Sujet national pour l'ensemble des centres de gestion organisateurs

TECHNICIEN TERRITORIAL PRINCIPAL DE 2ème CLASSE

CONCOURS INTERNE ET DE TROISIÈME VOIE

SESSION 2014

Étude de cas portant sur la spécialité au titre de laquelle le candidat concourt.

Durée : 4 heures
Coefficient 1

SPÉCIALITÉ : INGENIERIE, INFORMATIQUE ET SYSTEMES D'INFORMATION

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni votre numéro de convocation, ni signature ou paraphe.

- Aucune référence (nom de collectivité, nom de personne, …) **autre que celles figurant le cas échéant sur le sujet ou dans le dossier** ne doit apparaître dans votre copie.

- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.

- Les feuilles de brouillon ne seront en aucun cas prises en compte.

- L'utilisation d'une calculatrice de fonctionnement autonome et sans imprimante est autorisée.

Ce sujet comprend 16 pages
Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué

- Vous préciserez le numéro de la question et le cas échéant de la sous-question auxquelles vous répondrez.
- Des réponses rédigées sont attendues et peuvent être accompagnées si besoin de tableaux, graphiques, schémas…

Vous êtes technicien principal de 2ème classe à la communauté de communes de Technicommunauté.

La communauté de communes regroupe, sur 150 km^2, 45 communes pour environ 55 000 habitants. Ces communes ont décidé de couvrir une nouvelle compétence : gérer la mise à disposition auprès des communes de 40 éducateurs sportifs pour les 105 écoles maternelles et élémentaires.

Ces éducateurs interviendront dans le cadre des activités sportives sur le temps scolaire, mais aussi, dans le cadre de la réforme des rythmes scolaires.

Dans le cadre de la gestion de cette nouvelle activité, la communauté de communes aura la responsabilité :
- Du recrutement des éducateurs contractuels ou fonctionnaires, à temps plein ou à temps partiel,
- De la gestion de la carrière des agents,
- De la gestion des agents,
- De l'organisation du planning d'activité des agents en relation avec les écoles du territoire.

La communauté de communes a donc besoin d'une application qui prendra en charge la gestion de tous ces aspects. Toutes les communes, toutes les écoles accèderont à l'application.

La communauté de communes dispose de ressources limitées dans le domaine des systèmes d'information. En effet, la direction des systèmes d'information compte pour l'instant un seul administrateur réseau, un développeur Web et webmaster, 10 techniciens en maintenance de parc, et pas d'administrateur de base de données. Elle exploite une application de ressources humaines, et une application de gestion financière et comptable.

Vous êtes chargé par le Président de la communauté de communes de proposer une solution informatique prenant en charge toutes les responsabilités de la communauté de communes sur ce dossier.

Vous proposerez un schéma d'organisation autour du nouveau système d'information et son urbanisation dans le système d'information de la communauté de communes.

Il vous demande d'être particulièrement vigilant sur les aspects de sécurité, de disponibilité, d'accessibilité, de fiabilité de la solution. Aussi, vous devez prendre en compte les aspects de conduite du changement à mettre en oeuvre auprès des acteurs que vous aurez identifiés comme impactés par cette nouvelle compétence de la communauté de communes.

Pour honorer la demande du Président de la communauté de communes, vous répondrez aux questions suivantes, à partir des éléments fournis, de vos connaissances et de votre expérience professionnelle :

Question 1 (5 points) : Décrivez la démarche de gestion de projet que vous allez mettre en place pour mener le projet qui vous est confié et proposez un planning de réalisation.

Question 2 (6 points) :
a) Proposer une architecture technique complète de la solution que vous pensez implémenter. Vous devrez justifier vos choix et vous donnerez également des indications sur le budget prévisionnel de l'opération.
b) Proposer les critères d'attribution.

Question 3 (4 points) : Détailler les mesures que vous prendrez afin de garantir la sécurité du nouveau système.

Question 4 (5 points) : Dans le cadre d'une démarche de conduite du changement, expliquez les principaux leviers que vous utiliserez et donnez des exemples.

Liste des documents joints :

Document 1 : « Les modes SaaS » - *wikipédia* – 3 pages

Document 2 : « Le logiciel en tant que service ou Software, pourquoi s'y intéresser ? » - *01Business* – avril 2012 – 2 pages

Document 3 : « 10 conseils pour la sécurité de votre système d'information » - *CNIL* – 3 pages

Document 4 : « La conduite du changement en 5 étapes clés » - *Business.lesechos.fr* – 1 page

Document 5 : «iDTGV fait le choix du SaaS avec Eurécia » - *www .eurecia.com* – 2010 – 2 pages

Document 6 : « La sécurité, un des avantages des applications SaaS » - *itdmanager.com* – 23 août 2009 – 2 pages

Le logiciel en tant que service ou Software as a Service (SaaS) est un modèle d'exploitation commerciale des logiciels dans lequel ceux-ci sont installés sur des serveurs distants plutôt que sur la machine de l'utilisateur. Les clients ne paient pas de licence d'utilisation pour une version, mais utilisent généralement gratuitement le service en ligne ou payent un abonnement récurrent.

Le logiciel en tant que service (SaaS) est donc la livraison conjointe de moyens, de services et d'expertise qui permettent aux entreprises d'externaliser intégralement un aspect de leur système d'information (messagerie, sécurité…) et de l'assimiler à un coût de fonctionnement plutôt qu'à un investissement. Le contrat de services est essentiel pour définir le niveau de qualité de service (SLA). Le logiciel en tant que service (SaaS) peut être vu comme l'équivalent commercial de l'architecture orientée service (SOA).

Historique

Le terme SaaS (logiciel en tant que service) remplace les termes ASP (Application Service Provider) ou encore « On Demand », précédemment employés. Il est apparu le 28 février 2001, dans un article « Strategic Backgrounder: Software As A Service » publié par The Software & Information Industry's (SIIA) eBusiness Division, édition de Washington DC3.

La différence entre le logiciel en tant que service (SaaS) et les précédents modèles tels que ASP réside dans le fait que les applications s'appuyant sur ce modèle ont été nativement conçues pour l'accès via Internet. Précédemment, il s'agissait en général d'un frontal web appliqué à des applications traditionnelles.

Une étude menée par MARKESS International montre que des domaines comme les solutions collaboratives et la communication d'entreprise sont maintenant largement adoptés en mode le logiciel en tant que service (SaaS). Les exemples de services collaboratifs les plus utilisés en mode SaaS (logiciel en tant que service) sont le partage d'agendas en ligne, les outils de conférence à distance, les services de gestion de contacts et de présence, la gestion documentaire et/ou de contenu ainsi que la messagerie d'entreprise. L'adoption de ces outils devrait considérablement augmenter d'ici 2010.

En 2007, le marché des logiciels en tant que service (SaaS) était estimé à près de 5 milliards de dollars US dans le monde et 122 millions d'euros en France. Une étude de Gartner Group prédisait alors le doublement du marché d'ici 2014. En 2010, la progression s'avère plus modeste que prévue5 et les prévisions sont revues à la baisse.

Avantages et inconvénients

Les solutions logicielles en tant que service (SaaS) sont principalement développées à destination d'entreprises. Depuis quelques années le marché des SaaS est en très forte croissance. Les logiciels en tant que service (SaaS) présentent pour les entreprises divers avantages et inconvénients.

Avantages

L'utilisation de solutions logicielles en tant que service (SaaS) en entreprise permet un meilleur contrôle des charges techniques. L'ensemble des solutions techniques étant délocalisées le coût devient fixe, généralement fonction du nombre de personnes utilisant la solution SaaS. Le prix par utilisateur englobe le coût des licences des logiciels, de la maintenance et de l'infrastructure. Il revient

à l'entreprise utilisatrice de faire son choix entre utilisation en SaaS, d'une part, et acquisition des licences puis déploiement en interne, d'autre part.

Les avantages du SaaS présentent un impact budgétaire et financier plutôt moindre. Les coûts totaux d'acquisition et de maintenance de la solution (TCO, total cost of ownership) s'avèrent moyens, contrairement à une acquisition traditionnelle de licence qui est généralement passée en immobilisation (CAPEX, hors maintenance).

Un avantage manifeste pour les entreprises est la rapidité de déploiement lorsque le logiciel SaaS correspond exactement au besoin (et qu'il ne nécessite aucune adaptation). Les solutions SaaS étant déjà pré-existantes le temps de déploiement est extrêmement faible.

Un autre avantage pourrait être de réduire la consommation électrique en permettant la mutualisation des ressources sur des serveurs partagés par plusieurs entreprises ainsi que l'usage d'un ordinateur à faible consommation muni d'un simple navigateur Web sans autres licences associées.

Inconvénients

Lors de la mise en place de solutions SaaS, les données relatives à l'entreprise cliente sont, généralement, stockées sur les serveurs du prestataire fournissant la solution. Lorsqu'il s'agit de données sensibles ou confidentielles, l'entreprise est obligée de prendre des dispositions contractuelles avec le fournisseur.

La délocalisation des serveurs de la solution SaaS permet également un accès nomade aux données de l'entreprise. Cet accès entraîne un souci de sécurité de l'information lors du départ de collaborateurs. Il est indispensable d'avoir mis en place des procédures permettant, lors d'un départ, de supprimer l'habilitation de l'ancien collaborateur à accéder aux données de l'entreprise.

Par ailleurs, l'intégration des applications SaaS entre elles ainsi qu'avec les autres applications du système d'information, hébergées dans les centres de données de l'entreprise, figure parmi les principaux handicaps du SaaS 6. De nouveaux profils d'acteurs apparaissent pour répondre à cet enjeu à travers des plates-formes applicatives de type PaaS (Platform as a Service) fournissant des briques complémentaires ou des APIs permettant à ces applications de dialoguer entre elles.

Il est également important d'adapter son Plan de Continuité de l'Activité à l'intégration de solutions SaaS ainsi que de prévoir les divers scénarios possibles en cas de problèmes avec le prestataire de la solution SaaS.

En termes de contrôles internes, il est recommandé que le prestataire de service fournisse un certificat de type SSAE16 à son client afin de garantir de la bonne qualité de son propre système de contrôles internes. Le cas échéant, le client doit prendre des mesures compensatoires comblant les manquements de son fournisseur de service.

Les migrations informatiques peuvent être compliquées puisqu'il faut basculer les données de la plate-forme d'un fournisseur vers celle d'un autre, avec divers problèmes associés (compatibilité, apparence pour le client, etc.). Dans le cadre du SaaS, le client se trouve lié à son fournisseur.

Le même service nécessite le fonctionnement de deux ordinateurs (client/prestataire) au lieu d'un seul. Cela peut augmenter la consommation électrique, notamment lorsque l'on utilise un poste client à forte consommation et un serveur non mutualisé. Il y a également un troisième acteur, c'est le fournisseur d'accès internet (FAI) car c'est lui qui assure la communication entre le client et le prestataire, donc une ligne hors service est égale à l'arrêt total de l'activité de la société d'où la

nécessité de se procurer des lignes redondantes avec un débit minimal fixe assuré par l'opérateur télécom.

Bien entendu ces solutions nécessitent de disposer d'un accès Internet ce qui est loin d'être le cas pour les clients nomades se déplaçant dans des régions non couvertes ou avec une couverture médiocre.

Source : Article Wikipedia (http://fr.wikipedia.org/wiki/SaaS)

Le logiciel en tant que service ou Software Pourquoi s'y intéresser ?

Les logiciels de CRM, de collaboration ou les ERP sont aujourd'hui consommables sur le web. Cela présente des avantages mais aussi de sérieux inconvénients qu'il faut évaluer.

Quels sont les gains ?

1. Un investissement allégé

L'atout clé du Saas, avant toute notion technique ou fonctionnelle, est la transformation d'un investissement comptable en charge liée à l'usage. Le mode locatif élimine l'apport initial utile à tout projet informatique (achat de serveurs, de licences) et le transforme en mensualités.

2. La performance à faible prix

Généralement facturés quelques dizaines d'euros par utilisateur et par mois, les services Saas se veulent résolument moins coûteux que les logiciels traditionnels (on-premise). Ils donnent accès à des applications disposant des fonctions les plus modernes à un prix abordable, notamment pour les PME.

3. Une mise en œuvre rapide

La phase d'intégration d'un projet Saas est beaucoup plus courte que celle des projets traditionnels. De plus, ce mode apporte une souplesse incomparable : plus de soucis de montée en charge de l'application, ni d'impact sur la plate-forme technique en cas d'ajout d'utilisateurs.

4. un logiciel toujours à jour

Les offres Saas fonctionnant généralement sur des plates-formes multitenants (multilocataires), elles sont à jour en permanence. Toute problématique de montée de version disparaît, et les utilisateurs bénéficient, au fil du temps, de nouvelles fonctionnalités innovantes. Ce mode étant le plus souvent proposé sur des applications web, aucun déploiement n'est nécessaire au niveau des postes clients.

Quelles sont les limites ?

1. Personnalisation et intégration sont limitées

Pour les chefs d'entreprise habitués à demander aux intégrateurs des personnalisations poussées de leurs progiciels, le Saas constitue une révolution culturelle. Certes, personnaliser en partie certains services Saas est possible, mais la force de ce mode reste l'utilisation de l'offre standard. Les capacités d'intégration, notamment en temps réel, avec les données d'autres systèmes sont restreintes, même si les éditeurs de services Saas et ceux d'outils d'intégration ont désormais inclus des connecteurs d'échange.

2. Quel coût sur le long terme ?

Si, à court terme, le coût des applications Saas paraît imbattable comparé à ceux d'infrastructure (serveurs, stockage), de licence et de maintenance d'un logiciel traditionnel, le calcul peut s'inverser sur le long terme. Dans le cas d'une utilisation ponctuelle, sur un projet par exemple, le mode locatif

est très avantageux. Pour un emploi plus structurant sur cinq à dix ans, un logiciel on-premise pourra s'avérer plus pertinent. Une évaluation des coûts est nécessaire.

3. Attention aux conditions juridiques

Le mode Saas présente des spécificités : les données sont hébergées chez un tiers, souvent à l'étranger, et parfois même hors d'Europe. Il convient de s'assurer de la légalité de l'export de ses données vers le pays cible. Certains secteurs d'activité l'interdisent formellement. Les entreprises opérant dans des secteurs sensibles doivent envisager l'option Saas avec prudence. En outre, il faut vérifier les clauses contractuelles en cas d'indisponibilité du service, voire de défaillance du prestataire.

4. S'assurer de la réversibilité du choix

S'il est facile de monter dans le cloud, puisqu'il suffit de quelques clics pour s'abonner, quitter un service Saas nécessite quelques précautions préalables. Il s'agit, en particulier, de s'assurer des moyens dont on dispose pour extraire ses données de la plate-forme et mener une migration vers l'infrastructure cible.

Source : O1Business, avril 2012 (http://pro.01net.com/editorial/563280/le-saas-explique-a-votre-directeur-general/)

10 conseils pour la sécurité de votre système d'information

La loi "informatique et libertés" impose que les organismes mettant en œuvre des fichiers garantissent la sécurité des données qui y sont traitées. Cette exigence se traduit par un ensemble de mesures que les détenteurs de fichiers doivent mettre en œuvre, essentiellement par l'intermédiaire de leur direction des systèmes d'information (DSI) ou de leur responsable informatique.

1. Adopter une politique de mot de passe rigoureuse

L'accès à un poste de travail informatique ou à un fichier par identifiant et mot de passe est la première des protections. Le mot de passe doit être individuel, difficile à deviner et rester secret. Il ne doit donc être écrit sur aucun support. La DSI ou le responsable informatique devra mettre en place une politique de gestion des mots de passe rigoureuse : un mot de passe doit comporter au minimum 8 caractères incluant chiffres, lettres et caractères spéciaux et doit être renouvelé fréquemment (par exemple tous les 3 mois). Le système doit contraindre l'utilisateur à choisir un mot de passe différent des trois qu'il a utilisés précédemment. Généralement attribué par l'administrateur du système, le mot de passe doit être modifié obligatoirement par l'utilisateur dès la première connexion. Enfin, les administrateurs des systèmes et du réseau doivent veiller à modifier les mots de passe qu'ils utilisent eux-mêmes.

2. Concevoir une procédure de création et de suppression des comptes utilisateurs

L'accès aux postes de travail et aux applications doit s'effectuer à l'aide de comptes utilisateurs nominatifs, et non « génériques » (compta1, compta2…), afin de pouvoir éventuellement être capables de tracer les actions faites sur un fichier et, ainsi, de responsabiliser l'ensemble des intervenants. En effet, les comptes « génériques » ne permettent pas d'identifier précisément une personne. Cette règle doit également s'appliquer aux comptes des administrateurs systèmes et réseaux et des autres agents chargés de l'exploitation du système d'information.

3. Sécuriser les postes de travail

Les postes des agents doivent être paramétrés afin qu'ils se verrouillent automatiquement au-delà d'une période d'inactivité (10 minutes maximum) ; les utilisateurs doivent également être incités à verrouiller systématiquement leur poste dès qu'ils s'absentent de leur bureau. Ces dispositions sont de nature à restreindre les risques d'une utilisation frauduleuse d'une application en cas d'absence momentanée de l'agent du poste concerné. Par ailleurs, le contrôle de l'usage des ports USB sur les postes « sensibles », interdisant par exemple la copie de l'ensemble des données contenues dans un fichier, est fortement recommandé.

4. Identifier précisément qui peut avoir accès aux fichiers

L'accès aux données personnelles traitées dans un fichier doit être limité aux seules personnes qui peuvent légitimement y avoir accès pour l'exécution des missions qui leur sont confiées. De cette analyse, dépend « le profil d'habilitation » de l'agent ou du salarié concerné. Pour chaque mouvement ou nouvelle affectation d'un salarié à un poste, le supérieur hiérarchique concerné doit identifier le ou les fichiers auxquels celui-ci a besoin d'accéder et faire procéder à la mise à jour de ses droits d'accès. Une vérification périodique des profils des applications et des droits d'accès aux répertoires sur les

serveurs est donc nécessaire afin de s'assurer de l'adéquation des droits offerts et de la réalité des fonctions occupées par chacun.

5. Veiller à la confidentialité des données vis-à-vis des prestataires

Les interventions des divers sous-traitants du système d'information d'un responsable de traitement doivent présenter les garanties suffisantes en terme de sécurité et de confidentialité à l'égard des données auxquels ceux-ci peuvent, le cas échéant, avoir accès. La loi impose ainsi qu'une clause de confidentialité soit prévue dans les contrats de sous-traitance. Les éventuelles interventions d'un prestataire sur des bases de données doivent se dérouler en présence d'un salarié du service informatique et être consignées dans un registre. Les données qui peuvent être considérées « sensibles » au regard de la loi, par exemple des données de santé ou des données relatives à des moyens de paiement, doivent au surplus faire l'objet d'un chiffrement.

« A noter » : l'administrateur systèmes et réseau n'est pas forcément habilité à accéder à l'ensemble des données de l'organisme. Pourtant, il a besoin d'accéder aux plates-formes ou aux bases de données pour les administrer et les maintenir. En chiffrant les données avec une clé dont il n'a pas connaissance, et qui est détenue par une personne qui n'a pas accès à ces données (le responsable de la sécurité par exemple), l'administrateur peut mener à bien ses missions et la confidentialité est respectée.

6. Sécuriser le réseau local

Un système d'information doit être sécurisé vis-à-vis des attaques extérieures.

Un premier niveau de protection doit être assuré par des dispositifs de sécurité logique spécifiques tels que des routeurs filtrants (ACL), pare-feu, sonde anti intrusions, etc. Une protection fiable contre les virus et logiciels espions suppose une veille constante pour mettre à jour ces outils, tant sur le serveur que sur les postes des agents. La messagerie électronique doit évidemment faire l'objet d'une vigilance particulière. Les connexions entre les sites parfois distants d'une entreprise ou d'une collectivité locale doivent s'effectuer de manière sécurisée, par l'intermédiaire des liaisons privées ou des canaux sécurisés par technique de « tunneling » ou VPN (réseau privé virtuel). Il est également indispensable de sécuriser les réseaux sans fil compte tenu de la possibilité d'intercepter à distance les informations qui y circulent : utilisation de clés de chiffrement, contrôle des adresses physiques des postes clients autorisés, etc. Enfin, les accès distants au système d'information par les postes nomades doivent faire préalablement l'objet d'une authentification de l'utilisateur et du poste. Les accès par internet aux outils d'administration électronique nécessitent également des mesures de sécurité fortes, notamment par l'utilisation de protocoles IPsec, SSL/TLS ou encore HTTPS.

« A noter » : Un référentiel général de sécurité, relatif aux échanges électroniques entre les usagers et les autorités administratives (ordonnance 2005-1516), doit voir le jour prochainement (voir projet sur le site www.ssi.gouv.fr). Il imposera à chacun des acteurs des mesures de sécurité spécifiques.

7. Sécuriser l'accès physique aux locaux

L'accès aux locaux sensibles, tels que les salles hébergeant les serveurs informatiques et les éléments du réseau, doit être limité aux personnels habilités. Ces locaux doivent faire l'objet d'une sécurisation particulière : vérification des habilitations, gardiennage, portes fermées à clé, digicode, contrôle d'accès par badge nominatifs, etc. La DSI ou le responsable informatique doit veiller à ce que les documentations techniques, plans d'adressages réseau, contrats, etc. soient eux aussi protégés.

8. Anticiper le risque de perte ou de divulgation des données

La perte ou la divulgation de données peut avoir plusieurs origines : erreur ou malveillance d'un salarié ou d'un agent, vol d'un ordinateur portable, panne matérielle, ou encore conséquence d'un dégât des eaux ou d'un incendie. Il faut veiller à stocker les données sur des espaces serveurs prévus à cet effet et faisant l'objet de sauvegardes régulières. Les supports de sauvegarde doivent être stockés dans un local distinct de celui qui héberge les serveurs, idéalement dans un coffre ignifugé. Les serveurs hébergeant des données sensibles ou capitales pour l'activité l'organisme concerné doivent être sauvegardés et pourront être dotés d'un dispositif de tolérance de panne. Il est recommandé d'écrire une procédure « urgence – secours » qui décrira comment remonter rapidement ces serveurs en cas de panne ou de sinistre majeur. Les supports nomades (ordinateurs portables, clé USB, assistants personnels etc.) doivent faire l'objet d'une sécurisation particulière, par chiffrement, au regard de la sensibilité des dossiers ou documents qu'ils peuvent stocker. Les matériels informatiques en fin de vie, tels que les ordinateurs ou les copieurs, doivent être physiquement détruits avant d'être jetés, ou expurgés de leurs disques durs avant d'être donnés à des associations. Les disques durs et les périphériques de stockage amovibles en réparation, réaffectés ou recyclés, doivent faire l'objet au préalable d'un formatage de bas niveau destiné à effacer les données qui peuvent y être stockées.

9. Anticiper et formaliser une politique de sécurité du système d'information

L'ensemble des règles relatives à la sécurité informatique doit être formalisé dans un document accessible à l'ensemble des agents ou des salariés. Sa rédaction requiert l'inventaire préalable des éventuelles menaces et vulnérabilités qui pèsent sur un système d'information. Il convient de faire évoluer régulièrement ce document, au regard des modifications des systèmes et outils informatiques utilisés par l'organisme concerné. Enfin, le paramètre « sécurité » doit être pris en compte en amont de tout projet lié au système d'information.

10. Sensibiliser les utilisateurs aux « risques informatiques » et à la loi "informatique et libertés"

Le principal risque en matière de sécurité informatique est l'erreur humaine. Les utilisateurs du système d'information doivent donc être particulièrement sensibilisés aux risques informatiques liés à l'utilisation de bases de données. Cette sensibilisation peut prendre la forme de formations, de diffusion de notes de service, ou de l'envoi périodique de fiches pratiques. Elle sera également formalisée dans un document, de type « charte informatique », qui pourra préciser les règles à respecter en matière de sécurité informatique, mais aussi celles relatives au bon usage de la téléphonie, de la messagerie électronique ou encore d'internet. Ce document devrait également rappeler les conditions dans lesquelles un salarié ou un agent peut créer un fichier contenant des données personnelles, par exemple après avoir obtenu l'accord de son responsable, du service juridique ou du CIL de l'entreprise ou de l'organisme dans lequel il travaille.

Ce document doit s'accompagner d'un engagement de responsabilité à signer par chaque utilisateur.

A noter : veiller à ce que les utilisateurs nettoient régulièrement leurs vieux documents et messages électroniques sur leurs postes. De même, nettoyer régulièrement le répertoire d'échange partagé entre les différents services afin qu'il ne se transforme pas en espace « fourre-tout » (fichiers personnels des agents mélangés avec des dossiers sensibles)

Source : site internet de la CNIL (http://www.cnil.fr/les-themes/securite/fiche-pratique/article/10-conseils-pour-securiser-votre-systeme-dinformation-1/)

La conduite du changement en 5 étapes clés

Si l'accompagnement des collaborateurs a toujours été indispensable en période de changement, il est d'autant plus important dans un contexte de crise, sur fond de budgets serrés et de pression accrue. Conseils de Florence Géraud, manager chez ConvictionsRH.

Étape n°1 : Anticiper les résistances

« *Il faut penser à la conduite du changement dès même la réflexion stratégique du projet. Cela passe par une* ***cartographie précise de tous les acteurs*** *(actifs et passifs) de l'entreprise, puis par l'étude de chaque sous-population et de leurs caractéristiques, afin de définir à quel moment, et qui en particulier sera le plus fragile face au bouleversement de l'organisation* »

Étape n°2 : Anticiper les ressources et les charges

« *Former deux ou trois groupes d'utilisateurs, au sein de l'entreprise, c'est un strict minimum. L'idéal étant de nommer un* ***chef de projet qui prendra la casquette de Change Leader*** *: cette personne et son équipe dédiée auront alors pour mission de sécuriser le déploiement du projet et seront les interlocuteurs privilégiés en cas d'inquiétude ou d'interrogation de la part des autres collaborateurs de l'entreprise* ».

Étape n°3 : Communiquer en interne

« *Aucune population de l'entreprise ne doit être oubliée. Ainsi, pour toucher tous les acteurs de l'entreprise, le plus judicieux est de* ***créer un réseau interne et, surtout, de l'animer****. Cela permet de rendre le projet concret auprès de tous les collaborateurs, que ce soit au niveau local, régional, national ou international. Cette transparence permet de* ***transformer les résistances en opportunités****.* »

Étape n°4 : Adopter une méthodologie

« *La conduite du changement répond à différentes étapes à définir en amont : la phase de cadrage ; l'analyse des impacts ; la définition de la stratégie ; puis enfin la mise en place. En établissant une* ***feuille de route adaptée aux spécificités de l'entreprise*** *et à celles de ses équipes, en* ***tenant compte du calendrier social****, on s'assure une fois de plus l'adhésion de toutes les parties prenantes.* »

Étape n°5 : Reconnaître et saluer l'adaptabilité

« *La dernière phase, une fois la transformation opérée, est d'****évaluer les bonnes et mauvaises pratiques*** *liées au changement. En plus de permettre de tirer les leçons de ce qui s'est passé, cela doit s'accompagner de la valorisation du changement et du comportement des équipes. Il ne faut pas hésiter à* ***communiquer sur les bons résultats et sur la bonne adaptation de tous****.* »

Source : Article de Julie Le Bolzer (http://business.lesechos.fr/directions-ressources-humaines/management/la-conduite-du-changement-en-5-etapes-cles-8390.php)

eurécia
LOGICIELS RH EN MODE SAAS

CAS CLIENT

GESTION ADMINISTRATIVE DU PERSONNEL

iDTGV fait le choix du SaaS avec Eurécia

Du suivi des temps de travail à la gestion des notes de frais, en passant par la gestion des congés et des absences, c'est toute la gestion administrative du personnel iDTGV qui est gérée avec les solutions d'Eurécia. La DSI d'iDTGV a été séduite par les fonctionnalités, la rapidité de déploiement, la simplicité d'utilisation et la tarification extrêmement intéressante des solutions proposées par l'éditeur toulousain.

iDTGV

CLIENT : iDTGV
GROUPE : SNCF
SECTEUR D'ACTIVITÉ : Transport
SIÈGE SOCIAL : Paris (75)

LE PROJET EN BREF

iDTGV a d'abord retenu et déployé le module de suivi des temps et des activités pour les besoins internes de la Direction des Systèmes d'Information (DSI), qui souhaitait disposer d'une visibilité sur le temps passé par ses équipes par tâches, projets et directions.
Satisfaite de l'outil de time-tracking, iDTGV a ensuite mis en œuvre les modules de gestion des absences et des congés, de gestion des notes de frais et de suivi du dossier RH, sur un périmètre élargi (l'ensemble des collaborateurs de la société).

Suivi des temps et des activités de la DSI, pour optimiser son organisation

Créée en 2004 par la SNCF, iDTGV propose une offre 100% Internet pour l'achat de billets de train de son offre (réservation en ligne, billets à imprimer…), avec des spécificités très appréciées des voyageurs : tarifs attractifs, choix de l'ambiance de voyage, de l'emplacement du siège, etc. A l'origine expérimentée sur la liaison Paris - Marseille, la liste des destinations couvertes par iDTGV s'enrichit chaque année. Aujourd'hui, iDTGV dessert plus de 30 villes et transporte près de 15 000 passagers par jour. Avec un modèle 100% Web, l'activité d'iDTGV repose en grande partie sur son système d'information. Sa DSI occupe d'ailleurs à elle seule près d'un tiers des effectifs : 20 collaborateurs sur un total de 70.

A son arrivée en 2010, le nouveau DSI d'iDTGV souhaite optimiser l'organisation de sa direction. Pour cela, il a besoin de disposer d'une visibilité sur le temps passé par ses équipes par tâches, par projets, et par directions. Jusque-là, le reporting était réalisé grâce à des feuilles Excel, avec les limites de cet outil : problèmes d'accès partagé et de consolidation des données, absence de suivi en temps réel… Il se met alors à la recherche d'une solution de gestion des temps et des activités (GTA), adaptée à une structure de quelques dizaines de salariés, et disponible en mode SaaS, afin d'éviter des dépenses d'infrastructure.

Déploiement rapide et simplicité d'utilisation

En mars 2010, après une recherche sur Internet, le DSI identifie très rapidement Eurécia, l'un des seuls éditeurs de solutions de GTA en mode SaaS à répondre à l'ensemble de ses critères, et contacte la société afin de pouvoir tester l'outil.

LES BESOINS

Besoins de la DSI :

• Remplacer les feuilles Excel pour le suivi des temps et activités
• Homogénéiser les processus de reporting des temps et activités
• Disposer d'une visibilité sur le temps passé par tâches, projets et par directions.

Besoins de la DAF :

• Pour l'ensemble des collaborateurs, remplacer une solution de gestion des absences et des congés, de gestion des notes de frais et de suivi du dossier RH, qui ne donnait pas satisfaction, et qui était coûteuse.

MODULES RETENUS

• Suivi des temps et des activités (GTA) pour la DSI
• Gestion des absences et des congés, des notes de frais et suivi du dossier RH pour l'ensemble des collaborateurs

POURQUOI EURECIA ?

• Outils intuitifs
• Fonctionnalités disponibles
• Solutions en mode SaaS (pas de dépenses d'infrastructure)
• Connecteurs avec l'outil de gestion de la paie (ADP)
• Tarification très intéressante

PRINCIPAUX BÉNÉFICES

• Déploiement en moins de 15 jours
• Appropriation rapide des outils par les utilisateurs
• Amélioration de la qualité de service de la DSI vis-à-vis de ses « clients internes »
• Gestion administrative des RH et suivi opérationnel des collaborateurs avec la même suite logicielle
• Bascule automatique des données de congés et absences vers le logiciel de paie ADP

Outre toutes les fonctionnalités qu'il recherchait, il est séduit par les interfaces simples et de qualité, et par la tarification extrêmement intéressante de la solution.

Le projet est lancé en avril 2010. Une fois définis les axes et comptes analytiques sur lesquels les activités devaient être imputées, le déploiement ne prendra pas plus de 15 jours. « *Ce projet a été très structurant pour la DSI, explique Fabrice Flottes de Pouzols, Directeur des Systèmes d'Information d'iDTGV. Notre plus grande difficulté a été de structurer et de figer la liste des directions, activités et différentes tâches sur lesquels les temps étaient à déclarer, en fonction de nos objectifs d'analyse et de contrôle interne* ».

Avec la solution de time-tracking d'Eurécia, la DSI d'iDTGV dispose désormais d'une visibilité fine sur la ventilation des temps et activités par tâches, projets et directions, et a pu structurer et homogénéiser ses processus. Ce qui lui permet de mieux estimer les délais pour réaliser de nouveaux projets, augmentant de facto la qualité de service vis-à-vis de ses « *clients internes* ».

Une extension à la gestion des congés et absences, et à la gestion des notes de frais

Satisfaite de son outil de gestion des temps et des activités, la DSI d'iDTGV propose à la Direction de l'Administration et des Finances (DAF), en juillet 2011, de mettre en œuvre d'autres modules proposés par Eurécia, cette fois-ci sur un périmètre élargi (les 70 collaborateurs de la société). La gestion des congés et absences, des notes de frais et déplacements, ainsi que le suivi des dossiers salariés et des tableaux de bords RH (gestion des entrées et sorties, contrats de travail et avenants, salaire, visites médicales, entretiens annuels, formations…), sont ainsi déployés, en remplacement d'une solution qui ne donnait pas satisfaction, car trop complexe et plus coûteuse. Les nouveaux modules, incluant un connecteur ADP, pour basculer automatiquement les données congés et absences vers le logiciel de paie ADP, sont mis en œuvre en quelques jours. « *Les outils d'Eurécia sont tellement intuitifs que les utilisateurs se les sont immédiatement appropriés* », souligne Fabrice Flottes de Pouzols.

A terme, la DSI d'iDTGV envisage d'utiliser les solutions d'Eurécia pour gérer et refacturer des projets réalisés pour le compte d'entités externes, mais appartenant au groupe SNCF.

À PROPOS D'EURECIA...

Eurécia est un éditeur de logiciels de gestion administrative des RH et de suivi opérationnel des collaborateurs. Disponible uniquement en mode SaaS (Software as a Service), son offre s'articule autour de cinq principaux modules : la gestion des congés et des absences, des notes de frais, des temps et des activités (GTA), du planning ressources et du suivi RH.
Les solutions d'Eurécia sont utilisées par plus de 300 sociétés (20.000 utilisateurs) en France et à l'international. Elles répondent aux besoins de toutes les entreprises, quels que soient leur taille et leur secteur d'activité. L'éditeur compte parmi ses clients des sociétés telles que Berger-Levrault, Bic, Garmin, Gras Savoye, Hi-Media, iDTGV, LaCie, Locatel, Lufthansa, Pulsat, Netbooster, Rexel, Toshiba, UCPA, Vinci Energies…
Créée en 2006 par Pascal Grémiaux, la société est basée à Toulouse. Depuis sa création, l'éditeur double son chiffre d'affaires tous les ans.

EURECIA S.A.S. : 2, rue du Stade - 31320 Toulouse (Castanet) – France | +33 (0)5 62 20 03 69 - Email : contact@eurecia.com
Site : www.eurecia.com

La sécurité, un des avantages des applications SaaS ?

Publié le 23 août 2009

20090823 La sécurité des données et la protection des données personnelles constituent la préoccupation citée en premier par les cadres dirigeants interrogés sur les applications en mode SaaS (Software as a service), devant les capacités d'intégration avec les applications d'entreprise existantes et l'adaptation aux besoins des clients. C'est ce qu'indique un rapport publié par le cabinet Saugatuck intitulé *« Data Breaches Belie Security Concerns Regarding On-Premise vs SaaS and Cloud »*.

Les diverses études, notamment celles réalisées par le Gartner montrent que la sécurité est un sujet de préoccupation majeur. Cette dernière enquête réalisée par le cabinet Saugatuck le confirme une fois de plus. Mais l'élément nouveau ici concerne la sécurité des applications SaaS.

Préoccupations des cadres dirigeants concernant les applications SaaS

2006	2009
Sécurité	Sécurité des données et protection des données personnelles
Possibilité de personnalisation	Intégration des applications SaaS avec les applications du SI
Scalabilité	Personnalisation des applications aux besoins des clients
Questions liées à la réglementation	Intégration des données avec les données stockées sur les systèmes de l'entreprise
Intégration	Intégrité des données et des transactions
Contrôle de la DSI sur le SI	Performances correspondant aux accords SLA

A ce jour, *« aucun éditeur/hébergeur d'applications SaaS n'a rapporté des problèmes majeurs de*

sécurité ou de pertes de données », précise Bruce Guptill, analyse de Saugatuck et auteur du rapport. Cela contraste avec les informations régulièrement publiées sur les incidents de sécurité. Par exemple, récemment aux Etats-Unis, 130 millions d'enregistrement de transactions traité sur les systèmes de la sécurité de la société Heartland Payment Systems ou encore la perte de données par la chaîne hôtelière Radison sur un historique de six mois de transactions (numéros de cartes de crédit, dates d'expiration, noms de possesseur de cartes...).

La majorité des incidents résultent d'erreurs internes

La question qui est posée consiste à savoir si ce bon résultat est lié aux performances des éditeurs d'applications SaaS ou si c'est parce que les hackers portent toujours leur attention et leurs efforts sur les applications résidant sur les systèmes d'entreprise (On-Premise).

Sur les incidents de sécurité liés à des applications installées sur les serveurs des entreprises, 60 % sont causés par des erreurs des équipes informatiques internes. Les 40 % restants correspondent à des tentatives de fraudes effectuées par des personnes étrangères à l'entreprise (contre 21% en 2007). Les entreprises qui ont connu de tels incidents indiquent pourtant avoir mis en œuvre des technologies et des politiques de sécurité adéquates.

« Et pourtant, le nombre et l'importance des incidents n'arrêtent pas d'augmenter. Alors que les fournisseurs d'applications SaaS n'ont pas encore fait état de problèmes majeurs, leurs systèmes sont toujours perçu comme n'offrant pas un bon niveau de sécurité », précise Bruce Gupthill.

Deux types de préoccupations

Concernant les fournisseurs SaaS, les préoccupations liées à la sécurité des données sont de deux ordres. D'abord, elles concernent les menaces habituelles d'accès non autorisés aux systèmes et aux données. Ces attaques sont motivées pour récupérer des données pouvant être assez facilement subtilisées et monétisables. Cela concerne des données d'identité et financières. La grande majorité de ces données est hébergé sur les systèmes internes des entreprises.

Le second niveau de préoccupations est lié au fait que les données partagent les mêmes environnements/serveurs que celles d'autres entreprises. Ils souhaitent être sûrs que leurs données ne peuvent être visibles ou/et utilisés par d'autres entreprises. C'est là la problématique de ce que l'on appelle les architectures multi-tenants. Quelle est l'efficacité de la séparation entre les données et l'instance de l'application ?

Selon le cabinet Saugatuck, les fournisseurs de solutions SaaS/Cloud ont développé des systèmes de sécurité qui vont bien au-delà de ce que habituellement les entreprises mettent en place pour elles-mêmes. Par ailleurs, la sécurité a été intégrée dès la conception des systèmes qu'ils ont mis en place plutôt que développée sur des systèmes existants.

C'est la raison pour laquelle l'auteur de ce rapport conclut que ç la s®curit®devrait °tre un avantage r®el que les fournisseurs de solutions SaaS devraient mettre en avant è.