MAÎTRISER LES RISQUES DE L'INFOGÉRANCE

Externalisation des systèmes d'information

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Agence Nationale de la Sécurité des Systèmes d'Information

Introduction

Dans le domaine des systèmes d'information, le recours à l'externalisation est devenu une pratique courante qui présente un certain nombre d'avantages, mais aussi de risques qu'il convient d'évaluer avant de prendre cette décision.

Il convient à cet égard de ne pas opposer sécurité et externalisation. En effet, le recours à un prestataire peut permettre de pallier l'absence ou l'insuffisance de moyens internes, à condition que le prestataire s'engage sur la sécurité.

Les risques en matière de sécurité des systèmes d'information peuvent être liés au contexte de l'opération d'externalisation mais aussi à des spécifications contractuelles déficientes ou incomplètes.

Forte de ce constat, l'ANSSI a donc entrepris de rédiger un guide, poursuivant les objectifs suivants :

- faire prendre conscience aux décideurs informatiques des risques en matière de sécurité des systèmes d'information (SSI) liés à toute opération d'externalisation ;
- fournir une démarche cohérente de prise en compte des aspects SSI lors de la rédaction du cahier des charges d'une opération d'externalisation ;
- fournir un ensemble de clauses types ainsi qu'une base d'exigences de sécurité, à adapter et personnaliser en fonction du contexte particulier de chaque projet d'externalisation.

La démarche fournie dans ce guide vise à réduire les risques associés à une opération d'externalisation.

Avant-propos

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) publie un certain nombre de méthodes, guides et bonnes pratiques afin d'aider les organismes du secteur public et du secteur privé à gérer la sécurité de leurs systèmes d'information (SI).

Les publications de l'ANSSI sont diffusées sur son site Internet :
http://www.ssi.gouv.fr/publications/

Toutes remarques sur ce guide peuvent être adressées à conseil@ssi.gouv.fr

Table des matières

INTRODUCTION **1**
AVANT-PROPOS **2**
LA DÉMARCHE D'EXTERNALISATION **5**
Terminologie 5
Typologie de l'infogérance 5
LES RISQUES INHÉRENTS À L'EXTERNALISATION **7**
Risques liés à la perte de maîtrise de son système d'information 7
Risques liés à la sous-traitance *7*
Risques liés à la localisation des données *7*
Risques liés aux données à caractère personnel *8*
Risques liés aux choix techniques du prestataire *9*
Risques liés aux interventions à distance 10
Champ d'application *10*
Risques inhérents aux interventions distantes *11*
Recommandations *11*
Mise en œuvre d'une passerelle sécurisée *12*
Risques liés à l'hébergement mutualisé 13
Champ d'application *13*
Risques inhérents à l'hébergement mutualisé *13*
Recommandations *14*
L'informatique en nuage ou nébuleuse 16
PRISE EN COMPTE DE LA SÉCURITÉ DANS LES APPELS D'OFFRES **19**
Apprécier les risques et déterminer les objectifs de sécurité 19
Rédaction du cahier des charges 20
Choix du prestataire 20
LE PLAN D'ASSURANCE SÉCURITÉ **23**
1. Objet du document 24
2. Documents de référence 24
3. Description du système externalisé 24
4. Rappel des exigences 24

5. Organisation....25
6. Responsabilités liées au PAS....27
7. Procédure d'évolution du PAS....27
8. Applicabilité du PAS....28
9. Mesures de sécurité....29
10. Matrice de couverture des exigences de sécurité....30
11. Documentation de suivi....30
CLAUSES DE SÉCURITÉ....31
Transfert du système....31
Responsabilité....31
Obligations du prestataire....31
Comité de suivi....32
Confidentialité....32
Localisation des données....33
Convention de service....33
Audits de sécurité....34
Application des plans gouvernementaux....34
Sécurité des développements applicatifs....35
Gestion des évolutions....35
Réversibilité....35
Résiliation....37
ANNEXE 1 : CLAUSE DE CONFIDENTIALITÉ TYPE EN CAS DE SOUS-TRAITANCE 39
ANNEXE 2 : EXIGENCES DE SÉCURITÉ TYPES....41
ANNEXE 3 : BONNES PRATIQUES POUR L'HEBERGEMENT MUTUALISE....49

1 La démarche d'externalisation

1.1 Terminologie

L'externalisation (en anglais « *outsourcing* ») est une démarche consistant à confier à un tiers tout ou partie d'une activité qui jusqu'alors était réalisée en interne.

L'infogérance est le terme consacré à l'externalisation appliquée au domaine des systèmes d'information.

Selon la définition de l'Agence française de normalisation (AFNOR)[1], « l'infogérance est un service défini comme le résultat d'une intégration d'un ensemble de services élémentaires, visant à confier à un prestataire informatique tout ou partie du système d'information d'un client, dans le cadre d'un contrat pluriannuel, à base forfaitaire, avec un niveau de services et une durée définis. »

1.2 Typologie de l'infogérance

L'infogérance recouvre un large spectre de prestations. Diverses déclinaisons de ce type de service et une multitude d'acronymes ont fait leur apparition : MCO (maintien en condition opérationnelle), TMA (tierce maintenance applicative), ASP (*Application Service Provider*), SAAS (*Software as a service*), MSSP (*Managed Security Service Provider*), etc.

En outre, la nature et le contour des prestations associées à ces termes correspondent souvent à des réalités différentes selon les prestataires.

Les tâches externalisées peuvent être réalisées dans les locaux du prestataire, lorsque le système du client y est hébergé par exemple, ou au moyen d'une liaison permettant d'intervenir à distance sur le système du client. Les tâches externalisées peuvent également être réalisées dans les locaux du client par des équipes du prestataire en charge de ces travaux.

Bien que protéiforme, l'infogérance peut être classée en trois grandes catégories :

- **la gestion d'infrastructures :** il peut s'agir de la maintenance d'un parc informatique, de l'hébergement et/ou de l'administration de serveurs, de la supervision d'équipements réseau et de sécurité, de la gestion de baies de stockage ou de solutions de sauvegarde, etc. ;

[1] Norme AFNOR Z 67 801-1.

- **la gestion des applications** : on peut regrouper dans cette catégorie les activités de support fonctionnel, de maintenance préventive ou corrective, et de gestion des évolutions[2]. Les applications éligibles sont souvent des applications web ou des progiciels de gestion intégrée (« *ERP* » en anglais) ;
- **l'hébergement de service** : le prestataire héberge pour le compte de son client une application utilisée comme un service, accessible le plus souvent par le biais d'un navigateur web ou d'un application spécifique.
  Dans ce cas, le client n'est pas gestionnaire de l'application qu'il exploite pour traiter ses données et s'affranchit totalement des moyens pour la mettre en œuvre. Avec l'apparition des services web, les fournisseurs d'applications hébergées peuvent également fournir à leurs clients une solution plus modulaire, en mettant à leur disposition un service interrogeable à distance et complètement intégrable au sein des applications distantes.

[2] Il est préférable de parler de « gestion des évolutions » que de « maintenance évolutive ». En effet, l'AFNOR définit la maintenance comme l'ensemble des actions permettant de maintenir ou de rétablir un bien dans un état spécifié, ou dans un état où il est en mesure d'assurer un service déterminé.

2 Les risques inhérents à l'externalisation

2.1 Risques liés à la perte de maîtrise de son système d'information

2.1.1 Risques liés à la sous-traitance

Pour répondre à un appel d'offres, un candidat peut se présenter seul, au sein d'un groupement avec une ou plusieurs entreprises, ou encore recourir à la sous-traitance.

Le titulaire du marché peut donc sous-traiter l'exécution de certaines parties de ce dernier, à condition toutefois d'avoir obtenu du pouvoir adjudicateur l'acceptation de chaque sous-traitant et l'agrément de ses conditions de paiement.

Même si le titulaire reste personnellement responsable de toutes les obligations résultant du marché, il convient de vérifier que le ou les sous-traitants disposent des capacités techniques et financières nécessaires à la bonne exécution des prestations.

Il convient également de s'assurer qu'une sous-traitance en cascade ne conduira pas à rendre inefficaces les contraintes de sécurité exigées du titulaire du marché.

En fonction de la nature des prestations sous-traitées et du besoin de sécurité identifié, le donneur d'ordres doit se réserver le droit de récuser tout sous-traitant ne présentant pas les garanties suffisantes pour exécuter les prestations conformément aux exigences de sécurité.

2.1.2 Risques liés à la localisation des données

Il convient de s'assurer que l'ensemble des lieux d'hébergement (site principal, site(s) de secours, de sauvegarde, etc.) répondent d'une part aux exigences de sécurité du donneur d'ordres, et d'autre part aux obligations légales et réglementaires, notamment en ce qui concerne la protection des données à caractère personnel. Il en va de même des sites de télémaintenance s'ils peuvent accéder aux données.

Certains types d'infogérance ne permettent pas de localiser avec certitude les données hébergées. Ce peut être le cas de solutions d'hébergement reposant sur des infrastructures réparties, telles que l'informatique en nuage (voir page 16).

De telles solutions peuvent dans certains cas améliorer la disponibilité du système d'information, mais constituent souvent un facteur d'aggravation des risques d'atteinte à la confidentialité des données.

De manière générale, le risque de divulgation d'informations sensibles dans une opération d'infogérance doit être systématiquement évalué. Là encore, l'analyse de risques doit permettre de bien évaluer la nature et la gravité des impacts consécutifs à une divulgation d'informations et de prendre une décision en connaissance de cause.

Une localisation de données non maîtrisée peut comporter d'autres risques :

- difficulté à exercer un droit de regard et de contrôle sur les personnels du prestataire ;
- difficulté à effectuer un audit de sécurité de l'infrastructure sous-jacente ;
- difficulté à répondre à d'éventuelles injonctions de la justice, pour des raisons fiscales par exemple, ou d'autres raisons d'ordre juridique.

2.1.3 Risques liés aux données à caractère personnel

En outre, le transfert des données à caractère personnel en dehors des frontières de l'Union européenne est réglementé par la directive européenne 95/46/CE et la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

À ce titre, il convient de déterminer si le destinataire du transfert intervient en qualité de « responsable de traitement » ou de « sous-traitant » (au sens de la loi du 6 janvier 1978 modifiée). En effet, cette qualification a des implications importantes en termes de responsabilité.

Comme il n'est pas toujours évident de faire la distinction entre ces deux notions, la Commission Nationale de l'informatique et des Libertés (CNIL) a récemment apporté un éclairage sur leurs rôles respectifs :

- le responsable de traitement se caractérise par son autonomie dans la mise en place et la gestion d'un traitement ;
- le sous-traitant, quant à lui, a pour mission d'exécuter des tâches sur les instructions et sous la responsabilité du responsable de traitement.

Tout traitement de données personnelles par un sous-traitant, ou transfert de données personnelles d'un responsable de traitement à un sous-traitant, ne peut être réalisé que sur instruction du responsable de traitement et à condition qu'un contrat garantissant les mesures de sécurité et de confidentialité mises en place par le sous-traitant soit signé. Un modèle de clause pouvant être utilisé en cas de sous-traitance figure en annexe 1.

Enfin, certaines données font l'objet d'une réglementation spécifique.

Les hébergeurs de données de santé sont par exemple tenus à des obligations de sécurité précises, définies notamment par le Code de la santé publique. Ces derniers doivent disposer d'un agrément délivré par le ministère de la santé.

Les établissements de crédit sont eux aussi assujettis à des garanties spécifiques de sécurité.

Dans tous les cas, il convient de vérifier que les obligations légales spécifiques peuvent être respectées dans l'environnement d'externalisation et, dans l'affirmative, de veiller à leur bonne exécution par le prestataire d'externalisation.

En effet, il faut garder à l'esprit que le donneur d'ordres, en tant que responsable de traitement, encourt des sanctions pénales en cas de non-respect des dispositions de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

2.1.4 Risques liés aux choix techniques du prestataire

La nécessité de faire évoluer le système, pour diverses raisons (obsolescence, montée en charge, nouvelles fonctionnalités demandées), peut nécessiter la mise en œuvre de nouvelles solutions logicielles ou matérielles.

Les choix du prestataire peuvent souffrir de limitations en termes de sécurité, notamment pour des raisons économiques, ce qui pourrait entraîner son incapacité à satisfaire certaines exigences de sécurité du donneur d'ordres. Il convient par conséquent de prévoir que le contrat permette de valider les choix du prestataire, après que ce dernier ait apporté la justification de la conformité avec les exigences de sécurité.

En outre, il faut être particulièrement vigilant sur l'utilisation d'applications propriétaires peu répandues ou de certaines fonctionnalités développées par le prestataire, greffées sur des applications standard. En effet, le prestataire peut à tout moment décider de ne plus maintenir une application ou d'abandonner une fonctionnalité offerte auparavant.

Les applications utilisées doivent être dans la mesure du possible interopérables (*a minima* compatibilité assurée avec les systèmes d'exploitation et bases de données les plus courants).

Il convient de s'assurer que les données peuvent être restituées à tout moment dans un format standard, et si possible ouvert, gage de leur intégration future dans d'autres applications. La description précise de cette restitution (conditions, délais, formats) doit figurer dans le contrat.

De façon générale, la question de la réversibilité doit être une préoccupation permanente du donneur d'ordres. Quelles que soient les évolutions du système, il doit

être en mesure d'en reprendre l'exploitation à son compte, ou de la confier à un autre tiers de son choix, et ce, à tout moment et sans difficulté particulière.

2.2 Risques liés aux interventions à distance

2.2.1 Champ d'application

L'infogérance implique souvent la mise en place de liaisons permettant d'intervenir à distance. En évitant le déplacement d'un ou plusieurs techniciens, les interventions à distance permettent une réduction significative des coûts et des délais d'intervention.

Les principaux modes d'intervention à distance sont :

- le télédiagnostic : supervision d'équipements réseau et sécurité, diagnostic d'anomalies sur une application, etc. ;
- la télémaintenance : réalisation, après le diagnostic, des opérations à distance sur le dispositif ;
- la télédistribution : mise à jour d'une application à distance.

Les interventions à distance concernent d'abord les moyens informatiques :

- serveurs, postes de travail ;
- baies de stockage (SAN, NAS, sauvegardes) ;
- équipements réseau, sécurité ;
- imprimantes, photocopieurs ;
- progiciels de gestion intégrée ;
- etc.

Mais aussi les systèmes de servitude et d'environnement :

- climatisation ;
- onduleurs ;
- autocommutateurs téléphoniques privés (PABX) ;
- surveillance des accès ;
- ascenseurs ;
- etc.

Dans certains cas, la mise en œuvre d'une liaison permettant d'intervenir à distance est indispensable, notamment en cas de besoin élevé en disponibilité du système d'information. On peut citer en exemple le support de solutions de stockage de données ou le télédiagnostic d'un progiciel de gestion intégrée sur un système en production.

2.2.2 Risques inhérents aux interventions distantes

Les risques dépendent des caractéristiques des dispositifs utilisés et du contexte dans lequel ils sont mis en œuvre. Voici un certain nombre de vulnérabilités fréquemment liées aux dispositifs de télémaintenance :

- liaison établie de façon permanente avec l'extérieur ;
- mots de passe par défaut (connus dans le monde entier) ou faibles ;
- présence de failles dans les interfaces d'accès ;
- systèmes d'exploitation des dispositifs non tenus à jour ;
- absence de traçabilité des actions ;
- personnels responsables de ces dispositifs non conscients des problèmes de sécurité ou mal formés ;
- interconnexion de systèmes sécurisés de confiance à des systèmes de niveau faible (internet par exemple).

L'exploitation de vulnérabilités sur un dispositif de télémaintenance est susceptible de faciliter les intrusions dans le système d'information et d'affecter ainsi la sécurité de l'ensemble du SI.

Les principaux risques liés aux dispositifs dédiés aux interventions à distance sont :

- l'intrusion dans le système d'information par une personne non autorisée (exploitation d'un mot de passe faible, d'une faille ou d'une porte dérobée) avec des conséquences plus ou moins graves selon les motivations de l'attaquant et sa capacité à ne pas être détecté :
  - indisponibilité de l'équipement pouvant entraîner l'indisponibilité du système d'information ;
  - atteinte à la confidentialité ou à l'intégrité des données présentes sur le système d'information ;
- l'abus de droits d'un technicien du centre de support lors d'une intervention :
  - accès à des données confidentielles ou téléchargement massif de ces dernières ;
  - modification de données sur le système d'information, éventuellement sans laisser de traces (absence de fonction de traçabilité ou possibilité d'effacer les traces à postériori).

2.2.3 Recommandations

Il est recommandé de demander aux candidats de recenser et de justifier les dispositifs de télémaintenance qu'ils envisagent de mettre en œuvre sur le système du client.

Il doit leur être également demandé un descriptif des dispositifs de télémaintenance et des mesures de sécurité techniques et organisationnelles proposés :

- la sécurité de la liaison : réseau public ou ligne spécialisée, type de VPN, etc. ;
- les dispositifs techniques de sécurité : filtrage des accès réseau, droits d'accès, etc. ;
- les mesures organisationnelles, les procédures retenues pour déclencher une intervention ;
- les mécanismes d'authentification des techniciens assurant le support ;
- la traçabilité des actions ;
- la protection des accès aux données confidentielles en cas d'utilisation sur un système de production ;
- les éventuels rapports d'audit et plans d'action afférents.

Une analyse de risques est nécessaire pour formaliser des objectifs de sécurité ainsi que des mesures adaptées au contexte. Selon la complexité et les enjeux de sécurité du SI, elle pourra être complétée par les documents suivants :

- un document de **procédures d'exploitation de sécurité**, fixant les modalités générales d'exploitation de sécurité des dispositifs de télémaintenance ;
- des **fiches réflexes** permettant de garantir la bonne application des procédures d'exploitation de sécurité par les personnels en charge de l'utilisation ou de l'administration des dispositifs de télémaintenance ;
- un **protocole d'accord** entre le client et la société en charge de la télémaintenance pour formaliser des procédures spécifiques.

2.2.4 Mise en œuvre d'une passerelle sécurisée

Afin que les dispositifs de télémaintenance présentent les garanties suffisantes au regard des risques qu'ils font peser sur le système d'information, il est vivement recommandé de prevoir une passerelle sécurisée dédiée à la télémaintenance.

La mise en place d'une telle passerelle doit permettre de répondre aux objectifs de sécurité suivants :

- authentifier la machine distante et la personne en charge du support ;
- prévenir l'exploitation de vulnérabilités ou de portes dérobées sur le dispositif de télémaintenance ;
- garantir la confidentialité et l'intégrité des données sur le SI ;
- assurer une traçabilité de confiance des actions effectuées par le technicien du centre de support ;
- garantir l'innocuité de la fonction de télémaintenance vis-à-vis du système faisant l'objet du télédiagnostic ainsi que des systèmes connexes ;
- garantir l'absence de fuite d'informations vers l'extérieur.

Il est recommandé de faire procéder à un **audit de la passerelle** pour vérifier que les mesures de sécurité sont effectives et en adéquation avec les objectifs de sécurité.

2.3 Risques liés à l'hébergement mutualisé[3]

2.3.1 Champ d'application

L'hébergement mutualisé consiste à héberger plusieurs services sur un seul et même serveur, afin de rationaliser les ressources. Dans la majorité des cas, les services concernés sont des sites Web, des services de messagerie ou des bases de données.

Les clients n'ont pas accès directement aux serveurs ou aux ressources mutualisées en tant qu'administrateurs. La configuration est réalisée puis gérée par l'hébergeur ou une société tierce.

2.3.2 Risques inhérents à l'hébergement mutualisé

Les risques proviennent du fait que le service hébergé est plus ou moins étroitement lié à d'autres services, certains étant plus vulnérables que les autres. D'autre part, les attaques ciblant une des ressources mutualisées (réseau, logiciel, matériel) pourront avoir des conséquences sur l'ensemble des services co-hébergés.

Du point de vue de la sécurité des systèmes d'information, les principaux risques liés au co-hébergement et leurs répercussions sont les suivants :

- **perte de disponibilité** :
  - une attaque par déni de service provoque l'indisponibilité du serveur hébergeant la cible de l'attaque. Si plusieurs services sont hébergés sur le même serveur, les services qui n'étaient pas pris pour cible, de même que les équipements présents sur le chemin critique (pare-feu, routeurs, etc.) peuvent être indirectement victimes de l'attaque ;
  - les ressources reposent sur un matériel qui n'est pas contrôlé par le propriétaire de la ressource, mais par l'hébergeur. Il se peut qu'un problème matériel non contrôlé ait une répercussion à plus ou moins long terme sur la ressource confiée à l'hébergeur ;
- **perte d'intégrité** :
  - les vulnérabilités permettent souvent, par exécution de code arbitraire, de s'introduire sur dans le système : installation d'une porte

[3] Ce paragraphe s'inspire de la note d'information publiée sur le site du CERTA (Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques), n° CERTA-2005-INF-005, relative aux bonnes pratiques concernant l'hébergement mutualisé.

dérobée, défiguration de site web, vol d'informations, rebond d'attaques, etc.
Si un des services hébergés est pris pour cible d'une telle attaque, l'exécution de code peut toucher l'ensemble des services ;
- un changement de logiciel (voulu ou non) peut avoir une répercussion indirecte sur un service hébergé (non compatibilité, erreurs, etc.) ;

- perte de confidentialité :
  - le fait de voir les services partager le même environnement physique peut conduire à des croisements d'information (contenu des fichiers clients de plusieurs sites dans la même base de données, ou le même sous répertoire, etc.).

Les risques auxquels s'expose un service co-hébergé sont donc augmentés de façon significative dans un environnement non maîtrisé.

Par ailleurs, l'hébergement mutualisé introduit par nature des obstacles au traitement des incidents :

- manque de réactivité dû à la difficulté de trouver un interlocuteur dédié chez l'hébergeur ;
- mauvaises conditions d'analyses dues aux impacts éventuels sur les autres services hébergés (refus ou impossibilité d'isoler du réseau la machine physique qui héberge le service victime de l'attaque) ;
- refus de l'hébergeur de communiquer les journaux d'événements du serveur et des équipements périphériques, pour respecter la confidentialité des autres services.

2.3.3 Recommandations

L'hébergement sur une machine spécifique doit être privilégié. Il convient de préciser que, sauf demande explicite, une solution d'hébergement mutualisé sera prioritairement retenue par l'hébergeur.

Si toutefois le choix d'un hébergement mutualisé est retenu, il convient de bien analyser les conséquences de toutes les attaques potentielles, et de prévoir dans le contrat les actions permettant un traitement efficace d'un incident, notamment la récupération de tous les journaux et l'isolement du réseau sans extinction des machines impliquées.

Si le prestataire met en œuvre des techniques de virtualisation des serveurs, il doit fournir à l'hébergé des compartiments logiques et physiques suffisamment étanches ainsi que des moyens de contrôle.

En cas de recours à un co-hébergement, la réversibilité du contrat d'hébergement est primordiale. En outre, quatre domaines méritent de faire l'objet de prescriptions explicites, en coordination avec le service juridique :

- les journaux d'événements ;
- le suivi du service hébergé (mises à jour, maintenances, sauvegardes, etc.) ;
- les modalités de prévention d'une attaque ;
- la réaction suite à incident.

Ces quatre domaines sont détaillés en annexe 3.

L'informatique en nuage ou nébuleuse

➢ Champ d'application

L'informatique en nuage (en anglais *cloud computing*) est définie par le Journal Officiel du 6 juin 2010 comme « *un mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire* ».

Comme le précise également la définition du JO, il s'agit d'une « *forme de gérance informatique dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients* ».

Les architectures de *cloud computing* mettent généralement en œuvre des technologies de calcul distribué et de virtualisation. Par extension, le *cloud computing* tend à désigner toutes les offres de services qui s'appuient sur de telles architectures, accessibles via Internet ou un autre réseau, qu'elles soient publiques ou restreintes à une communauté (« nuage communautaire ») ou encore à usage interne de l'entreprise (« nuage privé »).

Les offres proposées dans ce type d'architecture sont de trois types :

- *Infrastructure as a Service* : fourniture de ressources matérielles abstraites, typiquement des machines virtuelles, permettant d'installer à distance le système d'exploitation et les applications de son choix ;
- *Platform as a Service* : fourniture de plateformes permettant le développement d'applications à partir d'interfaces de programmation (API) déployées et configurables à distance ;
- *Software as a Service* : fourniture d'applications directement utilisables à distance.

➢ Les risques de l'informatique en nuage

Compte tenu des principes et des technologies mis en œuvre dans l'informatique en nuage, on retrouve la plupart des risques de l'infogérance « *classique* ».

Risques liés à la localisation des données :

En Europe, le cadre juridique de protection des données à caractère personnel s'appuie sur le principe suivant : il doit être possible de constater à tout moment la localisation des données (principe de territorialité).

Or, le plus souvent dans un nuage public, cette localisation est impossible. En effet, les données peuvent être déplacées très rapidement, d'un État à un autre, en fonction des ressources disponibles au sein des infrastructures du prestataire.

L'impossibilité de localiser les données dans les nuages publics pose le problème de la compétence des juridictions et du droit applicable. L'impossibilité de réaliser des audits, parfois imposés par un cadre réglementaire, ne permet pas de vérifier la mise en œuvre des mesures de sécurité.

En l'absence d'un niveau homogène de protection des données personnelles, et de garantie quant aux mesures de sécurités mises en œuvre, la confidentialité des données est incertaine.

Risques de perte de maîtrise de son SI :

- **perte de gouvernance** : en utilisant les services d'une infrastructure d'informatique en nuage, le client concède au prestataire un contrôle total, y compris sur la gestion des incidents de sécurité ;
- **dépendance technologique** : les offres ne garantissent pas toujours la portabilité des données, des applications ou des services. Il paraît difficile dans ces conditions d'envisager un changement de prestataire ou de réinternaliser le système.

Risques liés à la mutualisation des ressources :

- **isolation défaillante** : les mécanismes de séparation des ressources (stockage, mémoire) peuvent être défaillants et l'intégrité ou la confidentialité des données compromises ;
- **effacement incomplet ou non sécurisé** : il n'y a aucune garantie que les données soient réellement effacées ou qu'il n'existe pas d'autres copies stockées dans le nuage.

Enfin, il est plus difficile de se prémunir de ces risques que dans l'infogérance classique. En effet, le client souscrit le plus souvent à des offres par validation d'un contrat type, qu'il est souvent impossible de personnaliser en y intégrant des clauses particulières en matière de sécurité.

➢ Recommandations

On portera une attention particulière à l'appréciation des risques, en particulier en ce qui concerne les données dites « sensibles » (données à caractère personnel, médicales, financières, secrets industriels, etc.).

Il faut être conscient des risques que comporte l'externalisation des services d'une messagerie d'entreprise ou d'une suite bureautique auprès d'un prestataire d'informatique en nuage. Les informations échangées ou traitées par ce biais (pièces jointes, agendas des décideurs, etc.) peuvent revêtir un caractère « sensible », et sont susceptibles d'intéresser la concurrence (intelligence économique).

Comme expliqué précédemment, en l'absence de cadre juridique international adapté à l'informatique en nuage, il est préférable de s'assurer que les données à caractère personnel restent localisées sur des serveurs exclusivement situés dans l'Union européenne – voire en France – et de prévoir les moyens de contrôle de cette obligation.

Enfin il est recommandé d'étudier attentivement les conditions des offres, en particulier le régime juridique auquel sont soumises les données et les mesures mises en œuvre pour assurer leur confidentialité.

3 Prise en compte de la sécurité dans les appels d'offres

La démarche présentée ci-dessous doit aboutir à la rédaction d'un Plan d'Assurance Sécurité (PAS) par le titulaire, dont l'objet est de spécifier les dispositions contractuelles prises par ce dernier, pour répondre aux exigences de sécurité du donneur d'ordres.

3.1 Apprécier les risques et déterminer les objectifs de sécurité

L'étude préalable doit permettre d'apprécier les risques pesant sur le système d'information dans le contexte spécifique de l'opération d'infogérance, en réalisant une analyse de risques.

Les risques ainsi appréciés peuvent être traités selon différentes stratégies :

- réduction du risque : on pourra traiter de cette façon les risques dont la gravité et/ou la vraisemblance (probabilité d'occurrence) peuvent être considérablement réduites par des mesures agissant sur les composantes du risque (source, impact, vulnérabilités, menace) ;
- prise du risque : on pourra maintenir les risques ayant une gravité et une vraisemblance faibles, en particulier si le coût des mesures de réduction est élevé ;
- transfert du risque : en cas de risque financier, une assurance ou toute autre forme de couverture du risque peut être contractée par le donneur d'ordres ; cependant, ce transfert ne peut concerner le risque pénal ;
- évitement du risque : l'analyse de risques peut mettre en évidence le fait que certaines fonctions ou informations particulièrement sensibles ne doivent pas être externalisées dans le contexte de l'opération envisagée.

L'étude des risques doit permettre de déterminer les objectifs de sécurité permettant de rendre les risques acceptables.

L'ensemble des objectifs de sécurité ainsi formalisés permet de définir une cible de sécurité servant de cadre au contrat établi avec le futur prestataire, tout en veillant à lui laisser une certaine marge de manœuvre nécessaire au fonctionnement de ses processus internes.

3.2 Rédaction du cahier des charges

Après avoir déterminé les objectifs de sécurité, le donneur d'ordres spécifie les exigences de sécurité ainsi que les clauses de sécurité dans le cahier des charges.

Les candidats doivent fournir, en réponse à la consultation, un document contractuel appelé Plan d'Assurance Sécurité. Ce document précise les dispositions prises par le futur prestataire pour répondre aux exigences de sécurité du donneur d'ordres pendant toute la durée du contrat.

Le Plan d'Assurance Sécurité doit être inclus dans la liste des documents contractuels. Il peut être cité immédiatement après le Plan d'Assurance Qualité.

Un plan-type d'assurance sécurité, tel que celui proposé au paragraphe 4, sera joint pour servir de cadre de réponse. Il facilitera ainsi la comparaison entre les différentes offres.

Enfin, une clause doit préciser que le prestataire s'engage à exécuter ses obligations selon un Plan d'Assurance Sécurité (PAS), défini en accord avec le donneur d'ordres. Le cas échéant, cette clause doit annuler et remplacer la clause de sécurité générique proposée par le prestataire dans son contrat type.

Plan d'Assurance Sécurité :
Le titulaire s'engage à exécuter ses obligations en termes de sécurité des systèmes d'information selon le Plan d'Assurance Sécurité, dénommé PAS, décrit en annexe du contrat. Le titulaire est responsable de la rédaction initiale du PAS ainsi que de ses évolutions nécessaires pour satisfaire aux exigences de sécurité du donneur d'ordres pendant toute la durée des prestations.

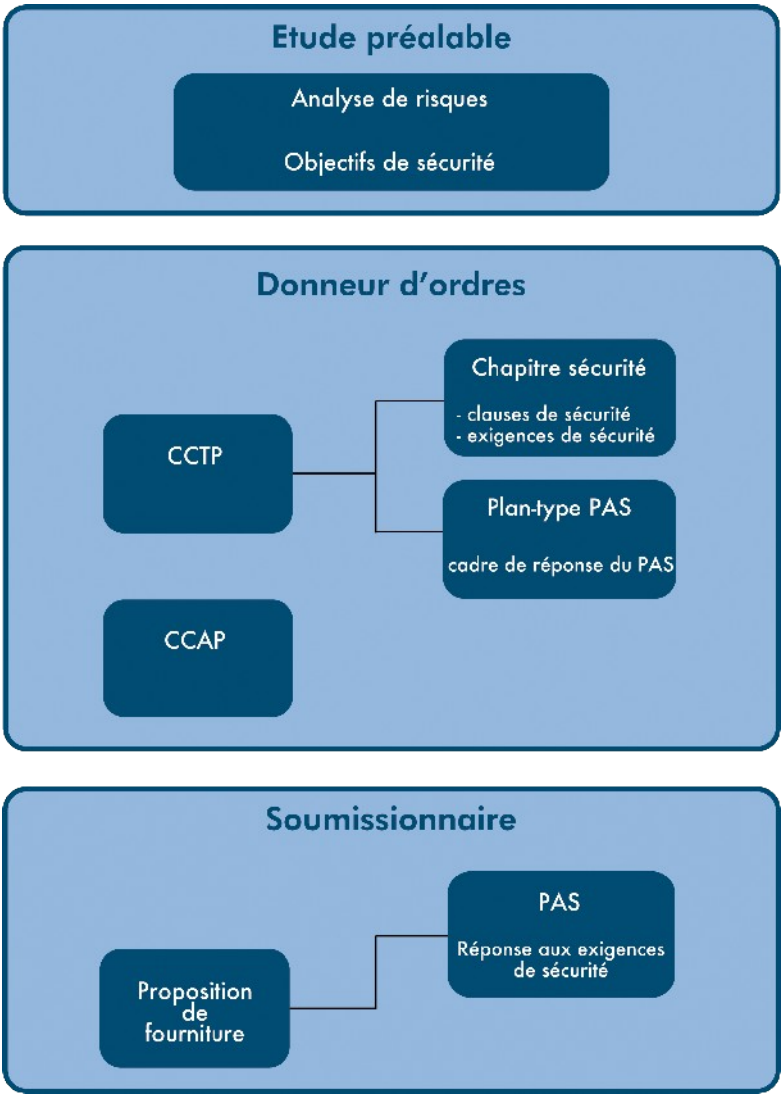
3.3 Choix du prestataire

Il appartient au donneur d'ordres de s'assurer de la recevabilité du Plan d'Assurance Sécurité fourni par les candidats, au regard du plan type et des exigences formulées.

Compte tenu de la pondération des différents critères de choix des offres, il est possible que le candidat retenu n'offre pas les meilleures garanties sur la partie sécurité. Dans ce cas, le Plan d'Assurance Sécurité peut éventuellement faire l'objet d'une mise au point avec lui avant la notification du contrat.

Le Plan d'Assurance Sécurité proposé par le prestataire, et accepté par le donneur d'ordres en conformité avec ses exigences, est annexé au contrat.

Par exemple, dans le cadre d'un marché de l'administration, ces différents documents peuvent être reliés aux cahiers des clauses administratives et techniques particulières (CCAP et CCTP) selon le schéma ci-dessous.


Etude préalable
Analyse de risques
Objectifs de sécurité
Donneur d'ordres
Chapitre sécurité
- clauses de sécurité
- exigences de sécurité
CCTP
Plan-type PAS
cadre de réponse du PAS
CCAP
Soumissionnaire
PAS
Réponse aux exigences de sécurité
Proposition de fourniture

4 Le plan d'assurance sécurité

Le Plan d'Assurance Sécurité (PAS) doit être demandé dans l'appel d'offres. Document contractuel, il décrit l'ensemble des dispositions spécifiques que les candidats s'engagent à mettre en œuvre pour garantir le respect des exigences de sécurité du donneur d'ordres.

C'est aussi un cadre de réponse : il offre une structure pour la réponse des candidats aux exigences de sécurité, ce qui permet de mieux évaluer la pertinence de la couverture des exigences. Il facilite ainsi la comparaison entre les différentes offres.

Une fois le prestataire retenu, le PAS est annexé au contrat. Il se substitue aux éventuelles clauses génériques de sécurité du prestataire.

Le plan-type proposé ci-après pourra être joint à l'appel d'offres comme base de rédaction du Plan d'Assurance Sécurité qui sera fourni par les candidats en réponse à la consultation.

Les paragraphes *en italique* constituent des propositions de contenu du Plan d'Assurance Sécurité à fournir par le prestataire d'externalisation. Ils devront être adaptés selon la nature de l'opération d'externalisation.

1. Objet du document

Ce document décrit les dispositions que <le prestataire d'externalisation> s'engage à mettre en oeuvre pour répondre aux éxigences de sécurité de <le client>. Il définit en particulier l'organisation qui sera mise en place, la méthodologie à suivre pour gérer la sécurité du projet d'externalisation et les mesures techniques, organisationnelles et procédurales qui seront mises en œuvre.

Le candidat précisera le circuit d'approbation du Plan d'Assurance Sécurité, ses modalités d'application et l'étendue de sa diffusion.

2. Documents de référence

Ce paragraphe liste les documents de référence pour le Plan d'Assurance Sécurité.

À titre d'exemple, les documents applicables peuvent être les suivants :

- *le contrat ;*
- *le cahier des charges, incluant les exigences de sécurité du client ;*
- *le plan d'assurance qualité ;*
- *etc.*

3. Description du système externalisé

Ce paragraphe présente succinctement le système faisant l'objet de l'opération d'externalisation. L'accent sera mis sur les points qui justifient la mise en œuvre de mesures de sécurité.

4. Rappel des exigences

Le candidat rappellera les exigences de sécurité du client ou fera référence au document les spécifiant.

5. Organisation

Le candidat indiquera l'organisation qu'il propose pour gérer la sécurité dans le projet d'externalisation.

On y trouve au minimum :

- le maître d'ouvrage agissant en tant que client ;
- le prestataire d'externalisation.

Si des co-traitants, sous-traitants ou fournisseurs peuvent intervenir directement, il indiquera leur rôle et précisera éventuellement les modalités de leur participation à la gestion de la sécurité du projet.

Il décrira l'organisation mise en place pour assurer les relations avec le maître d'ouvrage concernant les aspects sécurité :

- comité de suivi de la sécurité : fréquence, participants, modalités, périmètre du suivi ;
- organisation de la maîtrise d'ouvrage : responsable sécurité, rôle et moyens ; intervenants techniques ;
- organisation du prestataire : responsable sécurité, rôle et moyens ; responsables techniques, implication des co-traitants et sous-traitants éventuels ;
- diffusion du Plan d'assurance sécurité et des documents de suivi ;
- audits, contrôles réalisés par la maîtrise d'ouvrage ou à la demande de celle-ci : modalités, périmètre, exploitation des résultats.

Organisation de la maîtrise d'œuvre :

En tant que maître d'œuvre, <le prestataire d'externalisation> désignera un interlocuteur responsable de la sécurité, pilotant l'ensemble de la sécurité du projet : sécurité des développements, sécurité du système d'information cible et intégration des composants sécurité. Il est rattaché directement au responsable de l'opération, au directeur de projet par exemple, désigné par le <prestataire d'externalisation>.

Le responsable de la sécurité désigné par <le prestataire d'externalisation> prend en charge l'organisation des comités de suivi sécurité : convocation, proposition d'ordre du jour, rédaction des comptes-rendus [cf clause Comité de suivi].

Il pourra convier à ces réunions les intervenants impliqués dans les sujets inscrits à l'ordre du jour : sécurité applicative, sécurité des serveurs, sécurité des échanges…

Il conseille le client dans son approche de la sécurité du projet, selon les audits, les incidents perçus sur le système ou les évolutions du contexte opérationnel.

Organisation de la maîtrise d'ouvrage :

<Le client> désignera un interlocuteur responsable de la sécurité du projet <projet d'externalisation>. Cet interlocuteur unique sera rattaché directement au directeur de projet. Cet interlocuteur sera responsable de l'ensemble de la sécurité du projet pour <le client>, tant sur les aspects sécurité du système d'information cible que sur les aspects sécurité des interfaces avec le prestataire d'externalisation.

Des réunions de pilotage sécurité seront programmées tous les <période à évaluer>. Les participants à ces réunions pour <le client> seront le directeur du projet, le responsable de la sécurité, <liste à compléter> ainsi que le responsable technique ou fonctionnel lorsqu'ils sont impliqués dans les points à l'ordre du jour.

La sécurité globale de <l'opération d'externalisation> repose sur la participation active des différents intervenants : personnel interne qui avait un rôle dans le fonctionnement antérieur du système ou service faisant l'objet de l'opération d'externalisation [intégrateur, développeur, administrateur, exploitant, responsable technique, etc.], maîtrise d'ouvrage et maître d'œuvre.

Le responsable de la sécurité désigné par <le client> a pour mission de faciliter les relations entre les différents intervenants, et de mettre à disposition de la maîtrise d'œuvre l'ensemble des documents nécessaires au bon déroulement du projet sécurité lié à l'opération d'externalisation : politique de sécurité interne du <client>, documentation technique du système [documents d'ingénierie, documents d'exploitation, etc.], spécifications, etc.

Il a également pour mission de s'assurer de la prise en compte globale de la sécurité, par la maîtrise d'ouvrage et la maîtrise d'œuvre.

Il décide de la conduite à tenir selon le résultat des audits, des incidents ou des conseils remontés par le prestataire d'externalisation.

Il valide l'ensemble des actions réalisées au titre de la gestion de la sécurité du projet.

6. Responsabilités liées au PAS

Le candidat, au travers de son responsable de la sécurité désigné, est responsable de la rédaction, de l'évolution et de l'application du Plan d'Assurance Sécurité.

Il s'applique à l'ensemble des équipes de la maîtrise d'œuvre (et aux sous-traitants éventuels).

Sa rédaction relève du responsable sécurité désigné par <le prestataire d'externalisation>. Il doit être approuvé par la maîtrise d'ouvrage ; sa bonne exécution est de la responsabilité du <prestataire d'externalisation> en tant que maître d'œuvre.

La cohérence de l'ensemble des mesures pourra être analysée et réévaluée lors des réunions d'avancement (ou revues de pilotage).

7. Procédure d'évolution du PAS

Le titulaire est responsable de la rédaction du PAS initial et de ses évolutions pour répondre aux exigences de sécurité du donneur d'ordres pendant toute la durée du contrat.

Voici une liste (non exhaustive) des situations susceptibles d'entraîner une modification du PAS :

- évolution du système d'information (configuration logicielle ou matérielle) ;
- évolution de l'environnement du système d'information (locaux, personnels, procédures, etc.) ;
- évolution du périmètre de l'opération.

En cas d'évolution du système, de son environnement, ou du périmètre de l'opération d'externalisation, le titulaire vérifie si le PAS doit être modifié. Si tel est le cas, il propose une modification au client. Si cette modification est acceptée, le PAS est révisé et soumis au client pour validation formelle.

Le responsable sécurité désigné par <le prestataire d'externalisation> est responsable de la rédaction du Plan d'Assurance Sécurité initial et de ses évolutions.

Une révision du Plan d'Assurance Sécurité pourra être réalisée en cas d'évolution du périmètre de l'opération ou des exigences de la maîtrise d'ouvrage, après accord de la maîtrise d'œuvre. Cette révision sera réalisée par le responsable sécurité désigné par <le prestataire d'externalisation>. La version révisée du PAS sera transmise à la maîtrise d'ouvrage pour validation, et diffusée à l'ensemble des acteurs pour application.

8. Applicabilité du PAS

L'applicabilité du PAS s'articule autour des trois points suivants :

- quelles sont les procédures à suivre lors de non respect du PAS ?
- quelle est la procédure à suivre pour une demande de dérogation ?
- quelles sont les pénalités encourues ?

Le Plan d'Assurance Sécurité est applicable à l'ensemble des acteurs du projet, au même titre que le Plan d'Assurance Qualité et avec la même priorité.

Un acteur du projet identifiant un non respect du PAS dans ses procédures et mesures doit en référer immédiatement au <prestataire d'externalisation>, qui en avertira la maîtrise d'ouvrage. Un modèle type de rapport de non respect sera annexé au PAS définitif, spécifiant la forme du rapport, la liste de diffusion, les responsabilités des acteurs, et le planning de traitement de la clause de non respect.

Si la cause du non respect n'est pas corrigée dans un délai de <délai à estimer>, <le prestataire d'externalisation> subira une pénalité suivant la formule : <formule à calculer>.

Un acteur du projet n'étant pas à même de remplir l'ensemble des clauses du PAS devra effectuer une demande de dérogation auprès du <prestataire d'externalisation>, qui négociera avec <le client> l'ensemble des demandes de dérogation. Un modèle type de demande de dérogation sera annexé au PAS définitif, spécifiant la forme de la demande, la liste de diffusion, les responsabilités des acteurs, et le planning de traitement de la demande de dérogation.

9. Mesures de sécurité

Le candidat décrira les mesures destinées à assurer la sécurité du système cible de l'opération d'externalisation pendant les différentes phases contractuelles : phase de transfert, phase d'exploitation, phase de réversibilité ou fin de contrat.

9.1 Transfert

Le candidat présentera dans ce paragraphe les mesures proposées pour sécuriser la phase de transfert du système (transfert de matériels ou de logiciels dans un projet d'externalisation) *[cf clause de transfert]*.

Il décrira les procédures de contrôle de la sécurité du transfert mises en œuvre et identifiera ses obligations de *reporting* au comité de suivi sécurité *[cf clause de contrôle des prestations et des résultats]*.

Les exigences de sécurité formulées par le client indiquent le niveau de confidentialité maximum des informations manipulées notamment lors du transfert. Une liste de personnes susceptibles de participer au transfert pourra être rédigée et communiquée au client. Le client devra indiquer s'il juge nécessaire que le personnel soit soumis à une clause de confidentialité ou procéder à une habilitation *[cf clause de confidentialité]*.

9.2 Exploitation

Le candidat présentera dans ce paragraphe les mesures mises en place pour assurer la protection du système externalisé en réponse aux exigences identifiées par le client.

9.3. Réversibilité

Le candidat s'engagera à apporter l'assistance nécessaire durant la période de migration pour faciliter le transfert des moyens de sécurité matériels et logiciels, et la reprise de leur exploitation par le client, ou par un autre prestataire de service *[cf clause de réversibilité]*.

10. Matrice de couverture des exigences de sécurité

Le candidat présentera les mesures de sécurité techniques, procédurales et organisationnelles retenues pour répondre aux exigences du donneur d'ordres. Il pourra pour ce faire reprendre dans un tableau les exigences énoncées, et lister la ou les mesure(s) répondant à chaque exigence.

11. Documentation de suivi

Le candidat recensera dans ce paragraphe l'ensemble de la documentation concernant la sécurité qu'il s'engage à fournir au titre du projet. Ces documents pourront être les suivants :

Nature du document :	Date de remise :
Plan d'Assurance Sécurité, version 1	Remise du dossier de réponse à consultation
Plan d'Assurance Sécurité, version définitive	Début de phase de transfert
Dossier de sécurité	Début de phase d'exploitation
Plan de secours	Début de phase d'exploitation
Plan de gestion des incidents	Début de phase d'exploitation
Comptes-rendus de réunion du comité de suivi	Une semaine après chaque réunion

5 Clauses de sécurité

Les clauses qui suivent couvrent l'ensemble des typologies d'externalisation. Elles ne sont donc pas adaptées à tous les marchés. Par exemple, la clause relative au transfert du système ne s'applique que lorsque celui-ci est hébergé chez le prestataire.

Il appartient au rédacteur du contrat d'externalisation de retenir les clauses pertinentes compte tenu du contexte, et d'en élargir leur portée si besoin.

5.1 Transfert du système

Le prestataire se porte garant de l'intégrité et de la confidentialité des données qui lui sont confiées pendant la phase de transfert du système d'information. Il appartient en particulier au prestataire de faire des sauvegardes des informations du client et de gérer ces sauvegardes de manière à permettre une reprise en cas d'incident lors de la bascule du système.

Cette clause doit également préciser les modalités de réception de la composante sécurité du système externalisé.

5.2 Responsabilité

La clause de responsabilité détermine les limites de responsabilité entre le prestataire et le client. En fonction de la nature des prestations et du système, il sera nécessaire de préciser le périmètre de responsabilité des acteurs sur l'ensemble des domaines, en particulier sous l'angle de la sécurité :

- la description de la nature des risques et des montants couverts par des contrats d'assurance de type responsabilité civile ;
- la déclaration d'existence de sous-traitants et la nature des relations avec ces derniers sur le plan des responsabilités.

5.3 Obligations du prestataire

Le prestataire reconnaît être tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art. En particulier il s'engage à informer le client des risques d'une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d'actions correctives ou de prévention.

Outre le respect de ses obligations au titre de la convention de service, le prestataire informera préalablement le client de toute opération susceptible de provoquer l'indisponibilité (ou une dégradation des performances) du système.

Le prestataire est responsable du maintien en condition de sécurité du système pendant toute la durée des prestations.

Les mécanismes de sécurité mis en œuvre doivent évoluer conformément à l'état de l'art : la découverte de failles dans un algorithme, un protocole, une implémentation logicielle ou matérielle, ou encore l'évolution des techniques de cryptanalyse et des capacités d'attaque par force brute doivent être pris en compte.

5.4 Comité de suivi

Cette clause permet de créer une instance qui va coordonner les actions prévues au contrat au titre de la sécurité. La création d'un Comité de suivi sécurité permettra de gérer la mise en place et l'évolution du volet sécurité de la prestation : respect du calendrier, conformité des prestations, respect de l'obligation de collaboration, validation des améliorations pour accroître la sécurité.

Il traitera également des questions techniques touchant à la sécurité : collaboration dans la gestion des droits et la gestion des incidents, détection des anomalies et préconisation d'améliorations, exploitation des résultats des audits de contrôle des prestations sécurité.

C'est également ce comité qui traitera des obligations liées à la loi du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux libertés : déclaration par le client auprès de la CNIL, communication des déclarations au prestataire, informations par le prestataire des modalités de gestion ou d'exploitation des applications et des modifications de celles-ci.

Le comité de suivi s'assurera également des conditions techniques et financières de transfert des moyens de sécurité matériels et logiciels mis en place, en cas de réversibilité de l'opération. Des réunions périodiques seront planifiées contractuellement.

5.5 Confidentialité

Une clause de confidentialité devra mentionner la nature juridique de l'obligation de confidentialité, l'étendue des informations couvertes par l'interdiction de divulgation, et spécifier les personnes soumises à cette obligation.

La clause de confidentialité doit indiquer les modalités d'application de l'obligation

dans le temps ; elle s'applique *a priori* pendant toute la durée de l'exécution du contrat, et doit dans la plupart des cas s'appliquer après la cessation de relations contractuelles.

Cette clause pourra être étendue à une obligation de suivre une procédure d'autorisation pour les personnels, voire d'habilitation pour les projets classifiés.

Les informations couvertes par l'interdiction de divulgation de confidentialité doivent concerner :

- le contenu hébergé : les informations ou fonctions traitées par le système ;
- les informations dont la divulgation est de nature à porter atteinte à la sécurité du système (mots de passe, clés de chiffrement, documentations relative à l'architecture et la sécurité du système, etc.).

Un modèle de clause de confidentialité spécifique à la sous-traitance figure en annexe 1.

5.6 Localisation des données

Les lieux d'hébergement des données doivent satisfaire aux exigences de sécurité du donneur d'ordres et aux dispositions de la loi du 6 janvier 1978 modifiée, relative à la protection des données personnelles.

Le prestataire doit communiquer la liste de tous les lieux de stockage de données (site d'hébergement principal, site(s) de secours, etc.). Si la faisabilité technique de cette exigence peut s'avérer délicate dans le cadre d'architectures distribuées, il peut être demandé au prestataire d'être en mesure de localiser, *a posteriori*, et non en permanence, le lieu de stockage des données, en particulier suite à un incident.

Cette clause pourra être complétée par un certain nombre d'exigences, permettant notamment de garantir une bonne accessibilité des sites d'hébergement.

5.7 Convention de service

Cette clause est la formalisation d'un accord entre le prestataire et le client relatif au niveau de service attendu (*Service Level Agreement*). Ainsi, il pourra être demandé au prestataire des engagements concernant :

- le taux de disponibilité du système (en heures ouvrées / non ouvrées) ;
- la durée et l'occurrence maximale d'indisponibilité mensuelle, trimestrielle ou annuelle d'un composant ou du système ;
- le temps de réponse d'une application ou de certaines requêtes, la durée maximale de certains traitements ;
- le temps garanti d'intervention sur site (GTI) ;

- le temps garanti de remise en état d'un composant matériel ou logiciel défectueux (GTR), ou d'une chaîne de liaison ;
- le temps moyen entre deux pannes (MTBF) ;
- le taux de panne mensuel, trimestriel ou annuel d'un composant ou du système (taux de fiabilité).

Ces engagements pourront être définis pendant une phase probatoire, et réajustés à l'issue de celle-ci. Ils pourront également être redéfinis en cas de modification du périmètre de l'opération.

Les niveaux d'engagement, de même que les pénalités en cas de non respect de ces derniers, seront négociés selon les spécificités de chaque projet.

5.8 Audits de sécurité

Le client doit pouvoir, à tout moment, contrôler que les exigences de sécurité sont satisfaites par les dispositions prises par le prestataire.

Le périmètre et la périodicité des audits de sécurité doivent être précisément définis.

Les audits pourront être réalisés par le client, ou délégués à un tiers. Le contrôle s'effectuera selon des modalités contractuelles définies (visite des locaux du prestataire avec interviews individuelles des membres des équipes du prestataire, accès aux machines mises à la disposition du prestataire).

Cette visite sera notifiée au prestataire selon un délai prévu par le contrat. Un délai de 15 jours est recommandé car il permet à l'hébergeur de s'organiser (rassembler la documentation, s'assurer de la disponibilité des personnes concernées).

Le cas d'une intervention urgente du fait, par exemple, de la survenance d'un incident de sécurité à traiter doit être prévu.

La pratique de tests intrusifs doit être encadrée par une charte commune signée entre le prestataire, l'exécutant de l'audit et le client.

Le client doit se réserver le droit de requérir l'expertise d'un organisme ou d'une société tierce présentant des compétences en matière de sécurité.

5.9 Application des plans gouvernementaux

Dans le cadre de l'application de plans gouvernementaux, le Premier Ministre peut décider la mise en œuvre d'un ensemble de mesures spécifiques destinées à lutter contre des attaques notamment terroristes visant les systèmes d'information de l'État ou

les systèmes d'information et réseaux de télécommunications des opérateurs d'infrastructures vitales.

Dans le cadre de ce marché, le prestataire pourrait être concerné par ces alertes décidées au niveau gouvernemental, et s'engage à appliquer les consignes de sécurité données par le donneur d'ordres. Ces mesures sont susceptibles d'évoluer. Les modifications seront régulièrement transmises durant l'exécution du marché.

5.10 Sécurité des développements applicatifs

Le prestataire est tenu d'assurer la sécurité des développements conformément à l'état de l'art dans chacune des technologies mises en œuvre.

Voici une liste (non exhaustive) de règles applicables :

- environnement applicatif maintenu en tenant compte des recommandations d'application de correctifs par les éditeurs ;
- contrôle rigoureux des entrées utilisateurs ;
- sécurisation des accès aux fonctions d'administration ;
- installation du minimum de fonctions nécessaires lors de l'installation ;
- principe du moindre privilège ;
- utilisation de mots de passe dans le code interdite ;
- mise en œuvre d'une gestion efficace des erreurs.

Pour la mise en œuvre de technologies web, les développements pourront s'appuyer sur les recommandations de l'OWASP (*Open Web Application Security Project*).

La recette de l'application comprend une revue de code permettant de s'assurer d'une implémentation conforme aux exigences de sécurité. La correction d'éventuelles anomalies détectées lors de la revue de code sont à la charge du prestataire.

5.11 Gestion des évolutions

Les évolutions fonctionnelles ou techniques ne doivent pas remettre en cause le respect des exigences de sécurité ou compromettre une éventuelle opération de réversibilité. En cas d'évolution, le prestataire devra vérifier que sa mise en œuvre est conforme aux exigences contractuelles et en apporter la justification auprès du donneur d'ordres, avant validation par ce dernier.

5.12 Réversibilité

En raison des investissements importants qu'il nécessite, le contrat d'externalisation est destiné à s'inscrire dans la durée. Néanmoins, la clause de réversibilité doit permettre

au client de reprendre la gestion de la fonction externalisée, soit pour l'exploiter directement, soit pour en confier l'exploitation à un tiers de son choix.

Cette clause pourra être activée à tout moment en respectant le délai légal qui doit être stipulé dans le contrat, et ce, sans justification particulière. Un changement dans l'actionnariat du prestataire, une délocalisation des sites d'hébergement, ou le non suivi du Plan d'Assurance Sécurité sont des raisons envisageables pour activer la clause de réversibilité.

Le prestataire s'engage à apporter l'assistance nécessaire durant la période de migration pour faciliter le transfert des moyens de sécurité matériels et logiciels, et la reprise de leur exploitation par le client, ou par un autre prestataire de service.

Le prestataire s'engage à garantir, lors du transfert, la sécurité des données et des applications qui lui ont été confiées, conformément à ses obligations.

En outre, la phase de réversibilité ne doit pas, en principe, modifier la qualité, les termes et les conditions des services fournis durant le contrat et définis dans le *Service Level Agreement* (SLA).

En cas d'arrêt des prestations confiées au titulaire par le donneur d'ordres, l'ensemble des matériels, logiciels et documentations confiés au titulaire doivent être restitués.

Le déménagement de cet ensemble des locaux du titulaire sera assuré aux frais du titulaire dans un délai maximum d'un mois après l'arrêt des prestations confiées au titulaire.

Une non restitution de tout ou partie de cet ensemble sera considérée et traitée comme une perte.

Une restitution partielle peut être demandée par le donneur d'ordres, en cas d'arrêt d'une partie des prestations avant la fin du marché. Dans ce cas, le titulaire en sera informé au moins un mois avant la fin des prestations.

À la fin de l'exécution du présent marché, le titulaire est tenu :

- de transférer à l'équipe du futur titulaire les informations sur le contexte fonctionnel et technique de l'ensemble applicatif ainsi que sur les aspects de suivi du projet ;
- de préparer un support informatique défini par le donneur d'ordres contenant tous les éléments (documentations, programmes, chaînes de compilation…) gérés par le titulaire actuel et qui seront, à l'issue de cette prestation, placés sous la responsabilité du futur titulaire (cette mise à disposition devra être faite sous un format pouvant permettre au futur titulaire d'installer, le cas échéant, l'ensemble de ces éléments sur une plate-forme de son choix pour examen approfondi par celui-ci) ;

- d'assurer une formation fonctionnelle approfondie (du type formation utilisateur et administrateur) aux personnels du futur titulaire, avec travaux pratiques sur poste de travail, en présence de représentants du donneur d'ordres. Cette formation devra s'appuyer sur les documentations utilisateurs et techniques rédigées par le titulaire.

En particulier, au titre de cette prestation, le titulaire :

- lance la prestation avec le futur titulaire et les représentants du donneur d'ordres. Il s'agit, au plus, de deux jours de réunion en vue de valider le planning et les modalités pratiques de cette phase ;
- met à disposition tous les éléments et documents produits par ou remis au présent titulaire ;
- présente l'ensemble des composants techniques ou fonctionnels du projet ;
- répond aux questions du futur titulaire concernant l'organisation pratique des configurations et des documents techniques sous 48 heures ;
- présente l'organisation de la maintenance corrective actuelle et l'environnement de développement et d'exploitation (répertoires, installation, procédures mises en œuvre, périodicité et ordonnancement des opérations d'exploitation, etc.) ;
- accueille, durant deux semaines, deux ou trois personnes du futur titulaire afin de leur permettre d'observer l'activité assurée par l'équipe projet en place (assistance téléphonique, exploitation de serveurs de développement, etc.) ;
- communique au futur titulaire les réponses apportées aux demandes d'assistance téléphonique traitées.

5.13 Résiliation

Cette clause a pour but de prévoir les motifs de résiliation de plein droit du contrat.

Dans le cadre d'un manquement grave par le prestataire à l'une des obligations de sécurité mises à sa charge dans le présent contrat, le client pourra le mettre en demeure de réparer ce manquement dans un délai donné. À l'issue de ce délai, si le manquement n'est pas réparé, le client pourra résilier de plein droit le contrat.

De façon générale, tout manquement aux clauses doit entraîner des pénalités ou la résiliation, avec ou sans préavis.

ANNEXE 1 : CLAUSE DE CONFIDENTIALITÉ TYPE EN CAS DE SOUS-TRAITANCE[4]

Les supports informatiques et documents fournis par la société …… [identité du responsable de traitement] à la société …… [identité du prestataire] restent la propriété de la société …… [identité du responsable de traitement].

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226-13 du code pénal), il en va de même pour toutes les données dont la société …… [identité du prestataire] prend connaissance à l'occasion de l'exécution du présent contrat.

Conformément à l'article 34 de la loi informatique et libertés modifiée, la société …… [identité du prestataire] s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

La société …… [identité du prestataire] s'engage donc à respecter les obligations suivantes et à les faire respecter par son personnel :

- ne prendre aucune copie des documents et supports d'informations qui lui sont confiés, à l'exception de celles nécessaires à l'exécution de la présente prestation prévue au contrat, l'accord préalable du maître du fichier est nécessaire ;
- ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent contrat ;
- ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
- prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat ;
- prendre toutes mesures de sécurité, notamment matérielles, pour assurer la conservation et l'intégrité des documents et informations traités pendant la durée du présent contrat ;
- et en fin de contrat, à procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies.

À ce titre, la société …… [identité du prestataire] ne pourra sous-traiter l'exécution des prestations à une autre société, ni procéder à une cession de marché sans l'accord préalable de la société …… [identité du responsable de traitement].

[4] Clause de confidentialité inspirée de celle proposée par la CNIL en cas de sous-traitance.

La société …… [identité du responsable de traitement] se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par la société …… [identité du prestataire].

ANNEXE 2 : EXIGENCES DE SÉCURITÉ TYPES

Avertissement : les exigences de sécurité qui suivent doivent êtres sélectionnées avec prudence, d'une part en fonction des spécificités du système d'information, d'autre part en tenant compte de la nature des prestations externalisées.

➢ Gestion de la sécurité

Le candidat précisera les moyens mis en œuvre dans le cadre du processus d'amélioration continu de la sécurité de ses infrastructures d'hébergement.

Cette description peut être avantageusement présentée selon les 4 étapes de la méthode de gestion de la qualité PDCA (*Plan-Do-Check-Act*) :

- phase de préparation ;
- phase de réalisation ;
- phase de vérification : préciser la fréquence ainsi que le périmètre technique et organisationnel des audits réalisés en interne par les équipes du prestataire ou par une société tierce ;
- phase d'ajustement (mesures correctives suite aux insuffisances constatées lors de la vérification).

➢ Protection antivirale

Une politique antivirale stricte devra être mise en place au niveau des serveurs dont le titulaire a la charge. La mise à jour des signatures devra être automatique et d'une fréquence élevée (30 minutes).

La politique antivirale appliquée sur le système d'information du titulaire devra être précisée (postes de travail des exploitants notamment).

Le candidat fournira dans sa réponse une description des solutions anti-virus sur lesquelles se base son service de messagerie (logiciel, version) et décrira les modalités et la fréquence de mise à jour du service.

Un contrôle de non contamination des serveurs Web de production devra être effectué périodiquement. Le candidat précisera les modalités de mise en œuvre de ce contrôle.

➢ Mises à jour, correctifs de sécurité

Le titulaire applique les correctifs recommandés par les fournisseurs de solutions matérielles ou logicielles (logiciels système ou applicatifs, logiciels embarqués) sur tous les matériels dont il a la charge.

En cas d'alerte grave (attaque virale, faille critique) annoncée par le CERTA (Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques),

le correctif doit être appliqué dans un délai de 24 heures sur les infrastructures hébergeant le système du donneur d'ordres (serveurs, pare-feux, routeurs ouverts vers l'extérieur).

Lorsqu'aucun correctif n'est disponible, le titulaire doit suivre les recommandations de l'éditeur ou du CERTA dans le cadre d'un contournement provisoire. Si le contournement nécessite la désactivation d'une fonctionnalité indispensable au système, le titulaire s'engage à proposer des mesures permettant d'éviter l'exploitation de la vulnérabilité.

Le traitement des alertes mineures pourra intervenir durant les périodes de maintenance hebdomadaires ou mensuelles.

Les passages de correctifs doivent être précédés d'une sauvegarde spécifique du système et des données qu'il contient, ainsi que de tests sur un environnement de pré-production.

Le titulaire devra mettre à jour le dossier de définition avec la liste des correctifs de sécurité appliqués sur les serveurs et communiquer au donneur d'ordres la version actualisée du document.

La validation du bon fonctionnement du système se fera conjointement avec les équipes techniques du titulaire et le chef de projet responsable de l'application hébergée.

En cas d'alerte donnée par les équipes d'experts du titulaire, par l'administration ou le CERTA, le maître d'ouvrage sera notifié par téléphone et courrier électronique avant toutes opérations. La décision de l'action ne pourra être prise que par des personnels de la maîtrise d'ouvrage désignés par écrit. En particulier, le responsable sécurité de la maîtrise d'ouvrage sera le correspondant privilégié pour le suivi des opérations.

Le titulaire s'engage à fournir une adresse mail, un numéro de téléphone et les périodes correspondantes d'opération (H24, heures ouvrables, …) permettant au maître d'ouvrage de suivre le traitement d'une alerte.

- Sauvegardes et restauration

Le titulaire doit prendre toutes les mesures qui s'imposent en termes de sauvegarde et de restauration pour se conformer au niveau de service exigé.

Les opérations de sauvegardes donnent lieu à un compte-rendu par messagerie avec indicateur de réussite ou d'échec.

La fiabilité des sauvegardes sera mise à l'épreuve par des tests de restauration mensuels, dont les rapports seront communiqués dans le mois suivant les tests.

Un double exemplaire des sauvegardes doit être conservé dans des locaux physiquement séparés du centre informatique du prestataire hébergeant l'application du donneur d 'ordres.

Le titulaire doit prendre des mesures permettant de garantir la confidentialité des données relatives aux sauvegardes :

- confidentialité des flux lors des opérations de sauvegardes ;
- stockage sécurisé des sauvegardes.

En cas de sauvegarde externalisée, les sauvegardes doivent être chiffrées avant leur transfert et la clé de chiffrement connue seulement du titulaire et du donneur d'ordres.

Dans le cadre de plans de sécurité gouvernementaux, le donneur d'ordres pourra imposer une augmentation de la fréquence des sauvegardes.

➢ Continuité d'activité

Le titulaire doit prendre toutes les mesures nécessaires pour assurer la disponibilité du système d'information, conformément aux exigences définies dans la clause relative au niveau de service exigé.

Le candidat indiquera les mesures techniques, organisationnelles, procédurales qu'il s'engage à prendre pour assurer la continuité d'activité du système, ou en cas de sinistre la reprise d'activité conformément aux exigences définies dans la clause sur la convention de service.

Les procédures de sauvegarde et de secours seront auditées conformément aux modalités identifiées dans la clause relative aux audits de sécurité.

➢ Authentification

Pour chaque interface d'accès au système, (Interface Homme-Machine, interface entre applications) le titulaire doit fournir une documentation précisant :

- les mécanismes d'authentification mis en œuvre (protocoles, algorithmes de hachage et de chiffrement utilisés) ;
- la liste exhaustive des comptes d'accès existants ainsi que des rôles et privilèges qui y sont associés.

Les moyens d'authentification associés aux interfaces doivent être interopérables tant au niveau des applications clientes (par exemple navigateurs web) que des systèmes d'exploitation.

Les interfaces d'accès aux fonctionnalités bas niveau (exemple : configuration du BIOS) doivent impérativement authentifier un utilisateur (mise en place d'un mot de passe pour l'utilitaire de configuration du BIOS).

Les identifiants des comptes d'accès sont nominatifs. L'utilisation d'un même compte par plusieurs personnes n'est pas autorisée sauf si une contrainte le justifiant est acceptée par le donneur d'ordres. Dans ce cas, le candidat présentera les mesures techniques et/ou organisationnelles pour garantir l'imputabilité.

L'utilisation de mots de passe constructeur ou par défaut est interdite.

L'utilisation de protocoles dont l'authentification est en clair est interdite

Les mots de passe doivent satisfaire aux contraintes de complexité suivantes :

- Avoir une longueur minimale de 10 caractères (sauf limitation technique) ;
- Comporter au minimum une majuscule, un chiffre et un caractère spécial ;
- Ne pas être vulnérables aux attaques par dictionnaire.

L'utilisation de certificats clients et serveurs pour l'authentification est une alternative préférable aux mots de passe à condition que la clef privée soit protégée dans un matériel adéquat.

➢ Confidentialité et intégrité des flux

Tous les flux d'administration doivent être chiffrés par des procédés fiables (SSH, SSL, Ipsec,etc.), garantissant la confidentialité et l'intégrité des données.

De façon générale, tous les flux contenant des informations sensibles et circulant sur un réseau public doivent être chiffrés par des procédés apportant ces mêmes garanties.

Le choix et le dimensionnement des algorithmes cryptographiques doivent être effectués conformément aux règles et recommandations du RGS en la matière.

Le candidat indiquera l'ensemble des mécanismes et mesures mis en œuvre pour garantir la confidentialité et l'intégrité des flux d'administration.

➢ Contrôle et filtrage des flux

Au titre de la défense en profondeur, trois zones seront mises en place, chacune étant protégée par un dispositif de filtrage :

- une zone publique regroupant les machines qui hébergent des services ayant vocation à communiquer avec l'extérieur (Reverse Proxy, Serveur Web, FTP, Serveur de mail, DNS ,etc.) ;
- une zone privée regroupant les machines n'ayant pas vocation à communiquer avec l'extérieur ;
- un réseau dédié à l'administration des machines et des équipements à partir de postes de travail situés chez l'hébergeur.

Le trafic réseau en provenance et à destination du système doit faire l'objet d'un contrôle permanent afin de n'autoriser que les flux légitimes. Une matrice de flux (inventaire des flux légitimes) sera fournie par le prestataire.

La politique de filtrage est définie à partir de la matrice des flux. Les dispositifs de filtrage sont bloquants par défaut, tout ce qui n'est pas explicitement autorisé étant interdit.

Le service global doit être protégé contre les attaques classiques sur IP et les protocoles associés (filtrage sanitaire) notamment :

- attaque en déni de service (*TCP SYN Flood, Ping Flooding, SMURF, Ping of Death, large packet attacks*, etc.) ;
- IP options (*source routing*, etc.).

Le candidat décrira dans sa réponse les différents mécanismes de protection prévus au niveau des équipements pour contrer les attaques classiques sur IP et les protocoles associés.

Les interfaces d'administration des machines ou des équipements du système ne doivent pas être accessibles depuis l'extérieur. Les services correspondants seront donc configurés pour ne pas accepter de connexions sur les interfaces publiques.

Seuls les services utiles au bon fonctionnement de l'application doivent être activés. Les autres services doivent être désactivés et si possible désinstallés.

➢ Imputabilité, traçabilité

Les informations suivantes devront être enregistrées :

- entrée en session d'un utilisateur : date, heure, identifiant de l'utilisateur et du terminal ; réussite ou échec de la tentative ;
- actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits : date, heure, identité de l'utilisateur, nom de l'objet, type de la tentative d'accès, réussite ou échec de la tentative ;
- création/suppression d'un objet soumis à l'administration des droits : date, heure, identifiant de l'utilisateur, nom de l'objet, type de l'action ;
- actions d'utilisateurs autorisés affectant la sécurité de la cible : date, heure, identité de l'utilisateur, type de l'action, nom de l'objet sur lequel porte l'action.

➢ Marquage des supports de données et équipements sensibles

Préciser les mesures mises en œuvre pour assurer le recensement, la classification et le suivi des supports de données et équipements sensibles (boîtiers de chiffrement, pare-feux, etc.)

Le marquage des supports de stockage de données est obligatoire (disque dur, bandes de sauvegardes, etc.).

- **Personnels en charge des prestations**

Le titulaire s'engage à fournir une liste, régulièrement mise à jour, des personnels autorisés à intervenir sur le système d'information du maître d'ouvrage ainsi que leur niveau d'habilitation (types d'accès et ressources concernées du client).

Le candidat précisera les moyens mis en œuvre, dans le cadre de son processus de recrutement du personnel, pour vérifier les éventuelles condamnations, le cursus et l'expérience professionnelle des futurs employés.

Si le candidat ou des employés de son entreprise possèdent une habilitation au niveau Confidentiel-Défense, il pourra en faire mention.

Le candidat précisera dans son offre si d'autres clients peuvent accéder aux mêmes locaux que ceux utilisés par le maître d'ouvrage et dans quelle mesure il sera possible de limiter ces accès à la demande de ce dernier.

Dans le cadre de plans de sécurité gouvernementaux, le donneur d'ordres pourra imposer un renforcement des contrôles d'accès physiques et logiques à ces équipements.

- **Qualifications et expérience, formations et sensibilisation dans le domaine de la SSI des personnels en charge des prestations**

Le candidat indiquera dans sa réponse :

- les qualifications, diplômes ainsi que le niveau d'expérience des personnels retenus pour la réalisation des prestations d'infogérance ;
- la fréquence et le contenu des actions de formation et de sensibilisation des personnels de l'hébergeur aux enjeux de sécurité.

- **Exigences de sécurité concernant les personnels extérieurs (maintenance, entretien…)**

Le candidat précisera les moyens de contrôle mis en œuvre pour s'assurer du respect des exigences de sécurité du donneur d'ordres par ses sous-traitants éventuels, ainsi que des consultants ou techniciens amenés à intervenir dans le cadre du support et de la maintenance sur le système du client. Cette exigence peut être étendue à tous les types de soutiens (ménage, chauffage, climatisation, etc) si la sensibilité du système le justifie.

- **Continuité des services essentiels : énergie, climatisation et télécommunications**

Une solution de secours doit être mise en œuvre en cas de dysfonctionnement de l'alimentation électrique, de la climatisation ou des moyens de communication.

Le candidat décrira les moyens mis en œuvre afin d'assurer la continuité des services essentiels (énergie, climatisation, télécommunications) sur le site d'exploitation du système :

- situation et caractéristiques générales du site d'exploitation ;
- protection et redondance électriques (groupes électrogènes, onduleurs, protection contre les surtensions, etc.) ;
- contrats de service avec les fournisseurs d'accès, caractéristiques des liaisons de secours ;
- systèmes de climatisation ;
- moyens de supervision et remontées d'alarme ;
- les équipements utilisés par le système du donneur d'ordres, en particulier les composants redondants seront décrits (alimentations, disques, cartes contrôleurs, serveurs, équipements réseau, liens réseau) ;
- Le candidat précisera les éventuels agréments gouvernementaux ou certificats de conformités qu'il détient.

➢ Protection contre les incendies, la foudre et les dégâts des eaux

Le candidat décrira les moyens mis en œuvre en ce qui concerne :

- la prévention, la détection et le traitement des incendies ;
- la protection contre les dégâts des eaux ;
- la protection contre la foudre et les surtensions.

Il sera notamment indiqué dans la réponse si les bâtiments du site d'exploitation se situent ou non en zone inondable.

➢ Surveillance et contrôle des accès aux locaux de l'hébergeur, en particulier au local d'hébergement du système d'information

Le site d'hébergement doit être surveillé 24h/24 et 7j/7.

Le titulaire doit mettre en œuvre un dispositif permettant de réserver l'accès aux locaux hébergeant l'ensemble des machines et postes de travail utilisés aux seules personnes autorisées par le client : filtrage des accès au bâtiment ou aux étages, et filtrage des accès aux salles machines. Il définira les conditions d'accès du client au service (horaires d'ouverture, cas d'indisponibilité ponctuelle, etc.).

Le candidat doit détailler tous les moyens mis en œuvre afin d'assurer la sécurité des locaux d'hébergement, notamment :

- moyens de surveillance, dispositifs anti-intrusion ;
- contrôle et enregistrement des accès (gardiennage, sas, moyen d'identification, etc.) ;
- protection physique des équipements (verrouillage des baies, etc.).

➢ Intervention des sociétés de maintenance ou de support de solutions informatiques (matérielles ou logicielles)

Les intervenants des sociétés assurant la maintenance ou le support technique de solutions doivent être accompagnés par une personne habilitée à intervenir sur le système pendant toute la durée de leur intervention. Si un intervenant a besoin de se connecter au système, il doit utiliser un compte spécifique permettant de garantir l'imputabilité de ses actions.

Le candidat présentera les mesures techniques et organisationnelles pour empêcher les extractions massives d'information (par exemple : extraction d'une copie de la base de données à partir d'un poste dédié à l'administration).

Les supports de stockage de données (disques durs, bandes de sauvegardes, etc.) restent la propriété du client. Ils ne peuvent être mis au rebut ou emportés par une société de maintenance, ou encore réutilisés à d'autres fins que celles prévues initialement sans l'autorisation expresse du donneur d'ordres.

Ils doivent être conservés en lieu sûr par le titulaire, en attendant de procéder à leur effacement ou à leur destruction avec des moyens adaptés visant à s'assurer qu'aucune donnée ne puisse être récupérée. L'effacement ou la destruction ont lieu en présence d'un représentant du donneur d'ordres.

ANNEXE 3 : BONNES PRATIQUES POUR L'HEBERGEMENT MUTUALISE

Outre la réversibilité du contrat d'hébergement, quatre domaines méritent de faire l'objet de prescriptions explicites :

- journaux d'événements et conservation des traces ;
- suivi de la ressource hébergée ;
- prévention d'une attaque ;
- réaction sur incident.

➢ Journaux d'événements et conservation des traces

Le prestataire est tenu de s'assurer qu'une journalisation des accès et des événements (système, Web…) est activée sur tous les équipements dont il a la charge. Une politique de sauvegarde de ces traces doit exister (deux mois de sauvegarde sont demandés sur les pare-feux et les serveurs Web).

Le donneur d'ordres peut être amené à demander un extrait de ces traces, soit dans le cas d'un incident, soit à des fins de suivi de la (des) ressource(s).

Conditions d'accès à ces journaux :

- le client doit pouvoir avoir accès aux journaux d'événements (réduits éventuellement à un extrait) à sa demande et dans les délais contractualisés (ex. : dans la journée). L'idéal est que le client ait un moyen de suivi des événements en temps réel ;
- le client doit, de plus, être sûr que les journaux concernant ses ressources hébergées ne sont pas divulgués à d'autres organismes co-hébergés (garantie de confidentialité) ;
- l'hébergeur doit certifier que toutes les informations présentes sur les journaux sont exploitables au regard de l'état de l'art (pas de biais horaire ou biais horaire maîtrisé et documenté, journaux déportés ou copiés sur une autre machine, etc.).

Dans le cadre de plans de sécurité gouvernementaux, le donneur d'ordres pourra imposer une augmentation de la fréquence des sauvegardes des traces.

➢ Suivi du service hébergé

Outre le contrôle des journaux d'événements, il est nécessaire de pouvoir disposer d'indicateurs sur l'historique du service hébergé. Il est ainsi possible de dégager les principaux événements relatifs à l'utilisation du service, ce qui permet d'avoir accès à

des événements ayant précédé une éventuelle crise. Les indicateurs les plus courants sont (liste non exhaustive) :

- fréquence et suivi des mises à jour effectuées (indispensable) ;
- durée d'indisponibilité maximum et suivi de ces indisponibilités ;
- fréquence des sauvegardes et tests de restauration effectués ;
- indicateurs sur les ressources dont l'accès et la mise à disposition ne dégradent pas la sécurité du système d'information :
  - charge réseau pour le serveur et pour la ressource ;
  - charge processeur utilisée par la ressource et pourcentage de la charge du serveur ;
  - charge mémoire utilisée par la ressource et pourcentage de la charge du serveur ;
  - etc.

De la même manière, il est nécessaire que le client connaisse au préalable l'origine et/ou la teneur des services co-hébergés, ce qui permettra d'étayer son analyse de risques.

Dans le meilleur des cas, il conviendra d'opter pour une solution hybride de co-hébergement. Celle-ci consiste à n'héberger sur un serveur donné qu'un ensemble de ressources, appartenant toutes à la même organisation, ou fruit d'une communauté d'intérêt. Il sera alors plus facile d'obtenir un accord écrit de la communauté sur l'accès à la machine pour analyse en cas d'incident.

Prévention d'une attaque

Le contrat passé avec l'hébergeur doit prévoir le cas d'éventuelles attaques informatiques. La réactivité en cas d'incident étant extrêmement importante, il conviendra de faire figurer dans le contrat les points suivants :

- identification d'un contact technique (ou plusieurs) clairement identifié chez l'hébergeur ainsi que chez le client, joignable 24/24, 7/7, tous les jours de l'année ;
- identification d'un contact décisionnel (ou plusieurs) clairement identifié chez l'hébergeur ainsi que chez le client, joignable 24/24, 7/7, tous les jours de l'année ;
- garantie d'information immédiate : le client doit être tenu informé sans délai en cas d'attaque afin de déclencher le circuit de réaction adéquat ;
- définition des procédures de remontée d'incident ;
- définition claire et exhaustive avec l'hébergeur de ce que l'on entend par incident (défiguration, temps d'indisponibilité, etc.).

Réaction sur incident

En cas d'incident, le client seul doit avoir le contrôle total sur la marche à suivre. Ainsi, le contrat doit prévoir que :

- la désignation de l'organisme chargé de traiter l'incident doit être laissée à la seule appréciation du client ;
- cet organisme doit pouvoir jouir au nom du client d'un contrôle total de l'environnement de la ressource à des fins d'analyse. Par exemple :
  - prélèvement de tout élément nécessaire à l'analyse conformément aux règles de l'art ;
  - analyse du système en fonctionnement.
- la gestion de l'incident et de la conduite des actions postérieures sont à la seule initiative du client. Ceci comprend :
  - toute action sur la machine : redémarrage, arrêt, rétablissement d'une sauvegarde, isolement physique du reste du réseau, établissement d'un périmètre de sécurité, etc. ;
  - délai d'indisponibilité de la ressource ;
  - délai d'indisponibilité du serveur et pénalités d'astreinte éventuelles ;
  - contrôle sur les règles de filtrage.

© Agence nationale de la sécurité des systèmes d'information, 2010.

Ce guide est un document écrit et édité par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Il est soumis aux termes de la licence « information publique librement réutilisable » (LIP V1 2010.04.02), consultable à l'adresse suivante : http://www.rip.justice.fr/information_publique_librement_reutilisable.

L'URL à mentionner pour attribution est http://www.ssi.gouv.fr/externalisation.

Les demandes de permissions supplémentaires peuvent être adressées à communication@ssi.gouv.fr.

Décembre 2010

Licence « information publique librement réutilisable » (LIP V1 2010.04.02)

Agence nationale de la sécurité des systèmes d'information

ANSSI - SGDSN - 51 boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
Sites internet : www.ssi.gouv.fr et www.securite-informatique.gouv.fr
Messagerie : communication [at] ssi.gouv.fr