Anisse FOUKA ; Mourad AMGHAR ; Mehdi BERRADA ; Altay CEVIK

Rapport technique :

Réseau d’hôpital de campagne

Professeurs : Messieurs Canalda et Spies



# Introduction

## Contexte et objectifs du projet

## Présentation de l’établissement hospitalier

## Enjeux de la sécurité et besoins en infrastructure réseau

## Cahier des charges initial

## Méthodologie de travail et choix technologiques

# Analyse des besoins et conception de l’architecture réseau

## Analyse des besoins techniques et fonctionnels

## Besoins de connectivité, sécurité, performance et évolutivité

## Accessibilité des services et centralisation des données médicales

# Conception de l’architecture réseau

## Diagramme de l’architecture réseau et segmentation par VLAN

## Organisation des sous-réseaux pour les différents services (administration, médical, IoT, etc.)

## Choix des équipements et logiciels

## Routeurs, switchs, points d’accès (ex : borne Linksys), et serveurs

## Solutions logicielles pour la gestion des droits, des accès et de la sécurité réseau

# Configuration réseau : VLAN, DHCP, VPN et sécurité

## VLANs et segmentation du réseau

### Création des VLANs (ex : VLAN médical, administratif, IoT, Wi-Fi) et définition des adresses IP

### Isolation des réseaux pour limiter l’accès inter-VLANs

### Mise en œuvre des VLANs avec configuration des ports pour chaque service

## Configuration du DHCP et gestion des adresses IP

### Configuration du serveur DHCP pour l’attribution automatique d’adresses IP

### Attribution dynamique des adresses IP selon les VLANs

## Sécurité du réseau avec Stormshield

## Paramétrage des règles de firewall et d’ACL pour contrôler les flux réseau

## Règles de sécurité pour l’accès au réseau interne selon les rôles des utilisateurs

## Portail captif Wi-Fi et authentification

### Configuration de la borne Linksys pour un portail captif sécurisé

### Accès au réseau Wi-Fi contrôlé par authentification

## Configuration du VPN pour accès vers un autre hôpital

### Mise en place d’un VPN pour les accès distants

### Configuration des certificats et des droits d’accès sur le VPN

# Développement et intégration de l’application web

## Présentation des objectifs de l'application

### Rôle de l’application pour la gestion des patients, des imprimantes, et des consultations

## Architecture de l'application en Node.js, HTML, CSS et JavaScript

### Structure en Node.js pour le serveur back-end et gestion des requêtes http

### Utilisation de HTML et CSS pour la structure et le design des pages web

### Intégration de JavaScript pour la dynamique des pages et interactions utilisateur

## Gestion des utilisateurs et sécurité de l’application

### Middleware de sécurité et authentification pour l’accès (ex : express-session, JWT)

### Connexion sécurisée via Firebase et gestion des rôles (admin, personnel médical)

### Protection des pages sensibles selon le rôle de l’utilisateur

## Fonctionnalités principales de l’application

### Gestion des patients : ajout, modification, consultation

### Gestion des imprimantes et suivi des stocks d’encre

### Consultation des données médicales et statistiques

## Interaction avec les services réseaux et IoT

### Intégration des données de l’IoT pour le suivi en temps réel des salles (température, CO2)

### Communication avec le serveur Apache pour récupérer et afficher les données MQTT

## Sécurité et protection des données utilisateurs

### Utilisation des middlewares pour sécuriser les requêtes et limiter l’accès

### Chiffrement des données sensibles et protection des informations médicales

# Infrastructure IoT et gestion des données environnementales

## Déploiement et configuration des capteurs IoT (température, mouvement, etc.)

## Installation des capteurs et configuration avec le broker MQTT sur Raspberry Pi

## Suivi des données en temps réel et visualisation pour la gestion des environnements hospitaliers

## Collecte et interprétation des données avec Apache

### Configuration du serveur Apache pour récupérer les données MQTT

### Création de graphiques et de tableaux de bord pour visualiser les données de capteurs

## Sécurité des données IoT

### Mise en place de certificats TLS pour sécuriser la communication avec le broker MQTT

### Accès restreint aux données IoT et surveillance des flux réseau

# Tests et validations

## Résultats et validation des fonctionnalités de l’application web

## Tests de gestion des utilisateurs et de l’accès sécurisé aux données

## Vérification de la consultation et de l’intégration des données IoT

# Coût total du projet

## Coûts des équipements et infrastructures réseau

## Routeurs, switchs, bornes Wi-Fi, serveurs, capteurs, etc.

## Coûts logiciels et licences

## Solutions logicielles de sécurité (Stormshield), Firebase, logiciels de monitoring

## Coûts de développement de l’application

### Temps de développement en Node.js, HTML, CSS, et JavaScript

## Coûts d’installation et de formation

### Installation des équipements, configuration des VLANs, formation des utilisateurs

## Coût total estimé et plan de financement

# 8. Améliorations potentielles

## Améliorations de l’infrastructure réseau

### Ajout de redondance pour la haute disponibilité

### Mise à jour des équipements pour suivre les évolutions technologiques

## Optimisation de l’application web

### Ajout de nouvelles fonctionnalités, par exemple, gestion des rendez-vous et alertes

### Amélioration de l’interface utilisateur pour plus de convivialité

## Extension de l’IoT et collecte de nouvelles données

### Intégration de nouveaux capteurs pour une gestion plus fine de l’environnement

### Développement de tableaux de bord pour un suivi plus avancé des paramètres

# Conclusion

## Bilan du projet et atteinte des objectifs

## Perspectives futures et retours sur expérience

## **Introduction**

## **A. Contexte et objectifs du projet**

## L'évolution rapide des technologies numériques a transformé de nombreux secteurs, y compris le domaine de la santé. Les hôpitaux, en particulier, sont désormais confrontés à des défis technologiques importants pour offrir des soins de qualité tout en assurant la sécurité des données médicales. La digitalisation des établissements de santé, combinée à l'essor des objets connectés (IoT), exige une infrastructure réseau fiable et sécurisée pour gérer les informations sensibles et les dispositifs médicaux.

## Ce projet a pour objectif de moderniser l'infrastructure réseau d'un établissement hospitalier, en renforçant la sécurité des systèmes d'information et en intégrant des dispositifs IoT pour améliorer la gestion et la surveillance des données. Plus précisément, il s'agit de mettre en place une architecture réseau robuste, d'assurer la sécurité des communications internes et externes, et d'implémenter une solution de maintenance qui garantit la disponibilité des systèmes critiques. Le projet vise à répondre aux besoins actuels de l'hôpital tout en anticipant les évolutions futures des technologies de santé.

## **B. Présentation de l'établissement hospitalier**

## L'établissement hospitalier concerné est un centre de soins de taille moyenne, disposant de plusieurs services spécialisés, comme la médecine générale, la chirurgie, la pédiatrie et les soins intensifs. Il est doté d'une infrastructure informatique essentielle pour la gestion des dossiers patients, l'échange d'informations médicales entre services et la coordination des soins.

## Avec une augmentation du nombre de patients et de données générées, l'hôpital a besoin de moderniser son infrastructure pour garantir une gestion efficace des flux d'informations. Ce besoin de transformation numérique se traduit par une demande d'augmentation de connectivité sécurisée, d'accès distant pour le personnel médical, et de protection renforcée contre les cyberattaques. De plus, l'hôpital souhaite intégrer des dispositifs IoT pour la surveillance en temps réel de certains équipements et paramètres, tels que la température et le niveau de CO2 dans les salles, afin de garantir des conditions optimales de soins et de sécurité.

## **C. Enjeux de la sécurité et besoins en infrastructure réseau**

## La sécurité des données de santé est un enjeu crucial pour les établissements hospitaliers. Les informations médicales sont sensibles et doivent être protégées contre les accès non autorisés et les cyberattaques. En outre, l'infrastructure réseau doit être capable de gérer des flux de données importants et d'assurer une connectivité continue entre les différents services de l'hôpital.

## Les principaux enjeux de sécurité pour cet hôpital sont :

## **Protection des données patients** : Assurer la confidentialité et l'intégrité des informations médicales.

## **Sécurité des dispositifs IoT** : Mettre en place des mesures de sécurité pour les objets connectés, tels que les capteurs et badges d'accès, afin de limiter les risques de piratage.

## **Contrôle des accès** : définir des règles strictes pour limiter l'accès aux informations sensibles aux seuls membres autorisés du personnel.

## **Continuité de service** : Garantir une disponibilité constante des systèmes pour éviter tout risque d'interruption des soins.

## Pour répondre à ces enjeux, l'hôpital a besoin d'une infrastructure réseau modernisée et sécurisée, avec des dispositifs de cybersécurité avancés, une gestion des accès par badge RFID, un monitoring en temps réel, et un support de maintenance pour répondre aux incidents dans des délais rapides.

## **D. Cahier des charges initial**

## Le cahier des charges initial a défini les besoins spécifiques de l'hôpital en termes de sécurité, de performance et de gestion des données. Les principales exigences comprennent :

## **Architecture réseau sécurisée** : Mettre en place une architecture segmentée avec des VLAN pour cloisonner les services critiques et limiter les risques d'intrusion.

## **Gestion des accès et contrôle des identités** : Intégrer un système de gestion des badges RFID pour les différents niveaux de personnel, permettant un contrôle précis des accès.

## **Protection des données et surveillance réseau** : Installer des dispositifs de sécurité avancés (pare-feu, IDS/IPS) pour détecter et prévenir les cybermenaces en temps réel.

## **Intégration des dispositifs IoT** : Connecter et sécuriser les capteurs de température, de mouvement, et de CO2, ainsi que les caméras de surveillance, pour garantir un environnement de soin optimal.

## **Maintenance et support** : Proposer des options de maintenance incluant des interventions sur site et une surveillance à distance, avec des délais de réponse rapide en cas de panne.

## Ces exigences visaient à assurer un niveau élevé de sécurité et de disponibilité pour l'infrastructure de l'hôpital, tout en tenant compte de la flexibilité nécessaire pour s'adapter aux futures évolutions technologiques.

## **E. Méthodologie de travail et choix technologiques**

## Pour mener à bien ce projet, une **méthodologie Agile** a été adoptée, avec des sprints hebdomadaires permettant une planification, un suivi et un ajustement continu en fonction des retours. Cette méthodologie a permis une grande flexibilité, essentielle pour un projet impliquant des parties variées et des infrastructures complexes. Chaque sprint comprenait une phase de planification, de développement, de tests, et de validation, garantissant ainsi une progression contrôlée et un ajustement rapide en cas d'imprévus.

## Les **choix technologiques** ont été faits en fonction des exigences de sécurité, de performance et de durabilité. Parmi les principaux éléments technologiques retenus figurent :

## **Switches Cisco Catalyst et routeur Stormshield** : Choix pour leur robustesse et leur capacité à supporter un trafic important tout en offrant des fonctionnalités de segmentation et de filtrage des données.

## **Serveurs DELL et dispositifs IoT** : Utilisés pour la gestion des données et la surveillance en temps réel des conditions environnementales dans les salles.

## **Système de gestion des accès par badge RFID** : Permettant une gestion fine des autorisations et une traçabilité des accès pour renforcer la sécurité.

## **Dispositifs de cybersécurité** : Pare-feu et IDS/IPS pour la protection en temps réel contre les intrusions et les cybermenaces, assurant un haut niveau de sécurité pour les données critiques.

## **Logiciels de surveillance et de maintenance** : Intégration d'outils de suivi pour surveiller l'état des dispositifs en temps réel et intervenir rapidement en cas de problème.

## Ce choix technologique, combiné à une méthodologie de gestion de projet Agile, a permis de garantir une infrastructure sécurisée, évolutive, et capable de répondre aux besoins présents et futurs de l'établissement hospitalier.

## **II. Analyse des besoins et conception de l'architecture réseau**

## **A. Analyse des besoins techniques et fonctionnels**

## L'infrastructure réseau d'un hôpital doit répondre à des besoins spécifiques en raison de la nature sensible des données et des services fournis. Une analyse approfondie des besoins techniques et fonctionnels a été réalisée pour déterminer les éléments nécessaires à une infrastructure réseau sécurisée et performante, capable de supporter des services critiques.

## **Besoins techniques :**

## **Sécurité des données** : La protection des données médicales est primordiale pour garantir la confidentialité des informations des patients. Cela nécessite une architecture réseau incluant des dispositifs de sécurité avancés comme les pare-feu, les systèmes de détection/prévention d'intrusion (IDS/IPS), et des politiques de contrôle d'accès strictes.

## **Gestion des identités et des accès** : Le réseau doit permettre une gestion notamment centralisée des accès, afin de contrôler les droits d'accès des différents profils d'utilisateurs, via un système de badges RFID pour le personnel, avec des autorisations adaptées à chaque rôle.

## **Suivi et gestion des équipements IoT** : Avec l'intégration croissante des objets connectés dans le milieu hospitalier, tels que les capteurs de température, de mouvement et de CO2, il est nécessaire d'assurer un suivi rigoureux de ces équipements et de sécuriser les communications entre ces dispositifs et les systèmes centraux.

## **Continuité de service** : L'hôpital ayant une activité continue, il est impératif que l'infrastructure réseau soit résiliente et assure un temps de disponibilité maximal, avec des mécanismes de basculement en cas de défaillance (ex. redondance des serveurs et du réseau).

## **Besoins fonctionnels :**

## **Centralisation des données médicales** : La centralisation des dossiers médicaux et des informations critiques doit permettre un accès rapide et sécurisé aux données par le personnel soignant, tout en respectant les réglementations de confidentialité.

## **Connectivité multiservice** : L'infrastructure doit prendre en charge plusieurs types de services (médical, administratif, IoT, sécurité) avec une segmentation réseau appropriée pour éviter les risques de compromission.

## **Maintenance et surveillance en temps réel** : Un système de surveillance en temps réel est nécessaire pour surveiller l'état des équipements et des connexions réseau, permettant ainsi une intervention rapide en cas de dysfonctionnement.

## **B. Besoins de connectivité, sécurité, performance et évolutivité**

## Pour répondre aux exigences de l'hôpital, l'infrastructure réseau doit combiner des niveaux élevés de **connectivité** , de **sécurité** , de **performance** et d' **évolutivité** .

## **1. Connectivité**

## **Segmentation réseau** : Pour limiter les risques de propagation des attaques et isoler les différents services (ex. soins, administration, IoT), l'infrastructure utilise des VLAN. Chaque service dispose de son propre VLAN avec un accès restreint aux autres segments du réseau.

## **Support de la mobilité** : Le personnel hospitalier doit pouvoir se déplacer librement dans l'établissement tout en restant connecté. Des points d'accès Wi-Fi performants ont été déployés dans les zones clés, assurant une couverture complète et sécurisée du réseau sans fil.

## **2. Sécurité**

## **Pare-feu et IDS/IPS** : Des dispositifs de sécurité, comme les pare-feu et les systèmes IDS/IPS, sont utilisés pour surveiller le trafic réseau et détecter toute tentative d'intrusion ou d'attaque. Ces dispositifs permettent de réagir rapidement en cas d'incident et de bloquer l'accès aux zones sensibles.

## **Authentification multi-facteur et gestion des accès** : Un système d'authentification multi-facteur est mis en place pour les utilisateurs ayant accès aux données critiques, et des badges RFID permettent de gérer l'accès aux zones physiques sensibles.

## **Chiffrement des données** : Toutes les communications, en particulier celles contenant des informations médicales ou sensibles, sont chiffrées pour éviter toute interception. Les protocoles de chiffrement SSL/TLS sont utilisés pour les connexions externes et internes.

## **3. Performance**

## **Haute disponibilité et redondance** : Les équipements critiques (serveurs, routeurs) sont configurés avec des mécanismes de redondance pour assurer une continuité de service en cas de panne. Des switchs haute performance sont utilisés pour gérer un trafic élevé sans dégradation de la qualité de service.

## **Priorisation du trafic** : La gestion de la qualité de service (QoS) est essentielle pour garantir que les applications critiques, comme les systèmes de gestion des dossiers médicaux, bénéficient de la priorité sur le réseau en cas de congestion.

## **4. Évolutivité**

## **Préparation pour les évolutions futures** : L'architecture est conçue pour pouvoir intégrer facilement de nouveaux dispositifs IoT et des services supplémentaires. La capacité de stockage et de traitement est dimensionnée de manière à supporter les futurs besoins en connectivité et en gestion de données.

## **Gestion centralisée et évolutive** : La gestion de l'infrastructure est centralisée pour faciliter les mises à jour et l'ajout de nouveaux composants. Des systèmes de gestion de réseau avancés sont utilisés pour permettre des ajustements rapides et des extensions sans interruption de service.

## **C. Accessibilité des services et centralisation des données médicales**

## Dans un environnement hospitalier, l' **accessibilité des services** et la **centralisation des données médicales** sont des éléments essentiels pour assurer une prise en charge rapide et efficace des patients. La centralisation permet au personnel médical d'accéder en temps réel aux dossiers patients et aux informations critiques, déterminant de leur emplacement au sein de l'hôpital.

## **1. Centralisation des données médicales**

## **Stockage centralisé et sécurisé** : Toutes les données médicales et administratives sont stockées dans un système de gestion centralisé, accessible uniquement par le personnel autorisé. Ce stockage centralisé simplifie la gestion des dossiers et réduit les risques de perte ou de vol de données.

## **Accès contrôlé et traçabilité** : Les accès aux données médicales sont strictement contrôlés et enregistrés pour garantir la traçabilité. Les autorisations sont basées sur des profils définis en fonction du rôle et des responsabilités de chaque membre du personnel.

## **Interconnexion avec les dispositifs IoT** : Les dispositifs IoT, tels que les capteurs de température et les caméras de surveillance, sont connectés au système central, permettant une collecte et une visualisation des données en temps réel. Cela aide le personnel à surveiller l'environnement de soin et à intervenir rapidement en cas de besoin.

## **2. Accessibilité des services**

## **Accès mobile sécurisé** : Grâce à une infrastructure Wi-Fi sécurisée, les médecins et infirmiers peuvent accéder aux dossiers et aux applications médicales directement depuis des terminaux mobiles dans tout l'établissement.

## **Continuité d'accès** : En cas de panne, les mécanismes de redondance permettent de maintenir l'accès aux services critiques. Les systèmes vitaux et les bases de données sont protégés contre les interruptions, garantissant ainsi une continuité des soins.

## **Optimisation des flux de travail** : La centralisation des données et la facilité d'accès permettent une meilleure coordination entre les différents services, ainsi que les délais de prise en charge et la qualité des soins offerts aux patients.

## **VIII. Coût total du projet**

## **Coûts des équipements et infrastructures réseau**

## Pour mener à bien ce projet d'infrastructure réseau sécurisée au sein de l'hôpital, il a été nécessaire de prévoir un budget conséquent pour les équipements matériels. Ces équipements constituant le socle de l'infrastructure réseau, permettant de garantir une connectivité fiable, une performance élevée et une sécurité optimale. Les éléments matériels achetés incluent des switchs, des routeurs, des serveurs et des dispositifs IoT, chacun étant sélectionné pour ses caractéristiques de sécurité et de performance adaptées aux besoins hospitaliers.

## Le budget pour les équipements comprend :

## **Switches Cisco Catalyst** : Ces switchs permettent la gestion des VLAN et assurent une segmentation réseau fiable pour isoler les différents services de l'hôpital, intervenant ainsi les risques d'intrusion.

## **Routeur Stormshield** : Choisi pour ses fonctionnalités avancées de sécurité et de filtrage, ce routeur assure une protection efficace des flux de données entrants et sortants.

## **Serveurs DELL** : Utilisés pour la centralisation des données médicales et la gestion des dispositifs connectés, les serveurs sont dimensionnés pour assurer une haute disponibilité et des performances optimales.

## **Capteurs IoT et dispositifs de contrôle d'accès** : Divers capteurs (température, CO2, mouvements) et des badges RFID ont été intégrés pour la surveillance de l'environnement hospitalier et le contrôle des accès, garantissant la sécurité physique des installations.

## **B. Routeurs, switchs, bornes Wi-Fi, serveurs, capteurs, etc.**

## Les équipements suivants ont été nécessaires pour l'infrastructure réseau :

## **Bornes Wi-Fi** : Pour garantir une connectivité mobile sécurisée dans tout l'établissement, plusieurs bornes Wi-Fi ont été installées, offrant une couverture sans fil complète et supportant un grand nombre de connexions simultanées. Les bornes sont configurées pour restreindre l'accès aux utilisateurs autorisés et respecter les règles de confidentialité.

## **Dispositifs de surveillance et de contrôle** : Des caméras connectées, des capteurs de mouvements, et des capteurs de température et de CO2 sont installés pour surveiller les conditions de sécurité dans l'hôpital en temps réel.

## Ces équipements sont dimensionnés pour répondre aux besoins actuels de l'hôpital et sont évolutifs afin d'accommoder de futures extensions. Les coûts associés à ces équipements représentent une part importante du budget, mais ils sont indispensables pour assurer une infrastructure sécurisée, performante et adaptée aux exigences de l'hôpital.

## **C. Coûts logiciels et licences**

## Les logiciels et licences nécessaires pour sécuriser et gérer efficacement l'infrastructure réseau de l'hôpital incluent des solutions de sécurité, des plateformes de surveillance et des outils d'administration.

## **D. Solutions logicielles de sécurité (Stormshield), Firebase, logiciels de surveillance**

## **Stormshield** : Pour la sécurisation du réseau, la solution de pare-feu Stormshield a été choisie pour ses capacités avancées en matière de détection et de prévention des intrusions. Stormshield offre des fonctionnalités de filtrage des contenus, de protection contre les malwares, et de gestion des accès, garantissant une protection continue de l'infrastructure réseau.

## **Firebase** : Utilisé pour la gestion des connexions utilisateur et l'authentification, Firebase simplifie la centralisation des données d'authentification et renforce la sécurité des accès au réseau.

## **Logiciels de monitoring** : Des logiciels de monitoring ont été intégrés pour surveiller les performances du réseau et des dispositifs IoT en temps réel. Ces logiciels permettent de détecter toute anomalie, d'alerter les administrateurs en cas de problème, et de prendre des mesures correctives rapides pour éviter les interruptions de service.

## Ces solutions logicielles nécessitent des licences payantes, mais elles offrent des fonctionnalités critiques pour la protection et le suivi de l'infrastructure réseau, justifiant ainsi leur coût dans le budget total.

## **E. Coûts de développement de l'application**

## Le développement d'une application pour la gestion et la surveillance des infrastructures a été réalisé en interne, en utilisant des technologies adaptées aux besoins spécifiques de l'hôpital. L'application a été développée en utilisant **Node.js, HTML, CSS et JavaScript** .

## **Temps de développement** : Le temps de développement a été amélioré en fonction des fonctionnalités spécifiques de l'application, notamment la gestion des accès par badge RFID, le suivi des capteurs IoT, et la création de rapports pour le personnel hospitalier. Chaque fonctionnalité nécessite plusieurs cycles de développement et de tests pour garantir une interface utilisateur intuitive et une intégration parfaite avec le réseau de l'hôpital.

## Le coût de développement représente principalement le temps de travail des développeurs, leur expertise en cybersécurité, et les tests nécessaires pour garantir une application fiable et sécurisée.

## **F. Coûts d'installation et de formation**

## **1. Installation des équipements** : L'installation des équipements a été réalisée par une équipe de techniciens spécialisés. Elle comprenait la configuration des switchs et des routeurs, le déploiement des VLAN pour la segmentation du réseau, et l'intégration des dispositifs de contrôle d'accès et des capteurs IoT. Ces installations ont été réalisées selon une planification rigoureuse pour minimiser les interruptions de service au sein de l'hôpital.

## **2. Formation des utilisateurs** : Une formation a été dispensée au personnel hospitalier pour s'assurer qu'ils maîtrisent les nouvelles technologies mises en place. Cette formation inclut l'utilisation de l'application développée, la gestion des accès par badge RFID, et les bonnes pratiques de sécurité pour réduire les risques d'erreurs humaines.

## Ces coûts d'installation et de formation sont essentiels pour assurer la pérennité du projet. Ils garantissent que les utilisateurs finaux sont autonomes dans l'utilisation de l'infrastructure et qu'ils peuvent répondre aux exigences de sécurité de l'hôpital.

## **G. Coût total accru et plan de financement**

## **Estimation totale** : Le budget total pour ce projet a été coûté à **80 506,60 € TTC** , incluant la marge pour les imprévus. Ce montant couvre l'ensemble des équipements, des licences logicielles, du développement de l'application, ainsi que les coûts d'installation et de formation. La répartition est la suivante :

## **Équipements matériels** : 48 738,83 €

## **Main-d'œuvre et installation** : 18 350 €

## **Marge de sécurité** (20 %) : 13 417,77 €

## **Plan de financement** : Le financement du projet repose sur une combinaison de fonds propres et de subventions potentielles pour la transformation numérique et la sécurité dans les établissements de santé. L'hôpital peut également bénéficier de crédits d'impôt pour les dépenses liées à la recherche et au développement (R&D) dans le domaine de la santé et de la cybersécurité. Ce financement permettra de couvrir non seulement le coût initial du projet, mais également les frais de maintenance récurrents.