

# Politique d'Infrastructure de l'Entreprise Numérique

---

*Support des nouveaux usages numériques de l'entreprise*

Décembre 2012

## SYNTHÈSE

Aujourd'hui, l'arrivée massive du numérique dans les entreprises apporte une évolution des pratiques et des techniques. Parmi les principes globaux d'infrastructure que cela génère, on peut notamment prévoir une forte croissance des volumétries, que ce soit au niveau du réseau ou du stockage des données, la centralisation des infrastructures ou encore une nouvelle expérience utilisateur (*ATAWAD*<sup>1</sup>, *BYOD*<sup>2</sup>...). Le numérique abolit les frontières (sphère privée/professionnelle, accès aux services à toute heure, connaissance du SI également détenue par les utilisateurs), transforme le *business model* des entreprises. Le numérique est porteur d'opportunités mais apporte aussi de nouveaux risques.

Dans ce contexte, le CIGREF a lancé un groupe de travail en 2011-2012, afin de déterminer les évolutions dans les politiques d'infrastructure des grands groupes dans le cadre de la transformation des entreprises vers l'Entreprise Numérique.

Pour cela, le groupe s'est intéressé à quelques tendances structurantes apparues ces dernières années, et leur impact sur la production des Systèmes d'Information :

- Support des nouveaux usages dans l'entreprise :
  - Gestion des terminaux et applications mobiles
  - Virtualisation du poste de travail
  - Intégration de solutions Cloud
  - Systèmes de téléprésence
- La DSI comme centre de services partagés :
  - Standardisation des processus
  - Centralisation des datacenters
  - Virtualisation des serveurs et du stockage
- Impact sur les ressources humaines

Le numérique est une nouvelle source de performance et d'innovation dans l'entreprise. Mais si les usages sont de plus en plus maîtrisés par l'ensemble des collaborateurs, il est vital que la structure qui les porte soit à la fois solide (assurant la continuité d'activité et la sécurité du patrimoine informationnel) et flexible (permettant l'apparition de nouvelles pratiques dans le SI). La DSI doit pouvoir garantir de telles qualités sur son infrastructure en suivant un certain nombre de bonnes pratiques, qu'elles soient stratégiques, organisationnelles, ou techniques.

---

<sup>1</sup> ATAWAD : Any Time, AnyWhere, Any Device

<sup>2</sup> BYOD : Bring Your Own Device



Le CIGREF, réseau de Grandes Entreprises, a été créé en 1970. Il regroupe plus de cent très grandes entreprises et organismes français et européens de tous les secteurs d'activité (banque, assurance, énergie, distribution, industrie, services...). Le CIGREF a pour mission de promouvoir la culture numérique comme source d'innovation et de performance.

**Titre du rapport : Politique d'Infrastructure de l'Entreprise Numérique**

**Equipe du CIGREF**

Jean-François PÉPIN – Délégué général  
Sophie BOUTEILLER – Directrice de mission  
Anne-Sophie BOISARD – Chargée de recherche  
Josette WATRINEL – Secrétaire de direction

Frédéric LAU – Directeur de mission  
Matthieu BOUTIN – Chargé de mission  
Marie-Pierre LACROIX – Chef de projet  
Josette LEMAN – Assistante de direction

**Remerciements :**

Nos remerciements vont à Oliver URCEL, Directeur des Systèmes d'Information de Canal+, et à François COUTON, Directeur Analyse Prospective et Pilotage de la Performance de Canal+, qui ont piloté cette réflexion.

Nous remercions également les personnes qui ont participé à cette activité :

Laurent CHAIGNEAU – AIR FRANCE  
Emmanuel LE SUEUR – AREVA  
Jean-Philippe DE MICELI – AVIVA  
Philippe GIBERT – AVIVA  
Loïc RICHARD – AVIVA  
Eric TERRIER – BOUYGUES IMMOBILIER  
Frédéric DAMEZ – ESSILOR  
Grégory SILVAIN – EURO DISNEY  
Jean-Michel TURATI – EURO DISNEY  
Dominique FACE – France TELEVISIONS

Marie-Christine MOULLART – GENERALI  
Julio MARTINS – INSERM  
Stéphane LAFAILLE – LA POSTE  
Jean-Luc RAFFAELLI – LA POSTE  
Gérard GAGLIARDI – LISI AEROSPACE  
Mikael POUPON – MAAF  
Pierre ERARD – MAIF  
Jean-François LE ROUX – NEXANS  
Sylvain LAMBERT – POLE EMPLOI  
Soulimane SABIR - RENAULT

Ce document a été rédigé par Matthieu BOUTIN, Chargé de mission CIGREF.

**Pour tout renseignement concernant ce rapport, vous pouvez contacter le CIGREF aux coordonnées ci-dessous :**

CIGREF, Réseau de Grandes entreprises  
21, avenue de Messine 75008 Paris  
Tél. : + 33.1.56.59.70.00  
Courriel : [contact@cigref.fr](mailto:contact@cigref.fr)

Sites internet :  
<http://www.cigref.fr/>  
<http://www.fondation-cigref.org/>  
<http://www.histoire-cigref.org/>  
<http://www.collection-cigref.org/>  
<http://www.entreprises-et-cultures-numeriques.org>

## SOMMAIRE

Introduction .....	1
<b>1 L'Entreprise numérique : enjeux pour l'infrastructure .....</b>	<b>2</b>
1.1 Nouveaux usages numériques .....	2
1.2 Transformation numérique de l'entreprise .....	2
1.3 La standardisation pour gagner en flexibilité.....	3
<b>2 Soutenir les nouveaux usages du numérique .....</b>	<b>4</b>
2.1 <i>Bring Your Own Device</i> : Gestion des terminaux et applications mobiles .....	4
2.1.1 Nouvelle gestion des terminaux mobiles.....	4
2.1.2 Garantir la sécurité des données .....	5
2.1.3 Proposer un <i>set</i> applicatif de base .....	6
2.2 Virtualisation du poste de travail .....	6
2.2.1 Modèle du poste de travail virtualisé .....	6
2.2.2 Points d'attention.....	7
2.2.3 Centraliser les services fichiers, stockage, sauvegarde.....	8
2.2.4 Maîtriser la gestion des identités et des accès .....	8
2.2.5 Limiter les services installés sur le poste .....	9
2.3 Offres de services sur Cloud Externe.....	9
2.3.1 Typologie du <i>Cloud Computing</i> .....	10
2.3.2 Protection des données.....	10
2.3.3 Choix d'un Cloud externe : localisation et réversibilité des données.....	11
2.3.4 La bureautique dans le <i>Cloud</i> .....	12
2.4 Systèmes de téléprésence .....	12
<b>3 La DSI comme centre de services .....</b>	<b>14</b>
3.1 Modèle économique de l'infrastructure .....	14
3.1.1 Définir un nouveau modèle d'offres à destination des clients internes.....	14
3.1.2 Offrir un service comparable à celui des fournisseurs externes.....	15
3.1.3 Définir un modèle de refacturation à l'usage .....	15
3.2 Standardisation.....	16
3.2.1 Mettre en place des référentiels de processus.....	16
3.2.2 Définir des niveaux de service.....	17

<b>4</b>	<b>Quelle infrastructure pour supporter les services partagés.....</b>	<b>18</b>
4.1	Centralisation des <i>datacenters</i> .....	18
4.1.1	Organisation .....	18
4.1.2	Choix géographique.....	18
4.1.3	Consolider avant transformation .....	19
4.1.4	Mettre en place un PRA/PCA .....	20
4.2	Virtualisation des serveurs et du stockage.....	20
4.2.1	Mettre de la puissance informatique à disposition des métiers .....	20
4.3	Offres de services sur <i>Cloud</i> interne .....	21
4.3.1	Principes de mise en œuvre .....	21
4.3.2	<i>Business Case</i> .....	21
4.4	Problématiques réseau.....	22
4.4.1	Offrir aux sites distants le même accès au SI de l'entreprise .....	22
<b>5</b>	<b>Nouvelle gestion des ressources humaines de la production .....</b>	<b>23</b>
5.1	Nouvelles compétences .....	23
5.2	Gestion de l' <i>Offshoring</i> .....	23
5.2.1	Choix de l' <i>offshoring</i> .....	23
5.2.2	Compétences managériales et répartition des niveaux de support.....	24
	<b>Conclusion .....</b>	<b>26</b>

## INTRODUCTION

Avec la transformation numérique des entreprises, les enjeux d'infrastructure sont devenus clés, les entreprises étant amenées à gérer des croissances exponentielles de stockage, de puissance de calcul et de bande-passante. L'infrastructure est en effet la colonne vertébrale du système d'information, base indispensable pour supporter tous les usages numériques de l'entreprise.

Mais cette problématique ne concerne pas uniquement les serveurs, baies de stockage et autres matériels présents dans les datacenters. Le poste de travail est également concerné par cette révolution, avec un poste qui devient de plus en plus virtuel et ubiquitaire, accessible en mode synchrone et asynchrone, en mobilité, et sur tous les écrans.

Ces nouveaux paradigmes de l'infrastructure et de la croissance des ressources numériques se développent dans un modèle économique contraint et sur un plan technologique où de moins en moins de ressources sont gérées directement par l'entreprise.

Aussi, mettre en place une politique d'infrastructure de l'entreprise numérique, c'est déterminer l'ensemble des moyens et des techniques qui supporteront la transformation de l'entreprise, que ce soit en interne comme à l'extérieur. Une infrastructure unifiée et solide permettra de supporter l'intégralité des projets de la DSI. Pour cela, elle doit pouvoir marier l'utilisation des infrastructures déjà existantes dans les entreprises (plus traditionnelles) et les nouveaux paradigmes des dernières années que sont notamment les modèles de services *PaaS (Platform as a Service)* et *IaaS (Infrastructure as a Service)*.

Aujourd'hui, le *Time To Market* des entreprises tend à se réduire de plus en plus, et les infrastructures doivent pouvoir suivre le rythme. Néanmoins, la rationalisation de l'infrastructure est un processus long qui doit s'inscrire dans un plan de plusieurs années. Avoir une politique d'infrastructure pour l'entreprise numérique, c'est avoir une vision, une stratégie, mais aussi déterminer le chemin pour y parvenir. Les DSI doivent alors être les « barons Haussmann » de la transformation numérique en appliquant les concepts de l'urbanisation à l'infrastructure.

Ces nouvelles frontières interpellent les DSI des grandes entreprises françaises et internationales en posant des questions sur le rôle de la DSI et de sa maîtrise des infrastructures, qu'elles soient internes ou externes. Les risques de dépendances sont de plus en plus élevés, les ruptures technologiques de plus en plus rapides, et il est nécessaire de poser quelques principes d'urbanisation et de pilotage de l'infrastructure.

## 1 L'ENTREPRISE NUMÉRIQUE : ENJEUX POUR L'INFRASTRUCTURE

### 1.1 NOUVEAUX USAGES NUMÉRIQUES

Aujourd'hui, la révolution numérique bouleverse nos habitudes, que ce soit dans la sphère personnelle ou dans la sphère professionnelle. Elle se manifeste au travers de différents facteurs exogènes, dont l'entreprise doit prendre acte afin de modifier ses modèles de fonctionnement.

L'utilisateur des systèmes d'information a profondément changé. Il développe davantage sa propre vision des technologies de l'information et la manière de les consommer, ce qui cause une fusion de plus en plus importante entre l'IT<sup>3</sup> personnel et l'IT professionnel, notamment en termes de pratiques. A titre d'exemple, avec le développement de la mobilité, les utilisateurs ont pris l'habitude de rechercher des applications sur des boutiques en ligne pour les aider dans leurs tâches quotidiennes. En conséquence, cette pratique est maintenant souhaitée au sein de l'entreprise par les utilisateurs.

La pression du marché est également très forte sur les usages des technologies de l'information. Tous les trois mois, de nouveaux terminaux sont déployés sur le marché, et achetés par les utilisateurs de l'entreprise, à des fins privées. Accédant ainsi aux dernières technologies et à l'efficacité que celles-ci peuvent apporter, l'utilisateur souhaitera alors disposer des mêmes possibilités sur son lieu de travail. Comment l'entreprise peut-elle alors suivre le rythme ? Dans l'état actuel des processus de l'entreprise, pour chaque nouveauté, il faudrait établir de nouveaux processus de sécurité et mettre à jour le parc des processus et des applications, si bien qu'il faudrait environ un an pour ajouter le terminal au catalogue de l'entreprise, qui sera alors obsolète. Comment alors ne pas subir ce rythme ?

Enfin, à travers les nouvelles tendances du *Cloud Computing*, les directions métiers peuvent maintenant prendre directement des services sur internet sans passer par la DSI. Comment cette dernière peut-elle alors assurer la sécurité et la compatibilité des données et des processus sur l'ensemble du système d'information ?

### 1.2 TRANSFORMATION NUMÉRIQUE DE L'ENTREPRISE

Le numérique a un impact très fort sur l'organisation de l'entreprise. L'entreprise traditionnelle doit alors évoluer pour devenir une « entreprise numérique », en définissant

---

<sup>3</sup> IT : *Information Technology*

une vision numérique et un plan numérique pour toutes les dimensions de son modèle d'affaires. Les *business models* se transforment, et la plupart des sociétés se lancent dans la numérisation de leurs produits, qu'ils soient culturels, bancaires, issus de la grande distribution ou de l'industrie.

Au sein de l'entreprise, le numérique abolit un certain nombre de frontières. S'il y a imbrication des usages professionnels et privés sur le poste de travail, le phénomène va encore plus loin car les utilisateurs en viennent à importer leurs pratiques personnelles dans la sphère professionnelle, et demandent l'accès au système d'information à toute heure, tous les jours. De plus, les connaissances numériques ne sont plus détenues uniquement par la DSI, les Directions Métier ayant considérablement gagné en expertise et maturité sur ce sujet.

Ces nouvelles pratiques apportent un certain nombre de risques à prendre en compte, que ce soit au niveau de l'e-réputation, des données stratégiques, du risque systémique, de l'atteinte aux données personnelles ou de la conservation des données numériques.

Face à l'ensemble de ces problématiques, la DSI se doit d'accompagner l'entreprise dans sa révolution numérique. Devant faire face à ces nouvelles pratiques et aux nombreuses technologies émergentes, elle doit donc mettre en place une politique d'infrastructure solide, qui repose à la fois sur une revue de son modèle économique, sur une refonte de ses processus et de ses infrastructures, et sur une nouvelle organisation.

### 1.3 LA STANDARDISATION POUR GAGNER EN FLEXIBILITÉ

Les utilisateurs et les directions métiers, par leurs nouvelles pratiques numériques, attendent un service le plus personnalisé possible. A l'image des usages personnels, la DSI doit aujourd'hui avoir des offres qui correspondent le plus possible à ses clients, sous peine de se voir écarter au profit de prestations extérieures à l'entreprise. La DSI n'est plus nécessairement le seul fournisseur informatique dans l'entreprise. Ce point est important sur la réflexion de la politique d'infrastructure. Elle doit donc proposer une grande flexibilité dans ses offres, ce qui sera facilité par une standardisation de son infrastructure.

Ce rapport sera pour nous l'occasion de regarder les éléments d'infrastructure qui soutiennent les nouveaux usages du numérique dans l'entreprise, et de voir la politique à mettre en place pour gérer efficacement ces paradigmes.



## 2 SOUTENIR LES NOUVEAUX USAGES DU NUMÉRIQUE

Un certain nombre d'usages du numérique ont fait leur apparition dans l'entreprise ces dernières années et ont radicalement changé le lien entre l'utilisateur et le système d'information, si bien que deux éléments majeurs qui révolutionnent l'environnement de l'infrastructure pour les utilisateurs peuvent être identifiés.

Le premier point est que l'environnement de travail des collaborateurs de l'entreprise devient intégralement numérique, amenant de nouvelles règles induites. L'accélération des échanges et la connexion permanente des utilisateurs en sont des exemples.

Un deuxième élément est notre entrée dans une ère où les utilisateurs en savent autant, si ce n'est plus, que la DSI sur les usages du numérique et sont beaucoup plus impliqués dans la gestion de l'informatique de manière générale. Une responsabilité plus grande leur est donc donnée. Par exemple la sécurité du SI repose autant sur la mise en place technique faite par la DSI que sur la bonne utilisation dans le respect des règles (ex : complexité du mot de passe).

Dans ce contexte, le groupe de travail s'est notamment intéressé aux usages suivants :

- La gestion des terminaux et des applications mobiles,
- La gestion du poste de travail virtualisé,
- L'usage des modèles de services portés par le *Cloud Computing*.

### 2.1 BRING YOUR OWN DEVICE : GESTION DES TERMINAUX ET APPLICATIONS MOBILES

#### 2.1.1 Nouvelle gestion des terminaux mobiles

En France, le *Bring Your Own Device*, pratique visant à laisser le collaborateur de l'entreprise utiliser un terminal personnel dans le cadre professionnel, n'est pas une pratique largement répandue. Elle prend en effet davantage la forme de prospectives ou de pilotes sur certaines populations que d'actions concrètes.

Pourtant, la demande des utilisateurs finaux est forte. Les usages qu'ils ont de leurs terminaux personnels sont particulièrement évolués, facilitant leur vie de tous les jours, si bien qu'ils souhaiteraient les utiliser dans leur sphère professionnelle. Certaines entreprises ont d'ailleurs vues le *BYOD* s'implanter malgré elles, observant un nombre de connexions au SI par des terminaux plus grand que le nombre de terminaux distribués par l'entreprise.

La prise en compte de cette pratique nécessite une remise en question forte des pratiques d'infrastructure et de sécurité, ainsi que le développement d'une véritable « vision produit » sur le service rendu aux utilisateurs, puisque le matériel n'est plus imposé.

Pour ce faire, il est nécessaire de réaliser une étude de marché interne, en se posant quelques questions clés :

- Qui sont les « clients » ?
- Quels sont les usages souhaités ?
- Comment l'infrastructure de l'entreprise peut faire le lien entre ces clients et ces usages en garantissant accessibilité et sécurité ?

Afin de gérer au mieux cette problématique et de proposer l'accès au SI à tous les types d'appareils, il est nécessaire de s'affranchir du *device* d'entrée. Il n'est alors plus nécessaire d'intégrer les terminaux mobiles dans les flottes des entreprises, mais il faut néanmoins garantir la sécurité et l'accessibilité aux données de l'entreprise en poussant sur ces appareils un *set* applicatif<sup>4</sup> minimum, qui lui est géré par l'entreprise.

### 2.1.2 Garantir la sécurité des données

La sécurité des données sur les terminaux mobiles passe par deux aspects : la responsabilité humaine et les solutions techniques.

De tels projets sont forcément structurants pour l'entreprise et nécessitent de mettre à jour la politique d'usage. Dans ce cadre, les chartes informatiques existantes doivent être modifiées pour déléguer la responsabilité des données contenues dans le terminal aux utilisateurs concernés. Lui sera donc déléguée la gestion de ses accès (mots de passe), ainsi que l'entretien de son appareil.

D'un point de vue technique, il doit être notamment possible à l'entreprise d'effacer des données confidentielles d'un *device* perdu ou volé. Ce dernier doit donc nécessairement comporter un outil ou un paramétrage particulier permettant de réaliser cette manipulation. Ce point doit également être mentionné dans la charte d'utilisation informatique de l'entreprise afin de tenir l'utilisateur informé si la situation se présente.

Si les terminaux mobiles ne sont plus intégrés dans les flottes de l'entreprise, la sécurité sur ceux-ci ne peut plus être périmétrique (directement sur l'appareil), puisque l'entreprise ne gère pas le matériel. L'attention doit alors être portée directement sur les applications et les données de l'entreprise auxquelles l'utilisateur accédera.

---

<sup>4</sup> Ensemble cohérent d'applications nécessaires au bon fonctionnement du *device* ou du poste de travail dans le cadre d'une utilisation professionnelle.

Il est alors nécessaire de fournir une bulle applicative qui dépendra du mode de connexion. Il y aura donc de gros challenges de sécurité active sur la donnée en déterminant qui se connecte et par quel mode (*device* d'entreprise ou non), modifiant ainsi dynamiquement les sets applicatifs particuliers autorisés.

### **2.1.3 Proposer un set applicatif de base**

Pour garantir l'expérience utilisateur, la DSI doit donner à l'utilisateur, la possibilité de récupérer les applications de l'entreprise sur le terminal avec la même facilité que pour celles proposées dans le grand public. Par ce moyen, quel que soit l'objet technologique choisi par l'utilisateur, il aura la même garantie d'accès au système d'information.

Cette pratique impose à la DSI d'être capable d'assurer le support de ses applications sur toutes les plateformes existantes. Sur le plan organisationnel, là où des équipes se chargeaient auparavant de qualifier et d'intégrer des terminaux déterminés aux flottes, avec un support d'applications sur un nombre limité de plateformes, il faut désormais assurer le développement de chaque outil pour toutes les versions de terminaux et leurs systèmes d'exploitation associés.

Par ailleurs, par delà leur création, la mise à disposition d'applications d'entreprise impose la création d'« *Application Stores* » particuliers et sécurisés. Cela change la gestion des offres de services, à la fois pour les équipes techniques et pour les utilisateurs finaux. Auparavant, lorsqu'un collaborateur avait besoin d'une application, il devait laisser son poste à un opérationnel IT qui se chargeait de l'opération, en général lourde. Maintenant, la responsabilité est déchargée sur le client, qui gère lui-même l'installation de ses outils, les équipes techniques étant alors dédiées au support de la plateforme de récupération des applications.

## **2.2 VIRTUALISATION DU POSTE DE TRAVAIL**

Au-delà des terminaux mobiles, les usages numériques touchent le poste de travail. Aujourd'hui, afin d'augmenter la flexibilité de son utilisation, la virtualisation sort du cadre des datacenters pour s'attacher aux postes de travail et aux applications auxquelles ils permettent d'accéder.

### **2.2.1 Modèle du poste de travail virtualisé**

Le poste de travail évolue avec la mobilité des employés dans l'entreprise. L'utilisateur doit pouvoir accéder à ses données et ses applications en déplacement géographique, mais également d'un poste à un autre au sein d'un même lieu (par exemple une agence

commerciale, où les employés sont amenés à changer de fonction au cours de la journée). La virtualisation du poste de travail permet de répondre à ces nouvelles attentes.

Le *business case* de la virtualisation du poste de travail peut être justifié par la grande souplesse et l'agilité que ce procédé apporte. Le poste virtualisé n'est pas lié à une machine utilisatrice physique, mais est constitué d'une image hébergée sur une infrastructure centralisée (serveur et stockage) dans un *datacenter* de l'entreprise.

Ainsi, un certain nombre d'applications concrètes de la technologie sont observables. Le poste virtualisé offre notamment la possibilité d'ouvrir des services à l'international sans avoir à installer des infrastructures locales particulières, le seul besoin étant une connexion à Internet suffisamment rapide et sécurisée pour accéder au *datacenter* hébergeant l'image.

De même, dans le cas où un prestataire, *offshore* ou non, doit avoir accès au SI de l'entreprise, il est intéressant de l'équiper d'un poste de travail virtualisé, et hébergé dans les *datacenters* de l'entreprise cliente en France. Il est alors aisé d'organiser un changement de prestataire, sans s'inquiéter de la sécurité des données.

Enfin, le déploiement de postes de travail virtuels et la diffusion de nouvelles applications peuvent être réalisés à très grande vitesse. En effet, contrairement à une installation classique nécessitant une action manuelle sur chaque poste de travail, la constitution d'une image des applications et la sauvegarde des sessions utilisateurs sur les infrastructures centralisées sont suffisantes, leur diffusion étant automatisée.

### 2.2.2 Points d'attention

La virtualisation du poste de travail apporte un intérêt fort pour l'entreprise. Néanmoins, il y a certains pièges à éviter dans la mise en place de cette solution.

Un problème récurrent est celui de la compatibilité de certaines applications avec les systèmes d'exploitation ou d'autres programmes (comme certains navigateurs), majoritairement utilisés sur les postes de travail. Cela implique que toutes les applications ne sont pas virtualisables.

Il faut également se méfier de la volumétrie que représentent les postes virtualisés dans les *datacenters*. Il faut donc veiller à garder un *capacity planning*<sup>5</sup> cohérent dans la gestion du stockage.

Ensuite, la capacité du poste de travail à recevoir la session de l'utilisateur est primordiale. En effet, les connexions simultanées en fonction des moments clés de la journée (début de

---

<sup>5</sup> Plan de gestion de la capacité des ressources

matinée, retour de la pause déjeuner) peuvent entraîner des volumétries importantes en termes d'occupation du réseau, et peuvent en effet poser des problèmes sur l'infrastructure. Cette volumétrie de connexion de l'utilisateur doit alors être calculée lors du dimensionnement initial, au début du projet de mise en place de la virtualisation du poste de travail.

Enfin, les utilisations d'un poste de travail dans une entreprise peuvent être diamétralement opposées, si bien que le besoin d'avoir des socles avec des systèmes d'exploitation différents se fait sentir, en prenant compte des solutions Windows comme des solutions libres.

### **2.2.3 Centraliser les services fichiers, stockage, sauvegarde...**

Le poste de travail étant le premier moyen d'accès au système d'information, son changement nécessite la centralisation des infrastructures qui y sont liées : fichier, stockage, sauvegarde, etc.

Un certain nombre de services centralisés sont liés à l'utilisation du poste de travail. Parmi eux, on peut recenser :

- Des accélérateurs de flux, nécessaire pour faire afficher les bonnes applications et les bonnes données sur le poste utilisé ;
- Des services de fichiers ;
- Des applications métiers (applications financières par exemple)
- Des politiques de changement de mots de passe pour la gestion d'identité...

L'objectif de cette centralisation des services est de supprimer les serveurs de proximité. Elle reposera sur un *datacenter* centralisé et dupliqué pour gérer la sécurité.

Le corolaire de cette centralisation des services et du découplage matériel/logiciel est une modification des besoins de support aux utilisateurs. En effet, les demandes aux centres d'appels sont majoritairement de type applicatif, l'utilisateur n'ayant aucune visibilité sur ce qui est derrière ses applications.

### **2.2.4 Maîtriser la gestion des identités et des accès**

Avec la mutualisation des postes de travail physiques, il est nécessaire d'encadrer leur utilisation par de la gestion d'identité.

La gestion d'identité dans le cadre de la virtualisation de poste couple deux identifications : celle de la machine physique, et celle de l'utilisateur. La typologie des postes de travail de l'entreprise permet de définir rigoureusement la relation entre une catégorie particulière de postes et les applications autorisées à y fonctionner. De la même manière, il est nécessaire de déterminer les droits des utilisateurs à accéder aux applications. Ainsi, la gestion

d'identité permettra l'accès uniquement aux applications autorisées pour la machine et l'utilisateur.

Par ailleurs, un utilisateur s'identifie un très grand nombre fois dans la même journée, impliquant le besoin d'un accès transparent aux applications avec un mot de passe unique pour faciliter les usages. D'un point de vue métier, les employés n'ont pas nécessairement la même activité au cours de la journée et n'utilisent pas le même poste de travail physique. Ce point doit pouvoir être géré par le système de gestion d'identité.

Cette problématique s'applique aussi pour la téléphonie. Une authentification couplée peut être notamment réalisée par l'utilisation de *softphones*, logiciels utilisés pour faire de la téléphonie par internet depuis un ordinateur.

### **2.2.5 Limiter les services installés sur le poste**

Le poste s'appuie ainsi sur la publication locale des données de l'utilisateur, la virtualisation d'applications et la virtualisation du poste de travail, avec une identification du lieu d'exécution. Les seuls services obligatoires demeurant sur le poste client sont alors le service d'impression et le service d'inventaire et d'usage (y compris qualité).

## **2.3 OFFRES DE SERVICES SUR CLOUD EXTERNE**

Les offres de services basées sur les technologies de *Cloud Computing* constituent une nouvelle pratique sur laquelle les directeurs généraux et métiers peuvent challenger la DSI. Cette dernière doit donc être en mesure de dire si il faut y aller et pourquoi.

Les modèles de services *SaaS (Software as a Service)*, *PaaS (Platform as a Service)* et *IaaS (Infrastructure as a Service)* permettent en effet d'accéder à des services en ligne, sans se préoccuper des problématiques techniques qui les supportent. Ils peuvent être proposés par la DSI en interne de l'entreprise, ou bien par des sociétés prestataires extérieures.

En ce qui concerne la production en particulier, le *Cloud* est une opportunité car, qu'il soit interne ou externe, il apporte de nouvelles possibilités dans son panel de solutions. Parmi les avantages remarquables du *Cloud* pouvant être mis en avant, se trouve la possibilité de maîtriser ses coûts et même de les réduire puisque ces modèles engagent une facturation à l'usage pour les infrastructures et les services.

Dans cette partie, nous nous intéresserons aux usages du *Cloud* dans l'entreprise. Le point particulier de la mise en place d'un *Cloud* interne sera évoqué dans le chapitre « Quelle infrastructure pour supporter les services partagés » de ce rapport.

### 2.3.1 Typologie du *Cloud Computing*

Le groupe de travail « Le *Cloud* dans le SI des entreprises <sup>6</sup>», mené par le CIGREF en 2011/2012, a revisité les fondamentaux du *Cloud Computing*, et identifié trois règles essentielles qui le caractérisent. Le *Cloud* est donc un espace virtuel qui bénéficie d'une facturation à la demande, d'une allocation dynamique des ressources nécessaires, et qui a une seule version multi-tenant (évolutions des versions au fil de l'eau par le fournisseur, tous les clients étant sur la même version).

Le *Cloud Computing* peut être décomposé en quatre catégories, selon qu'il est :

- à usage dédié aux besoins propres de l'entreprise (**PRIVÉ**)
- ou dédié aux besoins du grand public ou d'une autre organisation externe à l'entreprise (**OUVERT**) ;
- et qu'il soit géré directement dans l'entreprise (**INTERNE**)
- ou par un autre opérateur (**EXTERNE**).

### 2.3.2 Protection des données

Le choix d'une solution de *Cloud* externe doit faire l'objet d'un processus de décision poussé, de par les enjeux existants, les données de l'entreprise étant confiées à une organisation tierce. La question de la sécurité des données et de leur réversibilité est primordiale.

Dans ce contexte, le CIGREF, l'IFACI et l'AFAI se sont associés pour écrire un guide pratique à l'attention des directions générales et opérationnelles titré « *Cloud Computing* et protection des données <sup>7</sup>» (2012). La position commune des trois associations comporte quatre messages clés :

- Le *Cloud* présente de nombreux avantages d'agilité, de souplesse et de réduction des coûts, mais il est aussi susceptible d'exposer les entreprises à des risques sur leurs données.
- Il est important de s'engager dans le *Cloud* avec les différentes parties prenantes, les métiers, la DSI, les Achats, l'audit interne, le Juridique, le *Risk Management*, le Contrôle Interne...
- Il est important de se poser les bonnes questions pour faire les bons choix : quel *Cloud* pour quel usage ?
- Il faut se doter des moyens de protection des données adaptés aux plans contractuels et opérationnels par la mise en place d'un environnement de contrôle.

---

<sup>6</sup> <http://www.cigref.fr/cloud-computing-si-entreprise-2012>

<sup>7</sup> <http://www.cigref.fr/cloud-protection-donnees-guide-pratique-direction-operationnelle-generale>

### 2.3.3 Choix d'un Cloud externe : localisation et réversibilité des données

Le choix de se tourner vers un prestataire de Cloud externe ou un autre est une réflexion propre à chaque entreprise, qui doit être réalisée minutieusement en considérant certains aspects clés. Ainsi, la sécurité des données, leur localisation et leur réversibilité sont des critères primordiaux à prendre en compte.

La localisation des données a des répercussions juridiques fortes. En effet, certains pays disposent de règles permettant à leur gouvernement d'accéder à tous types de données hébergées sur le territoire national. C'est le cas notamment des États-Unis avec le *Patriot Act*, mais également dans un grand nombre de pays européens. Cette problématique peut aujourd'hui être contournée grâce à l'émergence de solutions de *Clouds* souverains, comme le projet Andromède en France. Elles garantissent ainsi une localisation globale des données en France, les *datacenters* y étant tous situés.

Le principe même du Cloud comprend le fractionnement des données et leur répartition sur les datacenters de l'hébergeur. Ainsi, ce dernier n'est pas en mesure de déterminer avec précision la localisation exacte d'une information sur un serveur. Néanmoins, légalement, les données et leur traitement doivent être situés dans une même zone géographique. Il est donc important d'avoir une garantie contractuelle sur ce point avec le fournisseur de service.

A titre d'exemple, dans l'état actuel des choses, Google ne révèle pas le lieu de stockage de ses données, leur modèle de fonctionnement leur permettant de les basculer dynamiquement dans tous leurs datacenters. D'un autre côté, le modèle Office 365 de Microsoft fait que les données resteront dans la même zone géographique que le client. Ainsi, en fonction des prestataires et des typologies de services, on a un engagement ou pas sur le lieu de stockage de la donnée.

Une autre problématique importante à prendre en compte est la réversibilité des données. En effet, dès la contractualisation d'une offre *Cloud*, la question de la sortie de la prestation doit être abordée, et en particulier celle de la récupération en interne des données hébergées à l'extérieur, l'entreprise devant pouvoir retrouver son indépendance. Ce point doit s'appuyer à la fois sur des clauses contractuelles dédiées et des principes d'architecture permettant la compatibilité des données entre les systèmes de *Cloud* externe et le système d'information de l'entreprise.

A l'heure actuelle, les offres de Cloud Computing ne sont pas encore complètement matures, mais le marché avance à grande vitesse dans ce domaine. Les directions métiers pouvant souscrire elles-mêmes à des offres du marché, la DSI se doit d'avoir une expertise sur le sujet et un rôle de conseil quant aux risques et aux opportunités inhérentes à ce nouveau modèle de services. Après résolution des problématiques détaillées ci-dessus,



l'entreprise pourra choisir de prendre une offre de service dans un *Cloud* externe ou de lui préférer des solutions en interne.

### **2.3.4 La bureautique dans le *Cloud***

Parmi les choix de solutions à basculer dans le *Cloud* qui peuvent être réalisés, la migration des outils de bureautique sur des supports en ligne est particulière. Ainsi, l'usage d'un acteur du *Cloud* pour la messagerie et les documents modifie fortement les usages des utilisateurs. En effet, ce point touche la base même des habitudes de travail des salariés de l'entreprise.

Les outils de bureautique dans le *Cloud* apportent un grand nombre de nouvelles pratiques qui sont des opportunités pour améliorer la performance des salariés. A titre d'exemple, ils permettent notamment de simplifier le partage de documents, donnant l'opportunité à l'utilisateur de gérer les droits de modification des autres accédants, sans devoir passer par les informaticiens, tout en conservant les habitudes d'édition développées sur les outils historiques. Ce point doit faire l'objet d'une sensibilisation forte à la sécurité des informations gérées.

En ce qui concerne la messagerie, une solution en *Cloud* comme Google offre la possibilité de disposer de la vidéo avec la messagerie instantanée. Si ce cumul de possibilités est particulièrement appréciable, une attention particulière doit être portée lors de la définition de l'architecture supportant ces offres, car il faudra prévoir un réseau capable de supporter l'accroissement de la charge due à l'utilisation de ces nouveaux outils et usages.

Le modèle Google est un abonnement par utilisateur, pour l'intégralité des services possibles, avec entre autres les fonctions messagerie instantanée, messagerie, applications, sites... Ce périmètre applicatif large, accessible via une simple combinaison identifiant/mot de passe, doit faire l'objet d'une étude de sécurité, pour laquelle il est possible (voire nécessaire) de coupler une solution de protection/identification externe (SSO). Ici encore, il est primordial que les utilisateurs soient sensibilisés à la sécurité des systèmes.

Pour éviter un changement trop violent des habitudes, un basculement progressif peut être réalisé. Les licences déjà acquises de logiciels bureautiques installés permettent de les conserver sur le poste de travail, en parallèle des nouvelles solutions. La possibilité est donc laissée aux employés de travailler sur les deux solutions.

## **2.4 SYSTÈMES DE TÉLÉPRÉSENCE**

La téléprésence est une pratique collaborative permettant d'organiser des réunions de travail avec des intervenants à distance. Dans les entreprises multinationales, la multiplicité des sites impose la mise en place de systèmes de téléprésence, afin de réduire les

déplacements et, par extension, les coûts. Cet apport est mesurable en termes de retour sur investissement, représentant un gain net important.

Il est cependant nécessaire de faire attention à bien définir la volumétrie des besoins lors de la préparation du projet. Un dimensionnement insuffisant de l'infrastructure dédiée entraînerait en effet un retour aux pratiques antérieures (déplacements) à cause d'une surcharge du système. Il faut notamment avoir un nombre adéquat de salles de visioconférence, ou de toutes autres solutions alternatives (*webcams* dédiées, logiciels de visioconférence sur le poste de travail), ainsi qu'un accès au réseau suffisamment fiable, rapide et sécurisé.

### *Éléments clés du chapitre*

- **Gestion des terminaux et applications mobiles**
  - **BYOD : ne plus intégrer les terminaux mobiles dans les flottes**
  - **Faire de la sécurité sur la donnée et non de la sécurité périmétrique**
  - **Proposer un set applicatif de base**
- **Virtualisation du poste de travail**
  - **Centraliser les services fichiers, stockage, sauvegarde...**
  - **Maîtriser la gestion des identités et des accès**
  - **Limiter les services installés sur le poste**
- **Intégration de solutions *Cloud* externes**
  - **Assurer l'interface entre les services souscrits par les métiers et les infrastructures de l'entreprise**
- **Systemes de téléprésence**
  - **Prévoir un dimensionnement suffisant des infrastructures d'utilisation**

### 3 LA DSI COMME CENTRE DE SERVICES

#### 3.1 MODÈLE ÉCONOMIQUE DE L'INFRASTRUCTURE

Au sein de l'entreprise numérique, la maîtrise du Système d'Information n'est plus réservée à la seule DSI. Les directions métiers ne sont donc plus amenées à travailler avec la DSI de la même manière. En effet, elles peuvent désormais prendre leurs propres solutions, ne demander que certaines couches d'infrastructures à la DSI, ou bien continuer à fonctionner en mode projet avec elle. Le panel d'offres de la DSI augmente donc drastiquement et leur gestion doit faire l'objet d'une attention particulière.

##### 3.1.1 Définir un nouveau modèle d'offres à destination des clients internes

Si auparavant le modèle « *design, build, run* » suffisait pour faire fonctionner les projets communs avec les métiers de l'entreprise, il est nécessaire aujourd'hui de lui ajouter un modèle « *source, integrate, manage* » pour gérer l'ensemble des demandes et accompagner le changement de l'entreprise. La relation MOA-MOE laisse alors la place à une forme de relation client-fournisseur.

La gestion de l'infrastructure doit donc être revue et doit faire l'objet d'un nouveau modèle économique afin de répondre aux différentes sollicitations de l'entreprise.

La politique d'infrastructure de l'entreprise numérique est pilotée par trois principes phares, qui caractérisent les nouvelles attentes des utilisateurs du SI de l'entreprise :

- ATAWAD : *Any Time, Any Where, Any Device*,
- SOLOMO : Social, Local, Mobile,
- BYOD : *Bring Your Own Device*.

A la manière d'une entreprise indépendante, ce nouveau modèle d'affaires se doit de répondre à l'attente du marché. Il est alors nécessaire, pour chaque couche d'infrastructure, de proposer un certain nombre d'offres, qui seront accessibles à l'entreprise ou à son environnement.

Les infrastructures peuvent être segmentées en couches comme suit :

- Réseau
- Stockage
- Système
- Plateforme de Relation Client
- Terminaux mobiles et fixes
- Bureautique

Cette dernière est par ailleurs particulièrement liée aux nouveaux usages des utilisateurs et se doit de faire l'œuvre d'une attention particulière.

Par ailleurs, au-delà des usages, les avancées technologiques apportent également leur lot de problématiques. En effet, en ce qui concerne l'infrastructure interne, il faut intégrer une rupture technologique, notamment avec une nouvelle volumétrie de données et le *multidevice* amène des difficultés supplémentaires en matière de gestion.

### **3.1.2 Offrir un service comparable à celui des fournisseurs externes**

Avec l'avènement du *Cloud Computing*, le risque que les directions métiers externalisent leurs services est présent. La tentation de ne pas passer par le fournisseur interne qu'est la DSI est donc un facteur grandissant, notamment dans un contexte de crise, où la recherche de l'efficacité financière prime souvent sur la réflexion de l'architecture du SI et de la sécurité.

La contrainte de ce phénomène est donc forte sur les nouveaux modèles d'affaires de l'infrastructure, qui doit donc être non seulement efficace, mais également compétitive dans ses tarifs.

Pour faire valoir sa légitimité à supporter les projets des métiers, la DSI va alors devoir mettre en avant sa capacité à sécuriser les données stratégiques et sensibles de l'entreprise, à assurer la solidité de l'infrastructure, tout en proposant des solutions de facturation à la hauteur de celles du marché.

### **3.1.3 Définir un modèle de refacturation à l'usage**

Pour faire valoir ses nouvelles offres d'infrastructure, la DSI doit alors mettre en place un politique de facturation qui peut prendre deux formes :

- Un modèle de coût par service,
- Un modèle de refacturation à l'usage.

Le modèle de coût par service se base sur la mise en place d'un catalogue de services. Le client interne pourra donc faire ses achats, à la manière d'un utilisateur de boutique en ligne, et sera facturé directement en fonction des services choisis, sa demande étant satisfaite par les équipes de la DSI.

Le modèle de refacturation à l'usage permet la mise en place d'un « self-service » de la puissance informatique. L'utilisateur peut alors choisir la quantité de « puissance informatique » dont il a besoin, qu'il s'agisse d'espace de stockage, de capacité de sauvegarde ou de puissance processeurs... Il est à noter que cette solution n'est pas nécessairement la plus adaptée au client, car les architectes clients ne savent pas forcément

définir leurs besoins réels (volumétrie...) sans assistance de la DSI, entraînant une sous ou sur-utilisation de ressources.

Il s'agit ensuite de déterminer comment financer les infrastructures non utilisées. Un modèle possible est de répartir le coût de ces infrastructures entre les différentes entités utilisatrices au sein de l'entreprise.

## 3.2 STANDARDISATION

Dans l'entreprise numérique, la DSI fait face à une double problématique :

- augmenter son nombre d'offres pour coller le plus fidèlement possible aux attentes des utilisateurs,
- réduire au maximum le temps de distribution d'un service à l'utilisateur.

Pour résoudre ce point, il est nécessaire de mettre en place une standardisation des processus et des couches d'infrastructures les plus basses.

### 3.2.1 Mettre en place des référentiels de processus

La standardisation des processus passe par la mise en pratique d'un référentiel de bonnes pratiques. Dans ce contexte, ITIL est largement reconnu et utilisé au sein des grandes entreprises françaises.

Ce référentiel est particulièrement adapté à la considération du nouveau modèle d'affaire de la DSI. ITIL comprend plusieurs modules facilitant la mise en œuvre d'un centre de services focalisé sur l'utilisateur. En effet, la partie « catalogue de services » permet de structurer et de mettre à disposition des utilisateurs de l'entreprise l'ensemble des offres de la DSI. De la même manière, les parties « gestion des problèmes, des incidents et des changements » permettent de suivre efficacement l'activité opérationnelle de la DSI, et de structurer le support qui sera apporté aux utilisateurs.

Il faut néanmoins s'assurer de la pertinence à suivre une standardisation complète. En effet, selon les cas, il peut être nécessaire de procéder à une différenciation géographique des offres de services et du support, selon les réglementations en vigueur et les contraintes technologiques.

Ainsi, le département des infrastructures prend la forme d'un centre de services partagés global. Les clients sont les DSI métiers, avec une vision différente selon la zone géographique, permettant l'optimisation des zones déjà développées ou l'accompagnement de la croissance des autres.

L'apport d'offres standardisées pourra notamment répondre aux besoins en postes de travail, stockage, serveurs, réseau, etc.

### 3.2.2 Définir des niveaux de service

La standardisation des offres et des processus impose une surveillance continue de la qualité des services proposés. La définition de niveaux de service est alors primordiale, car elle permettra à la fois à la DSI de suivre son activité en repérant les points d'attention, mais également au client interne de bénéficier de garanties sur les offres de services qu'il a souscrites.

Parmi les actions à mener, la mise en place d'un « *Disaster Recovery Plan* » et d'options de sécurité particulières sont primordiales. Il faudra notamment veiller à supprimer l'ensemble des points de concentration (SPOF – *Single Points of Failure*).

#### *Éléments clés du chapitre*

- **Modèle économique de l'infrastructure**
  - Offrir un service comparable à celui des fournisseurs externes
  - Définir un modèle de refacturation à l'usage
  - Constituer des offres pour les clients internes
- **Standardisation**
  - Mettre en place des référentiels de processus
  - Définir des niveaux de service
- **Centralisation des services**
  - Mettre en place des catalogues de services pour les clients internes (*Self Service* pour les métiers)

## 4 QUELLE INFRASTRUCTURE POUR SUPPORTER LES SERVICES PARTAGÉS

### 4.1 CENTRALISATION DES *DATACENTERS*

Pour supporter la mise en place de services partagés et la standardisation des infrastructures, la limitation du nombre de *datacenters* à gérer s'avère primordiale. La rationalisation des infrastructures est également intéressante d'un point de vue des coûts de fonctionnement. En effet, lorsqu'une multiplication des *datacenters* est constatée, il apparaît souvent qu'une équipe IT indépendante est dédiée à chaque *datacenter*, et que l'espace physique utilisé est très faible par rapport à la contenance globale, représentant ainsi une perte nette.

Opérer une centralisation des *datacenters* est donc intéressante pour :

- Limiter les coûts de fonctionnement,
- Offrir des services centralisés,
- Assurer des niveaux de services élevés.

#### 4.1.1 Organisation

Pour un projet international d'une telle ampleur, il est nécessaire d'avoir un *leadership* fort au niveau central pour la gouvernance, pour pallier aux réticences des équipes de gestion locales des *datacenters* qui seront supprimés. Ainsi, il peut être envisagé de mettre en place un groupement d'intérêt économique (GIE) informatique spécifique pour suivre cette nouvelle infrastructure, aidé ou non d'un prestataire extérieur.

La taille d'un tel projet nécessite notamment de mettre en place une équipe dédiée d'acheteurs.

Le choix de mener une centralisation de *datacenters* entre dans le cadre d'une évolution de politique d'infrastructure globale. Les freins au changement qui peuvent exister seront majoritairement d'ordre légal (gestion des données) ou organisationnel (refonte de l'organigramme de gestion des sites distants).

#### 4.1.2 Choix géographique

La centralisation des *datacenters* implique de faire un grand nombre de choix structurants. Parmi ceux-ci, le choix de la position géographique des *datacenters* centraux est primordial, car ces derniers nécessiteront un certain nombre de sécurités.

Déjà, pour des raisons de protection des données, il est important de rester dans le cadre de l'Union Européenne. Mais au sein même des pays européens, des différences techniques

fortes subsistent, notamment au niveau de la qualité du réseau électrique et du réseau de communication. Pour ce point particulier, la France constitue un excellent choix car les garanties en matière de qualité de ces deux systèmes sont fortes.

Par ailleurs, force est de constater que certaines politiques de sécurité locales sur la gestion des données et des flux réseau empêchent de migrer certaines données et certains traitements. C'est le cas notamment de la Russie et de la Turquie, dont les principes juridiques liés aux données sont contrôlés par des organismes équivalents à la CNIL. Il sera donc nécessaire de conserver des salles machines locales, dédiées à la conservation et au traitement de ces données nationales sensibles (notamment les données à caractère personnel). Elles pourront toutefois être de taille fortement réduite. Dans ce cas, d'un point de vue technique, la question de l'administration à distance se pose. Certaines entreprises ont ici fait le choix de s'appuyer sur des équipes techniques locales qui se chargent du bon fonctionnement des infrastructures, mais l'administration à distance grâce aux technologies de virtualisation peut être une solution alternative ou complémentaire.

De plus, la conservation de sites locaux doit faire ressortir la question des flux réseau. S'ils sont trop importants (transferts de fichiers lourds par exemple), une limitation de bande passante pourra être mise en place afin de maîtriser l'allocation des ressources.

### 4.1.3 Consolider avant transformation

La centralisation de *datacenters* impose de mettre en place certains principes techniques structurants. Parmi les questions à se poser, on peut retenir les suivantes :

- Comment mettre en place un réseau *WAN* international ?
- Doit-on séparer les différents types d'infrastructure ? (séparer les infrastructures *mainframe* du reste)
- Comment organiser et réaliser la gestion des salles ?

L'organisation d'un tel projet doit s'appuyer au départ sur une vision locale, afin de travailler sur les standards et les outils à utiliser. Le choix des premiers pays concernés peut se faire en fonction de besoins particuliers, par exemple en profitant d'une migration de technologie.

Les bonnes pratiques permettant de réaliser cette transformation sont les suivantes :

- Utilisation de ressources matérielles internes,
- Consolidation avant transformation,
- Transfert des serveurs en 1 pour 1 vers le site de destination,
- Mise en place de la virtualisation à l'arrivée (axe déterminant pour la mise en place de l'infrastructure).



#### 4.1.4 Mettre en place un PRA/PCA

La centralisation de *datacenters* implique la localisation des données dans une zone géographique réduite. Il est alors indispensable de gérer les nouveaux risques inhérents à ce fait et de mettre en place des plans de reprise d'activité (PRA) ou de continuité d'activité (PCA) selon la criticité des processus et des données concernées.

Dans ce cadre, il est nécessaire d'avoir à disposition un site secondaire (*site backup*) qui permettra la réplication à l'identique des données et des processus. Ici encore, le choix de la réplication de site (synchrone ou asynchrone) doit être fait en fonction de la criticité des processus et des données pour l'entreprise. Une application vitale pour l'entreprise doit ainsi être basculée de manière invisible pour l'utilisateur en cas de perte de l'un des sites.

Les PRA et PCA doivent alors être détaillés, validés et testés régulièrement pour palier à toute éventualité, de la simple coupure de courant à la catastrophe. Les risques sont multiples dans la gestion d'un *datacenter* et peuvent venir de problématiques techniques (réseau, électricité, bug...), naturelles (catastrophe...) ou humaines (erreurs lors de manipulation).

## 4.2 VIRTUALISATION DES SERVEURS ET DU STOCKAGE

### 4.2.1 Mettre de la puissance informatique à disposition des métiers

La virtualisation est un procédé qui a maintenant fait ses preuves. Techniquement, elle permet de consolider plusieurs machines virtuelles sur une seule machine physique, en partageant ses ressources. Cela permet un gain de place dans les *datacenters*, une meilleure gestion de l'énergie nécessaire, une facilitation de l'administration des machines, et un transfert facilité des processus et des données gérés par la machine considérée.

Dans la mise en œuvre d'offres de service au sein de l'entreprise, la virtualisation permet de fournir au demandeur l'exacte quantité de puissance informatique qu'il souhaite, de par la grande liberté de paramétrage que ce procédé offre. Par ailleurs, ces machines pouvant être administrées à distance, le bénéficiaire de l'offre de service peut accéder et gérer facilement ses données. Ainsi, les phénomènes de démultiplication des besoins serveurs sont gérés grâce à la virtualisation.

La virtualisation peut inquiéter les équipes techniques devant gérer les *datacenters* car elle apporte un lot de nouveautés dans la gestion des infrastructures qui peut être déconcertant, par rapport à l'administration de machines physiques. En pratique, il est constaté que la virtualisation simplifie bien souvent les choses, et accélère les processus, comme par

exemple le démarrage. Ainsi, le redémarrage des systèmes après arrêt du *datacenter* est bien plus rapide et permet un suivi bien plus fin à travers des plateformes dédiées.

## 4.3 OFFRES DE SERVICES SUR *CLOUD* INTERNE

### 4.3.1 Principes de mise en œuvre

Si l'entreprise a une taille suffisamment importante, la mise en place d'un *Cloud* interne peut s'avérer très intéressante. Contrairement aux idées reçues, la mise en place d'une telle solution n'est pas un projet technique, en dehors des briques techniques incontournables (virtualisation, stockage...). En effet, les éléments les plus déterminants seront la définition des offres, des coûts et des modes de facturation, car l'entreprise va attendre de la DSI qu'elle ne facture pas à l'investissement mais à l'usage. Il faudra alors aussi gérer la définition des configurations et de ce qui doit être automatisé.

Ce type de projet a des impacts forts sur l'organisation du travail au sein de la DSI car les briques techniques se rapprochant énormément, les équipes serveur, stockage, réseau et autres vont devoir se regrouper pour travailler main dans la main. Par ailleurs, l'IT doit garder la gouvernance de l'ensemble des solutions *Clouds* internes et externes. Dans son rôle de maintien de la cohérence du système d'information, la DSI doit être en mesure de fournir les éléments techniques permettant l'interopérabilité des solutions entre elles.

### 4.3.2 *Business Case*

Un *Cloud* interne nécessite un *business case* déterminant le temps d'amortissement, avec des hypothèses sur l'utilisation des ressources virtuelles qui vont justifier le mode de refacturation, pour ensuite définir les produits et l'habillage portail qui sera apporté. Le retour d'expérience des entreprises montre généralement un pré-investissement réalisé par la DSI, suivi d'un modèle de refacturation, basé sur la réutilisation des serveurs. Il est également possible d'avoir un investissement initial porté par le groupe, calculé en fonction de l'historique des besoins et des coûts de production, et selon une durée d'amortissement déterminée en amont.

L'objectif pour la DSI est de fournir à son entreprise des offres comparables à celles des fournisseurs externes, sur un plan économique. Il est à noter qu'un avantage non négligeable réside dans le fait que la DSI n'a pas besoin de faire de marge sur les services proposés en interne de l'entreprise. Dans tous les cas, la DSI doit être capable de justifier une différence de coûts avec les offres externes.

Ce fonctionnement bouscule le modèle d'organisation de l'entreprise. Cela apporte de nouveaux besoins en termes de métiers et de compétences au sein des départements de

production. A titre d'exemple, des personnes ayant des fortes compétences en marketing et vente seront nécessaires pour concevoir et chiffrer les offres *Cloud*, *BYOD*, etc.

## 4.4 PROBLÉMATIQUES RÉSEAU

### 4.4.1 Offrir aux sites distants le même accès au SI de l'entreprise

Dans le cas des entreprises multinationales, il est fréquent d'avoir des sites distants dans des zones difficiles d'accès, dans lesquelles le réseau et l'électricité n'ont pas une qualité suffisante pour supporter les processus numériques standards de l'entreprise. Dans ces cas là, une politique particulière doit être mise en place, imposant un écart à la standardisation. Il faut alors mettre en place un réseau hybride, permettant de donner un accès internet local à la plupart des sites pour que la bande passante soit prise sur des lignes internet et non pas les lignes WAN internes. Ce problème est d'autant plus présent avec l'augmentation de l'utilisation de la vidéo dans les pratiques de l'entreprise.

Au niveau de la sélection des opérateurs de télécommunication, il faut faire un choix entre la cohérence du réseau, la facilité de gestion, et les coûts. Ainsi, certaines entreprises choisissent un seul opérateur par plaque géographique en dépit des avantages économiques de la mise en concurrence. Ce choix de s'adresser à un seul opérateur permet notamment d'être sûr que les vérifications techniques des liens peuvent être faites efficacement, sans discontinuité sur toute la zone considérée.

#### *Éléments clés du chapitre*

- **Centralisation des *datacenters***
  - **Consolider avant transformation**
  - **Mettre en place un PRA/PCA**
- **Virtualisation des serveurs et du stockage**
  - **Mettre à disposition des métiers de la puissance informatique**
- **Problématiques réseau**
  - **Offrir aux sites distants le même accès au SI de l'entreprise**

## 5 NOUVELLE GESTION DES RESSOURCES HUMAINES DE LA PRODUCTION

### 5.1 NOUVELLES COMPÉTENCES

Le numérique cause aujourd'hui l'émergence de nouveaux domaines d'activité au sein de la production.

Ainsi, il faut maintenant savoir concevoir des produits, des offres, définir des coûts, et il faut pouvoir les proposer aux clients. On va de plus en plus vers une production qui conçoit la gestion du portefeuille de projets comme une segmentation de clientèle. La production devient une « société de service » interne qui possède son propre *business model*. Elle doit donc se doter de nouvelles compétences commerciales comme le marketing ou l'entrepreneuriat.

Mais dans ce contexte, les fonctions traditionnelles de la production doivent également évoluer. Ainsi, ces nouvelles compétences ne doivent pas uniquement faire l'objet de nouveaux métiers, mais aussi s'ajouter aux métiers d'expert, de manager et de chef de projet. Sur un plan RH, il faut être capable de valoriser chacune de ces fonctions.

Par ailleurs, comme vu précédemment, la nécessité de conserver un système d'information cohérent lors de l'intégration de solutions de *Cloud Computing*, impose l'arrivée de nouvelles compétences transverses d'architecture d'entreprise. Les architectes doivent en effet avoir la capacité d'associer des briques applicatives et des briques d'infrastructure provenant soit de l'extérieur, soit de l'intérieur de l'entreprise, afin de concevoir des offres répondant parfaitement aux besoins des utilisateurs, tout en garantissant sécurité, accessibilité et cohérence des données.

### 5.2 GESTION DE L'*OFFSHORING*

#### 5.2.1 Choix de l'*offshoring*

L'*offshoring* et le *nearshoring* sont des domaines dans lesquels la France est en retard et dépend fortement des politiques d'entreprise. Ces pratiques sont déjà bien ancrées dans les pays anglo-saxons et l'Allemagne, alors qu'elles en sont aux balbutiements dans l'Europe du sud.

En matière de développement logiciel, un grand nombre d'expériences d'*offshore* a déjà été réalisé, et le phénomène atteint maintenant les départements infrastructure. Sur le plan

économique, on constate ainsi que 35 à 40% des coûts de production sont liés aux ressources humaines.

Ce sujet est extrêmement structurant en termes de choc culturel, de revue des processus et d'organisation du travail.

D'un point de vue pratique, s'il est conseillé de conserver les *datacenters* en Europe de l'ouest (France) car l'électricité y est stable et peu chère, avec une bonne irrigation en télécommunications et peu de catastrophes naturelles, il peut être intéressant financièrement d'en déléguer la gestion à des intervenants à distance. L'*offshoring* peut alors être fait de l'autre côté de la planète, mais il est également possible (généralement pour des raisons linguistiques) de pousser les équipes en province, si le siège est en région parisienne.

La tendance prend de l'importance en France et les entreprises devront choisir d'y aller ou non. Quoi qu'il en soit, la question doit être étudiée car la DSI devra être capable d'argumenter auprès des directions générales sur le choix fait.

Le choix de l'*offshore* peut aussi avoir un impact technique. En effet, pour gérer les problématiques de *turnover* de l'autre côté du monde, l'entreprise devra privilégier la mise en place de briques standards d'infrastructure sur lesquelles les équipes à distance sont déjà formées. En effet, l'utilisation de briques spécifiques impliquerait une formation particulière des nouveaux employés, ce qui imposerait des coûts supplémentaires importants.

### 5.2.2 Compétences managériales et répartition des niveaux de support

Les profils des managers en charge de faire fonctionner la production sont radicalement changés. Ainsi, le manager doit maintenant gérer une partie des experts et techniciens en local et une autre en Inde, à Singapour, etc. Ce qui change radicalement le travail au sein de la production, c'est le fait d'avoir de la distance, mais de pouvoir garder un contrôle complet sur les infrastructures. Le métier change, passant alors d'un management technique à un management d'activité.

Un modèle possible de répartition des rôles est le suivant :

- Mise en *offshore* des activités de support et des tâches à faible valeur ajoutée :
  - Pilotage de base (niveau 0)
  - Exécution manuelle de tâches procédurées (niveau 1)
  - Analyse et tâches peu procédurées (niveau 2)
- Conservation en France des activités :
  - Interface client
  - Projet
  - Expertise

Ce modèle ne doit, par contre, pas séparer les domaines techniques (réseau, systèmes, stockage...). En effet, l'éloignement de domaines techniques liés entraînerait des difficultés de gestion dans les interfaces entre les équipes techniques. Cette pratique permet d'avoir des équipes de production offshorées autonomes, qui n'ont besoin de remonter les incidents ou problèmes aux équipes managériales françaises que lorsqu'il y a besoin d'une analyse plus poussée.

Une bonne pratique managériale est alors de suivre le taux et le type des incidents remontés aux experts en France, et de déterminer alors les plans d'action, notamment en termes de formations pour les équipes offshorées pour qu'elles deviennent indépendantes dans la résolution des incidents courants.

### *Éléments clés du chapitre*

- **Nouvelles compétences**
  - **Se doter de compétences commerciales pour constituer les offres de service : marketing, entrepreneuriat...**
  - **Se doter de compétences transverses d'architecture pour maîtriser l'intégration de solutions Cloud dans les infrastructures internes**
- **Gestion de l'*offshoring***
  - **Répartir les niveaux de support en *offshore* et en *nearshore***
  - **S'assurer des problématiques juridiques et managériales**

## CONCLUSION

La transformation de l'entreprise dans le monde numérique affecte particulièrement la gestion des infrastructures dans l'entreprise. Que ce soit dans son modèle d'affaires, dans la gestion des compétences, dans ses offres de services ou dans les solutions techniques choisies, la DSI doit aujourd'hui fortement évoluer. Dans un cadre où les utilisateurs maîtrisent les usages numériques, elle doit prendre sa place face aux prestataires extérieurs et garantir la qualité du système d'information de l'entreprise.

Pour cela, de nombreux outils sont à sa disposition. Solutions de *Cloud*, mobilité, centralisation, compétences numériques, sont autant de leviers à actionner pour offrir à l'entreprise des sources d'innovation et de performance.

Dans ce contexte, l'infrastructure est particulièrement impactée par la place que prend la donnée dans le monde numérique. Elle doit faire face aux augmentations vertigineuses des volumes, à la protection des données sensibles, mais également en faire un atout pour le développement de l'entreprise. C'est notamment le cas avec le phénomène du *Big Data* qui permet de pousser l'analyse stratégique sur des volumes colossaux de données, ces données non structurées étant apportées, entre autres, par la richesse actuelle d'Internet (réseaux sociaux, vidéos, images...). Le défi est important pour les infrastructures qui doivent pouvoir apporter rapidement des capacités de stockage et de puissance informatique d'analyse, que ce soit par un apport interne aux entreprises ou par l'utilisation de solutions *Cloud* offrant une grande flexibilité.



## **CIGREF**

21 avenue de Messine  
75008 PARIS

Tel. : +33 1 56 59 70 00

Fax : +33 1 56 59 70 01

[cigref@cigref.fr](mailto:cigref@cigref.fr)

[www.cigref.fr](http://www.cigref.fr)