La maîtrise de son informatique, au sein d'un pouvoir local.

Réseau Informaticiens Communaux pas

Ce document a été réalisé par le comité du RIC, Réseau des Informaticiens Communaux et CPAS www.ric.be qui a pour but de promouvoir la mise en place de synergies entre ses membres et ce, en particulier, dans le domaine des technologies de l'information.

La version du présent document est numérotée 2018/01, correspondant au mois de janvier 2018.

Le présent document est disponible en ligne à l'adresse www.ric.be/public .

1. Introduction

Au cours des dernières décennies, l'informatique s'est introduite petit à petit dans les pouvoirs locaux. Cela s'est fait de manière plus ou moins organisée suivant les organismes et cette nouveauté fut considérée le plus souvent comme une contrainte et un mal nécessaire.

À l'heure actuelle, l'informatique est devenue inévitable et se positionne comme un maillon clé d'une administration ou service public pour remplir ses différentes missions, notamment vers le citoyen.

Et les nouvelles technologies vont encore devoir offrir une réponse efficace aux défis à relever ces prochaines années : smart cities, échanges accrus d'information inter-organismes, davantage de services en ligne vers le citoyen (incidents, documents, conseils participatifs, permis), intégration des réseaux sociaux, la nouvelle réglementation sur la protection des données (RGPD) en mai 2018, etc…

Pour faciliter cette transition et assurer pleinement ses missions à remplir, un pouvoir local doit et devra pouvoir maîtriser correctement son informatique, sous ses différents aspects (infrastructure et applications logicielles), tout en maintenant un niveau de sécurité important.
C'est à cette condition que les administrations pourront plus facilement suivre les évolutions technologiques continues et se moderniser.

Ce document vise à présenter (de manière la plus simple possible) les différents aspects de l'informatique, les risques qui y sont liés et des propositions de solutions pour y pallier.

2. L'informatique au sein d’un pouvoir local

2.1. Un outil de travail indispensable

L’outil informatique est dans les faits l’outil de travail principal des agents administratifs, utilisé par ces derniers pour remplir les missions principales de leur administration.
Les agents de terrain, des ouvriers communaux jusqu’aux agents constatateurs, peuvent l’utiliser de manière classique dans un bureau mais aussi en extérieur sur du matériel transportable.
Les services liés, comme les bibliothèques, les écoles, les offices du tourisme, les crèches, les hôpitaux, les maisons de repos, etc... sont aussi concernés.
On peut de facto dire qu’il s’agit à l’heure actuelle d’un outil incontournable, incluant des logiciels de gestion et permettant de communiquer entre services internes et avec le monde extérieur.

À travers plusieurs logiciels mis à disposition sur un ordinateur, l’agent peut accéder à différentes informations afin de gérer ses dossiers et produire in fine des actes officiels. On y décèle dès lors toute l’importance de l’outil à travers la sensibilité et l’importance de l’information, constituée de données personnelles et privées ainsi que de données professionnelles confidentielles.

L’outil informatique est la ressource principale d’un agent. Il doit lui permettre de réaliser son travail de manière correcte, et même in fine d'accroître son efficience.
Il peut également jouer un rôle en matière d’évolution de compétences non seulement à travers l’amélioration de l’utilisation qu’il en fait mais aussi comme support d’apprentissage.
Afin d’être le plus efficient possible, il est évidemment nécessaire de pouvoir maîtriser en tant qu’utilisateur son outil de travail et d’y être correctement formé.
Àl’heure actuelle, inclure dans un profil de fonction administrative - comme compétences nécessaires - des connaissances correctes dans l’outil bureautique et l’informatique de base est un minimum.

Il doit correspondre aux besoins fonctionnels liés au travail à remplir. Un outil pas ou peu adapté entraîne un travail plus conséquent et une réponse moins efficace de l’organisme.
Un outil adaptable permettra de suivre plus efficacement les inévitables évolutions liées à la fonction ou aux services à rendre.

L'outil informatique ne se limite pas à une utilisation par le personnel interne. Le citoyen est également en attente de réponses informatiques plus efficaces lui permettant de dialoguer et d'interagir avec son administration de manière distante et intemporelle.

Il doit donc répondre à la fois aux attentes spécifiques internes et à celles du citoyen.

L'outil informatique est souvent vu comme un outil en bout de chaîne dans la réalisation d'une mission. Or, il est bien plus efficace de l'intégrer dès le début de la réflexion sur une nouvelle procédure plutôt que de l'ajouter par la suite. Bien plus qu'un ensemble d'outils ou de programmes, l'informatique englobe par définition la gestion des processus de traitement de l'information au sens large. Et toute procédure traite l'information. L'analyse d'un processus est donc aussi automatiquement liée à une analyse informatique, qui repose justement sur des méthodologies de clarification des processus permettant d'éviter des erreurs.

Il a également certaines limites.
Le cadre légal est la première, à travers l'aspect législatif ou un règlement interne.
Il peut également y avoir des limites techniques, souvent liées aux moyens financiers associés.
Des limites humaines peuvent également prévaloir sur l'outil informatique, parfois à juste titre mais le plus souvent pour de mauvaises raisons amenées par les utilisateurs.

Au final, de simple machine à écrire dans le début des années '90, on constate que l'ordinateur et l'informatique sont devenus l'épine dorsale vitale de l'administration.Cela se constate facilement dès le moindre dysfonctionnement informatique, qui peut provoquer une réduction de l'efficacité d'un service jusqu'à la paralysie de toute l'administration (comme cela s'est déjà vu lors de problèmes de connectiques majeurs ou d'attaques de virus).

2.2. Un moyen de communication

L'outil informatique est au centre de toutes les communications modernes.

L'e-mail permet une communication interne plus rapide, plus facile et mieux sécurisée. Donc une communication de meilleure qualité, dans la mesure où cet outil est maîtrisé par les différents intervenants afin de produire des échanges clairs et précis.

Ce système de communication est également utilisé pour la communication externe, que ce soit avec d'autres organismes ou avec le citoyen.
Chaque service public a en effet des obligations légales de traitement et d'échanges de données via l'informatique: avec le Registre National, avec les différents SPF, avec la BCSS, avec la Région wallonne, etc...
L'informatique est donc aussi une porte vers le monde extérieur, dans les deux sens, et donc une voie d'entrée pour les nuisances extérieures intentionnelles ("virus" divers). Nuisances pour lesquelles l'outil informatique peut en partie faire barrage mais dont le barrage ultime (et potentiellement le plus évolué) est l'utilisateur final.

Le site internet est un autre moyen de communication mettant en ligne sur le web une vitrine de l'administration. Cette dernière permet de mettre à disposition des informations pratiques couvrant différents domaines. Le site web doit répondre à des normes de qualité, d'ergonomie et de "multi-modalité" afin de pouvoir être utilisé par les différents terminaux utilisé par le citoyen comme les ordinateurs, les tablettes, les smartphones, les télévisions connectées, les consoles, etc...

Le citoyen est également en attente d'outils en ligne lui permettant d'interagir avec son administration, sans devoir se déplacer et sans devoir respecter des contraintes horaires. Les moyens d'identification modernes comme la carte d'identité électronique permettent non seulement une authentification forte mais aussi la possibilité de signer et dématérialiser les documents.
Une administration communale a d'ailleurs l'obligation légale de mettre à disposition certains documents, comme les procès verbaux de conseils communaux.

Les moyens de communication modernes, comme les réseaux sociaux, sont une autre forme d'interaction pour communiquer, surtout de la part du citoyen. Celui-ci est le témoin immédiat et en temps réel de la vie de la commune et peut se servir de ces nouveaux médias pour communiquer avec d'autres citoyens ou vers son administration.

2.3. De multiples facettes

L'informatique présente de multiples facettes, qui nécessitent d'ailleurs des connaissances fort diverses.

Au niveau matériel, l'infrastructure informatique reprend 2 aspects:

- tout ce qui couvre la partie réseau de communication, qu'il s'agisse du câblage ou des différents appareils configurables qui gèrent ces transmissions

- les ordinateurs, pc, terminaux ou appareils mobiles faisant office d'interface avec l'utilisateur, ou encore les serveurs en arrière plan couvrant différents aspects fonctionnels

Au niveau logiciel, on peut considérer:

- les systèmes d'exploitation, dont Windows est le plus répandu pour les pc, mais également Linux plus répandu sur les serveurs et matériel, et encore MacOS pour les ordinateurs Apple
- la bureautique, comme outil principal des utilisateurs pour mettre en forme des documents, structurer des données dans un tableur, etc...
- les logiciels « métier », spécifiques à la gestion d'aspects fonctionnels particuliers et nécessitant aussi un apprentissage spécifique pour les utiliser
- les outils de gestion pour l'informatique elle-même, comme les tableaux de bord, etc...

Les éléments plus particuliers liés à la communication

- la gestion de l'accès à internet, avec toute la partie sécurité qui en découle, que ce soit au niveau câblé ou par wifi pour les appareils mobiles
- la gestion des e-mails
- la téléphonie IP de plus en plus souvent utilisée
- les écrans d'information ou les bornes interactives
- les échanges de données suivant différents protocoles à respecter avec différents acteurs
- les bornes de paiement
- le contrôle d'accès, les appareils de pointage, la vidéo-surveillance
- etc...

Le développement logiciel pour réaliser des applications internes, composé de différentes phases:

- l'analyse
- le développement initial et les évolutions
- la maintenance

Le support et la formation font aussi partie du travail à fournir envers les utilisateurs finaux. Cependant, le rôle de l'informaticien n'est pas de savoir utiliser les programmes liés au métier particulier d'un agent, mais plutôt d'en connaître les dépendances et fonctionnalités techniques. Il ne peut donc pas automatiquement apporter un support complet.

L'implication de l'informaticien est un processus continu, en amont de toute décision, en aval en cas de problème ou panne et surtout entre ces deux éléments où il a la tâche critique et méconnue d'analyser les flux d'information afin de maintenir le

réseau en fonctionnement optimal, de détecter et de prévenir les menaces et dysfonctionnements potentiels avant qu'ils ne se produisent ou deviennent trop importants.

Enfin, les aspects juridiques ne sont pas à ignorer, comme la protection des données personnelles, la confidentialité, la propriété intellectuelle, les droits d'auteur ou la responsabilité dans les communications, etc...

Tous ses aspects forts différents le sont tellement qu'ils représentent chacun différents métiers de l'informatique ! De la même façon qu'en médecine on trouve différents spécialistes. Il est donc compréhensible qu'une même personne ne puisse souvent gérer seule ces différents aspects et qu'il soit nécessaire pour l'institution de faire appel à des prestataires extérieurs, non seulement pour la réalisation et la mise en place mais aussi pour la gestion proprement dite.
Cependant, plus ces aspects sont laissés à des prestataires extérieurs, plus l'administration perd le contrôle sur ceux-ci et éventuellement sur les données qui y sont liées. L'importance de cette perte de maîtrise dépend du temps accordé au suivi des prestataires extérieurs et des contrats signés.

2.4. De multiples acteurs

Il est faux de croire que l'informatique concerne uniquement les informaticiens. Dans les faits, les intervenants suivants ont chacun un rôle à assurer.

La direction, qui a évidemment un pouvoir de décision, se doit donc d'apporter son soutien à la mise en place et à l'utilisation des outils informatiques, surtout par rapport aux utilisateurs. Ces derniers ont en effet souvent la réaction humaine de repousser le changement ou ce qui est vu comme une contrainte supplémentaire dans leur travail.

Les utilisateurs se voient trop souvent comme ayant un rôle passif. Or ils ont, d'une part, la possibilité de s'approprier correctement les outils mis à leur disposition afin d'en tirer le meilleur parti possible, et d'autre part ils sont le mieux placés pour renseigner les évolutions à apporter, car l'informatique n'est pas une chose figée mais vivante.

L'informaticien est souvent "simplement" vu comme l'agent en charge de l'informatique, le technicien gérant cette matière. Mais il occupe en fait une fonction assez complexe. Non seulement par rapport aux multiples facettes à gérer comme le précise le point précédent, mais aussi par la transversalité de sa matière qui

concerne de fait tous les services, et l'importance qui en découle. C'est aussi une matière pour laquelle le moindre problème est rapidement considéré comme bloquant, et peut en effet l'être réellement pour l'administration entière. On peut donc dire que la fonction d'informaticien est assez critique.

L'informaticien, pour pouvoir effectuer son travail correctement, doit également avoir accès sans restriction à tous les outils et donc à toute l'information gérée au sein du pouvoir local. Il occupe donc un poste de confiance, où déontologie et secret professionnel sont des notions importantes liées à la profession.

Le rôle de conseiller en sécurité est une obligation au sein d'un CPAS. Cette fonction consiste à s'occuper de l'ensemble des mesures de sécurité appliquées aux données à caractère social. Sur base des recommandations de la BCSS, le conseiller en sécurité doit gérer les mesures mises en place au sein de l'organisation, en collaboration avec l'informaticien. Ce n'est donc pas l'informaticien qui doit occuper cette fonction, afin de ne pas être juge et partie, mais une personne ayant les compétences nécessaires pour assurer cette fonction et placée sous l'autorité fonctionnelle directe du directeur général.

Le nouveau rôle de délégué à la protection des données personnelles, imposé dans le cadre du RGPD pour les entités publiques, sera un rôle central associé à toutes les questions relatives à la protection des données à caractère personnel. La fonction principale sera d'assurer la conformité avec le RGPD mais aussi d'informer et conseiller l'organisation. À nouveau, ce n'est pas l'informaticien qui devrait occuper cette fonction.

Les prestataires extérieurs sont engagés pour mettre en place et gérer certains outils, certaines facettes de l'informatique du pouvoir local. De ce fait, ils occupent pour cette partie la même fonction importante que celle décrite dans le paragraphe précédent mais avec un intérêt différent de celui du pouvoir local. Il faut juste s'en rendre bien compte, pour bien cadrer les choses, bien définir le rôle qu'on veut leur laisser.
Il est indispensable que prestataire et informaticien communiquent étroitement afin que ce dernier connaisse toute modification réalisée sur ses systèmes. Un élément d'apparence insignifiant peut avoir des conséquences néfastes sur le système d'information local.
La proportion de l'informatique gérée en externe dépend uniquement d'un choix fait par l'administration, suivant les moyens dont elle dispose ou la part de ceux-ci qu'elle veut accorder à la matière informatique.
D'autres institutions publiques, qu'elles soient régionales, provinciales, fédérales, etc... s'imposent dans le paysage du pouvoir local puisqu'il doit échanger de l'information et dialoguer avec ces premières. La complexité pour l'informaticien est

de gérer et coordonner la diversité de ces prestataires et de leurs solutions propres, qui sont parfois inadaptées au pouvoir local, fonctionnellement ou techniquement. Cette diversité peut engendrer différents problèmes d'instabilité ou de sécurité.

3. Les risques liés

Les risques liés à l'utilisation de l'informatique ne se limitent pas uniquement aux risques de piratage informatique, de virus ou de perte de données.

Si nous faisons l'analogie avec un système d'alarme, quel que soit son niveau de perfectionnement, c'est avant tout l'utilisation qui en est faite qui va conditionner son efficacité.
En effet, si l'utilisateur ne branche pas le système, cela n'a aucun intérêt.
S'il l'utilise sans maîtriser son utilisation, son efficacité est amoindrie.
Si le code est communiqué à différentes personnes, sans contrôle, le risque s'accroît.
Si le code est communiqué à quelqu'un qui se fait passer pour un technicien, par e-mail ou par téléphone, sans vérification, la faille devient béante.
Comme on le voit, l'utilisateur est un acteur vital quant au bon fonctionnement d'un système.

Les risques peuvent être regroupés en différentes catégories.

3.1. Une mauvaise utilisation de l'outil informatique

La perte de temps liée à une mauvaise utilisation est souvent sous-estimée. Cette mauvaise utilisation peut être due à un manque de connaissance, de formation, ou de mauvaises habitudes que l'utilisateur veut garder.
Par exemple, l'utilisation non maîtrisée de la messagerie électronique peut vite faire succomber les services sous un flux ingérable de messages. Au lieu de gagner en efficacité et rapidité, une mauvaise utilisation amènera seulement pertes de temps, incompréhensions et souvent tensions…

Un utilisateur mal formé peut, par manque de maîtrise d'un outil, provoquer des pertes de données via de mauvaises manipulations, ou effacer des fichiers sur un système de fichiers. Même s'il y a un backup pour récupérer l'information (encore faut-il s'en rendre compte), on en revient à la perte de temps induite.
L'altération des données est aussi liée à cette même problématique et est parfois plus compliquée à résoudre, car en général on le remarque moins vite qu'une perte brutale. Retrouver alors à quel moment les données étaient toujours correctes est beaucoup plus compliqué.

Un manque de compréhension d'un outil peut altérer la sécurité des données. Par exemple, le fait de changer le statut d'un élément de "privé" à "publié" modifie bien sûr la sécurité de l'élément en le rendant public et donc visible pour tout le monde. Il faut donc bien sûr en avoir conscience dans l'utilisation de l'outil. Le fait d'envoyer un extrait d'un programme à d'autres personnes (document, capture d'écran) peut contourner la sécurité de l'information qui était assurée dans ce programme. La diffusion incontrôlée enfreint la sécurité sous-jacente.

Les risques de sécurité venant de l'extérieur et visant l'utilisateur final sont nombreux. L'envoi d'e-mails malicieux est évidemment connu et ceux-ci ne peuvent pas être entièrement bloqués par les systèmes de protection. C'est donc l'utilisateur qui doit être formé pour détecter et vérifier le contenu des e-mails, que ce soit par rapport à l'expéditeur, au contenu lui-même, aux liens éventuels (avant de cliquer dessus), etc...
Certains sites internet présentent un risque plus important et l'utilisateur doit en avoir conscience. Le nom de domaine est important à vérifier avant d'y accéder. Les sites non professionnels induiront inutilement le risque d'obtenir un fichier contenant un virus.
L'utilisation de tout support amovible (clé usb, disque dur externe, appareil photo, smartphone, cd, etc...) est problématique. À partir du moment où il s'agit d'un support amovible, il pourra avoir été infecté automatiquement dans d'autres environnements. Dès que l'utilisateur le connectera dans son environnement de travail, il pourra infecter la machine et potentiellement tout le réseau.

Il est important de mentionner que les systèmes de protection automatiques (antivirus, anti-spam, etc...) ont toujours un temps de retard par rapport aux infections et ne peuvent protéger totalement et efficacement les systèmes !

Les risques de sécurité internes sont souvent négligés. Qu'il s'agisse de négligence, de "sabotage" ou d'indiscrétion, les risques venant du personnel interne sont plus nombreux par rapport aux attaques externes. Le manque de rigueur dans la gestion des droits et le manque de contrôle en sont souvent la cause.

L'abus des ressources mises à disposition peut impacter l'outil informatique. Que ce soient l'utilisation d'espace disque pour du contenu personnel, l'utilisation d'internet pour écouter la radio, pour l'accès aux réseaux sociaux ou télécharger des fichiers volumineux, l'utilisation de sa boîte de messagerie pour le privé, la multiplication de copies des mêmes fichiers, etc... Tout cela impacte le système informatique en consommant davantage de ressources et en multipliant les risques.

3.2. Le manque de cadre

L'utilisation non professionnelle de l'outil informatique, souvent tolérée sous la pression des utilisateurs, et déjà abordée dans la paragraphe précédent, provoque non seulement un abus des ressources professionnelles à des fins qui ne le sont pas, mais accroît également les risques de sécurité.

Le manque de gestion correcte des droits peut provoquer l'obtention de permissions inappropriées et excessives. Que ce soit sur l'ordinateur où l'utilisateur est mis comme administrateur (par imposition du fournisseur pour faire tourner son application), ou dans les applications où on donne plus de droit pour faciliter le travail, etc..., cette mauvaise gestion accroît à nouveau les risques de sécurité ou d'accès à des données non adéquates, que ce soit par l'utilisateur lui-même ou par un virus ou hacker.

Le manque de cadre dans la gestion des mots de passe est également problématique. Qu'il s'agisse d'une politique élaborée de mot de passe manquante parce que les utilisateurs trouvent cela trop compliqué, de mauvaises habitudes où les mots de passe sont les mêmes dans tous les outils, ou sont notés à côté de l'ordinateur, ou sont partagés entre collègues, etc..., tous ces manquements accroissent l'insécurité.

Le manque de déontologie dans l'exercice de sa fonction est parfois minimisé, certains utilisateurs n'hésitant pas à accéder à l'information par curiosité ou intérêt personnel.

Le manque de solidarité, d'esprit d'équipe et de discipline peut entraîner au sein des services des dysfonctionnements comme le manque ou refus de partage de l'information, le non respect de consignes, etc...

Le cadre de travail de l'informaticien peut ne pas être clairement défini ni adapté: il peut s'agir des limites d'intervention (certaines tâches qui pourraient être réalisées par d'autres ou à l'inverse les utilisateurs finaux qui empiètent sur les tâches principales à réaliser), des horaires de travail (certains travaux sont plus efficaces ou nécessaires à réaliser lorsque le personnel est absent, à horaire décalé), de son domaine d'influence (certains ignorent les consignes car l'informaticien n'est pas un responsable hiérarchique), de la place qu'on lui donne (lors du choix des logiciels ou même de l'analyse d'informatisation des procédures), etc...

3.3. Le manque de maîtrise interne de l'outil informatique

Il est important, au sein d'une administration, de pouvoir maîtriser l'outil informatique. Un manque de maîtrise pourra entraîner un manque d'appropriation de l'outil, une inadéquation par rapport à son rôle, un manque d'efficacité, des pertes de temps, l'accroissement des risques de sécurité, une dépendance à des prestataires extérieurs, etc...
Maîtriser demande évidemment des compétences dans le domaine.
Comme mentionné dans le premier point, l'informatique comporte de multiples facettes et nécessite donc des compétences variées, qui peuvent faire l'objet d'autant de spécialisations dans le métier.
Si l'on fait une comparaison avec le métier de médecin, on trouvera aussi en informatique le généraliste et les spécialistes. Il est évidemment compliqué, si pas impossible, qu'une même personne combine toutes les spécialisations.
Une solution réaliste sera donc de disposer d'un généraliste interne (au moins à temps partiel pour les plus petites administrations), faisant appel à des spécialistes extérieurs. Dans les plus grandes administrations, le personnel informatique pourra comporter plusieurs généralistes mais aussi des spécialistes.

La maîtrise de l'informatique ne consiste pas uniquement à disposer d'un informaticien. Il s'agit de la maîtrise de l'informatique par le pouvoir local et non pas uniquement par une seule personne, qui pourrait en cas de départ emporter toutes ses connaissances (cela est valable dans ce domaine comme dans tous les autres !).
Le travail de l'informaticien comporte une bonne partie de travail non visible par les utilisateurs mais essentielle. Il est important de transcrire toutes les informations de base pour assurer une reprise si nécessaire et transmettre cette information à sa hiérarchie, pour qu'elle aussi ait une vue complète et maîtrisée de l'informatique.

La maîtrise de son informatique inclut également la maîtrise des données que le pouvoir local gère. Cet aspect est très souvent négligé ou oublié. Les données représentent en effet le "produit" du pouvoir local. Elles lui appartiennent.
Il est donc important de pouvoir accéder à ses données indépendamment du logiciel qui les produit ou les utilise. Cela permet de pouvoir changer plus facilement de logiciel "métier" (ce qui explique que les firmes informatiques prennent souvent en otage celles-ci pour garder le contrôle) mais également d'exploiter les données dans des outils d'analyse ou de pouvoir les échanger en toute liberté.

Il est également important de pouvoir maîtriser les logiciels utilisés.

Une bonne connaissance des outils permet d'apporter à la fois une bonne information du point de vue de l'utilisation et un bon support interne.
Pouvoir configurer soi-même les logiciels permet aussi d'acquérir de l'indépendance dans la gestion (ne pas devoir payer pour changer un paramètre) et donc de s'adapter au mieux aux besoins locaux.
Le développement de logiciel en interne peut sembler apporter une meilleure maîtrise sur ceux-ci. En effet, une modification pourra plus facilement être réalisée dans le logiciel. Cependant, le coût interne du développement n'est pas à négliger et la dépendance à la seule personne qui aura créé le logiciel représente un risque important en cas de départ. Reprendre et maîtriser du développement informatique réalisé par une autre personne est souvent très compliqué.

3.4. De mauvais choix informatiques

Une lapalissade serait de dire qu'il faut bien choisir ses outils pour minimiser les risques et problèmes. De mauvais choix vont entraîner des coûts supplémentaires, en terme d'utilisation, d'évolution, de maintenance, de migration, etc...

Il n'y a hélas pas de formule magique pour être certain de ne pas se tromper.Cependant, il est possible de choisir en tenant compte de certains paramètres.

Il est important de choisir un logiciel en fonction de la pérennité visée.
Une société qui développe un logiciel peut arrêter son outil du jour au lendemain, pour raison stratégique ou autre.
Le logiciel libre, si tant est que le nombre de personnes dans la communauté est important, permet de s'affranchir de la dépendance à un seul acteur.

Certains logiciels sont achetés alors qu'ils sont inadaptés ou même non fonctionnels. Ce risque s'accroît d'autant plus si les utilisateurs n'ont pas l'occasion de tester l'outil ou si la sélection est faite sur une simple démonstration ou présentation. Sans pouvoir tester le logiciel en démonstration, on ne peut se rendre compte de son fonctionnement ni de ses limites.

Un mauvais choix de formats de fichiers va entraîner des problèmes de dépendances ou de compatibilité.
Les formats propriétaires peuvent uniquement être utilisés avec les logiciels propriétaires adéquats et parfois en fonction aussi de leur version. Par exemple, d'anciens documents Microsoft Word ne savent plus être ouvert par les versions récentes de ce même logiciel.

Des formats ouverts, comme ODF ou PDF, sont existants et permettent à tout logiciel qui le veut de pouvoir les ouvrir.

Certains choix informatiques sont parfois réalisés sans impliquer préalablement l'informaticien, en pensant qu'il n'y a pas de lien avec l'existant, alors qu'il y aura toujours un impact d'un point de vue sécurité, infrastructure, stockage, etc... Sans raison valable, on fait parfois plus confiance à un commercial vantant son produit et affirmant qu'il n'y aura aucun problème, qu'à son informaticien, qui pourrait freiner à juste titre l'adoption d'un nouvel outil...

Les aspects d'infrastructure comme la mise en réseau, les serveurs, etc... doivent être pensés sur le long terme et rester le plus évolutifs possible car ce sont des aspects de base du système informatique mis en place et donc plus lourd à remplacer.

Le manque d'homogénéité matérielle ou logicielle, ainsi que l'achat de matériel inadapté, peut amener à des lourdeurs de gestion et des soucis d'interopérabilité.

3.5. La sécurité interne et externe

Au niveau infrastructure, il est nécessaire de se protéger des accès physiques : des intrusions dans les locaux autant que des accès informatiques.
Pouvoir accéder physiquement à un élément du réseau (câble réseau, ordinateur, serveur) représente un problème de sécurité sur le réseau au complet.
Il en est de même lors de l'authentification sur le réseau, qui doit garantir un système de définition et gestion de mot de passe suffisamment "fort", et permettre une gestion des droits affinées.

Sur le plan logiciel, chaque logiciel doit proposer un système d'authentification et assurer une gestion de rôles efficace. Aucun outil, ni aucune technologie ne peut garantir un niveau de sécurité absolu mais, certains outils ou technologies offrent de meilleures garanties et sont donc à privilégier.
Concernant certains logiciels ou systèmes d'exploitation, il peut être intéressant de se poser la question de leur indépendance. Le fait d'avoir, pour Microsoft par exemple, conçu intentionnellement certaines failles pour que des organismes d'état s'en servent, a été reconnu...

La gestion des droits au sein du pouvoir local doit être efficace. Il peut devenir très laborieux de gérer par exemple des droits d'accès sur des répertoires du système de fichiers. Il y a toujours des exceptions qui entraînent des accès non désirés.

Le contrôle de l'information doit être maîtrisé. Tant l'administration publique que le CPAS traite de l'information privée et confidentielle relative au citoyen et des informations stratégiques au niveau politique. Il faut clairement analyser les données utilisées par chacun ainsi que les droits des intervenants internes et externes, afin d'assurer la bonne utilisation des données et se préserver des pertes de données. Ce sont les objectifs du nouveau RGPD.

Le matériel mobile amène un risque élevé de faille. Ce matériel pouvant contenir des informations confidentielles entre et sort couramment de l'administration.
Le vol ou la perte de ce matériel peut compromettre l'organisation.
Les appareils n'étant pas la propriété de l'administration - comme les téléphones, les tablettes, les portables, les clés usb - sont utilisés par le personnel (en partie professionnellement ou sans autorisation) mais ne sont pas gérés par l'informatique interne. Ils peuvent donc contenir de l'information qui risque de ne plus être protégée mais aussi contaminer l'administration.
Il en est de même pour les personnes externes qui viennent occasionnellement travailler au sein de l'administration (différents SPF, des permanences, des associations locales, etc...) avec leur propre matériel, nécessitant d'être connecté au réseau pour l'accès à internet ou l'impression. Il n'y a aucun contrôle sur ce matériel, qui doit être considéré comme hostile.

La faiblesse d'un système peut être accrue par les prérequis de certains fournisseurs demandant l'utilisation de certains outils (vieilles versions de navigateurs par exemple), proposant certaines facilités (faible sécurité de mot de passe) ou demandant des droits excessifs (administrateur du pc) tant pour eux que pour l'utilisateur final.

Il est important d'évaluer et prendre conscience de ce que représenterait la perte totale de ses données. Cela découle en général à une mise en place plus facile de systèmes de backup.

Les solutions d'outsourcing proposent en général des niveaux de fiabilité plus importants. Il faut néanmoins s'en assurer via les conditions présentes dans les contrats et assurer un backup externe de toutes ses données afin de se préserver d'une éventuelle faillite.

Les attaques et infections ont toujours besoin d'une porte d'entrée dans le système. Cette porte d'entrée est la plupart du temps ouverte de manière non-intentionnelle par l'utilisateur, et en moindre partie par des failles système. Pour ces dernières, il faut savoir qu'il n'existe aucun système de protection efficace à 100%. Les correctifs

de sécurité sont toujours en retard (par définition) par rapport aux attaques. Les logiciels anti-virus également.

3.6. Sanctions liées au Règlement Général sur la Protection des Données Personnelles

Cette nouvelle directive prévoit la mise en place d'amendes financières importantes en cas d'utilisation non autorisée de données personnelles, même en cas de perte/vol de données. Le règlement donne au régulateur (la Commission de la vie privée) le pouvoir d'infliger des amendes administratives en cas de non-respect du règlement.

4. Les actions à prendre

4.1. Le rôle de la direction

Comme expliqué précédemment, le rôle de la direction est essentiel dans le cadre de la maîtrise de son informatique. Cette dernière passant par un certain nombre de changements à réaliser, le support de la direction est absolument nécessaire pour mettre en oeuvre les actions à mener, tant au niveau de l'affirmation de cette volonté que de la légitimation des acteurs impliqués.
Il est en effet impossible pour l'informaticien de mener des actions "contraignantes" pour les utilisateurs sans avoir été légitimé pour le faire ni sans la confirmation de cette action envers les utilisateurs.
Il faut se reposer sur une implication et une communication claire de la direction vers son personnel pour garantir une réussite dans le changement.

La réalisation d'un plan directeur informatique doit être menée par la direction, afin d'effectuer un état des lieux de l'existant et définir et planifier les objectifs à réaliser. Il s'agit donc d'une gestion de projet, comme pour d'autres matières, passant par un état des lieux préalables et des actions à mener.

Vu l'importance de la matière informatique (telle que présentée jusqu'ici dans ce document), le rôle transversal de l'informaticien et son implication nécessaire dans les dossiers, il nous semble intéressant d'inclure l'informaticien à un niveau plus élevé de décisions, tel qu'au comité de direction quand il y en a un, afin de faciliter l'échange sur les points transversaux et améliorer le processus de gestion.

4.2. Mettre un cadre à l'utilisateur

Ce point est un des plus importants, tant au niveau du contrôle des risques que de la difficulté de mise en place.
Comme on l'a vu précédemment, l'utilisateur est au centre de l'informatique et par là-même il est de facto au centre de la maîtrise de l'informatique.
Ceci explique que les attaques informatiques sont à l'heure actuelle plus orientées vers l'utilisateur que vers le matériel.
Soyons clair : mettre un cadre à l'utilisateur va permettre d'accroître fortement la maîtrise de son informatique mais va augmenter les contraintes pour celui-ci. Pas

tellement sur son travail mais plutôt sur sa “liberté”. En général, l’utilisateur a eu trop de liberté, et la diminuer représente toujours une frustration pour lui. C’est cependant une étape nécessaire et importante.
Il faut partir du principe que rien n’est permis et ne permettre que ce qui est nécessaire dans le cadre du travail, au cas par cas.
Cela semble dur, car l’outil informatique est aussi ressenti comme un outil de liberté. Mais il s’agit ici de l’informatique dans un cadre professionnel et non pas à son domicile.
On l’admet clairement dans beaucoup d’autres domaines : il y a un cadre strict pour utiliser un véhicule sur la voie publique et on trouve cela normal et nécessaire, même si nous sommes parfois les premiers contrariés...

Plusieurs actions sont à mener :

4.2.1. Charte d’utilisation informatique et son contrôle

La charte d’utilisation informatique permet de définir un cadre clair quant à l’utilisation de l’outil informatique dans le contexte professionnel. On y indique les devoirs de l’utilisateur concernant l’outil qui lui est mis à disposition ainsi que les limites. Il s’agit donc d’un support de responsabilisation mais également un cadre permettant d’éventuelles sanctions sur une utilisation anormale par rapport à la charte.
Cette dernière est donc une première étape, qui n’a de sens que si un suivi régulier est effectué quant à son respect. Il est préférable d’effectuer de petits rappels réguliers plutôt que d’agir après un dérapage important. Sans contrôle visible, comme sur la route, l’utilisateur aura tendance à vite oublier le cadre.

4.2.2. Droits de l’utilisateur adéquats

Les droits de l’utilisateur doivent correspondre à ce qu’il peut faire dans le cadre de son travail, c’est-à-dire pouvoir effectuer les opérations nécessaires et avoir accès aux données adéquates, ni plus ni moins.
Donner trop de droit à l’utilisateur ou le rendre administrateur peut amener non seulement à une perte de maîtrise totale sur les programmes installés ou les changements de paramétrage effectués, mais aussi permettre à des logiciels malveillants de profiter de ces droits pour effectuer davantage d’opérations.
Il semble plus compliqué à l’heure actuelle de ne pas proposer d’adresse e-mail ou d’accès internet à l’utilisateur.

Dans ce dernier cas, il est cependant tout à fait possible de limiter l'accès à certains sites internet et de bloquer l'accès aux sites non professionnels.

4.2.3. Accès restreints aux périphériques

Le fait de connecter des supports amovibles aux ordinateurs représente un risque important pour le réseau informatique entier. En effet, tout support amovible comme les clés usb, les appareils photo, peuvent contenir des logiciels malveillants.
Il est donc nécessaire de bloquer l'utilisation des périphériques usb ou des lecteurs de carte sur les ordinateurs.
La solution est de proposer aux acteurs externes un espace protégé pour échanger des fichiers mais aussi de passer par un pc spécifique (non windows par exemple) pour connecter les supports amovibles. Ce n'est pas une protection ultime mais elle permet de limiter ce type d'opérations et de minimiser les risques.

4.2.4. Utilisation personnelle de l'informatique

L'utilisation personnelle de l'outil informatique professionnel est une menace pour sa bonne viabilité.
Amener du matériel personnel doit être interdit par la charte informatique.
Stocker des fichiers personnels également.
L'utilisation de matériel mobile comme les tablettes ou les smartphones à des fins personnelles aussi, même si un réseau wifi public séparé et réservé aux visiteurs est prévu.

4.2.5. Politique des mot de passe

Dans la protection des accès, la politique de mots de passe est très importante.
L'idéal est de centraliser la gestion des mots de passe et d'adopter une politique élaborée, demandant des mots de passe forts ainsi qu'un changement régulier.
Les différentes applications nécessitant un accès utilisateur protégé doivent aussi idéalement se connecter au système d'authentification centralisé.
Chaque utilisateur doit disposer de son propre accès, protégé par un mot de passe personnel.
L'utilisation d'un même accès pour plusieurs utilisateurs doit être proscrite : en plus de diminuer la sécurité, elle empêche la traçabilité des actions dans l'application.

4.3. La formation des utilisateurs

Comme expliqué auparavant, une bonne utilisation de l'outil informatique est très importante et intéressante, autant pour l'institution que pour l'utilisateur. En effet, il est souvent constaté de mauvaises utilisations de l'outil, par manque de connaissance et de formation, qui font perdre du temps à l'utilisateur. Pour ce dernier, il est désagréable de travailler dans un outil non maîtrisé, qui entraîne du doute et de l'inconfort. Il faut rendre à l'utilisateur une place d'acteur dans l'utilisation de l'outil.

Àl'heure actuelle, on peut raisonnablement exiger, lors de l'engagement de nouveaux agents administratifs, de disposer de compétences concernant l'utilisation de base de l'informatique. Cela peut être réalisé via un examen écrit par exemple, testant les connaissances générales sur l'utilisation d'un ordinateur ainsi que l'utilisation des outils bureautiques.

Pour les agents, il est utile et rentable à court terme, de proposer des petits modules de formation, espacés dans le temps pour laisser un temps d'absorption et de mise en oeuvre.
L'apprentissage via des modules en ligne est intéressant dans ce cas, puisqu'ils peuvent être réutilisé à des temps distincts, pour différentes personnes et être revus autant de fois que nécessaire. Un suivi est bien sûr nécessaire pour juger de l'apprentissage réel (également possible en ligne).

Des formations sur des outils plus spécifiques peuvent être réalisées par la société qui les proposent mais il sera toujours nécessaire de proposer à l'utilisateur une documentation et de lui apprendre à l'utiliser, ce qui est rarement un réflexe. Par facilité, on préfère demander ou renoncer, plutôt que de lire et chercher.
Il faut donc aussi motiver l'apprentissage.

La sensibilisation à la sécurité doit faire partie des formations.
Il est préférable de donner certaines clés pour évaluer la dangerosité d'un email par exemple plutôt que de communiquer des peurs vers l'utilisateur. À nouveau pour le rendre acteur et responsable.

La responsabilisation justement n'est possible que si l'information et la formation adéquates ont été préalablement données. L'utilisateur, n'ayant plus l'excuse de dire qu'il ne savait pas, va en général se responsabiliser ou peut être "invité" à l'être.

Les formations visent également à plus d'autonomisation de l'utilisateur par rapport à la résolution de petits problèmes récurrents.

4.4. Le responsable informatique

La partie de présentation concernant les aspects de l'informatique a montré combien ceux-ci peuvent être nombreux et variés.
Il est important de pouvoir maîtriser tous ceux-ci, dans le sens "avoir le contrôle". Sans ce contrôle, il n'est pas possible de prendre des décisions dans cette matière en toute connaissance de cause.
Il est donc important de disposer en interne d'un personne qui aura la maîtrise de la matière informatique, ce qui ne veut pas dire (pour rappel) une personne qui va être spécialiste dans tous les domaines, mais plutôt généraliste.

Le responsable informatique est donc une personne disposant des connaissances et compétences nécessaires pour maîtriser la matière informatique et en assurer la responsabilité, en donnant toutes les informations permettant à la direction de prendre les décisions en toute connaissance de cause, afin d'assurer un bon fonctionnement de l'informatique dans le cadre des missions à réaliser.
Il s'agira donc aussi de mesurer les risques et de proposer les actions à prendre.

Suivant la taille de l'administration, il y aura lieu de comparer les coûts en personnels internes / externes pour assurer les tâches nécessaires à un fonctionnement correct.
Il n'y a pas de formule miracle permettant de calculer le nombre idéal d'informaticiens internes. Et comme déjà énoncé, les plus petites administrations peuvent "partager" un informaticien et mutualiser les énergies en réalisant des projets allant dans le même sens.

Engager un informaticien est évidemment vu comme ayant un coût, et c'est vrai, mais une informatique ne fonctionnant pas bien a également un surcoût certain, pour une niveau d'efficacité très incertain.
Vu l'importance de la matière, il est indispensable de se donner les moyens de la maîtriser.

L'informaticien, face à une matière en constante évolution, aura également la responsabilité de s'informer et de faire de la veille technologique, en suivant des formations (comme celles du RIC), en lisant des articles, en participant à des ateliers, etc... Il faudra donc prévoir un espace dans son temps de travail pour le faire.

4.5. Contrôle et suivi

Afin de disposer d'une vue contrôlée de l'informatique, il est nécessaire d'établir un état des lieux, couramment mis à jour et d'apporter un compte-rendu régulier à la direction.
Cet état des lieux peut consister en les éléments suivants, listés de manière non exhaustives:

- un inventaire suivi du parc informatique, au niveau hardware et software
- un outil de gestion des interventions, afin de les organiser mais aussi de pouvoir faire une analyse "méta" à posteriori
- un outil de monitoring de l'infrastructure: réseau, serveur, etc...
- un outil de contrôle des données, l'objet de la RGPD
- de la documentation, d'un point de vue utilisateur mais aussi des éléments installés par l'informatique
- des rapports variés suivant des réunions régulières par service

5. Conclusion

Comme ce document a pu vous l'expliquer, l'informatique au sein d'un pouvoir local concerne beaucoup d'acteurs différents, tous ayant un rôle à jouer.

On pourrait faire l'analogie suivante pour résumer notre propos.
L'outil informatique est comme un véhicule automobile, mis à la disposition d'un usager pour le mener à destination:

- la direction fournit le véhicule,
- l'informaticien gère la mécanique,
- l'utilisateur conduit le véhicule.

Chaque intervenant occupe une fonction spécifique.
Le propriétaire gère le bien qu'il a acquis, fixe les règles de conduite et d'utilisation pour les conducteurs.
Le mécanicien prépare le véhicule, l'entretient préventivement et effectue les réparations nécessaires.
Le conducteur apprend à manipuler le véhicule, en connaît les possibilités et respecte le cadre d'utilisation.

Minimiser l'importance d'un acteur de ce système, de ses responsabilités et de ses actions mènera à un dysfonctionnement, tôt ou tard.

6. Annexes

Licence Creative Commons