Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Chancellerie fédérale ChF

Secteur Transformation numérique et gouvernance de l'informatique TNI

Principes relatifs à l'informatique en nuage de l'administration fédérale, AR010, version 1.2

Directive du secteur Transformation numérique et gouvernance de l'informatique (secteur TNI)

fondée sur l'art. 40 de l'ordonnance du 1er mai 2025 sur la numérisation (ONum)

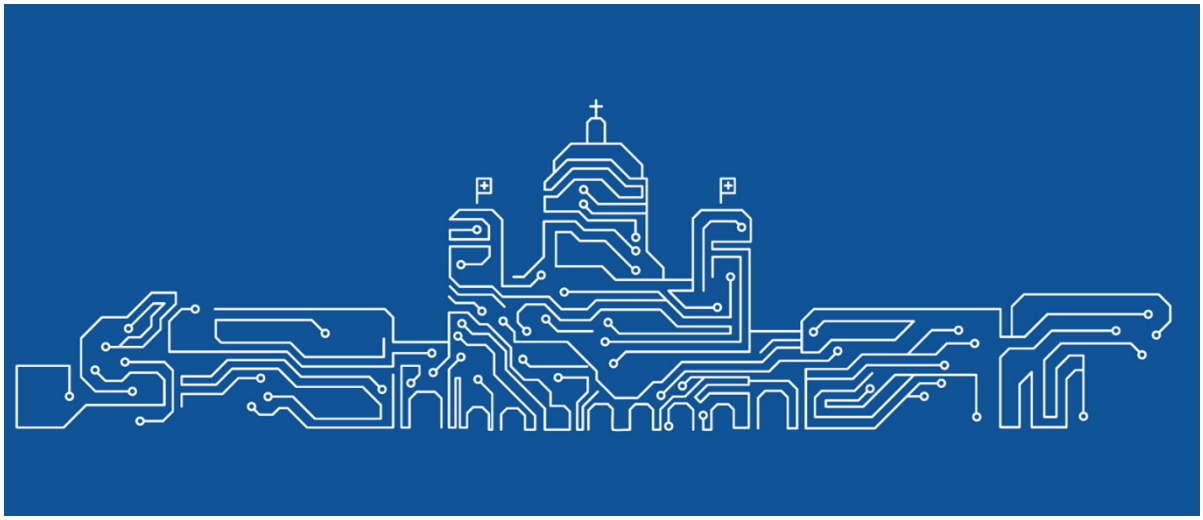


Figure 0 : logo des directives TNI

1 Résumé

1.1 À qui s’adresse le présent document ?

Le présent document s’adresse aux unités de l’administration fédérale centrale.

1.2 Quel est son objet ?

Il vise à permettre une utilisation sûre, efficace et ordonnée des services en nuage dans l’administration fédérale, qui soit un gage d’innovation, de modularité et de protection des données.

1.3 Que règle-t-il ?

Il règle la gouvernance du nuage (privé et public) de l’administration fédérale et fixe les lignes directrices que doit suivre la mise en œuvre de la stratégie d’informatique en nuage.

1.4 Quels sont ses objectifs ?

Les départements et les unités administratives utilisent les services infonuagiques selon des principes uniformes, dans la mesure où ceux-ci sont des directives (contraignantes).

Les départements / unités administratives sont assistés dans le choix du nuage de niveau adéquat pour leurs applications.

Les intermédiaires se fondent sur des principes uniformes.

Table des matières

Annexes

2 Dispositions générales

La stratégie d'informatique en nuage de l'administration fédérale [1], adoptée par le Conseil fédéral le 11 décembre 2020, vise à faciliter l'utilisation des services en nuage. Conformément à sa stratégie, la Confédération utilise les services en nuage (privé et public) **de manière sûre, efficace et ordonnée**.

Conformément à sa stratégie, l'administration fédérale mise toujours sur ses propres centres de données (cf. la stratégie sur les centres de données de l'administration fédérale civile [24]) et sur les nuages privés de la Confédération. Cette palette est complétée par les nuages publics de plusieurs fournisseurs. Cette **stratégie hybride**, qui combine nuages privés et nuages publics, couvre particulièrement bien l'ensemble des exigences de l'administration, notamment pour ce qui est de la sécurité de l'information, de la protection des données, de la résilience, de l'innovation, de la fonctionnalité, de la criticité et du degré d'intégration optimal.

Le présent document comprend

- trois directives du secteur Transformation numérique et gouvernance de l'informatique (TNI) de la Chancellerie fédérale (ChF) pertinentes pour le nuage (cf. ch. 5.1),
- des renvois à des documents pertinents dans ce domaine, élaborés par d'autres organes, et des recommandations du secteur TNI de la ChF (cf. ch. 5.2)

Il règle l'utilisation des services d'informatique en nuage public et privé dans l'administration fédérale. Les présents principes visent à harmoniser les pratiques au sein de l'administration fédérale.

2.1 Objet

1. Les principes relatifs à l'informatique en nuage règlent l'utilisation des services en nuage public dans l'administration fédérale aux niveaux *Infrastructure as a Service* (IaaS) et *Platform as a Service* (PaaS).
2. Ils s'adressent aux fournisseurs de prestations, aux bénéficiaires de prestations et à leurs responsables d'applications, conformément au champ d'application.
3. Ils sont groupés par thème et décrits au ch. 4 (cf. figure 1).

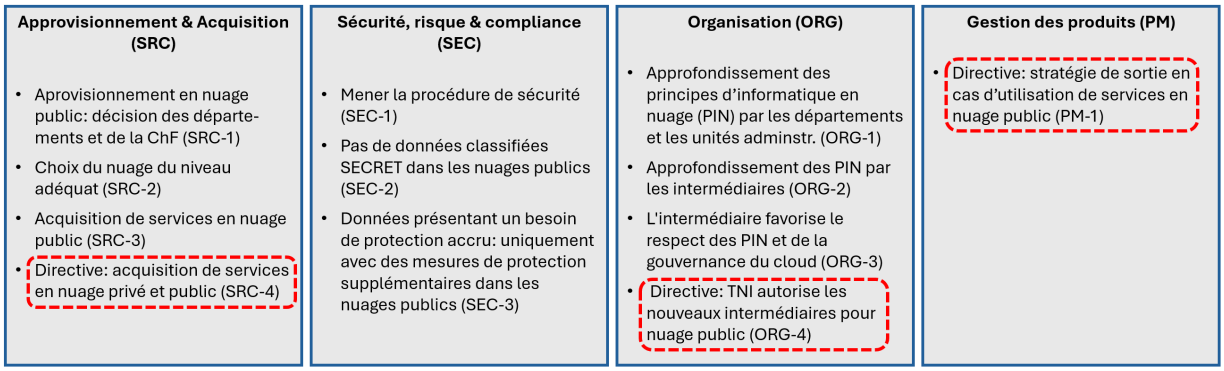


Figure 1 : vue d'ensemble des principes de l'informatique en nuage de l'administration fédérale

Les principes SRC-4, ORG-4 et PM-1 encadrés en rouge sont des directives du secteur TNI ; ils sont exposés au ch. 5.1. Les autres ont valeur de renvois à des documents complémentaires élaborés par d'autres organes, d'informations et de recommandations ; ils sont groupés par thème au ch. 5.2.

2.2 Champ d'application

1. Les principes relatifs à l'informatique en nuage s'appliquent aux unités de l'administration fédérale centrale.
2. Les principes SRC-4, ORG-4 et PM-1 sont des directives du secteur TNI de la ChF et, en tant que telles, contraignants.

2.3 Objectifs

Les principes relatifs à l'informatique en nuage visent les objectifs suivants :

1. Les départements et les unités administratives utilisent les services infonuagiques selon des principes uniformes, dans la mesure où ceux-ci sont des directives (contraignantes).
2. Les départements / unités administratives sont assistés dans le choix du nuage de niveau adéquat pour leurs applications.
3. Les intermédiaires se fondent sur des principes uniformes.

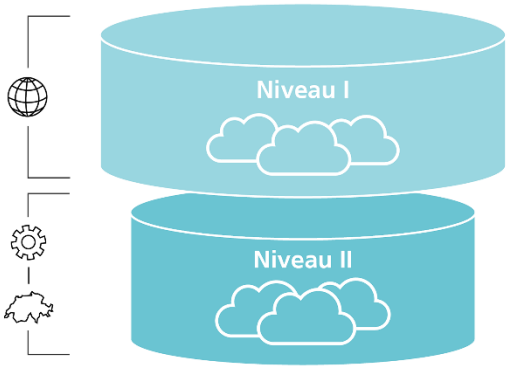
Le présent document se concentre sur les questions de gouvernance. Il vise à répondre aux questions suivantes :

- Quels sont les différents niveaux de protection des données et de sécurité de l'information pour l'utilisation du nuage au sein de l'administration fédérale (ch. 3) ?
- Sur quelles bases se fondent les principes de l'informatique en nuage de l'administration fédérale (ch. 4) ?
- Quels sont les principes de l'informatique en nuage que le secteur TNI de la ChF édicte sous forme de directives contraignantes pour toute l'administration fédérale (ch. 5) ?

3 Utilisation de l’informatique en nuage dans l’administration (modèle des niveaux)

Plusieurs options d’approvisionnement s’offrent aux unités administratives qui souhaitent faire usage de services de nuages privés ou publics. Le modèle des niveaux de l’informatique en nuage favorise une compréhension commune de ces solutions. Il aide les unités administratives à choisir la solution qui leur convient le mieux.

Les différents niveaux représentés dans la figure 2 se distinguent non seulement par leurs fonctionnalités, mais aussi par le type de données qui peuvent y être traitées. En général, plus le niveau est élevé, plus le besoin de protection des données est important. De plus, les niveaux s’additionnent en ce qui concerne le besoin de protection, c’est-à-dire que chaque nouveau niveau doit remplir les critères définis aux niveaux inférieurs.



Nuage public
- Nuage public avec un maximum de fonctionnalités[1]
- Protection des données et sécurité de l’information[2] :
  - respect au minimum de la protection informatique de base
  - respect de la LPD et de la LSI
  - législation internationale (Cloud Act, règlement e-evidence, etc.)
- Conservation et traitement des données au niveau global[3]

Nuage public Suisse
- Nuage public avec fournisseurs nationaux et internationaux
- Protection des données et sécurité de l’information[2] :
  - respect d’exigences élevées de la LPD et de la LSI
  - contrat de droit suisse et for juridique en Suisse (CLOUD Act, règlement e-evidence, etc., ne sont pas exclus)
- Conservation et traitement des données[3] sur le territoire suisse ou avec des mesures contractuelles, techniques ou organisationnelles supplémentaires

Nuage privé Confédération
- Nuage privé dans l’environnement fédéral destiné à de nombreux domaines d’application
- Protection des données et sécurité de l’information[2] :
  - respect d’exigences élevées de la LPD et de la LSI
  - législation suisse et for juridique en Suisse
- Conservation et traitement des données[3] sur des infrastructures fédérales renforcées conformes aux directives de la Confédération[4]
- Exploitation par du personnel ayant passé un contrôle de sécurité

Nuage privé sécurisé Confédération
- Nuage privé sécurisé dans l’environnement fédéral avec isolement physique[5] à tous les niveaux
- Protection des données et sécurité de l’information[2] :
  - respect d’exigences élevées de la LPD et de la LSI
  - législation suisse et for juridique en Suisse
  - pour les exigences de sécurité élevées à très élevées (LOA4 selon I050 / niveau de confiance 4 selon eCH-0170)
  - Conservation et traitement des données[3] sur des infrastructures fédérales renforcées dédiées conformes aux directives de la Confédération[6]
- Exploitation uniquement par du personnel de la Confédération ayant passé un contrôle de sécurité

Pas de nuage: il y a encore des applications de la Confédération qui sont exploitées exclusivement dans des centres de données de la Confédération.

1) L’informatique en périphérie (edge computing) est possible à tous les niveaux.
2) Soutien par des mesures contractuelles, techniques et organisationnelles au niveau des applications spécialisées
3) La conservation et le traitement des données se rapportent aux données personnelles et aux données métier (sans télémétrie).
4) Zones de serveur Basic Confédération & Basic Plus Confédération
5) Il existe une option pour l’isolement physique de mandants.
6) Zone de serveur Plus Enhanced Confédération

Figure 2 : utilisation de l’informatique en nuage dans l’administration fédérale (cf. aussi le cadre juridique [3])

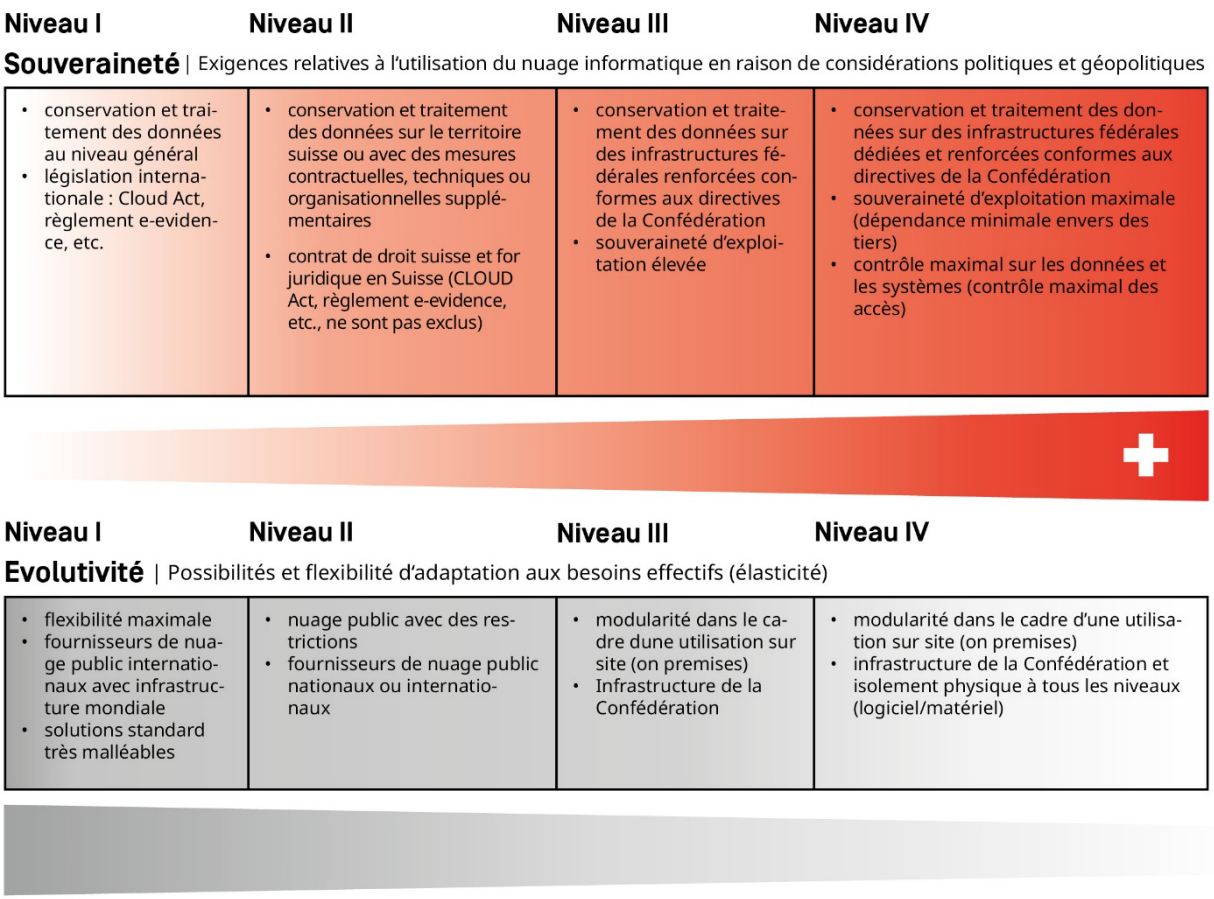
Lorsque l’administration fédérale utilise des services en nuage privé ou public, la souveraineté numérique, la sécurité de l’information et la protection des données sont cru-

ciales, de même que la fonctionnalité et la modularité. Les unités administratives doivent donc accorder la plus grande attention à ces aspects et tenir compte des compromis faits en la matière.

L'administration fédérale classifie les informations en fonction de leur besoin de protection dans les échelons suivants : « interne », « confidentiel » ou « secret » (cf. art. 13 de la loi sur la sécurité de l'information [4]). Elle vérifie en outre si les informations contiennent des données personnelles, voire des données sensibles (cf. loi fédérale sur la protection des données [5]) ou si elles doivent être protégées pour d'autres motifs (lois spéciales, secret de fonction).

L'unité administrative responsable vérifie notamment, pour chaque application, les bases légales pertinentes, le besoin de protection et les risques potentiels, conformément aux directives départementales. Se fondant sur les résultats de ces analyses, elle choisit l'option d'approvisionnement ou le niveau d'informatique en nuage qui convient, avec les mesures de protection nécessaires.

La limite entre les différents niveaux n'est cependant pas strictement définie. Il se peut par exemple qu'une application fonctionne en mode hybride sur des nuages de différents niveaux, avec des données sensibles stockées dans un nuage privé et des services qui utilisent des données non critiques proposés dans un nuage public. On notera toutefois que les solutions complexes entraînent des risques supplémentaires, tels qu'une mauvaise catégorisation des données.



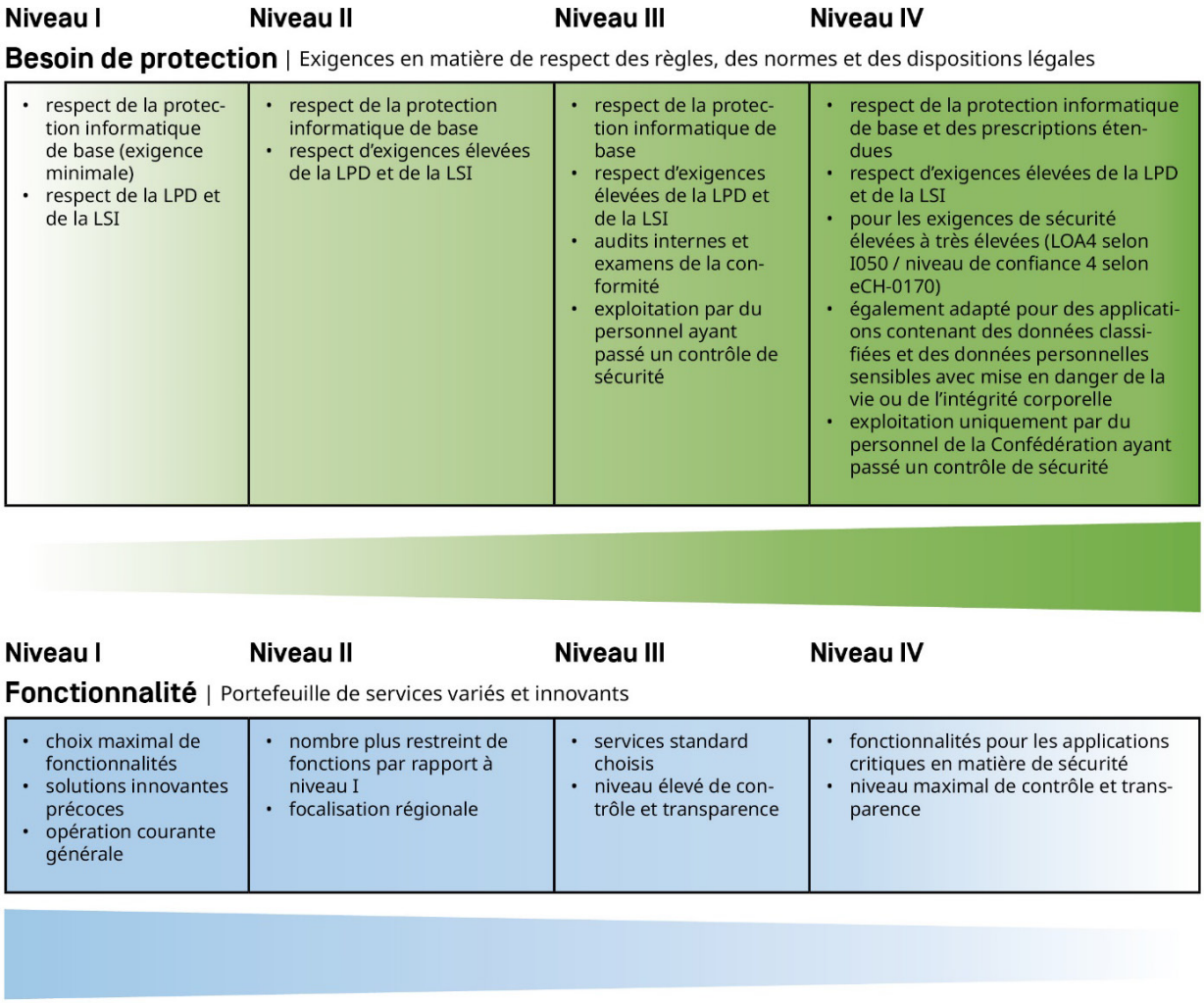


Figure 3 : vue d'ensemble des niveaux d'informatique en nuage en fonction des quatre dimensions pertinentes et des compromis dont elles font l'objet.

4 Gouvernance du nuage et principes

Les principes de l'informatique en nuage reposent sur deux éléments :

1. la gouvernance du nuage définit la façon dont la Confédération organise et pilote l'utilisation du nuage ;
2. les principes tirés de la stratégie d'informatique en nuage constituent la base des principes de l'informatique en nuage décrits au ch. 5.

Les bases et les principes essentiels de la stratégie d'informatique en nuage de l'administration fédérale [1] sont reproduits ci-après. Ils ont été adaptés conformément aux connaissances actuelles.

4.1 Gouvernance du nuage : interaction organisationnelle

Des mesures contractuelles, organisationnelles et techniques s'imposent afin que l'administration fédérale utilise les services en nuage public et privé de manière sûre, efficace et ordonnée. La figure 4 illustre le modèle cible organisationnel.

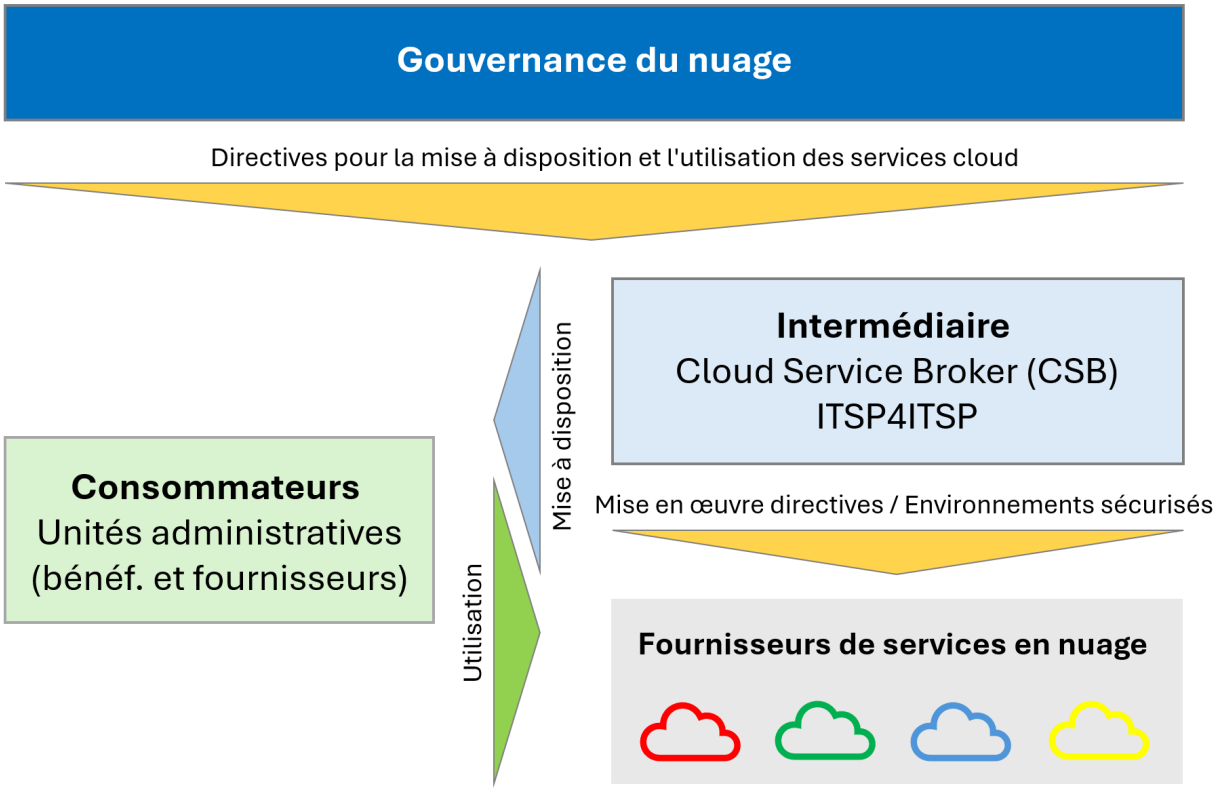


Figure 4 : Directives sur la gouvernance du cloud pour la mise à disposition de services cloud

Les fonctions représentées à la figure 4 sont précisées ci-après :

- **Gouvernance du nuage :** le secteur TNI de la ChF définit les principes de l'informatique en nuage qui doivent être respectés lors de l'utilisation de services en nuage privé et public, et décide des exceptions éventuelles. Il met à disposition d'autres outils de manière centralisée. Les départements, la ChF et les intermédiaires explicitent et élargissent la gouvernance dans leur domaine de responsabilité.

Le secteur TNI veille aussi à ce que les offres des fournisseurs de services en nuage et des intermédiaires soient conformes au modèle des niveaux. En cas de doute ou de différend, c'est le délégué TNI qui tranche après avoir entendu le conseil TNI. Les unités administratives restent responsables du choix du niveau adéquat, dans le respect de la gouvernance générale.

- **Intermédiaire :** l'intermédiaire ou *Cloud Service Broker* (CSB) soutient les unités administratives dans l'utilisation sûre, efficace et ordonnée des services d'informatique en nuage privé et public. Il peut expliciter et élargir les principes relatifs à l'informatique en nuage dans son domaine de compétence. Il conseille sur le choix d'un nuage de niveau adéquat pour les applications. Il fournit en outre des environnements sécurisés (« zones d'atterrissage » [7]) pour les projets infonuagiques dans lesquels des applications peuvent être développées et exploitées. Le secteur TNI de la ChF définit les exigences applicables aux intermédiaires dans leur cahier des charges, en accord avec le fournisseur de prestations.
  L'actuel CSB de l'Office fédéral de l'informatique et de la télécommunication (OFIT) joue le rôle d'intermédiaire de l'administration fédérale pour les commandes de services en nuage public (niveaux I et II) dans le cadre de l'appel d'offres OMC 20007. Avec le *Swiss Government Cloud* (SGC), l'OFIT assume le rôle d'intermédiaire de l'administration fédérale pour les services en nuage privé et public (niveaux I à III). L'offre de l'intermédiaire du SGC comprend le modèle « fournisseur de prestations informatiques pour un fournisseur de prestations informatiques » (ITSP4ITSP). Le CSB du Centre de services informatiques du Département fédéral de justice et police (CSI-DFJP) est l'intermédiaire de l'administration fédérale pour le nuage privé sécurisé (niveau IV). Il existe en outre pour le nuage public (niveaux I et II) des CSB dédiés qui couvrent les besoins spécifiques de certains départements ou offices fédéraux ou des domaines spécialisés (fin 2025 : Swisstopo, MétéoSuisse).
- **Fournisseur de services en nuage :** cette fonction est responsable de l'exploitation des services infonuagiques. Ce rôle est assuré par les fournisseurs de nuages privés et publics.
- **Consommateurs de services en nuage :** les unités administratives (bénéficiaires et fournisseurs de prestations) sont responsables de l'exploitation des applications spécialisées dans le nuage.

4.2 Principes

Les principes stratégiques constituent la base des principes relatifs à l'informatique en nuage décrits au ch. 4. Ils découlent de la stratégie d'informatique en nuage de l'administration fédérale [2] et ont été complétés ponctuellement.

Principe S-1 : options d'approvisionnement stratégiques

L'administration fédérale dispose de plusieurs options d'approvisionnement : elle peut traiter et stocker des données et exploiter des applications dans les nuages publics de grands fournisseurs internationaux ou de fournisseurs locaux, dans des nuages communautaires, dans les nuages privés internes, dans les centres de données de la Confédération (cf. la stratégie sur les centres de données de l'administration fédérale civile [24]) et dans les centres de données de partenaires d'externalisation classiques

(utilisation de services gérés, externalisation de services d'exploitation, etc.). Avec le SGC, le Conseil fédéral et le Parlement entendent en outre permettre à l'administration fédérale de couvrir la plupart de ses activités en nuage des niveaux I à III grâce à une solution cohérente (« Message concernant un crédit d'engagement pour la mise en place d'un Swiss Government Cloud » [25]).

Principe S-2 : les options d'approvisionnement stratégiques se complètent, y compris à long terme

Pour différentes raisons (par ex. exigences légales, souveraineté numérique), certaines applications et données doivent et devront continuer d'être exploitées ou traitées sur des infrastructures ou plateformes situées dans les centres de données de l'administration fédérale (cf. la stratégie sur les centres de données de l'administration fédérale civile [24]).

L'utilisation de nuages publics doit permettre aux unités de l'administration fédérale d'accéder efficacement et rapidement aux solutions innovantes et aux technologies les plus récentes des fournisseurs de nuages publics, pour autant qu'aucune raison ne s'y oppose (par ex. exigences légales, besoin de protection des données ou préoccupations concernant la souveraineté des données).

Principe S-3 : le choix d'une option d'approvisionnement, à l'exception des services standard, incombe aux départements, aux unités administratives devenues autonomes et à la ChF

Les départements, les unités administratives devenues autonomes et la ChF décident de manière décentralisée de la suite à donner aux demandes des bénéficiaires de prestations ou des unités administratives en ce qui concerne le choix de l'option d'approvisionnement pour des applications ou des données, après consultation des fournisseurs de prestations concernés.

Principe O-1 : gouvernance du nuage selon des principes communs

Les principes suivants relatifs à l'informatique en nuage sont édictés par le secteur TNI de la ChF en vue d'une utilisation sûre, efficace et ordonnée des services en nuage privé et public.

Les départements et les unités administratives peuvent expliciter et développer les principes et les recommandations du secteur TNI de la ChF dans leur domaine de compétence.

Principe D-1 : introduction progressive du traitement des données dans les nuages publics

Même si le cadre juridique en vigueur offre éventuellement une plus grande latitude (cf. rapport « Cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale » [3]), les unités administratives ont tout intérêt, dans un premier temps, à ne traiter dans les nuages que des informations

classifiées « interne » ou des données personnelles non sensibles. Elles doivent solliciter sur ce point les conseils de l'intermédiaire.

Les informations faisant l'objet d'une classification supérieure à « interne », les données sensibles ou les données qui doivent être protégées pour d'autres raisons (par ex. lois spéciales) peuvent être stockées ou traitées dans des nuages publics pour autant que le droit en vigueur soit respecté, que les concepts de protection nécessaires soient établis et que les mesures définies dans le cas d'espèce soient mises en œuvre. La Conférence des secrétaires généraux (CSG), le Secrétariat d'État à la politique de sécurité (SEPOS) et le préposé fédéral à la protection des données et à la transparence (PFPDT) doivent en être informés.

Les unités administratives sont tenues de procéder à une vérification de la conformité au droit (protection des données et obligations de garder le secret incluses, par ex. secret de fonction) et d'appliquer les procédures de sécurité pertinentes (cf. [3]) pour leurs données et leurs applications.

5 Principes de l’informatique en nuage de l’administration fédérale

Le présent chapitre expose les principes de l’informatique en nuage applicables à toute l’administration fédérale. Pour plus de lisibilité, ces principes sont catégorisés à la figure 5. Aucun principe d’application générale n’a encore été défini dans les catégories ombrées.

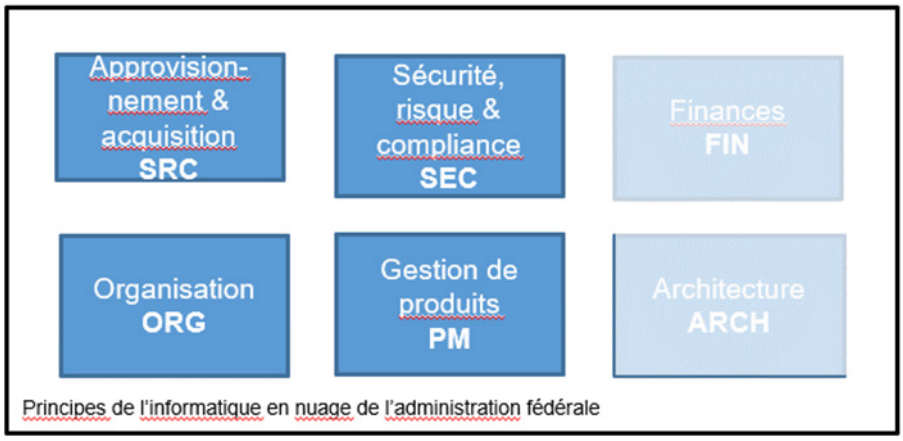


Figure 5 : catégorisation des principes de l’informatique en nuage

Les principes de l’informatique en nuage applicables à toute l’administration fédérale sont élaborés et gérés de manière centralisée par le secteur TNI de la ChF. Le ch. 5.1 traite des directives (niveau d’exigence). Les autres principes ont valeur de renvois à des documents élaborés par d’autres organes et pertinents dans le contexte nuagique, d’informations et de recommandations ; ils sont groupés par thème au ch. 5.2.

Les départements, les unités administratives ou les intermédiaires peuvent définir des principes spécifiques plus détaillés dans chaque catégorie. Ceux-ci ne sont pas mentionnés dans le présent document.

Les éléments plus détaillés ne concernant que les intermédiaires sont décrits dans le cahier des charges des intermédiaires [8] (tâches, compétences et responsabilités).

5.1 Directives (caractère contraignant)

Les principes énoncés dans le présent chapitre ont valeur de directives (caractère contraignant).

5.1.1 Approvisionnement & acquisition (SRC)

ID	Nom	Niveau d'exigence[1]	Principe d'informatique en nuage
SRC-4	**DIRECTIVE : acquisition de services en nuage privé et public**	**DOIT**	**S-1, O-1**
Dispositions Chaque unité administrative DOIT se procurer ses services en nuage privé et public IaaS et PaaS en faisant intervenir un intermédiaire. Elle DOIT se procurer les services en nuage privé de niveau III par l'intermédiaire du SGC si l'appel d'offres du SGC le permet. Ce principe ne s'applique pas au modèle logiciel en tant que service (*Software as a Service*, SaaS), aux offres ERP et à la bureautique.			
Commentaire Ce principe permet de canaliser les prestations et d'aider leurs bénéficiaires à respecter la gouvernance. Il permet d'organiser de manière ordonnée et efficace les achats pour les unités administratives et d'automatiser un maximum d'étapes pour l'intermédiaire. Le secteur TNI veille aussi à ce que les offres des fournisseurs de services en nuage et des intermédiaires soient conformes au modèle des niveaux. En cas de doute ou de différend, c'est le délégué TNI qui tranche après avoir entendu le conseil TNI.			
Niveaux de l'informatique en nuage Tous les niveaux			
Informations complémentaires Pour les définitions d'IaaS, de PaaS et de SaaS (National Institute of Standards and Technology (NIST), 2011): https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf			

[1] Pour les mots-clés définissant le niveau d'exigence, cf. annexe E.

5.1.2 Organisation (ORG)

ID	Nom	Niveau d'exigence	Principe d'informatique en nuage
ORG-4	**DIRECTIVE : le secteur TNI de la ChF autorise les nouveaux intermédiaires pour nuage public**	**DOIT**	**O-1**
Dispositions Si une unité administrative souhaite assumer la fonction d'intermédiaire pour nuage public, elle DOIT adresser une proposition motivée au secteur TNI de la ChF. Celui-ci vérifie les motifs et le respect du cahier des charges des intermédiaires. Le cas échéant, le secteur TNI de la ChF approuve la proposition.			
Commentaire Le principe O-1 prévoit qu'il peut y avoir, en plus des intermédiaires généraux de l'administration fédérale, des intermédiaires supplémentaires pour nuage public, dits intermédiaires ou CSB dédiés. Une unité administrative doit remplir certaines conditions pour jouer le rôle de CSB dédié. Ces conditions sont définies dans le cahier des charges des intermédiaires (Chancelerie fédérale (ChF), 2023). Celui-ci distingue l'intermédiaire de l'administration fédérale des CSB dédiés, lesquels doivent satisfaire à d'autres exigences. Si les conditions sont remplies et qu'il existe de bonnes raisons pour qu'une unité administrative assume la fonction d'intermédiaire pour nuage public, le secteur TNI de la ChF accepte la proposition par décision du délégué TNI, après avoir entendu le conseil TNI.			
Niveaux de l'informatique en nuage Niveaux I et II			
Informations complémentaires Cahier des charges des intermédiaires définissant les tâches, les compétences et les responsabilités de l'intermédiaire, cf. (Chancelerie fédérale (ChF), 2023)			

5.1.3 Gestion des produits (PM)

ID	Nom	Niveau d'exigence	Principe d'informatique en nuage
PM-1	**Directive : stratégie de sortie en cas d'utilisation de services en nuage public**	**DOIT**	**-**

Dispositions

Les unités administratives sont responsables de la gestion de la continuité des affaires (*Business Continuity Management* [BCM]) de leurs applications. Afin de gérer en connaissance de cause et de contrôler les dépendances vis-à-vis des fournisseurs de services en nuage public, l'unité administrative compétente DOIT définir une stratégie de sortie pour chaque projet (ou groupe d'applications) avec le soutien de l'intermédiaire responsable. Cette stratégie décrit comment une solution logicielle peut être transférée en temps utile sur une autre plateforme, un autre service ou une autre technologie. La stratégie de sortie DOIT être mise à jour en cas d'extension de l'application.

Commentaire

L'utilisation de services en nuage public génère des dépendances envers le fournisseur de services ou certaines technologies (enfermement propriétaire).

Le présent principe vise à faire prendre conscience de la nécessité de penser aux dépendances et à la possibilité d'enfermement propriétaire dès la conception d'une solution logicielle et avant d'utiliser des services infonuagiques. Cela permet d'anticiper les dépendances indésirables et de les atténuer dans la mesure du possible.

Les unités administratives veillent à ce que leurs applications puissent, dans la mesure du possible, être exploitées dans le nuage et restaurées sans dépendance vis-à-vis d'un fournisseur. Un moyen d'y parvenir est de prévoir une mise en œuvre indépendante de tout fournisseur ou le stockage (redondant) des données en dehors de la plateforme du fournisseur. Selon le contexte, il peut être utile de formuler une stratégie de sortie commune pour un groupe d'applications (par ex. toutes les applications d'une unité administrative qui fonctionnent chez le même fournisseur).

Les dépendances envers des fournisseurs ou des technologies sont également possibles dans les environnements en nuage privé et hors des nuages.

On trouvera des conseils et des astuces pour l'élaboration de la stratégie de sortie dans la directive sur la stratégie de sortie [6].

Niveaux de l'informatique en nuage

Niveaux I et II

Informations complémentaires

Néant

5.2 Recommandations et renvois à d'autres réglementations

Le présent chapitre expose, d'une part, des recommandations et, d'autre part, des principes qui trouvent leur origine ailleurs et dont l'applicabilité au contexte du nuage est expliquée par des renvois et des informations complémentaires.

5.2.1 Approvisionnement & acquisition (SRC)

ID	Nom	Principe d'informatique en nuage
SRC-1	**Modèle d'approvisionnement nuage – décision des départements et de la ChF**	**S-1**
Dispositions L'utilisation de services en nuage relève de la décision des départements, de la ChF ou des unités administratives devenues autonomes. Ce choix repose sur la stratégie d'approvisionnement informatique de la Confédération (Chancelerie fédérale (ChF), 2018), les directives et les normes de la Confédération en matière d'interopérabilité, l'architecture d'entreprise de l'unité administrative, une évaluation des risques et une vérification de la conformité au droit.		
Commentaire La décision quant au choix de l'approvisionnement de services en nuage est prise par analogie avec la décision relative à l'acquisition dans d'autres domaines d'approvisionnement (choix du nuage du niveau adéquat). Le pouvoir de décision correspond aux principes définis à l'art. 9 ONum (Der Schweizerische Bundesrat, 2020). La vérification de la conformité au droit porte essentiellement sur la protection des données, la sécurité de l'information et les éventuelles obligations relatives au maintien du secret.		
Niveaux de l'informatique en nuage Tous les niveaux		
Informations complémentaires Art. 9 (décision relative à l'acquisition de prestations) et 11 ONum (directives du chancelier de la Confédération sur des services standard avec obligation d'achat) (Der Schweizerische Bundesrat, 2020) : https://www.fedlex.admin.ch/eli/cc/2025/235/fr Stratégie d'approvisionnement informatique de la Confédération (Chancelerie fédérale (ChF), 2018) : https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/ikt-vorgaben/strategien-teilstrategien/sb017-ikt-strategie_sourcing.html Directives informatiques de la Confédération (Chancelerie fédérale (ChF), kein Datum): https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/vorgaben.html		

ID	Nom	Principe d'informatique en nuage
SRC-2	**Évaluation préalable du nuage de niveau adéquat**	**S-2, D-1**

Dispositions

Avant l'acquisition ou avant la procédure d'appel et l'exploitation de services en nuage public, la conformité au droit (analyse des bases légales) doit être vérifiée et une analyse des besoins de protection, ainsi que, le cas échéant, une analyse des risques doivent être menées. Une analyse d'impact relative à la protection des données doit être menée pour les données personnelles, le cas échéant.

En fonction des résultats des vérifications et des analyses, les unités administratives ou les départements optent pour une solution nuage public (niveaux I et II) ou nuage privé fédéral (niveau III et IV)), ou renoncent à tout nuage (cf. ch. 2). La responsabilité incombe à l'unité administrative concernée ou à son département.

Si des informations faisant l'objet d'une classification supérieure à « interne », des données sensibles ou des données qui nécessitent une protection particulière pour d'autres raisons (par ex. lois spéciales) sont traitées dans les nuages publics, la CSG, le SEPOS et le PFPDT doivent en être informés au préalable.

Commentaire

Le présent principe décrit le processus de décision concernant l'option d'approvisionnement adéquate : nuage public ou privé et le niveau approprié. Les analyses portant sur la cybersécurité se fondent sur les directives de l'Office fédéral de la cybersécurité (OFCS) (Office fédéral de la cybersécurité (OFCS), 2022).

Pour des précisions concernant l'application de la procédure de sécurité, cf. principe SEC-1.

Niveaux de l'informatique en nuage

Tous les niveaux

Informations complémentaires

Rapport « Cadre juridique pour l'utilisation de services d'informatique en nuage public dans l'administration fédérale » (Bundeskanzlei (BK), 2022) : https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html

Procédure de sécurité OFCS (Office fédéral de la cybersécurité (OFCS), 2022) : https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren.html

Méthode HERMES (Bundeskanzlei (BK)) : https://www.hermes.admin.ch/fr/

ID	Nom	Principe d'informatique en nuage
SRC-3	**Acquisition de services en nuage public**	**S-1, S-2, S-3**

Dispositions

Chaque unité administrative commande ses services en nuage public selon le modèle Iaas ou PaaS, sur la base de l'appel d'offres OMC 20007 ou par l'intermédiaire du SGC si l'appel d'offres OMC du SGC le permet.

Ce principe ne s'applique pas au modèle SaaS, aux offres ERP et au service standard bureautique. Il ne s'applique pas non plus aux offres d'entreprises tierces sur les marchés des fournisseurs de services en nuage public.

Le droit des marchés publics s'applique.

Commentaire

Si l'objet du marché n'est pas compris dans l'appel d'offres OMC 20007 ni dans celui du SGC ou si l'adjudicataire ne peut pas fournir les prestations demandées conformément à ces appels d'offres, une autre base légale doit être prévue.

Outre les SaaS, les offres ERP et la bureautique, les offres de sociétés tierces (c.-à-d. celles qui ne font pas partie des adjudicataires des appels d'offres OMC) sur les marchés des adjudicataires ne font pas partie des prestations couvertes par l'appel d'offres OMC 20007 ni par celui du SGC.

Niveaux de l'informatique en nuage

Niveaux I et II

Informations complémentaires

Pour les définitions d'IaaS, de PaaS et de SaaS (National Institute of Standards and Technology (NIST), 2011) : https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Loi fédérale sur les marchés publics (LMP ; RS 172.056.1) (Die Bundesversammlung der Schweizerischen Eidgenossenschaft, 2019): https://www.fedlex.admin.ch/eli/cc/2020/126/fr

Ordonnance sur les marchés publics (OMP ; RS 172.056.11) (Der Schweizerische Bundesrat, 2020) : https://www.fedlex.admin.ch/eli/cc/2020/127/fr

5.2.2 Sécurité, risque et compliance (SEC)

ID	Nom	Principe d'informatique en nuage
SEC-1	**Mener la procédure de sécurité**	**D-1**

Dispositions

Les départements et leurs unités administratives sont tenus de procéder, pour leurs applications et leurs données, à une vérification de la conformité au droit (protection des données et, le cas échéant, obligations de garder le secret) et d'appliquer les procédures de sécurité pertinentes.

Avant l'acquisition, la procédure d'appel ou l'exploitation de services en nuage public, une analyse des besoins de protection (SCHUBAN) doit être menée.

Si l'analyse des besoins de protection révèle un besoin de protection accru, un concept de sécurité de l'information et de protection des données (concept SIPD) avec analyse des risques doit être établi en plus de la documentation de la mise en œuvre de la protection informatique de base.

Le conseiller à la protection des données de l'unité administrative doit être consulté pour toute décision concernant l'externalisation de données personnelles dans un nuage et pour la conception de ce traitement (art. 26, al. 2, let. a, de l'ordonnance du 31 août 2022 sur la protection des données ; RS 235.11).

Lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, l'unité administrative doit procéder à une analyse d'impact relative à la protection des données personnelles. Le guide du PFPDT sur les mesures techniques et organisationnelles de la protection des données (Préposé fédéral à la protection des données et à la transparence (PFPDT), 2015) doit être consulté et on procédera, si nécessaire, à une analyse d'impact relative à la protection des données personnelles.

Commentaire

Les directives de l'OFCS concernant la procédure de sécurité (Office fédéral de la cybersécurité (OFCS), 2022) doivent également être appliquées aux projets potentiels de nuage public.

Ce principe renvoie aux processus d'analyse des besoins de protection SCHUBAN établis et au concept SIPD ; il garantit la conformité des logiciels aux règles de sécurité de l'information. Ces processus couvrent l'analyse et la gestion des risques.

Le rapport « Cadre juridique pour l'utilisation de services d'informatique en nuage public dans l'administration fédérale » (Bundeskanzlei (BK), 2022) et les listes de contrôle pertinentes (Bundeskanzlei, Digitale Transformation und IKT Steuerung (DTI), 2022) servent d'assise à la vérification de la conformité au droit.

Niveaux de l'informatique en nuage

Tous les niveaux

Informations complémentaires

Page d'information sur l'informatique en nuage dans l'administration fédérale (Bundeskanzlei, Digitale Transformation und IKT Steuerung (DTI), 2022) : https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html

Rapport « Cadre juridique pour l'utilisation de services d'informatique en nuage public dans l'administration fédérale » (Bundeskanzlei (BK), 2022) : https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html Procédure de sécurité OFCS (Office fédéral de la cybersécurité (OFCS), 2022) : https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren.html Méthode HERMES (Bundeskanzlei (BK)) : https://www.hermes.admin.ch/ Guide du PFPDT relatif aux mesures techniques et organisationnelles de la protection des données (Préposé fédéral à la protection des données et à la transparence (PFPDT), 2015) : https://www.edoeb.admin.ch/dam/fr/sd-web/eVhrh8wY3QcR/leitfaden_tom.pdf Directives du Conseil fédéral concernant l'examen préalable des risques et l'analyse d'impact relative à la protection des données personnelles en cas de traitement de données personnelles par l'administration fédérale (Directives AIPD ; FF 2023 1882) (Der Schweizerische Bundesrat, 2023) : https://www.fedlex.admin.ch/eli/fga/2023/1882/fr Instrument d'examen préalable des risques et guide AIPD (Bundesamt für Justiz, kein Datum) : https://www.bj.admin.ch/bj/fr/home/staat/datenschutz/info-bundesbehoerden.html

ID	Nom	Principe d'informatique en nuage
SEC-2	**Pas de données classifiées « secret » dans les nuages publics**	**D-1**
Dispositions Il est interdit de stocker et de traiter des données classifiées « secret » dans les nuages publics (niveaux I et II) et dans les nuages privés de niveau III.		
Commentaire L'unité administrative veille à ce que les données classifiées « secret » restent sous le contrôle exclusif de l'administration fédérale. Cela s'applique également aux moyens informatiques qui relèvent de la catégorie de sécurité « protection très élevée » au sens de la LSI [4]		
Niveaux de l'informatique en nuage Niveaux I, II et III		
Informations complémentaires Rapport « Cadre juridique pour l'utilisation de services d'informatique en nuage public dans l'administration fédérale » (Bundeskanzlei (BK), 2022): https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html Loi sur la sécurité de l'information (LSI) (Die Bundesversammlung der Schweizerischen Eidgenossenschaft, 2020) : https://www.fedlex.admin.ch/eli/fga/2020/2696/fr Ordonnance sur la sécurité de l'information (OSI) (Der Schweizerische Bundesrat, 2022 (tritt am 1.1.2024 in Kraft)) : https://www.fedlex.admin.ch/eli/cc/2023/735/fr		

ID	Nom	Principe d'informatique en nuage
SEC-3	**Données présentant un besoin de protection accru : uniquement avec des mesures de protection supplémentaires dans les nuages publics**	**D-1**

Dispositions

Des mesures contractuelles, techniques et organisationnelles de protection adéquates garantissant le respect du droit applicable doivent être prises pour traiter et stocker dans un nuage public des informations classifiées « confidentiel » ou des données couvertes par une obligation de garder le secret.

La règle s'applique également aux données sensibles si les clarifications révèlent un risque pour la personnalité des personnes concernées. Lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, le responsable du traitement doit procéder au préalable à une analyse d'impact relative à la protection des données personnelles, conformément à l'art. 22, al. 1, de la LPD (cf. SEC-1).

Si le volume de l'externalisation et la nature des données externalisées présentent un risque élevé pour la souveraineté de l'État, on doit vérifier si des mesures adéquates permettent un traitement dans un nuage public.

Commentaire

L'analyse des besoins de protection permet de déterminer si une application contient ou génère des données classifiées ou des données personnelles.

Si, en l'espèce, des mesures contractuelles, techniques et organisationnelles de protection adéquates garantissent le respect du droit applicable, des données présentant un besoin de protection accru ou protégées par la législation sur la protection des données peuvent aussi être stockées et traitées dans un nuage public.

La procédure de sécurité OFCS (Office fédéral de la cybersécurité (OFCS), 2022) ou une analyse d'impact relative à la protection des données personnelles permet de vérifier si les mesures de protection envisagées sont suffisantes.

Les mesures techniques de protection actuelles comprennent notamment le cryptage lors du stockage, le cryptage des données en transit ou l'utilisation de technologies particulières (*Bring Your Own Key, Hold Your Own Key, Confidential Computing*, etc.).

Le stockage redondant (nuage public et centre de données de l'administration fédérale) permet par exemple d'assurer la souveraineté numérique en garantissant la disponibilité des données.

De telles mesures devraient être coordonnées avec le département compétent.

Niveaux de l'informatique en nuage

Niveaux I et II

Informations complémentaires

Rapport « Cadre juridique pour l'utilisation de services en nuage public dans l'administration fédérale » (Bundeskanzlei (BK), 2022) : Informatique en nuage (admin.ch)

Procédure de sécurité OFCS (Office fédéral de la cybersécurité (OFCS), 2022) : https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren.html

Guide du PFPDT relatif aux mesures techniques et organisationnelles de la protection des données (Préposé fédéral à la protection des données et à la transparence (PFPDT), 2015) : https://www.edoeb.admin.ch/dam/fr/sd-web/eVhrh8wY3QcR/leitfaden_tom.pdf

5.2.3 Organisation (ORG)

ID	Nom	Principe d'informatique en nuage
ORG-1	**Explicitation et développement des principes de l'informatique en nuage par les départements et les unités administratives**	**O-1**
Dispositions Les principes de l'informatique en nuage sont applicables à toute l'administration fédérale. Les départements et les unités administratives peuvent expliciter ou compléter ces principes dans leur domaine de compétence, dans les limites du droit en vigueur.		
Commentaire Le présent principe permet aux départements et aux unités administratives d'adapter librement les principes généraux à leurs spécificités. Ils peuvent notamment renforcer, préciser ou compléter les principes communs ou en ajouter de nouveaux.		
Niveaux de l'informatique en nuage Tous les niveaux		
Informations complémentaires Loi sur l'organisation du gouvernement et de l'administration (LOGA) (Die Bundesversammlung der Schweizerischen Eidgenossenschaft, 1997) : https://www.fedlex.admin.ch/eli/cc/1997/2022_2022_2022/fr		

ID	Nom	Principe d'informatique en nuage
ORG-2	**Explicitation et développement des principes de l'informatique en nuage par les intermédiaires**	**O-1**
Dispositions Les intermédiaires peuvent expliciter ou compléter les principes de l'informatique en nuage dans leur domaine de compétence. Les clients ont la possibilité d'influencer les adaptations des principes de l'informatique en nuage effectuées par l'intermédiaire responsable. Ces adaptations ne s'appliquent qu'aux clients de l'intermédiaire concerné.		
Commentaire Le présent principe permet aux intermédiaires d'adapter librement les principes généraux à leurs spécificités. Ils peuvent notamment renforcer, préciser ou compléter les principes communs ou en ajouter de nouveaux.		
Niveaux de l'informatique en nuage Tous les niveaux		
Informations complémentaires Loi sur l'organisation du gouvernement et de l'administration (LOGA) (Die Bundesversammlung der Schweizerischen Eidgenossenschaft, 1997) : https://www.fedlex.admin.ch/eli/cc/1997/2022_2022_2022/fr		

ID	Nom	Principe d'informatique en nuage
ORG-3	**L'intermédiaire apporte son soutien au respect des principes de l'informatique en nuage et à la gouvernance du nuage**	**O-1**
Dispositions L'intermédiaire doit soutenir ses clients dans l'exercice de leurs activités en relation avec le respect des principes de l'informatique en nuage et de la gouvernance du nuage définie.		
Commentaire Ce principe formule l'une des tâches de l'intermédiaire : il aide les départements et les unités administratives à respecter les principes de l'informatique en nuage et les directives relatives à la gouvernance. L'unité administrative concernée demeure toutefois responsable du respect des principes et des directives.		
Niveaux de l'informatique en nuage Tous les niveaux		
Informations complémentaires Cahier des charges des intermédiaires définissant les tâches, les compétences et les responsabilités de l'intermédiaire, cf. (Chancelerie fédérale (ChF), 2023)		

Annexes

A. Informations générales sur le document

Version et statut	version 1.2, en vigueur
Langue originale	allemand
Décision du	10 décembre 2025
Entrée en vigueur le	1. Januar 2026
Date d'expiration	le secteur TNI de la ChF vérifie régulièrement l'actualité et l'adéquation des principes de l'informatique en nuage, et au plus tard quatre ans après leur entrée en vigueur.

B. Abrogation

La présente version remplace la version 1.1.

C. Dispositions transitoires et dispositions finales

1. *Dispositions transitoires relatives aux directives SRC-4, ORG-4 et PM-1*
   Les applications réalisées avant l'entrée en vigueur du présent document peuvent continuer à fonctionner sans changement. Lors du prochain renouvellement ou de l'extension des fonctionnalités de l'application, les directives devront être vérifiées et leur respect initialisé.
2. *Respect des directives SRC-4, ORG-4 et PM-1*
   En vertu de l'art. 6 ONum, les départements et la ChF sont responsables de l'application des directives dans leurs domaines de compétence respectifs.

D. Modifications par rapport à la version précédente

Extension du rôle d'intermédiaire à tous les niveaux (nuages privé et public), prise en compte de l'offre de nuage privé sécurisé du CSI-DFJP pour l'ensemble de la Confédération et passage des « nuages publics » (OMC 20007) au SGC.

E. Signification des mots-clés déterminant le niveau d'exigence

Le niveau d'exigence des différentes dispositions du présent document est indiqué par les mots-clés ci-après écrits en capitales. Ces niveaux sont repris de la norme internationale IETF/RFC 2119 BCP14 et correspondent donc à une pratique courante au niveau international.

Mot-clé	Niveau d'exigence
DOIT / EXIGE	Ordre, exigence ou disposition à respecter absolument. Les exceptions et les dérogations doivent faire l'objet d'une demande écrite et être approuvées par le secteur TNI de la ChF. (MUST, REQUIRED, SHALL)

DEVRAIT / RECOMMANDÉ	Ordre, exigence ou disposition à respecter. Les exceptions et les dérogations, par exemple pour des raisons pratiques ou des raisons de sécurité, doivent être justifiées par écrit. Il n'est pas nécessaire d'obtenir une dérogation explicite du secteur TNI de la ChF. (SHOULD, RECOMMENDED)
NE DOIT PAS	Option qui ne peut pas être choisie ou mesure qui ne peut pas être mise en œuvre. (MUST NOT, SHALL NOT)
PEUT (facultatif)	Option explicitement autorisée. Les utilisateurs potentiels décident s'ils veulent l'utiliser. Le fournisseur doit proposer l'option en question.
PEUT (optionnel)	Option admise. Le fournisseur décide s'il veut la proposer.

F. Annexes, documents de référence et informations complémentaires

ID	Document de référence
[1]	ChF, secteur TNI, Stratégie d'informatique en nuage de l'administration fédérale, 2020 ; https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/vorgaben/sb020-cloud-strategie_der_bundesverwaltung.html.
[2]	Ordonnance du 2 avril 2025 sur la numérisation (ONum), *RS 172.019.1*, https://www.fedlex.admin.ch/eli/cc/2025/235/fr.
[3]	Rapport de la ChF « Cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale » (version 2.0), 2025, https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html.
[4]	Loi du 18 décembre 2020 sur la sécurité de l'information (LSI), *RS 128*,https://www.fedlex.admin.ch/eli/cc/2020/2696/fr.
[5]	Loi fédérale du 25 septembre 2020 sur la protection des données (LPD), *RS 235*.1https://www.fedlex.admin.ch/eli/cc/2022/491/fr.
[6]	ChF, Cloud-Exit-Strategie-Guideline [en cours d'élaboration].
[7]	IT-Business, Was ist eine Landing Zone?, 2022, https://www.it-business.de/was-ist-eine-landing-zone-a-0c951fabad3e2dcc1bf4e7cd50d2d2f5/ [en allemand, consulté le 29.10.2025].
[8]	ChF, Cahier des charges des intermédiaires [en cours d'élaboration].
[9]	National Institute of Standards and Technology (NIST), The NIST Definition of Cloud Computing, 2011, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (en anglais).
[10]	ChF, Stratégie d'approvisionnement informatique de la Confédération 2018-2023, 2018, https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/ikt-vorgaben/strategien-teilstrategien/sb017-ikt-strategie_sourcing.html

ID	Document de référence
[11]	ChF, directives informatiques, https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/vorgaben.html.
[12]	OFCS, Procédure de sécurité, 2022, https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren.html.
[13]	ChF, méthode de gestion de projet HERMES, https://www.hermes.admin.ch/fr/.
[14]	Loi fédérale du 21 juin 2019 sur les marchés publics (LMP), *RS 172.056.1*, https://www.fedlex.admin.ch/eli/cc/2020/126/fr.
[15]	Ordonnance du 12 février 2020 sur les marchés publics (OMP), *RS 172.056.11*, https://www.fedlex.admin.ch/eli/cc/2020/127/fr.
[16]	PFPDT, Guide relatif aux mesures techniques et organisationnelles de la protection des données, 2024, https://www.edoeb.admin.ch/dam/fr/sd-web/eVhrh8wY3QcR/leitfaden_tom.pdf.
[17]	ChF, secteur TNI, Informatique en nuage, 2025, https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html.
[18]	Directives du Conseil fédéral concernant l'examen préalable des risques et l'analyse d'impact relative à la protection des données personnelles en cas de traitement de données personnelles par l'administration fédérale, 2023, https://www.fedlex.admin.ch/eli/fga/2023/1882/fr.
[19]	Office fédéral de la justice, instrument d'examen préalable des risques et guide AIPD, https://www.bj.admin.ch/bj/fr/home/staat/datenschutz/info-bundesbehoerden.html.
[20]	Ordonnance du 8 novembre 2023 sur la sécurité de l'information (OSI), *RS 128.1*, https://www.fedlex.admin.ch/eli/cc/2023/735/fr.
[21]	Loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA), *RS 172.010*, https://www.fedlex.admin.ch/eli/cc/1997/2022_2022_2022/fr.
[22]	Cloudcomputing Insider, Cloud Governance, 2021, https://www.cloudcomputing-insider.de/was-ist-cloud-governance-a-990452/ [en allemand, consulté le 29.10.2025].
[23]	OFIT, Shared Responsibility Model, 2022, https://confluence.bit.admin.ch/x/I5vzFw.
[24]	SB022 – Stratégie Centres de données de l'administration fédérale civile, 2025, https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/vorgaben/sb022-strategie-rechenzentren-der-zivilen-bundesverwaltung.html.
[25]	Message du Conseil fédéral concernant un crédit d'engagement pour la mise en place d'un Swiss Government Cloud, FF **2024** 1408, https://www.fedlex.admin.ch/eli/fga/2024/1408/fr.

Informations complémentaires

Néant

G. Glossaire

Abréviation / terme	Signification
ChF	Chancellerie fédérale
Conseil TNI	Conseil de la transformation numérique et de la gouvernance informatique de la Confédération
CSB	*Cloud Service Broker* (courtier de services en nuage, cf. intermédiaire)
CSG	Conférence des secrétaires généraux
Gouvernance du nuage	La gouvernance du nuage vise à garantir l'utilisation judicieuse, sûre et conforme aux règles des services infonuagiques. Elle se compose d'un ensemble de règles et de mesures organisationnelles et techniques qui concernent différents aspects de l'utilisation du nuage (Cloudcomputing Insider, 2021).
IaaS	*Infrastructure as a Service* (infrastructure en tant que service)
ID	identifiant
Intermédiaire	L'intermédiaire ou CSB soutient les unités administratives dans l'utilisation sûre, efficace et ordonnée des services d'informatique en nuage privé et public.
ITSM	gestion des services informatiques
ITSP4ITSP	fournisseur de prestations informatiques pour un fournisseur de prestations informatiques (modèle du SGC par l'intermédiaire duquel les fournisseurs de prestations informatiques peuvent proposer à leurs clients appartenant à la Confédération et à d'autres services de l'administration publique des prestations à partir du SGC).
OFCS	Office fédéral de la cybersécurité
PaaS	*Platform as a Service* (plateforme en tant que service)
PFPDT	Préposé fédéral à la protection des données et à la transparence
SaaS	*Software as a Service* (logiciel en tant que service)
SCHUBAN	analyse des besoins de protection (de l'allemand *Schutzberdarfanalyse*)
SEPOS	Secrétariat d'État à la politique de sécurité
SGC	*Swiss Government Cloud*
SIPD	concept de sécurité de l'information et de protection des données
SS	service standard
TNI	Transformation numérique et gouvernance de l'informatique (secteur de la ChF)
UA	unité administrative

Abréviation / terme	Signification
Zone d’atterrissage	environnement sécurisé dans le nuage, auquel différents utilisateurs peuvent accéder. Elle permet de mettre à disposition et d’utiliser des applications et des charges de travail. Sa structure dépend des besoins de l’entreprise (IT-Business, 2022).

H. Métadonnées (optimisation des recherches en ligne)

Thème (art. 40, al. 1, ONum)	Processus
Lien avec la stratégie	L’administration comme plateforme (et interopérabilité)
Domaine de capacité	Services & applications Développement, livraison & exploitation
Lien avec la vision de l’architecture 2050	L’interopérabilité comme nouveau standard
Hiérarchie des documents	Les directives W010 Principes d’architecture et W012 Souveraineté numérique de l’administration fédérale priment le présent document.