BULLETIN OFFICIEL DES ARMÉES

Édition Chronologique n° 16 du 15 avril 2019

TEXTE TECHNIQUE

Texte 15

INSTRUCTION GÉNÉRALE

relative à la politique générale sur le logiciel.

Du *08 février 2019*

DGNUM :

SDTNUM

INSTRUCTION GÉNÉRALE relative à la politique générale sur le logiciel.

Du 08 février 2019

NOR A R M D 1 9 5 2 4 1 4 J

Pièce(s) jointe(s) :

Quatre annexes.

Classement dans l'édition méthodique :

BOEM 160.1.3.

Référence de publication :

SOMMAIRE

1. SYNTHESE

L'essor rapide de nouvelles technologies digitales contribue à transformer radicalement la nature de l'action des grandes organisations. Non seulement cet essor induit un bouleversement dans la façon dont les institutions délivrent des services, *via* notamment la prise en compte de l'expérience utilisateurs, la mise à disposition de plateformes de services selon des politiques SI centrées sur l'usager et la donnée, mais il a induit également des savoir-faire nouveaux.

Afin de s'adapter à ce changement profond de paradigme, de répondre aux exigences nouvelles des usagers et d'être en capacité de suivre le rythme de ruptures que celui-ci engendre, le ministère des armées doit faire évoluer son système d'information et de communication en cohérence avec le cadre de politique générale sur le logiciel et en inscrivant le besoin essentiel de sécurisation comme un des critères majeurs de choix et de mise en œuvre.

La vision globale de cette transformation numérique a été définie dans le ***document d'Ambition Numérique*** publié en novembre 2017. Le ***schéma directeur de la transformation numérique***, qui traduit cette ambition numérique, vise dans une démarche fédératrice à :

- orienter la transformation numérique du ministère des armées ;
- aider les métiers à réaliser leur transformation numérique.

Dans ce contexte, et au regard de la réflexion de l'État en la matière, le ministère des armées s'est ainsi engagé dans la définition et le déploiement de sa stratégie numérique et réactualise en conséquence sa politique générale sur le logiciel.

Que l'on soit dans une démarche de « faire-faire » ou d'un développement en interne du ministère des armées pour concevoir et réaliser de nouveaux logiciels, cette politique est destinée à orienter l'action des directions d'application et des maitrises d'œuvre et s'applique à tous les systèmes d'information et de communication de la défense, à savoir les systèmes d'information opérationnels et de communication (SIOC), les systèmes d'information scientifiques et techniques (SIST) et les systèmes d'information, d'administration et de gestion (SIAG).

Cette politique générale logicielle s'articule ainsi autour des principes liés à l'innovation, à l'agilité, à la capacité à répondre rapidement aux demandes d'évolutions et au partage global et cohérent de l'information.

Il apparaît alors essentiel de bâtir cette politique sur la base de 3 principes majeurs :

- une **architecture modulaire**, orientée services et usages métier ;
- la **standardisation des échanges** entre logiciels ;
- l'**indépendance du logiciel** vis-à-vis de l'infrastructure sous-jacente.

dont les objectifs sont de :

- favoriser l'interopérabilité par un **recours aux standards**, protocoles et formats d'échanges ouverts ;
- garantir la souveraineté (confiance et sécurisation) numérique du ministère des armées ;
- avoir une **politique équilibrée** concernant les adhérences entre composants logiciels conciliant les différents contextes et écosystèmes, notamment en appréhendant le cout global et les effets d'échelle ;
- **maitriser et rationaliser** les choix technologiques ;
- promouvoir le **partage** et la **réutilisation** des composants logiciels ;
- maîtriser l'architecture du SI, en ayant tout particulièrement une approche modulaire orientée services et usages métier ;
- **exposer des ressources** (services et données) via les principes d'APIsation.

2. LA STRATEGIE NUMERIQUE DU MINISTERE DES ARMEES

De nombreuses initiatives de l'État permettent aux ministères de définir un cadre et une trajectoire de prise en compte des enjeux de la transformation numérique. Ainsi, la loi pour une république numérique et le chantier numérique de la démarche Action Publique 2022 (AP 2022) visant l'accélération de la transformation publique, porté par la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC), contribuent à la définition du cap de la politique générale du logiciel du ministère des armées.

Les systèmes numériques constituent aujourd'hui une part essentielle de la performance du ministère, tant opérationnelle qu'administrative. Ces systèmes numériques sont aujourd'hui au cœur d'une accélération sans précédent de nos modes de vie qui touche tous les pans des sociétés modernes et en bouleverse les modes de fonctionnement et d'organisation : l'expérience de l'immédiateté rend les usagers plus exigeants et plus impatients, le rythme des ruptures technologiques s'accélère et les usages sont sans cesse renouvelés.

Afin de s'adapter à ce changement profond de paradigme, de répondre aux exigences nouvelles des usagers et d'être en capacité de suivre le rythme de ruptures que celui-ci engendre, le ministère des armées doit se doter des capacités de réalisation de services et produits digitaux à travers un processus dédié tout en assurant le besoin essentiel de sécurisation.

La ministre des armées a lancé en septembre 2017 la ***démarche de transformation numérique*** du ministère des armées. Celle-ci a une résonance particulière pour les armées qui sont confrontées à une course à la supériorité opérationnelle passant en particulier par la maîtrise du numérique. Cette démarche de transformation intègre donc les enjeux de souveraineté comme ceux de sécurité qui en constituent un prérequis indispensable.

La vision globale de cette transformation numérique a été définie dans le ***document d'Ambition Numérique*** publié en novembre 2017 et qui fixe 3 objectifs stratégiques :

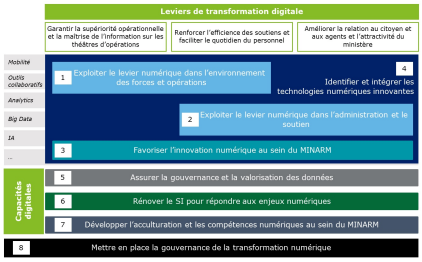
- garantir la supériorité opérationnelle et la maîtrise de l'information sur les théâtres d'opérations ;
- renforcer l'efficience des soutiens et faciliter le quotidien des personnels ;
- améliorer la relation au citoyen et l'attractivité du ministère.

Le ***schéma directeur de la transformation numérique***, qui traduit cette ambition numérique, vise dans une démarche fédératrice à :

- orienter la transformation numérique du ministère des armées ;
- aider les métiers à réaliser leur transformation numérique.

D'un point de vue métier, il a vocation à guider la transformation des métiers tout en restant évolutif afin de pouvoir s'adapter au contexte, aux directives ministérielles, aux besoins des agents du ministère, à l'évolution des technologies et des usages numériques ainsi qu'à la disponibilité des ressources.

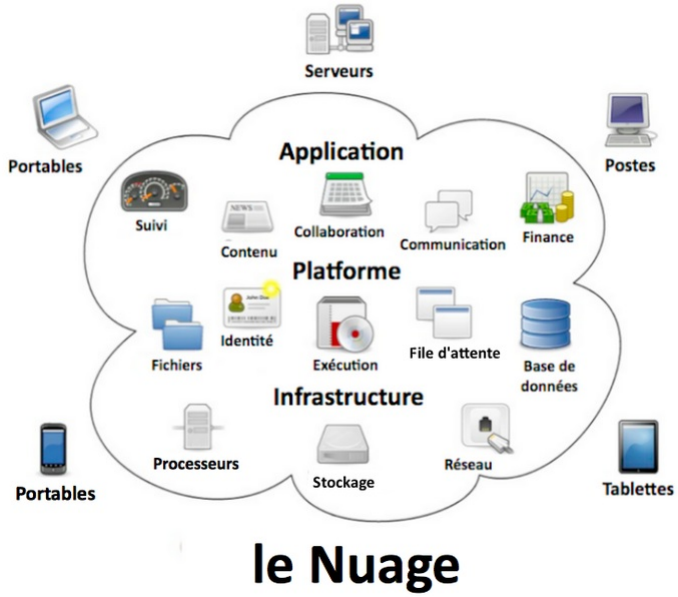
Dans ce contexte, et au regard de la réflexion de l'État en la matière, le ministère des armées s'est ainsi engagé dans la définition et le déploiement de sa stratégie numérique et réactualise en conséquence sa politique générale sur le logiciel (cf. Annexe §6.2 sur la définition d'un système d'information et d'un logiciel), en déclinaison des principes susmentionnés.



3. PRESENTATION DE LA POLITIQUE LOGICIELLE

armées pour concevoir et réaliser de nouveaux logiciels, tout en assurant les évolutions et la maintenance de notre parc applicatif, cette politique est destinée à orienter l'action des directions d'application et des maitrises d'œuvre.

Elle s'applique à tous les systèmes d'information et de communication de la défense, à savoir les systèmes d'information opérationnels et de communication (SIOC), les systèmes d'information scientifiques et techniques (SIST) et les systèmes d'information, d'administration et de gestion (SIAG) ainsi qu'à l'ensemble des données du ministère (Instruction ministérielle n° 2 portant sur la gouvernance des données).



Les logiciels, parties intégrantes des systèmes d'information du ministère, s'inscrivent dans un environnement composé d'infrastructures techniques permettant son développement, son intégration, son installation, son suivi, son exécution, son maintien en condition, et dans un écosystème avec lequel ils interagissent. Les logiciels sont mis en œuvre afin de délivrer des ***services*** aux utilisateurs : soutenants, soutenus, bénéficiaires hors du ministère ou externes au ministère, etc. amenés à s'en servir dans le cadre de leurs fonctions.

Ces services sont de deux natures :

- les **services** « **communs** » (messagerie, suite bureautique, casier numérique, etc.) sont des services s'appuyant sur des logiciels pérennes et dont le choix doit être bâti sur une utilisation dans la durée, la sécurité et la stabilité afin d'éviter des actions de conduites du changement couteuses ;
- les **services** « **métier** » s'appuyant sur des logiciels développés pour répondre à un (ou à des) besoin(s) spécifique(s) dans une organisation et un contexte donné. Ces logiciels doivent par nature être en capacité de s'adapter rapidement aux changements de contexte (règlementaire, sécuritaire, organisationnel, opérationnel, etc.).

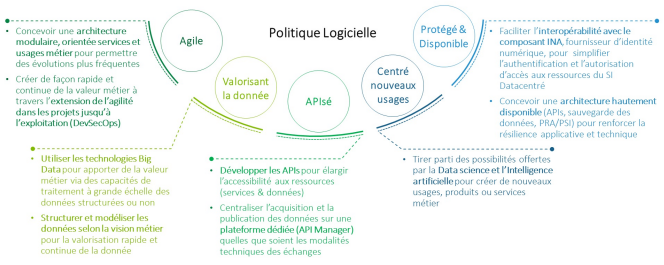
Cette politique logicielle reprend ainsi l'ensemble des éléments ayant une influence potentielle sur l'acquisition, le paramétrage, le développement, l'intégration, le suivi et l'exécution des logiciels nécessaires à la délivrance des services aux usagers du ministère dans le cadre de la transformation numérique du ministère.

Ces services sont de deux natures :

- les **services** « **communs** » (messagerie, suite bureautique, casier numérique, etc.) sont des services s'appuyant sur des logiciels pérennes et dont le choix doit être bâti sur une utilisation dans la durée, la sécurité et la stabilité afin d'éviter des actions de conduites du changement couteuses ;
- les **services** « **métier** » s'appuyant sur des logiciels développés pour répondre à un (ou à des) besoin(s) spécifique(s) dans une organisation et un contexte donné. Ces logiciels doivent par nature être en capacité de s'adapter rapidement aux changements de contexte (règlementaire, sécuritaire, organisationnel, opérationnel, etc.).

Cette politique logicielle reprend ainsi l'ensemble des éléments ayant une influence potentielle sur l'acquisition, le paramétrage, le développement, l'intégration, le suivi et l'exécution des logiciels nécessaires à la délivrance des services aux usagers du ministère dans le cadre de la transformation numérique du ministère.

Les principaux objectifs structurants de cette politique sont présentés dans le schéma ci-dessous :



3.1. Une politique logicielle reposant sur 3 piliers majeurs

Au regard des facteurs conduisant à la mise en place de cette politique logicielle et des besoins émis par le ministère des armées, il apparaît essentiel de **bâtir cette politique sur la base de 3 principaux piliers** :

- la capacité de **modularité du système d'information** dans lequel s'insère le logiciel ;
- la **standardisation des échanges** entre logiciels ;
- l'**indépendance du logiciel** vis-à-vis de l'infrastructure sous-jacente.

Pour chacun de ces piliers, une définition de l'attendu et des aspects sous-tendus par l'objectif a été dans un premier temps apportée. Dans un second temps, chacun des piliers a été abordé selon les ***6 axes clés*** [1] ***définis par le Schéma directeur de la transformation numérique (SDNUM),*** ceci afin de s'assurer que la présente politique logicielle répond de façon pragmatique au schéma directeur.

L'objectif de cette démarche est ainsi de ***formaliser un cadre à la fois cohérent avec la feuille de route du ministère et le schéma directeur de la transformation numérique***, tout en optimisant les opérations réalisées au sein des systèmes d'information et en délivrant des logiciels à forte valeur ajoutée, facilement exploitables par les agents ministériels et extrêmement accessibles par tous les bénéficiaires : à savoir respectant les exigences du Référentiel général d'accessibilité pour les administrations (RGAA) mais également accessibles en terme d'approche ergonomique ou bien encore accessibles en terme de connexion, même en mobilité, sur n'importe quel type de terminal.

3.1.1. *Une architecture modulaire, orientée services et usages métier*

Remettre l'usager au centre des préoccupations du ministère suppose de mettre à disposition une offre de services cohérente avec les attentes. La définition de cette offre passe par la **définition de parcours clients** (bénéficiaires des systèmes d'information) avec généralement une mise en évidence des interactions les plus contributives ou destructives à l'expérience client (moments de vérité, irritants, etc.). Cette démarche permet d'identifier et de prioriser les différents services qui seront proposés par le système d'information, de façon la plus efficiente possible, tout en tenant compte des contraintes règlementaires, administratives ou encore sécuritaires. Cette réflexion passe par une connaissance fine des attentes de tous les acteurs impliqués, et une capacité à prioriser les fonctionnalités à mettre en œuvre. Il est à noter que les services, selon qu'il s'agisse de services « communs » ou de services « métiers », comme évoqués ci avant dans le présent chapitre, ont un caractère plus ou moins évolutif selon les attentes des usagers, les services « métiers » devant ainsi être capables de s'adapter rapidement selon **leur valeur d'usage**.

D'un point de vue technique, les systèmes et logiciels permettant de mettre à disposition ces services doivent être spécifiés et conçus (architecture, développement, intégration) de façon à permettre à la fois des usages génériques de haut niveau mais aussi intégrer des capacités d'évolutions rapides et de réutilisation. Ainsi, l'articulation entre les logiciels et les services implique que les Directions d'application soient en ***capacité de faire le lien entre les différents logiciels existants et d'en assurer la cohérence*** sans en complexifier la maintenance technique, **de sorte à concevoir un système d'information modulaire**, orienté services et usages métier et ainsi permettre des évolutions plus fréquentes. De facto, toute évolution de logiciel induite par une volonté d'optimisation de réponse à un besoin fonctionnel devra dès lors pouvoir être coordonnée facilement avec d'autres évolutions potentiellement nécessaires de logiciels existants.

Cela implique à minima une évolution de la **démarche d'urbanisation** de ces systèmes et de ces logiciels afin de valoriser les éléments offrant des services et une communication ad'hoc vers les directions d'application de ces offres de services. Cette démarche devra en parallèle être renforcée par la création d'une plateforme de partage de code.

L'emploi de ***logiciels libres*** (cf. §4.2) favorise cette architecture modulaire et autorise une plus grande efficience dans son évolutivité là où cela est nécessaire. Cela constitue un apport très fort à l'innovation. Les logiciels libres permettent le développement de modules sur mesure, limités au strict besoin initial. L'usage du logiciel libre permet en effet de « piocher », en cohérence avec le Cadre de Cohérence Technique (CCT), dans les souches disponibles proposées par les communautés du logiciel libre. À cet égard, le CCT ne doit pas être considéré comme un frein à l'innovation mais comme une obligation de réflexion à des architectures prenant en compte l'écosystème global de la défense et n'entraînant pas au niveau du ministère une augmentation de la dette technique. Le CCT est ouvert à la prise en compte de nouvelles technologies ou de nouveaux logiciels dès lors qu'ils sont dûment justifiés et s'inscrivent dans cette logique globale liée au métier (adéquation au besoin), à l'évolution technologique (innovation, ...), aux principes d'architecture (non adhérence, modularité, etc.), et aux contraintes techniques (passage à l'échelle, soutien, maintien en condition opérationnel et de sécurité, etc.) et financières (droits d'usage...).

La DGNUM s'attache à préconiser l'usage de logiciels libres dès lors qu'ils répondent à cette préoccupation. À titre d'exemple, la DGNUM a produit une note relative au choix en matière de systèmes de gestion de bases de données relationnelles (SGBDR) qui rappelle les recommandations du CCT sur les solutions très matures de bases de données en open source et impose une instruction préalable en bureau SC2 pour des choix de solutions propriétaires.

La modularité progressive du système d'information du ministère va ainsi favoriser **l'innovation numérique** et cette démarche s'intègre pleinement avec la mise en œuvre d'une démarche Agile. La réalisation de logiciels en ***mode Agile*** répond en effet aux besoins de réactivité aux changements de l'environnement et des organisations ainsi qu'à l'évolution rapide de la technologie, avec l'objectif d'apporter de la souplesse dans les modes de travail et un gain de temps en termes de livraison de nouvelles versions, pouvant même viser, selon la maturité des équipes, à un mode de livraison en continue (approche DEVOPS).

Pour rappel, comme le stipule le *Manifeste Agile*, les méthodes Agile s'appuient sur 4 valeurs clés :

- une **approche centrée sur les individus et leurs interactions** plus que sur les processus et les outils
- des **logiciels opérationnels** plus qu'une documentation exhaustive
- la **collaboration** avec les clients (en l'espèce, clients internes ou usagers) plus que la négociation contractuelle
- l'**adaptation au changement** plus que le suivi d'un plan.

À l'heure actuelle, les méthodes de développement ou d'intégration agiles telles que la méthode PHARE, le framework SAFe® ou l'approche DEV(sec)OPS sont mises en place au sein du ministère sur de nombreux projets, que ce soit sur des projets d'innovation ou bien sur des sujets d'envergure tels que les services numériques du socle. Ces démarches Agile devront être de plus en plus généralisées.

3.1.2. *une plus grande standardisation des échanges*

Dans une logique d'optimisation des développements et de la maintenance des applicatifs, il est indispensable de standardiser les échanges de données entre logiciels. Cela implique d'assurer une plus grande indépendance entre ces derniers, c'est-à-dire de ***limiter les interconnexions propriétaires entre logiciels au sein d'un même SI, ou entre SI.*** Ces développements spécifiques sont en effet souvent sources de complexification des mises à jour de versions ou encore d'incompatibilités techniques (ex : incompatibilité d'interfaces, blocage de flux, etc.) en cas d'évolution des systèmes (ex : développement d'un nouveau logiciel, montée de version, etc.), voire de failles de sécurité importantes.

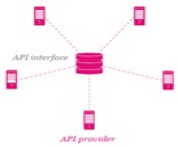
La standardisation des flux entre logiciels implique de favoriser l'interopérabilité par un **recours aux standards**, protocoles et formats d'échanges ouverts.

La directive n°19 portant sur les échanges inter-applicatifs définit les règles applicables pour ces échanges. Les règles énoncées participent à la maîtrise des échanges inter-applicatifs et à la rationalisation des technologies mises en œuvre.

La standardisation des échanges implique de ***trouver un degré adapté d'homogénéisation des flux***. En effet, une homogénéité absolue est source de vulnérabilité et de dépendance. Elle est hors d'atteinte pour un parc matériel et logiciel aussi important que celui du ministère des armées. À l'inverse, une hétérogénéité trop grande pose un problème de cohérence, de compatibilité, de maintien de la compétence, de coût d'exploitation et à terme de maîtrise du système d'information. En conséquence, une hétérogénéité maîtrisée doit être recherchée, tout en respectant les préconisations technologiques inscrites dans le cadre de cohérence technique (CCT) dont c'est d'ailleurs l'un des principes directeurs.

Cette standardisation des flux entre logiciels repose principalement sur une « **APIsation** » des logiciels, c'est-à-dire une capacité à développer des APIs afin d'élargir l'accessibilité aux ressources (services et données) et à centraliser l'acquisition et la publication des données sur une plateforme dédiée (via un API Manager) quelles que soient les modalités techniques des échanges définies.

A l'instar d'une voiture composée de plusieurs sous-systèmes conçus par différentes équipes spécialisées qui communiquent entre elles tout au long du processus de conception....



....une API est une brique logicielle qui permet à un SI de partager des données, du contenu et des fonctionnalités avec d'autres, de créer de nouveaux services basés sur ces données, ce contenu et ces fonctionnalités (c'est-à-dire en utilisant une ou plusieurs briques). Le service créé peut utiliser une ou plusieurs API du même fournisseur ou

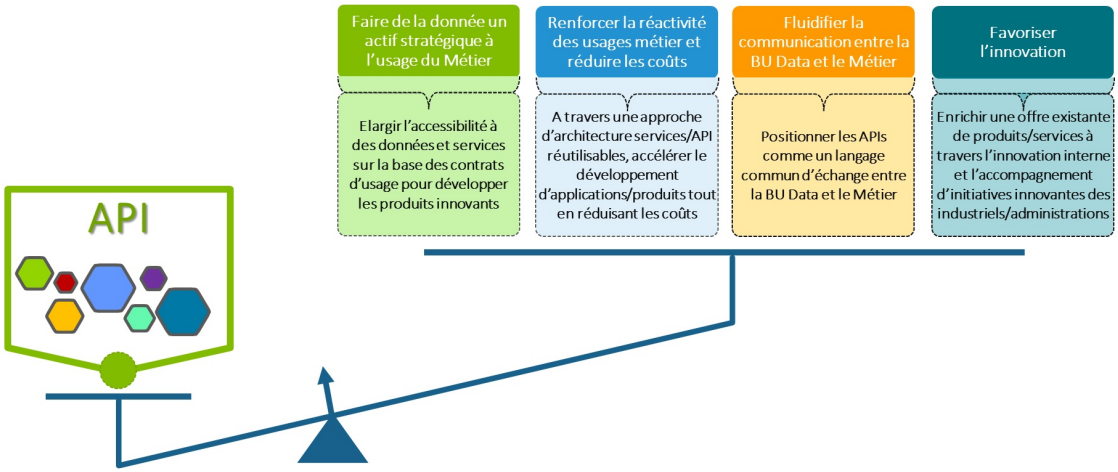
L'APIsation vise ainsi à rendre les logiciels indépendants les uns des autres et à créer des interfaces normées. Cette démarche est notamment indispensable en cas de mise en place de robotisation de processus (RPA), de logiciels d'intelligence artificielle (IA), qui impliquent des échanges de données automatisés de masse et à haute fréquence.

Parmi les trois défis majeurs de la transformation numérique du ministère, la maitrise et le traitement des données sont au cœur de la performance digitale. Manipulées via les processus, traitées par les applications, les données sont en effet au cœur du système d'information. À ce titre, leur qualité a un impact majeur sur l'exécution des missions du ministère dépendant du système d'information et par la même sur sa performance. L'instruction ministérielle n°2 relative à la gouvernance des données vise justement à accompagner la maitrise et le traitement des données pour en faciliter le partage et la circulation et en faire un vecteur d'innovation dans toutes les activités couvertes par le ministère.

L'objectif de la directive n°35 portant sur la gouvernance de la qualité des données du ministère est de garantir la qualité des données en fixant les règles d'organisation, de production de travaux de standardisation et de prise en compte de ces productions par les projets de systèmes d'information. Il est donc obligatoire d'insérer les clauses relatives à la gouvernance de la qualité des données proposées par cette directive dans tout cahier des clauses techniques particulières (CCTP) de marché public relatif à l'acquisition ou à la maintenance de système d'information.

L'exposition de la donnée passe ainsi par une offre de services mis en œuvre par des API. Le recours aux API offre de nombreux avantages en matière d'interopérabilité, d'impact, d'innovation et de réduction des coûts et constitue un levier stratégique de mise en valeur du SI ; la politique API du ministère des armées vise 4 principaux enjeux :

- faire de la donnée un actif stratégique à l'usage des métiers ;
- renforcer la réactivité des usages métier et réduire les coûts ;
- fluidifier la communication entre les métiers ;
- favoriser l'innovation.



Les lignes directrices pour guider la conception et le développement des APIs sont développées plus amplement dans le document de politique sur les API (à paraitre).

3.1.3. *Une indépendance vis-à-vis de l'infrastructure*

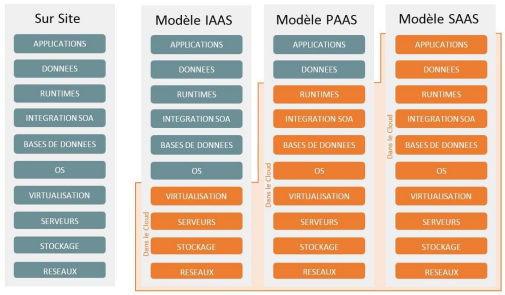
L'***indépendance du logiciel*** au regard de l'infrastructure est un facteur clé de la mise en place de la politique logicielle ministérielle et facilitera, à terme, l'évolution de notre système d'information vers une stratégie de Cloud Computing. Il est notamment fréquent que les logiciels développés s'appuient sur des infrastructures spécifiques, en particulier du fait de contraintes imposées par les intégrateurs, rendant de facto d'autant plus complexes le déploiement de nouveaux logiciels ou la mise en place d'interfaces entre applicatifs. Outre la réduction des coûts liés à l'infrastructure physique, cette indépendance permet de disposer d'un environnement SI plus flexible et de simplifier et centraliser si besoin l'administration des logiciels.

Dans le domaine du Cloud computing, on identifie 3 modèles principaux de services vers lesquelles notre système d'information pourra évaluer :

- le modèle Infrastructure as a Service (IaaS) ;
- le modèle Plateform as a Service (PaaS) ;
- le modèle Software as a Service (SaaS).

A minima il s'agit d'adapter notre SI à un modèle IAAS. Les nouvelles applications devront donc être autant que possible sans adhérence logicielle avec le socle d'infrastructure.

Ce développement « sans adhérence logicielle » peut reposer sur des processus de « ***virtualisation*** » voire de « ***containerisation*** » permettant de le dissocier physiquement de son infrastructure support. La mise en place d'outils de virtualisation permet de simplifier considérablement l'articulation entre les infrastructures techniques (datacenters, serveurs, équipements de communication, etc.) et les logiciels développés par une organisation.



Une réflexion sur l'empreinte géographique de l'utilisation du logiciel doit également être menée, impliquant potentiellement l'usage de technologies de edge-computing (il s'agit d'une architecture informatique distribuée ouverte qui présente une puissance de calcul au plus près de la donnée collectée, en vue de remonter en central seulement les informations nécessaires voire déjà traitées). Une réflexion préalable doit être dans tous les cas menés à ce sujet (localisation des sources de données et des bénéficiaires, puissance de calcul estimée, volume de données manipulées, etc.). En effet, les ressources matérielles, et particulièrement réseau, ne sont pas infinies, et ces technologies permettent naturellement de les économiser. Elles peuvent avoir un impact sur la façon de développer ou d'intégrer le logiciel. Une vigilance particulière devra être apportée à la continuité du service (y compris durant les phases d'évolution majeure du système d'information) et à la qualité des flux de données entrants et sortants du logiciel.

La mise en œuvre de ces nouvelles technologies suppose de maîtriser parfaitement l'architecture du SI, les interdépendances existantes et les conséquences attendues du déploiement d'une telle technologie, dans une logique toujours d'approche orientée services et usages métier.

3.1.3.1. *un logiciel intègre et sécurisé*

L'intégration, au sein d'un système d'information, de logiciels pouvant interagir entre eux, nécessite un haut niveau de confiance envers chacun d'eux et pose la question ***de la maîtrise, l'intégrité et la sécurité des données***. De plus, dans un esprit général de *« on ne le dit qu'une fois »*, les données doivent être disponibles, selon leur catégorie, à ***un seul et même endroit***, facilitant ainsi maintien à jour et sécurité générale.

Cette confiance s'obtient de différentes manières, entre autres par :

- l'évaluation de sécurité* d'un produit par un centre spécialisé qui est un préalable nécessaire à une qualification formelle ;
- la disponibilité du code source documenté avec le droit de le recompiler à des fins d'analyse qui est un facteur de confiance. Cette disponibilité peut être exigée, notamment pour les produits qui concourent à la sécurité ;
- l'application de la directive « développements sécurisés ». En effet, une approche périmétrique (chiffrement, pare-feu, détection d'intrusion, etc.) de la sécurité des systèmes d'information n'apporte pas de réponse satisfaisante aux menaces visant les couches applicatives : injections SQL1, injections de codes malveillants, etc.

Tant le COMCYBER que l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) font régulièrement état d'attaques ou de vulnérabilités de ce type permettant une intrusion pouvant conduire à un vol massif de données. C'est dans ce contexte de lutte contre ces menaces que s'inscrivent la sécurité applicative et la directive n°40 portant sur le développement des applications informatiques et des logiciels robustes du ministère des armées (DIR DEV.SEC). Il s'agit d'un ensemble d'exigences et de règles permettant de réaliser au profit du ministère des armées des développements d'applications informatiques ou des logiciels robustes capables de fonctionner correctement en présence d'événements inattendus (valeurs hors normes ou mal formatées, etc.).

De façon générale, la mise en place de logiciels dans le cadre d'un SI modulaire doit s'appuyer sur un tissu industriel de confiance et le respect des référentiels en vigueur dans l'administration :

- référentiel général d'interopérabilité (RGI) ;
- référentiel général de sécurité (RGS).

Cette approche s'inscrit pleinement avec la démarche d'homologation d'un système d'information, composante de la gestion de la sécurité réalisée tout au long du cycle de vie d'un système d'information, dont les principes et les démarches à suivre sont définis dans la directive n°27 portant sur l'homologation des systèmes d'information du ministère (DIR HSI).

En termes de sécurité et pour éviter une sensibilité trop grande liée à un amalgame trop important de données non classifiées à un seul et même endroit, les technologies **blockchain** pourront être utilisées. La blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle. Par extension, une blockchain (littéralement une « chaîne de blocs ») désigne une base de données sécurisée et décentralisée, qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne. Une blockchain peut donc être assimilée à un grand livre comptable transparent, pseudonyme et infalsifiable.

4. MISE EN OEUVRE DE CETTE POLITIQUE LOGICIELLE

La présente politique logicielle ouvre la voie à l'utilisation de nouvelles technologies visant à harmoniser l'utilisation des logiciels au sein du ministère et à adopter une démarche véritablement orientée services et usages métier, c'est-à-dire en capacité de répondre au plus près des besoins des usagers et des agents publics.

Cependant, pour l'ensemble du SIC du ministère des armées, la continuité du service est une priorité, y compris durant les phases d'évolution majeure du système d'information. De fait, il n'est pas question de faire table rase de l'existant pour mettre en place un système cible radicalement différent. Ce dernier reste un objectif à long terme, hors d'atteinte dans l'immédiat, car les organisations et les méthodes de travail doivent

s'adapter et accompagner le changement. Ce dernier point est de la responsabilité de la maîtrise d'ouvrage et des groupes utilisateurs. Il s'agit donc d'une démarche par paliers privilégiant des phases courtes. De plus, les réseaux et leurs capacités actuelles conditionnent les capacités d'évolution du SI.

Enfin, la maîtrise de cette évolution suppose un suivi adapté des configurations.

4.1. **initialiser le cadre d'application de cette politique**

Avant d'acquérir ou de développer un logiciel, il est indispensable pour le service demandeur d'identifier dans quel cadre il sera en mesure d'appliquer la présente politique logicielle.

Pour cela, ***6 questions clés*** doivent être identifiées en amont :

- **quelles sont les spécificités du besoin** (ex : problématique opérationnelle, problématique de sécurité, de confidentialité, etc.), permettant de fixer le contexte et d'orienter les choix logiciels ? Une analyse du parcours usager a-t-elle été faite ?
- **quelle est l'échelle d'application du logiciel** , tant d'un point de vue géographique qu'en termes de nombre d'utilisateurs ? Cette dimension peut en effet venir induire des contraintes d'application ;
- **quels sont les types de « briques » nécessaires au développement du logiciel cible** ? Sont-elles existantes / ou en cours de développement au sein du ministère ; des experts sont-ils disponibles ou en cours de recrutement ? Le cas échéant, le calendrier d'acquisition / déploiement est-il contraint ? Les réponses à ces questions demandent une action soutenue en continue, en amont, d'urbanisation exhaustive et évolutive des systèmes d'information existants ou en cours de déploiements et des ressources / expertises disponibles ;
- **existe-t-il déjà des briques mutualisées que je peux intégrer** ?
- **les données que je souhaite mettre en œuvre sont-elles produites par ailleurs ?** Dans l'affirmative, existe-t-il une API offrant les données ou les services associés dont j'ai besoin ?
- **les documents contractuels découlant du projet prennent-ils en compte les différents éléments de la présente politique ?**

L'anticipation de ce cadre d'application fournit une aide à la décision et permet en outre de sécuriser l'acquisition ou le développement d'un logiciel ministériel le cas échéant.

Il convient par ailleurs de favoriser l'adoption et la maîtrise de ***logiciels accessibles à tous les utilisateurs***. En conséquence, seront privilégiés les logiciels :

- conformes au RGAA ;
- présentant une interface en français, incluant les aides interactives et les documentations ;
- supportant le mécanisme de multilinguisme* pour une utilisation dans un contexte international quand le besoin est avéré ;
- implémentant une approche de conception Web (connu sous le terme anglais de Responsive Web design) qui vise à l'élaboration de sites offrant une expérience de lecture et de navigation optimales pour l'utilisateur quelle que soit sa gamme d'appareil (téléphones mobiles, tablettes, liseuses, moniteurs d'ordinateur de bureau) ;
- recourant et implémentant des interfaces conformes aux normes et standards en vigueur sur les OS support. Ces logiciels doivent être également en mesure d'implémenter les chartes graphiques en vigueur.

4.2. privilégier les logiciels à coût, risques et efficacité comparables

Le choix d'une solution est fondé sur une analyse de décisions, telle l'évaluation du coût prévisionnel global* de possession au moyen de la méthode MAREVA 2*, la disponibilité du code source, son caractère libre ou attaché à un grand fournisseur, son type de couplage - lâche (standardisation des interfaces) ou intégré, pour ne citer que ces exemples.

Outre les avantages liés à la disponibilité du code source, les logiciels libres permettent entre autres de favoriser le respect des standards et s'intègrent pleinement avec une volonté d'une architecture modulaire du SI.

Le ministère des armées doit s'efforcer, avant toute acquisition ou tout développement interne ou sous-traité, d'identifier dans le domaine du logiciel libre disponible des solutions alternatives à des solutions intégrées proposées par de grands fournisseurs, de fonctionnalités équivalentes ou approchantes des besoins exprimés.

Il faut donc rechercher la libre disponibilité pour les logiciels acquis par le ministère des armées, cette recherche devant s'appuyer sur plusieurs axes d'analyse, entre autres :

- la taille et la complexité du système d'information du ministère, la rapidité et l'automatisation des mises à jour système et applicatives :
- à coût global, risques [2] et efficacité opérationnelle comparables, le logiciel libre est privilégié ;
- l'utilisation de certains logiciels libres peut être imposée aux contractants ;
- le bien fondé de solutions comprenant tout ou partie de logiciels libres doit être systématiquement étudié ;
- la capacité de passage à l'échelle de la solution choisie (dans le périmètre cible des utilisateurs du logiciel), notamment sur le critère de performance, doit être un facteur discriminant ;
- l'automatisation des processus de validation et de déploiement des mises à jour système et applicatives, notamment sur le critère de rapidité pour répondre particulièrement à des besoins de sécurité ;
- les impacts sur l'hébergement et la courbe de complexité, quand ils sont utilisés de façon massive sur les réseaux étendus, doivent également être étudiés ;
- l'analyse juridique du type de licence associée à chaque logiciel open source (Apache, BSD, GNU, MIT, ...) (Cf. Annexe III sur les licences open source).

4.3. rénover le système d'information

La mise en œuvre de cette politique logicielle n'est pas réduite aux seuls nouveaux développements. La rénovation de notre système d'information (le legacy) peut revêtir de nombreuses formes. Afin de mieux préparer le legacy à des montées de version de plus en plus fréquentes du socle d'infostructure, la première étape de cette rénovation consiste à réaliser une étape d'observation, de recensement des composants logiciels présentant des adhérences entre le SI et ledit socle. La deuxième étape consiste alors à identifier des solutions alternatives pouvant supprimer, à minima atténuer les adhérences. La dernière étape identifie une feuille de route de rénovation du système d'information du ministère en fonction des effets de gains (humains et financiers) obtenus par l'introduction de nouveaux composants ou techniques.

La logique de standardisation va de pair avec la mise en œuvre d'une ***architecture scalable et résiliente*** (pas de session côté serveur, par exemple).

Elle doit également garantir la compatibilité des logiciels et utiliser des briques d'infrastructures et/ou mutualisées et notamment les composants proposés par Défense Plateforme. Si les systèmes legacy ne doivent pas forcément faire l'objet d'investissements lourds pour permettre cette standardisation (ou alors de façon opportuniste), tout nouveau logiciel intégré ou développé au sein du ministère doit respecter ces contraintes.

4.4. développer l'acculturation et les compétences numériques

Que l'on soit dans une démarche de « faire-faire » ou un développement en interne pour concevoir et réaliser de nouveaux logiciels, il convient dans tous les cas de conserver la maîtrise du logiciel en maintenant une réelle compétence technique d'architecture, de spécification, de développement, d'évaluation et d'intégration mais également une compétence méthodologique et managériale pour le pilotage des projets SIC.

La mise en place de nouvelles technologies qui ne sont pas toujours matures et pérennes, et l'utilisation de méthodes innovantes au regard de la culture existante implique donc une ***acculturation par le personnel et la nécessité d'une acquisition de compétences adaptées****.

En interne, la montée en compétence des équipes, *via* notamment des formations aux démarches Agile, notamment le framework « SAFe® » ou la méthode PHARE [3] est un prérequis. Les nouveaux rôles induits par cette méthode devront être définis et adaptés au contexte du ministère.

Il est à noter que, selon la valeur de services apportés à l'usager ainsi que selon la stratégie du ministère en matière de compétences, la question de l'internalisation ou de l'externalisation des ressources se pose. Dans ce cadre, la politique du développement interne (à paraitre) présente une matrice de décision du faire ou du faire-faire pour les projets du legacy ou pour les services digitaux.

En parallèle, la technicité induite par ces nouvelles technologies peut nécessiter des expertises parfois non disponibles en interne. De fait, la mise en place de logiciels spécifiques pourra impliquer d'avoir recours à de ressources externes spécialisées, permettant, selon les choix du ministère, la montée en compétences d'équipes internes ou le maintien de ces expertises en externe. Dans tous les cas de figure (internalisation ou externalisation), une expertise technologique d'une capacité significative doit être maintenue, à minima pour assurer une spécification et un pilotage contractuel de bon niveau, en ayant notamment pratiqué ces technologies.

Ces éléments témoignent de la nécessité de mettre en œuvre une véritable politique de gestion des compétences.

En tant que maître d'ouvrage de systèmes, le ministère des armées doit posséder une expertise significative en matière de logiciels, reposant sur des compétences spécifiques, approfondies, mises à jour régulièrement et en nombre suffisant. Le pilotage de cette expertise suppose la mise en place d'une véritable gestion des compétences en matière de SIC.

Afin de garantir la disponibilité d'une réelle expertise, notamment sur les nouvelles techniques informatiques, la formation en interne sera complétée par un examen de certification des connaissances pour les experts volontaires.

Cette gestion des compétences s'inscrit dans le contexte plus général de la gestion de compétence de la famille professionnelle SIC au sein du référentiel des emplois ministériel (REM).

Appliquée aux logiciels, elle doit comprendre :

- le recensement des pôles de compétence existants, de leur patrimoine technique et l'identification des compétences à acquérir ;
- la mise en réseau des pôles de compétence ;
- l'animation de ces réseaux ;
- la mise en relation des maîtrises d'ouvrage avec les pôles de compétence ;
- la prise en compte des nouvelles compétences en matière de logiciels dans la mise à jour du REM ;
- l'adéquation des formations des personnels du ministère de la défense aux technologies actuelles et futures et leur coordination ;
- le maintien d'une capacité à faire interne dûment dimensionnée.

4.5. **assurer une ville technologique et numérique**

Si aujourd'hui la standardisation passe par une stratégie d'APIsation des systèmes, il reste nécessaire de maintenir un niveau de veille suffisant pour anticiper et comprendre les évolutions en la matière, notamment en termes d'organisation et d'instrumentalisation du management des API.

Il en est de même pour tous les éléments de la pile logicielle. Les évolutions des conditions d'utilisation de certains composants, notamment sur l'axe financier, peut amener à revoir notre politique sur l'utilisation de certains composants (au travers du CCT) ou directement par les directions d'application en faisant évoluer leur SI avec des solutions alternatives.

Une veille technologique est donc à assurer afin de prendre en compte dès que possible les évolutions. Cette veille, de responsabilité de tous, doit être remontée et enrichir le CCT.

Par ailleurs, si l'évolution des services offerts aux usagers nécessite une écoute de leurs besoins, une autre source d'évolution consistant en une veille technologique et numérique reste nécessaire. Elle permet d'anticiper les besoins des usagers mais également de connaître les évolutions du marché en matière technologique, et de choisir de façon éclairée de les suivre ou non (ATAWAD [4] , BYOD [5] , chatbot, etc.).

La DGNUM, avec l'appui du CASID, est en charge de cette veille technologique et numérique.

5. ASSURER LE SUIVI DE LA MISE EN ŒUVRE DE CETTE POLITIQUE

Sous l'égide du Comité Exécutif du Conseil du NUMérique et des SIC, CECNUM, placé sous la présidence du DGNUM, la mise en œuvre de cette politique devra être assurée par les trois instances de gouvernance des SIOC, SIST et SIAG du ministère des armées dans le cadre des projets et programmes SIC relevant de leur responsabilité.

Les opérateurs défense appliqueront cette politique générale pour les aspects transverses du SIC défense. La DIRISI sera l'interlocutrice privilégiée des maîtrises d'ouvrage en matière d'infrastructure technique, de mise en œuvre et de soutien, dès les phases des projets entrant en amont de son périmètre de responsabilité.

Les commissions « métier » (CSIOC, CSIAG et CIST) et les commissions ministérielles spécialisées veilleront quant à elles au respect de cette politique générale.

Les formes du contrôle d'application de cette politique générale tiendront compte :

- de l'état d'avancement dans le cycle de vie des projets et programmes et de la maturité des informations à chaque jalon ;
- du respect des règles de la mise en concurrence pour les logiciels en acquisition, à charge pour le cahier des clauses techniques particulières (CCTP) de tenir compte des orientations indiquées dans le présent document.

Les directions d'application et les maitrises d'œuvre (étatiques et industrielles) (dans le cadre du respect du cahier des charges) appliqueront cette politique générale du logiciel. Les demandes de dérogations feront l'objet d'une saisine de la DGNUM par l'organisme d'appartenance de la maîtrise d'ouvrage concernée. Les cas structurants seront débattus dans les comités ad hoc. Les questions d'interopérabilité opérationnelle interalliée devront être traitées de façon prioritaire.

6. ANNEXES

6.1. **Annexe I. Textes de référence**

Ce document s'inscrit dans un cadre ministériel et interministériel notamment défini par :

Nom référence	Objet	Accès Intradef ou internet

Circulaire Ayrault, de septembre 2012	Relative aux orientations pour l'usage des logiciels libres dans l'administration	Internet, site de la DINSIC
Loi numérique	Loi pour une République Numérique du 7 octobre 2016	Internet, site de la DINSIC
	Politique de contribution de l'État aux logiciels libres du 15 mai 2018	Internet, site de la DINSIC
Arrêté du 20 avril 2016 portant approbation du référentiel général d'interopérabilité	Référentiel général d'interopérabilité (RGI)	https://synoptic.intradef.gouv.fr/ressource-documentaire/referentiel-general-d-interoperabilite-rgi-v2-approuve-par-arrete-du-20-avril
RGAA - Version 2016 publiée le 23 juin 2016	Référentiel général d'accessibilité pour les administrations (RGAA)	https://references.modernisation.gouv.fr/rgaa/2016/index.html
RGS	Référentiel général de sécurité (RGS)	
Décret n° 2018-532 du 28 juin 2018	fixant l'organisation du système d'information et de communication de la défense et portant création de la direction générale du numérique et des systèmes d'information et de communication (DGNUM)	
Lettre n°2776/DEF/CAB/CC5A du 28/03/2013	Politique ministérielle des SIC du ministère de la défense	https://synoptic.intradef.gouv.fr/ressource-documentaire/politique-du-systeme-d-information-du-ministere-de-la-defense

	Plan Stratégique pour l'Administration Electronique qui comporte un volet sur l'emploi des logiciels par les administrations	
Circulaire n°5725/SG du 17/07/2014 relative à la PSSIE	Politique de la sécurité des systèmes d'information de l'État	https://synoptic.intradef.gouv.fr/ressource-documentaire/circulaire-ndeg-5725sg-du-17-juillet-2014-relative-la-politique-de-securite
Directive n°40/DEF/DGSIC du 17 mai 2017	Portant sur le développement des applications informatiques et des logiciels robustes du ministère de la Défense (DIR DEV.SEC)	https://synoptic.intradef.gouv.fr/ressource-documentaire/directive-ndeg40defdgsic-du-17-mai-2017-portant-sur-le-developpement-des
Directive N°27/DEF/DGSIC	Portant sur l'homologation des systèmes d'information du ministère (DIR HSI).	https://synoptic.intradef.gouv.fr/ressource-documentaire/directive-ndeg27defdgsic-du-24-janvier-2013-portant-sur-l-homologation-des
Directive n°19/DEF/DGSIC du 24 aout 2011	Portant sur l'architecture technique applicative, les normes et les standards devant être appliqués ou utilisés par les maîtrises d'ouvrage et maîtrises d'œuvre des systèmes informatiques pour les échanges inter-applicatifs.	https://synoptic.intradef.gouv.fr/ressource-documentaire/directive-ndeg19defdgsic-du-24-aout-2011-portant-sur-les-echanges

CCT	Le Cadre de Cohérence Technique [CCT] constitue le référentiel ministériel des préconisations et des choix techniques dans le domaine des SIC.	https://synoptic.intradef.gouv.fr/ressource-documentaire/cadre-de-coherence-technique-des-sic-du-ministere-de-la-defense
ATG	Le document ATG a vocation à fournir une vision d'ensemble de l'architecture technique SIC du ministère. Il s'adresse à tous les acteurs du domaine SIC.	https://synoptic.intradef.gouv.fr/ressource-documentaire/architecture-technique-generale-v1
Note n° 266 /ARM /DGSIC/DG/ DR du 04 juillet 2017	Politique en matière de gestion des actifs logiciels au ministère des armées	https://synoptic.intradef.gouv.fr/sites/default/files/20170704_dr_dgsic-dg_266-no-politique-en-matiere-de-gestion-des-actifs-logiciels-au-ministere-des-armees.pdf
Directive N° 37 /DEF/DGSIC/NP	Traitement d'un dossier éligible à l'article 3 du Décret N° 2014-879 du 1er aout 2014 relatif au système d'information et de communication de l'État	https://synoptic.intradef.gouv.fr/ressource-documentaire/directive-ndeg37-defdgsicnp-du-8-fevrier-2016-portant-sur-le-traitement-d-un
MAREVA2 :	Méthode d'Analyse et de REmontée de la Valeur est une nouvelle version de la méthode pour évaluer les projets informatiques.	https://references.modernisation.gouv.fr/mareva-2

Instruction ministérielle n°1/ARM/DGNUM du 24/10/2018	Portant sur le visa de conformité des projets SIC (article 5) à la politique du système d'information du ministère	https://synoptic.intradef.gouv.fr/sites/default/files/20181025_np_dgnum_2018-253-im-portant-sur-le-visa-de-conformite-des-10180896.pdf
Directive N°35/DEF/DGSIC	Portant sur la gouvernance de la qualité des données du ministère	https://synoptic.intradef.gouv.fr/ressource-documentaire/directive-ndeg35defdgsic-du-11-juin-2015-portant-sur-la-gouvernance-de-la
Guide n°15/ARM/DGSIC	Porte sur l'agilité dans le cadre de la transformation numérique	https://synoptic.intradef.gouv.fr/ressource-documentaire/guide-ndeg15armdgsic-portant-sur-l-agilite-dans-le-cadre-de-la-transformation
Note N°196/DEF/DGSIC/DG/NP	Schéma directeur ministériel de la formation SIC	https://synoptic.intradef.gouv.fr/ressource-documentaire/schema-directeur-ministeriel-de-la-formation-sic
Directive N°30/DEF/DGSIC	Portant sur la mise en œuvre de la démarche d'archivage des contenus gérés par un système d'information et de communication	https://synoptic.intradef.gouv.fr/ressource-documentaire/directive-ndeg30defdgsic-du-05-decembre-2013-portant-sur-la-mise-en-oeuvre-de

6.2. **Annexe II. Qu'est-ce qu'un logiciel et dans quel contexte s'insère-t-il ?**

Ce document portant sur la politique générale des ***logiciels***, il convient de clarifier le vocabulaire utilisé afin d'éviter toute confusion.

Les *Systèmes d'information*

Le décret du 28 juin 2018 fixant l'organisation du système d'information et de communication de la défense et portant création de la direction générale du numérique et des systèmes d'information et de communication fournit une définition éclairante d'un système d'information dans son Chapitre Ier :

« *Le système d'information et de communication de la défense est constitué de l'ensemble organisé des ressources permettant de collecter, traiter, transmettre et stocker les données sous format numérique qui concourent aux missions du ministère, à l'exception des ressources mises en œuvre par la direction générale de la sécurité extérieure*. »

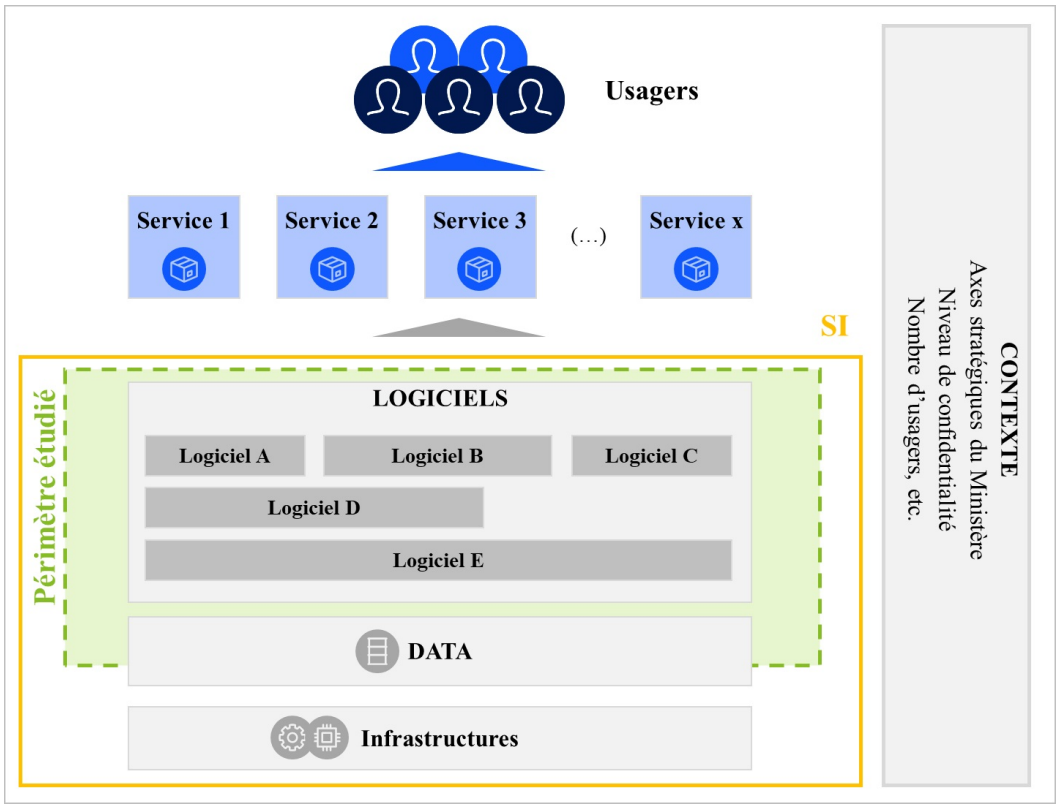
De fait, le système d'information impacte l'organisme ou l'entreprise à trois niveaux :

- le niveau fonctionnel : le SI vient supporter les processus des entreprises ;
- le niveau tactique : l'information captée et traitée par le SI permet de produire des indicateurs servant à la prise de décision ;
- niveau stratégique : le SI, de par le fait qu'il est omniprésent dans l'environnement de l'entreprise (interne comme externe) devient un enjeu stratégique devant contribuer à assurer la pérennité de ses missions.

Les logiciels

Les logiciels correspondent à l'ensemble des programmes et des procédures nécessaires au fonctionnement d'un système d'information. Ils en sont donc des composants.

Comme illustré dans le schéma ci-après, le logiciel s'insère dans un système d'information. Il peut interagir avec d'autres logiciels et vise à répondre à un ensemble de services dédiés aux utilisateurs ou aux agents ministériels amenés à l'utiliser.



6.3. Annexe III. Qu'est-ce qu'un logiciel Open Source ? qu'en est-il des licences ?

Une définition précise de ce que signifie Open source a été rédigée par l'OSI (Open Source Initiative). Elle est aujourd'hui reconnue de manière universelle.

Cette définition comporte dix points. Les principaux sont les 3 premiers qui composent cette définition :

- libre redistribution : la licence ne doit pas interdire à qui que ce soit de vendre ou donner le programme ;
- code source : la licence doit permettre la distribution du logiciel sous forme de code source. Si celui-ci n'accompagne pas le programme, il doit être disponible de manière facile et gratuite ;
- travaux dérivés : la licence doit permettre des modifications et des travaux dérivés. Ces travaux doivent pouvoir être distribués sous les mêmes termes de licence que le logiciel original. La licence doit au minimum permettre de redistribuer les travaux dérivés sous la même licence. Elle ne doit pas nécessairement l'obliger.

Mis à la disposition du grand public, ce code source est généralement le résultat d'une collaboration entre programmeurs, réunis au sein de communautés.

Les licences libres ont été créées dans le but de proposer une alternative aux licences propriétaires existantes, représentées par le Copyright© ou le TradeMark ™. Les droits d'auteur sont détenus par le développeur qui a écrit le programme ou par l'entreprise qui l'emploie.

L'auteur des droits est libre de changer les conditions de la licence ou d'y apporter des aménagements. Le logiciel libre se définit par le respect de libertés fondamentales :

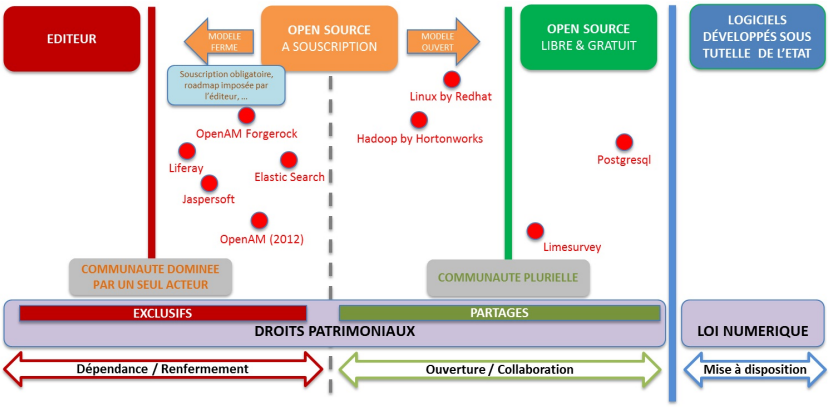
- la liberté d'utiliser le logiciel à n'importe quelle fin ;
- la liberté de modifier le programme pour répondre à ses besoins ;
- la liberté de redistribuer des copies ;
- la liberté de partager avec d'autres les modifications apportées.

Quand une licence offre à ses utilisateurs toutes ces libertés, le logiciel peut être qualifié de logiciel libre. Un programme Open Source n'est donc pas uniquement un programme où les sources sont diffusées gratuitement mais il s'agit d'un logiciel distribué avec une licence libre où est inscrit le droit, à l'utiliser, le modifier, le redistribuer librement. C'est cela qui fait qu'un logiciel est dit « Open source ». Les licences Open Source sont classées selon plusieurs critères :

- le respect des conditions d'une licence de logiciel libre ;
- la présence d'un copyleft [6] ou non ;
- la compatibilité avec la GNU GPL (sauf indication contraire, les licences compatibles le sont avec les versions 2 et 3 de la GPL) ;
- l'identification de cas spécifiques dans l'utilisation du logiciel lié.

Par contre, l'utilisateur (ou l'entreprise) finale du logiciel Open Source, n'est pas libre. En effet, il est lié par les termes de la licence fourni avec le logiciel et donc doit se soumettre aux conditions indiquées dans cette licence. Si l'utilisateur ou l'entreprise utilisatrice refuse les conditions indiquées dans la licence, cela entraîne le non droit d'utiliser ce programme.

Les logiciels Open Source ont plusieurs modèles économiques dont le schéma ci-dessous résume les 5 grandes familles.



Les enjeux portés par l'Open Source sont multiples. On peut notamment citer les enjeux suivants :

- **enjeu n°1 - réduction des coûts en ciblant essentiellement les investissements sur le métier :** L'investissement porte sur l'intégration et le développement de logiciels spécifiques au cœur de métier du ministère. Contrairement au modèle propriétaire, la licence Open Source est gratuite et définit les termes d'utilisation du logiciel ;
- **enjeu n°2 - pérennité et interopérabilité par le respect des standards ouverts :** Le respect des standards ouverts permet d'assurer la pérennité des applications internes. Il favorise également l'interopérabilité des systèmes inter et intra-entreprises, ainsi qu'entre partenaires ;
- **Enjeu n°3 - conformité & sécurité obtenues par l'accès au code source :** Le code des logiciels open source est ouvert et analysable : il y a donc la possibilité de vérifier la conformité d'un logiciel avec les réglementations. Cela induit également une sécurité par transparence. En effet, si la disponibilité du code source ne garantit pas la sécurité, la capacité de modifier celui-ci garantit au moins la possibilité d'obtenir un correctif en cas d'exposition à une vulnérabilité ;
- **enjeu n°4 - réactivité obtenue par le développement communautaire :** Les « bonnes » communautés développent chaque partie des logiciels Open Source. Le développement communautaire favorise en outre la réactivité lorsqu'il s'agit de corriger une anomalie de fonctionnement ou une faille de sécurité ;
- **enjeu n°5 - favoriser l'agilité :** L'open source est un levier qui permet de diminuer les contraintes et de proposer des solutions « sur étagère » proches du besoin recherché pour chaque itération du développement du logiciel, l'intégration progressive étant favorisée par notamment le respect des standards.

Par ailleurs, dans la continuité de l'action interministérielle sur le logiciel libre initiée par la circulaire Ayrault de septembre 2012, la loi pour une République Numérique du 7 octobre 2016 donne aux codes sources de certains systèmes d'information, relevant uniquement des SIAG, le statut de documents administratifs communicables et réutilisables.

Engagé dans la modernisation de son infrastructure informatique et le développement de nouveaux services, l'État compte plus que jamais sur le logiciel libre et sur ses communautés. Au-delà des outils, il entend promouvoir des méthodes : le partage du code, la confiance envers les développeurs, l'accueil de la contribution. Ainsi, une politique interministérielle de contribution aux logiciels libres détaillant les modalités d'ouverture des codes sources est officiellement en vigueur depuis le 15 mai 2018.

Cette politique de contribution couvre les codes sources de tout **nouveau** logiciel développé en interne par l'administration ou par des prestataires externes pour le compte de l'administration, afin qu'ils respectent les bonnes pratiques. Pour l'ouverture de codes sources existants, des actions complémentaires seront nécessaires, telles que la définition du périmètre d'ouverture du code, sa revue qualité, sa revue sécurité, l'analyse de conformité, le respect du besoin d'en connaître et du degré de classification éventuelle des algorithmes ou commentaires et l'analyse de la propriété intellectuelle.

Les objectifs poursuivis sont notamment de guider les développeurs de la fonction publique (titulaires ou contractuels) et les prestataires de l'État, dans l'ouverture des codes sources.

Le rôle des communautés du logiciel libre est essentiel à la fois pour bénéficier de codes de qualité, maintenus, plus sûrs et améliorés en permanence, pour mutualiser les ressources et les expertises entre les services de l'État, mais également pour s'ouvrir vers l'extérieur. C'est un moyen de dynamiser les projets et de contribuer à leur pérennité.

Avec la loi pour une République numérique, l'objectif du gouvernement est double : « donner une longueur d'avance à la France dans le domaine du numérique en favorisant une politique d'ouverture des données et des connaissances » et « adopter une approche progressiste du numérique, qui s'appuie sur les individus, pour renforcer leur pouvoir d'agir et leurs droits dans le monde numérique ».

Pour ce faire, la loi s'organise autour de trois axes :

- la circulation des données et du savoir,
- la protection des individus dans la société du numérique,
- l'accès au numérique pour tous.

C'est une loi majeure pour l'informatique. Elle succède à la Loi pour la confiance dans l'économie numérique (LCEN) de 2004.

Par ailleurs, des travaux engagés sous l'égide de la DINSIC ont donné lieu à des réalisations, des offres de service ou des projets encore en cours, parmi lesquels :

- le réseau interministériel de l'état (RIE) ;
- la transformation des centres informatiques ;
- le socle interministériel des logiciels libres (SILL) ;
- la démarche open.data.gouv.fr : relative à l'ouverture des données de l'état ;
- la démarche d'API donnant lieu à un portail de publication des API ;
- la démarche « *FranceConnect* » dont une des principales réalisations est « *FranceConnect* ***Particulier*** », permettant l'authentification des particuliers (voir description) ; les composants « *FranceConnect* ***Agent*** » et « *FranceConnect* ***Entreprise*** » sont en cours de réalisation.

Ces travaux sont pris en compte par le ministère tant dans le cadre de sa politique logicielle que de la construction de son système d'information, soit en s'appuyant

directement sur les résultats de ces travaux, soit en déclinant les démarches proposées au niveau interministériel.

6.4. **Annexe IV. Glossaire**

Agrément (voir aussi Évaluation de sécurité) : reconnaissance formelle qu'un produit ou système évalué peut protéger des informations jusqu'à un niveau spécifié dans les conditions d'emploi définies. [900/DISSI/DCSSI]

Alignement stratégique IT : L'alignement stratégique consiste à mettre en adéquation la stratégie IT avec les besoins et les objectifs métiers. (Henderson, 1993) & (Chan, 1997)

Application : Une application est un ensemble de composants logiciels.

À noter : un SI au sens de SICLADE peut s'être concrétisé en différentes applications ou modules (identifiés ici comme application). En effet le niveau déclaratif d'un SI pouvant être un programme d'armement, il s'agit en fait souvent de plusieurs applications en termes de réalisation ; c'est la transversalité (échange ou partage) entre ces applications qui est recherchée. Dans les cas les plus simples, un SI = 1 Application.

API first : une interface de programmation applicative (souvent désignée par le terme API pour *Application Programming Interface*) est un ensemble normalisé de classes, de méthodes ou de fonctions qui sert de façade par laquelle un logiciel offre des services, des données à d'autres logiciels. Elle est offerte par une bibliothèque logicielle ou un service web, le plus souvent accompagnée d'une description qui spécifie comment des programmes consommateurs peuvent se servir des fonctionnalités du programme fournisseur. Concevoir son système d'information autour de la mise en œuvre d'API est ce que l'on nomme l'API first.

Architecture logicielle : l'architecture d'un système d'information (SI) se décline sous forme matérielle (équipements qui le supportent) mais aussi logicielle car un SI est composé de plusieurs applicatifs qui interagissent et nécessitent une compatibilité/interopérabilité parfaite pour garantir le service rendu par le SI. L'ensemble de ces applicatifs ou composants logiciels, constitue la configuration logicielle du SI et l'ajout, l'évolution, la suppression, le remplacement d'un composant doit faire l'objet d'un contrôle de compatibilité appelé « intégration ». La maîtrise du SI passe par la capacité à gérer la configuration logicielle et à intégrer les composants.

Architecture « User centric » : la conception centrée sur l'utilisateur ou conception orientée utilisateur (UCD, user-centered design en anglais) est une démarche de conception surtout présente en ergonomie informatique, où les besoins, les attentes et les caractéristiques propres des utilisateurs finaux sont pris en compte à chaque étape du processus de développement d'un produit. Elle s'appuie sur des critères d'ergonomie et d'utilisabilité. Cette démarche se distingue fortement d'autres démarches de conception en cherchant à adapter le produit (généralement l'interface utilisateur) à l'utilisateur final plutôt que de lui imposer un mode d'utilisation choisi par les concepteurs.

Cadre de cohérence technique [CCT] : ce document constitue le référentiel ministériel des recommandations et choix techniques relatifs au socle du système d'information du ministère des armées et aux grands composants d'architecture technique. Il a pour objet d'assurer la maîtrise et la sécurité du système d'information du ministère en tenant compte des ressources disponibles et au meilleur coût. A ce titre, il offre des garanties de service rendu, de sécurité, de maîtrise des budgets et des délais aux directions d'application. Le CCT est ouvert à l'innovation et l'évolution technologique dans le respect d'une approche globale de l'écosystème du SIC de la défense

Coût global de possession : ensemble des coûts liés à l'acquisition, l'entretien, l'emploi et l'élimination d'un système (exemple : achat, développement, déploiement, intégration, mise en œuvre, exploitation, migration, accompagnement, maintenance, etc.). Dans le cas de l'article 3 de la DINSIC, avec l'application de la méthode MAREVA2, le cout global de possession prend en compte 2 années d'utilisation.

Évaluation de sécurité/agrément : l'ANSSI entretient un catalogue des produits de sécurité « d'usage général » ayant fait l'objet d'une évaluation de sécurité débouchant sur un visa de l'agence (http://www.ssi.gouv.fr/administration/qualifications/produits-recommandes-par-lanssi/les-produits/).

Information : On appelle information tout renseignement ou tout élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement. (*Source : Instruction générale interministérielle sur la protection du secret et des informations concernant la défense nationale et la sûreté de l'État n° 1300/SGDN/ PSE/SSD du 25 août 2003 - Voir : Arrêté du 23 juillet 2010 portant approbation de l'instruction générale interministérielle sur la protection du secret de la défense nationale – NOR : PRMD1019225A*).

Intégrateur d'applications/architecte/urbaniste : au sens du Club Informatique des Grandes Entreprises Françaises (CIGREF), sous la responsabilité du chef de projet maîtrise d'œuvre, l'intégrateur d'applications participe au choix des différents composants logiciels (progiciels, bases de données, développements spécifiques…) et en assure l'assemblage dans le respect du plan d'urbanisme des systèmes d'information de l'entreprise et de l'architecture retenue pour le projet. En ce qui concerne les développements spécifiques, les travaux sont effectués soit en interne par le développeur, soit en externe avec l'aide d'une société de services.

L'architecte d'entreprise définit l'architecture du système d'information. Il garantit la cohérence de l'ensemble des moyens informatiques (matériels, applicatifs, bases de données, réseaux, middleware, système d'exploitation) et de leur évolution, en exploitant au mieux les possibilités de l'art, dans le cadre du plan d'urbanisme de l'entreprise. De ce fait, l'architecte technique est en relation étroite avec l'urbaniste du système d'information, qui en garantit l'évolution cohérente dans le respect des objectifs de l'entreprise, du domaine fonctionnel…et des contraintes externes et internes (de risques, de coûts, de délais…).

Interopérabilité : l'interopérabilité des SIC traduit la capacité à échanger des informations et à créer les conditions d'un véritable travail en commun dans le respect des règles de sécurité appropriées. Ceci implique que des informations ou des services puissent être échangés directement et de façon satisfaisante entre les SIC eux-mêmes ou leurs utilisateurs (Politique des SIC du ministère de la défense). On identifie généralement trois niveaux d'interopérabilité : technique, sémantique et organisationnelle.

Licence libératoire : un progiciel est un produit spécifique, conçu pour un usage donné et développé généralement par un éditeur ou une société de service ; on n'achète pas un progiciel : on en acquiert un droit d'usage. Le propriétaire d'une licence acquiert le droit d'utiliser le progiciel conformément aux conditions stipulées par le titulaire des droits d'auteur et aux dispositions prévues par la loi. Les logiciels en « OpenSource » sont également protégés par un droit d'auteur et il convient de lire précisément la licence qui les accompagne.

Les entreprises utilisatrices et les éditeurs interprètent parfois différemment la notion de droit d'usage des logiciels. Cet aspect se révèle d'autant plus important que les modèles de licences sont de plus en plus compliqués.

Logiciel : ensemble des programmes, des procédures et de la documentation, et des données éventuellement associées (ISO CEI 12207), relatif au fonctionnement d'un ensemble de traitement de l'information.

Logiciel libre/propriétaire : l'expression « Logiciel libre », issue de l'anglais free software, n'est pas liée à la gratuité mais fait référence à la liberté pour les utilisateurs d'exécuter, de copier, de distribuer, d'étudier, de modifier et d'améliorer le logiciel. Plus précisément, elle fait référence à quatre types de liberté pour l'utilisateur du logiciel :

- la liberté d'exécuter le logiciel pour tous les usages (liberté 0) ;
- la liberté d'étudier le fonctionnement du logiciel et de l'adapter à ses besoins (liberté 1), Pour ceci l'accès au code source est une condition requise ;
- la liberté de redistribuer des copies, donc d'aider d'autres utilisateurs (liberté 2) ;
- la liberté d'améliorer le logiciel et de publier ses améliorations, pour en faire profiter toute la communauté (liberté 3) pour ceci l'accès au code source est une condition requise.

Un programme est un logiciel libre si les utilisateurs ont toutes ces libertés (définition Free Software Foundation). Par opposition, un logiciel est propriétaire si une de ces libertés n'est pas garantie ; son utilisation est généralement encadrée par un contrat de licence. Il est à noter que les logiciels freeware et shareware, et pour lesquelles on ne dispose généralement pas du code, sont propriétaires.

Maître d'ouvrage (MOA) : personne physique, ou le plus souvent morale, qui exprime le besoin, fixe les objectifs, l'enveloppe budgétaire et les délais souhaités pour le projet (dictionnaire du management de projets AFNOR).

Maître d'œuvre (MOE) : personne physique ou le plus souvent morale, qui réalise le projet à partir des besoins, des objectifs, des délais et des coûts fixés par le maître d'ouvrage. Il est responsable des méthodes, techniques et personnes qu'il mobilise pour réaliser le projet (dictionnaire du management de projets AFNOR).

MAREVA 2 : MAREVA2 est la méthode interministérielle d'analyse de la valeur des projets SI. Il s'agit d'une aide à la prise de décision stratégique du lancement des projets SI puis au pilotage de leur valeur au fil du temps. MAREVA2 a été éprouvée au sein de la sphère publique et reste au service d'une ambition plus large de sécurisation des projets. Elle offre une grille de lecture de la valeur des projets SI.

Mobilité : en pleine expansion, la mobilité doit permettre à un utilisateur, doté de plus en plus souvent d'équipements portables, d'accéder au système d'information du ministère en tout lieu et tout instant. Cette mobilité idéale peut être déclinée en une mobilité interne sur les sites de l'intranet et en une mobilité externe, communément appelée nomadisme. Ce dernier, plus particulièrement, doit concilier les enjeux et les risques de l'accès distant.

Modèle (conceptuel) de données : ensemble de concepts et de règles permettant de définir comment représenter des informations dans un système informatique.

Multi-plates-formes : capacité d'un logiciel à être exploité sur des ordinateurs indépendamment de leur système d'exploitation (Linux, Android, Unix, Windows, MacOS, etc.).

PHARE : (Processus Harmonisé pour l'Analyse, la Réalisation et l'Elaboration) est la méthode de gestion de projet soutenue par le ministère des armées pour la réalisation de ses projets informatiques selon un processus itératif et incrémental. Voir à cette effet le guide n°15/ARM/DGSIC portant sur l'agilité dans le cadre de la transformation numérique.

SAFe® : SAFe® (Scaled Agile Framework) a été créé par Dean Leffingwell en 2011 afin d'accompagner les entreprises, dans le déploiement de l'agilité à l'échelle, à travers un framework structuré. L'agilité à l'échelle consiste à encadrer par une méthode la multiplication en volume des principes Agiles, ceux de SCRUM notamment. Pour développer ce framework, son auteur s'est appuyé sur l'ensemble des bonnes pratiques issues du lean, de la culture Agile et des REX des transformations d'entreprises.

Standard et norme : une norme est une définition détaillée validée par un organisme de normalisation qui regroupe des représentants des États. Un standard est une définition détaillée validée par un organisme de standardisation qui regroupe des industriels et/ou des associations d'utilisateurs. Un standard de fait est le résultat de la prédominance d'un acteur industriel du marché qui seul maîtrise et fait évoluer ce standard.

On entend par standard ouvert tout protocole de communication, d'interconnexion ou d'échange et tout format de données, interopérable et dont les spécifications techniques sont publiques et sans restriction d'accès ni de mise en œuvre (LCEN, Chapitre 1er, article 4).

Système informatique : Ensemble des moyens d'acquisition et de restitution, de traitement et de stockage des données dédié au traitement des informations (origine : Marché-public.fr).

SIOC : Systèmes d'Information Opérationnels et de Communication.

SIAG : Systèmes d'Information d'Administration et de Gestion.

SIST : Systèmes d'Information Scientifiques et Techniques.

TMA : Les prestations de Tierce Maintenance Applicative (TMA) couvrent les taches de maintenance appliquée à un logiciel (« applicative ») et assurée par un prestataire externe dans le domaine des technologies de l'information et de la communication.

TME : Les prestations de Tierce Maintenance d'Exploitation (TME) couvrent les tâches de supervision, d'administration et d'exploitation des environnements applicatifs et permettent d'assurer leur Maintien en Condition Opérationnelle (MCO) et de Sécurité (MCS).

L'objectif est de disposer de systèmes optimums selon les quatre axes principaux suivants :

- **disponibilité :** les utilisateurs doivent pouvoir exécuter leurs tâches aux moments imposés par leur activité ;
- **sécurité :** les utilisateurs doivent pouvoir accéder à leurs données transactions, quel que soient leur localisation, avec la plus grande confidentialité des données manipulées ;
- **performances :** les temps de réponse et de traitement des applications ne doivent pas impacter le travail quotidien des utilisateurs ;

- **évolutivité :** les environnements applicatifs doivent être régulièrement mis à jour et être en mesure de soutenir les mises en œuvre de fonctionnalités ou technologies nouvelles.

Notes

[1] Ces 6 axes clés sont, pour rappel :

- Axe 1 : Déployer de nouvelles technologies ;
- Axe 2 : Organiser l'innovation numérique ;
- Axe 3 : Maîtriser l'ouverture des données pour mieux les valoriser ;
- Axe 4 : Rénover le système d'information pour permettre la transformation numérique ;
- Axe 5 : Développer l'acculturation et les compétences numériques ;
- Axe 6 : Assurer une veille technologique et numérique.

[2] Vulnérabilité, pérennité, spécificités techniques et juridiques, support.

[3] Voir à cette effet le guide n°15/ARM/DGSIC portant sur l'agilité dans le cadre de la transformation numérique.Voir à cette effet le guide n°15/ARM/DGSIC portant sur l'agilité dans le cadre de la transformation numérique.

[4] ATAWAD : Any Time, Any Way, Any Device - ("n'importe quand, n'importe où, sur n'importe quel terminal" en français). Le terme « mobiquité » (pour « mobilité » et « ubiquité ») est parfois utilisé comme synonyme d'Atawad.

[5] BYOD : abréviation de l'anglais « bring your own device », en français, PAP pour « prenez vos appareils personnels » ou AVEC pour « apportez votre équipement personnel de communication », est une pratique qui consiste à utiliser ses équipements personnels (smartphone, ordinateur portable, tablette électronique) dans un environnement professionnel.

[6] Un « Copyleft » est un jeu de mot en référence au « copyright ». Ce jeu de mot peut être traduit par « gauche d'auteur » (vs. « droit d'auteur »). Cependant, le Copyleft diffère significativement du Copyright. Le copyleft est une méthode générale pour rendre libre un programme (ou toute autre œuvre) et obliger toutes les versions modifiées ou étendues de ce programme à être libres également.

Le vice-amiral d’escadre

directeur général du numérique et des systèmes d’information et de communication,

Arnaud COUSTILLÈRE.