Cahier des charges du projet global

1. Contexte et objectifs du projet

1.1. Contexte du projet

Ce projet s'inscrit dans le cadre de la digitalisation et de la sécurisation des systèmes d'information d'un hôpital. Il a pour but de fournir une plateforme intégrée, regroupant la gestion des utilisateurs, des contenus, ainsi que la sécurisation des communications internes et externes via un réseau VPN sécurisé. Ce projet aborde les enjeux de protection des données médicales et administratives, les problématiques d'échanges de données sensibles avec d'autres hôpitaux, et l'intégration d'objets connectés pour améliorer la gestion des patients et des dispositifs médicaux.

1.2. Objectifs du projet

Les objectifs du projet sont multiples :
- Sécuriser le système informatique : Protéger les données sensibles contre les cyberattaques grâce à une infrastructure réseau robuste, un VPN sécurisé et des systèmes de chiffrement avancés.
- Optimiser la gestion des utilisateurs : Mettre en place une gestion fine des rôles et permissions pour chaque type d'utilisateur (direction, administration, personnel médical).
- Améliorer la continuité des services : Assurer une haute disponibilité des services grâce à la mise en place de procédures de sauvegarde régulières et de systèmes de redondance.
- Intégration d'objets connectés : Mettre en place des dispositifs de surveillance et de suivi médical grâce à des capteurs connectés pour améliorer le suivi des patients et l'efficacité des équipements médicaux.
- Assurer la conformité légale : Respecter les normes de protection des données telles que le RGPD et les bonnes pratiques de la HDS (Hébergeurs de Données de Santé) pour garantir la confidentialité et la sécurité des données médicales.

2. Architecture globale du projet

2.1. Composants matériels (HW)

2.1.1. Serveurs physiques et virtualisés

- Serveurs dédiés : Utilisation de serveurs physiques dans un datacenter sécurisé ou en mode Cloud, garantissant des ressources dédiées pour les bases de données, le VPN et l'application.
- Redondance et répartition de charge : Mise en place d'un système de répartition de charge (Load Balancer) pour garantir une continuité de service même en cas de panne d'un serveur.
- Stockage sécurisé : Systèmes de stockage en réseau (NAS/SAN) pour garantir une gestion sécurisée des données avec chiffrement intégré.

2.1.2. Réseau et équipements de connectivité

- Switches Cisco Catalyst et Routeur Cisco 1841/1900 : Ces équipements assurent une gestion performante du trafic réseau et permettent une configuration flexible des VLANs pour cloisonner les différents départements (direction, administration, médical).
- Bornes Wi-Fi : Borne WiFi Linksys WRT54G compatible avec les normes de sécurité avancées, notamment l'authentification via 802.1X, assurant un accès sécurisé au réseau sans fil pour le personnel.

2.1.3. Équipements utilisateurs finaux

- PC, Mac, et terminaux mobiles : Dispositifs utilisés par les administrateurs, personnels médicaux et direction. Compatibilité avec les technologies de sécurité réseau comme 802.1X pour le contrôle d'accès.

2.2. Composants logiciels (SW)

2.2.1. Systèmes d'exploitation

- Serveurs : Systèmes d'exploitation basés sur Linux (CentOS, Ubuntu Server), reconnus pour leur robustesse, sécurité et leur compatibilité avec des environnements réseau complexes.
- Clients : Windows, Mac OS, iOS et Android pour les utilisateurs finaux, offrant une flexibilité maximale dans l'accès à la plateforme.

2.2.2. Backend et middleware

- Frameworks web (Django, Laravel, Node.js) : Utilisés pour gérer les API qui serviront de passerelles entre le frontend et la base de données.
- API RESTful : Utilisation d'APIs sécurisées via TLS pour la communication entre les composants de l'architecture, garantissant une sécurité maximale lors de l'échange de données.

2.2.3. Base de données

- PostgreSQL ou MySQL : Bases de données relationnelles performantes, supportant le chiffrement des données au repos et en transit, et permettant une gestion fine des permissions pour garantir l'accès restreint aux informations sensibles.

2.2.4. Gestion des contenus

- CMS intégré : Un système de gestion de contenu permettant la modération, l'édition et la suppression des contenus de manière centralisée, pour les utilisateurs ayant les droits appropriés.

2.3. Architecture réseau

2.3.1. Segmentation du réseau

L'architecture réseau doit permettre la séparation stricte des différents départements :
1. Réseau direction : Accès aux données de la direction, incluant les informations administratives sensibles.
2. Réseau administration : Cloisonné pour les besoins administratifs uniquement.
3. Réseau médical : Réseau dédié à la gestion des données de santé des patients et à l'échange de données avec d'autres établissements médicaux.

2.3.2. Accès et authentification

- Standard 802.1X : Authentification réseau centralisée par Radius pour contrôler l'accès aux segments du réseau.
- VPN sécurisé : Configuration d'un VPN sécurisé pour permettre la consultation et l'échange de données médicales avec d'autres hôpitaux ou entités externes. Utilisation de protocoles IPsec ou OpenVPN pour garantir la sécurité des communications.

2.3.3. Sécurisation des communications

- TLS/SSL : Chiffrement des communications entre les différents composants du système pour protéger les données en transit.
- Firewall de nouvelle génération : Pour filtrer le trafic entrant et sortant, surveiller les connexions non autorisées, et bloquer les tentatives d'intrusion.

3. Phases de développement et organisation du projet

3.1. Méthodologie de développement

Le développement sera réalisé selon une approche Agile/Scrum avec des sprints de 2 semaines, permettant une livraison progressive et une révision régulière des priorités. Les principales étapes sont :

1. Planification : Définition des objectifs détaillés, des ressources nécessaires, et des risques.
2. Conception : Conception des schémas d'architecture réseau, des diagrammes d'interaction entre les systèmes, et des maquettes (wireframes) des interfaces utilisateur.
3. Développement :
    - Backend : Création des API, gestion des bases de données, implémentation des mécanismes de sécurité (chiffrement, authentification).
    - Frontend : Développement des interfaces utilisateur.
4. Tests :
    - Tests unitaires, de performance et de charge.
    - Tests de sécurité (pentests, audits de vulnérabilité).
5. Déploiement : Configuration des serveurs, mise en place du VPN, et déploiement des applications.
6. Maintenance : Suivi post-lancement avec monitoring et correction des bugs.

3.2. Organisation de l’équipe

L’équipe de développement comprendra :
- Chef de projet : Gestion des ressources, du calendrier et de la communication client.
- Développeurs Backend : Responsables des bases de données, de la sécurité et des API.
- Développeurs Frontend : En charge des interfaces utilisateur (USR et Admin).
- Testeurs QA : Vérification de la qualité via des tests rigoureux.
- Administrateurs système : Gérer les serveurs et le déploiement du réseau VPN.

4. Sécurité informatique et cybersécurité

La sécurité informatique est primordiale dans un environnement hospitalier où les données sensibles (données des patients, résultats médicaux, informations administratives) doivent être protégées des cyberattaques. Le projet inclut la mise en place de mesures avancées pour garantir la sécurité des systèmes, des réseaux et des données critiques.

4.1. Pare-feu (Firewall)

4.1.1. Mise en place d’un firewall de protection réseau

Un firewall (pare-feu) est essentiel pour filtrer et contrôler le trafic réseau entrant et sortant de l’hôpital. Il protège contre les menaces externes en bloquant les connexions non autorisées.

- Pare-feu matériel : Utilisation d’un pare-feu matériel dédié (comme Cisco ASA, Palo Alto, ou Fortinet) pour la sécurisation du réseau principal de l’hôpital. Ce firewall sera configuré pour filtrer les requêtes en fonction des protocoles, adresses IP, et types de connexion.

- Pare-feu logiciel : Mise en place d'un firewall logiciel sur les serveurs (ex : iptables sur les systèmes Linux) pour un niveau de protection supplémentaire, particulièrement pour les bases de données et les serveurs critiques.

4.1.2. Stratégies de sécurité via le firewall

- Filtrage des adresses IP : Limitation des connexions autorisées aux adresses IP internes et à certains partenaires de confiance.
- Gestion des ports ouverts : Seuls les ports nécessaires au bon fonctionnement des services seront ouverts (par exemple, ports pour le VPN, les bases de données, les interfaces de gestion).
- Inspection des paquets (DPI) : Inspection en profondeur des paquets réseau pour détecter les tentatives d'intrusion, les malwares, et les comportements anormaux.

4.2. Sécurisation de la base de données

4.2.1. Architecture de la base de données

Les bases de données hospitalières doivent être rigoureusement sécurisées car elles contiennent des informations sensibles, notamment les dossiers médicaux des patients et les données administratives.

- Base de données relationnelle : Utilisation de bases de données robustes et sécurisées comme PostgreSQL ou MySQL, qui offrent des fonctions natives de chiffrement, de journalisation des accès et de gestion des permissions.

- Chiffrement des données : Les données en transit et au repos doivent être chiffrées. Utilisation de l'AES-256 pour le chiffrement des données sensibles stockées dans la base de données et l'SSL/TLS pour sécuriser les échanges entre les applications et la base de données.

4.2.2. Contrôle d'accès à la base de données

- Authentification forte (MFA) : Mise en place d'une authentification à plusieurs facteurs pour l'accès des administrateurs à la base de données.
- Permissions minimales : Attribution de droits d'accès basés sur le principe du moindre privilège, permettant uniquement aux utilisateurs et applications d'accéder aux informations strictement nécessaires.
- Surveillance et audit : Journaux d'accès détaillés pour chaque connexion à la base de données avec des alertes automatiques en cas de comportement suspect (tentatives répétées de connexion, accès non autorisé).

4.2.3. Protection contre les injections SQL

- Requêtes paramétrées : Utilisation de requêtes SQL paramétrées et ORM (Object-Relational Mapping) pour prévenir les injections SQL.
- Validation des entrées utilisateur : Mise en place de processus de validation pour tous les champs de saisie afin de bloquer les tentatives d'injection de code malveillant.

4.3. Application ou site de gestion de la base de données

4.3.1. Développement d'une interface de gestion sécurisée

Création d'une application web ou d'un site sécurisé, accessible uniquement au personnel autorisé, pour la gestion des bases de données et des dossiers médicaux.

- Framework sécurisé : Développement de l'application via un framework sécurisé comme Django ou Laravel. Ces frameworks offrent des mécanismes intégrés pour la gestion des accès et la prévention des failles de sécurité.

- Chiffrement SSL/TLS : Tous les échanges entre l'interface de gestion et la base de données doivent être protégés par SSL/TLS pour empêcher les interceptions de données.

4.3.2. Fonctionnalités de l'application de gestion

- Gestion des utilisateurs et des permissions : L'interface doit permettre de créer, modifier et supprimer des utilisateurs, ainsi que de gérer leurs permissions d'accès.
- Consultation des journaux d'accès : Fonctionnalité pour consulter les logs d'accès à la base de données et les modifications apportées aux dossiers.
- Backups et restauration : Outils pour réaliser des backups automatiques ou manuels des données, ainsi qu'un système de restauration en cas d'incident.

4.4. VPN (Réseau privé virtuel)

4.4.1. Installation d'un VPN sécurisé

Un VPN (Virtual Private Network) sera déployé pour permettre une connexion sécurisée entre les différents sites de l'hôpital ou entre hôpitaux partenaires. Ce réseau privé virtuel garantira que les données médicales échangées entre les établissements sont protégées des interceptions.

- Technologies VPN : Utilisation de technologies robustes comme IPSec ou OpenVPN pour sécuriser les connexions entre les sites.
- Chiffrement des communications VPN : Le trafic passant par le VPN doit être chiffré via AES-256, garantissant la confidentialité des données échangées.

4.4.2. Utilisation des VPNs inter-hôpitaux

- Échange sécurisé des données médicales : Les données médicales échangées entre les hôpitaux partenaires via le VPN seront cryptées de bout en bout pour protéger les dossiers des patients.
- Accès aux bases de données via VPN : Les utilisateurs des autres hôpitaux pourront accéder aux bases de données partagées de manière sécurisée à travers le VPN.

4.5. Plan de Reprise d'Activité (PRA)

4.5.1. Élaboration d'un PRA pour cyberattaques

Un Plan de Reprise d'Activité (PRA) est essentiel pour assurer la continuité des opérations en cas d'attaque informatique, de perte de données, ou de défaillance des systèmes.

- Scénarios de reprise : Prévoir plusieurs scénarios de reprise pour différentes menaces : ransomware, attaque DDoS, panne de serveur critique, etc.
- Temps de reprise : Fixer des objectifs clairs pour le Recovery Time Objective (RTO) et le Recovery Point Objective (RPO), c'est-à-dire le temps maximal d'arrêt acceptable et la perte maximale de données.

4.5.2. Sauvegardes régulières et externalisées

- Sauvegardes automatiques : Mise en place de sauvegardes automatiques quotidiennes des bases de données et systèmes critiques sur des serveurs sécurisés.

- Stockage en cloud sécurisé : Utilisation de solutions cloud pour conserver des copies des données critiques hors site, réduisant ainsi les risques liés aux sinistres physiques.

4.5.3. Test et maintenance du PRA

- Tests réguliers : Réalisation de tests de récupération annuels ou semestriels pour s'assurer que le PRA est fonctionnel et à jour.
- Révisions périodiques : Le plan doit être revu et mis à jour régulièrement en fonction des nouvelles menaces et des évolutions technologiques.

4.6. Protection contre les cyberattaques

4.6.1. Outils de détection et de prévention d'intrusion (IDS/IPS)

Pour détecter et bloquer les tentatives d'intrusion ou d'attaque, il est nécessaire d'installer des systèmes de détection (IDS) et de prévention d'intrusion (IPS) dans le réseau de l'hôpital.

- Surveillance en temps réel : Utilisation de solutions comme Snort, Suricata ou OSSEC pour surveiller en temps réel les menaces et générer des alertes.
- Réaction automatisée : Configuration de l'IPS pour bloquer automatiquement les adresses IP ou les utilisateurs suspectés d'activités malveillantes.

4.6.2. Gestion des correctifs et des vulnérabilités

- Mises à jour régulières : Les systèmes et applications doivent être mis à jour régulièrement pour appliquer les derniers correctifs de sécurité et patcher les vulnérabilités connues.
- Scan de vulnérabilités : Mise en place d'outils de scan comme Nessus ou OpenVAS pour détecter les vulnérabilités avant qu'elles ne soient exploitées par des attaquants.

5. Intégration de l'IOT (Internet des Objets)

L'Internet des Objets (IOT) est une composante clé dans la gestion moderne des infrastructures hospitalières. En intégrant des dispositifs connectés, il devient possible d'optimiser la sécurité, la maintenance et le suivi en temps réel des équipements, tout en améliorant la gestion des accès et des alertes en cas d'incident.

5.1. Capteurs médicaux connectés

Les capteurs médicaux connectés sont utilisés pour :
- Surveiller en temps réel les signes vitaux des patients (pression artérielle, température, fréquence cardiaque) et transmettre ces données aux équipes médicales via une plateforme centralisée.

- Suivi des patients à distance : Les dispositifs portables, comme des bracelets connectés, permettent de suivre les patients en temps réel, d'alerter en cas de chute, de surveiller les patients en mobilité ou en rééducation.

5.2. Gestion des badges et des serrures connectées

La sécurité des accès dans l'hôpital est renforcée grâce à l'utilisation de badges RFID/NFC, qui sont couplés à des serrures connectées pour contrôler l'accès à certaines zones sensibles de l'hôpital (salles d'opération, services de réanimation, zones de stockage de médicaments).

5.2.1. Système de badges RFID/NFC

- Gravage des badges personnalisés : Chaque badge est gravé et lié au profil d'un employé spécifique (médecin, infirmier, personnel administratif) dans le système de gestion des accès.
- Programmation des accès : Chaque badge peut être programmé pour n'accorder l'accès qu'à certaines zones définies (par exemple, accès uniquement aux zones médicales pour le personnel soignant, zones administratives pour la direction).
- Gestion des permissions en temps réel : Les autorisations d'accès peuvent être modifiées à distance via une interface centralisée en fonction des besoins et des rôles du personnel. Un historique des accès est conservé pour garantir un audit de sécurité détaillé.

5.2.2. Serrures connectées

- Serrures contrôlées à distance : Les serrures peuvent être ouvertes ou verrouillées via une application ou un tableau de bord centralisé, permettant de sécuriser des zones spécifiques en cas d'incident.
- Alarme anti-intrusion : Si une tentative d'ouverture non autorisée est détectée, une alerte est immédiatement envoyée aux équipes de sécurité et l'accès est bloqué.
- Intégration avec le système de gestion des alarmes incendie : Les serrures connectées peuvent se désactiver automatiquement en cas d'alerte incendie, pour permettre une évacuation rapide des zones.

5.3. Gestion des alarmes incendie et de la sécurité

La sécurité incendie est un aspect critique de la gestion d'un hôpital, et les systèmes d'alarmes connectés permettent une réponse plus rapide et plus coordonnée en cas d'incident.

5.3.1. Système d'alarme incendie connecté

- Capteurs de fumée et de chaleur : Ces capteurs sont installés dans toutes les zones à risque de l'hôpital (blocs opératoires, zones de stockage des produits inflammables). Lorsqu'une anomalie est détectée, une alerte est immédiatement envoyée aux équipes d'intervention et à l'interface centralisée.

- Déclenchement automatique des alarmes : En cas d'incendie détecté, les alarmes incendie sont déclenchées automatiquement et peuvent être visualisées à distance depuis une application de gestion de crise.
- Système d'évacuation intelligente : Les capteurs IOT peuvent indiquer les sorties d'évacuation les plus proches et débloquer automatiquement les portes sécurisées pour faciliter l'évacuation.

5.3.2. Gestion des systèmes de sécurité et des caméras à distance

- Surveillance vidéo : Installation de caméras IP connectées dans les zones critiques (accès principal, zones sensibles) pour permettre une surveillance 24/7 avec visionnage à distance par le personnel de sécurité via une interface web ou une application mobile.
- Connexion à distance des caméras : Les caméras peuvent être consultées en temps réel depuis une application dédiée, ce qui permet aux équipes de sécurité de surveiller l'hôpital à distance, même en dehors du site. En cas d'intrusion détectée ou d'alarme incendie, une notification est immédiatement envoyée aux responsables.
- Stockage sécurisé des vidéos : Les flux vidéo peuvent être enregistrés et stockés dans des serveurs sécurisés avec une option de sauvegarde en cloud, garantissant une conservation des preuves en cas d'incidents.

5.3.3. Intégration des caméras avec le système d'alerte

- Alerte automatique en cas d'anomalie : Si un mouvement suspect ou une intrusion est détecté par les caméras de sécurité, une alerte est envoyée aux équipes de sécurité ainsi qu'aux responsables via une application de gestion des incidents. Les zones surveillées peuvent être visionnées en temps réel.
- Capteurs de mouvement connectés : Ces capteurs sont intégrés au système de caméras pour déclencher des enregistrements automatiques en cas de détection de mouvement non autorisé.

5.4. Autres équipements et fonctionnalités IOT à intégrer

5.4.1. Système de gestion des lumières intelligentes

- Capteurs de présence : Utilisation de capteurs de mouvement pour gérer l'éclairage automatique dans les couloirs, salles d'attente et autres zones de l'hôpital. Ce système contribue à la réduction des coûts énergétiques tout en garantissant un environnement sûr et bien éclairé.
- Gestion à distance : Les lumières peuvent être allumées, éteintes ou modifiées (intensité, couleur) depuis une interface centralisée, permettant une gestion efficace de l'énergie.

5.4.2. Surveillance de l'environnement

- Capteurs de qualité de l'air : Installation de capteurs pour surveiller la qualité de l'air dans les salles d'opération, chambres des patients et zones critiques, garantissant ainsi un environnement sain.

- Système de régulation de la température : Gestion intelligente des systèmes de chauffage et climatisation (HVAC) pour optimiser la température et l'humidité dans les différentes zones de l'hôpital.

5.4.3. Gestion intelligente des stocks

- Capteurs pour la gestion des stocks médicaux : Des capteurs de niveau peuvent être installés pour suivre en temps réel les niveaux de stock des produits essentiels (médicaments, équipements de protection, etc.), alertant le personnel logistique lorsqu'il faut réapprovisionner.

5.4.4. Suivi des équipements hospitaliers

- Tagging RFID pour les équipements : Chaque équipement médical (lits, fauteuils roulants, dispositifs médicaux portables) est étiqueté avec un tag RFID, permettant au personnel de suivre en temps réel leur localisation dans l'hôpital et d'assurer une gestion optimisée des ressources.

5.5. Sécurité des dispositifs IOT

La sécurité des dispositifs IOT est une priorité, car ces dispositifs représentent des points d'entrée potentiels pour des attaques malveillantes.

5.5.1. Chiffrement des communications IOT

- Protocoles sécurisés (TLS, MQTT, CoAP) : Tous les dispositifs IOT doivent utiliser des protocoles de communication sécurisés pour protéger les données échangées entre les capteurs et les serveurs centraux.
- Chiffrement des données transmises : Les données collectées par les dispositifs (signes vitaux, accès aux zones, vidéos de surveillance) sont chiffrées avant leur transmission pour éviter les écoutes ou manipulations malveillantes.

5.5.2. Authentification renforcée

- Authentification à plusieurs facteurs (MFA) : Les dispositifs critiques, comme les caméras de sécurité ou les systèmes de contrôle d'accès, nécessitent une authentification à plusieurs facteurs pour éviter toute utilisation non autorisée.
- Gestion des certificats : Tous les dispositifs connectés doivent être associés à des certificats numériques pour garantir leur authenticité et empêcher toute tentative de prise de contrôle par un tiers non autorisé.

5.3 Matériel et logiciels supplémentaires à intégrer

Pour une gestion complète de l'infrastructure IOT et de la sécurité de l'hôpital, il est nécessaire d'intégrer les équipements et solutions suivants :

1. Serveurs IOT dédiés : Ces serveurs doivent gérer la collecte, le traitement et le stockage sécurisé des données issues des capteurs et autres dispositifs connectés.
2. Systèmes de monitoring : Solutions logicielles pour surveiller en temps réel l'état des équipements IOT et des capteurs de sécurité (comme Nagios ou Zabbix).
3. Firewalls et IDS/IPS : Des systèmes de détection et de prévention d'intrusion spécifiques aux réseaux IOT doivent être mis en place pour protéger les communications entre les dispositifs connectés et les

7. Pilotage de Projet (PILPRO)

La gestion d'un projet hospitalier de cette envergure nécessite un pilotage rigoureux afin de respecter les contraintes de coût, de qualité et de délai. La réussite du projet dépend de la coordination des équipes techniques et administratives, ainsi que de la satisfaction des parties prenantes (administration hospitalière, équipes médicales, etc.).

7.1. Chiffrement du projet

7.1.1. Chiffrement des coûts du projet

- Estimation précise des coûts : L'établissement d'un budget prévisionnel doit être fait avec soin pour couvrir toutes les phases du projet, du développement à la mise en œuvre et à la maintenance. Cela inclut les coûts des équipements, des logiciels, des ressources humaines, et des services externes.

- Détails des coûts :
- Coût des équipements : Estimation du coût des matériels (serveurs, capteurs IOT, dispositifs de sécurité).
- Coût des logiciels : Licensing des systèmes, logiciels de gestion des accès, de surveillance et de cybersécurité.
- Coût des services : Tarification des services de développement, d'installation, et de maintenance (contrat de support, services cloud).
- Coût des ressources humaines : Salaires des équipes de développement, des consultants en cybersécurité, du personnel de maintenance.

7.1.2. Suivi des coûts et gestion des écarts

- Outils de gestion des coûts : Utilisation de logiciels comme Microsoft Project ou Primavera pour suivre les dépenses par rapport au budget alloué.
- Gestion des écarts budgétaires : Mise en place d'un processus de gestion des écarts en cas de dépassement budgétaire, avec un suivi mensuel des dépenses et des rapports de performance.

7.1.3. Optimisation des coûts

- Stratégies de réduction des coûts : Négociations avec les fournisseurs, choix de solutions open-source (si applicables), réduction des coûts liés à la gestion énergétique des dispositifs IOT via des systèmes intelligents.

7.2. Contrat de démarrage et clôturation

7.2.1. Contrat de démarrage

Le contrat de démarrage formalise l'engagement entre le client (l'hôpital) et le fournisseur (prestataire). Ce contrat doit spécifier les termes de début du projet, les attentes, les délais et les étapes clés.

- Définitions des objectifs : Le contrat doit détailler les objectifs clairs et mesurables (déploiement de l'infrastructure IOT, mise en place de la cybersécurité, gestion des accès).
- Calendrier prévisionnel : Un calendrier avec des jalons (milestones) pour les principales phases du projet (installation des systèmes, tests, validation des utilisateurs).
- Responsabilités des parties : Attribution claire des responsabilités (développement, intégration, gestion des risques, validation des livrables).

7.2.2. Contrat de clôturation

Le contrat de clôture est signé à la fin du projet pour attester de sa réalisation conformément aux attentes et aux spécifications.

- Critères d'acceptation : Les critères de validation doivent être clairement définis (tests de performance des systèmes, vérification des fonctionnalités de cybersécurité, intégration des équipements).
- Rapport final : Remise d'un rapport final comprenant les résultats des tests, la documentation technique et les recommandations pour les futures améliorations.
- Signature des parties : Validation formelle par toutes les parties prenantes pour attester de la livraison conforme et en bon état du projet.

7.3. Contrat de maintenance

7.3.1. Maintenance préventive et corrective

Le contrat de maintenance définit les responsabilités du prestataire pour la maintenance des systèmes installés, garantissant ainsi la continuité de service après le déploiement.

- Maintenance préventive : Planification de la maintenance régulière pour éviter les pannes et garantir la disponibilité continue des équipements critiques (caméras, serrures connectées, serveurs).
- Maintenance corrective : Intervention rapide en cas de panne ou d'incident. Le contrat doit spécifier un temps de réponse garanti (SLA) pour toute demande de réparation ou d'assistance technique.

7.3.2. Mise à jour et sécurité

- Mises à jour des logiciels : Engagement à fournir des mises à jour de sécurité régulières pour les systèmes d'exploitation, les logiciels de gestion des accès, et les solutions de cybersécurité.
- Monitoring et support : Surveillance proactive des systèmes IOT et de sécurité avec un support 24/7 en cas d'alerte ou de menace détectée.

7.3.3. Durée et conditions du contrat

Le contrat de maintenance doit préciser la durée du service, avec une possibilité de renouvellement annuel ou biannuel, et inclure des clauses pour l'éventuelle résiliation anticipée en cas de non-respect des engagements.

7.4. Consultation des prospects et parties prenantes hospitalières

7.4.1. Consultation des utilisateurs finaux

Les prospects incluent les différentes parties prenantes de l'hôpital qui interagiront directement ou indirectement avec les systèmes mis en place : administrateurs, médecins, infirmiers, et équipes techniques.

- Enquête auprès des équipes médicales : Identifier les besoins spécifiques des médecins et infirmiers en termes d'accès aux données des patients, d'intégration des équipements médicaux connectés, et d'outils de suivi.

- Consultation du personnel administratif : Clarification des besoins en termes de gestion des accès, des dossiers médicaux électroniques et des fonctionnalités de cybersécurité pour protéger les données sensibles.

7.4.2. Collaboration avec l'équipe informatique de l'hôpital

L'équipe informatique doit être impliquée pour assurer la compatibilité des nouveaux systèmes avec l'infrastructure existante, notamment pour l'intégration des réseaux, des bases de données, et des équipements de surveillance.

7.5. Partie financière : Cahier des charges

7.5.1. Préparation d'un cahier des charges financier

La partie financière du cahier des charges doit inclure une estimation détaillée des coûts et un plan de financement pour l'acquisition et la maintenance des systèmes.

- Évaluation du ROI (Retour sur Investissement) : Justification des coûts par rapport aux gains attendus en termes d'efficacité, de sécurité, et de réduction des risques.
- Financement et amortissement : Planification du financement à travers des subventions, des prêts, ou des partenariats public-privé, avec une attention particulière à l'amortissement des coûts sur une période de plusieurs années.

7.5.2. Planification des coûts récurrents

- Contrats de maintenance : Budget dédié pour la maintenance des systèmes, y compris le renouvellement des licences logicielles, les mises à jour et les interventions techniques.
- Coûts énergétiques : Calcul des coûts liés à l'utilisation des systèmes IOT et des serveurs de données, avec une optimisation possible par des systèmes d'énergie renouvelable.

7.6. Administration financière : Cahier des charges

7.6.1. Gestion budgétaire et contrôle des dépenses

L'administration financière de l'hôpital doit avoir accès à un tableau de bord financier pour surveiller les dépenses en temps réel et ajuster les budgets en fonction des priorités et des imprévus.

- Suivi budgétaire : Mise en place de logiciels de gestion financière permettant un suivi précis des coûts engagés, avec des rapports détaillés pour chaque phase du projet.
- Procédures de validation des paiements : Processus de validation par étapes pour les paiements des fournisseurs, des sous-traitants et des prestataires de services.

7.6.2. Reporting financier

- Rapports financiers mensuels : Préparation de rapports financiers réguliers détaillant les coûts réels par rapport aux estimations initiales, avec une analyse des écarts et des prévisions de dépenses.
- Audits financiers : Organisation d'audits réguliers pour vérifier la conformité des dépenses avec les budgets alloués et les contrats signés.

7.7. Documentation marketing

7.7.1. Création de documentation technique et marketing

Une documentation détaillée doit être préparée pour soutenir les efforts de communication et de promotion du projet auprès des parties prenantes internes (direction, personnel médical) et externes (partenaires, investisseurs).

- Documentation technique : Fiches techniques des équipements et logiciels installés, protocoles de sécurité, et manuels d'utilisation pour les administrateurs et les utilisateurs finaux.
- Brochures et présentations : Création de brochures et de supports de présentation pour expliquer les bénéfices du projet, ses objectifs, et son impact sur la sécurité et l'efficacité de l'hôpital.

7.7.2. Communication avec les parties prenantes

- Campagne d’information interne : Sensibilisation du personnel hospitalier aux nouvelles technologies mises