Version 2024

PROJET APPLI-FRAIS

Mise en place d'une architecture technique et des fonctions de sécurisation pour l'application de suivi des comptes rendus et des frais de remboursement

Définition du besoin

Forme de l'objet

L'application Web destinée aux visiteurs, délégués et responsables de secteur sera en ligne, accessible depuis un ordinateur connecté à Internet mais aussi de l'ensemble des différents sites qui composent le réseau GSB.

Accessibilité/Sécurité

L'environnement doit être accessible aux seuls acteurs de l'entreprise.
Une authentification préalable sera nécessaire pour l'accès au contenu.
Tous les échanges produits doivent être chiffrés par le serveur Web.

Architecture

L'architecture réseau devra comporter des périmètres de sécurité permettant de cloisonner dans des réseaux différents les machines du LAN et les serveurs publics destinés à une consultation externe.

Les accès provenant des réseaux publics vers les serveurs seront filtrés afin de ne laisser passer que les flux nécessaires.
Le serveur de base de données sera situé dans un réseau différent de celui du serveur web, ses accès seront sécurisés.

Le prestataire fournira un schéma montrant les échanges de flux entre les différents périmètres de sécurité.

Le projet consiste à mettre en place la solution technique sur le réseau de l'entreprise, en intégrant les différents serveurs en DMZ ou sur le LAN et en activant les différentes techniques de sécurisation : authentifications, chiffrement sur le serveur web, filtrage par le firewall…
L'ensembles des services répondant aux besoins exprimés devront être reproduit dans votre maquette.

Si vous avez un peu de patience,
vous découvrirez qu'on peut utiliser les immenses ressources du Web
pour perdre son temps avec une efficacité que vous n'aviez jamais osé imaginer.
Dave Barry

CAHIER DES CHARGES

Définition du besoin

Définition de l'objet
Le laboratoire désire mettre à disposition des visiteurs médicaux une application Web permettant de centraliser les comptes-rendus de visite.

L'entreprise a choisi d'héberger en interne les serveurs exécutant l'application.
L'achat de nouveaux équipements peut être envisagé si le besoin le justifie.

Cahier des charges

1. **Environnement**

L'environnement des serveurs est à déterminer : Linux, Windows Server, autre..

2. **Services**

Pour chaque service, on précise les fonctionnalités à mettre en œuvre.

3. Pour **le service de gestion des rapports**

- Un serveur Web sécurisé exécutant des pages de script côté serveur (PHP, ASP.net, JSP, autre)
- Une base de données relationnelle
- Les deux serveurs sont distincts
- On ne veut pas d'outils pré-configurés (LAMP, WAMP, EasyPHP, etc) mais des modules indépendants.
- Le projet porte uniquement sur la partie architecture, la partie développement sera assurée par une autre équipe

4. Pour la **mise à jour des pages Web**

- un service sécurisé avec authentification (par base de données, annuaire ou autre gestion d'utilisateurs) limitant l'accès aux seuls développeurs de l'entreprise.
- Ce service est limité à un accès interne. Il ne doit pas être ouvert à l'extérieur.

5. Pour la **gestion des frais**

- les visiteurs alimentent les frais engagés par le biais du serveur web de gestion des rapports
- le service comptable met à jour la base de données par une page Web intégrée à l'intranet ou par un module de traitement automatique suite aux enregistrements comptables réalisés sur le PGI.

6. Accès WEB

On souhaite une application en ligne, sécurisée, accessible par un **FQDN (nom pleinement qualifié)** de type **visite.gsb.coop.**
Le système doit donc être accessible depuis un navigateur installé sur un poste intérieur ou extérieur à l'entreprise.

7. Accessibilité/Sécurité

L'environnement doit être accessible aux seuls acteurs de l'entreprise.
Les données ne doivent pas être accessibles directement de l'extérieur mais uniquement par des interrogations réalisées par le serveur Web.

Une authentification préalable sera nécessaire pour l'accès au contenu.
Les échanges avec l'extérieur doivent être sécurisés.

8. Filtrage

- L'architecture technique sera construite de manière à ne permettre que les accès strictement utiles aux différents serveurs. Pour cela plusieurs périmètres de sécurité seront mis en place et les échanges entre ces périmètres seront contrôlés et filtrés.
- Les restrictions d'accès aux serveurs eux-mêmes seront étudiés.

L'architecture proposée et la politique de filtrage retenue feront l'objet d'un compte-rendu argumenté et illustré.

9. Sauvegarde

L'ensemble des données peut être perdu.
La sauvegarde des informations est donc cruciale.

10. Administration de la base de données

Le commanditaire souhaite pouvoir faire évoluer ses bases dans le futur, il souhaite que le prestataire lui laisse un mode opératoire lui permettant :

- De faire évoluer la base : ajout/suppression de colonnes ou de tables
- De modifier les droits d'accès sur les données et de créer ou supprimer des utilisateurs

Il vous demande d'écrire des **requêtes** pour s'entrainer à ces futures évolutions :

- Sur votre serveur bdd, créer 3 utilisateurs (correspond à chacun des membres de votre trinôme).
- Le chef de projet de votre équipe devra avoir tous les droits sur l'ensemble des BDD du serveur.
- La personne responsable de la mise en place de la bdd GSB aura tous les droits possibles sur cette bdd gsb.
- Le dernier étudiant pourra uniquement lire et modifier les données de la bdd gsb et non la structure de cette bdd.

- Créer une table REGION qui contiendra la liste des régions françaises (identifiant et nom)
- Ajouter un champ idregion dans la table VISITEUR
- Créer un lien entre le champ idregion de VISITEUR et celui de la nouvelle table REGION (clé étrangère).
- Remplir la table REGION avec les différents noms de région qui existent en France.
- Modifier les enregistrements de quelques visiteurs pour leur attribuer leur région.
- Créer une vue qui liste les visiteurs des Pays de la Loire.

11. Cybersécurité

Conscient de l'enjeu critique des deux aspects principaux de la sécurité :

- prévenir les **accidents**
- prévenir les **actes de malveillance**

LA DSI vous demande de présenter pour chacun des aspects du projet (contraintes 1 à 13) qui pourrait présenter des risques de cette nature, l'e*nsemble des mesures techniques mises en œuvre permettant au système d'information de résister à des événements susceptibles de compromettre*

- *la disponibilité*
- *l'intégrité*
- *ou la confidentialité*

des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

Vous indiquerez les thématiques concernées par vos préconisations dans les normes ISO 27001 et 27002, et celles qui restent à explorer.

Un outils de détection et de prévention des intrusions (IDS/IPS) sera nécessaire dans le cadre de ce projet.

12. Synchronisation temporelle des matériels critiques

L'administrateur a noté des variations sensibles sur l'horloge interne des serveurs, ce qui pourrait à terme corrompre l'intégrité de certaines sauvegardes ou synchronisations. Il souhaite donc mettre en place un serveur de temps sur lequel seront synchronisés tous les serveurs et matériels actifs de GSB.

Un enregistrement nommé SRV_Temps sera ajouté sur le serveur DNS afin de faciliter son accessibilité à partir des matériels concernés.

Afin de convaincre le directeur financier de l'opportunité de celui-ci, il souhaite que vous rédigiez un argumentaire justifiant l'opportunité de sa mise en place.

13. Liaison avec la succursale de Gacilly

La société **GSB**, dans le cadre de son **développement**, souhaite se **rapprocher** géographiquement des **sources** « **biologiques** » des molécules utilisés dans les futures nouvelles gammes de médicaments. Cela lui permettra d'être plus **indépendant** des entreprises lui fournissant ce type de molécules à ce jour, mais aussi d'entrer dans une démarche plus **écologique** en étant plus proche de la matière première.

Elle désire s'implanter à la **Gacilly** en Bretagne afin de se rapprocher des Laboratoires Yves Rocher et des laboratoires Daniel Jouvance situés sur l'**île de Houat** ; tous les deux menant des recherches sur le bienfait d'éléments présents dans les plantes et/ou l'océan. Une **joint-venture** a été réalisée afin de formaliser les relations entre les différents laboratoires.

Le DSI désire centraliser la gestion des services et des ressources informatiques de l'entreprise sur le site du siège social. Par exemple :

- **l'authentification** des utilisateurs sera **centralisée**, réalisée par les services Active Directory gérés au siège social ;

- les **accès** aux ressources **Internet** seront gérés par un serveur **mandataire.**
L'installation de ce serveur fera l'étude des paramétrages qui permettent la meilleure sécurité possible.

Pour cela, on vous demande de réfléchir à l'ensemble des solutions permettant la mise en œuvre :

- de **connexions** permanentes **sécurisées** entre les différents **sites** ;

- d'un outil de **partage**, de **gestion**, de **filtrage** et de sécurisation des **accès** à **l'internet**.

Le **DSI** vous demande de réfléchir à faire évoluer les accès à la plateforme WEB proposés aux visiteurs médicaux. Pour des raisons de sécurité, on vous demande de réfléchir et de mettre en œuvre une solution permettant à ces derniers de se

connecter via un VPN. Ils se connectent à partir de leurs ordinateurs, smartphones, tablettes. On peut imaginer qu'à partir d'une icône présente sur leur STA qu'ils puissent se connecter automatiquement au VPN, qu'un navigateur WEB ouvre automatiquement l'accès à l'application développée à leur destination. On concentrera les premiers essais sur des plateformes Windows ; cela permettra de valider ou non le projet et d'envisager la portabilité de la solution sur d'autres environnements.

14. Architecture physique et logique du nouveau bâtiment

Le nouveau bâtiment regroupe les services « recherche et développement », « marketing » et « packaging ».
Il est possible d'utiliser la rocade arrivant du VLAN 404 en utilisant les adresses IP réservées.

a) Segmentation

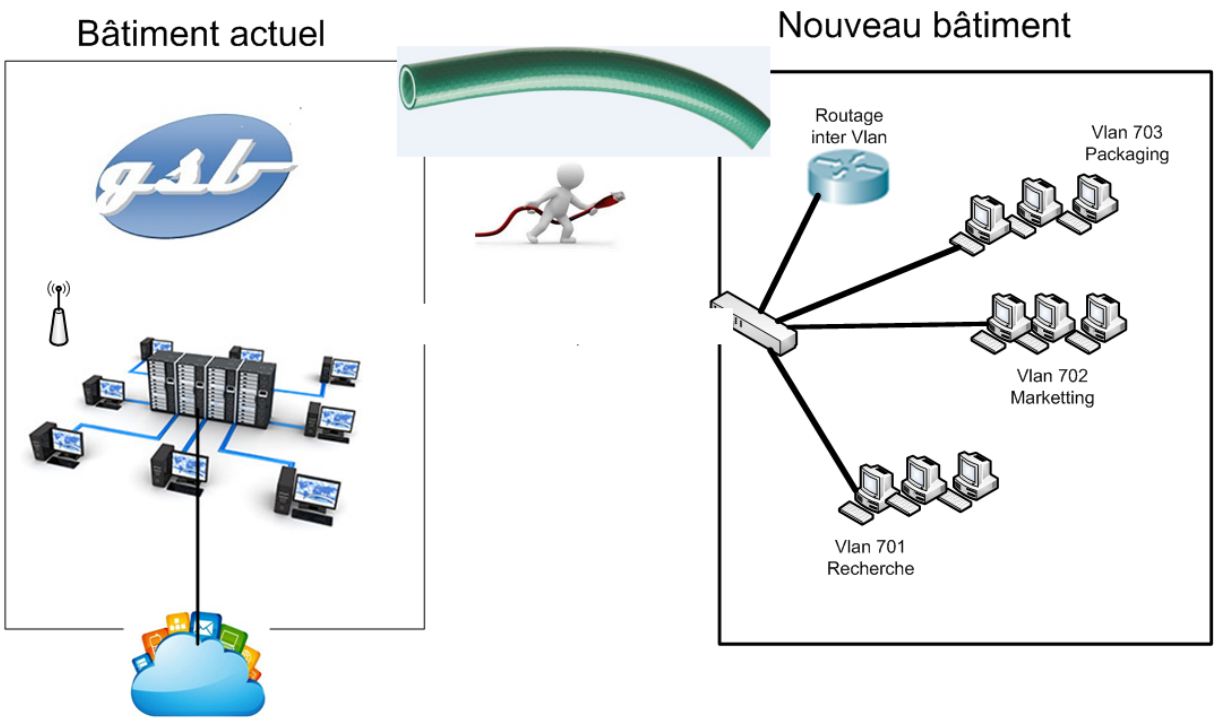
L'organisation du nouveau VLAN et de l'adressage IP est la suivante :

N° VLAN	***Service***	***réseau***	***passerelle***
701	recherche et développement	192.168.71.0/24	192.168.71.254
702	marketing	192.168.72.0/24	192.168.72.254
703	packaging	192.168.73.0/24	192.168.73.254

Les règles à mettre en place concernant les nouveaux vlans sont les suivantes :

- chaque nouveau vlan peut accéder à Internet en HTTP et HTTPS.
  Ils seront par ailleurs routés sur l'infrastructure centrale de l'entreprise, et pourront accéder aux serveurs de GSB comme les autres postes du LAN.
- le vlan " recherche et développement " est inaccessible aux autres vlans.
- les 2 vlans « marketing » et « packaging » partagent des ressources matérielles et logicielles et leurs serveurs donc mutuellement accessibles.

On pourra envisager la mise en place d'un serveur DHCP commun aux 3 nouveaux vlans.



b) Administration des matériels actifs

Les routeurs ou commutateurs mis en place pour le nouveau bâtiment feront l'objet d'une politique sévère en termes de sécurité. Ainsi, ils seront administrables uniquement en mode console ou en SSH (pas d'accès en TELNET ou en HTTP).

Comme les serveurs, ils seront synchronisés sur le serveur de temps SRV_Temps de GSB.
Un serveur TFTP accueillera les sauvegardes des configurations. Des tests de restauration seront effectués.

Ces matériels pourront être ajoutés dans le fichier de zone gsb.coop pour faciliter leur administration distante.

15. Continuité de service

GSB souhaite que vous lui fassiez des propositions pour améliorer la fiabilité des services installés. Ainsi vous choisirez un service mis en place pendant votre intervention et lui proposerez au choix une solution :

- Garantissant la continuité d'un service
- Garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion
- Permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion

16. Contraintes globales

Le prestataire est à l'initiative de toute proposition technique.
Le prestataire fournira un système opérationnel, une documentation technique permettant un transfert de compétences, une documentation de l'architecture (matériel, services, fichiers de configuration) et des options particulières retenues dans le contexte.

Qualité de services

L'ensemble des services réseaux et des matériels actifs mis en œuvre doit fonctionner dans les meilleures conditions possibles en termes de disponibilité, de débits, etc. ». Afin de prévenir certains incidents dus à des défaillances matérielles ou à la saturation des ressources disponibles, **une surveillance de l'ensemble** sera mise en place et l'administrateur sera alerté en cas de problème.

Il vous est aussi demandé de mettre en service une solution de gestion des incidents afin de pouvoir analyser les requêtes, et les statistiques, sources d'évolution futures.

Gestion de parc / Gestion des incidents

L'ensemble des matériels présents sur le système d'information doit être référencé avec une solution de gestion de parc (PC, serveurs, switchs, routeurs, etc.) de manière à assurer un suivi matériel et logiciel de ce parc.

17. Documentation

- La documentation complète, rédigée et mise en forme sera à rendre sous format électronique éditable et accessible par le commanditaire.
- Une fiche reprendra tous les éléments de configuration sans rédaction (paramétrages des services, adressage IP, comptes et mots de passe, etc.)
- Une fiche de tests sera élaborée. Elle reprendra les points exigés dans le cahier des charges, et vérifiera que chaque contrainte est bien respectée. La forme est libre.

(cf : https://fr.wikipedia.org/wiki/Test_d'acceptation)

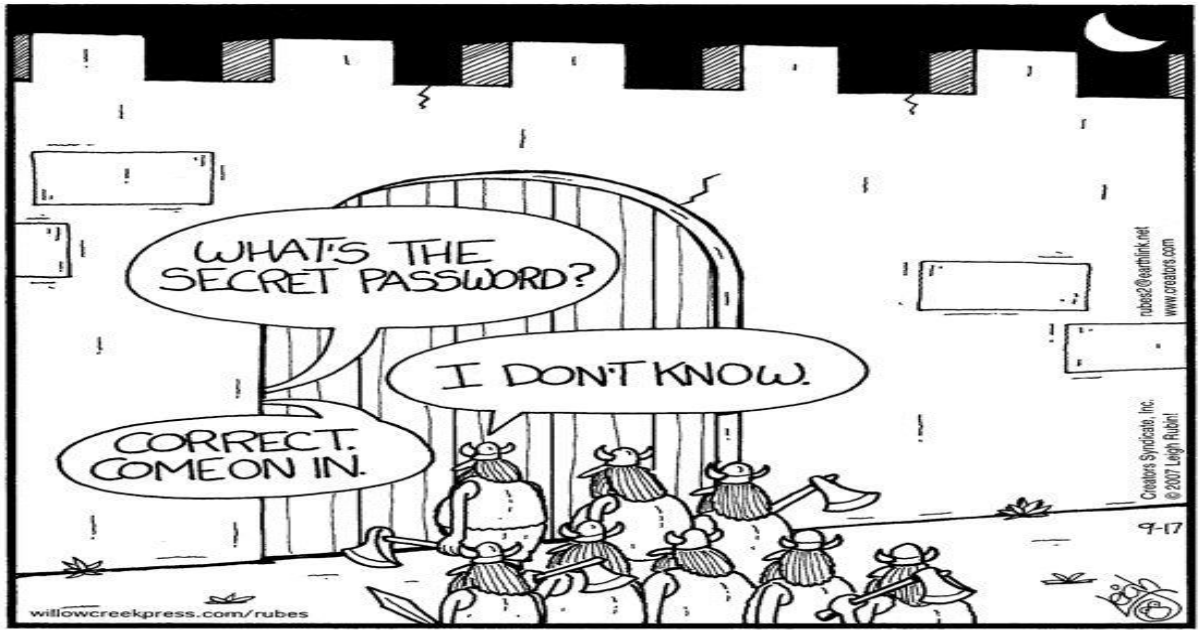
18. Responsabilités

Le commanditaire fournira à la demande toute information sur le contexte nécessaire à la mise en place de l'infrastructure.
Le commanditaire fournira une documentation et des sources exploitables pour la phase de test : base de données exemple, modélisation, scripts ...

Le prestataire est à l'initiative de toute proposition technique. Notamment, il proposera des noms pertinents pour l'accès aux services.
Le prestataire fournira un système opérationnel, une documentation technique permettant un transfert de compétences, une documentation de description de l'architecture (matériel, services et code) et des options particulières retenues dans le contexte.

19. Evolutivité

Lorsque que le cahier des charges ci-dessus est entièrement réalisé et validé par le commanditaire, le prestataire peut s'il le souhaite faire des propositions d'amélioration du projet, notamment en ce qui concerne la haute disponibilité, les sauvegardes, la sécurité, la reprise sur incident….



Why great care and consideration should be taken when selecting the proper password

Annexe : Description du laboratoire GSB

Le secteur d'activité

L'industrie pharmaceutique est un secteur très lucratif dans lequel le mouvement de fusion acquisition est très fort. Les regroupements de laboratoires ces dernières années ont donné naissance à des entités gigantesques au sein desquelles le travail est longtemps resté organisé selon les anciennes structures.

Des déboires divers récents autour de médicaments ou molécules ayant entraîné des complications médicales ont fait s'élever des voix contre une partie de l'activité des laboratoires : la visite médicale, réputée être le lieu d'arrangements entre l'industrie et les praticiens, et tout du moins un terrain d'influence opaque.

L'entreprise

Le laboratoire Galaxy Swiss Bourdin (GSB) est issu de la fusion entre le géant américain Galaxy (spécialisé dans le secteur des maladies virales dont le SIDA et les hépatites) et le conglomérat européen Swiss Bourdin (travaillant sur des médicaments plus conventionnels), lui même déjà union de trois petits laboratoires .

En 2009, les deux géants pharmaceutiques ont uni leurs forces pour créer un leader de ce secteur industriel. L'entité Galaxy Swiss Bourdin Europe a établi son siège administratif à Paris.

Le siège social de la multinationale est situé à Philadelphie, Pennsylvanie, aux Etats-Unis.

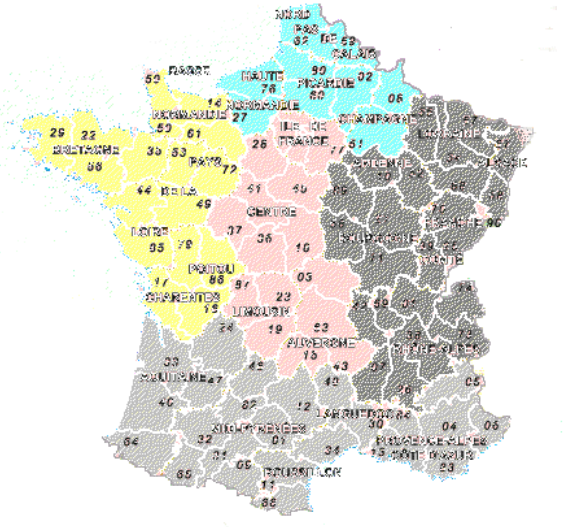
La France a été choisie comme témoin pour l'amélioration du suivi de l'activité de visite.

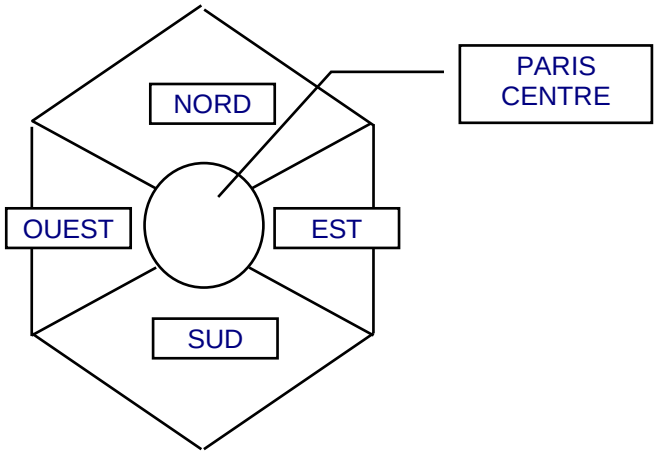
Réorganisation

Une conséquence de cette fusion, est la recherche d'une optimisation de l'activité du groupe ainsi constitué en réalisant des économies d'échelle dans la production et la distribution des médicaments (en passant par une nécessaire restructuration et vague de licenciement), tout en prenant le meilleur des deux laboratoires sur les produits concurrents.

L'entreprise compte 480 visiteurs médicaux en France métropolitaine (Corse comprise), et 60 dans les départements et territoires d'outre-mer. Les territoires sont répartis en 6 secteurs géographiques (Paris-Centre, Sud, Nord, Ouest, Est, DTOM Caraïbes-Amériques, DTOM Asie-Afrique).

Une vision partielle de cette organisation est présentée ci-dessous.





Après deux années de réorganisations internes, tant au niveau du personnel que du fonctionnement administratif, l'entreprise GSB souhaite moderniser l'activité de visite médicale.

Description du Système Informatique

Le système informatique
Sur le site parisien, toutes les fonctions administratives (gestion des ressources humaines, comptabilité, direction, commerciale, etc.) sont présentes. On trouve en outre un service *labo-recherche*, le service juridique et le service communication.

La salle serveur occupe le 6ème étage du bâtiment et les accès y sont restreints (étage accessible par ascenseur à l'aide d'une clé sécurisée, portes d'accès par escalier munies d'un lecteur de badge, sas d'entrée avec gardien présent 24h/24).

Les serveurs assurent les fonctions de base du réseau (DHCP, DNS, Annuaire et gestion centralisée des environnements) et les fonctions de communication (Intranet, Messagerie, Agenda partagé, etc.).
On trouve aussi de nombreuses applications métier (base d'information pharmaceutique, serveurs dédiés à la recherche, base de données des produits du laboratoire, base de données des licences d'exploitation pharmaceutique, etc.) et les fonctions plus génériques de toute entreprise (Progiciel de Gestion Intégré avec ses modules RH, GRC, etc.).
Un nombre croissant de serveurs est virtualisé.

Constitué autour de VLAN, le réseau segmente les services de manière à fluidifier le trafic.

Les données de l'entreprises sont considérées comme stratégiques et ne peuvent tolérer ni fuite, ni destruction. L'ensemble des informations est répliqué quotidiennement aux Etats-Unis par un lien dédié. Toutes les fonctions de redondances (RAID, alimentation, lien réseau redondant, Spanning-tree, clustering, etc.) sont mises en œuvre pour assurer une tolérance aux pannes maximale.

La gestion informatique
La DSI (Direction des Services Informatiques) est une entité importante de la structure Europe qui participe aux choix stratégiques.
Pour Swiss-Bourdin, qui occupait le siège parisien avant la fusion, l'outil informatique et l'utilisation d'outils décisionnels pour améliorer la vision et la planification de l'activité ont toujours fait partie de la politique maison, en particulier pour ce qui concerne la partie recherche, production, communication et juridique.
La partie commerciale a été le parent pauvre de cette informatisation, les visiteurs étant vus comme des acteurs distants autonomes. La DSI a convaincu l'entreprise que l'intégration des données fournies par cette partie aura un impact important sur l'ensemble de l'activité.

L'équipement
L'informatique est fortement répandue sur le site. Chaque employé est équipé d'un poste fixe relié au système central. On dénombre ainsi plus de 350 équipements terminaux et

On trouve aussi des stations de travail plus puissantes dans la partie *labo-recherche*, et une multitude d'ordinateurs portables (personnels de direction, service informatique, services commerciaux, etc).

Les visiteurs médicaux reçoivent une indemnité bisannuelle pour s'équiper en informatique (politique Swiss-Bourdin) ou une dotation en équipement (politique Galaxy). Il n'y a pas à l'heure actuelle d'uniformisation des machines ni du mode de fonctionnement

Chaque employé de l'entreprise a une adresse de messagerie de la forme *nomUtilisateur@swiss-galaxy.com*. Les anciennes adresses de chaque laboratoire ont été définitivement fermées au 1er janvier 2018.

"On se goinfre de progrès.
En une minute, on peut appeler Bogota.
Mais on ne sait qui appeler ni quoi dire."
Jean-Luc Godard

Salle serveur et connexion internet

Les serveurs sont virtualisés.

Le réseau assure un fonctionnement de niveau 3. À ce titre, un routage inter-vlan est réalisé en limitant les communications grâce à des listes de contrôles d'accès (ACL).

Le serveur de messagerie et l'intranet sont limités à un usage interne au site parisien. Des services externalisés (relais de messagerie auprès de l'opérateur et recopie d'une partie du serveur intranet sur le serveur Web hébergé chez un prestataire) permettent aux visiteurs médicaux d'utiliser la messagerie de l'entreprise et d'avoir accès aux principales informations de l'intranet (Comité d'entreprise, circulaires importantes, stratégie de l'entreprise, comptes rendus de CA, etc.).

" La vertu d'un homme ne doit pas se mesurer par ses efforts, mais par ce qu'il fait d'ordinaire. "
Blaise Pascal ; Les pensées (1670)

Domaine d'étude

L'entreprise souhaite porter une attention nouvelle à sa force commerciale dans un double objectif : obtenir une vision plus régulière et efficace de l'activité menée sur le terrain auprès des praticiens, mais aussi redonner confiance aux équipes malmenées par les fusions récentes.

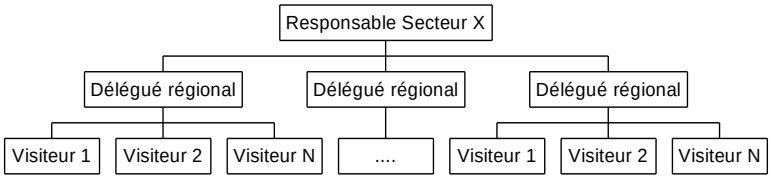
Les visiteurs
La force commerciale d'un laboratoire pharmaceutique est assurée par un travail de conseil et d'information auprès des prescripteurs. Les visiteurs médicaux (ou délégués) démarchent les médecins, pharmaciens, infirmières et autres métiers de santé susceptibles de prescrire aux patients les produits du laboratoire.

L'objectif d'une visite est d'actualiser et rafraîchir la connaissance des professionnels de santé sur les produits de l'entreprise. Les visiteurs ne font pas de vente, mais leurs interventions ont un impact certain sur la prescription de la pharmacopée du laboratoire.

Pour donner une organisation commune aux délégués médicaux, l'entreprise a adopté l'organisation de la flotte de visiteurs existant chez Galaxy, selon un système hiérarchique par région et, à un niveau supérieur, par secteur géographique (Sud, Nord, Paris-Centre, etc).

Il n'y a pas eu d'harmonisation de la relation entre les personnels de terrain (Visiteurs et Délégués régionaux) et les responsables de secteur. Les habitudes en cours avant la fusion ont été adaptées sans que soient données des directives au niveau local.

Hiérarchie par Secteur



On souhaite améliorer le contact entre ces acteurs mobiles autonomes et les différents services du siège parisien de l'entité Europe. Il s'agit d'uniformiser la gestion du suivi des visites.

Les visiteurs et les autres services
Les déplacements et actions de terrain menées par les visiteurs engendrent des frais qui doivent être pris en charge par la comptabilité. On cherche à agir au plus juste de manière à limiter les excès sans pour autant diminuer les frais de représentation qui font partie de l'image de marque d'un laboratoire.

Responsabilités

Les **équipes du service développement** auront notamment à produire puis à fournir les éléments applicatifs permettant :

- l'enregistrement d'informations en provenance des visiteurs
- la gestion des frais de déplacement

Les **équipes du service Réseau et système** fourniront les équipements et configuration réseau, ainsi que les ressources serveur nécessaires à héberger les applications mises à disposition de la flotte visite.