Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

GUIDE SUR LA DÉFENSE EN PROFONDEUR POUR LES SERVICES FONDÉS SUR L'INFONUAGIQUE

ITSP.50.104

Mai 2020

SÉRIE PRATICIENS

Canada

AVANT-PROPOS

L'ITSP.50.104, *Conseils sur la défense en profondeur pour les services infonuagiques*, est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour de plus amples renseignements ou pour des suggestions de modifications, prière de communiquer avec le Centre d'appel du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) :

Centre d'appel du Centre pour la cybersécurité

contact@cyber.gc.ca

613-949-7048

Numéro sans frais : 1-833-CYBER-88

DATE D'ENTRÉE EN VIGUEUR

Le présent document entre en vigueur le (25/05/2020).

APERÇU

Le paradigme de l'informatique partagée sur lequel repose l'infonuagique permet aux organisations de toutes tailles de se prévaloir d'une large gamme de solutions de technologies de l'information (TI) en évitant un investissement initial coûteux. L'infonuagique se fonde sur un modèle par abonnement axé sur l'auto-approvisionnement en ressources informatiques sur demande, selon un mode libre-service.

Les caractéristiques de l'infonuagique ont une incidence considérable sur les risques, les responsabilités et les rôles liés à la sécurité des TI. Il faut planifier soigneusement les stratégies de sécurité afin d'éviter de porter préjudice aux activités opérationnelles de l'organisation. Avant d'avoir recours à des services infonuagiques, les organisations doivent bien comprendre les répercussions sur les contrôles de sécurité et adapter leur approche de sécurité en fonction des changements relevés dans les divers domaines touchés.

L'infonuagique ne comporte pas de solution simple permettant de protéger les biens opérationnels. Nous recommandons aux organisations d'envisager une approche de mise en œuvre des contrôles de sécurité par couches pour leurs charges de travail infonuagiques. La défense en profondeur est un élément fondamental de la protection contre les risques liés à l'utilisation de l'infonuagique. Le présent document d'orientation sur la sécurité vise à aider les organisations à adapter leur architecture et leurs contrôles de sécurité aux capacités qu'offre l'infonuagique, ainsi qu'à tenir compte des changements qu'entraînera l'adoption de l'infonuagique pour la posture de risque. L'ITSP 50.104 et ses annexes :

- portent sur les responsabilités partagées et définissent les termes de la défense en profondeur;
- décrivent les avantages et les inconvénients de l'adoption de l'infonuagique pour la sécurité;
- présentent les considérations liées à l'architecture et aux contrôles de sécurité en ce qui concerne la mise en œuvre et l'exécution des charges de travail dans les plateformes infonuagiques;
- présentent des recommandations sur chaque domaine de contrôle.

L'ITSP 50.104 fait partie d'une série de documents élaborés par le Centre pour la cybersécurité pour sécuriser les services infonuagiques, à l'appui de l'approche de gestion des risques liés à la sécurité infonuagique établie dans l'ITSM.50.062, *Gestion des risques liés à la sécurité infonuagique*[1][1].

[1] Les chiffres entre crochets renvoient aux références citées dans la section Contenu complémentaire du présent document.

TABLE DES MATIÈRES

LISTE DES FIGURES

1 INTRODUCTION

Les organisations des secteurs public et privé dépendent de plus en plus de la technologie infonuagique pour atteindre leurs objectifs opérationnels. Ces solutions infonuagiques sont l'objet de sérieuses menaces susceptibles de perturber les activités opérationnelles. La compromission des services infonuagiques peut coûter cher et porter atteinte à la disponibilité, à la confidentialité et à l'intégrité des données, des systèmes d'information et des processus opérationnels.

Les contrôles de sécurité représentent des éléments essentiels de la conception et de l'utilisation de services infonuagiques. Bien qu'un grand nombre des contrôles mis en œuvre dans l'infrastructure conventionnelle s'appliquent aussi aux environnements infonuagiques, les organisations doivent bien comprendre les particularités de l'infonuagique et adapter leurs contrôles et leur architecture de sécurité en conséquence. Les organisations peuvent bénéficier de la vaste gamme de capacités et fonctions de sécurité qu'offrent les plateformes infonuagiques modernes si elles les utilisent efficacement. Toutefois, si les contrôles de sécurité sont déployés sans tenir compte des capacités, des responsabilités partagées et des risques, les charges de travail infonuagiques sont susceptibles d'être moins sécurisées que dans l'informatique conventionnelle.

L'ITSP.50.104 aidera les organisations à adapter leur architecture et leurs contrôles de sécurité pour réduire les risques liés à l'adoption du nuage.

1.1 POLITIQUES DÉTERMINANTES

La défense en profondeur permet de protéger efficacement les services infonuagiques contre les cybermenaces et les vulnérabilités. La nécessité d'avoir recours à la défense en profondeur est généralement déterminée en fonction des politiques, des directives, des règles, des normes et des lignes directrices applicables à chaque organisation. Les organisations peuvent consulter les documents de référence ci-dessous au moment de créer leur architecture de sécurité infonuagique et d'établir leurs contrôles de sécurité :

- ITSP.50.103 du Centre pour la cybersécurité, *Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique* [2][2];
- National Institute of Standards and Technology (NIST), *Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing* [3];
- NIST, *Special Publication 500-292, Cloud Computing Reference Architecture* [4];
- Cloud Security Alliance (CSA), *Security Guidance for Critical Areas of Focus in Cloud Computing*, version 4.0 [5].

[2] Des profils de contrôle de sécurité ont été établis pour les services fondés sur l'infonuagique selon les profils de base présentés à l'annexe 4 de l'ITSG-33 du Centre pour la cybersécurité, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* [6]. Les profils de contrôles de la sécurité infonuagique sont présentés dans l'annexe de l'ITSP 50.103[2] du Centre pour la cybersécurité, *Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique*.

1.2 ENVIRONNEMENTS CONCERNÉS

L'information contenue dans le présent guide s'applique aux organisations des secteurs public et privé. Les conseils peuvent être appliqués à tous les services infonuagiques, quels que soient le modèle de déploiement et le modèle de service.

1.3 RAPPORT AVEC LA GESTION DES RISQUES LIÉS À L'INFONUAGIQUE

L'ITSG-33 du Centre pour la cybersécurité [6] propose un ensemble d'activités pour chacun des deux niveaux organisationnels suivants : niveau de l'organisation et niveau du système d'information.

Comme l'indique la figure 1, les activités associées au niveau de l'organisation sont intégrées au programme de sécurité de l'organisation pour planifier, évaluer et améliorer la gestion des risques liés à la sécurité des TI. À ce niveau, la défense en profondeur appuie la gestion des risques organisationnels en définissant les approches de sécurité pour les profils de contrôle de sécurité.

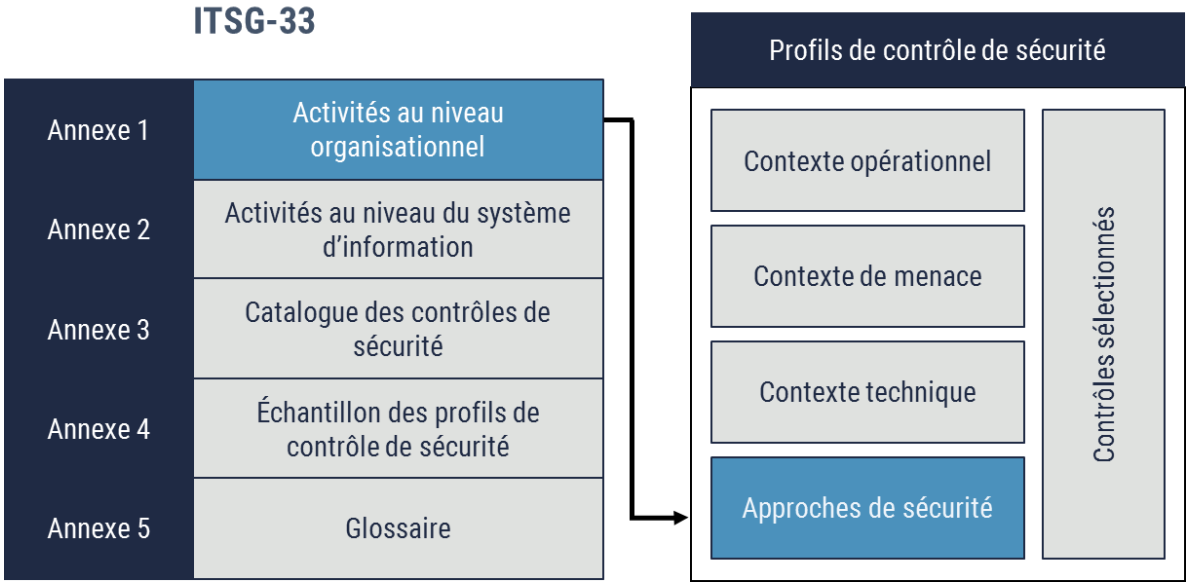

Figure 1 – Rapport entre la défense en profondeur et la gestion des risques de l'organisation

Les activités associées au niveau des systèmes d'information sont intégrées au cycle de développement des systèmes (CDS). Ces activités comprennent l'ingénierie de sécurité, l'évaluation des menaces et des risques, l'évaluation de la sécurité et l'autorisation des systèmes d'information. L'approche de gestion des risques liés à la sécurité infonuagique du Centre pour la cybersécurité s'aligne sur les activités du niveau des systèmes d'information. Comme l'indique la figure 2, la défense en profondeur appuie la cinquième étape de l'approche de gestion des risques liés à la sécurité infonuagique. Elle comporte une approche par couches sur laquelle les fournisseurs de services infonuagiques (FSI) et les organisations peuvent s'appuyer pour établir et mettre en œuvre les contrôles de la sécurité infonuagique.

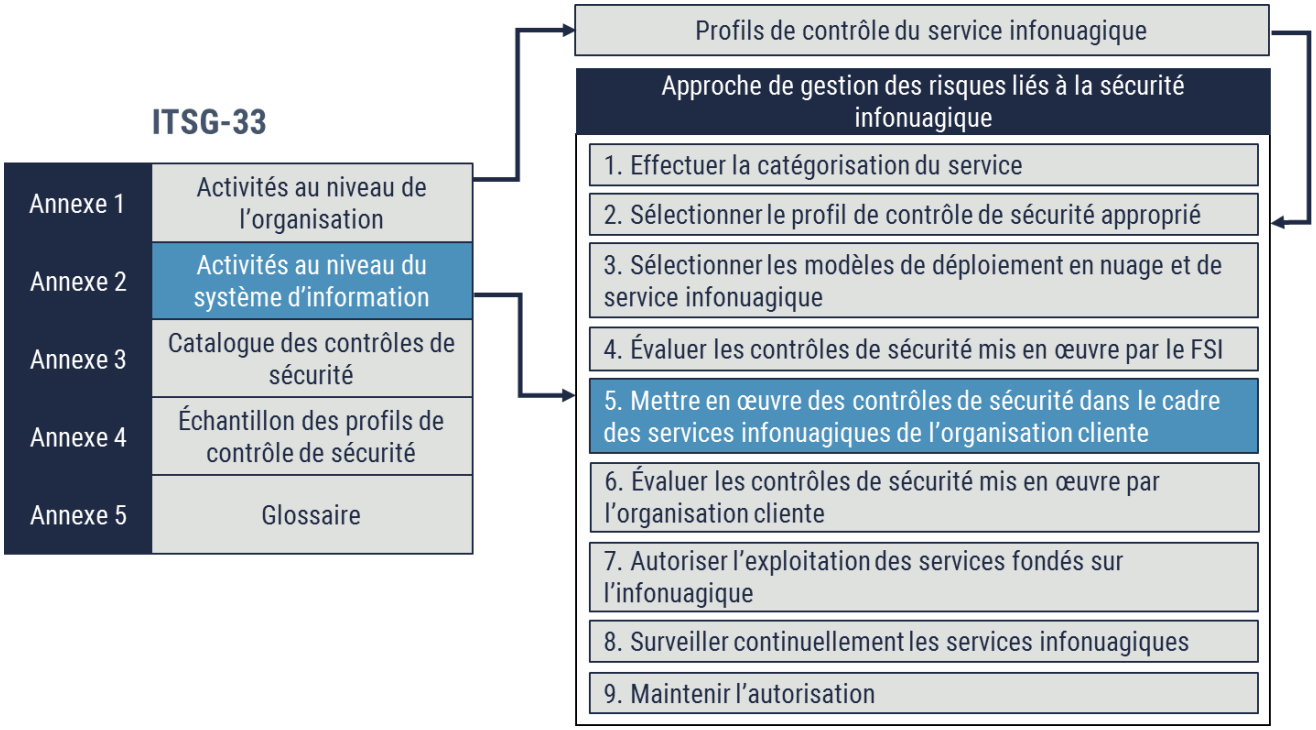

Figure 2 –Rapport entre la défense en profondeur et les activités associées au niveau des systèmes d'information et l'approche de gestion des risques liés à la sécurité infonuagique

2 CONTEXTE

Le présent guide sur la défense en profondeur pour les services fondés sur l'infonuagique tient compte principalement des orientations suivantes en matière d'infonuagique et de gestion des risques liés à la sécurité des systèmes d'information :

- National Institute of Standards and Technology (NIST), *Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing* [3];
- Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing*, version 4.0 [5].

2.1 QU'EST-CE QUE LA DÉFENSE EN PROFONDEUR POUR L'INFONUAGIQUE?

Les profils des contrôles de la sécurité infonuagique créés par le Centre pour la cybersécurité définissent la défense en profondeur comme étant l'intégration stratégique de mesures de protection (procédures, mesures techniques, ou les deux) dans l'architecture de sécurité, de manière à ce que les adversaires doivent contourner de multiples mesures de protection pour atteindre leur objectif[3].

Avant d'appliquer les principes de défense en profondeur à l'infonuagique, les organisations doivent comprendre le rapport entre les contrôles de sécurité recommandés et les menaces, les vulnérabilités, les responsabilités partagées et les capacités des plateformes infonuagiques. Elles seront ainsi mieux en mesure de protéger la confidentialité, l'intégrité et la disponibilité des activités opérationnelles soutenues par des services infonuagiques.

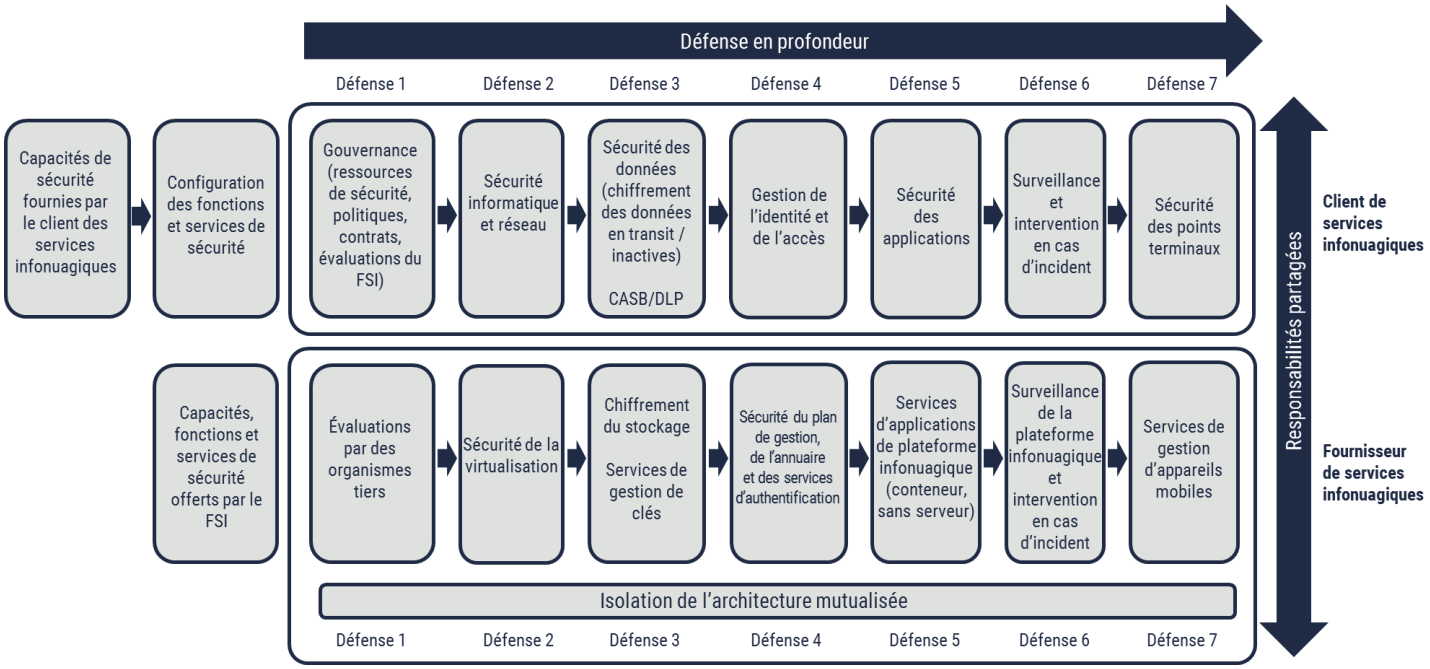

Figure 3 – Concept de la défense en profondeur pour l'infonuagique

[3] ITSP.50.103 [2], *Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique*, PL-8(1) – Architecture de la sécurité de l'information – Défense en profondeur

2.2 MODÈLES DE DÉPLOIEMENT EN NUAGE

Avant d'adopter des services infonuagiques, nous recommandons aux organisations de déterminer le modèle de déploiement en nuage et de service infonuagique qui convient à leurs services TI. Le présent guide reprend les définitions détaillées de concepts de l'infonuagique établies dans la publication spéciale 800-145 du NIST [7]. Les modèles de déploiement décrivent le rapport entre le fournisseur de services infonuagiques et le client.

La figure 4 présente les quatre modèles de déploiement en nuage établis par le NIST : public, privé, communautaire et hybride. Avant de choisir un modèle de déploiement en nuage, nous recommandons aux organisations de tenir compte de certains facteurs, notamment la souplesse, la sécurité, l'extensibilité, le coût, l'automatisation, le niveau de contrôle de l'infrastructure, la localisation et les niveaux de service offerts par chaque modèle de déploiement[4]. « Sur site » fait référence au matériel informatique, aux logiciels et à toutes autres technologies de l'information installés à l'intérieur des limites physiques de votre organisation. « Hors site » fait référence au matériel informatique, aux logiciels et à toutes autres technologies de l'information installés en dehors des limites physiques de votre organisation. Les considérations liées à la sélection d'un modèle de déploiement en nuage sont présentées dans l'ITSP 50.103.[2]

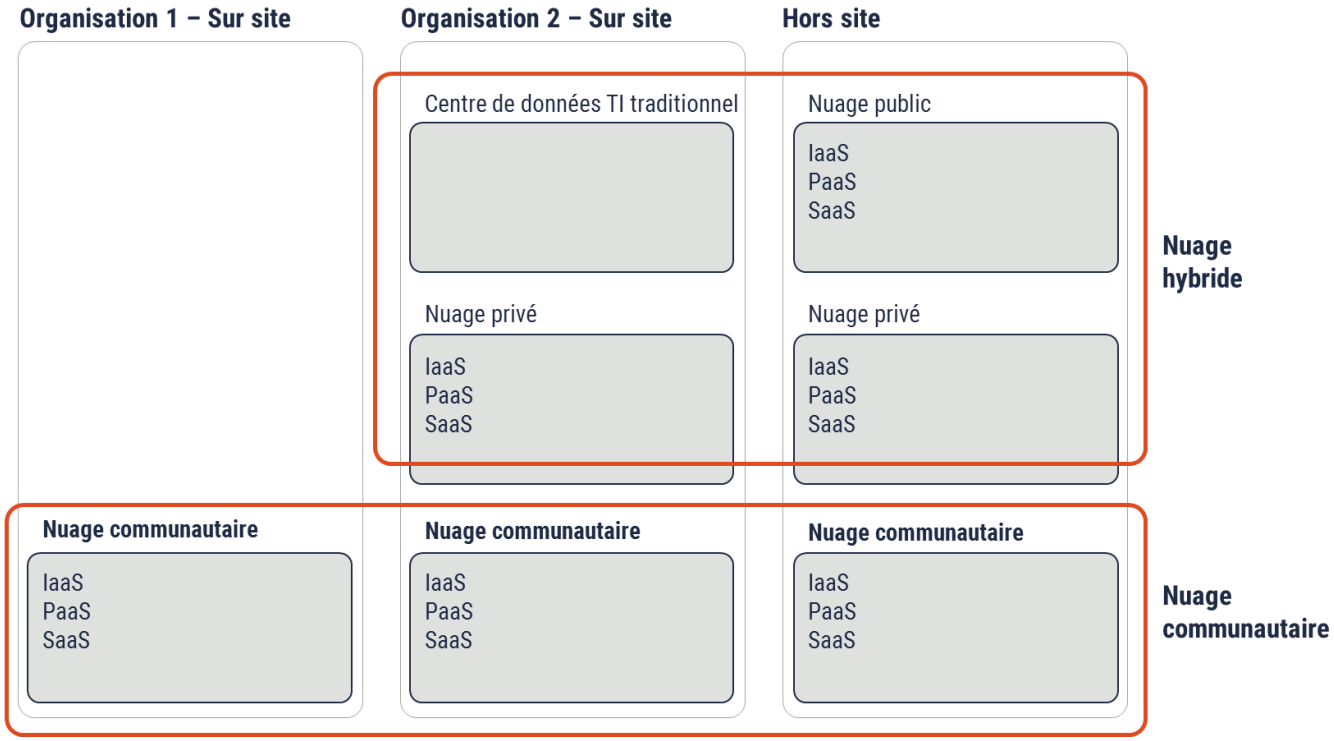

Figure 4 – Modèles de déploiement en nuage

2.2.1 MODÈLE DE DÉPLOIEMENT EN NUAGE PUBLIC

Dans le modèle de déploiement en nuage public, l'infrastructure infonuagique est ouverte à tous. Le nuage peut appartenir à une entreprise, à un établissement scolaire ou à un organisme gouvernemental, ou encore à un regroupement de ces

[4] Cloud Standard Customer Council, *Practical Guide to Hybrid Computing* [8].

intervenants. Le ou les propriétaires se chargent de la gestion et de l'exploitation du nuage, lequel est hébergé dans les installations du fournisseur de services infonuagiques.

2.2.2 MODÈLE DE DÉPLOIEMENT EN NUAGE PRIVÉ

Dans le modèle de déploiement en nuage privé, l'infrastructure infonuagique est mise en place aux fins d'utilisation exclusive par une seule organisation formée de plusieurs clients (p. ex. unités opérationnelles). Le nuage peut appartenir à une organisation, à un tiers, ou aux deux. Le ou les propriétaires se chargent de gérer et d'exploiter le nuage, lequel peut être hébergé localement ou à distance.

2.2.3 MODÈLE DE DÉPLOIEMENT EN NUAGE HYBRIDE

Selon la définition du NIST, le modèle hybride est un environnement composé d'au moins deux infrastructures infonuagiques distinctes (nuage privé, communautaire ou public) qui demeurent des entités uniques, tout en étant liées par une technologie normalisée ou propriétaire permettant la portabilité des données et des applications. Lorsque l'infrastructure TI locale est combinée à un ou plusieurs nuages publics, privés ou communautaires, il s'agit d'un nuage hybride.

2.2.4 MODÈLE DE DÉPLOIEMENT EN NUAGE COMMUNAUTAIRE

Un nuage communautaire est mis en place aux fins d'utilisation exclusive par une communauté particulière de clients provenant d'organismes partageant des enjeux communs (p. ex. mission, exigences de sécurité, politiques, considérations liées à la conformité). Une ou plusieurs organisations de la communauté ou une tierce partie, ou une combinaison de ces intervenants, peuvent être propriétaire du nuage, le gérer et l'exploiter, et ce nuage peut être mis en place localement ou à distance. Comme les coûts sont répartis parmi moins d'utilisateurs qu'un nuage public (mais plus qu'un nuage privé), les utilisateurs ne bénéficient pas de toutes les économies possibles de l'infonuagique.

2.3 MODÈLES DE SERVICE INFONUAGIQUE

Le NIST définit trois modèles de service :

- Le **logiciel en tant que service (SaaS pour *Software as a Service*)** permet au client d'utiliser les applications du fournisseur qui sont exécutées dans une infrastructure en nuage. Ces applications sont accessibles à partir de divers dispositifs clients par l'intermédiaire d'une interface client léger comme un navigateur Web (p. ex. services de courrier Web) ou d'une interface de programmation;
- La **plateforme en tant que service (PaaS pour *Platform as a Service*)** permet au client de déployer sur son infrastructure infonuagique des applications qu'il a acquises ou créées à l'aide de langages, de bibliothèques, de services et d'outils de programmation pris en charge par le fournisseur;
- L'**infrastructure en tant que service (IaaS pour *Infrastructure as a Service*)** offre au client le traitement, le stockage, les réseaux ainsi que d'autres ressources informatiques fondamentales, grâce auxquels le client peut déployer et exécuter des logiciels arbitraires, y compris des systèmes d'exploitation et des applications.

2.4 SERVICES GÉRÉS PAR RAPPORT AUX SERVICES INFONUAGIQUES

Il importe de comprendre ce qui distingue les contrôles et les responsabilités partagées des services gérés de ceux des services infonuagiques.

Les services gérés permettent aux organisations de se consacrer à leurs activités principales avec peu de personnel et d'expertise en TI, tout en sachant que leur infrastructure TI est bien gérée. Dans les services gérés conventionnels, les organisations se procurent l'équipement, les logiciels et tout autre composant de l'infrastructure; elles en sont propriétaires et les contrôlent entièrement. Le fournisseur de services gérés (FSG) se charge d'effectuer les tâches que le personnel de TI de l'organisation ferait normalement (p. ex., externalisation de la sauvegarde et de la récupération des données, de la surveillance et de la gestion des systèmes, et de la gestion des correctifs). L'exécution des activités externalisées coûte généralement moins cher et des frais mensuels s'appliquent à chaque service pris en charge.

En ayant recours à des services infonuagiques, les organisations n'ont pas à investir dans l'équipement TI et des logiciels. Elles utilisent plutôt des services sur demande et payent chaque service infonuagique à l'utilisation. Or, les organisations auront tout de même la responsabilité de configurer, de gérer et d'exploiter en toute sécurité les services infonuagiques en fonction du modèle de service qu'elles auront choisi. Comme dans le cas d'une infrastructure TI conventionnelle, si les organisations n'ont pas le personnel ou l'expertise nécessaire pour acheter, déployer, sécuriser et gérer leurs services infonuagiques, elles peuvent décider d'impartir ces responsabilités à un fournisseur de services gérés.

2.5 RESPONSABILITÉS PARTAGÉES ET DÉFENSE EN PROFONDEUR

Il est essentiel de bien comprendre l'effet des différents modèles de services infonuagiques sur la défense en profondeur. Les organisations ne doivent pas supposer qu'elles peuvent attribuer aux FSI la majorité des responsabilités liées à la protection de la vie privée, à la sécurité et à la conformité. Elles doivent comprendre le rôle qu'elles jouent dans le maintien de la sécurité des services opérationnels fondés sur l'infonuagique. La figure 5 présente le partage des responsabilités entre les organisations clientes de services infonuagiques et les FSI.

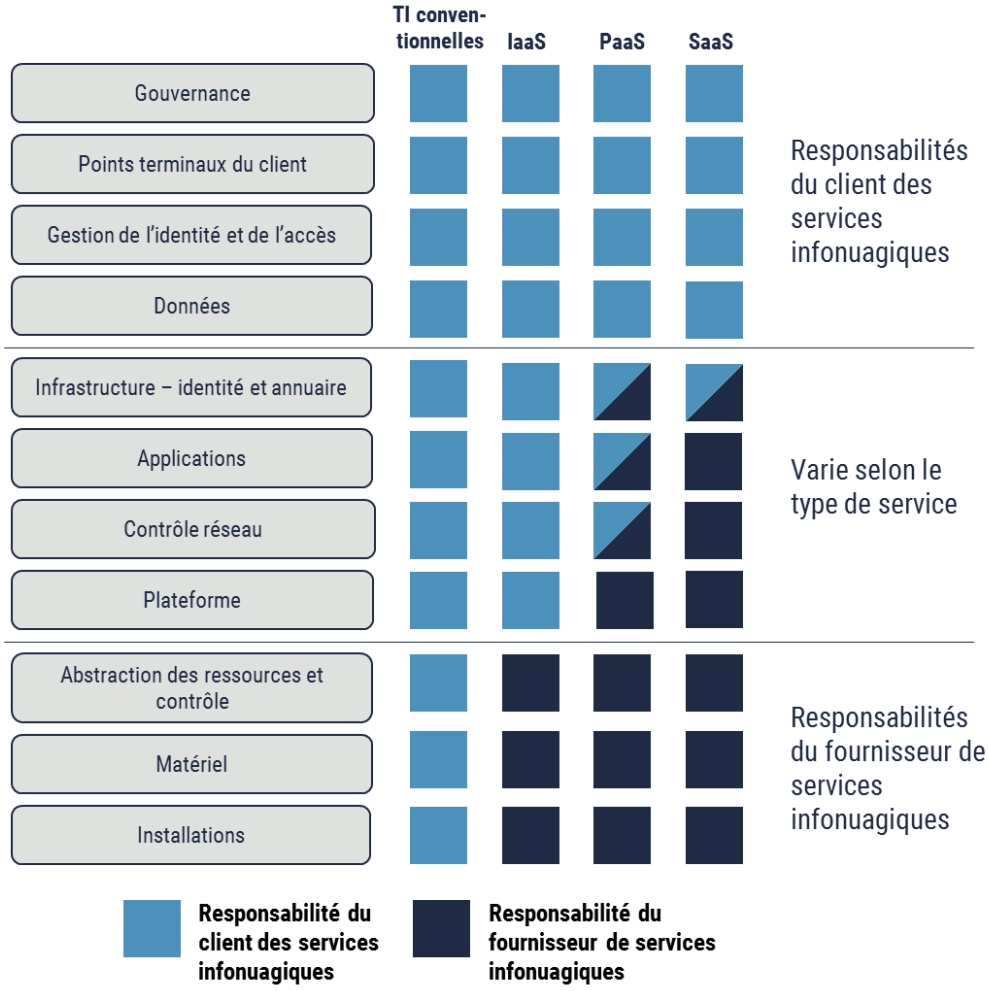

Figure 5 – Responsabilités partagées et défense en profondeur

Comme l'indique la figure 5, au moment d'établir l'architecture de défense en profondeur, nous recommandons aux organisations de tenir compte des contrôles de sécurité gérés par le FSI et des contrôles gérés par le client.

Les contrôles de sécurité gérés par le FSI assurent la sécurité **du nuage** et protègent les produits SaaS, PaaS et IaaS qu'il offre. Ces contrôles permettent d'assurer :

- l'isolation et la virtualisation de l'infrastructure infonuagique;

- la sécurité du plan de gestion;
- les portails libre-service et interfaces de programmation d'applications (API pour *Application Program Interface*);
- les mécanismes qui protègent le nuage contre les menaces physiques et réseau.

Les FSI sont également responsables de la prestation de capacités de sécurité clés aux organisations, notamment :

- le chiffrement des données inactives;
- la gestion de l'identité et de l'accès;
- la gestion sécurisée des clés;
- l'authentification multifactorielle.

Les organisations sont responsables des contrôles de sécurité gérés qui assurent la sécurité **dans le nuage**. Voici des exemples de contrôles de sécurité qui protègent les charges de travail infonuagiques :

- les passerelles d'applications Web;
- les groupes de sécurité réseau;
- les groupes de disponibilité;
- le chiffrement du stockage et la segmentation en unités;
- les appliances de sécurité réseau;
- le renforcement des mesures de sécurité de base;
- la configuration de fonctions et de capacités de sécurité clés fournies par le FSI.

Les responsabilités en matière de gestion revenant au FSI et au client varient selon le modèle de service infonuagique choisi.

3 AVANTAGES ET INCONVÉNIENTS DE L'INFONUAGIQUE

3.1 AVANTAGES POSSIBLES

Bien que votre organisme doive céder le contrôle direct d'une partie de son infrastructure TI en passant au nuage, il peut également en tirer certains avantages sur le plan de la sécurité. En voici quelques-uns[5] :

- **Spécialisation du personnel de sécurité :** Les petites et moyennes organisations ne possèdent pas nécessairement les ressources voulues pour développer de l'expertise sur tous les aspects de la sécurité et mettre en œuvre une multitude de solutions de sécurité. Les FSI ont la motivation et les ressources nécessaires pour établir des équipes de sécurité d'expérience et mettre en œuvre des solutions de sécurité avancées afin de protéger l'infrastructure infonuagique et les services qu'ils fournissent.
- **Riche écosystème de capacités de sécurité :** En règle générale, les FSI développent et offrent une vaste gamme de capacités de sécurité, y compris le chiffrement, les groupes à haute disponibilité et l'authentification multifactorielle. Les capacités avancées peuvent inclure la détection avancée des menaces, la surveillance de la sécurité et de la conformité, ainsi que la génération de rapports.
- **Réduction des tâches manuelles :** Les plateformes infonuagiques modernes offrent de nombreux outils d'automatisation, modèles et langages de script permettant d'appliquer la configuration de sécurité de base et de générer des rapports à ce sujet. Ces outils réduisent les erreurs de configuration ainsi que le niveau d'effort nécessaire pour appliquer la conformité.
- **Souplesse :** Les services infonuagiques simplifient le déploiement de capacités de sécurité dans de multiples centres de données du FSI ou dans diverses régions, et ce déploiement peut être effectué sur demande dans de multiples emplacements. De plus, il est beaucoup plus simple de mettre en œuvre des environnements temporaires pour faire l'essai de nouvelles capacités de sécurité.
- **Force de la plateforme :** L'uniformité de l'infrastructure infonuagique facilite le déploiement et l'automatisation des contrôles de sécurité, ce qui simplifie le renforcement de la sécurité de base, la gestion des vulnérabilités et de la sécurité, ainsi que l'intervention en cas d'incident. En outre, les FSI doivent recevoir une certification officielle d'un tiers indépendant qui confirme qu'ils respectent les divers règlements de l'industrie[6].
- **Disponibilité des ressources :** Le nuage public offre une très grande extensibilité, ce qui permet aux organisations de répondre aux périodes de demande élevée et d'intervenir en cas d'attaques par déni de service distribué. Les FSI offrent divers services de haute disponibilité à leurs clients, notamment la capacité de répartir les charges de travail infonuagiques parmi de multiples centres de données et hôtes de virtualisation afin de protéger les charges de travail contre toute défaillance de l'infrastructure. Les services des FSI permettent également de réduire

[5] Pour obtenir une description plus détaillée des avantages pour la sécurité, prière de consulter le document du NIST intitulé *Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing* [2].

[6] Règlements de l'industrie comme les normes de sécurité sur les données de l'industrie des cartes de paiement (PCI DSS pour *Payment Card Industry Data Security Standard*), le Service Organization Control (SOC) 1 et 2, la *Health Insurance Portability and Accountability Act* (HIPAA), et les normes de l'Organisation internationale de normalisation (ISO 27001, 27017, et 27018).

l'interruption des charges de travail des clients du nuage pendant les périodes de maintenance de l'infrastructure infonuagique.

- **Sauvegarde et récupération :** Les environnements infonuagiques modernes fournissent généralement des capacités de stockage, de sauvegarde et de récupération qui excèdent celles des organisations. Les plateformes infonuagiques offrent diverses fonctions de résilience et de réplication des données que les organisations peuvent configurer afin d'assurer la géoredondance des données et des copies de sauvegarde. Grâce aux capacités de sauvegarde et de récupération des FSI, les organisations pourraient également récupérer les données plus rapidement en cas d'incident.

3.2 INCONVÉNIENTS POSSIBLES

Bien que l'infonuagique comporte de nombreux avantages sur le plan de la sécurité, certains inconvénients se présentent :

- **Complexité :** Les environnements infonuagiques sont beaucoup plus complexes que les environnements informatiques conventionnels. Les FSI ont recours à un certain nombre de technologies complexes afin de procéder à l'isolation et à la virtualisation de l'infrastructure infonuagique, du plan de gestion et des interfaces libre-service nécessaires pour l'interaction avec les organisations. De plus, les FSI offrent d'importantes fonctions de sécurité, des outils et des mesures de protection des charges de travail.
  - En raison d'un manque possible de connaissances et d'expérience liées aux nouvelles fonctions de sécurité, les organisations risquent de mal configurer la plateforme infonuagique. Nous recommandons aux organisations d'investir des ressources dans le développement des compétences de leur personnel des TI et de la sécurité en ce qui a trait à la sécurité infonuagique. Les organisations doivent également s'assurer de bien comprendre les éléments qui relèvent de leur responsabilité et ceux qui reviennent aux FSI.
- **Dépendance :** En ayant recours aux fonctions de sécurité clés d'un FSI, les organisations risquent de rester « captives » des services de sécurité du FSI et d'avoir de la difficulté à passer aux services d'un FSI différent.
- **Architecture mutualisée :** En règle générale, dans les modèles d'architecture mutualisée (multilocataire), les ressources informatiques, les réseaux et le stockage sont partagés. Toute défaillance ou erreur de configuration dans la virtualisation ou l'isolation de l'infrastructure du FSI risque d'avoir des répercussions sur la confidentialité, l'intégrité et la disponibilité des charges de travail et des données des organisations.
- **Services connectés à Internet :** En raison de l'accès réseau élargi du nuage, les services sont toujours exposés à des menaces provenant d'Internet. De plus, toute défaillance de la connectivité Internet locale risque d'empêcher les organisations d'accéder aux services opérationnels déployés dans l'infrastructure infonuagique. Nous recommandons aux organisations d'envisager la mise en œuvre de la connectivité spécialisée pour réduire le risque de défaillance ou de dégradation de la performance de la connexion Internet.
- **Perte de contrôle et de visibilité :** Les clients de services infonuagiques ont une visibilité et un contrôle limités des composants du nuage qui relèvent de la responsabilité du FSI. Or, il pourrait être important de voir et de contrôler les éléments où l'organisation et le FSI se partagent les responsabilités, ainsi que dans certains scénarios de conformité (p. ex. la surveillance de la sécurité et l'intervention en cas d'incident). Nous recommandons aux organisations de bien comprendre les responsabilités qu'elles partagent avec leur FSI. Les accords sur les niveaux

de service (ANS), les contrats et les évaluations des FSI par des organismes tiers peuvent permettre de régler les préoccupations soulevées.

- **Conformité :** Nous recommandons aux organisations de s'assurer de bien comprendre leurs obligations en vertu des lois canadiennes de protection de la vie privée visant le secteur privé, y compris celles découlant de certaines lois provinciales en la matière. De plus, elles doivent évaluer minutieusement les risques par rapport aux avantages[7]. À moins que les organisations ne fassent affaire avec un FSI canadien à part entière, elles devraient également tenir compte des règlements internationaux, notamment le *Règlement général sur la protection des données 2016/679* de l'Union européenne et la *Cloud Act* des États-Unis.

[7] Commissariat à la protection de la vie privée du Canada, *L'infonuagique pour les petites et moyennes entreprises* [9].

4 CONSIDÉRATIONS LIÉES À LA DÉFENSE EN PROFONDEUR EN INFONUAGIQUE

4.1 ISOLATION

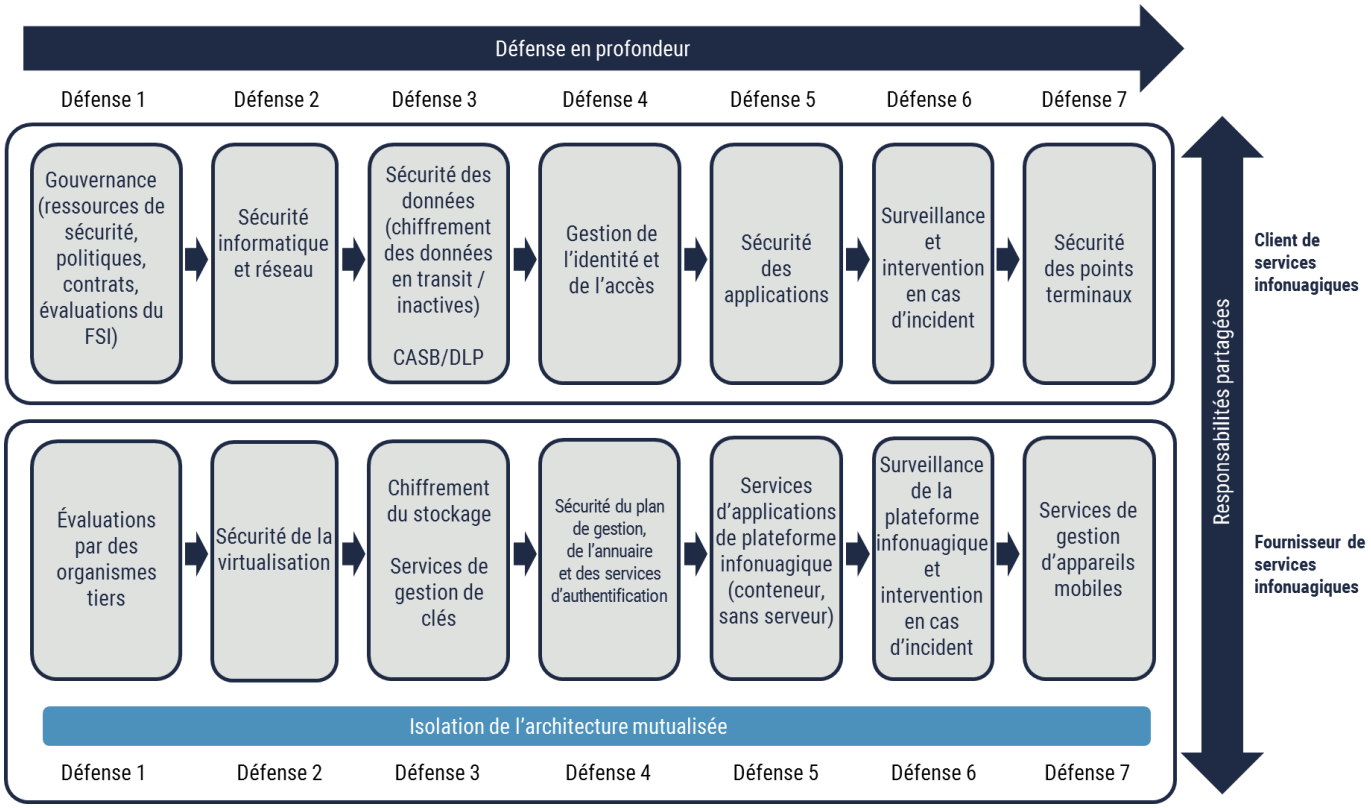

Figure 6 – Isolation de l'architecture mutualisée

Les infrastructures infonuagiques partent du principe que le partage de ressources entre de multiples clients entraîne des économies d'échelle, ce qui se traduit par des coûts moins élevés pour les organisations. C'est ce qu'on appelle une architecture mutualisée (voir la figure 6). Dans un environnement mutualisé, il faut absolument que les locataires soient isolés les uns des autres pour éviter qu'une éventuelle compromission de la sécurité d'un locataire se répercute sur la confidentialité, la disponibilité et l'intégrité des charges de travail et des données des autres locataires.

Bien qu'il revienne aux FSI d'assurer l'isolation des ressources attribuées à chaque locataire, il importe que les organisations comprennent les moyens employés par le FSI pour isoler les différents locataires ainsi que le niveau d'isolation offert pour chacun de ses services infonuagiques. Les organisations seront ainsi en mesure de choisir les services infonuagiques appropriés pour obtenir le niveau d'isolation et de sécurité voulu. Par exemple, les FSI offrent souvent des services infonuagiques dédiés ou partagés. Les services dédiés permettent d'accroître le niveau d'isolation. Les organisations pourraient choisir un service infonuagique fourni en tant qu'instance dédiée dans leur propre réseau virtuel à l'aide d'une adresse privée, contrairement à un service fourni dans le cadre de ressources partagées accessibles par des adresses publiques.

Dans le cas d'un grand nombre des fonctions de sécurité offertes par les fournisseurs de services infonuagiques, les organisations devraient trouver des moyens d'accroître l'isolation entre elles et leur FSI, ainsi qu'entre elles et les environnements des autres clients. Par exemple, nous recommandons aux organisations de déployer le chiffrement du stockage, d'avoir recours à des modules de sécurité matériels (HSM pour *Hardware Security Module*) pour protéger les clés et les secrets, et de se procurer des instances dédiées de machines virtuelles (VM pour *Virtual Machine*).

4.2 GOUVERNANCE ET GESTION DES RISQUES POUR LA SÉCURITÉ INFONUAGIQUE

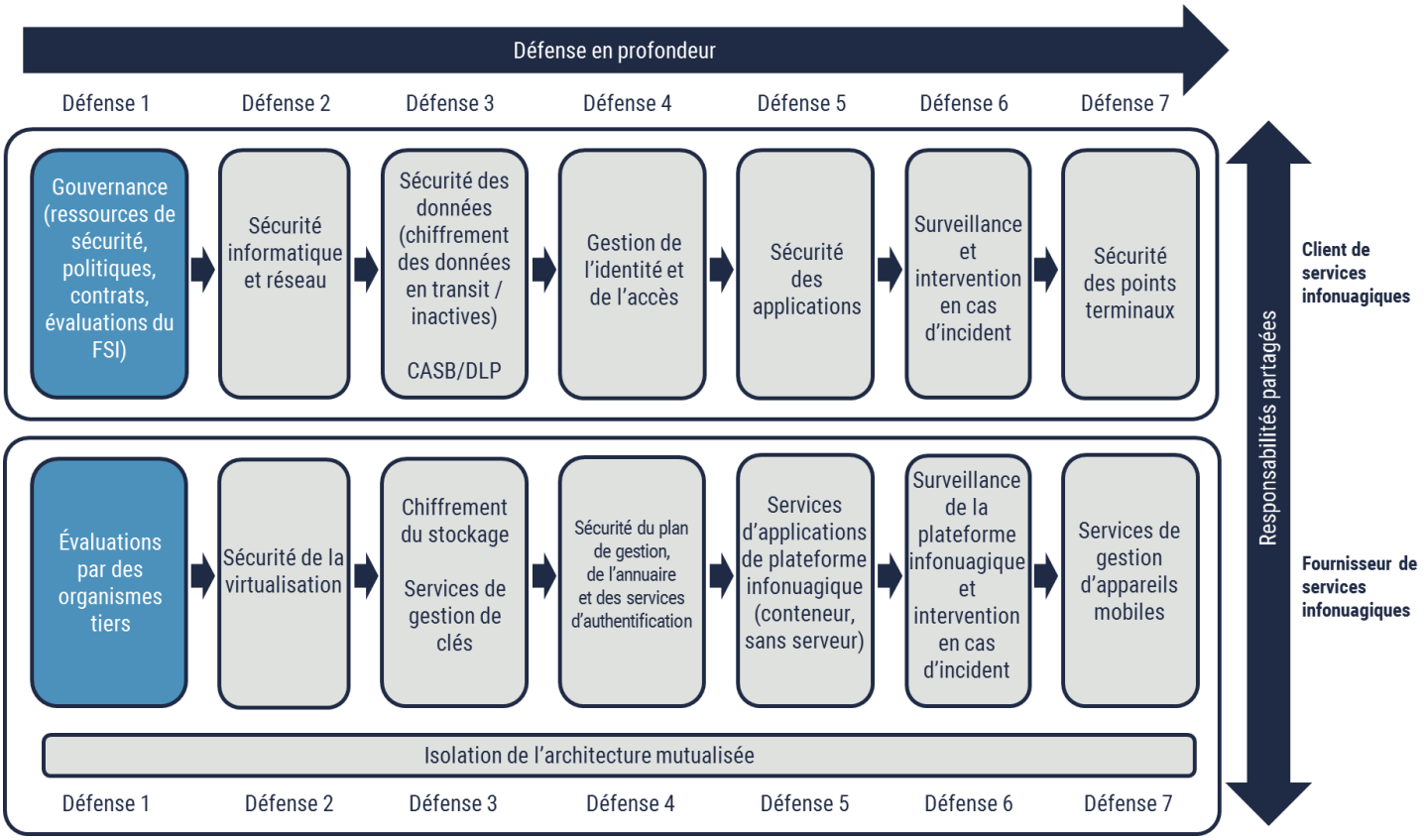

Figure 7 – Gouvernance et gestion des risques pour la sécurité infonuagique

Comme on l'a vu dans les sections précédentes, l'infonuagique comporte de nombreux avantages possibles sur le plan de la sécurité de même qu'un certain nombre d'inconvénients. Dans l'infonuagique, les organisations ne voient pas la technologie et les politiques et procédures connexes des FSI, et elles n'exercent aucun contrôle sur ces éléments. Les organisations ne possèdent peut-être pas l'expertise nécessaire pour déployer en toute sécurité les charges de travail infonuagiques. En l'absence des politiques, des processus et des normes nécessaires pour mener leurs activités dans le nuage, les organisations sont susceptibles d'exposer leurs biens opérationnels à des risques accrus.

La défense en profondeur se fonde sur la gouvernance et la gestion des risques liés à la sécurité infonuagique. Ces deux éléments régissent les aspects juridiques et la conformité pour la transition vers le nuage, établissent clairement les rôles et responsabilités et fournissent les principes directeurs de la protection des données et des processus opérationnels contre les auteurs de menace. Les responsabilités en matière de gouvernance reviennent toujours aux organisations, notamment :

- l'attribution de ressources de sécurité;
- l'établissement de politiques et de lignes directrices;
- les évaluations officielles par des organismes tiers;
- les contrats de service infonuagique.

4.2.1 ATTRIBUTION DE RESSOURCES DE SÉCURITÉ

Nous recommandons aux organisations d'attribuer des ressources de sécurité suffisantes au moment d'adopter l'infonuagique. Elles devraient envisager de désigner un responsable de l'infonuagique pour diriger des équipes de base[8] chargées des divers aspects de la transformation (p. ex. sécurité infonuagique et processus de gestion des risques, approvisionnement, licences, rôles et responsabilités). La haute direction devra communiquer son soutien pour l'infonuagique et encourager les employés à développer leurs compétences en sécurité infonuagique par l'intermédiaire de formations et d'expérience en milieu de travail (incluant, si possible, un processus d'évaluation et de validation des compétences acquises).

4.2.2 ÉTABLISSEMENT DE POLITIQUES ET DE LIGNES DIRECTRICES

Les organisations supposent peut-être que leurs politiques actuelles protègent déjà adéquatement les données et les services opérationnels déployés dans des environnements infonuagiques. Or, lorsque les organisations adoptent l'infonuagique, il importe qu'elles élaborent ou mettent à jour des politiques et des lignes directrices sur la sécurité.

En raison de la nature de l'infonuagique, les organisations devront peut-être adapter leurs politiques de sécurité pour suivre le rythme de l'évolution technologique. Il conviendra de revoir notamment les éléments ci-dessous :

- l'utilisation acceptable de l'infonuagique;
- les modèles de déploiement en nuage et de service infonuagique acceptables;
- les rôles et responsabilités;
- la résidence des données;
- les exigences liées aux évaluations par des organismes tiers;
- les exigences contractuelles;
- l'intégration au processus de gestion de l'identité;
- la connectivité avec les fournisseurs de services externes;
- le chiffrement et la gestion des clés;
- la sauvegarde des données;
- la mise hors service des services.

[8] Secrétariat du Conseil du Trésor du Canada, *Approche et procédures de gestion des risques à la sécurité de l'informatique en nuage* [10]

4.2.3 ÉVALUATIONS OFFICIELLES PAR DES ORGANISMES TIERS

Comme l'indique l'ITSM.50.062[1], *Gestion des risques liés à la sécurité infonuagique*, les organisations ne contrôlent pas ou ne voient pas toujours la conception, l'installation et l'évaluation des contrôles de sécurité du FSI. Nous recommandons d'adopter une autre approche d'évaluation de la sécurité, notamment en faisant appel à d'autres évaluations de la sécurité fiables. Les résultats de ces évaluations, s'ils sont fiables et applicables, peuvent être intégrés aux évaluations de la sécurité des organisations.

Dans le contexte de l'approche de gestion des risques liés à la sécurité infonuagique, ces évaluations de la sécurité fiables consistent principalement en des attestations de tierces parties qui sont beaucoup plus valables que les autoévaluations. Les évaluations par des organismes tiers portent souvent sur divers règlements et diverses exigences de l'industrie[9].

Ces attestations doivent être accordées par un organisme tiers indépendant qui est tenu d'être objectif et d'appliquer les normes professionnelles aux pièces justificatives qu'il examine et produit. Cependant, les attestations d'organismes tiers ne couvrent généralement pas toutes les exigences de sécurité indiquées dans le profil de contrôle de sécurité sélectionné. Les exigences de sécurité et des clauses contractuelles supplémentaires pourraient être requises pour veiller à ce que le FSI fournisse les pièces justificatives nécessaires aux activités d'évaluation de la sécurité.

Souvent, les organisations devront signer une entente de non-divulgation pour obtenir les attestations officielles d'organismes tiers. Comme il s'agit d'une évaluation ponctuelle des contrôles de sécurité et des services infonuagiques particuliers du fournisseur, il importe que les organisations surveillent la situation pour relever tout changement dans la portée, l'état et les constatations au fil du temps.

Pour obtenir de plus amples renseignements sur les évaluations par des organismes tiers, prière de consulter l'ITSM.50.100 du Centre pour la cybersécurité, *Programme d'évaluation de la sécurité des technologies de l'information s'appliquant aux fournisseurs de services infonuagiques*.[11]

4.2.4 CONTRATS DE SERVICE INFONUAGIQUE

En infonuagique, les organisations dépendent davantage des contrats pour étendre leur gouvernance au nuage[10]. Nous recommandons fortement aux organisations de se pencher attentivement sur le contrat de services infonuagiques, l'outil principal qui leur permettra :

- d'étendre leur gouvernance au nuage;
- de consigner les responsabilités du FSI et de l'organisation;
- de documenter et d'appliquer les accords sur les niveaux de service (ANS);
- de déterminer la propriété des données;
- de déterminer la résidence des données;

---

[9] Règlements de l'industrie comme les normes de sécurité sur les données de l'industrie des cartes de paiement (PCI DSS pour *Payment Card Industry Data Security Standard*), le Service Organization Control (SOC) 1 et 2, la *Health Insurance Portability and Accountability Act* (HIPAA), et les normes de l'Organisation internationale de normalisation (ISO 27001, 27017, et 27018).

[10] Les organisations bénéficieront d'une plus grande souplesse dans la négociation de la gouvernance du nuage dans un modèle de déploiement en nuage privé que dans un modèle de déploiement en nuage public.

- de déterminer les exigences en matière d'évaluation par des organismes tiers;
- de combler les lacunes des évaluations par un organisme tiers.

Le contrat de services infonuagiques devrait également inclure des dispositions régissant la manière précise dont l'organisation sera avisée dans l'éventualité d'un incident de sécurité, et le délai précis dans lequel elle sera avisée.

Pour demeurer concurrentiels, les FSI développent constamment de nouveaux services qui risquent de ne pas être visés par les contrats actuels. Avant d'utiliser ces nouveaux services, nous recommandons aux organisations de vérifier qu'ils ont été évalués officiellement par des organismes tiers et qu'ils sont couverts par les contrats en vigueur. Si tel n'est pas le cas, lesdits contrats devraient être modifiés avant que ces nouveaux services soient déployés.

4.3 SÉCURITÉ RÉSEAU

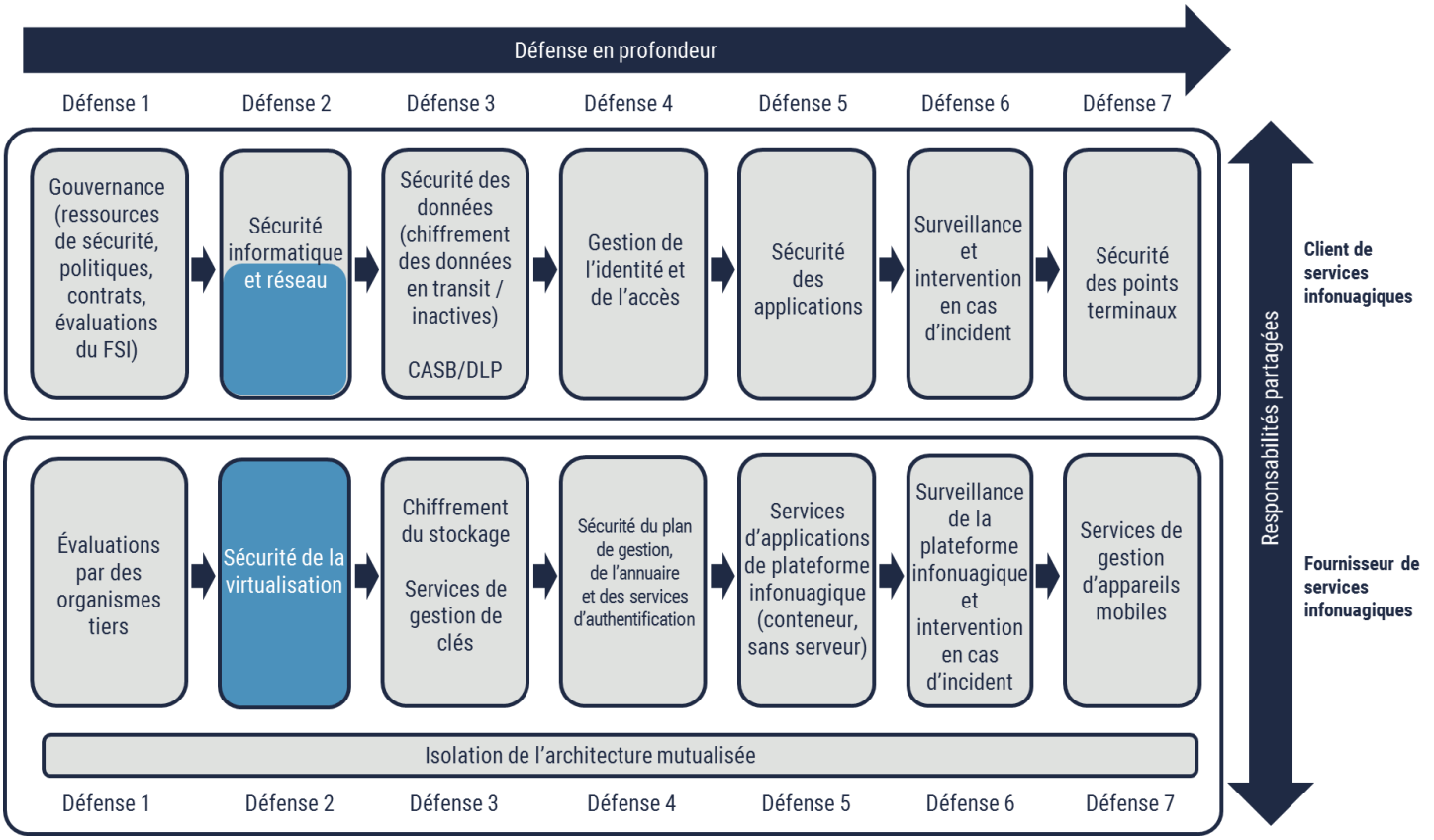

Figure 8 – Sécurité réseau

4.3.1 RESPONSABILITÉS PARTAGÉES LIÉES AU RÉSEAUTAGE

Les responsabilités liées au réseautage comportent notamment la gestion et la configuration de la sécurité des composants matériels, des réseaux virtuels, des équilibreurs de charge, des appliances réseau virtuelles, des serveurs de noms de domaine (DNS pour *Domain Name Server*) et des passerelles réseau.

Dans tous les modèles de service, les FSI sont responsables de la mise en œuvre et de la gestion des contrôles de sécurité réseau visant à protéger leurs plateformes infonuagiques contre les vecteurs de menace réseau. Pour sécuriser les réseaux, les FSI ont normalement recours à des mesures de protection contre les attaques par déni de service distribué (DDoS pour *Distributed Denial of Service*), à des systèmes de prévention d'intrusion (SPI) et à des pare-feux. Il revient aux FSI de mettre en œuvre les processus de virtualisation nécessaires pour assurer l'isolation entre leurs clients dans le nuage. Les FSI doivent veiller à ce que toute information sensible soit épurée avant de réintégrer les instances virtuelles dans les ressources partagées.

Dans le modèle IaaS, les organisations sont responsables de protéger leur réseau virtuel contre les menaces réseau. Nous encourageons les organisations à utiliser et à configurer les fonctions de sécurité offertes par les FSI ou d'autres entités, notamment les groupes de sécurité, les équilibreurs de charge virtuels, les pare-feux d'applications Web et d'autres appliances de sécurité réseau virtuelles de tiers.

Dans le modèle PaaS, la majorité des responsabilités en matière de gestion et de sécurité reviennent aux FSI. À titre de client du nuage, les responsabilités de l'organisation dépendront des services infonuagiques qu'elle choisit. Par exemple, certains services PaaS offerts par les FSI permettent aux organisations de placer l'instance PaaS directement dans leur réseau virtuel. Dans de tels cas, nous recommandons aux organisations d'utiliser les appliances réseau virtuelles ou les fonctions de sécurité du FSI afin de protéger l'accès à leur instance PaaS.

Dans le modèle SaaS, les fonctions de gestion et de sécurité du réseau relèvent de la responsabilité du FSI et sont incluses dans les logiciels offerts. Les organisations pourront peut-être configurer des restrictions réseau à l'aide de paramètres de configuration de sécurité SaaS et limiter l'accès à leurs logiciels à des emplacements réseau particuliers (p. ex. au réseau local seulement).

4.3.2 PARTICULARITÉS LIÉES AU RÉSEAUTAGE

Le concept de l'infonuagique se fonde sur des réseaux définis par logiciel (SDN pour *Software Defined Network*). Les SDN permettent de séparer la fonction de contrôle du réseau (c'est-à-dire celle qui décide où envoyer les paquets) de la fonction de transfert du réseau (c'est-à-dire le transfert de paquets en tant que tel). Cette séparation de la fonction de contrôle du réseau en permet la programmabilité et améliore grandement l'extensibilité et la souplesse par rapport aux réseaux locaux virtuels (VLAN pour *Virtual Local Area Network*) conventionnels.

Le réseautage infonuagique peut avoir un certain nombre de répercussions sur la sécurité. Par exemple, comme la fonction de contrôle du réseau est virtualisée, il n'est pas possible de mettre en place des systèmes de prévention d'intrusion réseau (NIPS pour *Network Intrusion Prevention System*) par la mise en miroir de ports physiques. Il faut plutôt mettre en œuvre la fonctionnalité des NIPS par l'intermédiaire d'appliances réseau virtuelles (NVA pour *Network Virtual Appliance*) ou de capteurs réseau au niveau de l'hôte. De tels capteurs ne sont pas disponibles pour toutes les charges de travail. Ils sont faciles à contourner si l'hôte est compromis, et leur extensibilité est limitée. Les NVA, quant à elles, créent des goulots d'étranglement, car elles doivent être déployées dans la voie du trafic à surveiller, ce qui risque de faire augmenter les coûts ainsi que le temps système du processeur pour la NVA (nécessitant ainsi des VM plus puissantes pour déployer les fonctions de la NVA). Certains FSI offrent des services TAP virtuels pour surveiller les flux de données, mais ces services ne correspondent généralement pas aux capacités d'un TAP réseau physique.

Les FSI offrent habituellement des outils infonuagiques natifs (comme les groupes de sécurité réseau) qui facilitent l'application des règles d'accès, la segmentation réseau et la surveillance. Toutefois, un grand nombre de ces outils ne sont pas compatibles avec la couche application. Les NVA tierces comportent souvent des capacités mieux développées et plus avancées que leurs équivalents infonuagiques natifs, mais elles ne sont pas nécessairement conçues en fonction de l'élasticité. Il peut être difficile de procéder à la mise à l'échelle automatique de ces NVA pour les faire correspondre à l'élasticité et à la courte durée de vie des autres composantes du nuage.

4.3.3 SEGMENTATION ET ZONAGE RÉSEAU

La segmentation réseau joue un rôle important dans la protection des charges de travail infonuagiques. La segmentation est une approche clé à l'appui de la défense en profondeur qui améliore le contrôle d'accès, la surveillance et le confinement. Si un bien est compromis dans une zone réseau, la segmentation limite l'impact sur les biens d'autres zones.

L'infonuagique n'emploie pas les mêmes techniques que le réseautage conventionnel. Les plateformes infonuagiques dépendent souvent de la mise en réseau à définition logicielle (SDN pour *Software Defined Networking*) pour la segmentation réseau et pour offrir des capacités que le réseautage conventionnel ne peut prendre en charge.

Les FSI offrent normalement un certain nombre de processus de segmentation dans le cadre de leurs services réseau virtuels. Il importe que les organisations comprennent les techniques de segmentation réseau offertes par leur FSI, qui pourraient comporter les capacités ci-dessous :

- configurer des sous-réseaux publics ou privés;
- mettre en service chaque charge de travail infonuagique et les données connexes dans leur propre réseau virtuel;
- mettre en service des instances dédiées des services infonuagiques directement dans le réseau virtuel du client;
- utiliser des fonctions de sécurité infonuagique natives pour réguler le trafic entre les segments (comme les groupes de sécurité);
- avoir recours à des NVA comme les pare-feux et les équilibreurs de charge pour réguler le trafic entre les segments;
- réguler le trafic à l'aide de balises ou d'autres attributs plutôt que d'adresses IP.

Au moment d'élaborer les stratégies de segmentation réseau, nous recommandons aux organisations d'utiliser les fonctions offertes par leur FSI afin de limiter les mouvements latéraux dans l'éventualité d'une compromission de la sécurité. Par exemple, les organisations voudront peut-être créer des charges de travail d'application dans leur propre réseau virtuel ou encore isoler davantage les charges de travail à l'aide de groupes de sécurité, ce qui permettra de les séparer les unes des autres à la suite d'une éventuelle compromission.

Nous recommandons fortement aux organisations d'adopter un modèle de sécurité **qui anticipe une atteinte à la sécurité** et d'employer des techniques comme la microsegmentation et le périmètre à définition logicielle. Dans le cas de la micro-segmentation, les politiques sont appliquées directement aux VM ou aux applications par l'intermédiaire de logiciels. Les politiques sont liées aux VM et aux applications au lieu d'être mises en œuvre sur une applicance physique ou virtuelle distincte comme un pare-feu. Ces politiques suivront la VM ou l'application même si elle est déplacée. Les politiques ne sont plus rattachées à la topologie du réseau; elles sont plutôt mises en œuvre dans chaque composante de l'infrastructure. Essentiellement, les charges de travail sont divisées en unités plus petites pour que la compromission de l'une d'entre elles ne touche pas les autres.

4.3.4 ROUTAGE

Dans le modèle IaaS, la responsabilité du routage revient surtout au client du nuage. Les organisations sont responsables de la connectivité et du contrôle d'accès réseau aux services informatiques et infonuagiques, ainsi qu'aux services de stockage et de données. Le routage constitue l'un des principaux mécanismes permettant de contrôler les flux de données et de mettre en œuvre les zones de sécurité réseau. Le routage appuie la défense en profondeur en dirigeant le trafic vers les appliances réseau virtuelles, en contrôlant les flux de données entre les réseaux virtuels et en assurant la connectivité aux réseaux locaux.

Grâce aux SDN, les FSI ont d'innombrables options lorsqu'ils développent leurs capacités de réseautage virtuel. Par conséquent, les capacités réseau varient grandement d'un fournisseur à l'autre. Il importe que les organisations comprennent la manière dont les FSI effectuent le routage et comment leurs choix soutiennent la segmentation réseau et les zones de sécurité.

Le fait de mal comprendre et de mal configurer les comportements de routage risque d'avoir de graves répercussions sur la sécurité, tout particulièrement dans le déploiement en nuage hybride, car le comportement de routage peut être différent pour chaque FSI. Nous encourageons les organisations à poser les questions suivantes au moment d'élaborer et de mettre en œuvre leurs solutions IaaS :

- Faut-il préciser explicitement les itinéraires avant que le trafic soit autorisé entre le sous-réseau source et le sous-réseau de destination?
- Le routage entre tous les sous-réseaux est-il autorisé par défaut dans un réseau virtuel?
- Y a-t-il un itinéraire par défaut vers Internet?
- Les réseaux virtuels peuvent-ils être mis en service sans itinéraire vers Internet?
- Quelle est l'incidence de l'appairage de deux réseaux virtuels sur la connectivité à chaque sous-réseau?
- Faut-il avoir un itinéraire pour forcer le trafic vers les appliances réseau virtuelles?

4.3.5 RÉSEAUTAGE DANS LE NUAGE HYBRIDE

Dans le cas des services clients et opérationnels hébergés dans un nuage à l'extérieur des installations du client, l'accès se fait par l'Internet public. Cela pose un risque pour la disponibilité et le rendement des services opérationnels, car les organisations n'ont alors aucun contrôle direct sur la sécurité, la fiabilité, la gestion de la bande passante et la latence de la connectivité Internet.

Comme l'indique la figure 9, les FSI offrent des connexions réseau privées et dédiées entre l'infrastructure locale et les installations des fournisseurs d'accès Internet (FAI). Les installations des FAI servent de point de présence du FSI pour la connectivité privée et comportent les avantages ci-dessous :

- bande passante dédiée pour le client du nuage;
- connectivité fiable à faible latence;
- sécurité réseau accrue.

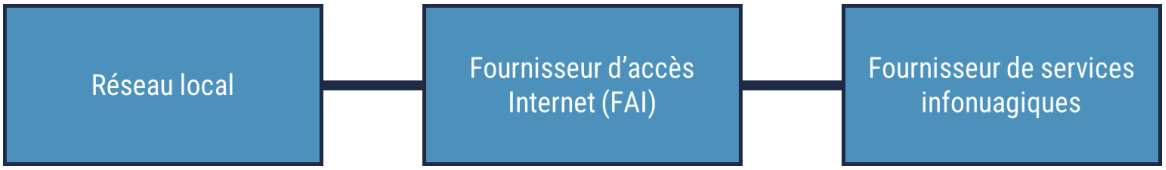

Figure 9 – Connexion privée à un FSI par l'intermédiaire d'un fournisseur d'accès Internet

Lors de la mise en œuvre de connexions réseau privées et dédiées, nous recommandons aux organisations de veiller à ce qu'une séparation adéquate soit appliquée afin de surveiller et de contrôler le trafic entre les réseaux locaux et les environnements infonuagiques à distance. La séparation est normalement assurée par le routage, les contrôles d'accès, les pare-feux ou les NVA entre les deux environnements.

Les nuages hybrides utilisent souvent des réseaux virtuels bastions ou de transit pour connecter de multiples réseaux virtuels à des centres de données locaux[11]. Comme l'indique la figure 10, les connexions réseau privées et dédiées entre les installations locales et le nuage se terminent dans le réseau bastion, lequel est alors appairé avec les autres réseaux virtuels du nuage. Les réseaux bastions peuvent être utilisés pour appliquer la séparation par l'intermédiaire du routage et ils peuvent constituer un emplacement approprié où mettre en œuvre le contrôle d'accès et d'autres outils de sécurité entre les deux réseaux. Nous encourageons les organisations à envisager également la mise en place de contrôles semblables du côté local de la connexion dédiée afin de protéger les services locaux.

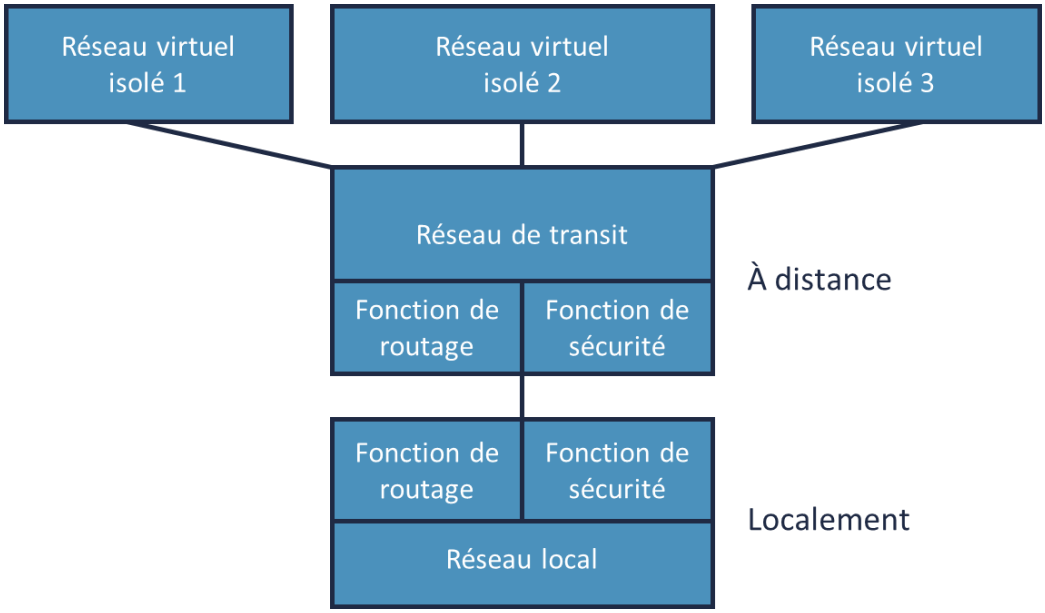

Figure 10 – Concept du réseau bastion ou de transit

[11] Cloud Security Alliance Security, *Guidance for Critical Areas of Focus in Cloud Computing*, section 7.3.5 (Hybrid Cloud Considerations).

4.4 INFORMATIQUE

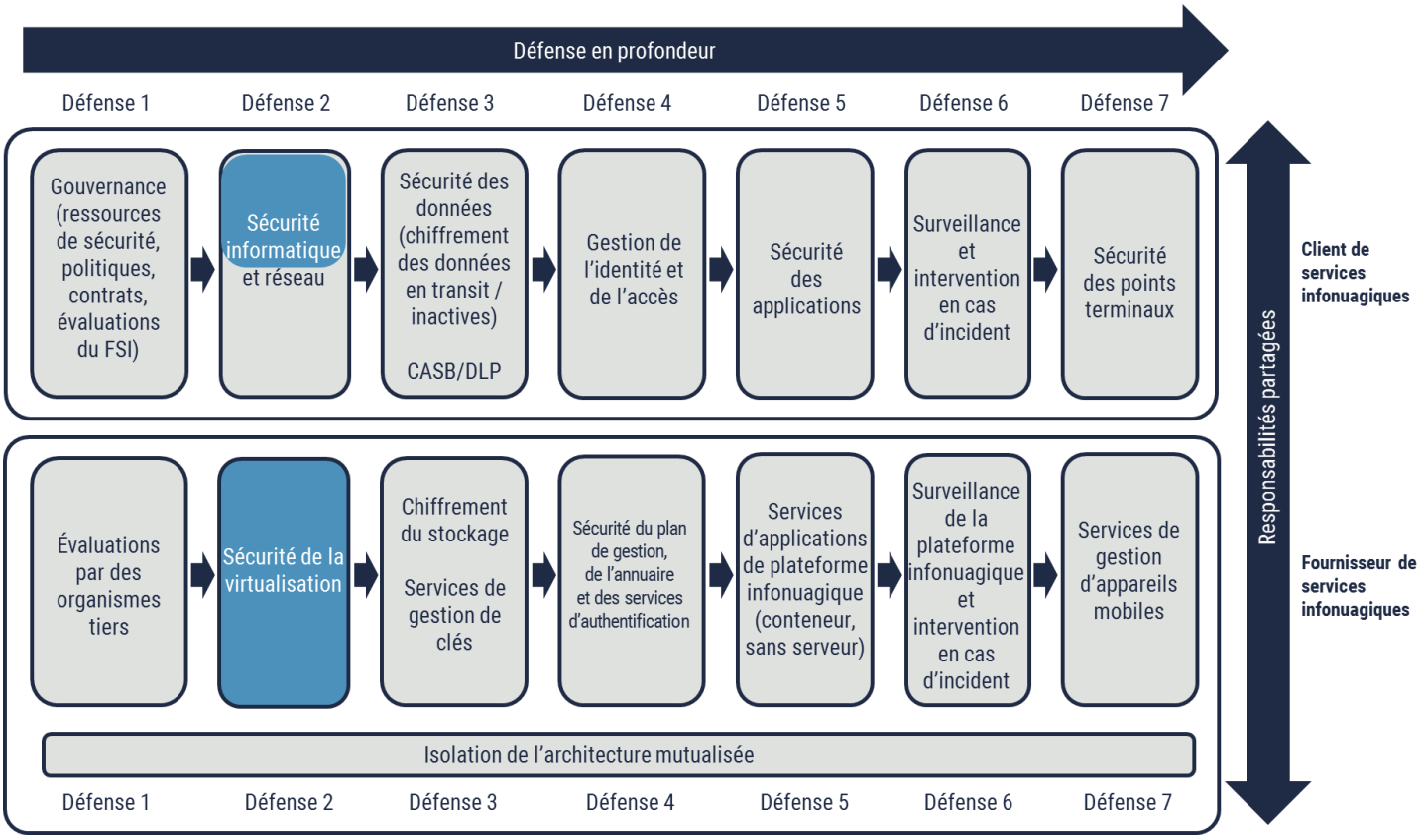

Figure 11 – Informatique

4.4.1 RESPONSABILITÉS PARTAGÉES

Les responsabilités en matière d'informatique comportent notamment la gestion et la configuration de la sécurité des hôtes physiques, des processeurs, des hyperviseurs, des machines virtuelles, des conteneurs et des plateformes sans serveur.

Les FSI sont responsables de la sécurité de l'hôte physique et de l'hyperviseur. Ils doivent veiller à ce que les contrôles nécessaires soient en place afin de maintenir l'isolation des charges de travail. Dans les modèles SaaS et PaaS, le FSI est responsable principalement des machines virtuelles et des charges de travail sans serveur.

Dans le modèle IaaS, les organisations clientes sont responsables de la gestion et de la configuration de la sécurité des machines virtuelles. Il s'agit notamment de l'application de correctifs, de la configuration de sécurité de base, du contrôle d'accès, de la gestion de l'identité et de la surveillance de la sécurité.

La responsabilité de la sécurité des charges de travail des conteneurs varie selon les services offerts par chaque FSI. Elle peut revenir au FSI ou au client, ou encore être partagée.

4.4.2 PARTICULARITÉS

Les charges de travail informatiques peuvent prendre la forme d'une VM, d'un conteneur, du traitement par lots, du calcul parallèle de haute performance, de l'informatique sans serveur, de l'informatique en périphérie ou d'autres plateformes.

Nous recommandons aux organisations de se pencher sur les considérations liées à la sécurité pour chaque type de charge de travail.

La plupart des contrôles de sécurité déployés localement s'appliquent aussi aux VM fondées sur l'infonuagique. Il faut toutefois tenir compte de certaines considérations liées à la sécurité en ce qui concerne le déploiement en nuage. Les organisations devraient prendre les mesures ci-dessous :

- inclure de multiples VM et d'autres fonctions de haute disponibilité dans la conception des charges de travail;
- tirer profit des capacités d'automatisation infonuagique pour appliquer les bases de référence de la sécurité des VM;
- avoir recours à la mise à l'échelle automatique pour améliorer la disponibilité;
- utiliser des agents qui prennent en charge la mise à l'échelle automatique;
- éviter les agents non conçus pour l'infonuagique (qui peuvent nuire à la performance);
- aviser les FSI avant de réaliser une évaluation des vulnérabilités;
- effectuer la capture de journaux à l'externe (les charges de travail peuvent être dynamiques et de courte durée);
- déployer les VM dans les régions approuvées par le FSI.

Dans le cas des charges de travail informatiques autres que celles des machines virtuelles (gérées par les fournisseurs de services), les organisations contrôlent et voient peu la sécurité de l'infrastructure de base du FSI. Ce dernier peut offrir aux organisations un certain nombre d'options et de contrôles de sécurité, mais celles-ci risquent :

- de ne pas pouvoir exécuter des agents logiciels;
- d'avoir un accès limité aux journaux;
- de ne pas pouvoir réaliser des évaluations des vulnérabilités.

4.4.3 GESTION DE L'IMAGE

Un grand nombre de systèmes virtuels dans l'environnement infonuagique d'aujourd'hui sont jetables. Ils sont constamment créés, remplacés, détruits et redimensionnés. La conception change fréquemment, et les solutions doivent être mises en œuvre dans de courts délais. En raison de l'élasticité et de la mise à l'échelle automatique, les charges de travail sont de courte durée. Il ne convient donc pas d'appliquer des correctifs de sécurité ou d'autres modifications à des charges de travail en exécution puisqu'ils seraient perdus dès que la charge de travail se termine. Il faut trouver une autre approche de gestion de l'image afin de composer avec cette situation.

Les organisations qui souhaitent faire appel à la mise à l'échelle automatique et aux conteneurs devraient étudier de nouvelles approches de gestion de l'image, notamment :

- les mises à jour automatisées fréquentes de l'image visant à appliquer les correctifs de sécurité et les signatures de maliciels;
- l'application des bases de référence de la sécurité de l'image automatisée lors de la création de l'image;
- les tests de sécurité automatisés lors de la création de l'image;
- la désactivation de l'ouverture de session et la restriction des services avant le déploiement de l'image.

Ces nouvelles approches de gestion de l'image permettent d'améliorer la sécurité de plusieurs façons, notamment par :

- la simplification du processus d'application de correctifs;
- l'automatisation de la gestion de la configuration;
- L'application de stratégies de sécurité répétables;
- l'absence de dérive de la configuration de sécurité;
- la validation de l'infrastructure avant le déploiement;
- des processus de restauration et de récupération simples.

4.5 SÉCURITÉ DES DONNÉES

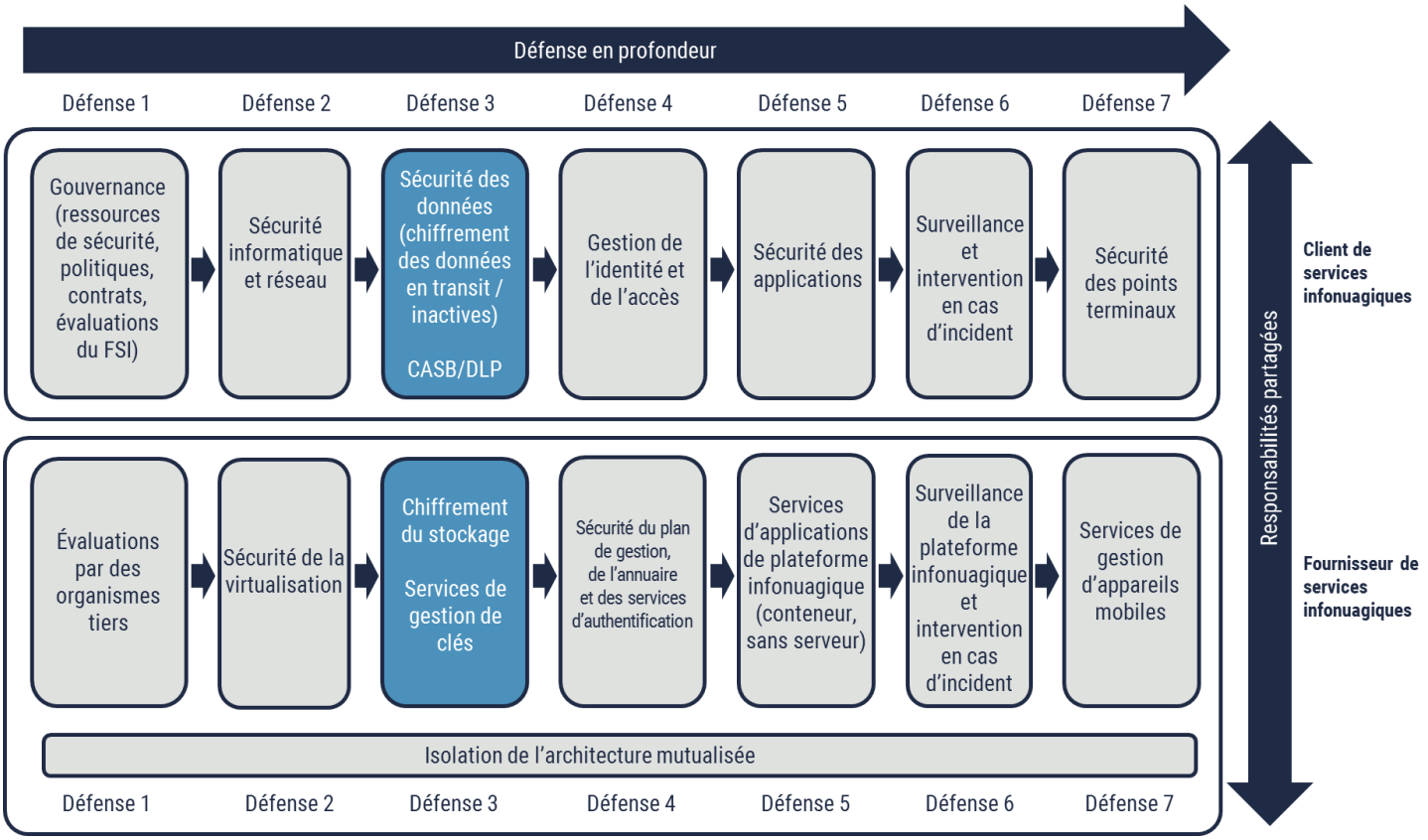

Figure 12 – Sécurité des données

La sécurité des données est l'une des principales préoccupations des clients de services infonuagiques. Avant d'héberger des charges de travail et des données sur des plateformes infonuagiques, les clients devraient établir soigneusement un plan et tenir compte de la stratégie de sécurité pour la migration des données, de la sécurité des données pendant qu'elles se trouvent dans le nuage, et des considérations liées à la sécurité découlant du retrait des applications ou de leur transfert à l'infrastructure locale ou à un autre fournisseur de services. L'adoption d'une stratégie de sécurité à plusieurs couches constitue la meilleure façon de protéger les données. La gouvernance, la sécurité de l'infrastructure, la gestion de l'identité

et de l'accès, la sécurité des applications et la gestion de l'intervention en cas d'incident ont toutes un rôle à jouer dans la sécurité des données.

4.5.1 RESPONSABILITÉS PARTAGÉES

Les responsabilités liées à la sécurité des données comportent notamment le contrôle d'accès, le chiffrement, la gestion des clés, la surveillance, la gestion du cycle de vie, la migration des données et d'autres composantes particulières de plateformes infonuagiques.

Il revient aux organisations d'assurer la sécurité des données sensibles. Les organisations doivent déterminer les données dont le stockage dans le nuage est autorisé, surveiller les migrations, le traitement ou le stockage des données dans l'infrastructure infonuagique et chiffrer les données à mesure qu'elles sont transmises au nuage. Les organisations assument également les responsabilités globales liées à la gestion du cycle de vie en ce qui concerne l'emplacement des données, la résidence des données, la continuité des activités et les exigences en matière de conformité et de protection des renseignements personnels. Dans le cas des plateformes IaaS, les organisations sont responsables des copies de sauvegarde et de la récupération des données.

Les FSI sont responsables de la sécurité de l'infrastructure de stockage. Ils doivent veiller à ce que des contrôles soient mis en place afin d'assurer l'isolation des comptes de stockage, le nettoyage des supports avant leur élimination ainsi que le nettoyage des supports de stockage virtuels avant de les réintégrer aux ressources partagées.

Les FSI offrent à leurs clients de nombreuses options de contrôle d'accès et de services de gestion des clés. Dans les modèles PaaS et SaaS, les FSI se chargent généralement des copies de sauvegarde et de la récupération des données.

La responsabilité du chiffrement des données inactives varie selon le modèle de service et le type de stockage.

4.5.2 PARTICULARITÉS

Un grand nombre des moyens employés pour sécuriser l'infrastructure TI conventionnelle s'appliquent également au nuage. L'une des considérations principales liées à la sécurité infonuagique concerne le type de stockage offert (p. ex. stockage de blocs, de fichiers et d'objets). Cela dit, la virtualisation offre d'autres options de stockage, notamment :

- des disques durs virtuels pour des machines virtuelles basées sur une solution IaaS;
- diverses plateformes de bases de données pour les modèles PaaS;
- diverses plateformes de stockage d'applications (p. ex. stockage de table, file d'attente de messages, mise en cache);
- des réseaux de diffusion de contenu (RDC).

La mise en œuvre sécurisée de ces solutions de stockage peut s'avérer complexe et varier grandement selon les services de stockage infonuagique de chaque FSI. Il convient de noter que la configuration de sécurité par défaut de ces services de stockage n'est pas toujours adéquate. Les organisations doivent connaître les options de configuration de sécurité pour chacun des services de stockage qu'elles prévoient utiliser. Des options de configuration courantes pour la sécurité du stockage sont présentées ci-dessous :

1. **Emplacement des données** : Il importe de connaître le lieu géographique où sont stockées les données dans le nuage, tout particulièrement pour les clients de secteurs gouvernementaux ou d'industries réglementées, ou dans les pays où des lois sévères de protection des données sont en vigueur. En règle générale, le client sait où sont stockées les données dans les nuages privés et communautaires, mais dans le modèle de déploiement en nuage public, il risque de ne pas être avisé de l'emplacement, à moins que le FSI ait offert des politiques facultatives de restriction géographique et que le client ait configuré son compte pour demander des restrictions géographiques précises[12].
2. **Protocole d'accès** : Les clients accèdent aux données dans le nuage par l'intermédiaire de protocoles Internet. Comme le stockage infonuagique n'est pas toujours configuré pour utiliser un protocole sécurisé par défaut, les clients devraient s'assurer de configurer des protocoles sécurisés (p. ex. HTTPS) pour l'accès aux données dans le nuage.
3. **Stockage public** : Les services de stockage infonuagique sont généralement offerts en option publique ou privée. Les organisations devraient surveiller tout changement aux autorisations de stockage qui permettraient un accès public par erreur.
4. **Clés d'accès de stockage** : En nuage privé, les clients accèdent généralement aux services de stockage à l'aide de clés d'accès de stockage obtenues par l'intermédiaire du portail de gestion de chaque FSI. Nous recommandons aux organisations d'établir un processus documenté de gestion et de rotation des clés afin de prévenir la divulgation non autorisée des clés d'accès de stockage et des données.
5. **Points de terminaison de service** : Un grand nombre des options de stockage offertes par les FSI sont des services infonuagiques à l'extérieur du périmètre ou du réseau virtuel de l'organisation. Par exemple, un service de base de données PaaS se trouve normalement à l'extérieur du périmètre réseau de l'organisation et l'accès se fait par l'adresse IP publique de celle-ci. Un point de terminaison de service permet d'accéder à une base de données ou aux services infonuagiques PaaS comme s'ils se trouvaient à l'intérieur du périmètre réseau plutôt qu'en traversant le périmètre vers Internet. Bien que les FSI n'offrent pas des capacités de point de terminaison de service pour tous les services infonuagiques, les organisations devraient y avoir recours dans la mesure du possible pour contrôler l'accès aux services PaaS par l'intermédiaire de leur réseau virtuel.
6. **Protection du stockage par pare-feu** : Certains FSI offrent la capacité de restreindre l'accès au stockage infonuagique en mettant les adresses IP sources sur une liste blanche ou une liste noire. Une fois authentifiés, les points terminaux dont les adresses IP sont autorisées auront accès au stockage infonuagique. Les organisations devraient se servir de cette capacité pour restreindre l'accès au stockage infonuagique.
7. **Nettoyage des supports de données** : Les clients de services infonuagiques ne contrôlent pas les supports de stockage physiques et ne pourront peut-être pas les nettoyer puisque plusieurs locataires se partagent les ressources infonuagiques. Les clients devraient envisager de chiffrer les données inactives pour veiller à ce que les données soient nettoyées avant que les ressources de stockage infonuagique soient réintégrées aux ressources partagées du FSI.

[12] NIST, *Special Publication 800-146, Cloud Computing Synopsis and Recommendations* [12].

8. **Chiffrement des données inactives** : Les organisations devraient songer à utiliser les options de chiffrement et de stockage gérées par le fournisseur. Toutefois, dans les environnements à sécurité élevée, elles devraient envisager d'utiliser des clés gérées par le client. Pour en savoir plus, prière de consulter l'ITSP.50.106 du Centre pour la cybersécurité, *Chiffrement des données* [13].

4.5.3 MIGRATION DES DONNÉES

La migration des données vers le nuage peut s'avérer complexe. Une migration inappropriée risque de compromettre la confidentialité, l'intégrité et la disponibilité de l'information, en plus des processus opérationnels de l'organisation qui passent au nuage. Les risques liés à la migration des données comportent notamment la divulgation non autorisée, la perte et la corruption de données, les périodes d'indisponibilité prolongées et la non-conformité. De plus, les divers types de données (données opérationnelles, métadonnées, code source, etc.) ont des exigences particulières en matière de migration. Les clients de services infonuagiques doivent faire la planification nécessaire pour régler les questions liées à la sécurité avant d'entamer la migration des données vers le nuage.

Il faut d'abord déterminer les données qui seront autorisées à passer au nuage. Dans le cadre de la planification de la migration, nous recommandons aux organisations de passer en revue leurs politiques de sécurité, les exigences liées à la conformité et la catégorisation des processus opérationnels et des biens d'information[13]. Ce processus permettra aux organisations de relever les contraintes en matière de conformité ainsi que les contraintes juridiques, contractuelles et opérationnelles. Elles devront également définir les besoins concernant la résidence et l'emplacement des données, les obligations liées à la conservation des données et la catégorisation de sécurité des biens d'information.

Nous encourageons les organisations à choisir le profil de sécurité infonuagique qui correspond à la catégorie de sécurité de leurs biens d'information[14]. Le profil de contrôle de la sécurité infonuagique établit les contrôles de sécurité recommandés que devraient appliquer les FSI et les clients à l'appui des services fondés sur l'infonuagique.

La sécurité des données est importante non seulement pendant qu'elles se trouvent dans le nuage, mais aussi pendant la migration vers le nuage. Par exemple, avant la migration, les organisations devraient s'assurer que les données sont sauvegardées, chiffrées en transit et protégées dans les destinations de stockage temporaires et permanentes, et veiller à ce que la confidentialité et l'intégrité des données soient maintenues tout au long de la migration.

En plus de la planification de la migration, nous recommandons aux organisations de mettre en place des mécanismes pour surveiller la migration de grandes quantités de données et les activités connexes de façon continue. La surveillance des activités liées aux bases de données et aux fichiers, les courtiers de sécurité d'accès au nuage (CASB pour *Cloud Access Security Broker*), le filtrage d'URL et les mécanismes de prévention de la perte de données (DLP pour *Data Loss Prevention*) sont des exemples d'outils pouvant assurer la visibilité nécessaire pour détecter et prévenir la migration non autorisée de données et l'utilisation de services infonuagiques non autorisés.

---

[13] L'ITSP.50.103 [2] recommande une approche permettant de répertorier et de catégoriser les processus opérationnels et les biens d'information.

[14] Votre organisation devrait choisir un des profils de contrôle de la sécurité infonuagique élaborés par le Centre pour la cybersécurité qui se trouvent aux annexes A et B de l'ITSP.50.103. [2]

4.5.4 LA SÉCURITÉ DES DONNÉES DANS LE NUAGE

4.5.4.1 SÉCURITÉ DU PLAN DE GESTION

Le rôle du plan de gestion comporte notamment la gestion des opérations pouvant être executées sur les ressources de stockage. Les organisations devraient faire appel au contrôle d'accès axé sur le rôle pour définir les utilisateurs autorisés à créer, à configurer et à supprimer des ressources de stockage, y compris les clés d'accès de stockage.

4.5.4.2 DONNÉES EN TRANSIT

Le transit des flux de données à destination, en provenance et à l'intérieur d'environnements infonuagiques passe par une infrastructure réseau hors du contrôle des organisations. Des auteurs de menace pourraient intercepter ces communications et compromettre la confidentialité et l'intégrité de l'information. Nous recommandons fortement aux organisations de veiller à ce que les données en transit soient chiffrées afin de sécuriser les communications à destination et en provenance des environnements infonuagiques.

Les organisations contrôlent le périmètre IaaS, mais les communications comporteront sans doute un échange d'information avec des services infonuagiques à l'extérieur du périmètre. Elles ne connaîtront pas non plus l'emplacement des instances qui contribuent au transfert de données. Par exemple, les instances de VM d'une organisation se trouvent peut-être dans différents centres de données du FSI, et les communications peuvent être transmises sur une infrastructure réseau qui ne relève pas du contrôle du client ni du FSI. Il convient donc de chiffrer les communications de données dans un environnement infonuagique dès qu'il s'agit d'information sensible.

Bien qu'on puisse avoir recours au chiffrement côté client avant de procéder à un transfert de données, il est recommandé d'utiliser le protocole HTTPS (chiffrement de bout en bout) pour garantir l'intégrité des données. Nous recommandons également aux organisations de prendre les mesures suivantes :

- utiliser le protocole HTTPS pour accéder aux services de stockage infonuagique et aux API;
- désactiver les algorithmes de chiffrement faibles;
- activer d'autres protocoles réseau chiffrés en fonction d'applications particulières (p. ex. le protocole SMB pour l'accès au stockage de fichiers).

4.5.4.3 DONNÉES INACTIVES

Le chiffrement des données inactives permet de protéger ces données lorsqu'elles sont stockées sur des supports physiques ou virtuels, en plus d'en prévenir la divulgation ou la modification non autorisée. Le chiffrement des données inactives s'inscrit dans l'approche globale de défense en profondeur. Les organisations clientes et les FSI auront peut-être mis en œuvre des contrôles à divers niveaux afin de protéger les données, mais le chiffrement des données inactives offre une protection additionnelle advenant l'échec des autres mesures de sécurité.

Nous recommandons fortement aux organisations de prévoir le chiffrement des données inactives dans leur stratégie de défense en profondeur. Elles devraient également mettre à jour leurs politiques de sécurité de manière à exiger le chiffrement des données inactives et à définir la catégorie de données qu'il faut chiffrer aux fins du stockage infonuagique. Nous suggérons aux organisations d'envisager le chiffrement des données inactives afin de protéger la confidentialité et l'intégrité des données, des images de VM, des applications et des copies de sauvegarde.

Dans une architecture infonuagique mutualisée, le chiffrement des données inactives peut servir à isoler davantage les données d'une organisation de celles des autres locataires et du FSI. Les organisations pourraient devoir mettre en œuvre le chiffrement des données inactives pour se conformer aux lois sur la protection de la vie privée, aux règlements de l'industrie et du gouvernement, ainsi qu'à d'autre réglementation. Le chiffrement des données inactives permet de nettoyer les données avant que les ressources de stockage soient réintégrées aux ressources partagées du FSI.

Les approches de chiffrement des données inactives varient considérablement selon les modèles IaaS, PaaS et SaaS. Diverses techniques s'offrent également pour la gestion des clés de chiffrement, ce qui complique la situation. Dans le document *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0* [5], le CSA décrit chacune des approches de chiffrement des données inactives. La figure 13 en fait un résumé. Pour obtenir de plus amples renseignements, prière de consulter l'ITSP.50.106, *Chiffrement des données* [13].

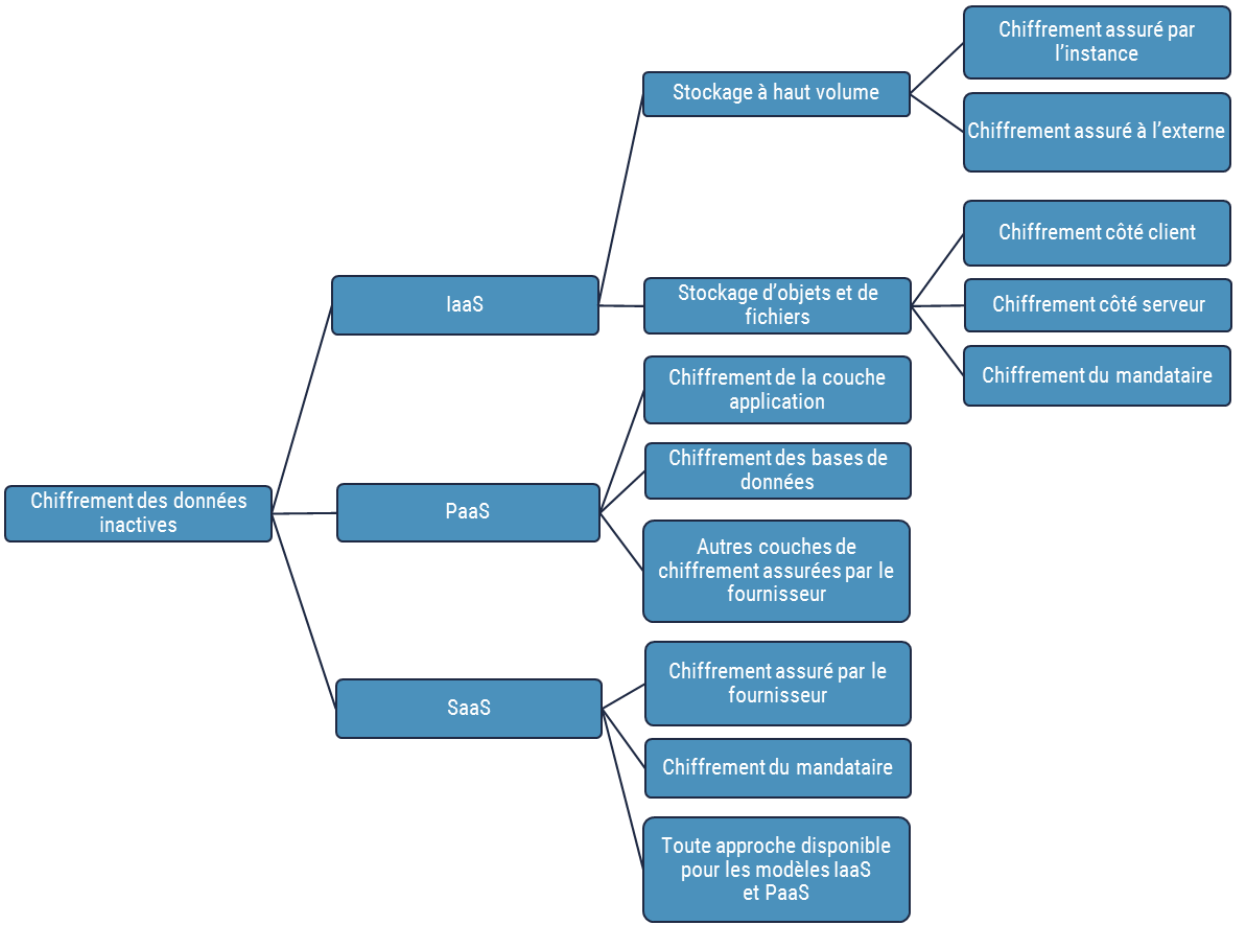

Figure 13 – Approches de chiffrement des données inactives

Le FSI active souvent par défaut le chiffrement du stockage d'objets et de fichiers, mais la configuration par défaut peut changer au fil du temps. Les organisations devraient avoir recours à la configuration de sécurité de base et à la surveillance continue pour veiller à l'application du chiffrement des données inactives. Toutes les approches de chiffrement des données présentées à la figure 13 protégeront la confidentialité et l'intégrité des données contre l'accès non autorisé aux supports physiques. Elles ne fourniront cependant pas toutes une protection efficace contre la compromission de plateformes, de systèmes d'exploitation ou d'applications.

Les organisations devraient tenir compte d'un certain nombre de facteurs avant de choisir une stratégie de chiffrement des données inactives, notamment le type de stockage, l'environnement où se trouvent les données (plateforme, système d'exploitation, application), la quantité de données et les menaces qui pèsent sur les données. Par exemple, les options de chiffrement du modèle PaaS pourraient varier d'une plateforme à l'autre, tandis que les fournisseurs de modèles SaaS pourraient utiliser n'importe quelle option de la figure 13.

Il ne faut pas sous-estimer l'importance de la gestion des clés pour le chiffrement des données inactives. Bien qu'elle soit complexe, la gestion des clés peut être effectuée par le FSI ou le client. Il s'agit de générer, de distribuer, de stocker, de récupérer et de détruire les clés de chiffrement. Un processus inefficace de gestion des clés risque de compromettre la confidentialité et l'intégrité des données ou, pire encore, de rendre les données inutilisables. Nous recommandons aux organisations d'accroître l'isolation avec leur FSI en gérant elles-mêmes les clés de chiffrement, notamment en prenant les mesures ci-dessous :

- disposer de processus de gestion des clés bien conçus, documentés et mis à l'essai;
- mettre à profit le service de gestion des clés de leur FSI afin de simplifier les processus;
- envisager une solution HSM dédiée du FSI pour les environnements à sécurité élevée.

4.5.4.4 RÉPLICATION DES DONNÉES

La réplication assure la durabilité et la haute disponibilité des données[15] dans l'éventualité d'événements prévus et imprévus, y compris les interruptions liées aux pannes de courant, à la défaillance de matériel ou du réseau et aux catastrophes naturelles.

Le stockage géoredondant comporte la réplication des données dans plusieurs lieux géographiques. Tout dépendant des options et des services offerts par le FSI, les données peuvent être répliquées dans un même centre de données, dans plusieurs centres de données dans la même région (au plus à quelques kilomètres de distance), ou dans plusieurs centres de données dans différentes régions géographiques. Les FSI offrent normalement par défaut un certain niveau de réplication de données, de même qu'un certain nombre d'options de réplication. Les organisations devraient s'assurer de bien comprendre les options de réplication des données et de choisir celles qui répondent à leurs besoins en matière de disponibilité, de durabilité et de continuité des activités.

---

[15] Western Digital définit la disponibilité du stockage comme étant le *temps de disponibilité du système de stockage*, c'est-à-dire que le système de stockage est fonctionnel et en mesure de livrer des données sur demande. Cette fonction est normalement assurée par la redondance du matériel. La durabilité, quant à elle, renvoie à la *protection à long terme des données*, c'est-à-dire que les données stockées ne sont pas détériorées, dégradées ou autrement corrompues. Elle porte sur la redondance des données plutôt que la redondance du matériel, de manière à éviter la perte ou la compromission des données.

4.5.4.5 RÉMANENCE DES DONNÉES

Par rémanence des données, on entend la représentation physique résiduelle qui persiste sur un dispositif de stockage malgré les mesures prises pour les éliminer. Après l'effacement de données sur un dispositif de stockage, certaines caractéristiques physiques résiduelles pourraient permettre de reconstituer les données. La rémanence des données peut mener à la divulgation non intentionnelle d'information sensible si le dispositif de stockage est utilisé ou perdu dans un environnement non contrôlé. Le nettoyage et l'élimination des supports visent à protéger la confidentialité des données résiduelles qui s'y trouvent. Ces mesures pourraient également devoir être prises afin de se conformer aux politiques de sécurité de l'organisation, de même qu'aux lois sur la protection de la vie privée et aux règlements du gouvernement et de l'industrie.

Selon le document *Special Publication 800-88, Guidelines for Media Sanitization* du NIST [14], le nettoyage des supports constitut un processus visant à rendre l'accès aux données cibles sur le support impossible selon un niveau d'effort donné. Cette pratique permet de garantir la confidentialité des données qui pourraient subsister dans les supports et de minimiser les risques de divulgation non autorisée. Dans une architecture mutualisée, les organisations ne contrôlent pas les supports de stockage physiques. Le client des services infonuagiques ne peut donc pas utiliser les techniques de nettoyage qui exigent un accès physique aux supports. Il faut adopter une autre approche, par exemple, l'effacement cryptographique (CE pour *Crypto Erase*). D'après l'ITSP.40.006 v.2 du Centre pour la cybersécurité, *Nettoyage des supports de TI* [15], l'effacement cryptographique est un processus de nettoyage consistant à effacer la clé de chiffrement qui est employée sur un support chiffré pour rendre les données illisibles. Cette méthode peut être utilisée pour nettoyer les supports de stockage infonuagique avant de les réintégrer aux ressources partagées du FSI.

Le recours au chiffrement tout au long du cycle de vie d'un support de stockage accélère et optimise le processus de nettoyage, et simplifie les exigences visant la destruction des supports en fin de vie. Nous recommandons aux organisations de chiffrer régulièrement tous les supports pendant la durée de leur cycle de vie, de façon à protéger la confidentialité des données, même après que ces supports ont été déclassés et éliminés. Cette pratique permet de garantir la confidentialité des données qui pourraient subsister dans les supports et de minimiser les risques de divulgation non autorisée[16]. Les organisations devraient envisager d'avoir recours au HSM ou aux services de gestion des clés offerts par leur FSI afin de protéger les clés de chiffrement de clés (KEK pour *Key Encryption Key*).

[16] ITSP.40.006 (version 2) du Centre pour la cybersécurité*, Nettoyage des supports de TI* [15].

4.6 GESTION DE L'IDENTITÉ ET DE L'ACCÈS

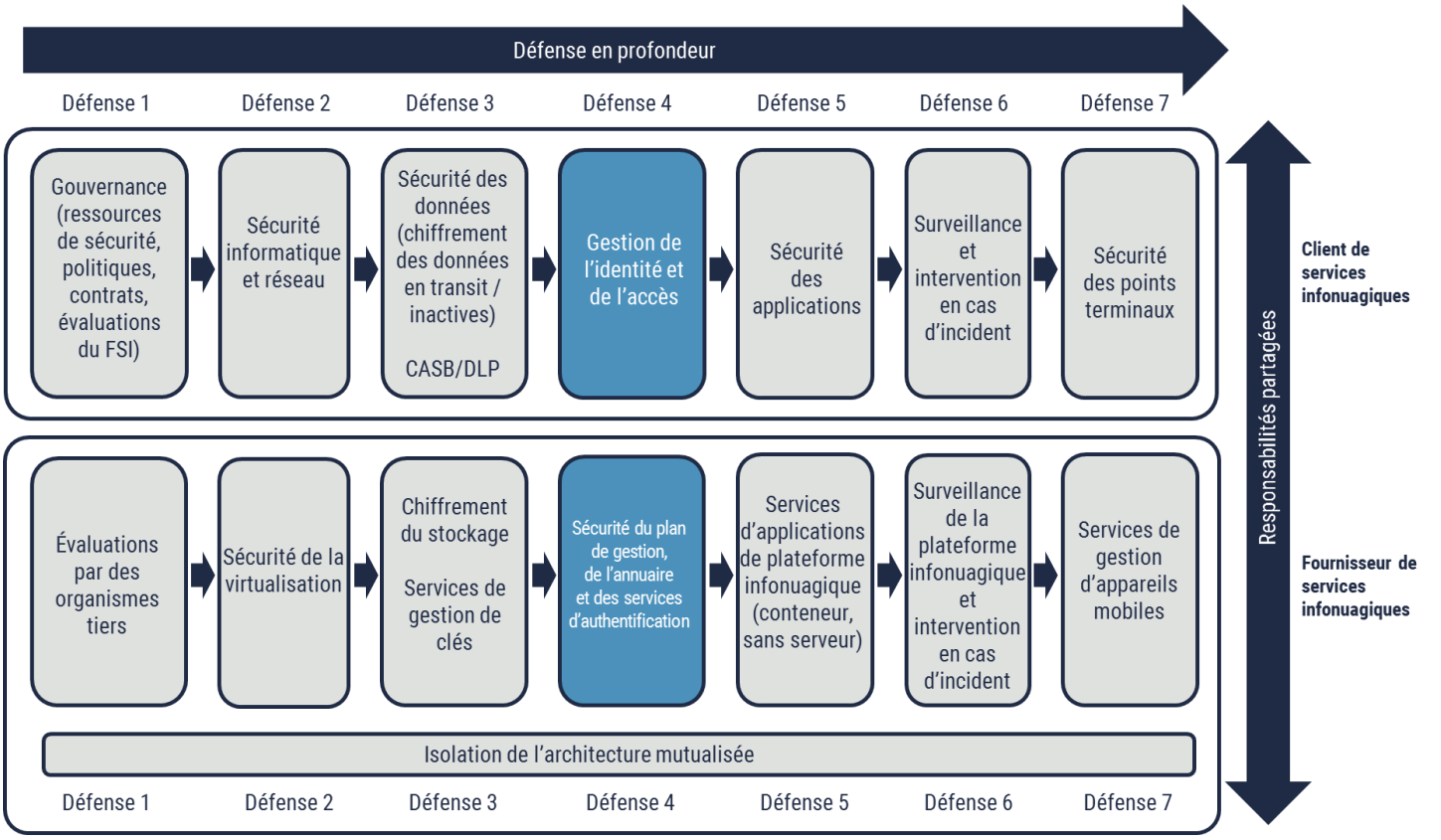

Figure 14 – Gestion de l'identité et de l'accès

La gestion de l'identité et de l'accès (GIA) constitue l'une des mesures de protection les plus importantes d'une stratégie de défense en profondeur. La GIA détermine qui peut faire quoi avec quelles ressources et dans quel contexte. Comme l'indique la figure 14, il s'agit d'un des éléments clés qui permet de contrôler l'accès aux ressources, aux applications et à l'information et de prévenir la compromission non intentionnelle ou malveillante des biens opérationnels essentiels.

4.6.1 RESPONSABILITÉS PARTAGÉES

Les responsabilités liées à la gestion de l'identité et de l'accès comportent notamment :

- l'établissement du fournisseur d'identité (IdP pour *Identity Provider*);
- la configuration du fournisseur d'identité dans les applications fondées sur l'infonuagique;
- l'inscription, l'attribution, la propagation, la gestion et la suppression d'identités d'utilisateurs;
- la création et la gestion des rôles d'accès;
- la gestion de l'accès aux ressources.

Dans le modèle IaaS, la gestion de l'identité et de l'accès revient principalement au client des services infonuagiques.

Dans les modèles PaaS et SaaS, la gestion de l'identité et de l'accès est une responsabilité partagée. En règle générale, les FSI sont responsables de la mise en œuvre des services d'annuaire et d'authentification, de la sécurité de l'interface de programmation d'applications (API pour *Application Program Interface*) et de la fonction d'audit. Les organisations sont responsables des politiques, des processus et des procédures de GIA, et de la configuration des capacités de GIA fournies par les FSI. Elles peuvent également choisir de tirer parti des services d'authentification unique (SSO pour *Single Sign-On*) et d'authentification multifactorielle (MFA pour *Multi-Factor Authentication*) des FSI ou d'autres organismes tiers.

Dans tous les modèles de service, il revient au FSI d'appliquer les autorisations et les contrôles d'accès du plan de gestion de la plateforme infonuagique.

4.6.2 PARTICULARITÉS

4.6.2.1 FÉDÉRATION

L'une des principales différences de la GIA en infonuagique est que le FSI et les organisations clientes se partagent les responsabilités. Dans un environnement infonuagique, la GIA comporte la gestion des identités de diverses organisations, et ces organisations doivent se faire confiance. La fédération de l'identité permet de répondre à ces besoins. Par fédération, on entend la délégation de la fonction d'authentification par une partie de confiance (PC) à un IdP. Par exemple, en déléguant la fonction d'authentification à un IdP, une application fondée sur le modèle SaaS utilisera l'assertion de l'identité du requérant par l'IdP pour exécuter la décision d'autorisation soit en accordant, soit en refusant l'accès à l'application. Ce processus permet aux organisations de fournir une assertion confirmant l'identité du requérant à l'application SaaS sans devoir révéler au FSI les justificatifs d'identité ou tout autre attribut de l'utilisateur. De multiples services locaux et infonuagiques peuvent faire confiance à l'assertion de l'identité du requérant fournie par l'IdP afin d'assurer la capacité d'authentification unique.

4.6.2.2 BESOIN ACCRU D'AUTHENTIFICATION FORTE

Les environnements TI locaux conventionnels dépendent d'un périmètre de confiance bien défini. Pour accéder aux applications et aux données, les utilisateurs doivent être sur le réseau local et devraient utiliser un dispositif géré par le client. Comme l'effectif est de plus en plus mobile et utilise souvent des appareils personnels, le périmètre de confiance conventionnel n'est pas efficace. En infonuagique, l'accès réseau est élargi par nature, ce qui signifie qu'on peut accéder aux services fondés sur l'infonuagique n'importe où et à partir de n'importe quel dispositif client. Dans le cas de la fédération pour l'authentification unique, la compromission des justificatifs d'un utilisateur pourrait permettre à un auteur de menace d'accéder à un plus grand nombre de services fondés sur l'infonuagique et de les compromettre à partir de n'importe quel lieu. Dans un tel environnement, l'authentification fondée sur un seul facteur (comme le nom d'utilisateur et le mot de passe) entraîne des risques très élevés.

Les organisations qui adoptent l'infonuagique devraient envisager l'authentification multifactorielle pour réduire le risque de compromission des comptes[17], tout particulièrement pour les comptes privilégiés et les systèmes opérationnels essentiels. Dans le cas des comptes privilégiés, nous recommandons aux organisations d'adopter des justificatifs et des mécanismes

[17] Pour de plus amples renseignements sur l'authentification multifactorielle, prière de consulter l'ITSP.30.031 (version 2) du Centre pour la cybersécurité, *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information* [16] et le document du NIST intitulé *Special Publication 800-63-3, Digital Identity Guidelines* [17].

d'authentification dont le niveau d'assurance est plus élevé[18] et de restreindre la gestion des charges de travail infonuagiques à l'aide d'un point d'accès distinct, d'un hôte bastion, ou les deux. Un hôte bastion est semblable à ce qu'on appelle un serveur intermédiaire (jump server ou jump host). Les deux ont pour fonction de contrôler l'accès et effectuer l'interface entre deux zones de niveaux de sécurité différents. Toutefois, un hôte bastion sépare spécifiquement un réseau non-sécurisé, comme le réseau Internet, et le réseau sécurisé privé qu'il protège.

4.6.2.3 NORMES ET PROTOCOLES

En règle générale, les environnements locaux dépendent de protocoles d'accès annuaire (p. ex. Lightweight Directory Access Protocol [LDAP] et Active Directory) et de protocoles d'authentification et d'autorisation (p. ex. Kerberos). Souvent, on doit pouvoir accéder aux environnements infonuagiques par Internet à partir de n'importe quel lieu et l'authentification doit passer par les pare-feux sans devoir modifier leur configuration. Le protocole d'authentification devrait également être en mesure de se rétablir à la suite de pannes de réseau Internet. Le langage SAML (Security Assertion Markup Language) et les standards ouverts OAuth et OpenID sont des normes et protocoles couramment pris en charge.

4.6.2.4 GESTION DE L'ACCÈS

La gestion de l'accès local conventionnel est généralement mise en œuvre à l'aide du contrôle d'accès basé sur les rôles (RBAC pour *Role-Based Access Control*). Le RBAC se fonde habituellement sur un seul attribut (rôle) pour autoriser l'accès. Cette approche n'offre pas la souplesse et la sécurité nécessaires pour les utilisateurs qui ont besoin d'accéder aux ressources à partir de n'importe où et depuis de multiples dispositifs. D'autres facteurs contextuels doivent être pris en compte dans les politiques et les décisions de gestion de l'accès, notamment la disponibilité et l'expertise du personnel de sécurité des TI de l'organisation ainsi que les exigences de sécurité des données et services organisationnels.

Dans le cas du contrôle d'accès basé sur les attributs (ABAC pour *Attribute-Based Access Control*), les décisions sont plus précises et axées sur le contexte. Autrement dit, les décisions sur le contrôle d'accès sont prises en tenant compte d'attributs multiples, comme le rôle, l'emplacement, le mode d'authentification, la conformité du dispositif, etc.[19]

Les services de GIA des FSI incluent normalement la prise en charge de l'ABAC. En tant que clientes de services infonuagiques, les organisations devraient privilégier les solutions ABAC plutôt que RBAC en raison de leur précision et de leur souplesse accrue pour la mise en œuvre de politiques et de décisions en matière d'accès dans un écosystème infonuagique en évolution rapide.

---

[18] Pour de plus amples renseignements sur le niveau d'assurance des justificatifs et de l'authentification, prière de consulter l'ITSP.30.031 (version 2) du Centre pour la cybersécurité, *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information* [16].

[19] Une explication plus détaillée de l'ABAC se trouve dans le document du NIST intitulé *Special Publication 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations* [18].

4.7 APPLICATIONS

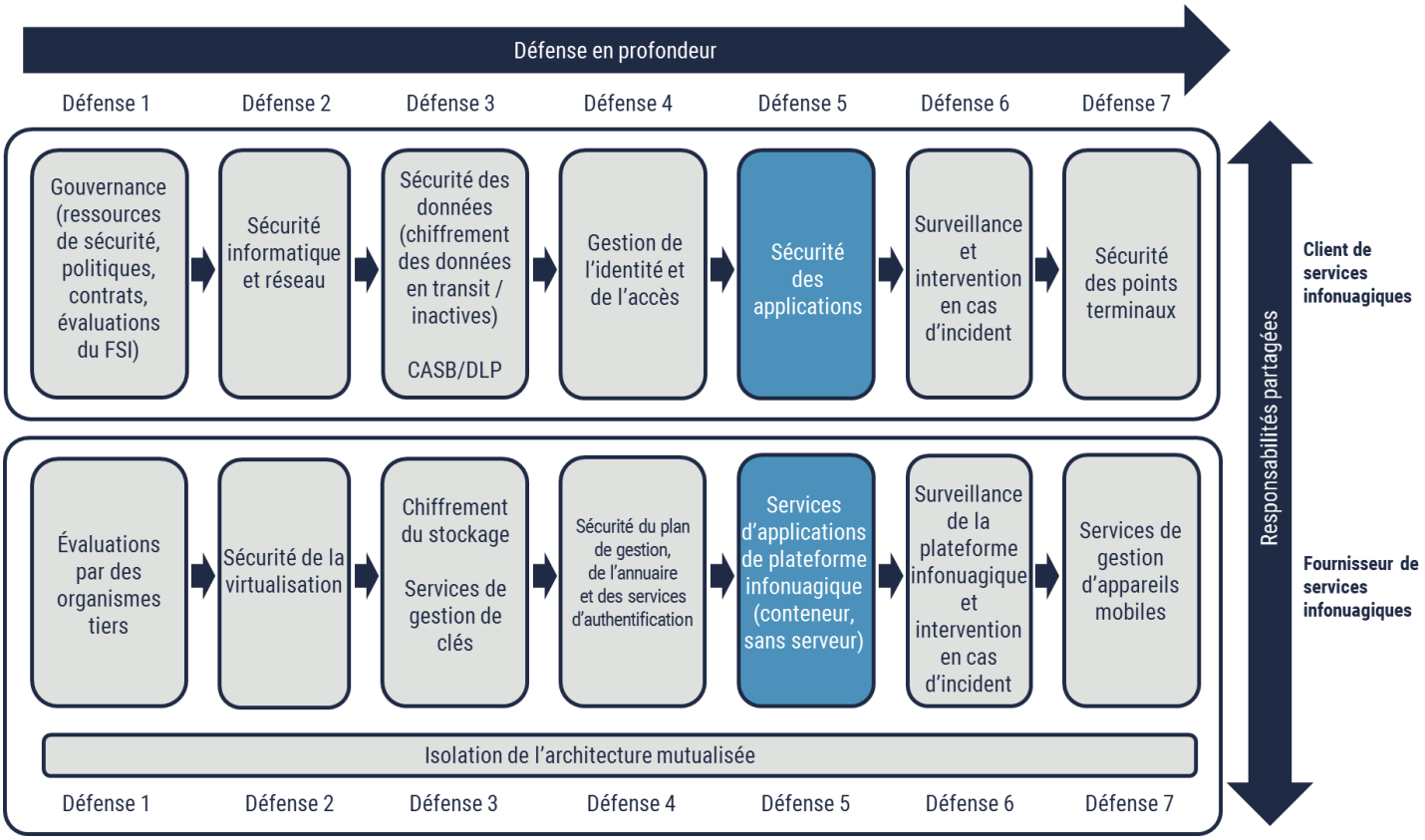

Figure 15 – Applications

4.7.1 RESPONSABILITÉS PARTAGÉES

Les responsabilités liées à la sécurité des applications comportent le développement d'applications sécurisées, l'analyse du code source, les tests de sécurité et de vulnérabilités, le déploiement sécurisé, la gestion des vulnérabilités d'exécution et la protection contre les menaces.

Dans le modèle SaaS, les FSI sont responsables de tous les aspects de la sécurité des applications alors que les organisations se chargent de configurer correctement ces services.

Dans les modèles IaaS et PaaS, les organisations sont responsables de la sécurité des applications. Les FSI fournissent les fonctions et services d'accès sécurisé, et les organisations doivent les configurer et établir les règles d'accès sécurisé, comme les droits accordés à des groupes et à des utilisateurs individuels.

4.7.2 PARTICULARITÉS

Si elles sont bien utilisées, les capacités infonuagiques peuvent améliorer la sécurité des applications. À cette fin, nous recommandons aux organisations d'apporter un certain nombre de changements aux politiques de développement d'applications, au cycle de vie du développement des logiciels, aux modèles de conception et aux opérations de sécurité.

Les organisations devraient développer une architecture de sécurité pour les applications infonuagique et préapprouver les modèles de conception de la sécurité des applications infonuagiques en prêtant une attention particulière aux éléments suivants : la sécurité des API, la sécurité du plan de gestion, le chiffrement, la GIA et les nouveaux modèles de sécurité infonuagique. Les organisations devront peut-être personnaliser ou mettre à jour les applications existantes avant de les migrer vers les services infonuagiques afin de les utiliser et de les sécuriser efficacement.

Les organisations devraient veiller à ce que le personnel de développement d'applications, des opérations et de la sécurité reçoivent la formation nécessaire sur les rudiments de la sécurité infonuagique et les services et capacités de sécurité techniques des fournisseurs de services infonuagiques.

Le document *Security Guidance for Critical Areas of Focus in Cloud Computing, version 4.0* [5] de la CSA présente en détail les différences propres à la sécurité des applications et les considérations liées à l'infonuagique. Voici quelques recommandations importantes en matière de sécurité[20] :

- passer à un processus de déploiement continu et automatiser la sécurité (y compris l'intégration des tests de sécurité dans le pipeline de déploiement);
- automatiser la sécurité dans le déploiement et les activités;
- surveiller les appels d'API au service infonuagique et au plan de gestion;
- veiller à ce que seuls les droits d'accès minimaux soient activés;
- tenir compte des fonctions, des services et des capacités de sécurité des plateformes infonuagiques des FSI dans les plans de sécurité;
- s'assurer qu'aucun justificatif statique intégré ne se trouve dans le code d'applications;
- avoir recours au KMS et au HSM pour l'information secrète et la gestion des clés;
- tirer parti de la sécurité et de l'architecture des microservices pour faciliter le verrouillage des charges de travail et réduire le nombre de services qui y sont exécutés;
- mettre à profit la sécurité et l'architecture de l'informatique sans serveur pour réduire la surface d'attaque.

[20] Pour obtenir des renseignements détaillés sur les particularités et les considerations liées à l'infonuagique, prière de consulter la section « Domain 10 » de la publication du CSA intitulée *Security guidance for critical areas of focus in cloud computing v4.0* [5].https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

4.8 SURVEILLANCE ET INTERVENTION EN CAS D'INCIDENT

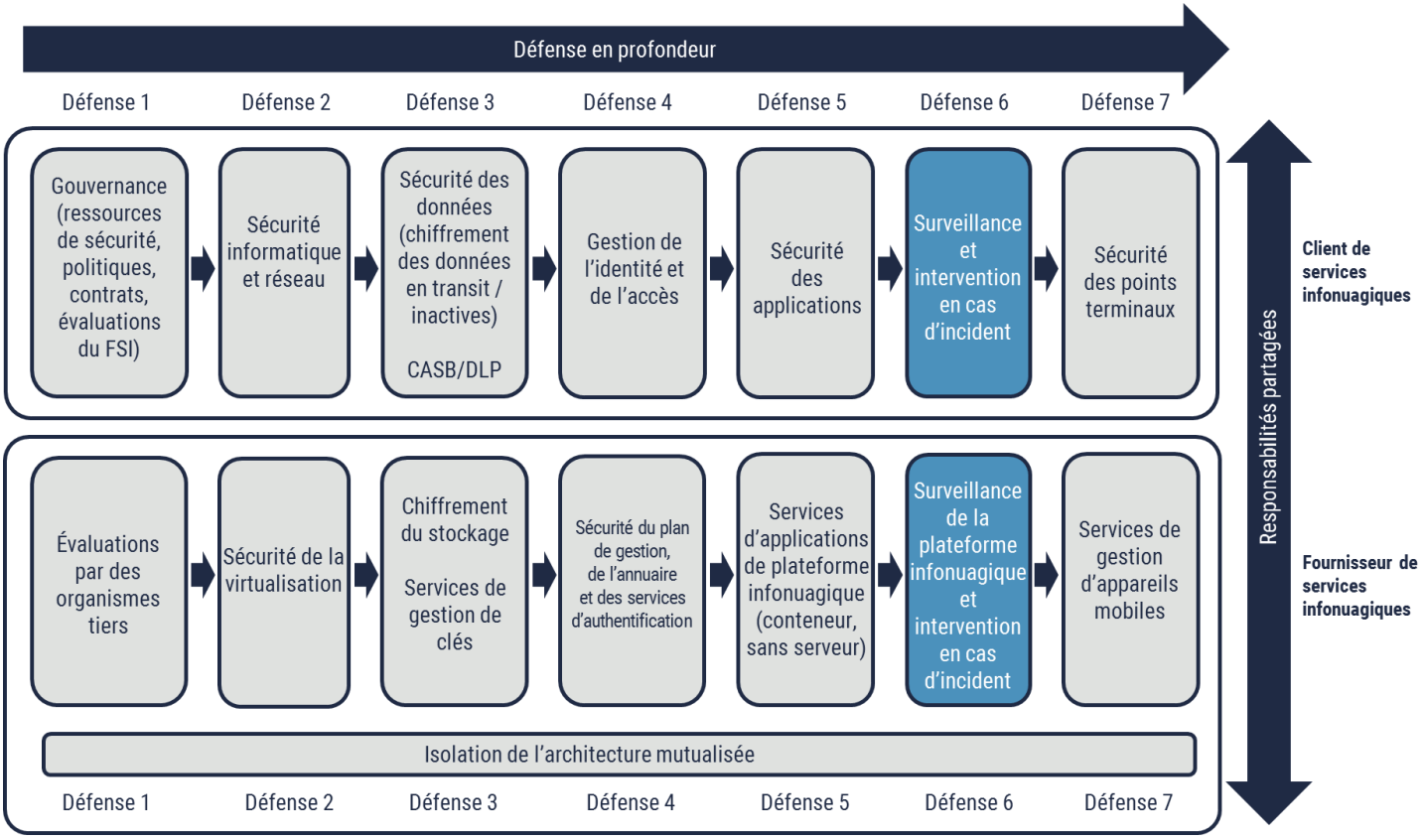

Figure 16 – Surveillance et intervention en cas d'incident

Comme on le voit à la figure 16, malgré tous les contrôles mis en œuvre afin de protéger l'environnement infonuagique, une bonne stratégie de défense en profondeur doit prévoir la surveillance de la sécurité et l'intervention en cas d'incident. Les organisations doivent mettre en place les politiques, le personnel, les procédures et les technologies nécessaires pour détecter les incidents de sécurité, intervenir, atténuer les conséquences et assurer la reprise des activités.

4.8.1 RESPONSABILITÉS PARTAGÉES

Le FSI et le client des services infonuagiques ont tous deux des responsabilités en matière de surveillance et d'intervention en cas d'incident. Le niveau de responsabilité varie selon le modèle de services (IaaS, PaaS, ou SaaS).

Il revient aux FSI de surveiller la plateforme infonuagique. Les FSI doivent informer les organisations clientes lorsque l'infrastructure où sont hébergés leurs services infonuagiques est touchée par un incident de sécurité et doivent établir un point de contact pour les communications liées à l'intervention en cas d'incident. Les FSI peuvent également offrir des options de surveillance de la sécurité qui peuvent appuyer les activités de surveillance et d'intervention en cas d'incident des organisations.

Dans un modèle IaaS, les organisations sont responsables de la surveillance des interfaces réseau et des appliances de sécurité virtuelles, des événements de sécurité de VM, des applications, des systèmes d'authentification, des bases de

données et des services infonuagiques qui leur sont fournis, y compris le plan de gestion et les événements de sécurité touchant les API. Les organisations sont responsables de mener les activités d'intervention en cas d'incident et d'aviser les utilisateurs touchés.

Dans le modèle PaaS, les organisations sont responsables de la surveillance des applications déployées dans le modèle PaaS, y compris le plan de gestion et les événements de sécurité touchant les API. Il leur revient également de mener les activités d'intervention en cas d'incident et d'aviser les utilisateurs touchés.

Dans le modèle SaaS, les responsabilités des organisations se limitent généralement à la surveillance de l'instance SaaS, à la notification des utilisateurs touchés et à la collaboration avec le FSI dans le cadre de la reprise des activités.

4.8.2 PARTICULARITÉS

L'adoption de l'infonuagique a des implications pour chaque étape de la surveillance et du cycle de vie de l'intervention en cas d'incident. Il faudra modifier l'approche d'intervention en cas d'incident en fonction de certains facteurs, notamment :

- la perte de contrôle en raison du modèle de responsabilités partagées;
- l'accord sur les niveaux de service, le temps de réponse et la coordination avec le FSI;
- l'absence possible d'un point de contact direct avec le fournisseur de service (il faudra peut-être utiliser le service de soutien standard);
- les instances de courte durée (qui ont une incidence sur la criminalistique et la journalisation);
- les lacunes possibles quant à la disponibilité des journaux et des données des composants qui relèvent des FSI;
- les avantages éventuels de l'automatisation infonuagique et des capacités d'isolation pour l'intervention en cas d'incident;
- la disponibilité d'outils du fournisseur de services à l'appui de l'intervention en cas d'incident.

Le tableau ci-dessous présente un résumé des considérations liées à la surveillance et à l'intervention en cas d'incident dans le contexte de l'infonuagique[21].

Phase du cycle de vie de la gestion des incidents	Considérations liées à la sécurité infonuagique
Préparation	• Comprendre l'ANS et la coordination avec le FSI. • Mettre à l'essai le processus d'intervention en cas d'incident avec le FSI. • Veiller à ce que la transmission de demandes à des niveaux supérieurs et les rôles et responsabilités soient clairs. • Veiller à ce que le FSI ait les coordonnées des personnes avec qui communiquer s'il détecte des incidents et à ce que ces avis soient intégrés aux processus de l'organisation.

[21] L'information présentée dans le tableau est tirée de la section « Domain 9 » de la publication du CSA intitulée *Security guidance for critical areas of focus in cloud computing v4.0* [5].
https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

Phase du cycle de vie de la gestion des incidents	Considérations liées à la sécurité infonuagique
	• Tenir à jour les coordonnées des personnes-ressources du FSI et en faire l'essai (y compris à l'aide de méthodes hors bande). • Comprendre et documenter les données et les journaux qui seront disponibles pour chaque service en cas d'incident. • Structurer l'architecture de l'environnement infonuagique de manière à accélérer la détection, l'enquête et l'intervention.
Détection et évaluation	• S'assurer que la portée de la surveillance inclut les activités du plan de gestion du nuage. • Avoir recours à la surveillance et aux alertes intégrées au nuage pour accélérer le processus d'intervention. • Intégrer les journaux des plateformes infonuagiques aux activités de sécurité et de surveillance de l'organisation. • Comprendre les éléments journalisés et les lacunes qui pourraient avoir une incidence sur l'analyse de l'incident. • Ouvrir fréquemment des sessions dans les charges de travail pour combler le manque de visibilité des journaux des plateformes infonuagiques. • Comprendre les éventuels problèmes liés à la chaîne de possession dans le contexte de la criminalistique et du soutien des enquêtes. • Automatiser les processus de criminalistique ou d'enquête dans les environnements infonuagiques pour composer avec le caractère dynamique et la grande vitesse des charges de travail infonuagiques (p. ex. instantanés de VM). • Mettre à profit les capacités de la plateforme infonuagique pour déterminer l'étendue d'une éventuelle compromission (p. ex. flux réseau, données de configuration, journaux d'accès).
Confinement, atténuation et reprise	• S'assurer qu'aucun attaquant ne se trouve dans le plan de gestion infonuagique. • Avoir recours aux capacités des plateformes infonuagiques pour accélérer la mise en quarantaine, l'éradication et la reprise des activités. • Confirmer que les modèles et la configuration des nouvelles applications de l'infrastructure n'ont pas été compromis.
Activité après l'événement	• Collaborer avec l'équipe d'intervention de l'organisation et le FSI pour déterminer ce qui s'est bien passé et ce qui n'a pas bien été. • Si le temps de réponse, les données ou tout autre soutien qui avait été convenu n'ont pas été adéquats, envisager de renégocier les ANS.

4.9 SÉCURITÉ DES POINTS TERMINAUX

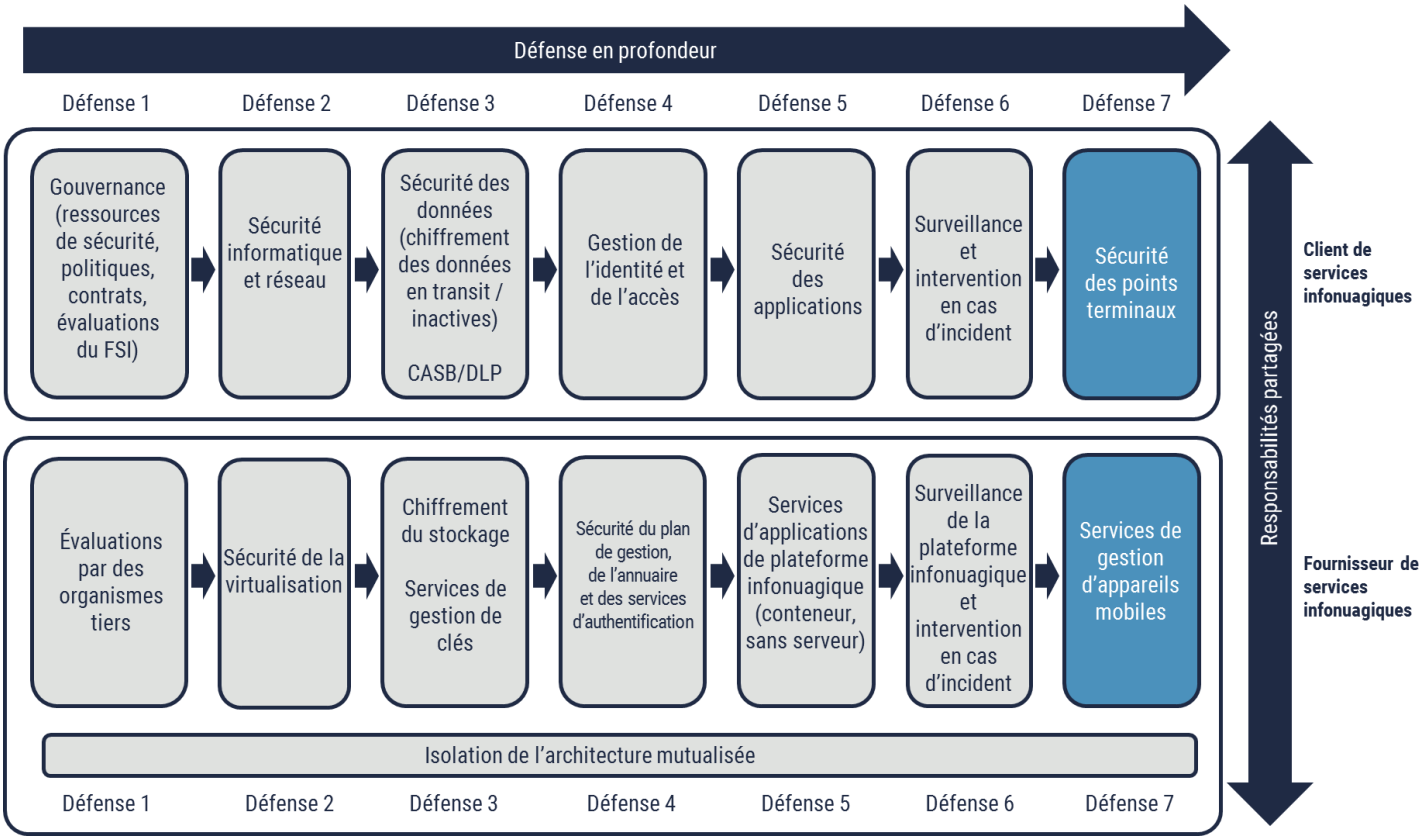

Figure 17 – Sécurité des points terminaux

Les organisations sont toujours responsables de la sécurité des points terminaux, c'est-à-dire les dispositifs avec lesquels les utilisateurs accèdent aux services infonuagiques. Cela dit, les FSI offrent parfois des solutions de gestion des postes mobiles (MDM pour *Mobile Device Management*) fondées sur l'infonuagique qui permettent de gérer les points terminaux. Dans de tels cas, les organisations sont responsables de la définition des exigences de sécurité des dispositifs, et le FSI se charge d'appliquer ces exigences par l'intermédiaire de la solution MDM.

5 RÉSUMÉ

Dans le cadre de la défense en profondeur, il importe que les organisations structurent adéquatement leur stratégie de déploiement en nuage. Pour établir une architecture efficace, les organisations doivent être conscientes des responsabilités partagées, du déploiement en nuage, des modèles de service, des menaces, des vulnérabilités, de l'architecture de la plateforme infonuagique et des capacités de sécurité. L'ITSP.50.104 peut aider votre organisation à comprendre les considérations architecturales nécessaires pour favoriser le déploiement sécurisé des services opérationnels sur les plateformes infonuagiques.

5.1 AIDE ET RENSEIGNEMENTS

Si votre organisation a besoin de conseils sur la défense en profondeur pour les services infonuagiques et souhaite obtenir de plus amples renseignements, veuillez communiquer avec :

Centre d'appel du Centre pour la cybersécurité
contact@cyber.gc.ca
613-949-7048

6 CONTENU COMPLÉMENTAIRE

6.1 LISTE D'ABRÉVIATIONS, D'ACRONYMES ET DE SIGLES

Terme	Définition
API	Interface de programme d'application (*Application Programming Interface*)
Centre pour la cybersécurité	Centre canadien pour la cybersécurité
CE	Effacement cryptographique (*Crypto Erase*)
CSA	Cloud Security Alliance
CST	Centre de la sécurité des télécommunications
FSI	Fournisseur de services infonuagiques
GC	Gouvernement du Canada
GFI	Gestion fédérée de l'identité
HSM	Module de sécurité matériel (*Hardware Security Module*)
HTTP	Protocole de transfert hypertexte (*Hypertext Transfer Protocol*)
HTTPS	Protocole de transfert hypertexte sécurisé (*Hypertext Transfer Protocol Secure*)
KEK	Clé de chiffrement de clés (*Key Encryption Key*)
KMS	Service de gestion de clés (*Key Management Service*)
MDM	Gestion des postes mobiles (*Mobile Device Management*)
MFA	Authentification multifactorielle (*Multi-Factor Authentication*)
NIPS	Système de prévention des intrusions réseau (*Network Intrusion Prevention System*)
NIST	National Institute of Standards and Technology
NVA	Appliance réseau virtuelle (*Network Virtual Appliance*)
SAML	Langage SAML (*Security Assertion Markup Language*)
SDN	Réseau à définition logicielle (*Software Defined Network*)
SMB	Bloc de messages de serveur (*Server Message Block*)
SSO	Authentification unique (*Single Sign-On*)
STI	Sécurité des technologies de l'information
TI	Technologie de l'information
VM	Machine virtuelle (*Virtual Machine*)

6.2 GLOSSAIRE

Terme	Définition
Architecture mutualisée	Répartition de ressources physiques ou virtuelles de manière à ce que les multiples locataires et leurs données et services informatiques soient isolés les uns des autres et donc inaccessibles aux autres locataires.
Authentification multifactorielle	Caractéristique d'un système d'authentification ou d'un jeton qui fait intervenir plus d'un facteur d'authentification. Les trois types de facteurs d'authentification sont les suivants : un élément que l'utilisateur connaît, un élément que l'utilisateur possède et un élément qui caractérise la personne de l'utilisateur.
Charge de travail	Unité de traitement pouvant se trouver dans une machine virtuelle, un conteneur ou toute autre abstraction.
Clé de chiffrement de clés (KEK)	Clé servant à chiffrer et à déchiffrer d'autres clés aux fins de protection de la confidentialité. Voir aussi *enveloppement de clés*.
Disponibilité du stockage	Temps de disponibilité du service de stockage, c'est-à-dire que le système de stockage est fonctionnel et en mesure de livrer des données sur demande. Cette fonction est normalement assurée par la redondance du matériel.
Durabilité du stockage	Protection à long terme des données, c'est-à-dire que les données stockées ne sont pas détériorées, dégradées ou autrement corrompues. Elle porte sur la redondance des données plutôt que la redondance du matériel, de manière à éviter la perte ou la compromission des données.
Effacement cryptographique	Processus de nettoyage consistant à effacer la clé de chiffrement qui est employée sur un support chiffré pour rendre les données illisibles.
Fournisseur d'identité (IdP pour *Identity Provider*)	Partie qui gère les justificatifs d'authentification principaux d'un abonné et qui produit des assertions en fonction de ces justificatifs.
Nettoyage	Processus consistant à retirer les données d'un support avant de réutiliser ce support dans un environnement dont le niveau de protection n'est pas acceptable pour les données qui s'y trouvaient avant le nettoyage. Les ressources TI doivent être nettoyées avant d'être dispensées des contrôles d'information classifiée ou d'être utilisées dans un niveau de classification inférieur.
OAuth	Standard d'autorisation de l'IETF largement répandu dans les services Web (y compris les services à la clientèle). OAuth est basé sur HTTP.
OpenID	Standard d'authentification fédérée largement pris en charge pour les services Web. Il est basé sur HTTP et les URL servent à identifier le fournisseur d'identité et l'utilisateur/l'identité (p. ex. identité.fournisseurdidentité.com).
Organisation cliente	Organisation souhaitant obtenir un service infonuagique auprès d'un FSI pour mettre en œuvre un service dans le nuage.
Plan de gestion	Partie d'un système qui effectue la configuration et la surveillance de toutes les couches du système et qui fournit des services de gestion, de surveillance et de configuration à ces couches.
Résidence des données	Emplacement physique ou géographique des données numériques inactives d'une organisation.
Security Assertion Mark-up Language (SAML)	Standard d'OASIS pour la gestion fédérée de l'identité qui prend en charge l'authentification ainsi que l'autorisation. Il utilise le langage XML pour faire des assertions entre un fournisseur d'identité et une partie de confiance. Ces assertions peuvent comporter des énoncés portant sur l'authentification, les attributs et les décisions sur l'autorisation.

6.3 RÉFÉRENCES

Numéro	Référence
[1]	Centre canadien pour la cybersécurité, *Gestion des risques liés à la sécurité infonuagique (ITSM.50.062)*, mars 2019.
[2]	Centre canadien pour la cybersécurité, *Guide sur la catégorisation de la sécurité des services fondés sur l'infonuagique (ITSP.50.103)*, mai 2020.
[3]	National Institute of Standards and Technology (NIST), *Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing*, décembre 2011.
[4]	National Institute of Standards and Technology (NIST), *Special Publication 500-292, Cloud Computing Reference Architecture*, septembre 2011.
[5]	Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing*, *version 4.0* (https://cloudsecurityalliance.org/download/security-guidance-v4), 2017.
[6]	Centre canadien pour la cybersécurité, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33), décembre 2014.
[7]	National Institute of Standards and Technology (NIST), *Special Publication 800-145, The NIST Definition of Cloud Computing*, septembre 2011.
[8]	Cloud Standard Customer Council, *Practical Guide to Hybrid Computing V3.0*, 2017.
[9]	Commissariat à la protection de la vie privée du Canada, *L'infonuagique pour les petites et moyennes entreprises*, juin 2012.
[10]	Secrétariat du Conseil du Trésor du Canada, *Approche et procédures de gestion des risques à la sécurité de l'informatique en nuage*, 2018.
[11]	Centre canadien pour la cybersécurité, *Processus d'évaluation de la sécurité des technologies de l'information s'appliquant aux fournisseurs de services infonuagiques (ITSM.50.100)*, octobre 2018.
[12]	National Institute of Standards and Technology (NIST), *Special Publication 800-146, Cloud Computing Synopsis and Recommendations*, mai 2012.
[13]	Centre canadien pour la cybersécurité, *Guide sur le chiffrement de données en infonuagique (ITSP.50.106)*, mai 2020.
[14]	National Institute of Standards and Technology (NIST), *Special Publication 800-88, Guidelines for Media Sanitization*, septembre 2006.
[15]	Centre canadien pour la cybersécurité, *Nettoyage des supports de TI (ITSP.40.006, version 2)*, juillet 2017.
[16]	Centre canadien pour la cybersécurité, *Guide sur l'authentification des utilisateurs dans les systèmes de TI (ITSP.30.031, version 2)*, août 2016.
[17]	National Institute of Standards and Technology (NIST), *Special Publication 800-63-3, Digital Identity Guidelines*, juin 2017.
[18]	National Institute of Standards and Technology (NIST), *Special Publication 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, janvier 2014.