LPP.INC

Projet SAS

GMSI 2018

Un projet présenté par:

Anthony M, Aurélien M, Luca B et Sébastien R

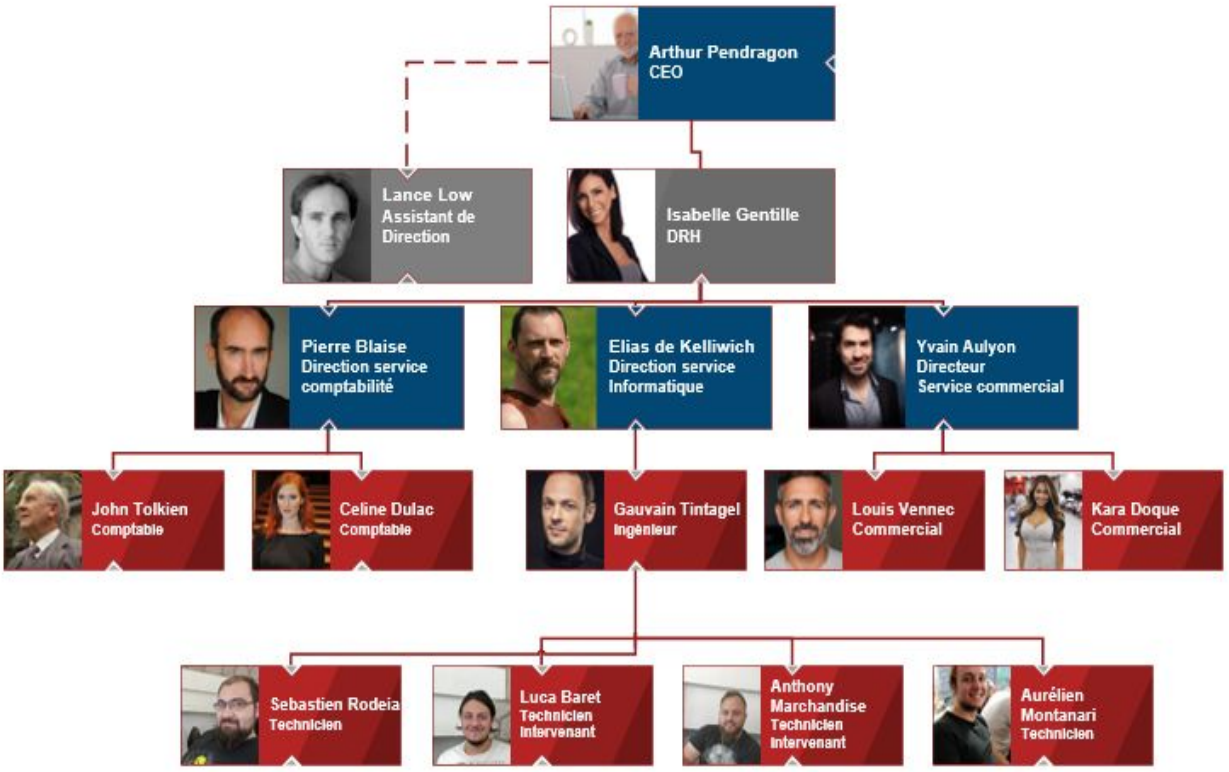
En partenariat avec le CESI Aix en Provence.

SOMMAIRE

LPP.INC
20 rue du Château,
13000 Marseille
04.92.08.09.10
support@lpp.inc

Du lundi au vendredi,
8h - 12h 14h - 17h
Possibilité d'astreinte

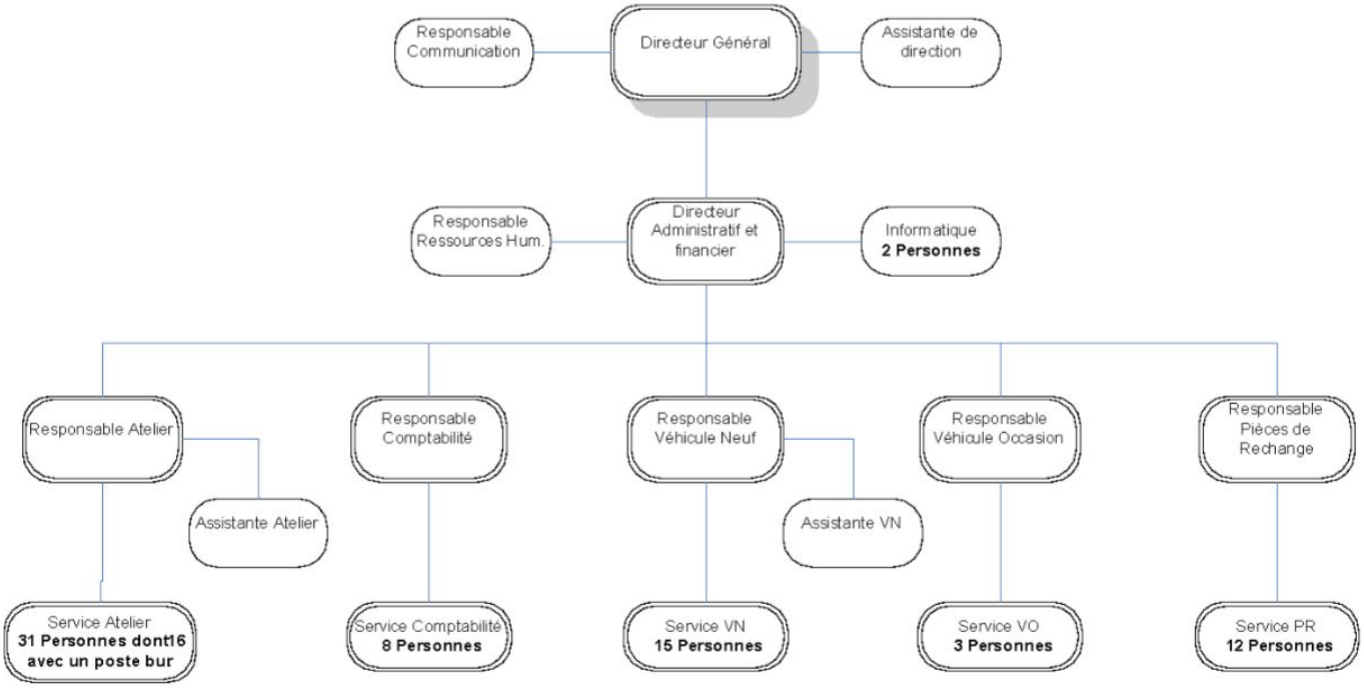
LPP.INC sarl, entreprise spécialisée dans la gestion et la maintenance de parc informatique pour les entreprises au chiffre d'affaire de 1 700 000€ et au capital de 365 000€. Siret 443 061 841 00047



Auto Concept
365 chemin de la Pioline,
ZC La Pioline,
13290 Aix-en-Provence
04.42.39.33.33

Lundi au samedi
8h - 12h 14h - 19h

Auto concept sarl, évolue sur le secteur d'activité : Commerce et réparation d'automobiles et de motocycles. Chiffre d'affaire de 66 102 711 € et au capital de 1 048 000€. Siret : 414 781 203 00040



ANALYSE DES BESOINS

Suite au rapport commercial fournis nous constatons une perte de 140 000€ suite à des problèmes informatiques non gérés ainsi qu'un gros problème au niveau des délais d'intervention, délais qui n'implique pas forcément une résolution du problème.

Des soucis de sûreté ont été signalés, certains postes n'ont pas de mots de passe et d'autres ont été pourvus de programmes piratés ce qui représente d'énormes failles de sécurité et un non respect de la Loi.

Un manque global de professionnalisme de la part des techniciens a été constaté, manque de ponctualité, tenues inappropriées et attitude désagréable.

Tableau de synthèse:

Problème	Type de problème	Solution à apporter
Crash disque	Technique	Plan de sauvegarde
Lenteur des postes	Technique	Maintenance des postes
Intrusion d'un client sur un poste commercial sans mot de passe	Organisationnel	Communication utilisateur / Formation Technicien
Tenue vestimentaire	Organisationnel	Formation Technicien
Planification d'intervention	Organisationnel	Formation Technicien
Message d'erreur windows "crack"	Technique	Maintenance des postes
Résolution durable d'incident	Organisationnel	Maintenance des postes
Problème de confidentialité	Juridique	Formation Technicien
Problème de gestion de stock	Organisationnel	Formation Technicien
Non prise en compte d'incident mineur	Organisationnel	Formation Technicien
Manque d'information sur les retour SAV	Organisationnel	Formation Technicien
Attitude du technicien	Organisationnel	Formation Technicien
Délais d'intervention	Organisationnel	Formation Technicien

SYNTHÈSE JURIDIQUE

Surveillance et vie privée

L'employeur peut contrôler et limiter l'utilisation d'internet (dispositifs de filtrage de sites, détection de virus...) et de la messagerie (outils de mesure de la fréquence des envois et/ou de la taille des messages, filtres « anti-spam »...).

Chaque utilisateur doit avoir une session personnelle protégée par un mot de passe, respectant la politique de mots de passe de l'entreprise

En contrepartie,

L'employeur ne peut pas recevoir en copie automatique tous les messages écrits ou reçus par ses employés, c'est excessif.

les « keyloggers » permettent d'enregistrer à distance toutes les actions accomplies sur un ordinateur. Sauf circonstance exceptionnelle liée à un fort impératif de sécurité, ce mode de surveillance est illicite.

les logs de connexion ne doivent pas être conservés plus de 6 mois.

Un employé a le droit, même au travail, au respect de sa vie privée et au secret de ses correspondances privées.

Un employeur ne peut pas librement consulter les courriels et fichiers personnels de ses employés, même s'il a interdit d'utiliser les outils de l'entreprise à des fins personnelles.

Pour qu'ils soient protégés, les messages et fichiers personnels doivent être identifiés comme tels, par exemple :

- en précisant dans leur objet « Personnel » ou « Privé »,
- en les stockant dans un répertoire intitulé « Personnel » ou « Privé ».

Textes de référence

Le code civil :

Article 9 (protection de l'intimité de la vie privée)

Le code du travail :

Article L. 1121-1 (droits et libertés dans l'entreprise)
Article L. 1222-3 et L. 1222-4 (information des employés)
Article L. 2323-47 (information/consultation du comité d'entreprise)

Le code pénal :

Articles 226-1 et suivants (protection de la vie privée)

Le Règlement européen sur la protection des données personnelles (RGPD)

Utilisation de logiciels pirates

Le piratage informatique est une infraction aux lois régissant les droits de la propriété intellectuelle, du droit d'auteur et la protection juridique des programmes d'ordinateurs.

Code de la Propriété Intellectuelle

Article L.335-3 : « Est (...) un délit de contrefaçon et la violation de l'un des droits de l'auteur d'un logiciel (...) »
Article L.122-4 : « Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur (...) est illicite »
Article L.335-2 : « La contrefaçon en france (...) est punie de deux ans d'emprisonnement et de 150.000 euros d'amende »

Les sanctions:

Les sanctions civiles :

Lors d'une procédure civile, le tribunal fixe librement le montant des dommages et intérêts que le contrefacteur doit payer à l'auteur, en fonction de la gravité du préjudice subi par ce dernier. Il n'y a pas d'échelle de peine prévue par les textes, mais le montant des dommages et intérêts peut atteindre plusieurs millions d'euros.

Les sanctions pénales :

Pour une personne physique. une personne physique est donc passible d'un emprisonnement maximum de deux ans et d'une amende maximale de 150.000 euros.
Pour une personne morale. Depuis le 1er mars 1994, les personnes morales sont également punissables au titre d'actes contrefaisants perpétrés pour leur compte par leurs organes ou représentants. Les peines encourues sont :

- une amende maximale de 750.000 euros,
- la dissolution, si la personne morale a été créée pour commettre l'acte de contrefaçon,
- l'interdiction définitive ou temporaire d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales,
- le placement sous surveillance judiciaire,
- dès la première infraction, la fermeture définitive ou temporaire des établissements de l'entreprise ayant servi à commettre l'infraction,
- l'exclusion définitive ou temporaire des marchés publics,
- l'interdiction définitive ou temporaire de faire appel public à l'épargne,
- l'interdiction d'émettre des chèques pour une durée de cinq ans au plus,
- la confiscation des matériels ayant servi à commettre l'infraction,
- l'affichage de la décision dans la presse.

Information aux employés

Les instances représentatives du personnel doivent être informées ou consultées avant la mise en œuvre d'un dispositif de contrôle de l'activité.
Chaque employé doit être notamment informé :

- des finalités poursuivies,
- de la base légale du dispositif (obligation issue du code du travail par exemple, ou intérêt légitime de l'employeur),
- des destinataires des données,
- de la durée de conservation des données,
- de son droit d'opposition pour motif légitime,
- de ses droits d'accès et de rectification,
- de la possibilité d'introduire une réclamation auprès de la CNIL.

Cette information peut se faire au moyen d'une charte, annexée ou non au règlement intérieur, d'une note individuelle ou d'une note de service.

FORMATION DES COLLABORATEURS

L'utilisation de l'outil informatique est un sujet souvent mal compris, voir mal interprété dans les entreprises. L'utilisation commune de l'informatique hors du travail peut faire disparaître la frontière entre le PC personnel et le PC de travail. Dans cette optique nous pouvons proposer des formations aux collaborateurs pour leurs rappeler les règles qui régissent l'utilisation d'un ordinateur en entreprise.

Formation utilisateurs

Les utilisateurs sont les premiers à informer, en effet ils sont ceux qui utilise l'outil informatique pour leurs travails au quotidien. Il est donc primordial de leurs montrer la voie pour garder un espace de travail propre.

Le respect de la charte informatique mise en place par l'entreprise est le pilier de cette bonne utilisation. Chaque utilisateur doit l'avoir lu et signé avant de pouvoir se servir du matériel fournis. Cette charte est personnalisée par l'entreprise et contient tous les droits et devoirs qu'il se doivent respecter au sein de leur entreprise.

La politique de mots de passe, disponible dans la charte informatique la plupart du temps, permet de maintenir la sécurité et la confidentialité d'une session utilisateur. Il est très important de respecter cette politique qui permet d'avoir un mot de passe résistant à la casse. Le mot de passe d'un utilisateur est personnel et doit le rester.

La vie privé des utilisateurs est tolérée et défendues par la Loi au travail sous certaines conditions. En effet les utilisateurs peuvent utiliser l'outil informatique et la messagerie mail à des fins personnelles, mais le temps alloué à cela peut être régulé par l'entreprise. Tout fichier ne se trouvant pas dans un répertoire nommé "Privé" ou "Perso" par exemple sera considéré comme un fichier en rapport au travail et pourrait donc être consulté par l'entreprise. Il en va de même pour les mails, qui doivent être enregistrés dans une boite nommer Privé ou Perso, ou bien posséder cette mention dans l'objet du mail.

Garder son poste dans une optique d'outil de travail est très important, en effet un PC de travail ne représente en rien un PC personnel, l'entreprise peut donc restreindre l'accès à certains sites internet ou programmes. Certaines entreprises peuvent aussi imposer des règles quant à la personnalisation de l'ordinateur, par exemple, un fond d'écran choisis par l'entreprise et obligatoire sur tous les postes.

Formation des technicien

Le technicien est le garant du bon fonctionnement de l'outil informatique, cependant son savoir faire ne l'exclue pas de la charte informatique.

Le respect des autres est un point important dans la bonne entente avec les autres personnes de l'entreprise. L'attitude, la tenue vestimentaire et le respect des délais ne doivent pas être négligés.

Les explications simples, à la manière d'un médecin qui expliquerait une maladie à un patient, sont une part du travail d'un technicien. La vulgarisation technique peut permettre à un utilisateur de mieux comprendre l'origine d'un problème et de l'éviter à l'avenir.

L'organisation de son travail permet au technicien d'avoir un parc qui fonctionne. L'encadrement du parc lui permet de gagner beaucoup de temps sur les tâches de maintenance qu'il peut être amené à réaliser.

Le fonctionnement optimal de l'outil informatique repose donc sur des utilisateurs respectant les règles mises en place par l'entreprise mais aussi sur des techniciens capables d'être respectueux mais aussi pédagogues avec les utilisateurs de son parc informatique.

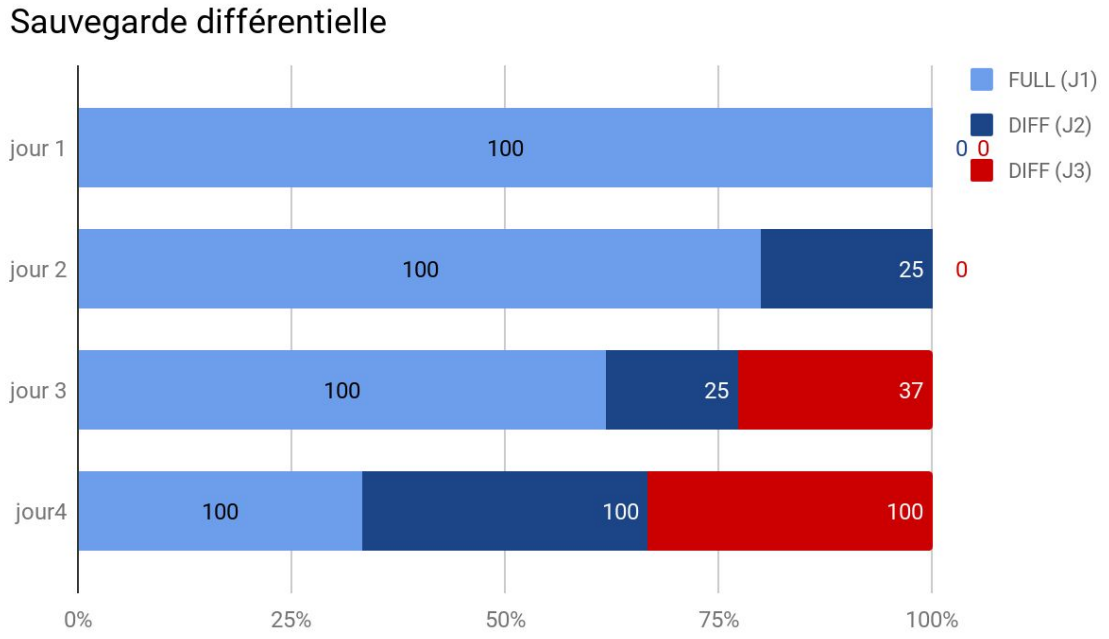
PLAN DE SECURISATION DES DONNEES

Ce qui est disponible

Nous disposons d'une infrastructure souple et flexible s'adaptant aux différentes problématiques de sauvegarde que chaque projet pourrait comporter. Nous pouvons grâce à Acronis, le logiciel que nous utilisons pour la sauvegarde, effectuer:

- **De la sauvegarde différentielle.** Cette sauvegarde consiste à stocker uniquement les modifications survenues après la dernière sauvegarde complète. Ce type de sauvegarde permet une restauration plus rapide des informations comparé à la sauvegarde incrémentale, car seule la première et la dernière sauvegarde sont utiles. Par contre, elle impose aussi d'effectuer des sauvegardes complètes régulièrement pour que les modifications ne finissent pas par prendre un espace plus important que la sauvegarde complète initiale. Il est possible de supprimer les sauvegardes intermédiaires.

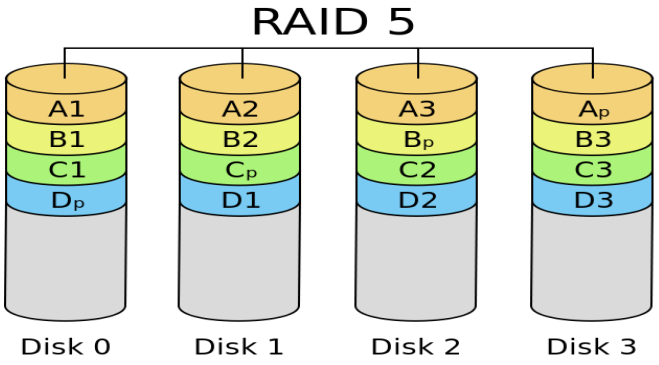
  Ainsi dans l'exemple ci dessous, si nous voulons restaurer la sauvegarde du troisième jour, il faudra restaurer la sauvegarde complète du premier jour et les sauvegardes différentielles du deuxième et du troisième jour.



- **De la sauvegarde complète.** Ce moyen de sauvegarde consiste à sauvegarder chaque jour la totalité des fichiers, qu'ils ai été modifiés ou non. Ce type de sauvegarde a pour avantage de restaurer très rapidement la sauvegarde de n'importe quel jour mais possède comme inconvénient d'être très gourmande en espace de stockage. De plus, les fichiers qui n'ont pas été modifiés seront sauvegardés plusieurs fois. Cette méthode a aussi pour avantage de permettre très simplement de supprimer les anciennes sauvegardes.

- **De la sauvegarde incrémentale.** La sauvegarde incrémentale stocke les fichiers ajoutés, modifiés ou supprimés entre deux sauvegardes complètes. Ce type de sauvegarde est très rapide à exécuter mais rend l'opération de restauration plus complexe et longue. En effet, il faut partir de la dernière sauvegarde complète puis restaurer chaque incrément un par un. Si un incrément est corrompu, une partie de la sauvegarde peut l'être aussi. Il faut donc effectuer régulièrement des sauvegardes complètes pour réduire le nombre d'incréments.

Toute notre infrastructure de disque dur est en RAID5, nous avons fait ce choix car le RAID5 tolère la panne d'un disque dur sans en affecter l'ensemble des données. Les différences avec les autres type de RAID sont qu'il nécessite un minimum de trois disques et qu'il assure la redondance des données en stockant des informations de parité plutôt que grâce à la copie en miroir.



Pour permettre de pallier aux risques ainsi que de maintenir un temps de rétablissement rapide avec efficacité, toutes nos sauvegardes sont répliquées sur notre site secondaire. Nos sites sont sécurisés grâce à un accès restreint, seul le responsable des données désigné par le client et les techniciens en charge du dossier peuvent y accéder avec le port d'un badge d'identification.

Objectif du plan de sauvegarde

L'objectif du plan de sauvegarde est de permettre la restauration rapide du système et des données en cas de panne du système ou du disque dur d'un poste. Il permet aussi de retrouver un document détruit volontairement ou non. Pour cela il est recommandé de conserver ses données sur une source externe au poste.

Ce que nous proposons pour AutoConcept

Dans l'optique de proposer une solution la plus adaptée possible au cas d'**AutoConcept** nous proposons un plan de sauvegarde complet en deux parties, une partie adaptée aux données critiques, une seconde adaptée à leurs données non critiques. afin d'assurer le bon déroulement de ce projet, l'établissement de la criticité des données est laissée libre à l'entreprise **AutoConcept**. Le plan de sauvegarde comprend une sauvegarde complète au démarrage du projet et cela pour chaque partie.

Première partie: les données critiques

Les données critiques seront sauvegardées tous les jours, en différentiel, automatiquement par le biais d'Acronis. Cette méthode permet de retrouver un document détruit volontairement ou non, mais aussi de retrouver un ordinateur opérationnel de manière immédiate après une défaillance de Windows. En revanche cela ne permet pas de sauvegarder toutes les données en cas de destruction ou de vol du PC.

En plus de cela, nous ferons une sauvegarde complètes des données critiques sur un serveur à bande tous les mois.

Deuxième partie: les données non critiques

Les données non critiques seront sauvegardées tous les trois jours, en différentiel, automatiquement par le biais d'Acronis. Cette méthode permet de retrouver un document détruit volontairement ou non, tout en permettant une meilleure gestion de l'espace de stockage comparé à la partie des données critiques.

En plus de cela, au même moment que pour les données critiques, nous ferons une sauvegarde complètes des données sur un serveur à bande tout les mois.

Grâce à ce plan de sauvegarde, **AutoConcept** perdrais au maximum une journée de travail pour ses données critiques et au maximum trois jours pour ses données non critiques. **AutoConcept** pourrait donc éviter de manière efficace les pertes monétaires suite à des problèmes de sauvegarde.

ANNEXE

1) Memo
2) Charte qualité
3) Charte informatique