CESi alternance

ÉCOLE SUPÉRIEURE DES MÉTIERS

RAPPORT DE PROJET

PROJET FIL ROUGE - WOOD - LOT 3

2020 - 2021

HAUGUEL Axel - WEBER Raphaël

RISR 19 – RESPONSABLE EN INGENIERIE SYSTEMES ET RESEAUX

TABLE DES MATIERES

I – INTRODUCTION

Ce livrable numéro trois a plusieurs cibles. Il suit les livrables techniques qui vous fournit toutes les solutions techniques que nous déploierons dans votre entreprise. Dans cette partie, nous vous présenterons les parties budgétaires, sécurisation du système d'information et vous démontrerons la viabilité du projet.

Par conséquent, le but de ce document est de déterminer les coûts associés au projet, ainsi que d'étudier la sécurité du système et de ses composants. Nous prouverons également que notre solution peut répondre à toutes les exigences exposées dans le livrable précédent.

II – PSSI

PSSI, qui signifie politique de sécurité du système d'information est un document construit par l'entreprise qui définit le plan d'action suivi par l'entreprise dans le but de sécuriser son système d'information. Le document est à destination de toutes les personnes intervenantes sur le système d'information (prestataires, utilisateurs, …).

Le PSSI est décomposé en 4 sections :

- L'introduction, ce présent document, permet de situer la place de la PSSI dans le référentiel normatif de la SSI au sein de l'organisme et de préciser les bases de légitimité sur lesquelles elle s'appuie ;
- La méthodologie présente, de façon détaillée, la conduite de projet d'élaboration d'une PSSI, ainsi que des recommandations pour la construction des règles de sécurité ;
- Le référentiel de principes de sécurité ;
- Une liste de documents de références de la SSI (critères d'évaluation, textes législatifs, normes, codes d'éthiques, notes complémentaires…).

II.2 – PERIMETRE

La politique de sécurité du système d'information s'applique à l'ensemble du groupe WOOD mais également tous ses prestataires ainsi que les intervenants sur le système d'information (stagiaires, salarié, sous-traitant, directeur des systèmes d'information…). Le plan s'appliquera donc à tous les sites du groupe WOOD.

- Le site de Lille : C'est le siège social. Il couvre les bureaux de la direction, un site de production et un entrepôt de stockage des matières premières et des produits finis.
- Le site de production (Dax) : Le site de Dax a été ouvert en 1993, il couvre un site de production, un entrepôt ainsi que des bureaux.
- Le site de production (Annecy) : Le site de Dax a été ouvert en 2012, il couvre un site de production, un entrepôt ainsi que des bureaux. Il a été ouvert pour les maisons modulaires en bois.
- Les magasins : Brest et Mâcon.

II.3 – AUDIT

Le tableau suivant énumère un extrait des exigences de sécurisation du système d'information du groupe WOOD.

N° Ex	Exigences	Niv.	Réal.	Niv 1	Niv 2
2.1	Assurer une protection efficace et homogène des locaux et serveurs hébergeant des informations sensibles ou applications critiques		90%	94%	87%
2.1.1	Sécurité physique des locaux et matériels		92%	100%	83%
2.1.2	Gestion des sauvegardes et archivage		82%	83%	80%
2.1.3	Gestion des procédures de démarrage des services		100%	100%	100%
2.1.4	Protection contre les virus et codes malveillants		100%	100%	100%
2.2	Mettre en place un cloisonnement des réseaux permettant de protéger les informations sensibles ou applications critiques		83%	100%	67%
2.3	Déployer une configuration sécurisée des postes de travail		100%	100%	100%
2.3.1	Identification et contrôle d'accès logique		100%	100%	100%
2.3.2	Bridage et mise à jour des postes de travail		100%	100%	100%
2.3.3	Reconstruction des postes de travail		100%	0%	100%
2.4	Etablir une classification opérationnelle de l'information		0%	0%	0%
2.5	Renforcer et communiquer sur les rôles et responsabilités des acteurs du point de vue de la sécurité.		100%	100%	100%
2.5.1	Droits et devoirs des utilisateurs		100%	100%	100%
2.5.6	Sensibiliser les partenaires à la SSI du ministère.		100%	0%	100%
2.6	Etablir un filtrage à l'accès Internet		33%	50%	

II.4 – LA SECURITE DANS LE SI

La sécurité d'un système d'information permet de limiter les risques qui peuvent corrompre le bon fonctionnement du système d'information. Cela sert également à limiter les impacts économiques et juridiques.

Il est nécessaire pour les organisations de connaitre leurs ressources en matière de sécurité de système d'information afin de garantir l'intégrité et la sécurité de leurs données et de celles de leurs clients.

Il y a deux types de sécurisation pour le système d'information :

- La sécurité logique : politique de mots de passe, sensibilisation des utilisateurs, restriction des connexions au réseau et le stockage des données sur les serveurs…
- La sécurité physique : Sécurisation des données de l'entreprise, sécurisation des postes informatique, sécurisation des salles informatique, sécurisation des sauvegardes…

II.4.1 – SECURISATION LOGIQUE

Sensibilisation des utilisateurs

Certaines failles de sécurité ne peuvent pas être bloquées directement, c'est pour cela que la vigilance des utilisateurs est importante. La mise en place d'une charte informatique explicative et détaillant différents points est nécessaire afin d'assurer une première couche de sécurité.

Sécurisation de la messagerie

Le service de messagerie est assuré par Microsoft Office. La sécurisation des serveurs et de l'infrastructure est prise en charge par Microsoft, nous devons simplement ajuster certains paramètres vis-à-vis des e-mails de phishing par exemple.

Sécurisation des postes informatiques

Afin de sécuriser les postes des utilisateurs, il est nécessaire de maintenir les postes informatiques à jour, que ce soit au niveau du système d'exploitation mais également au niveau des logiciels installés. Ces mises à jour sont effectuées automatiquement via un serveur et des stratégies de groupe, de manière programmée.

Il est également obligatoire de définir des politiques de sécurité sur les postes utilisateurs à savoir :

- Blocage des périphériques externes (clefs USB, disque dur externe, clef bootable)
- Mettre un mot de passe dans le BIOS
- Chiffrer le poste de l'utilisateur
- Verrouiller automatiquement la session de l'utilisateur après 5 minutes d'inactivité
- Obliger l'utilisateur à changer son mot de passe tous les 3 mois
- Bloquer l'enregistrement de mots de passe dans le navigateur
- Monter automatiquement les lecteurs réseau

Sécurisation du réseau local

La sécurité du réseau local est assurée par le pare-feu de notre opérateur SFR, ce sont des pare-feu manageable et intelligents qui nous permettent de réseau les flux entrants sur le réseau en créant des règles spécifiques, des listes blanches et des listes noires d'autorisation.

La mise en place de réseaux virtuels, VLANs permet de cloisonner les différentes parties de l'infrastructure par tiers.

- Tier 2 : Sans restriction d'accès (emplacement du serveur TSE par exemple)
- Tier 1 : Sécurisé (emplacement des serveurs de fichier par exemple)
- Tier 0 : Sécurisé (emplacement des contrôleurs de domaine)

Le réseau WIFI mis en place sera couplé à une authentification Active Directory (via RADIUS), et les utilisateurs externes seront invités à se connecter sur un réseau isolé (invité).

Pour bloquer les virus, nous utilisons la solution antivirus ESET. L'anti-virus est installé et configuré sur tous les postes clients et tous les serveurs de l'infrastructure. Il se passe place parmi les leaders du marché, par sa robustesse et sa facilité d'installation.

Cette solution offre également une réponse aux ransomwares car elle permet de bloquer les ransomwares.

Politique de mots de passe

Dans le but de sécuriser les informations de l'entreprise, il est recommandé d'utiliser des mots de passe fort, avec des majuscules, minuscules, caractères spéciaux, 15 caractères minimum et qui ne contient pas 3 lettres du nom ou du prénom qui se suivent, et pas un ancien mot de passe.

Le mot de passe devra également être changé tous les 90 jours, il ne doit pas être stocké sur l'ordinateur ou tout autre support sous quelconque forme que ce soit.

II.4.2 – SECURISATION PHYSIQUE

Sécurisation des données de l'entreprise

Les serveurs informatiques sont tous équipés de modules double alimentation afin de pallier la panne de l'une d'entre elles et d'envoyer une alerte à notre supervision. De plus, nous possédons une garantie matérielle sur tous les équipements, avec une intervention en 4h. Cela nous permet un rétablissement rapide en cas de panne.

Pour les fichiers informatiques, nous avons mis en place des serveurs de fichiers qui sont sauvegardés jusqu'à J-365. Nous pouvons donc récupérer un fichier jusqu'à 1 an auparavant.

La politique de sauvegarde se trouve en annexe.

Sécurisation des accès opérateur

L'accès à internet dans l'entreprise se faire par la présence de deux liaisons optiques et de deux routeurs pour chaque site.

Il y a un lien primaire et un lien secondaire. Nous utilisons le protocole VRRP afin de faire une passerelle virtuelle et qu'en cas de coupure, cela soit invisible pour les utilisateurs. Cela assure une continuité de service.

Cette solution nous permet d'avoir une haute disponibilité, proche de 99.99% et un taux de délivrance des paquets de 99.995%.

Sécurisation des liaisons du réseau local

Tous les sites bénéficient d'une sécurité par couche grâce à la redondance des liens réseau et des équipements.

Afin de garantir cette sécurité, nous utilisons différentes technologies :

- Une sécurité digne d'une solution « ceinture bretelle »
- Une agrégation de liens entre les cœurs de réseau.

Sur tous les sites, nous pouvons perdre jusqu'à une liaison par équipement sans qu'il y ait de coupure de service engageant une indisponibilité.

Sécurité électrique des équipements

Les équipements informatiques sont très sensibles aux microcoupures et aux variations de fréquence électrique, il est donc important de mettre en place un système permettant de résoudre ces soucis.

Une coupure électrique peut entrainer l'arrêt complet de l'infrastructure et même pire, la perte des données.

Dans le but de garantir une continuité de service et d'améliorer la sécurité des équipements actifs du réseau (switches, routeurs, serveurs…), nous avons mis en place des onduleurs. Cela permet, pendant un court terme, de fournir l'alimentation électrique aux équipements pendant une coupure. Si l'électricité n'est pas rétablie, cela laisse le temps d'éteindre l'infrastructure avec sa procédure normale.

Refroidissement des salles informatiques

Les équipements informatiques génèrent une grande quantité de chaleur. Si les équipements ne sont pas maintenus au frais, ils risquent de tomber en panne et de réduire considérablement leur durée de vie.

Pour des raisons économiques et écologiques, nous avons pris la décision de prendre des baies climatisées, ce qui permet de refroidir uniquement la baie et pas la salle. Cela a également un impact écologique positif, car l'énergie consommée est réduite.

Au vu de la croissance de l'entreprise, nous avons décidé de partir sur des baies de 42 unités.

Vous trouverez en annexe la documentation de cette baie.

Accès contrôlé aux salles informatiques

L'accès aux salles informatique se fait par badge unipersonnel ainsi qu'un code personnel afin d'identifier toute personne.

Via le logiciel de gestion des accès, il sera possible de récupérer l'heure d'arrivée, l'heure de sortie. Les entrées et les sorties sont filmées par des caméras de surveillance et la vidéo est sauvegarder pendant 30 jours. Une déclaration à la CNIL a été faite concernant la conservation de ces données.

Ces informations sont également cruciales en cas de départ d'incendie afin de savoir si quelqu'un se trouve dans les salles informatiques.

Il est également interdit pour des raisons de sécurité d'intervenir seul dans une salle informatique.

Les autorisations d'accès seront accordées sur demande au Directeur des services d'information, et la demande devra mentionner l'objectif de l'intervention et l'impact possible.

II.5 – PCA / PRA

II.5.1 – PCA

Le Plan de Continuité d'Activité (PCA) aura pour objectif de garantir la possibilité de continuer à travailler à la suite d'un évènement qui perturberait le fonctionnement habituel de l'entreprise.

Le PCA répond à plusieurs objectifs permettant la continuité des services critiques. Il en existe deux qu'il est impératif de ne pas oublier, la perte des données maximale admissible (PDAM) et la durée maximale d'indisponibilité admissible (DMIA). La PDAM introduit une notion d'intégrité et d'actualité des données, tandis que la DMIA détermine l'objectif de délai de reprise.

Le PCA sera mis en place à travers plusieurs mesures informatiques. Equipements :

- Serveurs : notre architecture système nous permet d'assurer une continuité d'activité au niveau des serveurs, grâce à un système de redondance. En effet, si l'un des deux serveurs venait à dysfonctionner, l'autre serveur prendrait le relai ;
- Réseau : Nous remplaçons les switchs mis en place, et conservons 2 switchs de spare ainsi qu'une partie des anciens switchs ;
- Postes clients : Nous remplaçons là aussi l'intégralité des postes clients et, comme pour les équipements réseaux, nous conservons une partie des anciens postes en guise de spare.

Stockage :
Les locaux contenant le matériel critique (serveurs, baie de stockage, onduleurs) devront être fermés à clé et l'accès sera restreint aux personnes habilitées.

Procédures :
Nous avons prévu de rédiger des procédures de déploiement, exploitation et installation pour les sauvegarder dans notre base de données. Des mises à jour des procédures sont prévues lors d'évolution ou de modification du parc informatique.

Électricité :
Nous équiperons les serveurs d'onduleurs leur permettant de continuer à fonctionner 20 minutes supplémentaires lors de coupures électriques afin de s'éteindre proprement.
L'onduleur va aussi nous permettre de protéger l'infrastructure de la foudre ou des perturbations potentielles du réseau électrique.

II.5.2 – PRA

À la différence du PCA, qui consistera à assurer la continuité de l'activité sans subir aucune interruption de service, le Plan de Reprise d'Activité (PRA), lui, assurera la reconstruction de l'infrastructure informatique ainsi que la remise en route des applications importantes de l'entreprise

Il y a de gros enjeux car si l'entreprise perd tous ces documents elle ne pourra peut-être plus repartir.

Le système de sauvegarde que nous vous proposons et l'une des plus grosses mesures du plan de reprise d'activité. Par exemple, si un bâtiment prend feu nous pouvons repartir en quelques heures grâce à la sauvegarde de l'autre bâtiment.

Grace aux sauvegardes complètes nous sommes capables de reproduire à l'identique votre infrastructure complète.

II.6 – RTO / RPO

En cas de panne, le groupe WOOD bénéficiera d'un meilleur temps de rétablissement de service. Cela permet de limiter l'impact financier, pendant laquelle l'entreprise ne produira aucun produit.

Les délais de rétablissement établis dans le tableau ci-dessous sont basés sur des systèmes redondants mais également sur l'engagement vis-à-vis de plusieurs prestataires.

Service	Impact sur la production	Durée d'interruption accepté (/mois)	Temps de rétablissement estimé
Serveur de sauvegarde	Majeur	2 heures	Inférieur à 1 heure
Réseau LAN	Majeur	15 minutes	Inférieur à 3 minutes
Réseau WAN	Majeur	15 minutes	Inférieur à 3 minutes
Serveurs de fichiers	Majeur	15 minutes	Inférieur à 3 minutes
Active Directory	Majeur	30 minutes	Inférieur à 3 minutes
Accès WI-FI	Mineur	5 heures	Inférieur à 3 heures
Supervision	Modéré	3 heures	Inférieur à 1 heure
Service d'assistance aux utilisateurs	Mineur	3 heures (astreinte disponible)	Inférieur à 1 heure
DNS	Majeur	30 minutes	Inférieur à 3 minutes
DHCP	Majeur	30 minutes	Inférieur à 3 minutes

III – PARTIE FINANCIERE

L'un des facteurs les plus importants dans les projets informatiques est le budget. En effet, dans de nombreux projets, le risque est qu'il soit dépassé, c'est pourquoi il est nécessaire d'organiser un suivi des coûts.

Nous identifions deux principales sources de dépenses :

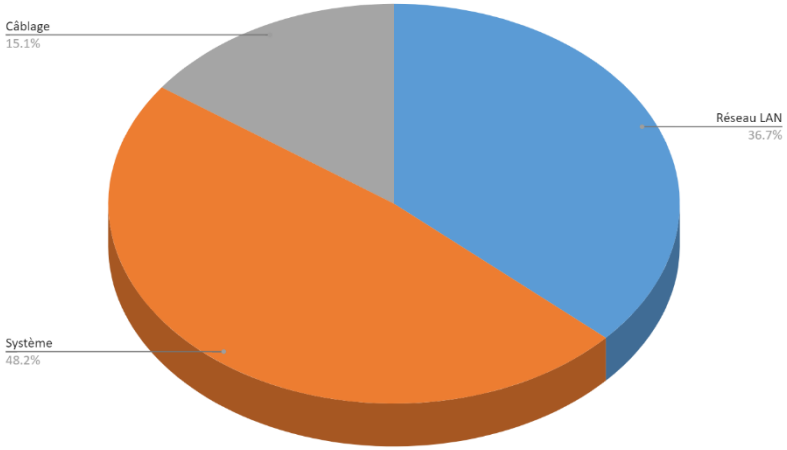
- L'OPEX, relatif aux couts d'exploitation ;
- Le CAPEX, relatif aux couts d'investissement ;
- Le coût humain, relatif à la main d'œuvre.

III.1 – CAPEX

Voici un tableau rationnalisant les couts d'investissement du projet.

Investissement (CAPEX)				
RESEAU LAN	Description	Prix unitaire HT €	Quantité	Total
Cœur de réseau	Switch 3750X – 24 ports -	3,232.24	10	32,322.40 €
Switch d'accès	Switch C2960X - 48 ports - 2 x 1 G SFP	1,552.64	7	10,868.48 €
Module SFP+ 10 G	SFP+ 10G SR	16.00	50	800.00 €
Fibre monomode	Fibre monomode LC	1,249.80	50	62,490.00 €
Module FIBRE 10G	4 ports fibre supplémentaire	295.00	21	6,195.00 €
Borne WIFI RUCKUS	Borne Wi-Fi	270.20	30	8,106.00 €
ZD1200	Contrôleur WIFI	1,414.00	5	7,070.00 €
Baie informatique	Baie climatisée 42U	1,400.00	5	7,000.00 €
				134,851.88 €

Système	Description	Prix unitaire HT €	Quantité	Total
Serveurs Hyperviseur	DELL R610	2400	2	9,600.00 €
Extension mémoire hyperviseurs	RAM 16GB - RAM Crucial	120.99	18	4,355.64 €
Serveur AD	Carte PCI 10GB + SFP+	200	2	800.00 €
Stockage serveur	Licence Idrac entreprise	444	2	1,776.00 €
NAS machines virtuelles	Synology SA3600	6332	1	12,664.00 €
Stockage NAS machines virtuelles	Seagate SkyHawk AI Surveillance HDD 5TB	163	10	3,260.00 €
Serveur de backup	Synplogy RackStation RS1219+	1163	1	2,326.00 €
PC fixe bureautique	DELL Vostro Desktop 3470 format SFF	385	41	15,785.00 €
Station de travail	DELL 3630	1500	18	27,000.00 €
Station TSE	Raspberry PI	30	110	3,300.00 €
PC Portables	DELL Latitude 5510	874	110	96,140.00 €
				177,006.64 €
Câblage (RJ45)		120	462	**55 540 €**



III.2 – OPEX

Voici un tableau rationnalisant les couts de fonctionnement du projet.

Fonctionnement (OPEX)				
Réseau LAN	Description	Prix unitaire HT €	Quantité	Total
Switchs 3750x	Contrat de maintenance à l'année : Cisco 3750X pour une GTR 4h	1565	10	**15,650.00 €**
Switchs 2960x	Contrat de maintenance à l'année : Cisco 2960X pour une GTR 4h	813	7	**5,691.00 €**
				21,341.00 €
Réseau WAN	Description	Prix unitaire HT €	Quantité	Total
Lien principal	Fibre Optique 200Mb/s (par mois)	899	3	2697.00
Lien principal	SDSL 20Mb/s (par mois)	600	2	1200.00
Lien secondaire	SDSL 20Mb/s (par mois)	400	2	800.00
Lien secondaire	ADSL 4 Mb/s	300	3	900.00
				67,164.00 €

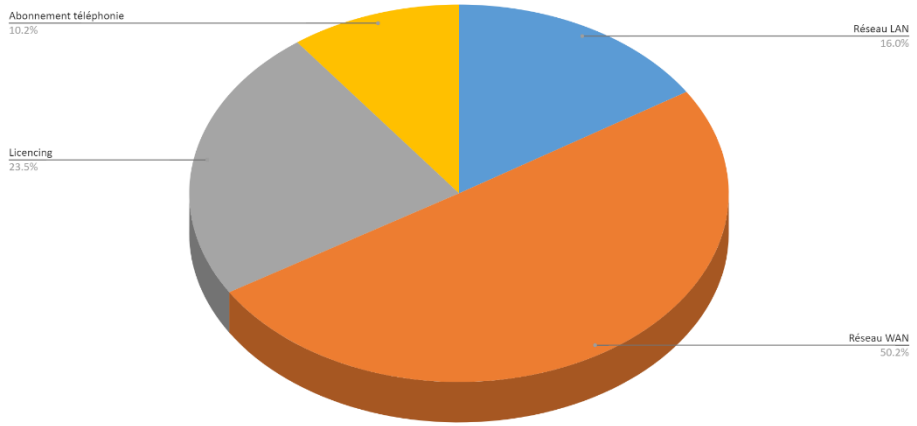
Téléphonie (caution)	SOFTPHONE	Caution Yealink CP920 Pas de caution, prêté par le fournisseur dans le contrat
Lille	0	0
Annecy	0	0
Dax	0	0
Mâcon	X	0
Brest	X	0
	0.00 €	0.00 €
	0	

Téléphonie (abonnement)	Coût abonnement annuel
Lille	7,644.08€
Annecy	2,744.58€
Dax	1,366.00€
Mâcon	935.00€
Brest	995.00€
	13,685 €

Licences		Prix unitaire HT €	Quantité	Total
Windows Serveur Datacenter		4,495.00 €	2	8,990.00 €
Licence VMWARE PME	2700+900+ 1200	4,800.00 €	1	4,800.00 €
Windows Server Standard		576.00 €	10	5,760.00 €
CAL		27.00 €	50	1,350.00 €
Office 365 (1 an)		10.50 €	194	2,037.00 €

VEEAM Backup (5 ans)		1,100.00 €	5	5,500.00 €
TeamViewer (pour 200 PC)		124.90 €	1	124.90 €
Zabbix				0.00 €
Antivirus		15.00 €	194	2,910.00 €
				31,471.90 €

Réseau LAN	**21,341.00 €**
Réseau WAN	**67,164.00 €**
Licencing	**31,471.90 €**
Abonnement téléphonie	**13,684.66 €**
Caution téléphones IP	**0.00 €**
	133,661.56 €



III.3 – COUT HUMAIN

À raison de 7h de travail par jour et par intervenant, nous avons estimé les couts de main d'œuvre qu'induit ce projet.

Nous retrouvons trois grands types d'intervenants avec leur coût horaire :

- Techniciens : 35€/h
- Administrateur : 45€/h
- Ingénieur : 65€/h

Chaque intervenant ne participe pas à toutes les phases, afin de calculer le coût humain de ce projet, les membres de l'équipe ont été affectés aux différentes tâches en se basant sur le planning de déploiement.

Voici les intervenants et leur présence sur les différentes phases :

4 techniciens :

- Pré-configuration du matériel : 10j/10
- Installation sur tous les sites : 38j/38

4 administrateurs :

- Pré-configuration du matériel : 8j/10
- Installation sur tous les sites : 38j/38

2 ingénieurs :

- Pré-configuration du matériel : 10j/10
- Installation sur tous les sites 7j/38

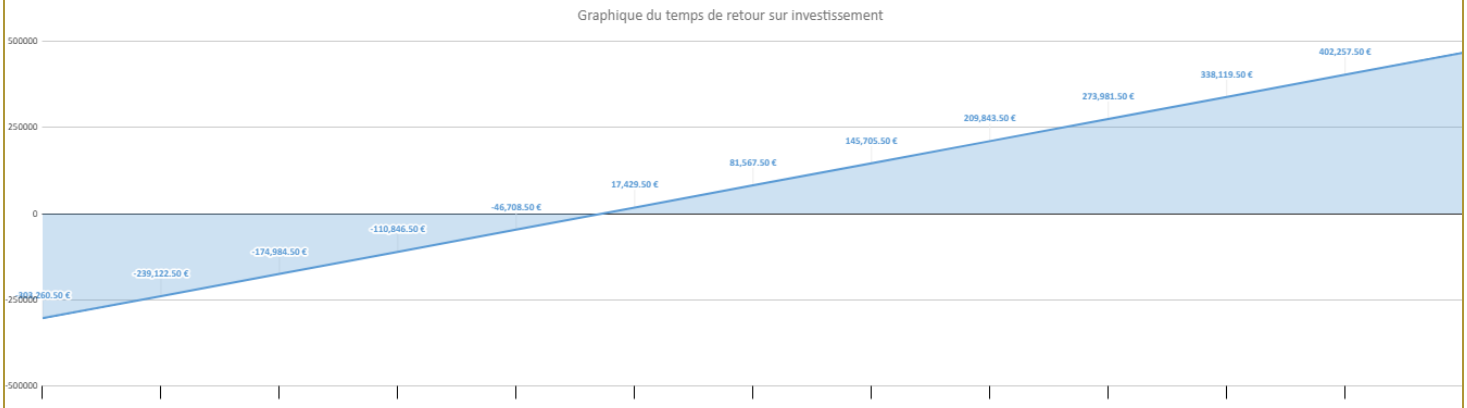
Le coût humain de ce projet s'élève donc à **120 470€**.

III.4 – TRI

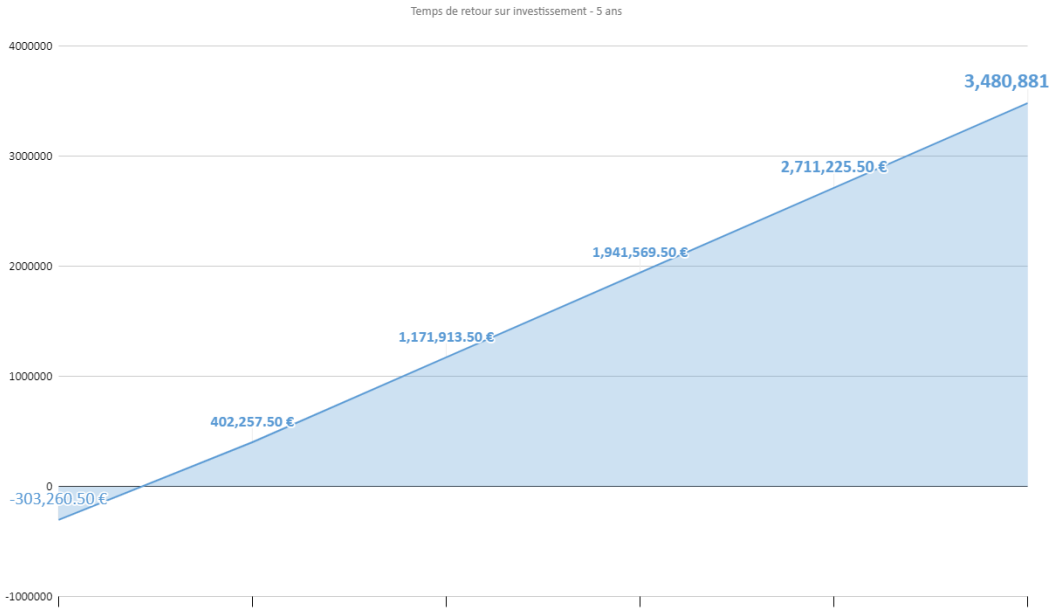
Afin de prouver la rationalité de l'investissement lié au projet, nous avons calculé le temps de retour sur investissement. Le calcul est basé sur l'investissement projet calculé dans la section CAPEX, le coût d'exploitation avant le projet et le coût d'exploitation obtenu grâce à la solution.

Le TRI se calcule de la façon suivante :

(Investissement + fonctionnement) – (réduction des pertes + réduction du coût de fonctionnement)



D'après nos calculs, nous pouvons constater que nous avons un temps de retour sur investissement positif à partir du sixième mois.

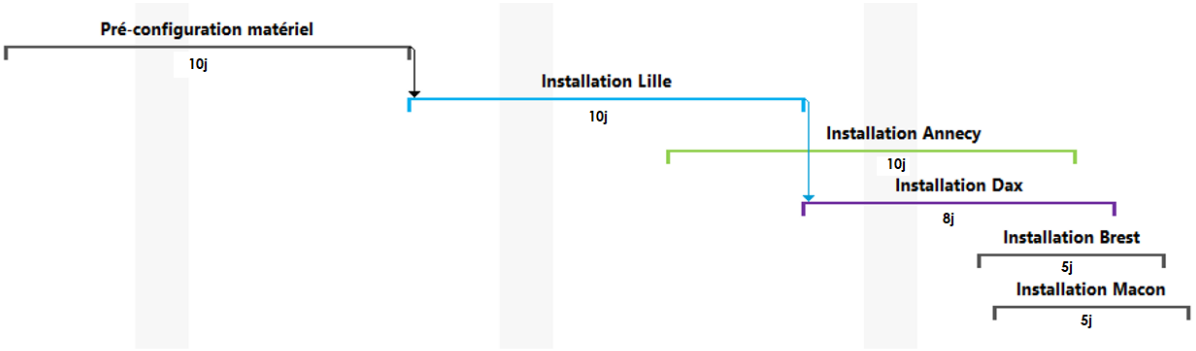


Ci-dessus, l'évolution des gains sur cinq années.

IV – DEPLOIEMENT DU PROJET

IV.1 – PLANIFICATION DU DEPLOIEMENT

Pour le déploiement de ce projet, nous prévoyons un temps total de 48 jours ouvrés.



IV.2 – TESTS DE RECETTAGE

Pour ce projet, nous avons mis en place des tests de recettage. Leur objectif est de vérifier le fonctionnement normal des équipements pendant le processus d'installation. Ces tests sont simples et complets, mais sont essentiels au bon fonctionnement du projet. Leurs résultats permettent à l'entreprise de services et au client d'avoir une compréhension transparente des actions à réaliser. Enfin, la signature permet de vérifier la bonne installation de l'équipement et la satisfaction du client des opérations effectuées.

Si les normes du client ne sont pas respectées, le client a le droit de ne pas vérifier le test et a le droit de demander de nouvelles interventions jusqu'à ce que les normes définies soient respectées.

En cas de litige, ces documents ont valeur légale. Ils peuvent mettre en évidence la cohérence de l'installation lorsque le technicien est absent. Par conséquent, lors du départ du technicien, le client sera responsable de l'équipement, et en aucun cas il ne pourra contester auprès de son prestataire de services pour non-respect des exigences d'installation.

V – ITIL

Aujourd'hui, l'entreprise ne peut pas optimiser son SI. Par conséquent, nous vous recommandons d'adopter le modèle ITIL, qui apportera de nombreux avantages au groupe :

- Gestion du changement ;
- La mise en place de CMDB permet de collecter et inventorier les matériels composants. Nous utiliserons la solution GLPI ;
- Utiliser l'outil de ticketing GLPI pour la gestion des incidents.

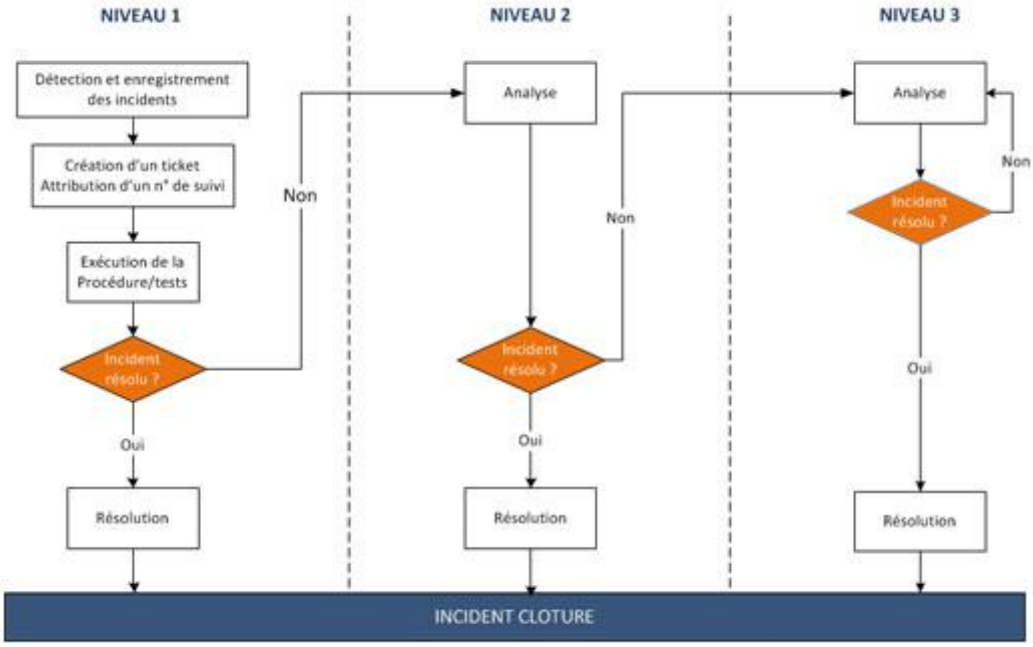
Par conséquent, ITIL va aider à gagner du temps pour effectuer les opérations, réduire les coûts de maintenance, définir les rôles et les responsabilités avec plus de précision et s'adapter plus facilement aux besoins des clients. Cela conduira à une meilleure satisfaction des utilisateurs et améliorera ainsi l'image du SI de l'entreprise.

En cas de problème avec le SI, l'utilisateur ouvrira un ticket d'incident ou appellera l'assistance. Selon cette demande, un système de 3 niveaux sera engagé.

Le premier est un technicien de base qui sera le premier intervenant du problème et tentera de le à distance. Si le problème dépasse ses capacités, il fera appel au deuxième niveau.

Le second niveau concerne les personnes plus qualifiées et expérimentées dans le domaine technique, ou un besoin d'intervention sur site.

Le troisième niveau correspond à la maintenance par les constructeurs (comme Sophos), qui pourront résoudre les problèmes de configuration.



VI – LES SLA

L'entreprise WOOD s'attend à ce que la disponibilité de son SI soit élevée. Une indisponibilité de service peut rapidement devenir très problématique. Afin de réduire la perte financière possible, et augmenter la disponibilité du SI. Diverses mesures ont été prises pour réduire le nombre et l'impact des interruptions de service pendant la mise en œuvre du projet. Le tableau suivant est un exemple des difficultés que WOOD peut rencontrer. Il indique comment les résoudre et combien de temps ils dureront.

Souci rencontré	Indisponibilité	Temps de rétablissement	Impact	Moyen mis en œuvre
Panne d'un commutateur	-Téléphonie -Wifi -Réseau filaire	-Sous 1h pour les éléments importants -Sous 24h ouvré pour un retour total à la normale	Important	- Utilisation de redondance de lien sur les postes et commutateur ; - Téléphonie et Wifi croisé pour proposer un wifi dégradé et une partie des téléphones opérationnelle ; - Remplacement du commutateur à j+1.
Coupure du lien principal internet	Coupure de quelques secondes	Rétablissement total en 4h maximum	Quasiment inexistant	-Liens redondés avec routeur opérateur sur chaque site ; -Bascule automatique de lien faite par le routeur en cas de coupure ; -SLA opérateur de 4h.
Panne d'un disque serveur	Pas d'indisponibilité	Rétablissement à la normale sous 48h	Inexistant	-Redondance des disques.
Suppression d'un fichier	Pas d'indisponibilité	-Restauration en moins de 15 mins pour un fichier de taille moyenne ; -Restauration en moins d'une heure pour un fichier volumineux.	Quasiment inexistant	- Utilisation de la fonction « Clichés instantanés » ; - Sauvegardes journalières.

VII – GREEN IT – DEEE

Soucieux de notre impact environnemental, tous les équipements que nous installons sont scrupuleusement étudiés et choisis afin de réduire l'empreinte carbone ainsi que la consommation électrique. Tout d'abord, auprès de nos fournisseurs, nous souhaitons qu'eux aussi soit engagés dans une démarche de respect environnemental pour la fabrication de leurs équipements. De plus, nous nous engageons dans une démarche de recyclage des matériels qui doivent être remplaces.

Nous travaillons avec des partenaires sélectionnés pour leur qualité afin de répondre au mieux à la mise aux normes DEEE. Les entreprises de recyclage assurent le ramassage et le recyclage ou la destruction des déchets de différentes catégories : le recyclage de gobelets plastique, canettes, le recyclage de déchets informatiques, le recyclage de cartouches d'encre, le recyclage de papier en entreprise et cartons, etc.

Afin de répondre à ce besoin de recyclage, nous vous conseillons la société Valotik, dont sa localisation se trouve à 27 km de Lille. Nous avons privilégié les contrats locaux pour des raisons d'écologie (transport des déchets, fiabilité, etc.).

La société VALOTIK nous propose de mettre en place un conteneur maritime de 50 pieds.

Une fois que le conteneur est rempli, nous réalisons par e-mail une demande de collecte auprès de la société, qui passera sous 24h ouvrées pour y déposer un container vide et récupérer le container plein.

Le prix de la prestation est de 90€/mois pour la benne et 4000€ un conteneur rempli à détruire.

VALOTIK fait également de la valorisation de matériel ce qui permet de réduire le prix du recyclage.

La pollution informatique existe bel et bien. Les émissions annuelles de CO2 liées à l'industrie informatique seraient deux fois supérieures à celles de l'industrie aéronautique commerciale. Des mesures simples permettent de polluer moins :

- Réduction de la facture électrique (recours au cloud computing et à la virtualisation) ;
- Réduction d'énergie des processeurs (utiliser des processeurs basse consommation) ;
- Vidéoconférence pour éviter les voyages en voitures, en avion, etc. ;
- Diminution des produits chimiques dangereux pour la fabrication des machines ;
- Utilisation de matériaux recyclés ;
- Réduction des coûts de matériel ;
- Réduction de l'empreinte carbone (entre autres en mesurant ses émissions globales de CO2 afin de mieux les réduire) ;
- Adopter le recyclage.

Il existe deux façons de définir le concept de Green-IT, appelé aussi « informatique verte » ou encore « éco-TIC » :

- C'est d'une part l'ensemble des technologies qui permettent aux entreprises de diminuer leur empreinte carbone, de réduire leurs émissions de gaz à effet de serre, leur consommation énergétique, etc. En somme, ce sont toutes les technologies qui vont permettre de réduire l'impact écologique dans le domaine de l'informatique (IT pour informatique) ;
- D'autre part, ce sont les principes et politiques économiques, sociales et philosophiques qui sont adoptés dans les entreprises écoresponsables afin de favoriser le développement durable.

VIII – BYOD / CYOD

VIII.1 – BYOD

BYOD est une pratique consistant à utiliser des appareils personnels (téléphones, ordinateurs portables, tablettes, etc.) dans un environnement professionnel. Ces appareils facilitent l'accès aux informations et aux applications de l'entreprise. Cette approche soulève des problèmes de sécurité de l'information et de protection des données, ainsi que des problèmes sociaux et juridiques.

Avec la direction du Groupe, pour des raisons de sécurité et de responsabilité, les postes individuels ne seront pas acceptés au sein de l'entreprise. Selon la loi, en raison de son affiliation personnelle, nous ne pouvons pas accéder au poste.

En revanche, les téléphones personnels des utilisateurs équipés de softphones seront exonérés de cette règle. Le but de cette exception est de faciliter l'utilisation du téléphone, limitant ainsi le nombre de téléphone mobile pour les employés nomades.

Cette particularité aura un impact sur la gestion et la sécurité de la société. Ces téléphones ne seront interconnectés avec la téléphonie de l'entreprise et les boîtes aux lettres professionnelles des employés. Les employés ne sont pas autorisés à utiliser leurs appareils personnels pour accéder aux données de l'entreprise. Dans les locaux de l'entreprise, ces téléphones pourront se connecter à un wifi spécifique et sécurisé. Il fournit spécifiquement une connexion garantie pour l'accès téléphonique et Internet.

VIII.2 – CYOD

CYOD est une habitude pour les employés de choisir leur propre équipement dans le catalogue de terminaux approuvé par l'entreprise. Par conséquent, ces configurations sont approuvées et intégrées dans l'entreprise, évitant ainsi tout problème lié à la législation et à la protection des données. Cependant, le matériel sélectionné n'est que la propriété professionnelle de l'entreprise.

Bien que cette solution soit de plus en plus envisagée, elle n'est pas aussi satisfaisante que le BYOD pour les salariés, mais elle est plus sécurisée pour les entreprises.

IX – CONCLUSION

Le projet de refonte du système d'information de Wood répond donc aux critères de disponibilité et de coût. Il ne dépasse pas un budget et offre une disponibilité avancée en cas de panne d'équipement. En effet, tous les équipements ont été remplacés et peuvent être garantis en cas de panne dans les prochaines années.

X – ANNEXES

X.1 – CHARTE INFORMATIQUE

Charte informatique de l'entreprise

Entreprise Wood

D'une manière générale, l'utilisateur doit s'imposer le respect des lois et, notamment, celles relatives aux publications à caractère injurieux, raciste, pornographique, diffamatoire, sur le harcèlement sexuel/moral.

1) Sécuriser l'accès au compte

Le contrôle d'accès logique permet d'identifier toute personne utilisant un ordinateur.

Cette identification permet, à chaque connexion, l'attribution de droits et privilèges propres à chaque utilisateur sur les ressources du système dont il a besoin pour son activité.

Une identification (login + mot de passe) unique est confiée à chaque utilisateur. Ce dernier est personnellement responsable de l'utilisation qui peut en être faite, et ne doit en aucun cas la communiquer.

Chaque mot de passe doit obligatoirement être modifié selon la fréquence suivante : 6 mois. Un mot de passe doit, pour être efficace, comporter 8 caractères alphanumériques. Il ne doit pas être, notamment, identique au login, même en inversant les caractères, comporter le nom et/ou prénom de l'utilisateur ou de membres de sa famille, le numéro de téléphone, la marque de la voiture ou toute référence à quelque chose appartenant à l'utilisateur, être un mot ou une liste de mots du dictionnaire ou un nom propre, nom de lieu, être écrit sur un document et être communiqué à un tiers.

2) Courrier électronique

Les éléments de fonctionnement de la messagerie à considérer sont les suivants.

Un message envoyé par Internet peut potentiellement être intercepté, même illégalement, et lu par n'importe qui.

En conséquence, aucune information stratégique ne doit circuler de cette manière, sauf à la crypter.

Il est interdit d'utiliser des services d'un site web spécialisé dans la messagerie.

Lors du départ d'un collaborateur, il doit être indiqué au responsable de l'administration du système ce qu'il sera fait des fichiers et courriers électroniques de l'utilisateur.

Les messages électroniques sont conservés sur le serveur de messagerie pendant une période de 30 jours et il existe des copies de sauvegarde pendant une période de 90 jours.

Ces copies de sauvegarde conservent tous les messages au moment où ils passent sur le serveur de messagerie, même s'ils ont été supprimés ensuite par leur destinataire.

2.1 Utilisation privée de la messagerie

L'utilisation du courrier électronique à des fins personnelles est autorisée dans des proportions raisonnables et à la condition de ne pas affecter le trafic normal des messages professionnels.

2.2 Contrôle de l'usage

Dans l'hypothèse la plus courante, le contrôle éventuellement mis en œuvre porte sur :

- le nombre des messages échangés ;
- la taille des messages échangés ;
- le format des pièces jointes.

3) Utilisation d'Internet

Chaque utilisateur doit prendre conscience qu'il est dangereux pour l'entreprise :

- de communiquer à des tiers des informations techniques concernant son matériel ;
- de connecter un micro à Internet via un modem :
- de diffuser des informations sur l'entreprise via des sites Internet ;
- de participer à des forums (même professionnels) ;
- de participer à des conversations en ligne (« chat »).

3.1 Utilisation d'Internet à des fins privées

L'utilisation d'Internet à des fins privées est tolérée dans des limites raisonnables et à condition que la navigation n'entrave pas l'accès professionnel.

3.2 Contrôles de l'usage

Dans l'hypothèse la plus courante, les contrôles portent sur :

- les durées des connexions ;
- les sites les plus visités ;

La politique et les modalités des contrôles font l'objet de discussions avec les représentants du personnel.

4) Pare-feu

Le pare-feu vérifie tout le trafic sortant de l'entreprise, aussi bien local que distant. Il vérifie également le trafic entrant constitué de fichiers.

Il détient toutes les traces de l'activité qui transite par lui s'agissant :

de la navigation sur Internet : sites visités, heures des visites, éléments téléchargés et leur nature (textes, images, vidéos ou logiciels) ;

- des messages envoyés et reçus : expéditeur, destinataire(s), objet, nature de la pièce jointe et le texte du message.

Il filtre les URL des sites non autorisés par le principe de la liste noire. Les catégories des sites visés sont les sites diffusant des données de nature pornographique, pédophile, raciste ou incitant à la haine raciale, révisionniste ou contenant des données jugées comme offensantes

5) Sauvegardes

La mise en œuvre du système de sécurité ne comporte pas des dispositifs de sauvegarde des informations et un dispositif miroir destiné à doubler le système en cas de défaillance.

Ceci implique, entre autres, que la suppression par un utilisateur d'un fichier de son disque dur n'est pas absolue et qu'il en reste une copie :

- sur le dispositif de sauvegarde ou miroir ;
- sur le serveur ;
- sur le proxy ;
- sur le firewall (pare-feu) ;
- chez le fournisseur d'accès.

Fait à le / /

Signature de l'employeur

X.2 – COUTS PAR SITE

X.2.1 – ANNECY

RESEAU LAN	Description	Prix unitaire HT €	Quantité	total
Cœur de réseau	Switch 3750X – 24 ports -	3,164.27	2	6,328.54 €
Switch d'accès	Switch C2960X - 48 ports - 2 x 1 G SFP	1,498.26	2	2,996.52 €
Module SFP+ 10 G	SFP+ 10G SR	14.00	10	140.00 €
Fibre monomode LC	Fibre monomode LC	4.16	10	41.60 €
Module fibre 3750x	4 ports fibre supplémentaire	512.62	2	1,025.24 €
	Contrat de maintenance à l'année : C2960x + 3750X pour une GTR 4h			2,378.00 €
Borne Wi-Fi - RUCKUS R320	Borne Wi-Fi	270.62 €	8	2,164.96 €
ZD1200 - Fastnet (licences incluses)	Contrôleur WIFI	1,414 €	1	1,414.01 €
Baie informatique	Baie climatisée 42U	1,400 €	1	1,400.00 €
				16,488.87 €

RESEAU WAN	Description	Prix unitaire HT €	Quantité	total
Lien principale	Fibre optique 200Mb/s	899 €/mois	1	1292.00
Lien secondaire	ADSL 4 Mb/s	300 €/mois	1	855.00
				25,764.00 €

TELEPHONIE	Caution téléphones (premiere année seulement)	Coût annuel abonnement HT	Quantité	total
46 employés	0.00 €	2,744.58 €	53 téléphones	**2,744.58 €**

PARC CLIENT	Description	Prix unitaire HT €	Quantité	total
PC fixe bureautique	DELL Vostro Desktop 3470 format SFF	385	6	2,310.00 €
Station de travail	DELL 3630	1500	15	22,500.00 €
Station TSE	Raspberry PI	30	5	150.00 €
PC Portables	DELL Latitude 5510	874	25	21,850.00 €
				24,960.00 €

Total ANNECY
69,957.45 €

X.2.2 – MACON

RESEAU LAN	Description	Prix unitaire HT €	Quantité	total
Cœur de réseau	Switch 3750X – 24 ports -	3,164.27	2	6,328.54 €
Switch d'accès	Switch C2960X - 48 ports - 2 x 1 G SFP	1,498.26	0	0.00 €
Module SFP+ 10 G	SFP+ 10G SR	14.00	10	140.00 €
Fibre monomode LC	Fibre monomode LC	4.16	10	41.60 €
Module fibre 3750x	4 ports fibre supplémentaire	512.62	2	1,025.24 €
	Contrat de maintenance à l'année : C2960x + 3750X pour une GTR 4h			2,378.00 €
Borne Wi-Fi - RUCKUS R320	Borne Wi-Fi	270.62 €	3	811.86 €
200 - Fastnet (licences inclu	Contrôleur WIFI	1,414 €	1	1,414.01 €
Baie informatique	Baie climatisée 42U	1,400 €	1	1,400.00 €
				9,913.38 €

RESEAU WAN	Description	Prix unitaire HT €	Quantité	total
Lien principal	SDSL 20 Mb/s	600 €/mois	1	700
Lien secondaire	ADSL 4 Mb/s	300 €/mois	1	200
				10,800.00 €

TELEPHONIE	Caution téléphones (premiere année seulement)	Coût annuel abonnement HT	Quantité	total
20 employés	0.00 €	995.30 €	5 téléphones	**995.30 €**

PARC CLIENT	Description	Prix unitaire HT €	Quantité	total
TSE	Raspberry PI	400	10	4,000.00 €
				4,000.00 €

Total MACON
25,708.68 €

X.2.3 – BREST

RESEAU LAN	Description	Prix unitaire HT €	Quantité	total
Cœur de réseau	Switch 3750X – 24 ports -	3,164.27	2	6,328.54 €
Switch d'accès	Switch C2960X - 48 ports - 2 x 1 G SFP	1,498.26	0	0.00 €
Module SFP+ 10 G	SFP+ 10G SR	14.00	10	140.00 €
Fibre monomode LC	Fibre monomode LC	4.16	10	41.60 €
Module fibre 3750x	4 ports fibre supplémentaire	512.62	2	1,025.24 €
	Contrat de maintenance à l'année : C2960x + 3750X pour une GTR 4h			2,378.00 €
Borne Wi-Fi - RUCKUS R320	Borne Wi-Fi	270.62 €	3	811.86 €
200 - Fastnet (licences inclu	Contrôleur WIFI	1,414 €	1	1,414.01 €
Baie informatique	Baie climatisée 42U	1,400 €	1	1,400.00 €
				9,913.38 €

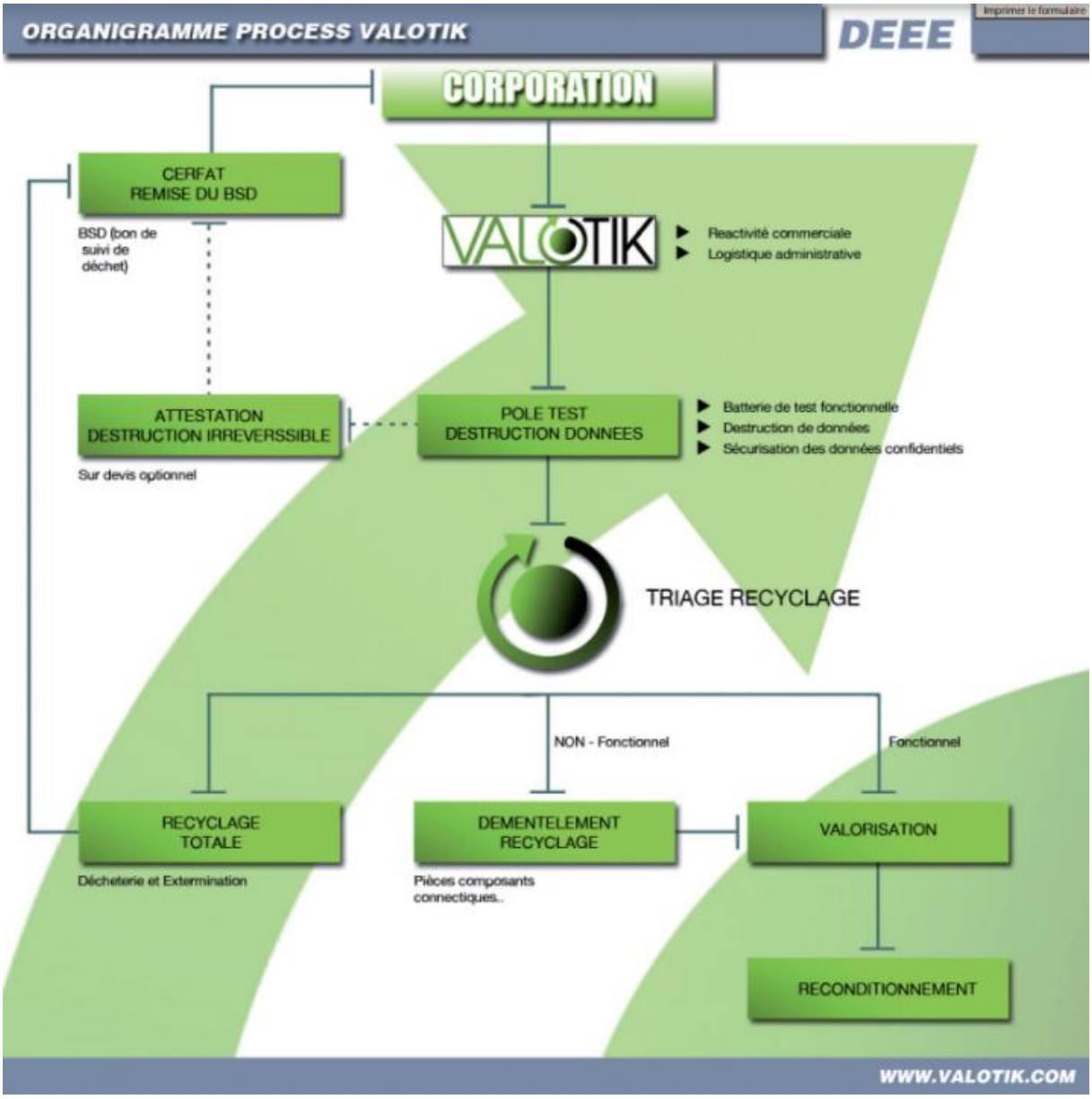
RESEAU WAN	Description	Prix unitaire HT €	Quantité	total
Lien principal	SDSL 20 Mb/s	600 €/mois	1	700
Lien secondaire	ADSL 4 Mb/s	300 €/mois	1	200
				10,800.00 €

TELEPHONIE	Caution téléphones (premiere année seulement)	Coût annuel abonnement HT	Quantité	total
20 employés	0.00 €	995.30 €	5 téléphones	**995.30 €**

PARC CLIENT	Description	Prix unitaire HT €	Quantité	total
TSE	Raspberry PI	400	10	4,000.00 €
				4,000.00 €

Total BREST
25,708.68 €

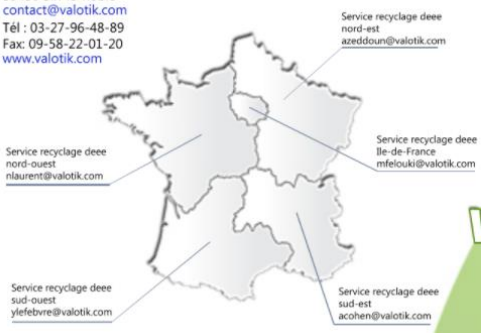
X.3 – VALOTIK


ORGANIGRAMME PROCESS VALOTIK
DEEE
Imprimer le formulaire
CORPORATION
CERFAT
REMISE DU BSD
BSD (bon de suivi de déchet)
VALOTIK
Reactivité commerciale
Logistique administrative
ATTESTATION
DESTRUCTION IRREVERSSIBLE
Sur devis optionnel
POLE TEST
DESTRUCTION DONNEES
Batterie de test fonctionnelle
Destruction de données
Sécurisation des données confidentiels
TRIAGE RECYCLAGE
NON - Fonctionnel
Fonctionnel
RECYCLAGE
TOTALE
Décheterie et Extermination
DEMENTELEMENT
RECYCLAGE
Pièces composants
connectiques..
VALORISATION
RECONDITIONNEMENT
WWW.VALOTIK.COM

www.valotik.com

VALOTIK valorisation & éthique

105 rue Paul Foucault
59450 Sin-le-noble
contact@valotik.com
Tél : 03-27-96-48-89
Fax: 09-58-22-01-20
www.valotik.com



Recylage de parcs informatiques

Valotik est la contraction de Valorisation et Ethique

Valorisation
pour le reconditionnement de matériel informatique.
Le réemploie de Deee afin d'optimiser à plus de 90% le recyclage par le biais de notre process effectué en interne.

Ethique
Pour l'aspect social de Valotik en employant des personnes handicapés et en réduisant la fracture sociale, en équipant des écoles, collèges, de France et des pays en voie de développement tout en donnant une seconde vie au matériel parfois obsolète.

DEEE
Déchets d'équipements électriques et électroniques

« Au bout du compte ce n'est pas tant ce que nous faisons mais ce que nous rendons possible grâce à vous qui est important... L'équipe valotik »

www.valotik.com

Qui sommes nous ?

Notre siège basé dans le nord de la france, Valotik regroupe une équipe de spécialistes possédant des compétences et des savoirs faires acquis dans des domaines d'activité industriels.

- Nous identifions les meilleurs pratiques, et nous optimisons les processus
- Nous améliorons la qualité, nous assurons la conformité des législations.
- Nous réduisons les risques et nous améliorons la productivité de vos DEEE.
- Nous rendons les industries, les entreprises et les Etats plus efficaces grâce à la protection de l'environnement

Soucieux de protéger l'environnement l'expérience respective de nos équipes leurs a donné l'envie d'établir une convergence entre les différents acteurs du processus de recyclage.

VOTRE PROJET :

* Audit expertise , revalorisation, Réemploie
* Entreposage, Emmagasinage, Clonage.
* Security confidential, Quick Audit, Customiser

Notre engagement
« charte qualité » en 10 points :

VALOTIK valorisation & éthique

www.valotik.com

Effacement sécurisé de données, destruction de disque dur.

La destruction, efficace et sécurisée de données sensibles ou confidentielles, est devenue incontournable aujourd'hui.
Nous traitons chaque jour dans notre laboratoire, des disques durs dans un état d'endommagement plus ou moins important. A ce titre, nous pouvons vous certifier qu'un simple effacement ou un simple formatage sont très insuffisants pour effacer réellement le contenu de votre disque dur. Aussi, un disque dur qui semble hors d'usage n'est pas vraiment un frein pour s'approprier vos données.

Recupération de données endommagées ou perdues

Notre service de récupération de données professionnelles n'est pas intrusif et respecte l'intégrité de vos précieuses données, ce qui n'est pas le cas des logiciels téléchargeables sur Internet qui aggravent dans la plupart des cas la perte de vos données. Faites le bon choix avec valotik.
Notre technique et notre expérience offrent la solution optimale avec le minimum de risques.

Notre devis est 100% GRATUIT et réalisé sous quelques heures.
Chaque cas est unique, quelle que soit la situation nous avons une solution.
Notre équipe fonctionne suivant 5 contrôles d'accès de sécurité et travaille couramment pour les PME/PMI, Grands groupes, l'administration et les services de l'État.

VALOTIK valorisation & ethique

- Effacement classique.
- Formatage bas niveau.
- Système Blancco.
- D.O.D Wipe out.
- Destruction physique.

PEEFV
Produits éléctriques et électroniques en fin de vie.

Effacement Récupération