



DIRECT IT
CONNECTING PEOPLE



CAS H1



ÉCOLE SUPÉRIEURE
DE L'ALTERNANCE



GMSI REGION 2019

ROBILLARD REMY, BERNA JEROME, DROUHARD LEONEL

DIRECT IT | 7, AVENUE ROBERT SCHUMAN 51100 REIMS

SOMMAIRE

TABLE DES MATIERES

I.	PRESENTATION DU PROJET PEDAGOGIQUE.....	4
A.	REFERENTIEL D'ACTIVITES ET DE COMPETENCES.....	4
B.	OBJECTIFS PEDAGOGIQUES.....	4
II.	INTRODUCTION	5
A.	PRESENTATION DE L'ENTREPRISE.....	5
B.	NOS PARTENAIRES	5
C.	ORGANIGRAMME	6
D.	NOTRE PRODUIT.....	7
III.	BESOINS.....	8
A.	CONTEXTE	8
B.	SITUATION ACTUELLE.....	8
C.	MATERIELS	9
D.	LOGICIELS	11
E.	ENVIRONNEMENT	11
F.	PERTES ECONOMIQUES.....	11
IV.	ANALYSES FONCTIONNELLES.....	13
A.	PRESENTATION.....	13
B.	ANALYSE FONCTIONNELLE MATERIEL.....	14
C.	ANALYSE FONCTIONNELLE LOGICIEL.....	15
D.	ANALYSE FONCTIONNELLE SUPPORT	16
E.	ANALYSE FONCTIONNELLE COMMUNICATION.....	18
F.	ANALYSE FONCTIONNELLE SECURITE.....	18
V.	CONTRAINTES.....	19
A.	CONTRAINTES TECHNIQUES.....	19
B.	CONTRAINTES HUMAINES	19
C.	CONTRAINTES ECONOMIQUES.....	19
D.	CONTRAINTES ECOLOGIQUES.....	19
	SUITES / EVOLUTIONS POSSIBLE.....	20
	ACTEURS IMPACTES	20

VI.	CADRE DE REPONSES	21
VII.	CONCLUSION	24
A.	CONCLUSION INDIVIDUELLES.....	24
	JEROME	24
	LEONEL	24
	REMY.....	24
I.	GESTION DE PROJET	26
II.	ANALYSE FONCTIONNELLE	27
A.	MATERIEL	27
B.	LOGICIEL	30
C.	SUPPORT	33
D.	COMMUNICATION.....	37
E.	SECURITE.....	40
III.	GLOSSAIRE	44
IV.	WEBOGRAPHIE	44

REMERCIEMENTS

Nous souhaitons adresser tous nos remerciements aux personnes qui nous ont aidé dans l'élaboration de ce projet.

Principalement les intervenants du CESI de Reims qui ont su nous transmettre leurs savoirs et nous aiguiller dans la réalisation de ce rapport.

Nous remercions aussi notre pilote de formation M. Éric POLFER pour le suivi et l'attention portée à notre apprentissage.

I. PRESENTATION DU PROJET PEDAGOGIQUE

A. REFERENTIEL D' ACTIVITES ET DE COMPETENCES

L'étude du Cas H1 vise à :

- Assurer la maintenance du parc informatique de l'Entreprise
- Assurer le support technique auprès des utilisateurs de l'Entreprise
- Participer à l'évolution du parc informatique

B. OBJECTIFS PEDAGOGIQUES

La Direction Générale souhaite mettre en place une organisation humaine et technique permettant d'anticiper au mieux l'évolution du Service d'Information, que ce soit en termes d'exploitation au quotidien que de stratégies d'investissement.

Ainsi, la société Direct-IT cherche des solutions visant à :

- Rationaliser les processus et mettre en œuvre les meilleures pratiques et outils
- Assurer une continuité de service
- Réaliser une gestion des contrats de maintenance
- Améliorer le niveau de satisfaction des utilisateurs
- S'inscrire dans une démarche de respect environnemental

II. INTRODUCTION

C. PRESENTATION DE L'ENTREPRISE

Direct IT à vu le jour en 2015, pour offrir une solution française de clef 4G, jeune sur le marché du matériel informatique Direct IT a su se diversifier et a su donner l'accès à la 5G au grand public.

L'activité principale de l'entreprise repose sur deux produits, l'élaboration et la revente de clef 4G dans un format USB mais aussi dans l'accès internet notamment dans les zones blanches avec une borne fixe en partenariat avec Orange.

Après plusieurs années de recherches et développements Direct IT a mis au point une borne 5G qui sera intégré à tous les nouveaux models de Box Orange en cas de coupure réseau.

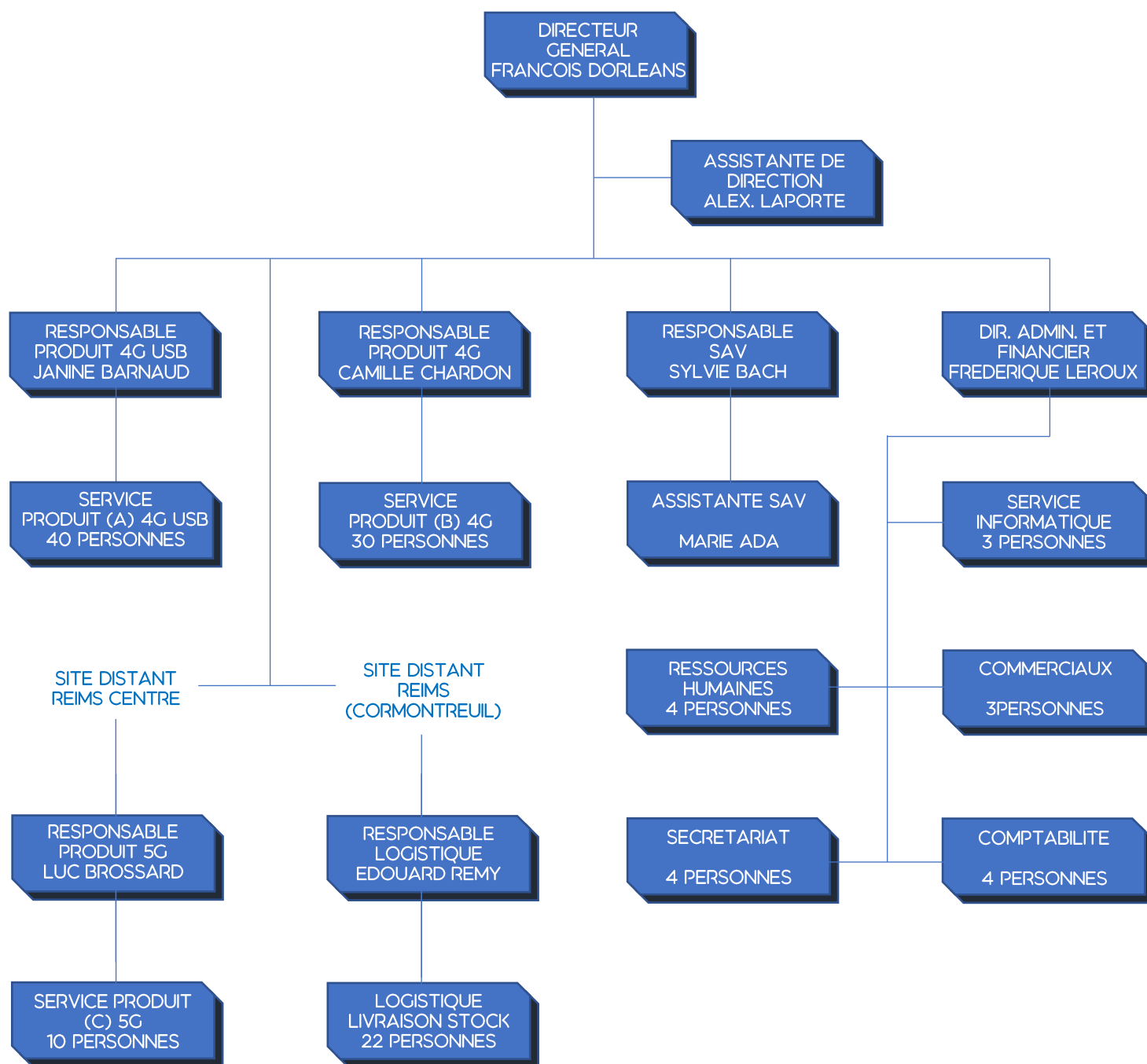


Notre société est consciente des enjeux environnementaux et s'engage à respecter un développement durable et prendre conscience de son impact environnemental.

D. NOS PARTENAIRES



C. ORGANIGRAMME



D. NOTRE PRODUIT

Notre entreprise propose des clefs 3G, 3G+ ainsi que 4G et bientôt 5G sur notre site internet d'e-commerce.

Une clé 4G fonctionne comme une clé USB, une fois branché à l'appareil souhaité, elle fonctionne comme un mini modem.

Nos clé 4G respecte les normes LTE, nos clé 3G et 3G+ sont aux normes UMTS et HSDPA.

Nos clefs sont conçues en partenariat avec la société Orange. Elles sont conçues pour être résistante, élégante et performante grâce aux réseaux 4G de notre partenaire Orange.



III. BESOINS

A. CONTEXTE

Après plusieurs années de très forte croissance, la société Direct-IT doit maintenant répondre à différents enjeux concernant son système d'information afin de maîtriser son évolution au travers d'un schéma directeur informatique.

Ces enjeux sont de différents ordres :

Financiers (poursuivre la croissance de l'entreprise), organisationnels et technologiques (assurer la continuité de l'activité) et environnementaux.

B. SITUATION ACTUELLE

Après un premier état des lieux, les constats faits par le Chef de Projet sont les suivants :

- L'inventaire du parc révèle une très forte hétérogénéité des équipements (postes de travail, smartphones, serveurs et équipements réseau) tant au niveau matériel que logiciel : types d'équipements, constructeurs, durée d'utilisation.
- Pas de plan de continuité d'activité ou de plan de continuité informatique
- Pas de plan de maintenance matérielle et/ou logicielle et subit donc de fortes pertes d'exploitations.
- Pas de gestion des contrats de maintenance et/ou gestion des garanties
- Aucune gestion des incidents ni suivi, pas de base de connaissance
- Les matériels informatiques sont régulièrement défectueux (surcharge de mémoire, arrêt des serveurs pour donner suite à une trop forte activité, surchauffe, poussière dans les PC, etc...). Le temps estimé de ses défaillances est de 1 heure pour les serveurs, et 4 heures pour l'ensemble des postes de travail par semaine (perte estimée à 80 000€/an)
- La société est en infraction avec les normes environnementales D3E
 - Aucune stratégie de gestion de la fin de vie des équipements
 - Aucune stratégie de sélection de fournisseurs orientés développement durable

C. MATERIELS

Notre principal problème concernant le matériel actuellement présent au sein de notre entreprise est que notre matériel est vieillissant, peu performant et également très hétérogène. Ce qui nous posent beaucoup de problème en termes de maintenance et de garantie. Nous allons donc vous présenter notre parc informatique actuel qui comprend les unités centrales, les ordinateurs portable, les smartphones, l'équipement réseaux ainsi que les imprimantes.

PARC INFORMATIQUE ACTUEL

Concernant les **ordinateurs de bureau**, actuellement notre parc informatique est composé de :

Modèle	Processeur	RAM	Disque Dur	OS	Quantité
Acer Aspire M1201-14 One Box	AMD Athlon 64x2 4450E	2Go DDR2	320Go	Vista	10
Acer Aspire M1641-17 One Box	Intel Pentium Dual-Core E2200	3Go DDR2	160Go	Seven	10
Dell Optiplex 790 SFF	Core i3-2120	4Go DDR3	250Go	Windows 8	30
Asus CP3130-FR002O	I3-2120	4Go DDR3	1To	Seven	10
Acer Aspire T150-SB7Z	AMD Sempron 3300+	2Go DDR2	200Go	XP	30

Les **smartphones** présents au sein de l'entreprise actuellement :

Modèle	OS	Quantité
iPhone 5	iOS 8.1.1	2
Samsung S4	Android 4.2.2	3
Huawei P7 Lite	Android 5.1	2
Windows Phone 8	Windows Phone 7.0	3

Les ordinateurs portables :

Modèle	Processeur	RAM	Disque Dur	OS	Quantité
Acer Aspire 3 A315	I3-6006U	4Go DDR3	1To	Windows 8	3
Acer Aspire 1 A114-31-C27V	Intel Celeron N3350	4Go DDR3	64Go	Windows 7	2
Acer Aspire 1 A114-32-C641	Intel Celeron N4000	4Go DDR3	64Go	Windows Vista	5

Et pour finir voici notre **équipement réseau** actuellement :

Modèle	Type	Quantité
Dell PowerEdge T320	Serveur	2
Nilox Easy 1040	Onduleur	2
Buffalo BS-GS2008P	Switch	10
SophosAppliance XG210	Firewall	1

Nous allons finir par les **imprimantes** :

Modèle	Marque	Type	Nombre	Date d'achat
Canon IP2600	Canon	Jet d'encre	3	2008
HP Envy 4520	HP	Jet d'encre	3	2011
Brother DCP1610W	Brother	Laser	2	2012
Canon IP2500	Canon	Jet d'encre	2	2007
HP Envy 4525	HP	Jet d'encre	3	2010

Nous avons également des écrans, des claviers et des souris. Nous n'avons pas jugé nécessaire de détailler nos périphériques reliés à l'unité central car il ne sera pas utile de les remplacer.

D. LOGICIELS

Concernant la partie logiciel, le principal problème que rencontre nos techniciens est qu'il n'y a aucune gestion des licences, ainsi ils perdent beaucoup de temps à remettre en place les licences expirées ou à essayer de contacter les différents supports logiciels.

Actuellement, il faut savoir qu'il y a également beaucoup de système d'exploitation différents au sein de l'entreprise, que ce soit au niveau des unités centrales ou des smartphones.

Ce qui ne permet pas une réelle centralisation des postes et des licences qui faciliterait grandement le déploiement de logiciels ainsi que de leurs licences.

Nous avons 4 systèmes d'exploitation différents au sein de notre parc informatique :

- Windows XP
- Windows Vista
- Windows Seven
- Windows 8

Concernant les smartphones nous avons 3 systèmes d'exploitation différents :

- iOS (8.1.1)
- Android (MAJ 4.2.2 et 5.1)
- Windows Phone (7.0)

E. ENVIRONNEMENT

La société étant actuellement en infraction avec la loi vis-à-vis des nouvelles normes environnementales D3E (Déchet d'équipements électriques et électroniques), il nous faut donc régler le problème très rapidement car l'entreprise s'expose actuellement à de lourdes amendes.

F. PERTES ECONOMIQUES

- Comme nous pouvons le constater le parc informatique est très hétérogène (ordinateurs, smartphones, équipement réseau, ...) et cause des soucis en termes de maintenance et en coût des pièces détachées. Le coût s'élève donc à 15 000€ par an uniquement en pièce détachées.
- L'entreprise a également aucune politique concernant la maintenance et subit donc de forte perte d'exploitation à ce niveau.

- Après une panne de matériel informatique et un appel fournisseur, celui-ci n'était plus sous garantie ni sous contrat de maintenance. Nous avons dû payer l'intervention, les pièces en panne, et surtout attendre 4 jours sans utiliser ce matériel (perte d'exploitation évaluée à **10 000€**)
- Comme dit précédemment, le matériel informatique étant vétuste, il est donc régulièrement défaillant (problèmes de mémoires, arrêt des serveurs à la suite d'une trop forte activité, surchauffe, poussière, etc...). Le temps estimé pour ses défaillances est de 1 heure pour les serveurs et 4 heures pour l'ensemble des postes de travail par semaine, la perte estimée est de **80 000€** par année.
- Le service informatique effectue en moyenne 20 interventions par semaine. Mais il faut savoir que la mauvaise gestion des incidents entraîne un retard du temps de dépannage qui équivaut à 2h par semaine. Cela génère donc une perte d'environ **7 500€** par année.
- La société est également en infraction vis-à-vis des normes environnementales D3E. L'entreprise s'expose donc à des amendes équivalentes à 450 € par déchets électriques et électroniques négligés.
- Les techniciens doivent également gérer les licences logiciel (Licences expirées, support logiciel, etc...). Les techniciens passent donc en moyenne 2 heures par semaine à gérer les problèmes logiciels, le coût estimé est d'environ **10 000€** par année.
- Nous pouvons également constater que les systèmes d'exploitation utilisés sur les ordinateurs et sur les smartphones sont différents. Cela engendre des problèmes au niveau de la maintenance des logiciels (compatibilité, etc...). Les techniciens doivent donc résoudre les problèmes de compatibilité, le coût estimé pour ses interventions est de **12 000€** par année.

Récapitulatif des pertes de la société par an :

- 80 000 € Arrêts de production
- 10 000 € Problèmes de Garanties
- 7500 € Temps de dépannage
- 450 € D3E par infractions
- 10 000 € Compatibilité
- 15 000 € Parc hétérogène

Minimum de 122 950 € de perte annuelle pour la société

Une base pour faire une proposition de solutions sur le retour d'investissement des sommes investies (ROI).

IV. ANALYSES FONCTIONNELLES

A. PRESENTATION

L'analyse fonctionnelle permet d'optimiser la conception d'un « produit » en s'appuyant sur les différentes fonctions de ce « produit ». Grâce à cela, nous pouvons déterminer les besoins pour en faire un document qui permettra d'avoir une ligne directrice.

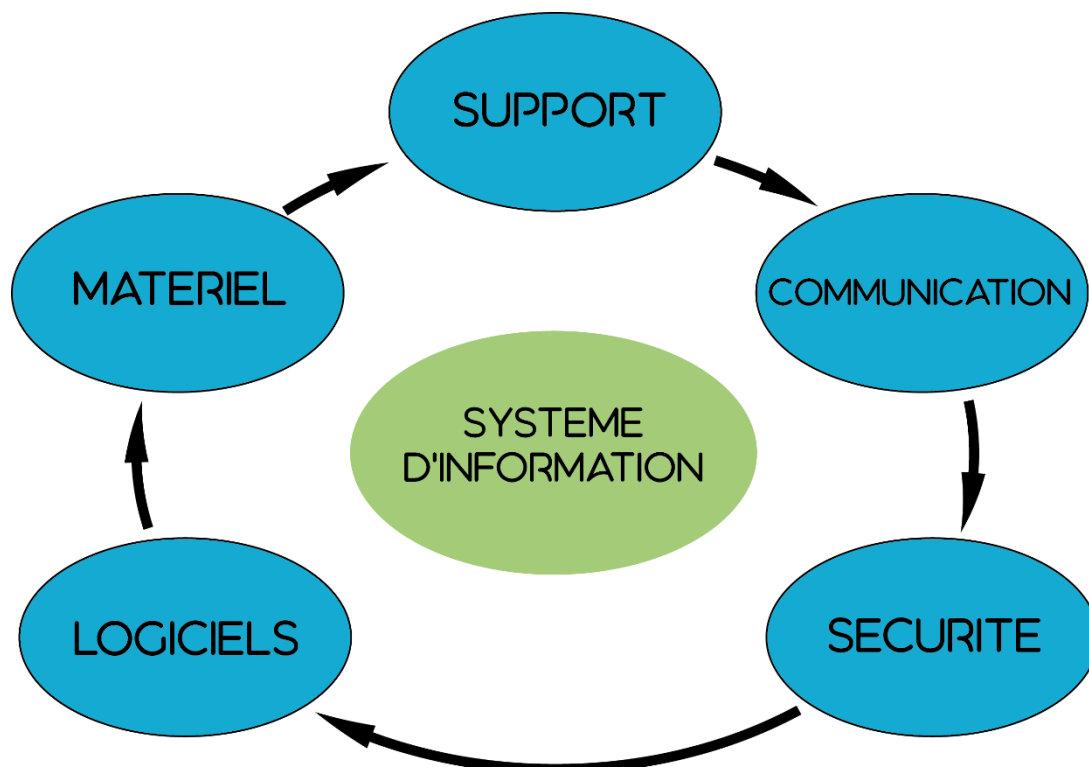
C'est La méthode APTE (**A**pplication aux **T**echniques d'**E**ntreprise)

Ici, en l'occurrence, notre « produit » est notre système d'information.

Concernant notre analyse fonctionnelle nous avons fonctionné de la manière suivante :

Nous avons fait une analyse fonctionnelle de notre système d'information complet, que nous avons ensuite découpé en 5 parties : **Support, communication, sécurité, logiciels, matériel**.

Chacune de ses sous-catégories a été représenté en diagramme pieuvre, nous en avons tiré différentes fonctions principales et différentes contraintes de chacune d'entre elles.



Grâce à notre analyse fonctionnelle nous avons pu mettre en évidence les différents problèmes qu'il y a actuellement au sein de notre système d'information.

Nous allons maintenant vous présenter les différentes sous-catégories de notre système d'information.

Le détail de chacune de ses sous-catégories (réalisation des diagrammes pieuvres, fonctions principales et contraintes) est disponible en annexes.

B. ANALYSE FONCTIONNELLE MATERIEL

Nous avons donc commencé nos analyses fonctionnelles par la partie qui concerne le matériel.

Grâce à l'analyse fonctionnelle concernant la partie matérielle nous en avons déduit qu'il y avait beaucoup de problème notamment des problèmes touchant la vétusté de nos équipements (surtout concernant les unités centrales ainsi que les smartphones).

Il y a également des problèmes d'homogénéité du parc tant au niveau des unités centrales, des smartphones, mais aussi des équipements réseaux et des serveurs eux-mêmes.

L'administrateur doit pouvoir avoir accès à une base de connaissances qui regroupe les procédures/tutoriels	Mise à jour de la base de connaissance	procédure pour chaque pratique ou materiel différent
		mise a jour et suivi des procedures
Permettre à l'utilisateur de réaliser le travail demander	matériel adapté en fonction de l'utilisateur	matériel adapté / ergonomique (trouble musculosqueletique)
	puissance des ordinateurs en fonction des logiciels metiers	configuration du materiel
le matériel doit etre recyclé par un organisme agréé par la D3E	vente du materiel	dons a des associations
	Organisme de recyclage	politique de reprise ou de vente
Nous devrions contacter uniquement des fournisseurs qui respectent les normes de sécurité et environnementale	Fournisseurs dans le norme D3E	Fournisseurs officiel / respect des normes
Le matériel devra être stocké dans une pièce approprié, et un inventaire devra être mis en place	pièce adapté	type de solution
	inventaire	Solution d'inventorisme
Certains des utilisateurs au sein de l'entreprise sont itinérant, il faudra donc palier à cette contrainte par l'achat de matériels itinérant (Smartphones, PC portable)	Matériel spécifique	Matériel déplaçable
Le matériel se devra d'être garantie	Vérification garantie	Garantie sur 5 ans

C. ANALYSE FONCTIONNELLE LOGICIEL

Concernant la partie logicielle, nous nous sommes rendu compte qu'il y avait beaucoup de problème de compatibilité (beaucoup de logiciels de différents concepteurs, différent système d'exploitation) ainsi que des problèmes de licences qui occupe donc souvent nos techniciens en informatique.

L'utilisateur doit disposer des licences valide pour pouvoir utiliser les différents logiciels (si nécessaire) dont il aura besoin.	Achat de licences	prix des licences
L'utilisateur doit avoir accès à une base de connaissances concernant l'utilisation de certains logiciels (procédures, tutoriels, etc...)	Accès base de connaissances par les utilisateurs	technique materiel
		Logiciels
L'administrateur doit avoir accès à des logiciels de gestion de parc informatique ou d'autres outils qui permettront à l'ensemble de l'entreprise de pouvoir continuer de produire	Logiciels de gestion	solution de gestion a distance
		solution de Gestion de parc informatique grâce aux logiciels
Pour faire fonctionner les logiciels il nous faudra obligatoirement avoir accès à un matériel pouvant supporter la charge du logiciel (que ce soit sur ordinateur ou smartphone).	Anticipation des besoins future	Le matériel doit être compatible
Il nous faudra obligatoirement une source d'énergie pour pouvoir faire fonctionner le matériel nécessaire à l'utilisation des logiciels	Energie	respect des normes nfc 15-100
		solution en cas de coupure
		Besoin en électricité
Les logiciels se devront d'être compatible avec le matériel ainsi qu'avec le système d'exploitation utilisé dans l'entreprise	Compatibilité	coût
		Logiciels, système d'exploitation et composants compatible

D. ANALYSE FONCTIONNELLE SUPPORT

Le support informatique étant très important au sein d'une entreprise, nous nous devons de faire une analyse fonctionnelle de notre support informatique.

En ayant effectué cette analyse fonctionnelle, nous nous sommes aperçus de tous les problèmes que peut rencontrer celui-ci. Manque d'optimisation du temps ainsi qu'une mauvaise gestion des contrats de maintenance. Aujourd'hui nous ne pouvons-nous permettre de telles pertes d'exploitations voilà pourquoi nous nous tournons vers une solution extérieure à la suite de l'analyse de notre Système d'information.

Utilisation de l'outil de gestion de parc des incidents pour les utilisateurs	Création des demandes	nombres de demandes par utilisateurs
	vérification de l'état de la demande	modification
		instantané
	information à la résolution de la demande	instantané
	reprise d'un incident passé	instantané
	fermeture de l'incident	instantané
l'Administrateur doit pouvoir administrer l'outil de gestion et prioriser les demandes clôturer	Satisfaction utilisateur	critères d'évaluation
	administration de l'outil	Contrôle total
	priorisation des demandes / clotures	Contrôle total
l'Administrateur peut consulter, créer et modifier les procédures dans une base de données interne à l'entreprise	affectation des tâches au tech	Contrôle total
	consultation	Contrôle total
	modification	Contrôle total
	espace disponible	modulable
l'utilisateur doit avoir accès aux procédures de dépannage en consultation	création	Contrôle total
	consultation	consultation uniquement

l'Administrateur doit avoir accès à toutes les statistiques de l'outil de gestion, les anciens incidents ainsi que les demandes non traitées et les avis utilisateurs	statistiques de satisfactions	par incidents
		globale
	exportation de statistiques	excel
	référencement des anciens incidents	base de données
Tous les incidents traités sont répertoriés dans une base de données automatiquement	gestion d'une base de données	base de données consultable
	automatisation des tâches	statistiques
		automatisation
Chaque utilisateur doit disposer d'un poste fonctionnel avec des logiciels métiers adaptés	déploiement de poste et logiciels en fonction de l'utilisateur	poste utilisable dès la première utilisation
L'administrateur doit pouvoir prendre la main sur tous les postes et logiciels de l'entreprise pour la résolution des incidents	vision sur les problèmes de l'utilisateur	en direct
	Résolution des incidents	en direct
		ressources humaines
L'administrateur doit informer l'utilisateur des bonnes pratiques à employer	réalisation de procédures	ressources humaines
	informations sur les bonnes pratiques	ressources humaines
L'utilisateur doit respecter les bonnes pratiques de l'entreprise	type de solution	type de solution
Les utilisateurs doivent être formés pour créer une demande ainsi que l'assistance pour le dépannage	formation des utilisateurs	temps par utilisateur
		coût
devoir de confidentialité	type de solution	type de solution
Prévention des défaillances	type de solution	type de solution
délais de résolution des incidents	reprise de production	délais d'intervention incident grave
		délais d'intervention incident moyen
		délais d'intervention incident léger
	respect des GTR	délais maximal

E. ANALYSE FONCTIONNELLE COMMUNICATION

Nous avons également décidé de faire une analyse de la partie communication de notre système d'information, il regroupe notre publicité ainsi que notre site internet et notre intranet qui n'est plus mis à jour.

Cela regroupe également toute la communication entre les employés via les différents logiciels mis en place ainsi que la téléphonie.

Nous avons mis en avant dans le cahier des charges une veille stratégique pour nous permettre de gagner une avance certaine face à la concurrence en restant à l'écoute des nouvelles technologies ainsi qu'au prises de position de nos concurrents direct en matière de technologie.

En vue d'expansion future, il nous paraît important de trouver un prestataire qui pourra s'occuper de l'anticipation de nos besoins et s'assurer ainsi que de nous orienter vers les bons virages technologiques.

Permet à l'administrateur de faire de la veille stratégique	Permet à l'administrateur de faire de la veille stratégique	Permet à l'administrateur de faire de la veille stratégique
Permet à l'administrateur d'anticiper les besoins	Vérifie l'existant avec les besoins des charges futures	suivi et veille techno
avoir un ordinateur (portable si itinérance)	ordinateur interconnecté	connectivité et autonomie
avoir un telephone (smartphone si itinérance)	telephone dect et smartphone connecter au reseau d'entreprise	compatibilité et connectivité

F. ANALYSE FONCTIONNELLE SECURITE

Présentons maintenant notre dernier diagramme pieuvre qui illustre notre système de sécurité. Notre système de sécurité regroupe donc la cybersécurité ainsi que la sécurité physique.

Nous avons décidé de regrouper également la notion de sauvegarde et de redondance de nos données au sein de ce système.

les administrateurs doivent avoir accès aux statistiques du système de sécurité	vérification du trafic du SI	Vision totale
	modification mots de passe	Contrôle totale
les utilisateurs doivent respecter les bonnes conduites	dans la saisie, l'accès et utilisation des données	type de solution

V. CONTRAINTES

A. CONTRAINTES TECHNIQUES

- Le nouveau parc informatique se devra d'être homogène
- Fournir des équipements capables de supporter et faire fonctionner les différents logiciels
- Validités des licences logiciels
- Déploiement de l'outil de maintenance sur les postes utilisateurs pour gérer les différents incidents

B. CONTRAINTES HUMAINES

- Formations nécessaires pour les techniciens ainsi que les utilisateurs sur les nouveaux systèmes d'exploitation
- Formations nécessaires pour les techniciens ainsi que les utilisateurs sur le nouveau matériel et les nouveaux logiciels
- Satisfaction des utilisateurs : Les utilisateurs devront être satisfait du nouveau système et du nouveau parc mis en place

C. CONTRAINTES ECONOMIQUES

- Evaluation des coûts concernant les prestations
- Evaluation des coûts Humain
- Respect du budget
- Essayer de ne pas gêner la production durant la mise en place du nouveau parc informatique et de son système

D. CONTRAINTES ECOLOGIQUES

- Respecter les normes D3E (Déchets d'Equipements Electriques et Electroniques)
- Respect des normes environnementales ISO 14000

SUITES / EVOLUTIONS POSSIBLE

Concernant l'évolution du parc informatique nous souhaitons passer sur un équipement de nouvelle génération concernant l'ensemble de notre parc informatique. Cela nous permettra de produire plus rapidement et plus sereinement qu'actuellement.

Il y a encore beaucoup de problèmes de compatibilité avec les nouveaux logiciels mis en place dû à la vétusté de notre parc informatique, cela cause donc beaucoup de problèmes de latences ainsi que de crash des postes informatiques mis en place pour les utilisateurs.

ACTEURS IMPACTES

Concernant les acteurs impactés, tout d'abord, il y aura évidemment le Service Informatique de notre entreprise (3 personnes), qui aura pour charge de rédiger le cahier des charges et qui devra également le superviser. La Direction Administrative et Financière jouera un rôle de décisionnaire concernant le cahier des charges.

Ensuite, concernant les acteurs extérieurs à l'entreprise il y aura tout d'abord le(s) prestataire(s) qui seront également impacté par notre projet. Ils auront également un rôle très important car ils devront respecter notre cahier des charges. Secondement, les fournisseurs, qui auront pour rôle d'approvisionner l'entreprise en matériel.

Dernièrement, les utilisateurs de notre entreprise (c'est-à-dire les employés) seront également impactés mais devront être le moins possible impactés par ces changements.

VI. CADRE DE REPONSES

Voici un le cadre de réponse de l'analyse fonctionnelle qui prend compte des besoins de notre entreprise.

Ce tableau reprend les fonctions, votre niveau sera évalué en fonction des réponses apportées au besoin de notre entreprise.

Un critère de priorité est attribué à chaque besoin et sera utilisé comme barème.

Fonctions	Fonction Principale	cadre de réponse
Comm.	Permet à l'administrateur de faire de la veille stratégique	
	Permet à l'administrateur d'anticiper les besoins	
	avoir un ordinateur (portable si itinérance)	
	avoir un telephone (smartphone si itinérance)	
Support	Utilisation de l'outils de gestion de parc des incidents pour les utilisateurs	
	l'Administrateur doit pouvoir administrer l'outils de gestion et prioriser les demandes cloturer	
	l'Administrateur peut consulter, créer et modifier les procédures dans une base de données interne à l'entreprise	
	l'utilisateur doit avoir accès aux procédures de dépannage en consultation	
	l'Administrateur doit avoir accès à toutes les statistiques de l'outils de gestion, les anciens incidents ainsi que les demandes non traitée et les avis utilisateurs	
	Tous les incidents traité sont répertorié dans une base de données automatiquement	
	Chaque utilisateur doit disposer d'un poste fonctionnel avec des logiciels métiers adaptés	
	L'administrateur doit pouvoir prendre la main sur tous les postes et logiciels de l'entreprise pour la résolutions des incidents	
	L'administrateur doit informer l'utilisateur des bonnes pratique a employer	
	L'utilisateur doit respecter les bonnes pratiques de l'entreprise	
	Les utilisateurs doivent être formé pour créer une demande ainsi que l'assistance pour le dépannage	
	devoir de confidentialité	
	Prévention des défaillances	
	délais de résolution des incidents	

Fonctions	Fonction Principale	Cadre de reponse
Sécurité	les administrateurs doivent avoir accès aux statistiques du système de sécurité	
	les utilisateurs doivent respecter les bonnes conduites	
Matériel	L'administrateur doit pouvoir avoir accès à une base de connaissances qui regroupe les procédures/tutoriels	
	Permettre à l'utilisateur de réaliser le travail demander	
	le matériel doit être recyclé par un organisme agréé par la D3E	
	Nous devrions contacter uniquement des fournisseurs qui respectent les normes de sécurité et environnementale	
	Le matériel devra être stocké dans une pièce approprié, et un inventaire devra être mis en place	
	Certains des utilisateurs au sein de l'entreprise sont itinérant, il faudra donc palier à cette contrainte par l'achat de matériels itinérant (Smartphones, PC portable)	
	Le matériel se devra d'être garantie	
Logiciel	L'utilisateur doit disposer des licences valide pour pouvoir utiliser les différents logiciels (si nécessaire) dont il aura besoin.	
	L'utilisateur doit avoir accès à une base de connaissances concernant l'utilisation de certains logiciels (procédures, tutoriels, etc...)	
	L'administrateur doit avoir accès à des logiciels de gestion de parc informatique ou d'autres outils qui permettront à l'ensemble de l'entreprise de pouvoir continuer de produire	
	Pour faire fonctionner les logiciels il nous faudra obligatoirement avoir accès à un matériel pouvant supporter la charge du logiciel (que ce soit sur ordinateur ou smartphone).	
	Il nous faudra obligatoirement une source d'énergie pour pouvoir faire fonctionner le matériel nécessaire à l'utilisation des logiciels	
	Les logiciels se devront d'être compatible avec le matériel ainsi qu'avec le système d'exploitation utilisé dans l'entreprise	

Tout soumissionnaire répondant à ce présent appel d'offre pourra faire appel à un sous-traitant mais devra nous présenter tous les documents suivant pour le suivi de son dossier pour son entreprise ainsi que pour le ou les sous-traitants sollicités :

Toutes les entreprises devront fournir :

- L'extrait Kbis qui devra comprendre :
 - ✓ Nom du greffe d'immatriculation
 - ✓ Raison sociale, sigle, enseigne
 - ✓ Numéro d'identification (anciennement numéro Siren) et code NAF
 - ✓ Forme juridique (SARL, SA, GIE, SCI...)
 - ✓ Montant du capital social

- ✓ Adresses du siège et du principal établissement, et des éventuels établissements secondaires en Union européenne ou dans l'Espace économique européen (EEE)
 - ✓ Durée de la société
 - ✓ Date de constitution
 - ✓ Activité détaillée
 - ✓ Nom de domaine du ou des sites internet de l'entreprise
 - ✓ Fonction, nom, prénom, date de naissance, commune de naissance, nationalité et adresse du dirigeant principal, des administrateurs et des commissaires aux comptes
 - ✓ Référence des autorisations obligatoires pour les professions réglementées.
-
- Un bilan financier
 - Les garanties et les assurances de l'entreprise
 - Les certifications obtenues par l'entreprise
 - Les prix ainsi qu'un devis détaillé
 - Les références passé de l'entreprise nous garantissant la maîtrise technique de votre entreprise
 - Une réponse complète au cahier des charges fonctionnelles
 - Un planning détaillé

Nous laissons la possibilité à tous les prestataires de nous proposer une solution annexe si celle-ci convient aux attentes de notre société.

Lors de la signature du contrat l'adjudicateur avec l'accord des soumissionnaires pourra allouer la réorganisation de son Système d'information en lots.

- Date pour le suivi du dossier et échéance des travaux
Les dossiers pourront être déposés à partir du 21/12/2019 jusqu'au 31/03/2020
Tous les travaux et changements dans le SI devront être effectifs le 01/08/2020
En cas de retard l'entreprise s'expose à des pénalités financières
- Les conditions et délais de règlement
A l'acceptation du contrat le prestataire s'engage à fournir tous les services auxquels il s'est engagé
Les frais seront payés par module en fonction des solutions apportées en suivant le devis préalable
- Référents
Pour toutes informations techniques vous pouvez contacter notre service informatique ainsi que Mme Laporte pour toutes les questions administratives.
- Accord de confidentialité devra être signé entre nos deux entreprises
- Closes de rupture
Si le prestataire manque à ses engagements dans les délais impartis il pourra s'en suivre une rupture de contrat
- Closes de renégociations
En cas d'apparition de nouvelles demandes lors de la prestation, des closes de renégociation pourront être ajoutées au contrat avec l'accord des deux parties.

VII. CONCLUSION

A. CONCLUSION INDIVIDUELLES

JEROME

Ce projet m'a permis de découvrir et de comprendre l'analyse fonctionnelle, les différents diagrammes nécessaires à sa conception ainsi qu'une nouvelle vision vis-à-vis d'un système d'information.

J'ai personnellement peu apprécié ce projet, mais il m'a permis d'apprendre de nouvelles choses et une nouvelle méthode de travail qui s'avère être plutôt efficace.

Il est cependant nécessaire de travailler sur un tel projet car il nous apporte une nouvelle vision globale du système d'information ainsi que des démarches à suivre pour améliorer un service informatique qui en a besoin.

LEONEL

Pour ce projet la prise en main et la compréhension conceptuel a demandé de l'adaptation qui généré une perte de temps dans le travail à fournir. Puis d'apporter une méthode efficace d'aborder les problématiques.

REMY

Ce projet est pour moi très important, il m'a permis d'avoir une vision d'ensemble de tout le Système d'information. L'analyse fonctionnelle et la réalisation de bête à corne nous permet de penser à tous les besoins et d'analyser un problème très précisément, sans avoir pour autant une expertise très poussée dans le domaine et de déterminer les fonctions principalement attendues. Ce projet nous confronte à la réalisation d'un appel d'offre ainsi qu'un cahier des charges fonctionnelles. Il nous a permis d'assimiler le diagramme de Kano, de décrypter les attentes implicites du client, d'analyser ses demandes et de voir comment répondre à ses attentes. Dans ce projet étant nous même du milieu informatique (société Direct-IT) nous avons choisi de détailler un maximum le cahier des charges fonctionnelles pour que l'entreprise garde le contrôle de son SI. Il est bien évident que de cette manière nous ne laissons pas forcément beaucoup de place à l'expertise du prestataire. Il est pour moi regrettable de ne pas avoir eu plus de temps pour enrichir ce projet par un cahier des besoins utilisateurs, un barème plus détaillé du cadre de réponse ou encore plus de précisions sur les closes de paiements, ruptures ou renégociations. Je remercie tous les intervenants qui nous ont accompagné durant l'élaboration du cas H1 et de nous avoir transmis leur expérience.

ANNEXE

I. GESTION DE PROJET

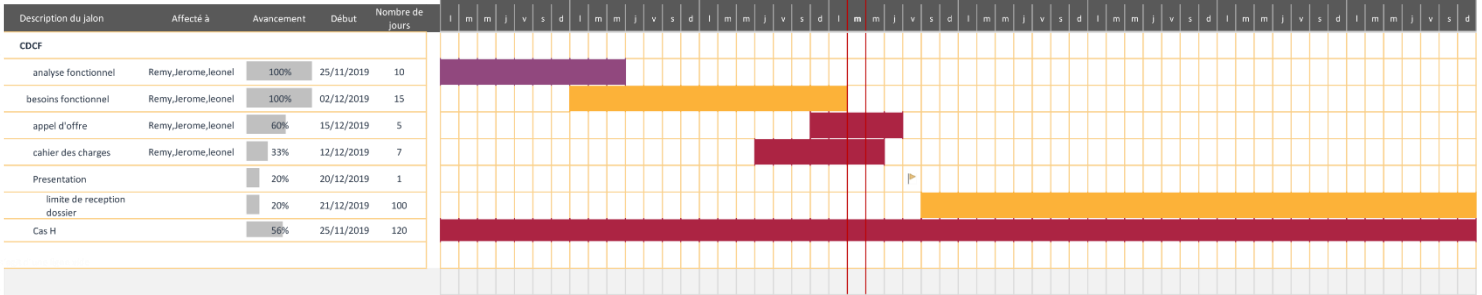
CAS H

Remy,Jerome,leonel



Date de début du projet : 25/11/2019

Incément de défilement : 0



Pour le suivi de notre projet nous avons mis en avant un travail d'équipe suivant la méthode RACI

- R : réalisateur
- A : approuvateur
- C : consulté
- I : informé

Qui nous a permis de découper les tâches par domaine de compétences dans l'équipe et nous avons répartis les différentes analyses fonctionnelles.

Avec la réalisation de plusieurs brainstormings nous avons défini les fonctions de notre Système d'information, déterminé notre besoin et réaliser un cahier des charges dans l'optique de diffuser un appel d'offre.

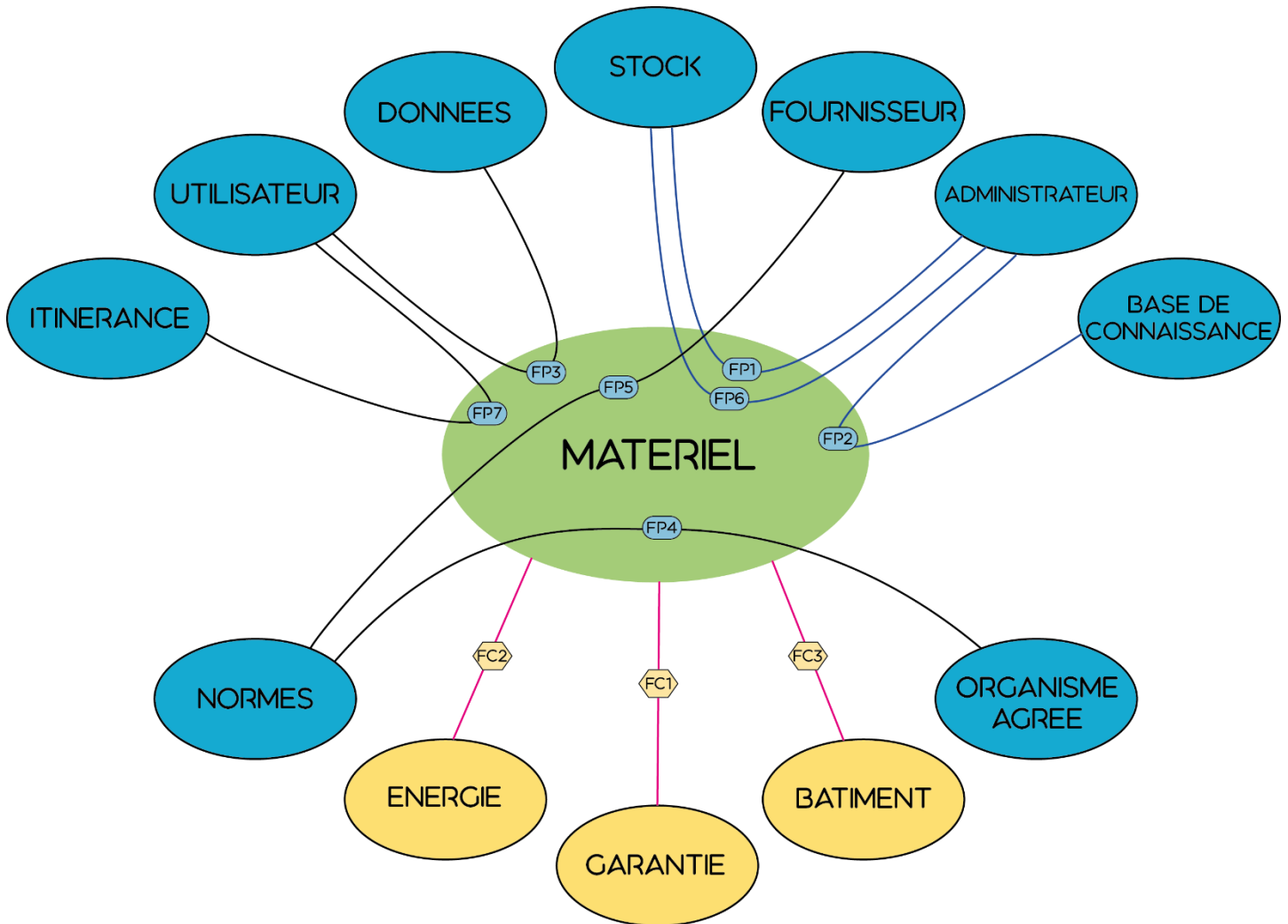
Pour le traitement des dossiers reçus nous devons tous les étudier de la même manière, pour ainsi les classer et les départager.

Nous allons organiser une réunion finale afin de traiter le suivi des demandes le 31/03/2020.

La décision définitive sera prise au plus tard le 13/04/2020

II. ANALYSE FONCTIONNELLE

G. MATERIEL



FP1 : Les administrateurs doivent pouvoir accéder au matériel pour l'installer

- Accessibilité du stock pour le service informatique autorisé
- Matériel libre de toute restriction d'utilisation pour l'administrateur

FP2 : L'administrateur doit pouvoir avoir accès à une base de connaissances qui regroupe les procédures/tutoriels, Mise à jour de la base de connaissance procédure pour chaque pratique ou matériel différent

- Administration de tutoriel pour les procédures et bons usages matériels

FP3 Permettre à l'utilisateur de réaliser le travail demander

- Matériel adapté en fonction de l'utilisateur
- Matériel adapté / ergonomique (trouble musculosquelettique)
- La puissance des ordinateurs en fonction des logiciels métiers

- Le matériel doit être adapté aux logiciels métiers de l'entreprise

FP4 : le matériel doit être recyclé par un organisme agréé par la D3E vente du matériel

- Don a des associations ou Organisme de recyclage (Entreprise agréée par l'état) ou revente de l'utilisateur
- un déchet est défini par la loi du 15 Juillet 2005, puis 13 Août 2005, l'identification de son producteur et le pictogramme de la « poubelle barrée » montrant que ce produit fait l'objet d'une collecte sélective (Norme EN 50419). Catégorie 3: Equipements Informatiques et de télécommunications (Dans le cadre français, sont ajoutées les catégories 3A : Ecrans, moniteurs et équipements comprenant des écrans d'une surface supérieure à 100 cm², 3B : Autres équipements informatiques et de télécommunications)
- Donc soumis à la catégorie 3 l'élimination du déchet dans le respect des réglementations environnementales

FP5 Nous devrions contacter uniquement des fournisseurs qui respectent les normes de sécurité et environnementales

- Fournisseurs dans la norme D3E
- Fournisseurs officiels / respect des normes
- La demande d'avoir un fournisseur qui respecte les normes et qui applique une politique environnementale, qui nous permettra de mieux trier ensuite nos déchets et limiter les produits non recyclables. Dans la démarche environnementale ISO 14001:2015 démarche de laquelle nous devrions nous rapprocher.

FP6 Le matériel devra être stocké dans une pièce appropriée, et un inventaire devra être mis en place pièce adaptée

- Une pièce dédiée au rangement du stock et un système d'inventaire pour gérer les besoins et commandes

FP7 Certains des utilisateurs au sein de l'entreprise sont itinérants, il faudra donc pallier à cette contrainte par l'achat de matériels itinérants (Smartphones, PC portable)

- Adapté le matériel à l'itinérance de certains personnels

FC1 Le matériel se devra d'être garanti

- La garantie du matériel achetée en accord avec le prix d'amortissement

FC2 Le matériel aura besoin d'énergie pour fonctionner, ici l'électricité sera privilégiée

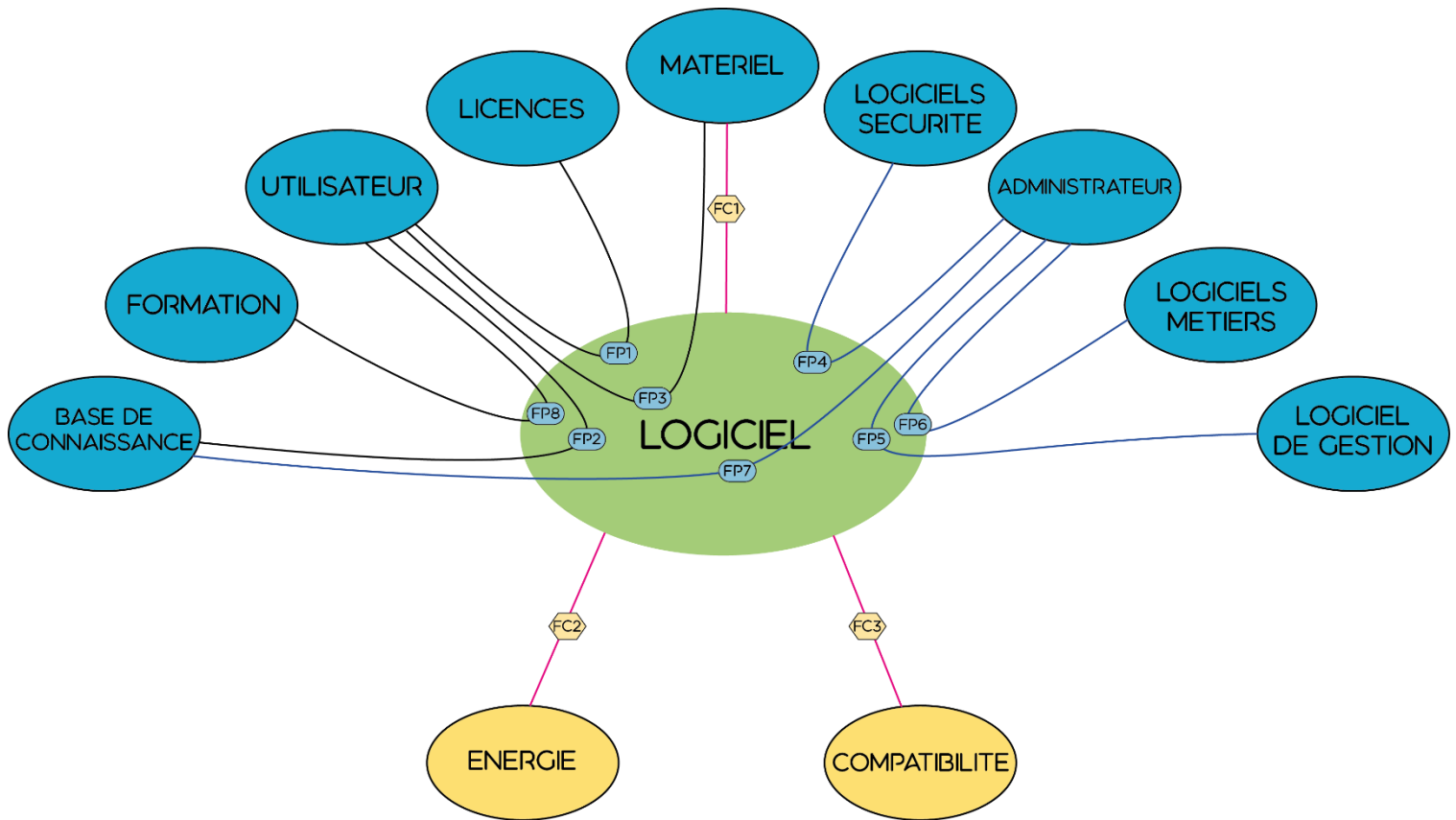
- Alimentation électrique dans les normes

FC3 Faire face aux contraintes liées aux bâtiments (ex : normes, dispositions des salles, dispositions des prises électriques, climatisation (salles serveurs) ...)

- Respect des normes environnementales
- Bâtiments dans les normes et le respect environnemental

Fonctions	FP	Fonction Principale	CRITERE D'APPRECIATION	NIVEAU	PRIORITE	Etat
Matériel	FP1	Les administrateurs doivent pouvoir accéder au matériel pour l'installer	Accessibilité	Quantité de stock minimal	1	Existant
				gestion des acces au stock	1	Existant
				accessibilité du stock pour le service informatique autorisé	1	Existant
	FP2	L'administrateur doit pouvoir avoir accès à une base de connaissances qui regroupe les procédures/tutoriels	Mise à jour de la base de connaissance	procédure pour chaque pratique ou materiel différent	2	A Traiter
				mise a jour et suivi des procedures	2	A Traiter
	FP3	Permettre à l'utilisateur de réaliser le travail demander	materiel adapté en fonction de l'utilisateur	materiel adapté / ergonomique (trouble musculosqueletique)	3	A Traiter
			puissance des ordinateurs en fonction des logiciels metiers	configuration du materiel	1	A remplacer
	FP4	le matériel doit etre recyclé par un organisme agréé par la D3E	vente du materiel	don a des associations	3	A Traiter
				politique de reprise ou de vente	1	A Traiter
			Organisme de recyclage	Entreprise agréé par l'état	1	A Traiter
	FP5	Nous devrions contacter uniquement des fournisseurs qui respectent les normes de sécurité et environnementale	Fournisseurs dans le norme D3E	Fournisseurs officiel / respect des normes	2	A Traiter
	FP6	Le matériel devra être stocké dans une pièce approprié, et un inventaire devra être mis en place	pièce adapté	type de solution	2	Existant
			inventaire	Solution d'inventorisme	1	A Traiter
	FP7	Certains des utilisateurs au sein de l'entreprise sont Itinérant, il faudra donc palier à cette contrainte par l'achat de matériels Itinérant (Smartphones, PC portable)	Matériel spécifique	Matériel déplaçable	2	A remplacer
	FC1	Le matériel se devra d'être garantie	Vérification garantie	Garantie sur 5 ans	1	A Traiter
	FC2	Le matériel aura besoin d'énergie pour fonctionner, ici l'électricité sera privilégiée	Energie	Respect des normes	1	Existant
	FC3	Faire face aux contraintes lié aux bâtiments (ex : normes, dispositions des salles, dispositions des prises électriques, climatisation (salles serveurs) ...)	Bâtiments	Respect des normes environnementales	3	Existant

H. LOGICIEL



FP1 L'utilisateur doit disposer des licences valides pour pouvoir utiliser les différents logiciels (si nécessaire) dont il aura besoin.

- L'anticipation des achats de licences nécessaire aux logiciels et matériel

FP2 L'utilisateur doit avoir accès à une base de connaissances concernant l'utilisation de certains logiciels (procédures, tutoriels, etc...) Accès base de connaissances par les utilisateurs

FP3 le matériel doit être simple d'utilisation et préconfigurer pour l'utilisation des logiciels métiers pré configuration des profils et des postes

- Profils déjà mis en place en fonction de l'utilisateur
- Organisation pour l'installation des postes suivant les besoins de logiciel

FP4 L'administrateur doit avoir accès à des logiciels de sécurité pour sécuriser le système d'information (ex : Antivirus, Anti-Malware, etc...)

- Prévoir des systèmes de sécurisations contre les virus et autres intrus

FP5 L'administrateur doit avoir accès à des logiciels de gestion de parc informatique ou d'autres outils qui permettront à l'ensemble de l'entreprise de pouvoir continuer de produire

- Logiciels de gestion

- Solution de gestion à distance
- Solution de Gestion de parc informatique grâce aux logiciels
- Un accès à l'entreprise devra être créé via l'extérieur pour les itinérants et autres personnels concernés

FP6 L'administrateur doit pouvoir paramétrer les applications métier

- Gestion des comptes utilisateurs
- Adapté les installations suivant les besoins

FP7 L'administrateur doit avoir accès à la base de connaissance pour pouvoir la consulter et la mettre à jour.

- Faire périodiquement la mise à jour de la documentation

FP8 Les utilisateurs doivent avoir accès aux formations (proposé par le SI ou autres). Pour pouvoir se former sur les nouveaux logiciels, si besoin.

- Formation guidée par un intervenant pour la formation personnel plus tutoriel mis à disposition

FC1 Pour faire fonctionner les logiciels il nous faudra obligatoirement avoir accès à un matériel pouvant supporter la charge du logiciel (que ce soit sur ordinateur ou smartphone). Anticipation des besoins futur

- Le matériel devra être adapté à la demande de ressources des logiciels

FC2 Il nous faudra obligatoirement une source d'énergie pour pouvoir faire fonctionner le matériel nécessaire à l'utilisation des logiciels

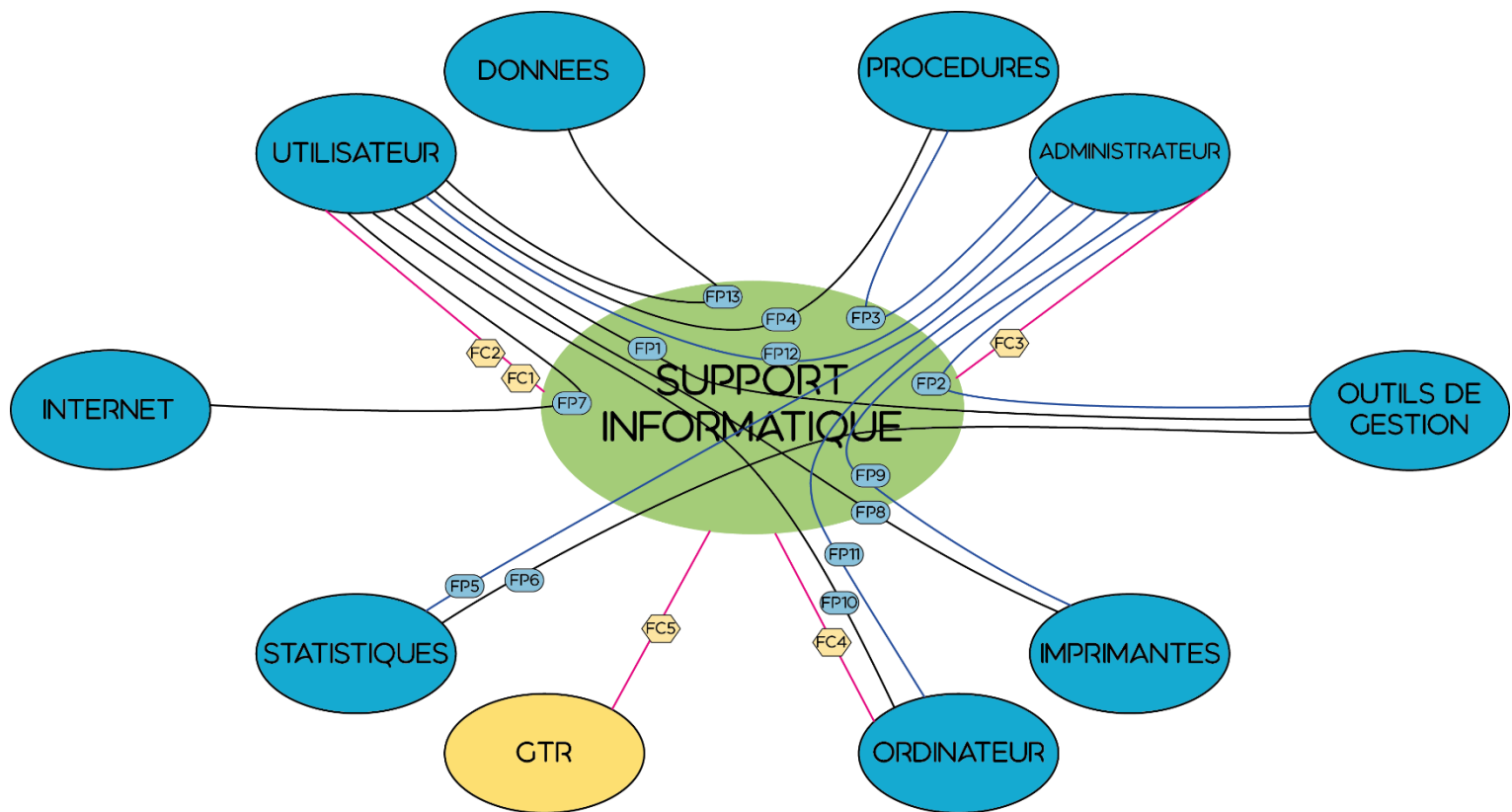
- Respect des normes nfc 15-100
- Solution en cas de coupure
- Alimentation électrique aux normes

FC3 Les logiciels se devront d'être compatibles avec le matériel ainsi qu'avec le système d'exploitation utilisé dans l'entreprise Compatibilité

- Logiciels, système d'exploitation et composants compatibles
- Le matériel devra être compatible avec les logiciels et leurs évolutions

Fonctions	FP	Fonction Principale	CRITERE D'APPRECIATION	NIVEAU	PRIORITE	Etat
Logiciel	FP1	L'utilisateur doit disposer des licences valide pour pouvoir utiliser les différents logiciels (si nécessaire) dont il aura besoin.	Achat de licences	prix des licences	1	A remplacer
	FP2	L'utilisateur doit avoir accès à une base de connaissances concernant l'utilisation de certains logiciels (procédures, tutoriels, etc...)	Accès base de connaissances par les utilisateurs	technique materiel	2	A remplacer
				Logiciels	2	Existant
	FP3	le matériel doit etre simple d'utilisation et préconfigurer pour l'utilisation des logiciels metiers	preconfiguration des profils et des postes	profils déjà mis en place en fonction de l'utilisateur	1	Existant
				Matériel préalablement installé	1	Existant
	FP4	L'administrateur doit avoir accès à des logiciels de sécurité pour sécuriser le système d'information (ex : Antivirus, Anti Malware, etc...)	Logiciels de sécurité	type de logiciels	1	Existant
	FP5	L'administrateur doit avoir accès à des logiciels de gestion de parc informatique ou d'autres outils qui permettront à l'ensemble de l'entreprise de pouvoir continuer de produire	Logiciels de gestion	solution de gestion a distance	2	A Traiter
				solution de Gestion de parc informatique grâce aux logiciels	1	A Traiter
	FP6	l'administrateur doit pouvoir paramétrer les applications metier	Logiciels métiers	type d'interface	2	Existant
				gestion des comptes utilisateurs	1	Existant
				niveau de parametrage en fonction des besoin de l'entreprise	1	Existant
	FP7	L'administrateur doit avoir accès à la base de connaissance pour pouvoir la consulter et la mettre à jour.	Mises à jour procédures	délais moyen de réalisation (25 pages)	2	Existant
				delais moyen de mises a jour (25 pages)	3	Existant
	FP8	Les utilisateurs doivent avoir accès aux formations (proposé par le SI ou autres). Pour pouvoir se former sur les nouveaux logiciels, si besoin.	formation guidé par un intervenant	nombre de personnes maximales par session	2	Existant
				prix par module	1	Existant
			Formation personnel	outils utilisé	2	Existant
	FC1	Pour faire fonctionner les logiciels Il nous faudra obligatoirement avoir accès à un matériel pouvant supporter la charge du logiciel (que ce soit sur ordinateur ou smartphone).	Anticipation des besoins future	Le matériel doit être compatible	1	A remplacer
	FC2	Il nous faudra obligatoirement une source d'énergie pour pouvoir faire fonctionner le matériel nécessaire à l'utilisation des logiciels	Energie	respect des normes nfc 15-100	1	Existant
				solution en cas de coupure	1	A Traiter
				Besoin en électricité	1	Existant
	FC3	Les logiciels se devront d'être compatible avec le matériel ainsi qu'avec le système d'exploitation utilisé dans l'entreprise	Compatibilité	coût	1	A Traiter
				Logiciels, système d'exploitation et composants compatible	2	A remplacer

C. SUPPORT



FP1 Utilisation de l'outil de gestion de parc des incidents pour les utilisateurs

- Les utilisateurs peuvent créer des demandes sur l'outil de gestion des incidents. Les Utilisateurs pourront se renseigner sur l'état de leurs demandes, recevront un message lorsque le problème sera résolu ainsi que donner leur avis sur la résolution du problème en cas de problème non résolu ils pourront reprendre l'incident fermé

FP2 L'Administrateur doit pouvoir administrer l'outil de gestion et prioriser les demandes/clôturer

- Les administrateurs pourront donner les permissions nécessaires à chacun des intervenants sur leur niveau d'habilitation
- La possibilité de priorisation des demandes permettra de traiter par gravité

FP3 L'Administrateur peut consulter, créer et modifier les procédures dans une base de données interne à l'Entreprise

- La base de données devra être administrable en consultation, création, modification suppression et gestion de l'espace

FP4 L'utilisateur doit avoir accès aux procédures de dépannage en consultation

- Un accès sans permissions particulières doit être créé dans les procédures les concernant pour permettre la consultation uniquement

FP5 L'Administrateur doit avoir accès à toutes les statistiques de l'outil de gestion les anciens incidents les demandes non traité les avis utilisateurs

- Chaque utilisateur doit pouvoir remplir un questionnaire de satisfaction dans la résolution de son problème dans le but d'amélioration futur, des exportations et référencements de statistiques seront nécessairement accessible

FP6 Tout les incidents traités sont répertorié dans une base de données automatiquement

- Répertoriassions des incidents, tri automatique et consultation par les intervenants

FP7 Tous les utilisateurs doivent avoir accès à internet

- Un accès sans permissions particulières doit être crée dans les procédures les concernant pour permettre la consultation uniquement

FP8 Tous les utilisateurs peuvent imprimer et on accès à leurs impressions

- Gestions des impressions suivant l'endroit, le profil et la priorisation

FP9 Les administrateurs peuvent vérifier l'état des imprimantes et les files d'impressions à partir de tous les postes

- La possibilité d'administrer les postes à distance va permettre un gain de temps dans la compréhension des problématiques et des résolutions
- Une fonction simple pour permettre l'accès à l'imprimante, son statut et historique

FP10 Chaque utilisateur doit disposer d'un poste fonctionnel avec des logiciels métiers adaptés

- Un poste de travail avec une installation cohérente avec l'emploi et les missions attribuées par l'entreprise

FP11 L'administrateur doit pouvoir prendre la main sur tous les postes et logiciels de l'entreprise pour la résolution des incidents

- Un accès administrateur sur tous les types d'appareils à distance, visibilité des incidents et résolutions, évitant le déplacement du personnel quand ce ne sera pas possible autrement.

FP12 L'administrateur doit informer l'utilisateur des bonnes pratiques à employer

- Une information de bonnes pratiques sera nécessaire évitant la répétition de l'incident, la mise par écrit permettra l'uniformisation et la diffusion également

FP13 L'Utilisateur doit avoir accès aux données nécessaire à son travail à la modification / consultation /création de celles-ci

FC1 L'utilisateur doit respecter les bonnes pratiques de l'entreprise

FC2 Les utilisateurs doivent être former pour créer une demande ainsi que l'assistance pour le dépannage

- Faire des formations d'utilisations et de bonnes pratiques pour les utilisateurs.

FC3 Devoir de confidentialité

- Sécurisation des sessions et communications

FC4 Prévention des défaillances

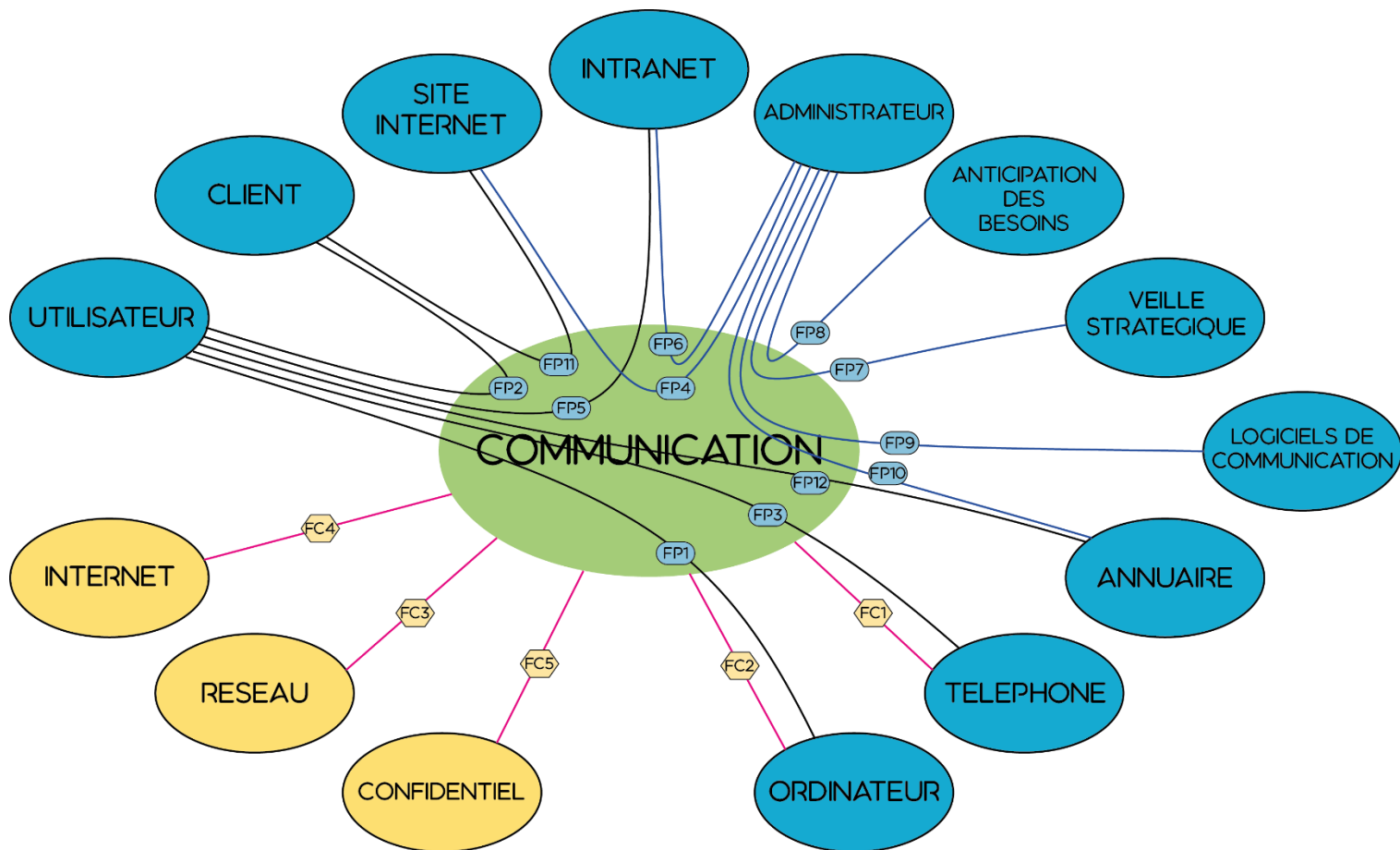
- Surveillance disque dur / taille / temps -- prévention des défaillances matériel

FC5 Délais de résolution des incidents

- Déterminé le temps acceptable pour une urgence grave, moyenne,
- Légère et mettre en place la garantie de s'y tenir
- GTI : Garantie de Temps d'Intervention
- GTR : Garantie de Temps de Rétablissement

Fonctions	FP	Fonction Principale	CRITERE D'APPRECIATION	NIVEAU	PRIORITE	Etat
Support	FP1	Utilisation de l'outil de gestion de parc des incidents pour les utilisateurs	Création des demandes	nombres de demandes par utilisateurs	1	A Traiter
			vérification de l'état de la demande	modification	4	A Traiter
				instantané	3	A Traiter
			information à la résolution de la demande	instantané	1	A Traiter
			reprise d'un incident passé	instantané	4	A Traiter
			fermeture de l'incident	instantané	2	A Traiter
			Satisfaction utilisateur	critères d'évaluation	4	A Traiter
	FP2	L'Administrateur doit pouvoir administrer l'outil de gestion et prioriser les demandes clôturées	administration de l'outil	Contrôle total	1	A Traiter
			priorisation des demandes / clôtures	Contrôle total	1	A Traiter
			affectation des tâches au tech	Contrôle total	1	A Traiter
	FP3	L'Administrateur peut consulter, créer et modifier les procédures dans une base de données interne à l'entreprise	consultation	Contrôle total	1	A Traiter
			modification	Contrôle total	1	A Traiter
			espace disponible	modulable	2	A Traiter
			création	Contrôle total	1	A Traiter
	FP4	L'utilisateur doit avoir accès aux procédures de dépannage en consultation	consultation	consultation uniquement	2	A Traiter
	FP5	L'Administrateur doit avoir accès à toutes les statistiques de l'outil de gestion : les anciens incidents, les demandes non traitées, les avis utilisateurs	statistique de satisfaction	par incidents	2	A Traiter
				globale	2	A Traiter
			exportation de statistiques	excel	1	A Traiter
			référencement des anciens incidents	base de données	1	A Traiter
	FP6	Tous les incidents traités sont répertoriés dans une base de données automatiquement	gestion d'une base de données	base de données consultable	1	A Traiter
			automatisation des tâches	statistiques	3	A Traiter
				automatisation	2	A Traiter
	FP7	Tous les utilisateurs doivent avoir accès à Internet	accès à la fibre	délais	1	Existant
	FP8	Tous les utilisateurs peuvent imprimer et ont accès à leurs impressions	Dépannage	délais	1	Existant
			localisation en fonction du poste	gestion des quotas d'impression	2	Existant
				sécurité des documents	1	Existant
	FP9	les administrateurs peuvent vérifier l'état des imprimantes et les files d'impressions à partir de tous les postes	administration à distance	accès aux configurations	1	Existant
			vérification des imprimantes	Statut en direct	1	Existant
	FP10	Chaque utilisateur doit disposer d'un poste fonctionnel avec des logiciels métiers adaptés	déploiement de poste et logiciels en fonction de l'utilisateur	poste utilisable dès la première utilisation	1	A Traiter
	FP11	L'administrateur doit pouvoir prendre la main sur tous les postes et logiciels de l'entreprise pour la résolution des incidents	vision sur les problèmes de l'utilisateur	en direct	1	A Traiter
			Résolution des incidents	en direct	1	A Traiter
				ressources humaines	2	A Traiter
	FP12	L'administrateur doit informer l'utilisateur des bonnes pratiques à employer	réalisation de procédures	ressources humaines	1	A Traiter
			informations sur les bonnes pratiques	ressources humaines	1	A Traiter
	FP13	L'utilisateur doit avoir accès aux données nécessaires à son travail à la modification / consultation / création de celles-ci	accès aux données et logiciels en fonction de la personne	contrôle limité pour l'utilisateur	1	Existant
	FC1	L'utilisateur doit respecter les bonnes pratiques de l'entreprise	type de solution	type de solution	1	A Traiter
	FC2	Les utilisateurs doivent être formés pour créer une demande ainsi que l'assistance pour le dépannage	formation des utilisateurs	temps par utilisateur	2	A Traiter
				coût	1	A Traiter
	FC3	devoir de confidentialité	type de solution	type de solution	1	A Traiter
	FC4	prévention des défaillances	type de solution	type de solution	3	A Traiter
	FC5	délais de résolution des incidents	reprise de production	délais d'intervention incident grave	1	A Traiter
				délais d'intervention incident moyen	2	A Traiter
				délais d'intervention incident léger	2	A Traiter
			respect des GTR	délais maximal	1	A Traiter

D. COMMUNICATION



FP1 : permettre aux utilisateurs de communiquer entre eux

- Une homogénéisation de la liaison entre les ordinateurs et matériel réseau

FP2 : mise en relation utilisateurs et clients

- Il faut que les utilisateurs puissent envoyer messages et documentation par le réseau de manière identifier et sécurisé

FP3 : mise en relation vocal avec l'utilisateur

- Plusieurs autres manières de communiquer sont indispensable suivant la sédentarité ou l'itinérance de chacun DECT pour l'interentreprise et les smartphones pour les itinérances

FP4 : permet à l'administrateur de gérer le site internet

- L'administration du site internet permet de gérer l'éventuel vitrine et les informations diffusés aux clients

FP5 : permet aux utilisateurs de communiquer en interne, diffuser, mettre à disposition des documents

- Les utilisateurs peuvent mettre à disposition diverses informations et documentations, calendriers

FP 6 : permet à l'administrateur de gérer l'intranet

- Une administration de l'intranet en local par nos informaticiens pour octroyer les droits rédactionnels à chacun

FP 7 : permet à l'administrateur de faire de la veille stratégique

- Une veille stratégique va permettre de comprendre les directions à prendre pour l'entreprise en termes de technologie concurrentiel une veille stratégique va permettre de comprendre les directions à prendre pour l'entreprise en termes de technologie concurrentiel

FP 8 : permet à l'administrateur de l'anticipation de besoin

- Un suivi des besoins de l'entreprise avec une veille technologique pour le maintien du niveau de l'entreprise

FP 9 : permet à l'administrateur de gérer le logiciel de communication

- Un accès aux créations et gestions des utilisateurs sur le logiciel de communication et sa sécurisation

FP 10 : permet à l'administrateur de gérer la base de connaissance

- Un accès à la base de connaissance en administrateur

FP 11 : permet au client d'obtenir des informations par le site internet

- La création d'un compte pour les clients va leurs permettre d'accéder à des informations de l'entreprise.

FP 12 : permet à l'utilisateur de consulter l'annuaire

- Permet l'utilisation de l'annuaire des contacts

FC1 : avoir un téléphone (smartphone si itinérance)

- Des téléphones pour tous avec une l'homogénéisation du parc

FC2 : avoir un ordinateur (portable si itinérance)

- Des postes pour chacun avec une l'homogénéisation du parc

FC3 : avoir un réseau dimensionné en fonction du parc pour la mise en relations les ordinateurs

- Prévoir l'évolution possible du parc et assuré l'interconnexion des ordinateurs

FC4 : accès internet dimensionné à l'activité de l'entreprise

- Accès à internet adapter au besoin de l'entreprise

FC5 : que les communications puissent être confidentiels et cryptés

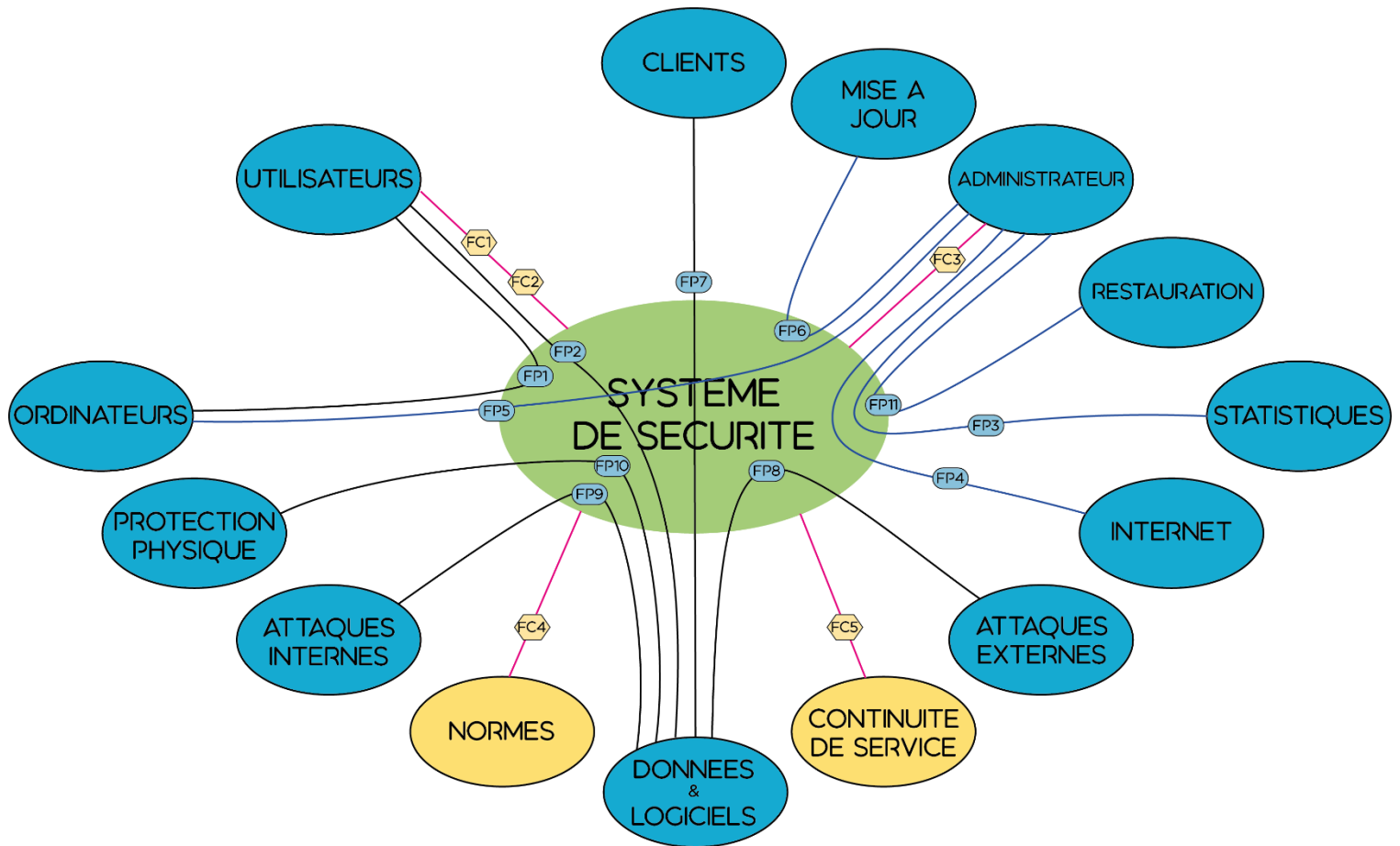
- Sécuriser les transmissions

FC6 avoir des logiciels de communication

- Logiciel de communication adapté à l'entreprise

Fonctions	FP	Fonction Principale	CRITERE D'APPRECIATION	NIVEAU	PRIORITE	Etat
Communication	FP1	Permettre aux utilisateurs de communiquer entre eux	connectivité et intégration dans le réseau d'entreprise de l'ordinateur	Entre 100Mb/s et 1Gb/s	1	Existant
	FP2	Mise en relation utilisateurs et clients	la possibilité d'envoi de message ou de documents par le logiciel de communication	taille pièces jointes et tailles de stockage	2	Existant
	FP3	Mise en relation vocal avec l'utilisateur	connectivité et intégration de dans le réseau d'entreprise	DECT et smartphone	2	Existant
	FP4	Permet à l'administrateur de gérer le site internet	interface de gestion du site , accès , option de paramétrage	Accès total	2	Existant
	FP5	Permet aux utilisateurs de communiquer en interne ,diffuser, mettre à disposition des documents	site de diffusion et de communication interne	messages entre utilisateurs et post suivant les droits rédactionnelles attribués	3	Existant
	FP6	Permet à l'administrateur de gérer l'intranet	interface d'attribution de droits	connexion des utilisateurs et gestion de permissions	4	Existant
	FP7	Permet à l'administrateur de faire de la veille stratégique	vérifie l'existant et les évolutions possibles par le biais de son réseau	réseau d'entreprise	1	A Traiter
	FP8	Permet à l'administrateur d'anticiper les besoins	vérifie l'existant avec les besoins des charges futures	suivi et veille techno	1	A Traiter
	FP9	Permet à l'administrateur de gérer le logiciel de communication	paramétrage et modification de compte par l'admin	accès total	1	Existant
	FP10	Permet à l'administrateur de gérer la base de connaissance	paramétrage et modification de compte par l'admin	accès total	1	Existant
	FP11	Permet aux clients d'obtenir des informations par le site internet	mise à disposition du client d'information via le site	compte client	3	Existant
	FP12	Permet à l'utilisateur de consulter l'annuaire	interface de recherche d'un autre utilisateur	fonction recherche	2	Existant
	FC2	Avoir un ordinateur (portable si itinérance)	ordinateur interconnecté	connectivité et autonomie	1	A Traiter
	FC1	Avoir un téléphone (smartphone si itinérance)	telephone dect et smartphone connecter au réseau d'entreprise	compatibilité et connectivité	1	A Traiter
	FC3	Avoir un réseau dimensionné en fonction du parc pour la mise en relations les ordinateurs	mise en relation des ordinateurs	en étoile tenant compte de la charge	1	Existant
	FC4	Accès internet dimensionné à l'activité de l'entreprise	internet	fibre 1Gb/s minimum	1	Existant
	FC5	Que les communications puissent être confidentiels et cryptés	cryptage et identification		1	Existant
	FC6	Avoir des logiciels de communication	logiciel de mise en relation	stockage et envoi 250mo minimum	1	Existant

E. SECURITE



FP1 les postes doivent être sécurisés en fonction des utilisateurs

- Connexion par login / mot de passe
- Tous les postes sont sécurisés et se verrouille automatiquement en cas d'absence
- La sécurisation des postes de chaque utilisateur

FP2 les utilisateurs doivent avoir accès aux données et aux logiciels métiers en fonction de leurs postes dans l'entreprise

- Hiérarchisations des niveaux d'accès au logiciels métiers et aux données en fonction du profil de la personne
- Créations d'une arborescence et hiérarchiser les droits et permissions de chacun

FP3 les administrateurs doivent avoir accès au Statistiques du système de sécurité vérification du trafic du SI

- Accès aux statistiques et possibilité de réinitialisé les mots de passe

FP4 les administrateurs peuvent autoriser ou refuser les entrées et sorties sur le SI contrôle des entrées et des sorties sur le SI

- Contrôle des flux entrant et sortant

FP5 les administrateurs peuvent changer les droits et permission administrer et prendre la main sur les postes des utilisateurs

- Contrôle avec la permission de l'utilisateur
- Les accès aux postes distances se feront sous l'autorisation de l'utilisateur
- Modification / Suppression de profil
- Gestions profiles

FP6 les administrateurs gèrent les mises à jour du SI et leurs déploiements

- Mise en place d'un niveau de sécurité pour contrôler les mises à jour à déployer sur le SI
- Espace de test
- Les mises à jour centralisé et diffère pour limiter l'impact sur le réseau
- Contrôle totale des mises à jour

FP7 les clients ont accès aux fiches produites sur le site internet de l'entreprise

- Téléchargement possible
- Espace de stockage pour les fiches produits
- Un site internet pour les clients, avec différents services, téléchargement des fiches produits ...
- Le site doit rester disponible pour les clients et leurs donner accès aux fiches produits
- 150 visites par jours / évolutif

FP8 Tout le système d'information doit être protégé des attaques externes

- Bloquer les accès non désiré identification de la personne
- Protections contre les attaques extérieurs par l'internet
- Accès impossible au personnes malveillantes
- Aucun accès aux sites malveillant
- Verrouillage systématique des sites dangereux

FP9 tout le système d'information doit être protégé des attaques internes surveillance du système isolation du problème et restauration des fichiers

- Bloquer le déploiement d'un programme malveillant de manière volontaire ou non au sein du SI
- Identification de la personne / poste
- Limité la possibilité d'accès a des sites malveillants, blocages des téléchargements dangereux ou non sécurisé
- Isolation du problème et restauration des fichiers

FP10 le système de sécurité doit être accessible uniquement aux personnes autorisées

- Protection physique des locaux protection des baies et salles serveur dans une pièce sécurisé par un badge
- Un dispositif physique de protection du si et d'indentification

FP11 l'administrateur doit pouvoir restaurer le système de sécurité en cas d'incident

- Possibilité de restauration
- Sauvegarde du système complet entré et sorties réseaux, droits, permissions etc.
- Isolement des données
- La possibilité de récupéré dans un temps rapide les données malgré de gros incidents
- Limité la possibilité d'accès et d'intrusions malveillantes dans le système

FC1 Seul les utilisateurs de l'entreprise doivent avoir accès aux données et au logiciels métier de l'entreprise

- Changement de mot de passe obligatoire tous les mois
- Sécurisation des accès aux logiciels métiers et aux données
- Mot de passe reste strictement personnel

FC2 les utilisateurs doivent respecter les bonnes conduites dans la saisie, l'accès et utilisation des données

- Mettre en place des règles de bonnes conduites

FC3 les administrateurs contrôlent le système de sécurité

- Paramétrage des flux d'entrée et sortie des données
- Mise à jour paramétrable par l'administrateur

FC4 le Système doit répondre aux normes de sécurité électriques protection du matériel et des personnes

- Respecter toutes les normes en vigueur
- NFC 15-100 / CE
- ISO/CEI 27001
- CNIL / RGPD

FC5 Une continuité de service doit être mis en place sur le système de sécurité

- Que la continuité de service soit assurée malgré une panne

Sécurité

Fonctions	FP	Fonction Principale	CRITERE D'APPRECIATION	NIVEAU	PRIORITE	Etat
Sécurité	FP1	les postes doivent être sécurisés en fonction des utilisateurs	connexion par login/mdp	tous les postes sont sécurisés et se verrouille automatiquement en cas d'absence	1	Existant
	FP2	les utilisateurs doivent avoir accès aux données et aux logiciels métiers en fonction de leurs postes dans l'entreprise	hiérarchisations des niveaux d'accès	accès aux logiciels métiers et aux données en fonction du profil de la personne	1	Existant
	FP3	les administrateurs doivent avoir accès aux statistiques du système de sécurité	vérification du trafic du SI	Vision totale	3	A Traiter
			modification mots de passe	Contrôle total	1	Existant
	FP4	les administrateurs peuvent autoriser ou refuser les entrées et sorties sur le SI	contrôle des entrées et des sorties sur le SI	Contrôle total	1	Existant
	FP5	les administrateurs peuvent changer les droits et permissions administrer et prendre la main sur les postes des utilisateurs	contrôle à distance	contrôle avec la permission de l'utilisateur	1	Existant
			Modification / Suppression de profil	Contrôle totale	1	Existant
	FP6	les administrateurs gèrent les mises à jours du SI et leurs déploiement	mise en place d'un niveau de sécurité pour contrôler les mises à jour à déployer sur le SI	Espace de test	3	Existant
				Contrôle totale des mises à jours	2	Existant
	FP7	les clients ont accès aux fiches produits sur le site internet de l'entreprise	téléchargement possible	libre	2	Existant
			espace de stockage pour les fiches produits	modulable	2	Existant
			le site doit rester disponible pour les clients et leurs donner accès aux fiches produits	150 visites par jours / évolutif	1	Existant
	FP8	tout le système d'information doit être protégé des attaques externes	bloquer les accès non désiré	identification de la personne	3	Existant
				accès impossible aux personnes malveillantes	1	Existant
			aucun accès aux sites malveillant	verrouillage systématique des sites dangereux	1	Existant
	FP9	tout le système d'information doit être protégé des attaques internes	surveillance du système	isolation du problème et restauration des fichiers	1	Existant
			bloquer le déploiement d'un programme malveillant de manière volontaire ou non au sein du SI	identification de la personne / poste	3	Existant
				isolation du problème et restauration des fichiers	1	Existant
	FP10	le système de sécurité doit être accessible uniquement aux personnes autorisées	protection physique des locaux protection des baies et salles serveur dans une pièce sécurisée par un badge	Protection des salles serveurs	1	Existant
				protection des baies	2	Existant
	FP11	l'administrateur doit pouvoir restaurer le système de sécurité en cas d'incidents	possibilité de restauration	délais	1	Existant
			Sauvegarde du système complet entrées et sorties réseaux, droits, permissions etc.	isolement des données	1	Existant
	FC1	Seul les utilisateurs de l'entreprise doivent avoir accès aux données et aux logiciels métier de l'entreprise	changement de mot de passe obligatoire tous les mois	obligation	1	Existant
			le mot de passe doit rester strictement personnel	type de solution	1	Existant
	FC2	les utilisateurs doivent respecter les bonnes conduites	dans la saisie, l'accès et utilisation des données	type de solution	1	A Traiter
	FC3	les administrateurs contrôlent le système de sécurité	entrées sorties	contrôle totale	1	Existant
			mise à jour	contrôle totale	1	Existant
	FC4	le Système doit répondre aux normes de sécurité	électriques protection du matériel et des personnes	nfc 15-100 / CE	1	Existant
			CNIL / RGPD	type de solution	1	Existant
			ISO/CEI 27001	ISO/CEI 27001	2	Existant
	FC5	Une continuité de service doit être mise en place sur le système de sécurité	maintien du service en cas de panne	Type de service maintenue	1	Existant

III. GLOSSAIRE

LTE : Long Term Evolution

UMTS : Universal Mobile Telecommunications System

HSDPA : High Speed Downloading Packet Access

RTO : Recovery Time Object

GTI : Garantie de Temps d'Intervention

GTR : Garantie de Temps de Rétablissement

DEEE : Aussi appelé D3E est la norme qui entoure les Déchets d'Equipements Electriques et Electroniques

DECT : Digital Enhanced Cordless Télécommunications signifie littéralement « téléphone sans-fil numérique amélioré »

ROI : Le retour sur investissement (Return On Investment)

IV. WEBOGRAPHIE

[https://fr.wikipedia.org/wiki/Retour sur investissement](https://fr.wikipedia.org/wiki/Retour_sur_investissement)

<https://www.sydem.fr/fr/definition-des-d3e.html>

<https://www.d3e.fr/>

<https://www.journaldunet.com/solutions/cloud-computing/1020522-rto-rpo-les-indicateurs-de-securite-en-cas-de-sinistre/>

https://fr.wikipedia.org/wiki/Dur%C3%A9e_maximale_d%27interruption_admissible

https://fr.wikipedia.org/wiki/Garantie_de_temps_de_r%C3%A9tablissement

<https://agiliste.fr/introduction-methodes-agiles/>

<https://www.unow.fr/blog/le-coin-des-experts/methode-agile-mieux-gerer-projets-entreprise/>