cahier des charges détaillé.

2. Phase de développement

- Durée approximative de 6 jours
- Installation de l'infrastructure réseau (câblage, serveurs, équipements) ;
- Déploiement du logiciel de gestion hospitalière ;
- Configuration des postes clients et du système de sécurité.

3. Phase de test

- Durée approximative de 2 jours
- Tests fonctionnels pour chaque service installé (prise de rendez-vous, prescriptions, etc)
- Test de sécurité (test d'intrusion, vérification des sauvegardes).

4. Phase de formation et déploiement

- Formation du personnel médical et administratif ;
- Mise en service progressive de l’infrastructure (c-à-d faire des tests en condition réelle).

5. Phase de maintenance et suivi

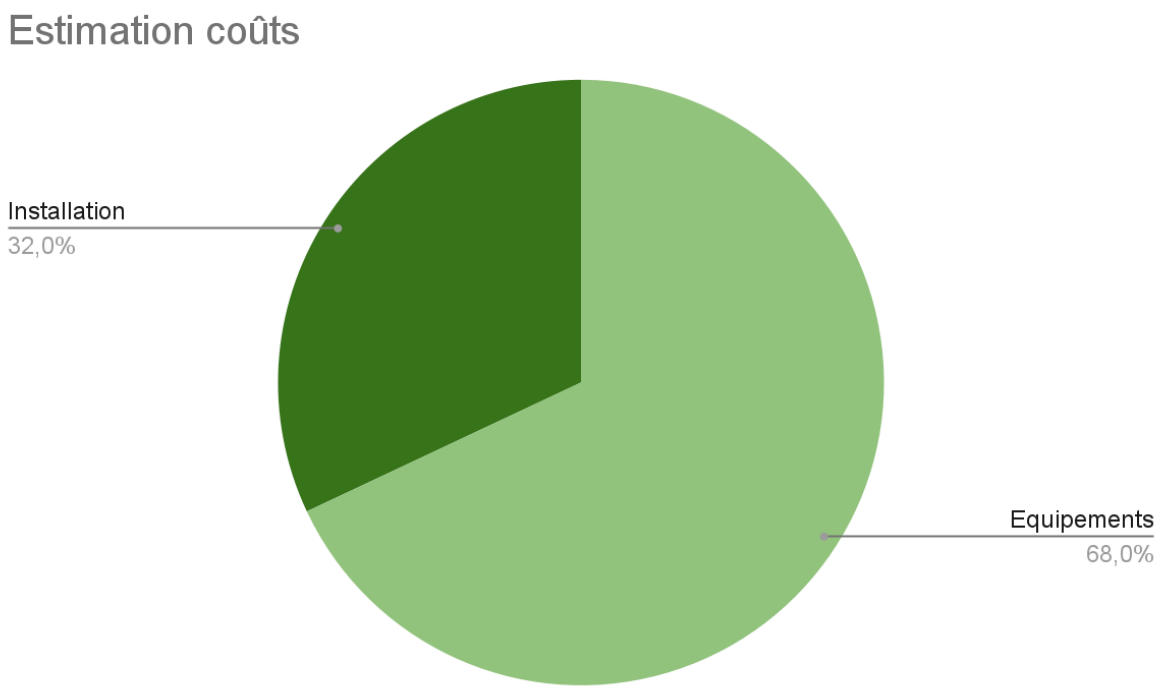
- Support technique sur site et à distance ;
- Maintenance préventive des systèmes, gestion des mises à jour de sécurité ;
- Documentation.

6. Estimation financière

Dans cette section, nous examinerons votre projet sous un angle financier. Nous passerons en revue différents aspects de l'analyse budgétaire du projet, notamment :

- Le budget des équipements qui seront mis en place
- Le budget d'intervention pour la mise en place des équipements

Ci-dessous vous pourrez observer un graphique qui mettra en évidence le budget associé aux équipements et à l'intervention des nouveaux équipements.



Cette répartition est effective pour un coûts théorique de 160 000 €

Nous vous présentons un contrat de service comprenant trois niveaux de durée : 1 an, 3 ans ou 5 ans. Vous trouverez ci-dessous la grille tarifaire correspondante :

	Année 1	Année 2	Année 3	Année 4	Année 5	Total
Contrat de service 5 ans	9600	9600	9600	9600	9600	48000
Contrat de service 3 ans	12800	12800	12800			38400
Contrat de service 1 an	16000					16000

Détails des services proposés dans le contrat :

- Supervision de l'infrastructure réseaux : Surveiller le réseau en temps réel pour détecter les problèmes et maintenir les services disponibles
- Réalisation de Backup : Sauvegarder régulièrement les données critiques pour une récupération rapide en cas de besoin.
- Support technique : Apporter une aide rapide en cas de problème pour minimiser les interruptions et assurer un bon fonctionnement. Un système de ticket serait à votre disposition en cas de problème avec un système de priorité.
- Un audit préventif trimestrielle
- Garantie de temps d'Intervention en 2H

Conclusion

Ce cahier des charges définit l'ensemble des besoins, des objectifs et des exigences nécessaires à la réalisation de l'infrastructure informatique de l'hôpital de campagne Hôpital Public Belfort Montbéliard. À travers ce document, nous avons précisé les attentes fonctionnelles, techniques, ainsi que les contraintes liées au budget, aux délais et aux ressources.

Le respect des spécifications détaillées dans ce cahier des charges est primordial pour assurer la réussite du projet et garantir que les livrables répondent aux attentes des parties prenantes. L'ensemble des acteurs impliqués devra suivre ce cadre pour permettre une gestion efficace et coordonnée du projet, tout en anticipant les risques et en assurant une flexibilité suffisante pour s'adapter aux imprévus.

En conclusion, ce document servira de référence tout au long du projet, tant pour les phases de développement que pour la mise en œuvre finale, dans l'objectif de fournir une solution conforme aux besoins identifiés. Nous restons disponibles pour toute clarification et adaptation nécessaire en fonction des évolutions potentielles du projet.