Plan directeur des systèmes d'information de l'IGF

Activité de référence	**A1.5**	Appuyer l'IGF à améliorer son système d'information

Préparé par	**Jorge Navas** **Juan Antonio Zapardiel** **Emilio Pérez** **Guillermo Obispo** **Fernando Paunero** **Begoña González** **Pedro García** **Jesús R. Ortega**
Date	30/07/2017
Version	1.1

Extrait du rapport

Ce rapport contient une proposition du Plan Directeur des Systèmes d'Information pour l'Inspection Générale de Finances.

Le rapport énumère un certain nombre d'actions pour établir les lignes directrices qui devront organiser les principales interventions à court et moyen terme. Nous analysons dans une premier temps la situation initiale en identifiant les ressources et les besoins basiques, et nous proposerons ensuite une planification des mesures concrètes à appliquer, en tenant constamment compte des effets possibles de l'implémentation du Plan Stratégique de Modernisation des Finances Publiques (PSMFP).

Disclaimer

Les opinions exprimées dans ce rapport sont de la seule responsabilité des auteurs.

Ils ne reflètent pas les vues de la Commission européenne.

INDEX

1 INTRODUCTION : vision, stratégie

Lorsqu'on pense à la configuration d'un Plan Directeur de Systèmes d'informations pour l'Inspection Générale de Finances (IGF), il est indispensable de dresser une analyse historique des décisions et des rôles qui ont généré la situation actuelle des systèmes d'information.

Comme le reste des directions du Ministère de Finances (MDF), les systèmes d'information de l'IGF sont la résultante d'une recherche de solutions spécifiques ponctuelles, sans ordre établi et sans une harmonisation avec les systèmes d'autres directions de l'organisation. Dans certains des cas, des applications spécifiques ad hoc ont été réalisées, et, dans les autres, certaines options de marché ont été acquises.

À l'exception de quelques services horizontaux comme le courrier électronique et l'accès à Internet, approvisionnés depuis la Direction de Systèmes d'Information (DSI), le reste des services sont restés dans les mains des directions. L'IGF a dans ce sens développé les applications dont elle a eues besoin pour pouvoir répondre aux nécessités qui se sont manifestées parallèlement au développement de son activité.

Il est difficile de poursuivre plus longtemps avec cette situation du fait de son inefficacité dans la mesure où elle empêche la création d'un système d'information centralisé pour tout le MDF. Un tel système aurait en effet permis de profiter des économies d'échelle au moyen de l'interconnexion de systèmes ou de l'utilisation de services et d'infrastructures communes.

La distribution inégale de ressources humaines et financières entre les directions a généré un modèle dont chaque direction s'est basée pour développer son propre système. Par conséquent, ces directions, fortes d'un plus grand contenu stratégique, ont pu atteindre un meilleur niveau de développement technologique, après avoir disposé de plus grandes ressources.

Pour autant, l'IGF maintient son propre réseau local sans intégration avec les réseaux des autres directions.

Pour tous ces motifs de fond, l'IGF, comme le reste de directions, a fait évoluer ses systèmes d'information de manière indépendante. Cette pratique systématique a néanmoins multiplié les frais puisqu'elle a entraîné le développement de plusieurs applications analogues dans les différentes directions.

Cette situation, conséquence d'une croissance chaotique, a pu se généraliser par l'inexistence d'un cadre juridique approprié dans le domaine des systèmes d'information, tant à l'échelle du MDF que de l'ensemble de l'administration publique. Aussi, le manque d'une gouvernance commune s'agissant de la coordination des ressources et du développement de systèmes horizontaux dont l'organisation aurait pu profiter, a constitué une contrainte considérable.

L'IGF est une direction qui ne présente pas de grandes nécessités dans le domaine des technologies de l'information et des communications (TIC), c'est pourquoi une allocation appropriée des ressources, avec l'appui technique nécessaire, permettrait de développer quelques systèmes modernes, stimulant ainsi, substantiellement, la performance de son activité.

Cependant, il serait inefficace de penser aux systèmes d'information de l'IGF sans tenir

compte des prévisions du Plan Stratégique de Modernisation des Finances Publiques (PSMFP). Le PSMFP part d'une situation initiale basée sur l'actuelle utilisation de la plate-forme SAP dans quelques projets des domaines fiscaux et budgétaires. Cela peut conditionner l'évolution des systèmes d'information au sein de toutes les directions, y compris à l'IGF. Toutefois, il est indispensable d'évaluer le coût des investissements nécessaires pour implanter la SAP dans toute l'organisation. En effet, le caractère dispendieux de ce coût pourrait mettre cette alternative en suspens.

De toutes les manières, la mise en œuvre du PSMFP est lente, et durant le temps d'exécution, les directions devront prendre leurs propres décisions concernant le développement de logiciels pour les processus métiers.

La création future d'un Data Center commun à tout le MDF (le délai prévu est de deux ans) peut résoudre beaucoup de problèmes relatifs au partage des ressources, mais surtout dans le domaine des services horizontaux.

Si l'on décidait finalement de généraliser l'implantation de la plate-forme SAP, il serait indispensable de doter toutes les directions des ressources suffisantes pour la mise en oeuvre de leurs logiciels, car, autrement, la situation actuelle sera maintenue et toutes les directions continueront de travailler en silo à ce niveau.

Par conséquent, il faudrait arriver au minimum à un scénario avec une structure de gouvernance des systèmes d'information qui favorise la connectivité et l'interopérabilité entre tous les systèmes, sans oublier la sécurité, et qui exige l'adaptation aux normes et aux standards internationaux sur des formats de données pour l'échange d'information. Cette solution devrait apporter aussi la création de plateformes de services horizontaux communs, et donc accessibles par tous les département de l'organisation.

Un scénario comme celui-ci résoudrait les difficultés actuelles que rencontre l'IGF. Elle pourrait ainsi avoir accès aux bases de données des autres directions du MDF, et notamment au système intégré des dépenses publiques, et travailler ainsi pour un meilleur développement de son activité et de son modèle d'affaire. Elle pourra aussi s'appuyer, dans cette démarche, sur une base de données extensive et un logiciel pour le suivi des différentes phases de la procédure d'audit, et donc, sur des plateformes technologiques efficaces.

Cependant, pour atteindre ces résultats potentiels, il faudra approuver la nouvelle loi de finances qui compose le cadre juridique nécessaire pour pouvoir développer une nouvelle structure de systèmes d'information moderne et opérationnelle.

2 SOMMAIRE

L'élaboration du Plan Directeur des Systèmes d'Information examine différents aspects sur la situation actuelle des technologies de l'information et des communications à l'IGF, sans oublier l'environnement des services horizontaux fournis par la DSI. L'obsolescence des infrastructures et des logiciels constitue le point de départ d'une nouvelle façon d'aborder l'avenir. La construction future d'un centre de données du MDF est, en ce sens, le meilleur moyen de stimuler la modernisation les systèmes de l'IGF, tout en assurant leur sécurité.

Il faut prévoir que les objectifs de l'IGF quant à l'évolution de ses systèmes d'information vont être influencés par le cadre technologique du Ministère de Finances. Il est de ce fait indispensable de connaître le degré d'autonomie dont jouit réellement l'IGF dans la prise de décisions, ainsi que sa marge de manœuvre dont le véritable baromètre restent les ressources (humaines et financières) qui lui sont allouées.

Les investissements en technologie doivent s'accompagner d'un plan de formation pour les effectifs de l'IGF qui ont pour mission de mettre en place des actions en direction du secteur de l'informatique.

Dans la stratégie de développement du Plan, l'interopérabilité occupe une grande place compte tenu des besoins de l'IGF quant à la standardisation des formats de fichiers de données, pour leur échange, ou l'accès à des bases de données d'autres directions du MDF.

Le travail quotidien des fonctionnaires de l'IGF implique un besoin de logiciels appropriés pour la performance de leurs actions qui découlent de leurs fonctions.

On peut distinguer cinq volets principaux dans ce Plan Directeur:

1. Une analyse SWOT, dans la section 6, qui informera les responsables de l'IGF des forces, opportunités, menaces et faiblesses de la structure des systèmes d'information avec lesquels ils travaillent.
2. Des propositions de changements dans l'organisation de l'IGF, notamment au niveau de la "sécurité des systèmes d'information", section 9, mais aussi de la nouvelle figure de Chef de projet fonctionnel et des responsables du contenu de l'Intranet et de site web de la IGF, section 11. Finalement, une recommandation a été faite pour renforcer la structure du Service des TI de l'IGF, en augmentant ses effectifs et ses compétences techniques, aussi à la section 11.
3. Quand on parle des systèmes d'information, il convient des applications. L'IGF doit en effet élaborer et maintenir à jour un catalogue des applications. Dans ce projet, il est demandé à l'IGF d'identifier des besoins pour élaborer des documents relatifs aux spécification fonctionnelles. Dans la section 15, cette relation est établie.
4. Mais pour mettre en oeuvre des applications, une infrastructure TI doit exister en amont. Dans la section 10, on propose une solution pratique pour l'infrastructure TI de l'IGF à court et moyen terme. La section 7 comporte une proposition de la structure du service de développement. Aussi, on y propose un plan de formation pour les effectifs du Services des TI qui leur permettra d'obtenir des connaissances en qui a trait au développement des applications modernes et actualisées. Une sous-section est dédiée à l'utilisation des mécanismes de formation en-ligne très accessible dans le marché et surtout, d'une grande qualité. Finalement, on propose la création d'un Centre d'assistance technique pour réceptionner et traiter les demandes de l'usager fonctionnel des systèmes d'information.
5. Le cinquième volet, peut être le plus pratique, est une liste de projets (section 16) de différentes tailles que l'IGF doit prendre en considération pour les adapter à ses

besoins et capacités financières. Cette liste est accompagnée d'un planning qualitatif pour mieux associer les besoins aux priorités.

3 PORTÉE DU PLAN

Dans la conception du Plan Directeur de Systèmes de l'Information, il faut voir à ce que soient prises en compte les actions suivantes :

- Identifier les besoins futurs (à court, moyen et long terme) tant sur le plan organisationnel et des ressources humaines de l'IGF, que celui de l'infrastructure technique, en fonction de son niveau de service prévu.
- Définir les stratégies et politiques corporatives TIC, en considérant l'actuel cadre organisationnel défini par les compétences de la DSI, sans oublier le scénario futur d'organisation et de gouvernance TIC prévu dans le Plan Stratégique de Modernisation des Finances Publiques (PSMFP).
- S'approprier ces stratégies, en tenant compte également de celles liées à l'Administration électronique du cadre général du Ministère de Finances.
- Planifier les ressources économiques pour ces besoins qui, au moins dans le court terme, ne pourront pas être comblés au travers d'une stratégie centralisée du Ministère de Finances.
- Disposer de plans d'action, en imaginant différentes alternatives selon les ressources de l'IGF, considérant les prévisions économiques proches, et différenciant les priorités d'agissement.
- Identifier des paramètres de mesure qui servent comme barème de l'état des technologies de l'information et des communications, tant au niveau de l'IGF que du Ministère dans son ensemble.
- Identifier les objectifs stratégiques du Ministère dans le domaine des TIC, déterminés dans le PSMFP.
- Analyser les procédures de relation sur le domaine TIC entre l'IGF et les autres directions du MDF, spécialement la DSI.
- Déterminer les nécessités en termes d'information de l'IGF liées aux objectifs du Ministère, tant actuelles que futures.
- Étudier la situation de départ de tous les éléments relatifs aux systèmes d'information de l'IGF (des systèmes, des équipements, des télécommunications...)
- Identifier les tendances technologiques existantes sur le marché, et recommander leur applicabilité à la problématique de l'IGF, dans un environnement compatible avec les solutions du MDF.
- Aligner les établissements de l'IGF avec la vision à moyen terme des autres directions, pour la définition de ses projets et nécessités.
- Analyser des faiblesses et des opportunités selon les résultats obtenus.
- Établir un outil de suivi qui permet l'actualisation continue des changements qui sont réalisés.
- Sur la base des actions antérieures, on fera une proposition qui couvre les nécessités réelles de l'IGF dans l'accomplissement de ses fonctions :
    - La création d'une base de données d'entités qui sont objets d'audit. La base de données contiendra l'information sur l'identification des entités, leur classification du point de vue juridique, la composition du capital, le cas échéant, leurs données budgétaires, ressources humaines, etc. On veillera à y

inclure des indicateurs de gestion et financiers qui permettront de générer un tableau de bord pour le suivi des entités de la part de l'IGF, et qui introduit à son tour une information additionnelle pour une sélection optimale de l'échantillon d'entités qui fera partie du Plan Annuel d'Audit de l'IGF.
- Le design d'un logiciel de suivi des différentes étapes de la procédure d'audit qui permet de réaliser un contrôle complet du flux de travail de chaque auditeur, des phases du rapport de mission, de l'accomplissement des recommandations, etc.
- La conception d'un logiciel qui facilite la formation du Plan Annuel d'Audit.
- La proposition d'autres applications qui traitent des activités complémentaires, comme des dépôts de documentation dans certains domaines : formation, réglementation, instructions internes, etc.

4 STRUCTURE ORGANISATIONNELLE INTERNE DES TI

La structure organisationnelle actuelle des départements TI centraux au sein du Ministère des Finances est la suivante :

- La Cellule de Modernisation des Finances Publiques (CMFP) est une structure du Ministère des Finances qui s'occupe de la planification stratégique et de la coordination des TI au sein du Ministère.
- L'Agence de l'Informatique pour les Finances Publiques (AIFP) est un nouveau département qui est en charge de la gestion du projet d'implantation d'un nouveau DataCenter corporatif sur le site de Birkhadem et qui hébergera, dans l'avenir, les services TI des différentes Régies.
- La DSI (Direction de Systèmes d'Information, 10 personnes) s'occupe de fournir un soutien technique basique aux différentes Régies du Ministère des Finances. Avec l'implantation du nouveau DataCenter, les compétences de la DSI ne sont pas encore clairement définies car certains services (par exemple, la connectivité à Internet) pourront basculer vers le nouveau DataCenter central.
    - Actuellement, il s'occupe du service d'accès à Internet du MdF, du serveur de courrier électronique corporatif, du réseau troncal LAN ainsi que du service VPN d'accès sécurisé.

Actuellement chaque Régie du Ministère s'organise et développe son informatique à sa manière.

La Direction des Méthodes, de Normalisation et de l'Informatique (DMNI, 4 effectifs techniques plus 10 effectifs administratifs) est le département en charge de l'informatisation de l'IGF.

5 ÉTAT DE LIEUX

Jusqu'à présent, les TI n'étaient pas organisées et chaque Régie développait ses systèmes d'une façon totalement indépendante. Pour éviter cette situation, la CMFP a rédigé le Plan Stratégique de Modernisation des Finances Publiques (PSMFP) : dans ce plan, il est question d'un projet de centralisation qui prévoit la création de systèmes d'information

intégrés basés sur la technologie SAP. Toutefois, nous ne disposons pas encore de la connaissance nécessaire sur l'effet que cette intégration peut avoir sur l'IGF dans un proche avenir, surtout si l'on prend en compte les restrictions budgétaires du Ministère des Finances qui concentre principalement ses dépenses sur la Direction Générale des Impôts (DGI) et la Direction Générale de Budget (DGB). Le PSMFP prévoit de lancer les actions suivantes :

- Implantation d'un nouveau DataCenter sur le site de Birkhadem (projet géré par l'AIFP) qui supportera les services TI des différents Régies, en assurant plusieurs services communs
- Un noyau central basé, en principe, sur l'ERP SAP (la décision n'est pas certaine à 100%). Dans une première phase, on commence avec l'informatisation des impôts et du budget, en donnant accès en mode consultation au personnel du Ministère des différentes Régies.
- Service intranet : dossiers créés pour le partage des fichiers en utilisant des systèmes modernes de stockage, avec des backups (miroir) en temps réel sur un autre site.
- Accès Internet : solution de sites Web pour les différentes Régies
- Il est aussi envisagé d'héberger dans le DataCenter des applications non-SAP des Régies. Pour le moment, il n'y a pas de documents qui expliquent les architectures qui seront supportées, mais on veut donner support aux applications multicouches basées sur des architectures orientées sur les services web.
- Définition des normes et des standards à suivre par les différentes Régies (en préparation).

La DSI s'occupe de fournir un soutien technique aux différentes Régies pour les services suivants :

- Gestion basique du réseau: plan d'adressage IP. Câblage.
- Gestion d'accès à internet : gestion des identités du logiciel proxy donnant accès à la navigation internet
- Gestion du courrier électronique: gestion des adresses e-mail.
- Gestion du logiciel Antivirus corporatif.
- Coordination des HelpDesk des Régies. Le premier niveau est assuré par le département informatique de chaque Régies. En cas de blocage, la DSI offre le soutien nécessaire.

L'avenir du rôle de la DSI n'est pas clair car il n'existe pas de document de gouvernance TI détaillant les relations entre la DSI, l'AIFP et la CMFP et leurs prérogatives.

La DMNI coordonne avec la DSI pour la mise en marche de nouveaux ordinateurs (câblage, adressage IP et identificateurs pour les comptes e-mail et la navigation web) mais elle travaille de façon indépendante, sans aucune directive du Ministère en ce qui concerne le développement des systèmes d'information. Entre autres fonctions, la DMNI est en charge des tâches suivantes :

- Propositions d'achats (à la DAM comme responsable de cette fonction); installation et maintenance des ordinateurs du personnel de l'IGF, en coordination avec la DSI.
- Gestion du HelpDesk TI de premier niveau pour le personnel de l'IGF.
- Développement, installation, opération et maintenance des logiciels spécifiques pour l'IGF. Il y a un technicien supérieur en informatique et deux programmeurs travaillant pour la DMNI qui gèrent un ancien serveur Windows 2003 (un budget a

été approuvé récemment pour acheter un matériel plus moderne) dans lequel il y a un environnement de développement Windev/WebDev, et une base de données SQL server. Ce serveur est très important car il est aussi le serveur en production pour les applications suivantes développées par la DMNI :

- LSM : Logiciel de Suivi des Missions, utilisé par 4 divisions, la DPAS et une inspection régionale (cette dernière est connectée avec une VPN). Le logiciel garde les données principales de l'activité de chaque mission, mais pour le moment, il ne garde pas les rapports des missions numérisés.
- LBD : Logiciel Base Documentaire, pour stocker l'information des documents existants dans la bibliothèque de l'IGF, ainsi que des rapports et d'autres documents.
- Planification du développement des nouveaux systèmes d'information :
  - Il y a un plan pour numériser les anciens rapports de mission et les rendre accessibles, soit avec une application, soit avec un intranet avec des répertoires Web, pour l'utilisation du personnel autorisé de la DPAS.
  - Base de données des établissements publics en plus d'un système de sélection automatique pour générer le programme annuel d'inspection.
  - Site Web de l'IGF.
  - Site intranet/dossiers partagés de l'IGF.

6 ANALYSE SWOT (analyse des forces, des faiblesses, des opportunités et des menaces)

6.1 Faiblesses:

- Les ressources humaines et financières de la DMNI sont très limitées. En conséquence, les services offerts par la DMNI ne sont pas conformes aux besoins réels de l'IGF.
- En plus, la capacité de recrutement de personnel technique est très limité dans le secteur publique.
- Au niveau du Ministère des Finances, il y a une unité de support TI horizontale (DSI), mais l'assistance fournie à l'IGF est minimale.
- Il n'existe pas de cadre juridique pour soutenir l'administration électronique.
- Les services horizontaux de base (courrier électronique, Internet, etc.) ne sont accessibles pour le moment qu'à certains effectifs du personnel.
- Il n'existe pas de plan de formation pour les techniciens de la DMNI.
- L'infrastructure technologique actuelle n'est pas évolutive. Il est donc nécessaire d'investir dans l'équipement pour doter la DMNI d'une architecture TI plus conforme aux besoins fonctionnels de l'IGF.
- Le service internet fourni par le Ministère des finances à travers la DSI est très insuffisant.

6.2 Opportunités:

- Il y a un Plan de Modernisation des Finances Publiques au niveau ministériel qui va dynamiser les TI en permettant de partager des informations aux différentes régies du Ministère des finances.
- Le niveau de l'implantation de l'informatique à l'IGF est très peu développé. Cela implique de démarrer de zéro et de choisir les technologies modernes les plus adéquates et mises à jour, car elles permettront de générer plus facilement de nouvelles solutions (il ne faut pas envisager des migrations compliquées des systèmes anciens).
- Bien que sensible par nature, le changement de technologie permettra à l'IGF d'avoir accès à des solutions performantes. En effet, le futur développement du Système Intégré de Dépenses publiques peut donner à l'IGF une nouvelle dimension performante et substantielle dans l'utilisation de ses systèmes d'information.
- L'UE est engagée avec l'Algérie pour financer des activités et des projets reliés aux systèmes d'information.

6.3 Menaces:

- Le projet de centralisation de l'informatique associé au Plan de Modernisation des Finances Publiques peut mettre encore plusieurs années avant qu'il ne soit en condition d'offrir des services performants à l'IGF.
- Dans la phase initiale de l'implantation du Plan Directeur des Systèmes d'information pour l'IGF, il faudra absolument un budget disponible pour faire l'achat d'une infrastructure basique (serveurs, dispositifs de stockage) et pouvoir

ainsi offrir un service avec des garanties de stabilité et de disponibilité.

- Les programmeurs de la DMNI doivent aussi se mettre à jour pour être capables de développer des applications web avec une architecture à plusieurs couches axée sur les services.

6.4 Forces :

- L'IGF connaît parfaitement sa vocation.
- Il y existe aussi un département interne (DMNI) avec des informaticiens ayant de solides connaissances des besoins fonctionnels de l'IGF
- Il y a une grande partie du personnel de l'IGF, parmi lequel plusieurs jeunes, qui sont très engagés sur le projet de modernisation.
- Le nombre d'utilisateurs est relativement petit et la taille des applications à faire est également relativement modeste.
- Il y a des procédures de HelpDesk informatique en marche.
- Il n'y aura pas dans le futur proche des utilisateurs externes, ce qui rend plus facile la mise en oeuvre de l'architecture et le développement des logiciels en matière de sécurité externe.

7 STRATEGIE DE DEVELOPPEMENT

7.1 Gestion de projets de développement

Pour le développement des nouveaux logiciels de l'IGF qui soutiendront ses fonctions, il est nécessaire d'utiliser une méthodologie de développement software de manière à ce que les quatre critères suivants soient satisfaits :

- Le système qui est fabriqué répond aux besoins (exigences) des utilisateurs (correction fonctionnelle).
- La qualité correspond au contrat de service initial. La qualité du logiciel est une notion multiforme qui recouvre notamment:
    - la validité : aptitude d'un logiciel à réaliser exactement les tâches définies par sa spécification,
    - la fiabilité : aptitude d'un logiciel à assurer de manière continue le service attendu,
    - la robustesse : aptitude d'un logiciel à fonctionner même dans des conditions anormales,
    - l'extensibilité : facilité d'adaptation d'un logiciel aux changements de spécification,
    - la réutilisabilité : aptitude d'un logiciel à être réutilisé en tout ou partie,
    - la compatibilité : aptitude des logiciels à pouvoir être combinés les uns aux autres,
    - l'efficacité : aptitude d'un logiciel à bien utiliser les ressources matérielles (mémoire, CPU...),
    - la portabilité : facilité à être porté sur de nouveaux environnements matériels et/ou logiciels,
    - la traçabilité : capacité à identifier et/ou suivre un élément du cahier des charges lié à un composant d'un logiciel,
    - la vérifiabilité : facilité de préparation des procédures de recette et de certification,
    - l'intégrité : aptitude d'un logiciel à protéger ses différents composants contre des accès ou des modifications non autorisés,
    - la facilité d'utilisation, d'entretien, etc.
- Les coûts restent dans les limites prévues au départ.
- Les délais restent dans les limites prévues au départ.

Une méthodologie de développement structure, planifie et contrôle le développement d'une application avec une ensemble de procédures, méthodes, techniques, outils et soutien documentaire pour spécifier l'ordre des procédures, produits intermédiaires et finals, l'information initial, des techniques à appliquer, des contrôles de qualité, etc.

Au sein de l'IGF, on recommande une construction incrémentale qui atteint son but par étapes où chaque résultat est atteint en étendant le précédent. On peut par exemple réaliser d'abord un noyau des fonctions essentielles et ajouter progressivement les aspects plus secondaires. Ou encore, construire une série de prototypes 'simulant' plus ou moins

complètement le système envisagé.

La construction incrémentale du software permet aux développeurs de créer rapidement les premières versions que les utilisateurs peuvent évaluer. Ce processus facilite la communication entre les utilisateurs dans la mesure où il pourront connaître leurs attentes. Ainsi, les systèmes se développent plus rapidement.

7.2 Gestion des versions

Un système de gestion de version (VCS en anglais pour Version Control System) est un outil qui enregistre l'évolution d'un fichier ou d'un ensemble de fichiers au cours du temps de manière à ce qu'on puisse rappeler une version antérieure d'un fichier à tout moment.

Un VCS permet de ramener un fichier ou le projet au complet à un état précédent, de visualiser les changements apportés dans le temps, de voir les modifications qui pourraient causer un problème, la personne à leur origine et la date à laquelle ont été apportées, et plus encore. Avec un VCS généralement, il est possible de revenir facilement à un état stable après une erreur ou perte des fichiers.

Dans les projets de développement SW de l'IG, il est fortement recommandé d'utiliser un VCS comme ***Subversion (SVN)*** pour gérer les différentes versions des logiciels pendant le développement.

7.3 Framework de développement

Un framework est un niveau d'abstraction qui permet de développer des applications plus puissantes plus rapidement en utilisant les fonctions du framework, sans nécessairement savoir comment ont-ils été programmés.

Pour le développement de logiciels dans l'IGF, il est recommandé d'utiliser un framework MVC.

Un ***framework MVC*** (correspond à "Modèle, Vue et Contrôleur") est une méthode normalisée pour diviser l'information d'un projet SW.

- **Modèle**

Le modèle est le code qui opère la gestion des données. Il n'y aura que le code PHP qui fait référence à une base de données, une connexion avec JSON, etc.

Comme le modèle est séparé du noyau du programme, si à l'avenir on change le gestionnaire de base de données, seul l'objet ou les fonctions du modèle devront changer et ce, sans aucune incidence sur le reste du logiciel.

- **Vue**

Cette partie est responsable de tout ce qui est relatif à HTML. Elle constitue autrement dit la structure du site web. Dans la vue, il n'y a pas de code, on ne spécifie pas quand présenter une donnée ou une autre puisqu'il revient au contrôleur de le faire.

Ainsi, il est très facile de changer la conception d'un web en changeant cette partie du logiciel.

- **Contrôleur**

Le contrôleur est le cœur du logiciel. C'est l'endroit où se trouve toute la programmation et où la logique qui met en œuvre ces fonctions réside.

Cette couche est responsable de rassembler et de contrôler l'ensemble des paramètres du logiciel.

Un *framework MVC* présente de nombreux avantages. Cependant, trois d'entre eux méritent d'être explicités :

- **Code séparé et ordonné**: pour modifier une partie du logiciel, il faut se diriger seulement à la partie affectée du framework (modèle, vue ou contrôleur).
- **Projet évolutif**: comme le code est bien structuré, on peut migrer ou changer quelques fonctions du logiciel de manière rapide. Ceci est particulièrement utile lorsqu'on a besoin de faire un projet évolutif.
- **Travail d'équipe**: il permet de séparer le projet en modules qui peuvent être développés par les différents membres de l'équipe.

7.3.1 Environnements

Dans les projets de développement de SW de l'IGF, il sera nécessaire d'avoir différents environnements pour les logiciels afin de coordonner les différentes tâches de l'équipe et d'effectuer différents tests sur le code développé. Chaque environnement a une fonction spécifique. Une application est créée dans l'environnement de développement et enfin installée dans l'environnement de production:

- **Environnement de développement/test**: l'équipe de programmeurs créera les logiciels dans cet environnement et en fera les premiers tests de base. En plus, on réalisera, dans cet environnement, les tests exhaustifs de l'intégration des logiciels.
- **Environnement de production**: où le logiciel est installé définitivement afin qu'il effectue les tâches pour lesquelles il a été conçu.

Il y a d'autres environnements optionnels qui peuvent être configurés dans le futur:

- **Environnement d'acceptation/formation**: une fois que le logiciel aura été testé, il peut être installé sur cet environnement pour l'acceptation de l'utilisateur. En outre, il peut être utilisé pour des tâches de formation du logiciel à l'utilisateur.
- **Environnement de pré-production**: Idéalement, cet environnement est identique à celui de production. Il permet l'exécution du logiciel pour vérifier que tout fonctionnera correctement dans l'environnement de production. Il est également utile pour effectuer des tests de charge avec des volumes de données et transactions similaires à l'environnement de production.

7.3.2 Multilinguisme

Une application multilingue a pour fonction de pouvoir présenter un contenu dans plus

d'une langue. L'information est exactement la même à l'exception de variations mineures qui n'altèrent pas la substance du message.

Dans le développement d'applications de l'IGF, le multilinguisme devrait être envisagé dans la mesure où devra être pris en compte l'arabe, langue officielle, et le français.

Il y a de nombreux aspects du développement de SW concernés par le multilinguisme, telles que la classification des noms de domaine, la configuration du serveur Web, la structure d'URL, la conception du logiciel et la traduction du contenu. En plus de tout cela, il faut tenir compte de l'accessibilité du site.

Dans le cas des logiciels multilingues la langue doit être correctement identifiée dans le code de la page afin que les technologies d'assistance en matière d'accessibilité puissent l'interpréter correctement. Une fois la langue reconnue, ces technologies peuvent changer automatiquement, ajuster l'accent, le ton et la vitesse de le discours en fonction de la langue en question (lecteurs d'écrans modernes tels que JAWS et Window Eyes peuvent parler plusieurs langues avec un accent approprié).

Le codage de caractères utilisé pour décoder la collection de lettres et de symboles utilisés dans le système doit être considéré. Le codage le plus utilisé est « Unicode », car il contient des caractères pour la plupart des langues et des scripts dans le monde et est soutenu par un très grand nombre de systèmes d'exploitation.

Lors de la conception d'un logiciel multilingue, il est important de considérer la taille de la police à utiliser par défaut parce qu'elle peut ne pas convenir à toutes les langues. Différentes langues telles que le chinois, le japonais ou l'arabe peuvent être difficiles à lire avec une petite police. De plus, la longueur des mots varie entre les différentes langues et, par exemple, les menus peuvent être affectés par ces changements de langage.

Par conséquent, il faudrait tenir compte de ces considérations dans la conception des logiciels à l'IGF afin qu'ils puissent évoluer automatiquement sans changer de structure, et s'adapter ainsi aux différentes résolutions des appareils mobiles dans le futur.

7.4 Équipe de travail

Pour répondre aux projets de développement de logiciels de l'IGF, il faut étendre la capacité de travail de la DMNI. Il est, dans ce sens, nécessaire d'augmenter le budget dédié aux TIC et qui se traduit par une augmentation de capacité. Cette augmentation de capacité peut être obtenue en incorporant à la DMNI du nouveau personnel, en augmentant leurs ressources technologiques ou en contractant des fournisseurs externes.

Pour prendre cette décision, il faut tenir compte de la stratégie du Ministère de Finances et se demander s'il faut avoir un vaste département spécialisé dans le développement de logiciels, entièrement autonome et sans la participation des entreprises privées. D'un autre côté, on peut considérer d'externaliser une partie du cycle de vie du développement et maintenir seulement un personnel de base du Ministère pour prendre le contrôle de certains projets. Autrement dit, il ne faut pas seulement évaluer les coûts d'externaliser ou non, mais il faudrait plutôt établir des choix en fonction de la stratégie du Ministère.

Au sein de cette stratégie, on peut considérer l'urgence de développer un grand nombre d'applications dans un court laps de temps. L'externalisation dans ce cas fournirait un net

avantage sur l'intégration du nouveau personnel interne à la DMNI.

> En tout cas s'il est décidé que les logiciels de l'IGF seront développés et maintenus à long terme par un fournisseur externe, il est essentiel de construire une équipe de spécialistes à la DMNI qui ont une grande connaissance des métiers de l'IGF et des technologies de développement utilisés. Cela permettra d'assurer la qualité des produits livrés par le fournisseur externe.

Par conséquent, l'un des aspects les plus importants au moment d'externaliser le développement de logiciels est de ne pas perdre le contrôle du développement à tout moment. Les projets doivent être dirigés par un chef de projet de l'IGF pour assurer une fonctionnalité adéquate des applications à développer.

En outre, le DMNI doit recueillir les exigences des unités fonctionnelles afin qu'une fois filtrées, élaborées et détaillées, elles soient livrées au fournisseur externe pour les mises en œuvre. De plus, le responsable de la DMNI devra participer au comité de pilotage de l'IGF en raison de son rôle central dans la spécification et le développement des exigences fonctionnelles de l'IGF.

Il faut considérer les aspects suivants pour que l'IGF maintienne le contrôle des projets externalisés:

- **Accord de niveau de service**

Les SLAs (Service Level Agreement) sont basés sur des indicateurs ou des paramètres utilisés pour déterminer l'efficacité du service réalisé par le fournisseur externe de la manière la plus objective et quantitative possible. Ils doivent être définis avant l'externalisation et inclus dans le contrat.

Dans un possible SLA de l'IGF avec un fournisseur externe il faut prendre en considération, entre autres, les indicateurs suivants: la déviation par rapport à la planification, le temps de résolution de problèmes, les erreurs qui se produisent au cours des tests ou à l'exploitation du logiciel, les infractions aux normes de qualité des logiciels (par exemple, le pourcentage de code qui a été répété ou si on a suivi le style de codage établi), etc.

Les SLAs sont généralement associés à un modèle qui spécifie les sanctions possibles ou des bonus à appliquer au fournisseur en fonction des indicateurs.

- **L'externalisation des processus**

Il faut définir la façon dont l'IGF travaillera en collaboration avec les fournisseurs, les rôles des acteurs, des outils, des activités, les flux de communication, etc.

- **Les exigences à remplir par le fournisseur**

Il est conseillé d'exiger un minimum de preuves sur la qualité de l'organisation à qui le développement de logiciels a été externalisé. Principalement, les certifications de la qualité de ses processus software comme les modèles CMMI ou ISO 15504, entre autres. D'autres certifications qui peuvent être nécessaires sont celles à caractère personnel et qui doivent être remplies par l'équipe de développement. En plus des technologies de programmation, on peut exiger d'autres comme CISA, PMP, CSQE, ITIL, ISTQB, etc.

- **Le cahier des charges des travaux à développer**

Les exigences, la gestion et les spécifications sont les points les plus importants pour la

réussite d'un projet de logiciel. Le manque d'une définition claire et précise des spécifications fonctionnelles est la principale cause de l'échec du développement des logiciels. Ce risque est décuplé dans un environnement de développement externalisé.

L'IGF doit travailler avec un ensemble complet et détaillé d'exigences. Celles-ci doivent être à la fois fonctionnelles et non fonctionnelles.

- **L'évaluation de la qualité**

Dans une externalisation, il est essentiel de se mettre d'accord sur la façon dont sera validée la qualité de la livraison. Il est nécessaire de définir une norme de qualité que le logiciel doit surmonter. Elle doit être connue par le développeur et il faudra vérifier que le logiciel l'atteigne. L'évaluation devrait inclure non seulement le logiciel en tant que tel, mais aussi les produits intermédiaires du cycle de vie, telles que la définition de l'architecture, l'analyse, etc.

7.5 Modèle de licences SW

En général, il est recommandé d'utiliser des logiciels ***Open source*** pour le développement d'applications à l'IGF.

Par rapport aux Environnements de Développement Intégrés pour le langage PHP, on peut citer:

- Yii
- Flight
- Medoo
- Phalcon
- Symfony
- Slim
- CakePHP
- FuelPHP
- CodeIgniter
- Zend
- Eclipse for PHP Developers

Pour la gestion des versions, on recommande SUBVERSION pour sa facilité de mise en oeuvre et d'utilisation. Mais on peut utiliser aussi GIT.

7.6 Outils collaboratifs

Au sein de l'IGF, il faudrait utiliser des outils collaboratifs pour améliorer l'engagement des équipes, diminuer les processus de travail, accroître la vitesse de décision, partager des informations...etc. Ces outils devraient se voir divisés en deux groupes:

- Des outils d'aide à l'organisation / à la planification : agenda partagé, sondage, partage de fichiers.
- Des outils d'aide à la communication à distance : visioconférence, conférence téléphonique, messagerie instantanée.

La majorité des outils collaboratifs utilisent le *cloud*. Ainsi, l'IGF devrait identifier quelles données et informations de travail peuvent être gérées par ces outils avec le risque de ne pas avoir le contrôle sur l'emplacement de l'information.

- **Doodle**: pour planifier une réunion.
- **Skype**: cette solution permet d'effectuer des appels audio et vidéo gratuitement à des personnes possédant ce même logiciel. Il possède également un système de messagerie instantanée.
- **Google Drive/Dropbox**: pour stocker des fichiers qui doivent être accessibles par plusieurs membres de l'équipe.
- **Google Docs et Google Sheet**: pour travailler avec des documents et feuilles de calculs collaboratifs en temps réel. Avec cet outil, on peut modifier à plusieurs un même document en étant à distance, en temps réel ou non. De plus, cet outil web inclut un système de révision et une messagerie instantanée pour plus d'efficacité.
- **Slides.com**, pour générer des présentations modernes, attractives et surtout adaptées aux technologies web.
- **Zendesk**, pour la gestion efficace et simple du Centre d'assistance technique
- **Redmine**, pour l'implantation de *wiki's* collaboratifs et départementaux, et pour favoriser les travaux de documentation technique.
- **Assana** et **Jira**, pour la gestion interne des travaux de développement
- **Lucidchart, Draw.io**, pour la réalisation des diagrammes
- **Pencil**, conçu pour fournir un outil de prototypage GUI gratuit et *open source*

7.7 Exigences de dimensionnement

Après avoir analysé tous les logiciels à développer dans ce projet de jumelage à l'IGF, on estime, au plus, environ 350 utilisateurs internes.

En principe, il n'y aura pas d'utilisateurs externes. Les entités qui doivent envoyer des informations le feront via e-mail (en format XML).

Cette situation correspond à une exigence moyenne-basse pour les capacités de l'infrastructure à mettre en œuvre. Différentes propositions pour l'infrastructure, y compris un type moyen-bas, sont détaillées dans le chapitre de l'architecture TI.

En ce qui concerne l'évolutivité, l'infrastructure devrait pouvoir permettre de doubler la capacité de manière aisée. Cette augmentation pourrait être faite, par exemple, en utilisant des techniques de virtualisation.

Enfin, en ce qui concerne la disponibilité, l'infrastructure proposée devrait comporter des éléments qui fourniraient la disponibilité au niveau moyen ou moyen-bas comme le fait de mettre en œuvre une disponibilité de type local. Cependant, cette infrastructure pourrait être élargie pour améliorer rapidement les indicateurs de disponibilité.

8 INTEROPERABILITÉ

Pour l'échange d'informations structurées au niveau de l'IGF, il faudra utiliser des systèmes automatisés par l'échange de donnés informatisées (EDI). Cela permettra la réduction des coûts des échanges, la diminution des erreurs, l'amélioration de la vitesse de traitement, la réalisation plus fréquente des échanges, l'automatisation du contrôle d'accès aux informations ainsi que l'enrichissement de l'information.

Pour chaque logiciel de l'IGF il faudra identifier :

- Les données à échanger en détails: définir une typologie d'échange d'informations, en veillant à ce que le sens de chaque type d'information soit le même pour tous les participants à l'échange.
- Les partenaires de l'échange: les entités du MdF qui échangeront des données entre elles.
- Les besoins en matière de sécurité: protéger les interfaces de connexion avec les organismes externes, classifier les données et définir les droits d'utilisation des données. Autrement dit, on devra faire une analyse sur le modèle conceptuel des données et le dictionnaire des données du MdF.

Les échanges de données entre administrations publiques devront suivre le principe de gratuité entre elles.

Il faudra aussi préparer les logiciels de l'IGF pour gérer les données des échanges. Les logiciels devront intégrer et stocker les données échangées et permettre leur exploitation. Les exigences d'interopérabilité sont détaillées dans les documents de spécifications fonctionnelles des logiciels qui devront être développés par l'IGF.

> On utilisera le standard Open source XML et/ou XBRL (eXtensible Business Reporting Language) pour l'échange d'informations au niveau de l'IGF.
>
> Il faudra aussi maîtriser les changements vers des fichiers Excel parce que ce type de documents est très utilisé dans les organisations publiques algériennes.

D'autre part, XBRL (basé en XML) est un standard dessiné pour les échanges financiers et basé sur XML. Il faudra donc définir la taxonomie XBRL, autrement dit, le dictionnaire dans lequel chaque information est identifiée de façon unique et qui permet être reconnue, traitée et présentée de différentes manières selon le type d'utilisation souhaitée.

9 SÉCURITÉ

En plus des dispositions et des lois ou règlements applicables, cette section vise à établir un guide sur l'utilisation de moyens électroniques, ce qui permet de mettre en oeuvre une protection adéquate du domaine de la sécurité de l'information.

Pour la gestion initiale de la sécurité, un ensemble de tâches à exécuter simultanément et de manière évolutive doivent être considérées :

- Développer une matrice pour la répartition des rôles et des responsabilités, avec l'attribution de ces rôles à des personnes identifiées dans l'organisation.
- Définition des mesures à appliquer dans chacun des niveaux de sécurité.
- Catégorisation des systèmes et services d'information.

9.1 Rôles et responsabilités

Dans toutes les organisations, il existe différentes responsabilités liées au domaine de la sécurité de l'information. Pour en effectuer une gestion efficace et complète, ces dernières doivent être regroupées dans un ensemble de rôles, et identifiées en cas d'incompatibilité lors de l'exécution. Ensuite, les rôles traditionnels sont répertoriés, ainsi que les responsabilités qui jouent habituellement. Il est primordial pour l'organisation d'adapter ce modèle à ses besoins et d'attribuer les rôles aux personnes qui leur incombent.

9.1.1 Responsable du Sécurité de l'Information

Il est le plus haut représentant de l'organisation dans le domaine de la sécurité de l'information et est aussi responsable de la mise en œuvre des mesures de sécurité pour les systèmes et services d'information de l'organisation. Il est aussi en charge de la préparation de la documentation réglementaire dans le domaine de la sécurité de l'information.

- Reçoit des rapports et informe les différentes personnes à propos de l'impact des décisions que peuvent faire chacun d'entre elles dans le domaine de la sécurité de l'information.
- Collabore à la catégorisation du niveau de sécurité des systèmes d'information et des services de l'organisation.
- Commande des audits et coordonne des contrôles des systèmes d'information et des services de l'organisation au niveau de la sécurité de l'information.

9.1.2 Responsable du Service

Il est responsable des autorisations d'accès et du traitement des données dans son service. Une personne peut être responsable de plus d'un service.

- Autorise l'accès et/ou refuse des permis aux systèmes d'information pour l'utilisateur dans son service.
- Désigne des responsables du système d'information dans son service.
- Adopte les mesures nécessaires pour faire respecter des règles, politiques, directives et procédures de l'organisation en matière de sécurité de l'information dans son

service.

9.1.3 Responsable du Système d'Information

Il est responsable des autorisations d'accès et du traitement des données dans son système d'information. Une personne peut être responsable de plus d'un système d'information.

- Connaître les fonctions et obligations du personnel ayant accès aux données ; autorise les demandes d'accès, et supervise la mise à jour de la liste des utilisateurs autorisés dans son système d'information.
- Désigne des Administrateurs dans son système d'information.
- Catégorise le niveau de sécurité de son système d'information, avec l'aide du Responsable du Sécurité de l'Information,
- Assure l'adoption des mesures nécessaires pour faire respecter des règles, politiques, directives et procédures, en plus des normes et mécanismes mis en place en matière de sécurité de l'information,
- Fournit de l'aide à la réalisation des audits de sécurité de son système d'information, reçoit des rapports d'audits, adopte et promeut des mesures correctives jugées appropriées.
- Il autorise la transmission d'informations dans différents formats à ceux qui sont enregistrés dans son système d'information. Il autorise également la récupération des données de sauvegarde et l'utilisation des données réelles dans les tests.

9.1.4 Administrateur du Système d'Information

Gère des autorisations d'accès et exécute des instructions, procédures et outils techniques désignés dans son système d'information. Une personne peut être administratrice de plus d'un système d'information.

- Matérialise des autorisations et réalise le profilage d'accès au son système d'information.
- Soutient et garde des données nécessaires sur l'autorisation ou le refus d'accès à des utilisateurs au système d'information.

9.1.5 Chef de Projet du Système d'Information

Accorder la plus grande attention à la prise de conscience des personnes impliquées dans le processus et leurs responsables hiérarchiques afin qu'elles ne soient pas sources de risque pour la sécurité : l'ignorance, l'instruction inadéquate ou le manque d'organisation ou de coordination. Une personne peut être chef de projet de plus d'un système d'information.

- Décider des exigences fonctionnelles et des niveaux de sécurité requis dans chaque dimension de la sécurité, de l'architecture technologique, sa topologie et ses méthodes de gestion, ainsi que l'établissement de critères pour l'utilisation et des

services liens.

- Définit le flux d'autorisation nécessaire pour accéder à son système d'information, la technologie, les paramètres de performance et les ressources requises en termes de sauvegarde et d'interopérabilité.
- Assure que les mesures de sécurité sont correctement intégrées et que les bonnes pratiques de sécurité sont présentes tout au long du cycle de vie dans son système d'information.
- Communique et collabore dans la résolution des incidents liés au système d'information.
- Reçoit des rapports d'audit, peut tirer des conclusions et est chargé de prendre les mesures correctives appropriées.
- Ordonne la mise en œuvre et la suspension du système d'information, dans chaque environnement d'exécution.

9.1.6 Développeur du Système d'Information

Il est engagé dans l'environnement de développement et s'occupe des activités identifiées par le chef de projet au cours du développement. Une personne peut être développeur de plus d'un système d'information.

- Responsable des produits réunissant les exigences de sécurité dans son système d'Information.
- N'utilise pas des données réelles dans les tests avec son système d'information.
- Intervient dans les révisions du code source.
- Assure l'implémentation des mécanismes d'identification, d'authentification, de protection et du traitement des registres d'audit, dans son système d'information.

9.1.7 Responsable de Service TI

Il est responsable de la gestion et l'administration des ressources allouées, y compris du personnel, des équipements, des services et des applications. Une personne peut être responsable de plus d'un service TI.

- Définit les règles d'accès dans son service TI et son niveau de sécurité, avec l'aide du Responsable de la Sécurité de l'Information.
- Soutient les groupes d'accès pour l'administration et la gestion dans son service TI.

9.1.8 Utilisateur

Un utilisateur est interne lorsqu'il est employé par l'organisation. Il est dans ce cadre autorisé à se connecter à des réseaux d'entreprise internes. Dans le cas contraire, l'utilisateur est externe.

9.2 Matrice de ségrégation des rôles.

- La cellule contenant un « x » signifie que ces deux rôles ne peuvent être assumés par

la même personne.

- La cellule contenant un « o » signifie que ces deux rôles ne devraient pas être assumés par la même personne, mais ils peuvent être admis des exceptions justifiées.

Rôles		1	2	3	4	5	6	7	8	9
Responsable de la Sécurité de l'Information	1		x	x	x	x	x	x		x
Responsable du Service	2	x				o	o			x
Responsable du Système d'Information	3	x			x	x	x			
Administrateur du Système d'Information	4	x		x		x	x			
Chef de Projet du Système d'Information	5	x	o	x	x					
Développeur du Système d'Information	6	x	o	x	x					
Responsable du Service TI	7	x								
Utilisateur interne	8									x
Utilisateur externe	9	x	x						x	

9.3 Unités organisationnelles de la sécurité de l'information

9.3.1 Comité de Direction pour la Sécurité de l'Information

Établit et approuve les lignes directrices, les normes et la performance organisationnelle concernant la sécurité de l'information de l'organisation et en particulier, la politique de contrôle d'accès au réseau et aux systèmes d'information et services.

Il doit se réunir périodiquement, et comprend les membres suivants :

- Président: un représentant de la direction de l'organisation.
- Secrétaire: responsable de la sécurité de l'information dans l'organisation.
- Participants: des directeurs représentant les services de l'organisation, des systèmes d'information et des services TI, avec capacité suffisante pour prendre des décisions dans le domaine de la sécurité de l'information au sein de l'organisation.

9.3.2 Le Groupe de Travail Technique pour la sécurité de l'information

Développe et présente les lignes directrices proposées, les règles et les mesures d'ordre organisationnel qui sont ordonnées par le Comité de Direction pour la Sécurité de l'Information.

Il doit se réunir périodiquement, et comprend les participants suivants:

- Président: le responsable de la sécurité de l'information
- Participants: représentants des systèmes d'information et des services TI disposant

d'une capacité suffisante pour mettre en oeuvre les décisions adoptées dans le domaine de la sécurité de l'information de l'organisation.

9.4 Recommandations pour le modèle de sécurité de l'IGF

Compte tenu de la taille de l'organisation et de la disponibilité des ressources, il est recommandé à l'IGF de dresser un design évolutif qui permette une gestion simple et complète de la sécurité de l'information, et qui intègre, dès le début, le soutien de la direction dans la mesure où c'est l'un des facteurs décisifs de succès dans tout projet lié à la sécurité de l'information.

If faut proposer ci-dessous un schéma minimal et quelques lignes directrices pour sa mise en oeuvre, ce qui implique l'adoption d'une proposition similaire qui peut être la structure développée plus tard, comme l'exige l'évolution de l'organisation.

Parmi les rôles décrits, le plus important de tous est sans doute le Responsable de la Sécurité de l'Information. Il est à ce titre fortement recommandé de trouver une personne au sein de la hiérarchie pour prendre des décisions et d'imposer des critères de sécurité dans l'organisation. Cette personne devrait être au courant de l'évolution des services de technologies de l'information et sensible aux conséquences éventuelles des décisions prises au niveau technique.

Les Responsables plausibles du Service sont déjà employés par l'organisation. Comme le nombre de systèmes d'information existant est très réduit, l'objectif est d'abord d'essayer d'éviter d'ajouter à la complexité du mécanisme d'autorisation d'accès.

Les rôles qui reviennent aux Responsable du Service et Responsable du Système d'Information peuvent être assurés par une seule personne dans un premier temps, jusqu'à ce que l'organisation acquiert la maturité et la taille suffisantes pour fournir du personnel différencié qui assumera ces responsabilités.

En revanche, les tâches des Administrateurs de Systèmes d'Information devraient être réalisés par des personnes autres que celles qui viennent d'être citées. Il y va de de la confiance, de la crédibilité et de la sécurité suffisantes et nécessaires au bon fonctionnement du système. Dans tous les cas, il faudra au final identifier les Chefs de Projets qui seront les figures les plus importantes des Systèmes d'Information en raison de leurs responsabilités.

Les rôles liés au développement, à savoir le Développeur de Système d'information et Responsable du Service TI, seront probablement assumés par le personnel de la DMNI et ce sans formalité nécessaire.

En ce qui concerne les rôles, il convient d'observer l'existence de certaines caractéristiques déjà mentionnées qui ne devraient pas être attribués à des utilisateurs externes dans la mesure où elles ne doivent en aucun cas être hors du contrôle de l'organisation.

Enfin, la gestion
organisationnelle de la sécurité de l'information pourrait être exercée en mettant
en œuvre un comité de direction, qui donne l'importance nécessaire aux
décisions prises, en laissant pour plus tard la création d'un groupe technique.

9.5 Mesures

En prenant comme référence le ENS[1] mis en ouvre pour la sécurité de l'Administration budgétaire, il est nécessaire d'ajouter, pour chacun des ensembles, un tableau indiquant les mesures de sécurité comprenant les conventions suivantes:

- Pour indiquer qu'une mesure de sécurité particulière devrait être appliquée à une ou plusieurs dimensions de la sécurité à aucun niveau, le terme « applicable » est utilisé.
- « n.a. » signifie « ne s'applique pas ».
- Pour indiquer que les exigences d'un niveau sont égales au niveau inférieur, il est utilisé « = ».
- Pour indiquer une gradation de l'augmentation des besoins en fonction du niveau de la dimension de sécurité, il est utilisé « + » et « ++ ».
- Pour indiquer qu'une mesure protège spécifiquement une certaine dimension de la sécurité, leur initiale est mentionnée : « D », « I », « C », « A » ou « N ».

Dans la première colonne de chaque table, sont indiquées les mesures proposées à l'IGF et sont présentées comme suit :

- Nécessaire : mesures recommandées à intégrer immédiatement.
- Souhaitable : mesures recommandées à intégrer à court terme.
- Potentiel : mesures recommandées à intégrer à moyen ou long terme.
- Secondaire: mesures qui peuvent être intégrées à long terme.

Le travail de l'organisation est de définir pour chacun des trois niveaux de sécurité (bas, moyen ou élevé) les actions obligatoires pour chaque mesure, c'est pourquoi des exemples sont donnés pour les mesures proposées de niveau Nécessaire ou Potentiel.

Ces mesures renvoient à un minimum de mise en oeuvre. Dans le cas contraire, il faudra formuler les raisons pour lesquelles elles ne le sont pas ou ont été remplacées par d'autres mesures de sécurité qui permettent d'atteindre le même effet protecteur sur l'information et les services.

9.5.1 Cadre organisationnel

Chaque organisation doit assurer la réalisation de ses objectifs. Elle doit veiller également à définir des rôles et à établir des responsabilités et des canaux de coordination. Cette structure permet la gestion quotidienne des activités de routine et la résolution ordonnée des incidents qui peuvent se produire.

IGF	Dimensions et niveaux				Mesures de sécurité	
	Affecté	Bas	Moyen	Élevé		
					org	Cadre organisationnelle
Nécessaire	n.a.	applicable	=	=	org.1	Politique de sécurité

[1] Schéma National de Sécurité est la référence en sécurité pour des administrations publiques espagnoles

Souhaitable	n.a.	applicable	=	=	org.2	Normatives sur la sécurité
Secondaire	n.a.	applicable	=	=	org.3	Procédures sur la sécurité
Souhaitable	n.a.	applicable	=	=	org.4	Processus d'autorisation

9.5.1.1 Politique de sécurité (Nécessaire)

Il s'agit d'un document de haut niveau qui définit la notion de « Sécurité de l'Information » dans une organisation. Le document doit être accessible et connu par tous les membres de l'organisation, et écrit d'un façon simple, précise et compréhensible. Il doit être bref, en laissant les détails techniques à d'autres documents normatifs. C'est dans ce document que sont établies les autorités au sein de l'organisation : rôles et responsabilités. Il est obligatoire pour tous les utilisateurs de l'organisation.

9.5.1.2 Normes de sécurité (Souhaitable)

Ensemble de documents définissant la manière d'aborder des questions de sécurité. Ils définissent la position de l'organisation sur certains aspects spécifiques et servent à indiquer comment agir si une circonstance n'est pas couverte par une procédure explicite pouvant être inexacte ou contradictoire avec les normes d'usage.

Exemples: la gestion d'accès, protection contre les logiciels malveillants, le développement et l'installation d'applications, l'accès à distance, le traitement des informations imprimées, utiliser le courrier électronique et la navigation, la classification des informations, le traitement des données personnelles, les sauvegardes, la gestion des mots de passe et cryptage, accords de confidentialité, dépannage, etc.

9.5.1.3 Processus d'autorisation (Souhaitable)

Les systèmes d'information et les systèmes d'organisation ne doivent pas admettre des éléments non autorisés qui minent la confiance dans le système en modifiant la surface d'attaque et en donnant naissance à de nouvelles vulnérabilités qui pourraient être exploitées.

Exemples: l'utilisation des installations du matériel d'entrée et les applications de production, établir des liens de communication avec d'autres systèmes, des médias, des informations sur l'utilisation des médias et des appareils mobiles, les services de tiers, l'utilisation de matériel appartenant à l'utilisateur (BYOD), etc.

9.5.2 Cadre opérationnel

Des mesures visant à protéger le fonctionnement du système en tant que composante intégrale définie pour atteindre un objectif. Beaucoup d'entre elles servent à obtenir une vision globale et inclusive de la façon dont la structure de l'organisation est gérée, et sont souvent présentés sous forme de documentaires d'ordre descriptif.

IGF	Dimensions et niveaux				Mesures de sécurité	
	Affecté	Bas	Moyen	Élevé		
					op	Cadre opérationnel
					op.pl	Planification

Souhaitable	n.a.	applicable	+	++	op.pl.1	Analyse des risques
Potentiel	n.a.	applicable	+	++	op.pl.2	Architecture de sécurité
Potentiel	n.a.	applicable	=	=	op.pl.3	Acquisition de nouveaux composants
Souhaitable	D	n.a.	applicable	=	op.pl.4	Gestion des dimensions
Secondaire	n.a.	n.a.	n.a.	applicable	op.pl.5	Composants certifiés
					op.acc	Contrôle d'accès
Potentiel	A T	applicable	=	=	op.acc.1	Identification
Potentiel	I C A T	applicable	=	=	op.acc.2	Conditions d'accès
Nécessaire	I C A T	n.a.	aplica	=	op.acc.3	La répartition des tâches
Souhaitable	I C A T	applicable	=	=	op.acc.4	Gestion processus des droits d'accès
Nécessaire	I C A T	applicable	+	++	op.acc.5	Mécanisme d'authentification
Potentiel	I C A T	applicable	+	++	op.acc.6	Accès local (local login)
Potentiel	I C A T	applicable	+	=	op.acc.7	Accès à distance *(remote login)*
					op.exp	Exploitation
Secondaire	n.a.	applicable	=	=	op.exp.1	Inventaire des biens
Potentiel	n.a.	applicable	=	=	op.exp.2	Paramètres de sécurité
Secondaire	n.a.	n.a.	applicable	=	op.exp.3	Gestion de la configuration
Secondaire	n.a.	applicable	=	=	op.exp.4	Entretien
Secondaire	n.a.	n.a.	applicable	=	op.exp.5	Gestion du changement
Potentiel	categoría	applicable	=	=	op.exp.6	Protection contre les codes malveillants
Potentiel	n.a.	n.a.	applicable	=	op.exp.7	Dépannage
Potentiel	T	applicable	+	++	op.exp.8	Enregistrement des activités
Secondaire	n.a.	n.a.	applicable	=	op.exp.9	Enregistrement de dépannage
Secondaire	T	n.a.	n.a.	applicable	op.exp.10	Protection enregistrements d'activité
Secondaire	n.a.	applicable	+	=	op.exp.11	Protection des clés cryptographiques
					op.ext	Services externes
Potentiel	n.a.	n.a.	applicable	=	op.ext.1	Contrats et accord de niveau de service
Secondaire	n.a.	n.a.	applicable	=	op.ext.2	Gestion quotidienne
Secondaire	D	n.a.	n.a.	applicable	op.ext.9	Des moyens alternatifs
					op.cont	La continuité du service

Secondaire	D	n.a.	applicable	=	op.cont.1	Analyse d'impact
Secondaire	D	n.a.	n.a.	applicable	op.cont.2	Plan de continuité
Potentiel	D	n.a.	n.a.	applicable	op.cont.3	Essais périodiques
					op.mon	Surveillance du système
Secondaire	n.a.	n.a.	applicable	=	op.mon.1	Détection d'intrusion
Secondaire	n.a.	n.a.	n.a.	applicable	op.mon.2	Système des métriques

9.5.2.1 Analyse des risques (Souhaitable)

Identification des actifs les plus précieux, les menaces les plus probables, les sauvegardes et les risques résiduels.

Exemples:

Bas niveau - Analyse informelle en langage naturel.

Niveau moyen - Analyse semi-formelle en langage spécifique, avec un catalogue de menaces, une sémantique défini et une évaluation quantitative.

Niveau Élevé - Analyse formelle en langage spécifique, avec une base mathématique reconnue internationalement, y compris des vulnérabilités.

9.5.2.2 Gestion de dimensionnement (Souhaitable)

Avant de décider de la nature de démarrage, une étude préalable couvrira le traitement, les besoins de stockage (en cours et rétention), la communication, le personnel (nombre et qualifications) et les installations.

9.5.2.3 La répartition des tâches (Nécessaire)

Le système de contrôle d'accès est organisé de telle sorte que l'accord de deux ou plusieurs personnes est nécessaires pour effectuer des tâches critiques, empêchant ainsi la possibilité qu'une personne autorisée puisse abuser de ses droits pour commettre toute action illicite. Cette responsabilité concerne les fonctions suivantes: Développement d'opérations; Configuration et de maintenance; Audit ou contrôle.

9.5.2.4 Gestion des processus des droits d'accès (Nécessaire)

Principe du moindre privilège - Les privilèges de chaque utilisateur seront réduits au minimum nécessaire pour répondre à leurs obligations. Ainsi, les dommages qu'il peut causer à une entité accidentellement ou intentionnellement, sont dimensionnés.

Besoin de savoir - Les privilèges seront limités afin que les utilisateurs puissent avoir accès seulement à la connaissance de ces informations nécessaires pour remplir leurs obligations.

Capacité d'autoriser - Personnel uniquement et exclusivement habilité à le faire, peut accorder, modifier ou annuler l'autorisation d'accès aux ressources, selon aux critères établis par la personne responsable.

9.5.2.5 Mécanisme d'authentification (Nécessaire)

Ils seront adaptés au niveau du système en fonction des différents facteurs

d'authentification (mémoriel - ce qu'il sait; matériel - ce qu'il possède; corporel - ce qu'il montre; réactionnel - ce qu'il fait).

Avant de fournir des informations d'authentification aux utilisateurs, ils doivent avoir été identifiés et enregistrés de manière fiable au système ou à un fournisseur d'identité électronique reconnu par l'organisation.

Les informations d'identification seront sous le contrôle exclusif de l'utilisateur et seront changées dans les intervalles marqués par l'organisation, selon le niveau de sécurité. Elles seront retirées lorsque l'entité mettra fin à sa relation avec le système.

Exemples:

Niveau bas - Une facteur d'authentification.

Niveau moyen - Deux facteurs d'authentification, et enregistrement préalable en personne.

Niveau élevé - En de ceux de niveau moyen, l'expiration des informations d'authentification après une période définie de non-utilisation.

9.5.3 Mesures de protection

Elles se concentrent sur la protection des actifs spécifiques, en fonction de leur nature, avec le niveau requis dans toutes les dimensions de la sécurité.

Ce sont des mesures visent à protéger le fonctionnement du système en tant que composante intégrale définie à un but. Beaucoup d'entre elles servent à obtenir une vision globale et inclusive de la façon dont la structure de l'organisation est gérée. Elles sont présentées sous forme de documentaires descriptifs.

IGF	Dimensions et niveaux				Mesures de sécurité	
	Affecté	Bas	Moyen	Élevé		
					mp	Mesures de protection
					mp.if	Protection des installations et des infrastructures
Potentiel	n.a.	applicable	=	=	mp.if.1	Des zones d'accès séparées et contrôlées
Potentiel	n.a.	applicable	=	=	mp.if.2	Identification des personnes
Secondaire	n.a.	applicable	=	=	mp.if.3	Aménagement des locaux
Secondaire	D	applicable	+	=	mp.if.4	Énergie électrique
Secondaire	D	applicable	=	=	mp.if.5	Protection contre l'incendie
Secondaire	D	n.a.	applicable	=	mp.if.6	Protection contre les inondations
Potentiel	n.a.	applicable	=	=	mp.if.7	Enregistrement d'entrée et sortie des équipements.
Secondaire	D	n.a.	n.a.	applicable	mp.if.9	d'Autres installations

					mp.per	Gestion du personnel
Souhaitable	n.a.	n.a.	applicable	=	mp.per.1	Caractérisation du travail
Souhaitable	n.a.	applicable	=	=	mp.per.2	Devoirs et obligations
Secondaire	categoría	applicable	=	=	mp.per.3	Conscience
Secondaire	categoría	applicable	=	=	mp.per.4	Formation
Secondaire	D	n.a.	n.a.	applicable	mp.per.9	Personnel suppléant
					mp.eq	Protection d'équipements
Secondaire	n.a.	applicable	+	=	mp.eq.1	Lieu de travail propre
Potentiel	A	n.a.	applicable	+	mp.eq.2	Blocage d'équipements
Souhaitable	categoría	applicable	=	+	mp.eq.3	Protection des ordinateurs portables
Secondaire	D	n.a.	applicable	=	mp.eq.9	Des moyens alternatifs
					mp.com	Protection des communications
Nécessaire	n.a.	applicable	=	+	mp.com.1	Sécurisation du périmètre
Potentiel	C	n.a.	applicable	+	mp.com.2	Protection de la confidentialité
Potentiel	I A	applicable	+	++	mp.com.3	Protection de l'authenticité et de l'intégrité
Secondaire	n.a.	n.a.	n.a.	applicable	mp.com.4	Ségrégation de réseaux
Secondaire	D	n.a.	n.a.	applicable	mp.com.9	Des moyens alternatifs
					mp.si	Protection des médias d'information
Secondaire	C	applicable	=	=	mp.si.1	Étiquetage
Secondaire	I C	n.a.	applicable	+	mp.si.2	Cryptographie
Potentiel	n.a.	applicable	=	=	mp.si.3	Garde
Potentiel	n.a.	applicable	=	=	mp.si.4	Transport
Secondaire	C	applicable	+	=	mp.si.5	Destruction et erasure
					mp.sw	Protection des applications
Potentiel	n.a.	n.a.	applicable	=	mp.sw.1	Développement
Potentiel	n.a.	applicable	+	++	mp.sw.2	Acceptation et mise en service
					mp.info	Protection d'information
Potentiel	n.a.	applicable	=	=	mp.info.1	Données personnelles
Potentiel	C	applicable	+	=	mp.info.2	Qualification d'information

Secondaire	C	n.a.	n.a.	applicable	mp.info.3	Chiffrement
Secondaire	I A	applicable	+	++	mp.info.4	Signature électronique
Secondaire	T	n.a.	n.a.	applicable	mp.info.5	Timestamps
Secondaire	C	applicable	=	=	mp.info.6	Nettoyage des documents
Souhaitable	D	applicable	=	=	mp.info.9	Sauvegarde (backup)
					mp.s	Protection des services
Souhaitable	n.a.	applicable	=	=	mp.s.1	Protection de courriel
Souhaitable	n.a.	applicable	=	+	mp.s.2	Protection des services et des applications Web
Secondaire	D	n.a.	applicable	+	mp.s.8	Protection contre déni de service
Secondaire	D	n.a.	n.a.	applicable	mp.s.9	Des moyens alternatifs

9.5.3.1 Caractérisation du travail (Souhaitable)

Il faut définir les responsabilités de sécurité pour chaque travail, les exigences à remplir par les personnes qui l'occuperont, en particulier en termes de confidentialité, y compris la vérification des antécédents d'emploi, de formation et d'autres références.

9.5.3.2 Devoirs et obligations (Souhaitable)

Il faut informer chaque utilisateur interne ou externe des systèmes d'informations, des fonctions et des responsabilités de la sécurité qui incombent à son travail, y compris des mesures disciplinaires.

9.5.3.3 Protection des ordinateurs portables (Souhaitable)

If faut mettre en place un inventaire des ordinateurs portables qui identifie la personne responsable de chacun d'eux, et vérifier régulièrement que l'équipement reste sous le contrôle de l'utilisateur désigné. Les utilisateurs recevront des instructions sur l'utilisation autorisée, la gestion quotidienne, les communications permises et la gestion des incidents en cas de dommage, perte ou de vol.

9.5.3.4 Sécurisation du périmètre (Nécessaire)

Il doit délimiter le périmètre logique du système; c'est-à-dire l'intégralité des points d'interconnexion avec l'extérieur. Il doit avoir un pare-feu qui autorise uniquement les flux de transit autorisés.

9.5.3.5 Sauvegarde (Souhaitable)

Il faut faire des copies de sauvegarde qui peuvent récupérer les données perdues accidentellement ou intentionnellement avec une longueur à déterminer par l'organisation. Ces copies doivent posséder le même niveau de sécurité que les données d'origine. Il est également recommandé d'établir un processus d'approbation pour la récupération des

copies.

9.5.3.6 Protection de courriels (Souhaitable)

Protection du corps des messages et des documents joints dans le routage des messages (DNS), contre les courriels non sollicités, les virus, les *vers (worm)*, les chevaux de Troie, les logiciels espions et les codes mobile de type applet.

9.5.3.7 Protection de services et des applications Web (Souhaitable)

Ce sont pour la plupart des mesures de prévention, qui mettent l'accent sur les processus de développement, les paramètres de sécurité, les contrôles de maintenance, et la séparation des protections des tâches.

9.6 Catégorisation

La catégorie de sécurité d'un système d'information module l'équilibre entre l'importance des informations traitées, les services fournis et les efforts de sécurité nécessaires, en fonction des risques auxquels elle est exposée et ce, à la discrétion du principe de proportionnalité.

La détermination de la catégorie sera basée sur l'évaluation de l'impact d'un incident affectant la sécurité de l'information ou sur des services qui mettent en danger chaque dimension de sécurité.

L'évaluation des conséquences d'un impact négatif sur la sécurité des informations et des services se fera en fonction de leur impact sur la capacité de l'organisation à atteindre ses objectifs, la protection de ses actifs, ses obligations de service, l'état de droit et les droits des utilisateurs.

Le travail de l'organisation est de prendre chacun des systèmes d'information existants séparément et le soumettre à un processus de catégorisation pour son évaluation dans chacune des dimensions de sécurité.

9.6.1 Dimensions

Afin de déterminer l'impact qu'aurait sur l'organisation un incident affectant la sécurité de l'information ou des systèmes, et d'établir l'état du système, les dimensions suivantes de la sécurité sont prises en compte.

9.6.1.1 Confidentialité

L'information n'est pas accessible aux non autorisés - En fonction des conséquences de sa révélation aux non-autorisés.

9.6.1.2 Intégrité

L'information n'a pas été falsifié - En fonction des conséquences de sa modification pour les non-autorisés.

9.6.1.3 Disponibilité

L'information est toujours destinée aux autorisés - En fonction des conséquences de ne pas pouvoir retracer qui a accès à l'information ou modifié le cas échéant.

9.6.1.4 Authenticité

L'information est vraie - En fonction des conséquences d'une information fausse.

9.6.1.5 Traçabilité (Non-refus)

La source d'information peut être identifiée de manière fiable - En fonction des conséquences des autorisés qui ne pouvaient pas accéder aux informations au besoin.

9.6.2 La détermination du niveau requis dans une dimension

Les informations ou le service peuvent être affectés dans une ou plusieurs des dimensions de sécurité. Chaque dimension de sécurité affectée est désignée à l'un des niveaux suivants: Bas, Moyen ou Élevé. Si une dimension de sécurité n'est pas affectée, elle ne sera désignée à aucun niveau.

9.6.3 Sans niveau

- (C) L'information à caractère public, accessible à tout le monde.
- Manque de conséquences ou ils seront réparés facilement et rapidement.
- Origine non pertinente ou largement connue par d'autres moyens.
- Destinataire non pertinent (diffusion anonyme).
- Il ne peut y avoir d'erreurs, ou elles sont faciles à réparer.
- Des infractions pertinentes qui ne peuvent pas être perpétrées.
- (D) Informations indispensables indéfiniment.
- (D) DMIA[2] supérieur à 5 jours ouvrables (une semaine).

9.6.4 Niveau Bas

Il sera utilisé lorsque les conséquences d'un incident de sécurité affectant l'une des dimensions de sécurité impliquent des blessures limitées sur les fonctions de l'organisation, ses actifs ou sur les personnes touchées :

- Réduction significative de la capacité de l'organisation à répondre efficacement à ses obligations actuelles, même si elles continuent de fonctionner.
- (C) L'information ne doit pas être connue par des personnes extérieures.
- Légère violation d'une règle.
- Des pertes économiques appréciables.
- Des dommages considérables à la réputation des citoyens ou organisations.
- De multiples manifestations individuelles.
- (D) DMIA entre 1 et 5 jours ouvrables (une semaine).
- (T) Difficulté à corriger les erreurs ou de poursuivre les crimes.

[2] DMIA - Durée Maximale d'Interruption Admissible

9.6.5 Niveau Moyen

Il sera utilisé lorsque les conséquences d'un incident de sécurité affectant l'une des dimensions de la sécurité impliquent des blessures graves sur les fonctions de l'organisation, ses actifs ou les personnes touchées.

- Réduction significative de la capacité de l'organisation à répondre efficacement à leurs obligations de base, bien que ceux-ci continuent de fonctionner.
- (C) L'information ne peut être connue qu'avec une autorisation explicite.
- Des dommages importants mais remédiables.
- Violation matérielle ou formelle d'une règle.
- Des pertes économiques importantes.
- Des dommages importants à la réputation des citoyens ou organisations.
- Manifestations publiques (perturbation de l'ordre public).
- (D) DMIA entre 4 et 24 heures (un jour).
- (T) Difficulté notable pour corriger des erreurs ou poursuivre des crimes.
- (T) Facilité à commettre des crimes.

9.6.6 Niveau Élevé

Il sera utilisé lorsque les conséquences d'un incident de sécurité affectant l'une des dimensions de la sécurité impliquent une blessure très grave sur les fonctions de l'organisation, ses actifs ou les personnes touchées.

- Annulation de la capacité de l'organisation à répondre à certaines de leurs obligations fondamentales qu'ils continuent à effectuer.
- (C) Information connue par un petit nombre de personnes.
- Des dommages graves, des réparations difficiles ou impossibles.
- Violation grave d'une règle.
- De grandes pertes économiques, ou d'importants changements financiers.
- Des dommages importants à la réputation des citoyens ou organisations.
- Des manifestations de masse (perturbation sérieuse de l'ordre public).
- (D) DMIA moins de 4 heures.
- (T) Une grande difficulté à corriger des erreurs ou poursuivre des crimes.
- (T) Une grande facilité à commettre des crimes graves.

9.7 La détermination de la catégorie d'un système d'information ou d'un service

La séquence d'actions pour déterminer la catégorie d'un système d'information ou d'un service comprend deux étapes:

1. Identifier le niveau correspondant à chaque dimension de sécurité.
2. Déterminer la catégorie du système d'information ou de service en fonction des critères suivants:
    a. Un système d'information ou service sera de catégorie élevée si l'une de ses dimensions de sécurité atteint le niveau élevé.
    b. Un système d'information ou service sera de catégorie moyenne si l'une de ses dimensions de sécurité atteint le niveau moyen, et aucune autre n'atteint un niveau plus élevé.
    c. Un système d'information ou service sera de catégorie basse si l'une de ses dimensions de sécurité atteint le niveau bas, et aucune autre n'atteint un niveau plus élevé.

10 ARCHITECTURE TI

10.1 Présentation générale

Cette section offre un aperçu sur les divers facteurs qui ont été pris en compte lors de la proposition de l'architecture appropriée pour l'IGF.
Etant donné que ces paramètres peuvent changer, l'architecture proposée est à la fois flexible et robuste et ce, dans le but d'être conforme aux besoins actuels et suffisamment évolutive pour répondre aux besoins futurs.

10.2 Scénario actuel

Actuellement, l'IGF a une infrastructure de TIC réduite, responsable principalement de la prestation de services aux inspecteurs, objectif atteint par le développement et mise en production des applications installées sur un serveur.
Dans ce scénario on peut remarquer les principes suivants, principes qui seront la base de la solution proposée:

- On devrait profiter de la connaissance en matière TIC du personnel de la DMNI, en particulier de son expérience avec le langage de programmation PHP et d'autres langages de balisage.

- Le personnel informatique de la DMNI n'a pas exprimé de préférences concernant l'architecture ou le type de logiciel à utiliser, alors que seront proposées les alternatives les plus actuelles et fiables afin de fournir à la DMNI la capacité de développer et de gérer des applications basées sur les technologies web.

- Aujourd'hui, l'IGF ne dispose pas d'un centre informatique mais l'infrastructure TI proposée est en mesure d'être placée dans le futur centre de données du MDF sur le site de Birkhadem tel que prévu par l'AIFP.

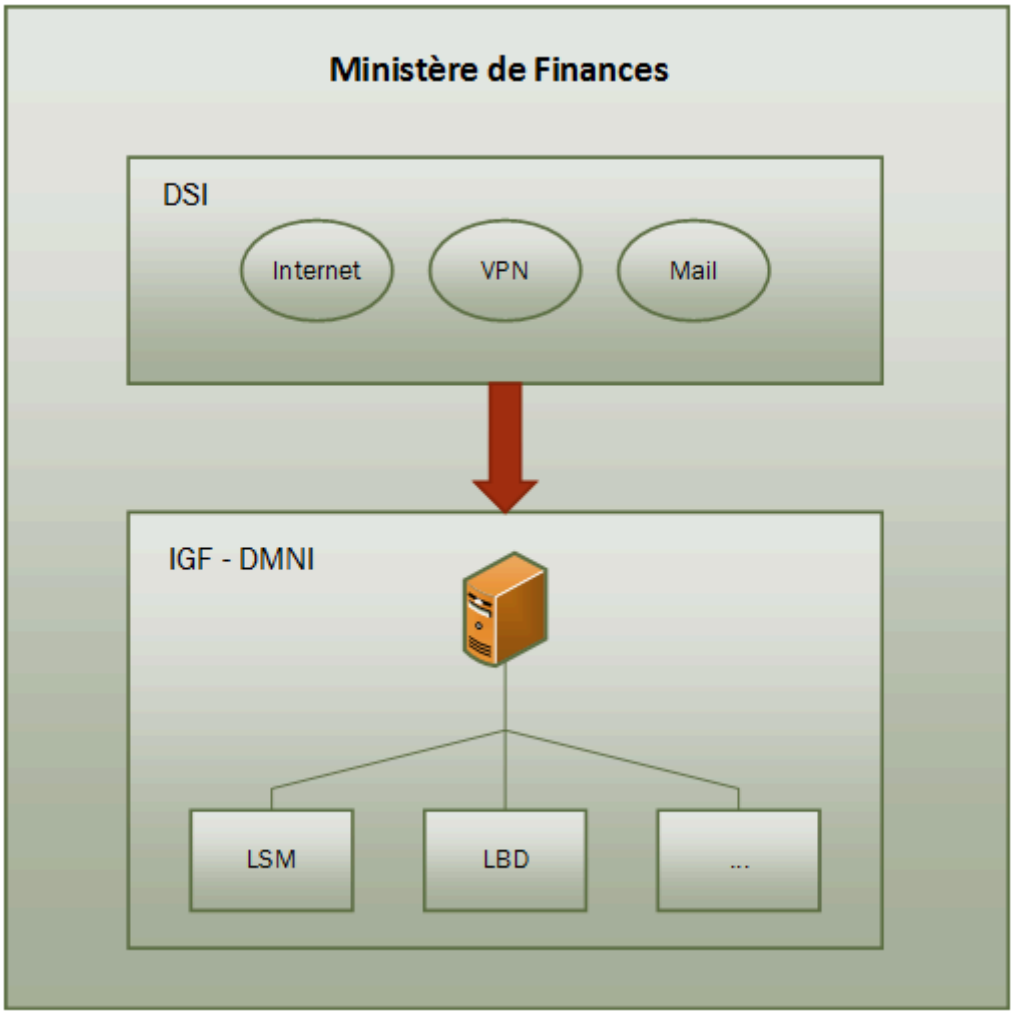
- Le nombre d'utilisateurs est relativement petit et la taille des applications à faire est modeste (pas plus de 400).

- La DMNI dispose d'un serveur physique qu'on peut réutiliser. Ce serveur utilise un système d'exploitation Windows 2003 Server. De même, la DMNI utilise un système d'annuaire Microsoft Active Directory, mais sans une configuration complète.

- Le serveur héberge les environnements de développement et de production. Cette situation présente des risques de tous types et doit être améliorée.

- Le serveur n'a pas la redondance appropriée, ce qui augmente le risque d'indisponibilité des applications et l'arrêt des processus de développement en cas de problème.

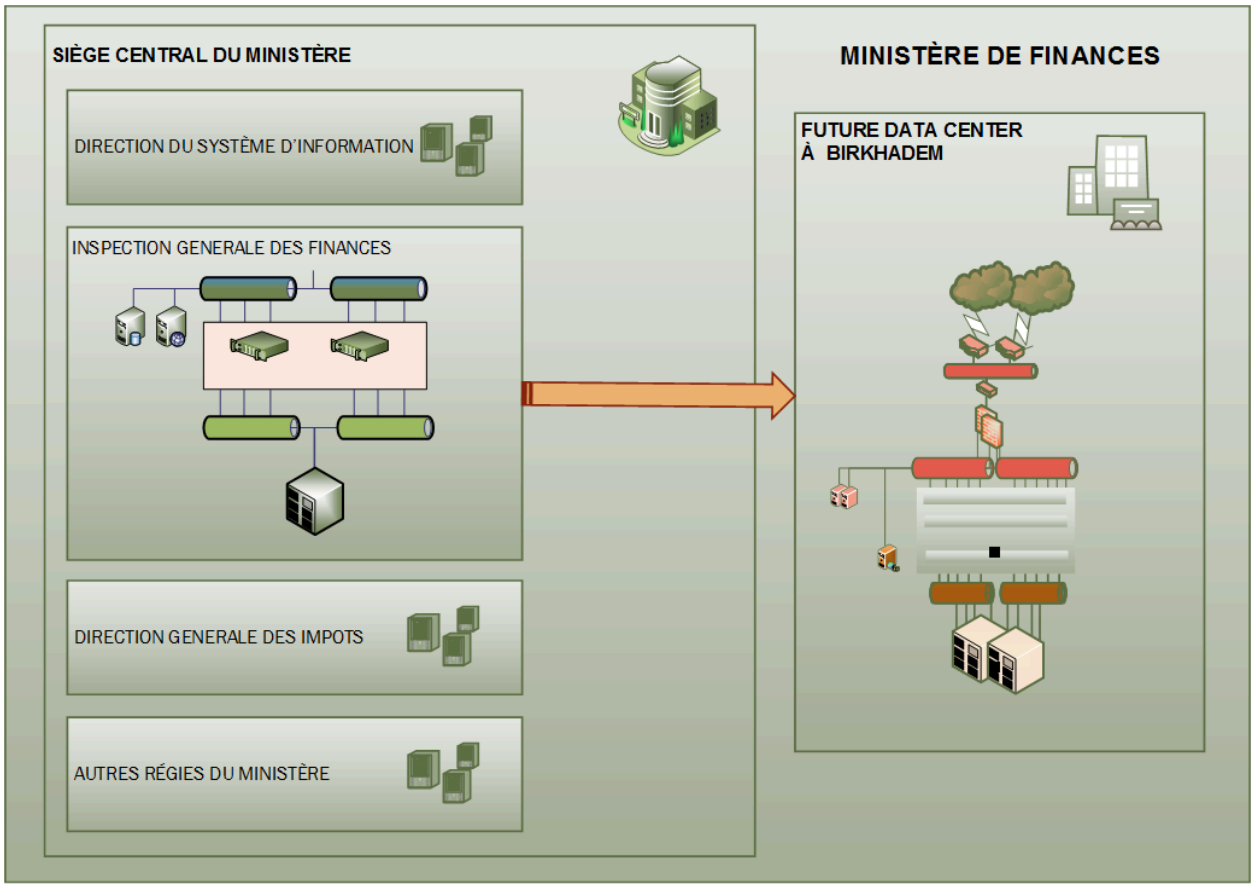
- Les services Internet, les services VPN et le service de courrier électronique sont approvisionnés par la DSI.



Pour la configuration de l'architecture informatique proposée, on a commencé à partir de la situation actuelle, présentée dans l'illustration ci-dessus. La cible est marquée par le futur Centre de traitement des données à Birkhadem, ce qui devrait permettre l'intégration de la nouvelle architecture de l'IGF.

10.3 Scénarios futurs

En tenant compte du fait de disposer d'un Centre de traitement des données prévu par le PSMFP et que la proposition TI faite ici envisage une architecture informatique prête pour sa future installation dans ce CPD, il a été proposé une architecture réaliste qui couvre les attentes de l'IGF.



10.4 Aperçu de l'architecture

L'architecture proposée pour l'IGF est centralisée. Il y aura un site central hébergeant les systèmes informatiques nécessaires pour soutenir, d'un côté, les bases de données de l'IGF et les logiciels nécessaires à la réalisation de leurs tâches y compris la base des données des entités, l'application du programme annuel des missions, les informations de suivi des missions et d'autres informations de base pour l'Intranet. Et d'un autre côté, seront soutenus les outils de développement et de maintenance des applications dont ont besoin les équipes techniques de la DMNI pour développer leur travail. On peut voir les avantages d'une architecture centralisée dans l'annexe technique Architecture centralisée par rapport à l'architecture distribuée.

En ce qui concerne le Cloud Computing et ses grands avantages, il a été proposé une solution d'infrastructure interne dans les locaux de l'IGF, en raison de deux problèmes découlant de l'utilisation du nuage par un organisme gouvernemental. D'une part, l'organisme gouvernemental n'a plus de garanties (autres que contractuelles) de l'utilisation qui est faite de leurs données, puisqu'elles les confient à des tiers. D'autre part, des questions juridiques peuvent se poser, notamment par l'absence de localisation précise des données du cloud computing. Les lois en vigueur s'appliquent, mais pour quel serveur, quel centre de données, et surtout quel pays ? Voir l'annexe technique Cloud Computing.

Une autre décision importante repose sur la question de savoir si l'on utilise la virtualisation ou pas. Pour ce projet, l'architecture proposée repose sur l'approche de virtualisation. À ce sujet, voir l'annexe technique Serveurs physiques versus serveurs

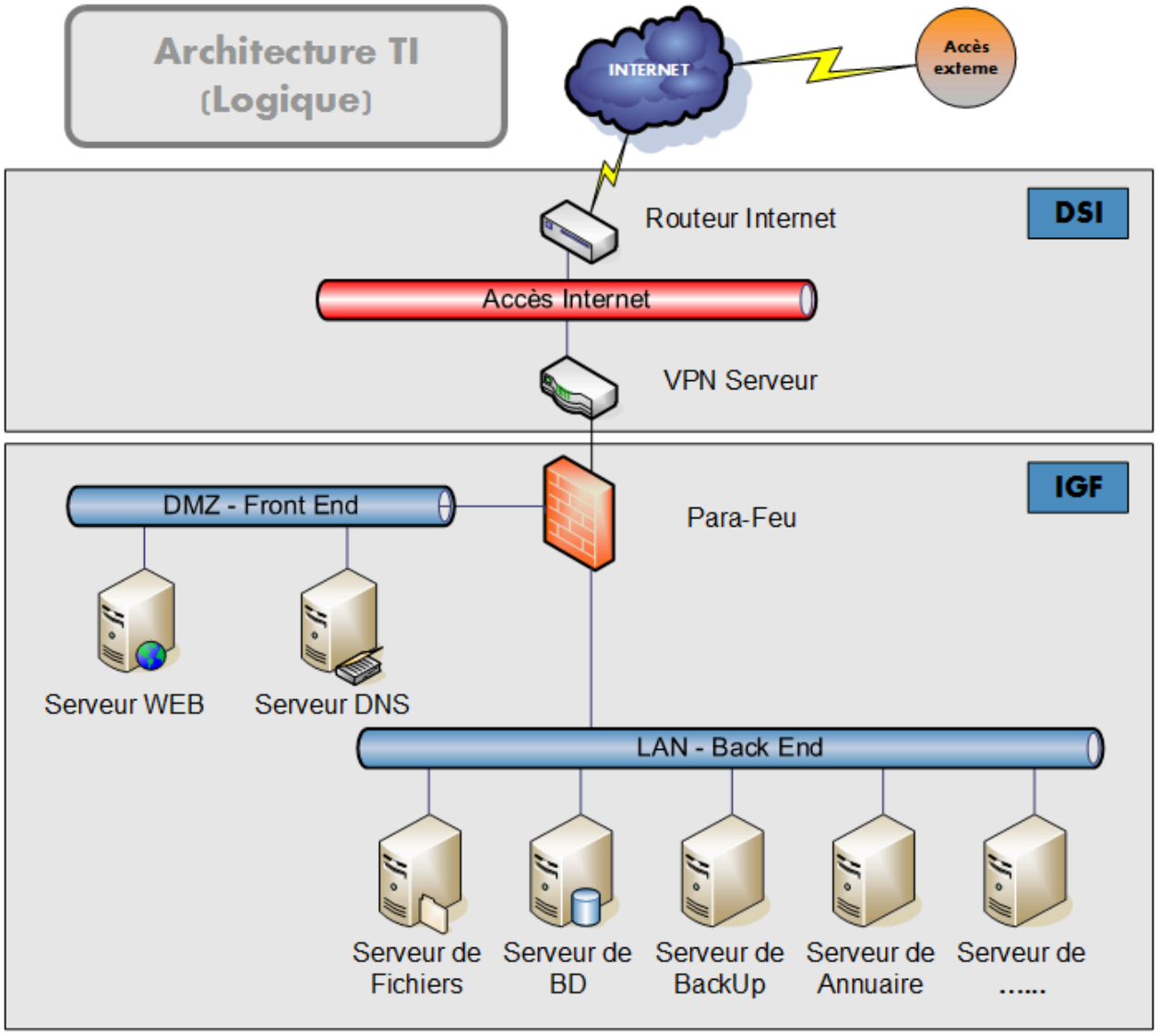
virtuels.

Compte tenu de ce qui précède, l'architecture proposée fournit le nombre minimum d'environnements, à savoir, le Développement et la Production. Toutefois, si les conditions budgétaires le permettent, il convient d'ajouter des environnements décrits dans la section consacrée à la définition des environnements afin d'être en mesure de poursuivre le cycle de déploiement recommandé dans l'annexe technique Architecture de déploiement.

10.4.1 Environnement de production (PRO)

10.4.1.1 Architecture logique

Vous pouvez voir dans l'image ci-dessous l'architecture logique, une architecture qui permettra couvrir les besoins de l'IGF.



Nous avons deux zones distinctes :

1. Une zone démilitarisée, DMZ, qui est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet (ou d'un autre réseau) par un commutateur. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet, c'est-à-dire, le Serveur du Domain et le Serveur WEB.
   Il est vrai que dans un premier temps il ne sera pas possible d'avoir un accès externe (Internet) sauf par VPN. Une fois que l'infrastructure existe, il sera prêt à fournir ce service.
   Afin d'éviter l'inconvénient découlant du fait qu'un seul et unique commutateur soit compromis, il est recommandé d'utiliser deux commutateurs en cascade afin d'éliminer ce risque. Voir l'annexe technique Réseau LAN.
2. Une zone interne protégée, la partie bien plus importante de l'infrastructure informatique de l'organisation où seront hébergées les bases de données et les informations les plus précieuses de l'IGF.
   Ici, tout utilisateur doit être identifié et authentifié dans un seul référentiel (ou annuaire d'entreprise) pour l'accès à l'ensemble des ressources ; dès que l'authentification sera assurée, l'intranet devra être en mesure de propager la session de l'utilisateur pendant toute son activité sans qu'il ait besoin de s'identifier à nouveau.
   L'Intranet proposé possède une architecture clients/serveur(s) n couches qui repose sur des composants suivants :

   - Serveur de fichiers pour le partage des données.
   - Serveur web de l'intranet pour le site web Intranet.
   - Serveur de bases de données pour le stockage des informations.
   - Serveur d'authentification pour identifier les utilisateurs et le stockage des annuaires.
   - Normalement, il y aurait un serveur de messagerie, mais dans notre cas, ce service est fourni par la DSI.
   - Des commutateurs comme éléments de l'infrastructure.
   - Serveurs pour fournir d'autres services: DHCP, annuaire, domain controller, Back-Up, etc.

10.4.1.2 Architecture physique

L'architecture physique proposée permettra de définir tous les services nécessaires pour l'environnement de production, y compris un éventuel environnement de pré-production. Comme le montre la figure suivante, le nombre d'éléments physiques (matériel) est relativement modeste.
L'objectif est d'utiliser des techniques de virtualisation, de sorte qu'avec quelques machines physiques, on puisse fournir tous les services indiqués dans l'architecture logique en définissant des serveurs virtuels.

L'infrastructure proposée comprend quatre serveurs physiques.

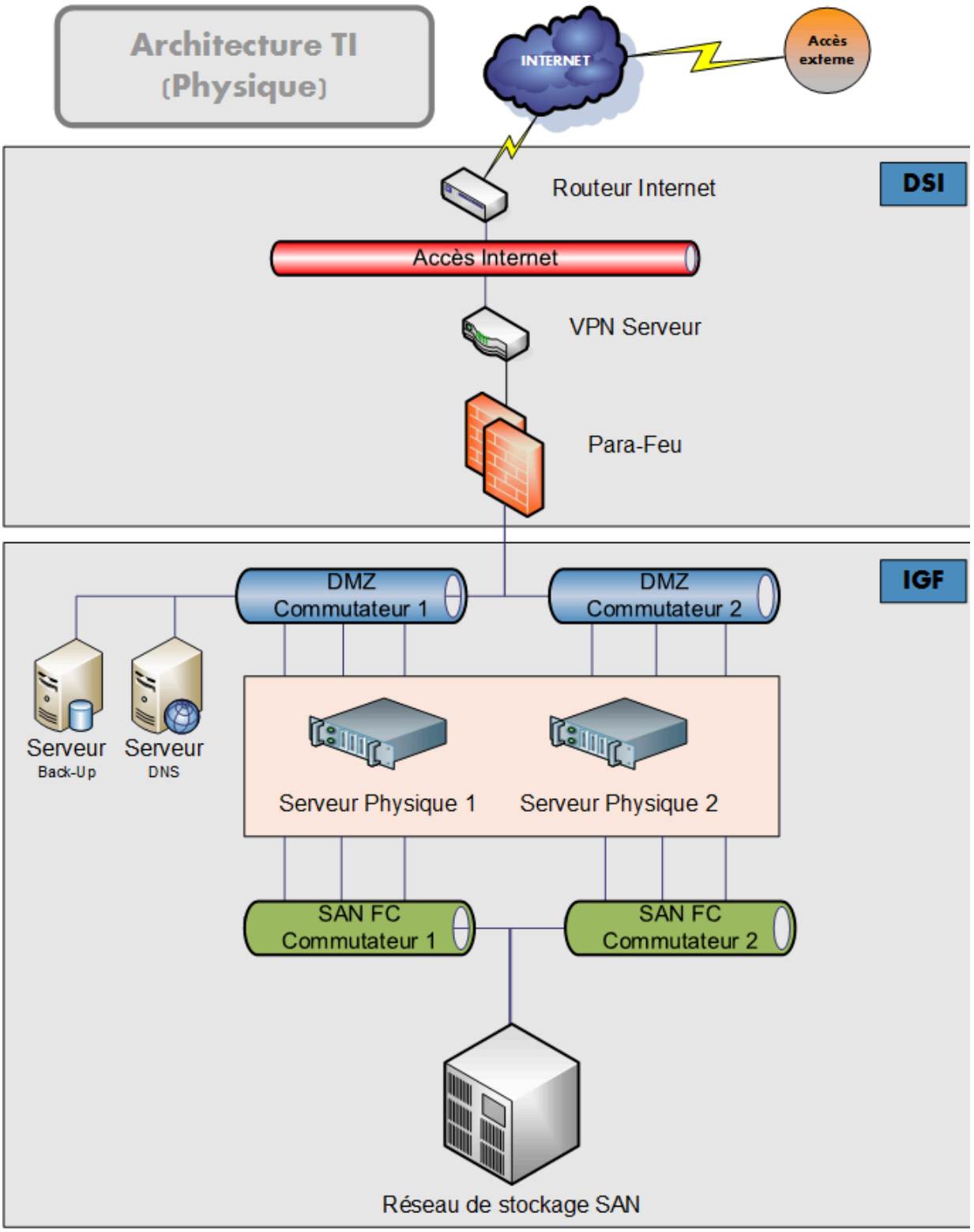
- Un serveur physique pour installer les services de DC+DNS+DHCP. Ce serveur peut être de petite/moyenne taille, et de type **tour** . On peut même réutiliser l'un de ceux déjà disponibles au sein de l'IGF.
- Un serveur physique pour le service de sauvegarde (BackUp). Comme dans le cas précédent, ce pourrait être un serveur type **tour** de taille petite/moyenne.

- Deux serveurs physiques pour installer l'hyperviseur virtuel sont nécessaires. Dans ce cas, de puissants serveurs sont proposés puisqu'ils vont héberger tous les serveurs virtuels de l'architecture. Bien que cette décision dépendra des caractéristiques des serveurs physiques choisis, les serveurs virtuels suivants doivent pour le moins être définis:
    - Un serveur pour la surveillance de l'infrastructure de serveurs et gérer l'hyperviseur de virtualisation.
    - Un serveur pour la gestion de sauvegarde.
    - Un serveur pour répliquer les services de DC+DNS+DHCP.
    - Un serveur comme serveur de données.
    - Un serveur comme serveur web.
    - Un serveur comme serveur de fichiers.
    - Un serveur pour le système de gestion de contenu.

En ce qui concerne les serveurs, la configuration optimale pour réduire au maximum des défaillances sur tous les services critiques, est de construire un cluster haute disponibilité de deux serveurs, situé sur deux machines physiques différentes, et configuré comme actif - actif.

Pour ce projet, la solution de stockage proposée est basée sur un réseau SAN. Il est conseillé, si l'on a assez de budget, que tous les composants du SAN soient dupliqués afin d'assurer le maximum de tolérance aux pannes:

- 2 commutateurs.
- 2 processeurs de contrôle.
- 2 alimentations.
- des grappes de disques en RAID 1, 5, 6, ...


Architecture TI
(Physique)
INTERNET
Accès externe
DSI
Routeur Internet
Accès Internet
VPN Serveur
Para-Feu
IGF
DMZ Commutateur 1
DMZ Commutateur 2
Serveur Back-Up
Serveur DNS
Serveur Physique 1
Serveur Physique 2
SAN FC Commutateur 1
SAN FC Commutateur 2
Réseau de stockage SAN

10.4.2 Environnement de pré-production (PRE)

Cet environnement devrait refléter le plus possible l'environnement de production actuel.

Il faut installer dans cet environnement les mêmes versions du logiciel de toutes les composantes installées à PRO. Cela permettra de détecter préalablement des problèmes avec la nouvelle version du logiciel à tester.

Le matériel utilisé sera d'une taille réduite, et plus bon marché, que celui de PRO.

Parfois, l'environnement de pré-production aura des données de type production (masquées), dans la mesure où il est utilisé pour enquêter sur les incidents de production et pour reproduire les tests le plus précisément.

Évidemment, le maintien de cet environnement a des coûts associés. On doit donc réfléchir aux moyens de les réduire au moyen, par exemple, de la virtualisation, de la réutilisabilité… etc.

10.4.3 Environnement de développement (DEV)

L'environnement de développement n'a pas besoin de machines puissantes quand il fait référence à des caractéristiques techniques. Néanmoins, cet environnement doit disposer des mêmes services que l'environnement de production en tant que bases de données, serveur web, serveur de fichiers, CMS, etc. Il n'est toutefois pas un environnement irremplaçable et nous pouvons mettre en œuvre tous ces services sur un seul serveur.

On pourrait avoir différents environnements de développement pour s'adapter aux besoins du projet à développer.

Ce serveur sera situé sur le réseau interne (LAN) et, en fonction de son utilisation, seules les équipes de développement de la DMNI auront accès à ce dernier.

11 NOUVEAUX RÔLES: PROPOSITION

11.1 Intranet

Pour la gestion de l'Intranet, il faut ajouter à l'organisation des nouvelles ressources humaines:

- L'Éditeur de l'Intranet.
  - responsable de valider, approuver et publier les articles sur l'Intranet
- Webmaster (rôle: Administrateur du Système d'information)
  - responsable de la gestion de l'Intranet
  - collabore avec l'Éditeur de l'Intranet dans les tâches d'approbation de contenu
  - Il est en charge de la maquettisation et publication des articles, et aussi de maintenir le système de mise à jour.

- Rédacteurs
  - responsable de la génération de contenu pour l'Intranet
  - chaque unité fonctionnelle aura un rédacteur
  - responsable d'envoyer le contenu généré à l'Éditeur Intranet

11.2 Service des TI

Pour la gestion des nouveaux systèmes d'information à mettre en marche à l'IGF, il faut ajouter à l'organisation des nouvelles ressources humaines :

- Responsable de Centre d'assistance technique
  - responsable de maintenir la qualité du service d'assistance technique fourni par le Service des TI
- Responsable du Service de Production: Chef d'exploitation
  - responsable de maintenir la disponibilité et la sécurité dans l'infrastructure de production et pré-production de l'IGF
- Responsable de Développement
  - responsable du développement des applications et de leur maintenance
  - il doit assurer la qualité des applications développées pour l'IGF (même celles développées avec l'aide d'un fournisseur extérieur)
- Ingénieur des systèmes. Administrateur de réseau
  - responsable de l'administration de l'infrastructure TI à implanter
    - Systèmes d'exploitation des serveurs, serveur web, passerelle SMTP,...
  - responsable des services de réseau (DNS, DHCP, SMTP, NTP, DA, Systèmes d'exploitation,...)
  - responsable technique des service Intranet
  - faire le support de niveau 2 (N2)

- Technicien des systèmes. Administrateur de LAN
  - responsable de l'administration de la LAN de la IGF et de l'interconnection avec la DSI
  - responsable de la configuration des postes de travail
  - faire le support de niveau 2 (N2)
- Technicien des supports niveau 1 (N1)
  - responsable de répondre aux demandes des usagers
  - responsable de l'installation et de la configuration des postes de travail
- Administrateur de base des données
  - responsable de l'administration des bases de données installées en PRO et PRE
  - appui aux équipes de développement des aspects reliés aux bases de données
  - faire le support de niveau 2 (N2)
- Analyste - Développeur web
  - Collaborer dans l'élaboration des spécifications fonctionnelles
  - Analyser les applications à développer
  - dessiner les applications à développer
  - développer des applications
  - documenter des applications
- Développeur/s web
  - Collaborer dans le dessin des applications à développer
  - développer des applications
  - faire le support de niveau 2 (N2)
- Développeur "front-end"
  - Dessiner l'aspect graphique et le "layout" des applications web à développer
  - Développer les interfaces d'usager (UX) des applications à développer
  - Améliorer l'usage des applications

11.3 Numérisation des rapports des mission

- Analyste d'information
  - Diriger les travaux de numérisation des rapports à réaliser
  - Analyser les rapports et associer des métadonnées, rédiger le sommaire du rapport et les stocker dans le répertoire des rapports des missions
  - Gérer le répertoire des rapports de missions numérisés
  - Faire le *backup* du répertoire web

11.4 Chef de projet fonctionnel

- Chef/s de projets fonctionnels
  - Diriger les travaux d'élaboration des spécifications fonctionnelles
  - Collaborer dans l'élaboration des spécifications fonctionnelles
  - Valider les travaux de développement des applications

- Proposer des améliorations aux applications développées
- Servir d'interface entre les responsables fonctionnels et les équipes de développement

11.5 L'Éditeur du site web

- L'Éditeur de le site web.
  - responsable de valider, approuver et envoyer à publication les articles sur le site web de l'IGF
  - responsable du contenu à publier sur les réseaux sociaux sur Internet

11.6 Sécurité de l'information

(voir section 9 : Sécurité)

- Responsable de la Sécurité de l'Information
  - Il est le responsable de la sécurité de l'information et est aussi responsable de la mise en oeuvre des mesures de sécurité pour les systèmes et services d'information, et de l'organisation et de la préparation de la documentation réglementaire dans le domaine de la sécurité de l'information.
  - Il dépend directement du Chef de l'IGF
- Responsable du Service
  - Il est responsable des autorisations d'accès, et du traitement des données dans son service. Une personne peut être responsable de plus d'un service.
  - Ce rôle est assimilable à un responsable d'une unité fonctionnelle
- Responsable du Système d'Information
  - Il est responsable des autorisations d'accès, et du traitement des données dans son système d'information. Une personne peut être responsable de plus d'un système d'information.
  - Dans une première phase, le Responsable du Système d'information peut être le même que le Responsable du Service
- Administrateur du Système d'Information
  - Gère des autorisations d'accès et exécute des instructions, procédures et outils techniques désignés dans son système d'information. Une personne peut administrer plus d'un système d'information.
  - Cet administrateur peut être placé dans une unité fonctionnelle ou dans le service de TI
  - Dans une première phase, ce rôle peut être assimilable à celui d'administrateur de base des données
- Chef de Projet du Système d'Information
  - Donne la plus grande importance à la prise de conscience des personnes impliquées dans le processus et leurs responsables hiérarchiques afin qu'ils ne soient pas sources de risque pour la sécurité: ni l'ignorance, ni l'instructions inadéquates ou encore le manque d'organisation ou de coordination. Une personne peut être chef de projet de plus d'un système d'information.
  - Ce rôle peut être assimilable à celui de Chef de projet fonctionnel
- Développeur du Système d'Information
  - Agit dans l'environnement de développement, s'occupe des activités

identifiées par le chef de projet au cours des stades de développement. Une personne peut être développeur de plus d'un système d'information.
    - Ce rôle peut être assimilable à celui de Développeur web
- Responsable du Service TI
    - Il est responsable de la gestion et l'administration des ressources allouées, y compris du personnel, des équipements, des services et des applications. Une personne peut être responsable de plus d'un service TI.
    - Ce rôle peut être assimilable à celui de Directeur de la DMNI

12 SERVICES DE SOUTIEN ET MAINTENANCE

Les tâches des services de soutien et maintenance font partie intégrante de tout projet TI. Dans les différents cahiers des charges à publier, les clauses de soutien et maintenance doivent être incluses.
Cette section décrit les aspects à couvrir, en général, par les clauses de soutien et maintenance.

12.1 Caractéristiques de la garantie du matériel

Tout le matériel acquis dans un processus d'achat publié dans le cahier de charges doit inclure :

- Réponse de 4 heures, couverture 24x7.
- Diagnostic et support de problèmes à distance.
- Support matériel sur place, matériaux inclus.
- Options de niveau de service avec différentes fenêtres de couverture et temps de réponse.
- Travaux jusqu'à la fin.
- La gestion des cas de hiérarchisation (escalade).
- Accès aux informations et aux services de support électronique.

12.2 Caractéristiques de la garantie du logiciel

Toutes les licences de logiciels acquis dans un processus d'achat publié dans le cahier de charges doivent inclure :

- Au moins 1 an de mise à jour gratuite des versions principales et tous les correctifs fonctionnels et de sécurité publiés par le fabricant.
- Support d'incident à distance.
- Accès aux informations et aux services de support électronique.
- De manière alternative, il conviendra de considérer services de conseil en logiciels pour couvrir des éléments tels que :
    - Support logiciel sur site.
    - Formation technique.
    - Résolution des problèmes de configuration logicielle.
    - Résolution des problèmes d'intégration de logiciels avec d'autres produits.
    - Options de niveau de service avec différentes fenêtres de couverture et temps de réponse.

- La gestion des cas de hiérarchisation (escalade).

12.3 Installation et configuration de l'infrastructure

Toutes les installations de l'infrastructure et des services de configuration doivent inclure :

- Une planification détaillée des essais à effectuer.
- Un processus de réglage et de réajustement précis.
- Les tâches ci-dessous se tiendront jusqu'à ce que l'infrastructure ait été validée par le personnel de l'IGF.
- Une garantie de 6 mois après la date de validation sera appliquée par l'entrepreneur afin de résoudre les problèmes cachés en raison d'une configuration insuffisante.

13 LE CENTRE D'ASSISTANCE TECHNIQUE (HELPDESK)

Le Service TI de l'IGF établira une infrastructure organisationnelle et technique pour fournir de l'assistance technique aux usagers de l'IGF.

Le Service des TI nommera un Responsable du Centre d'assistance technique qui sera responsable de maintenir la qualité du service fourni aux usagers de l'IGF.

Une procédure sera établie pour définir les processus et actions de ce service d'assistance.

Le service sera organisé à trois niveaux d'assistance:

13.1 Premier Niveau: N1

C'est le service directement relié aux usagers.

Les usagers qui ont besoin d'assistance technique quant à l'utilisation des applications de l'IGF font état de dysfonctionnement, d'applications non accessibles, de problèmes avec les ordinateurs personnels…etc. Ils enregistreront un "ticket" d'incident en utilisant un formulaire publié dans l'Intranet.

L'usager recevra un courrier électronique avec son numéro de "ticket" d'incident et simultanément, les techniciens de support recevront à leur tour un courrier électronique avec la description de la demande du support.

Le service doit être supporté par une application *helpdesk*.

Le responsable du Centre d'assistance assignera l'incident à un technicien de support.

Ce technicien essaiera de résoudre le problème dans le plus court délai. Si le technicien résout le problème, il en informera l'usager par courrier électronique. Le technicien saisira dans l'application de helpdesk les actions entreprises pour régler le problème. Par contre, si le technicien n'a pas pu le résoudre, il devra rediriger le cas au deuxième niveau (N2).

13.2 Deuxième Niveau: N2

Le niveau 2 de support du Centre d'assistance est composé de tous les autres techniciens du Service TI: développeurs, ingénieurs, administrateurs de réseau, administrateurs des bases des données, etc...

Le responsable du Centre d'assistance assignera un technicien pour régler le problème.

Si le technicien parvient à résoudre le problème, il en informera l'usager par courrier électronique. Le technicien saisira aussitôt dans l'application helpdesk les actions entreprises pour régler le problème. Par contre, si le technicien n'a pas pu le résoudre, il devra rediriger le cas au troisième niveau (N3).

13.3 Troisième Niveau: N3

Le niveau 3 de support du Centre d'assistance est composé de tous les services de support et de maintenance fournis par des entreprises externes (voir section 12): garanties, contrat du support, service de maintenance, etc...

Le technicien de N2 assigné fera le suivi de l'incident. Une fois que le problème est résolu, il en informera à l'usager par courrier électronique. Le technicien saisira aussitôt dans l'application helpdesk les actions entreprises pour régler le problème.

13.4 Application pour la gestion des demandes

Pour la gestion du Centre d'assistance, il faut ajouter un logiciel permettant de faire le suivi des incidents afin de mesurer la qualité des services fournis.

Il existe plusieurs services professionnels et bon marché sur Internet que l'IGF pourrait obtenir; par exemple ZendDesk. Le problème réside dans le fait que l'accès à ces services passe par une connection Internet pour tous les usagers.

Il y a aussi un solution simple et gratuite que le Service des TI de l'IGF peut configurer:

1. Un formulaire dans l'Intranet
    - pour l'enregistrement des demandes pour les usagers
2. Configuration de service SMTP
    - pour des alertes via courrier électronique
3. Utiliser une feuille de calcul *Google Sheet* avec quelques configurations faciles
    - partagées pour les techniciens N1 et N2 du Centre d'assistance
    - les techniciens N1 et N2 du Centre d'assistance doivent avoir accès à Internet

14 PLAN DE FORMATION DES TI

Étant donné que le personnel des TI de la DMNI est réduit, il doit être multidisciplinaire et polyvalent.. Ils devront développer de nouveaux services et veiller au développement, à l'acquisition et à l'adaptation des logiciels utilisés pour l'implémentation du matériel et des réseaux.

Cette équipe du personnel TI devrait maîtriser notamment les activités suivantes :

- Travail d'orientations des projets avec des processus et des méthodes standards.
- Développer des logiciels pour la mise en application de prestations, processus, produits et pilotages dans toutes les branches de l'IGF.
- Il faut tenir compte que les informaticiens tombent souvent sur des informations confidentielles et des secrets d'entreprise, et ont des accès illimités à des données sensibles. Par conséquent, ils doivent être dignes de confiance.
- Mettre en service de nouveaux appareils, vérifier les nouvelles versions de logiciels qui se présentent, et les introduire dans l'IGF.
- Surveiller les serveurs et processus.
- Assurer le support aux utilisateurs et surveiller la sécurité d'exploitation. A cet effet, ils doivent suivre très attentivement l'évolution des problèmes, les résoudre et proposer des solutions, démontrer aux utilisateurs comment fonctionne une nouvelle application.

La complexité des systèmes et le haut niveau d'exigences pour une exploitation sans interruption représentent un grand défi pour les compétences des professionnels. Ayant une relation directe avec les utilisateurs et autres professionnels, il leur est demandé de posséder également de très bonnes compétences sociales.

Les informaticiens de la DMNI doivent être formés sur toute la largeur des domaines informatiques, toutefois avec une profondeur moins prononcée que le personnel technique spécialisé. Ils peuvent être engagés dans divers domaines comme la technique des systèmes, le développement d'applications ou encore, dans l'exploitation. Ils doivent s'occuper de l'implémentation des systèmes, de la programmation et de l'exploitation des TI.

Les objectifs de formation peuvent être subdivisés comme suit :

1. Mise en service d'appareils TI.
    a. Évaluer et mettre en service une place de travail pour l'utilisateur.
    b. Installer et synchroniser sur le réseau interne des postes des utilisateurs.
    c. Connecter et configurer des appareils périphériques.
2. Mise en service, maintenance de services de serveurs et de réseaux
    a. Mettre en service des systèmes serveurs. Virtualisés et physiques.
    b. Installer des réseaux et leurs topologies.
    c. Élaborer et mettre en œuvre des concepts de sécurité des données, de sécurité des systèmes, et d'archivage.
3. Garantie de l'exploitation TI.
    a. Assurer la maintenance des réseaux et les développer.
    b. Assurer la maintenance et administrer des serveurs.
    c. Planifier, mettre en œuvre des services d'annuaires et des autorisations.
4. Assistance aux utilisateurs.

   a. Instruire et aider les utilisateurs dans l'utilisation des moyens informatiques.
   b. Assurer des tâches de support par le biais du contact client et résoudre les problèmes sur place.
5. Développement d'applications en tenant compte des caractéristiques de qualité.
   a. Développer et documenter des applications de manière conviviale en utilisant des modèles appropriés de déroulement.
   b. Développer et implémenter des interfaces utilisateurs pour des applications selon les besoins du client.
   c. Élaborer des concepts de tests, mettre en application divers déroulements de tests et tester systématiquement les applications.
6. Travaux dans le cadre de projets.
   a. Préparer, structurer, exécuter et documenter des travaux et des mandats de manière systématique et efficace.
   b. Collaborer à des projets.
   c. Dans le cadre de projets, communiquer de manière ciblée et adaptée à l'interlocuteur.

Bien que cela dépendra entièrement des technologies choisies pour mettre en œuvre des systèmes d'information, on va supposer que les hypothèses suivantes soient acceptées par l'IGF :

1. L'utilisation des logiciels gratuits sera encouragée.
2. La technologie de virtualisation sera utilisée.

Voici une liste récapitulative des cours possibles à inclure dans une formation technique qui couvre les objectifs décrites ci-dessus. (Dans la section sur la formation du personnel en matière des systèmes TI, des recommandations de logiciels ont été ajoutées).

1. Pour le personnel des systèmes TI.
   a. Installation de matériels, configuration et maintenance. Serveurs physiques, pare-feux, commutateurs, HBAs, etc.
   b. Installation et configuration du logiciel de virtualisation.
      i. VMware vSphere Hypervisor ESXi
   c. Installation et configuration des serveurs DNS.
      i. BIND
   d. Installation et configuration des serveurs WEB.
      i. Apache HTTP Server
   e. Installation et configuration des systèmes d'exploitation.
      i. Microsoft Windows
   f. Installation du logiciel de base de données.
      i. MySQL (ou MariaDB)
   g. Installation du système de gestion de contenu.
      i. WordPress
   h. Installation et maintenance d'un système de contrôle de version.
      i. Apache Subversion
   i. Installation et maintenance des services d'annuaire, DHCP, File Server etc.
      i. Microsoft Windows.
2. Pour le personnel de développement.
   a. Programmation orientée objet
   b. Modèle MVC
   c. Langage SQL

   d. Services Web
   e. PHP
   f. HTML5
   g. CSS3
   h. JavaScript et jQuery
   i. XML et JSON
   j. AJAX
3. Pour le personnel en charge des portails Internet et Intranet.
   a. Gestion des médias (bibliothèque), gestion de liens de téléchargements, publication de contenus, gestion des pages du site, gestion des formulaires sous WordPress.
   b. Les rôles dans WordPress : l'éditeur, l'auteur, le contributeur et l'abonné.

Il faut ajouter que l'acquisition de compétences professionnelles n'est qu'une partie de l'apprentissage moderne. Au moins dans l'environnement de la fonction publique, il s'agit de développer un comportement et une éthique professionnelle. Lors des enquêtes sur le champ professionnel des TI, ce sont la flexibilité, la créativité, les capacités de communication et de coopération, les capacités pour solutionner les problèmes et la capacité de décisions, la responsabilité personnelle, la pensée en réseau, l'orientation client, qui ont été plébiscitées et citées avec une signification croissante.

14.1 Formation on-line

Il faut souligner que l'IGF peut prendre en considération la vaste offre des cours en ligne pour former ses effectifs et surtout ceux du Service des TI.

En général, une grande partie de ces cours sont animés en anglais. Les développeurs et techniciens des systèmes, en général, doivent détenir une connaissance intermédiaire de cette lingua-franca pour les technologies. Néanmoins, sont aussi offerts des cours en français et en arabe sur Internet.

Il existe beaucoup des cours gratuits. Pour autant, ceux qui ne le sont pas sont en général assez bon marché.

Pour la codification

- HTML5rocks: https://www.html5rocks.com/
  - HTML5 nouveautés.
- CodeAcademy: https://www.codecademy.com/
  - javascript, php, html5, css3,...
- KhanAcademy: https://www.khanacademy.org/
  - … plus SQL, MySQL,...
- Udacity: https://www.udacity.com/
  - ...plus MVC, data analysis, …
- Edx: https://www.edx.org/
  - ...plus front-end développeur, cybersecurity,...

Pour la technique des systèmes

- Udemy: https://www.udemy.com
  - … plus windows server, dns, dhcp, active directory,..

Pour le CMS (Wordpress)

- WebBeginner: http://www.wpbeginner.com/
- Lynda: https://www.lynda.com/
- Udemy: https://www.udemy.com

15 RELATIONS DES APPLICATIONS, SERVICES ET SYSTÈMES D'INFORMATION

La relation des applications "métier" à développer par l'IGF est la suivante:

15.1 Base de données des entités ciblées (BDE)

La base de données des entités constitue le centre du système d'information de l'IGF, elle recense de manière exhaustive et permanente les entités couvertes dans le périmètre d'intervention de l'IGF, qu'elles soient de la sphère économique ou administrative.

Outre le recensement, la base de données collecte les différentes informations relatives aux entités, à l'instar des informations organisationnelles, juridiques, budgétaires et financières. Elle intègre, aussi, les informations relatives à l'évaluation du contrôle interne des entités grâce aux résultats des missions précédentes de l'IGF, ainsi que la cartographie des risques des entités, lorsque celle-ci existe.

La base de données des entités forme un support important à l'IGF du fait qu'elle permet l'accès aux informations de manière informatisée et sécurisée entre les différents intervenants de l'IGF, contribuant, ainsi, à l'amélioration de la préparation des missions, tant au niveau décisionnel qu'au niveau opérationnel.

En effet, le niveau décisionnel bénéficie des informations nécessaires à l'élaboration du plan annuel d'audit ainsi que le suivi des missions, avec autant d'indicateurs paramétrables que possible, ce qui contribue à l'enrichissement des critères de décisions de l'IGF.

Alors que les unités opérationnelles bénéficient des informations nécessaires à la préparation et au déroulement de leurs missions de manière instantanée, elles permettent l'amélioration de l'efficacité des missions à travers le gain de temps et la focalisation sur les travaux d'audit.

L'importance de la base de données des entités fait d'elle qu'elle forme la source d'information principale des autres modules/applications de l'IGF, notamment ceux relatifs au ;

1. Plan annuel d'audit ;
2. Logiciel de suivi des missions ;
3. Intranet.

15.2 Evolution du Logiciel de Suivi des Missions (SM2)

La DMNI (Direction des Méthodes, de Normalisation et de l'Informatique) a développé le Logiciel de Suivi de Missions (LSM), sous forme d'une application Windows (technologie client-serveur), ayant comme objectif le suivi de l'état d'avancement des missions de l'IGF.

Le logiciel LSM est opérationnel mais se trouve dans un état expérimental. Il est utilisé par les Directeurs de Mission, le secrétariat des CGF, la DPAS et le secrétariat du Chef de l'IGF (environ 20 utilisateurs). L'accès est exclusif au réseau interne du Ministère (en incluant aussi les Inspections Régionales liées avec une connexion VPN).

Après des discussions avec les différents acteurs du système (personnel de la DMNI, personnel de la DPAS, un Directeur de Mission, un Chef d'Inspection et un Contrôleur

Général des finances), en analysant les besoins de chacun, on a préparé une proposition d'évolution du logiciel existant en ajoutant des nouvelles fonctionnalités, détaillées dans l'annexe "Évolution du Logiciel de Suivi des Missions".

Il est prévu de faire une évolution technologique du développement actuel (vers une architecture Web trois tiers) ainsi qu'une évolution des fonctionnalités actuelles pour moderniser le traitement actuel et l'orienter vers un traitement dématérialisé.

La documentation des missions sera stockée en format numérique dans l'application (en spécial des fichiers en format éditable avec les différents versions des rapports de mission). En conséquence, on pourra offrir la possibilité d'un accès en-ligne aux rapports, avec un moteur de recherche implanté sur le logiciel pour trouver des rapports en saisissant le nom de l'entité, le secteur, les dates, etc.

La gestion du suivi de mission sera totalement dématérialisé. On évitera la circulation de documentation en papier en parallèle (comme la fiche de suivi), on saisira ce type d'information sur des champs spécifiques sur le logiciel qui seront donc stockées pour en faciliter l'exploitation statistique, la gestion automatique des alertes et la programmation de tableaux de bord.

15.3 Module pour la génération du plan annuel des missions de l'IGF (PAM)

Le Plan Annuel d'Audit de l'IGF est soumis à une procédure à laquelle participent plusieurs intervenants, et qui est structurée en différentes phases. Le présent document a pour but de proposer les spécifications fonctionnelles pour le développement d'un logiciel (exposées à l'Annexe IV: Génération du plan annuel des missions de l'IGF), permettant de gérer et coordonner l'ensemble des processus qui, finalement, se matérialisent dans le plan.

Ce projet devrait servir de cadre pour automatiser la plupart des procédures, compte tenu des flux de documentation et des différents niveaux de responsabilité des intervenants, avec l'objectif final de rationaliser les processus au moyen de l'exécution d'opérations à travers un système d'information.

La principale source d'information du logiciel est la base de données d'entités, c'est pour cela que ce projet établit une connexion fondamentale entre les deux éléments. D'un autre côté, le résultat final généré par ce logiciel, le plan annuel d'audit, est le point de départ pour le logiciel de suivi des missions.

Le logiciel est conçu comme un système intégré, dans un environnement de type web, composé de trois modules distincts mais complémentaires:

- **MODULE 1: SÉLECTION DE L'ÉCHANTILLON D'ENTITÉS.** Ce module disposera d'une fonctionnalité pour la sélection d'une population cible, plus réduite, qui peut être configurée à partir des critères stratégiques, et qui permettra de définir des différents scénarios selon les critères choisis.
  Après l'emploi de critères stratégiques, on peut appliquer des critères statistiques pour obtenir un échantillon représentatif du scénario choisi. Cela pourrait se faire en utilisant l'échantillonnage aléatoire simple, mais pour avoir un échantillon qui soit plus représentatif de la population cible (scénario), il est recommandé d'utiliser un échantillonnage aléatoire stratifié.
- **MODULE 2: GESTION DU PROJET DE PROGRAMME ANNUEL**. L'objectif de ce module est de mettre en place un système pour gérer les différentes phases de

l'élaboration du programme. C'est un module dynamique, qui informe les utilisateurs (au moyen d'un email) lorsqu'ils doivent faire une révision de la documentation. La documentation est toujours traitée en format numérique.

- **MODULE 3: RÉPARTITION DU PROGRAMME APPROUVÉ PAR LE MINISTRE.** L'objectif de ce module est de mettre à disposition des responsables des structures opérationnelles leur partie du programme, afin qu'ils puissent la télécharger et l'exécuter.

15.4 Répertoire historique des rapports d'audit

Cette section n'est pas une application mais renferme des recommandations pour le traitement des rapport de missions anciennes.

La première recommandation pour l'IGF est de commencer le plus tôt possible à établir le rapport de mission numérique comme le rapport par défaut.

Même si l'application Suivi de Missions v2 plus la BDE, ne sont pas encore développées, l'IGF doit stocker les rapports des missions, a partir de 2018, dans un format électronique, par exemple, dans un serveur de fichiers. La DPAS peut être la responsable de ce répertoire électronique.

Par rapport à la numérisation des anciens rapports de missions, la recommandation que nous faisons est de numériser les rapports des deux dernières années, à savoir 2016 et 2017. Ces rapports seront stockés dans le répertoire mentionné ci-dessus.

Ainsi, chaque fois qu'un inspecteur demande à consulter un rapport de mission, ce rapport devra avoir été numérisé et stocké dans le répertoire.

15.5 L'Intranet de l'IGF

L'Intranet est le point d'accès des employés de l'IGF à leur organisation.

Les sections à inclure dans la première version de cette plateforme sont les suivantes:

- Accueil
  - Il s'agit de la page principale de l'intranet.
- Accès à la législation
  - Il y sera aussi possible d'accéder à toute la législation (lois, ordonnances, avis et instruction, différents codes…) que l'Éditeur Intranet pense être d'utilité pour les inspecteurs, y compris les Réglementations et Actes administratifs internes
- Le Guide de fonctionnement de l'organisation
  - Le guide de fonctionnement est la compilation de toute l'information pertinente pour les inspecteurs qui leur permet de réaliser leur travail et de mener leurs interventions. Ce guide est décliné en plusieurs chapitres/sections qui se présentent comme suit :
  - Le Manuel d'Organisation
  - Le Manuel d'Intervention de l'IGF et guides spécifiques
  - Le Code de déontologie
- Les Comités de travail de l'IGF

- Cette section présentera les travaux d'amélioration, de normalisation et d'adaptation aux normes internationales des différents Comités de travail de l'IGF.

- Modèles de documents de travail
  - Le système d'information de l'IGF doit inclure un nombre important de documents indispensables au bon déroulement des missions et à l'amélioration de la communication au sein de l'institution.
- Rapports de l'IGF
  - Les rapports de missions ne seront pas accessibles directement via l'intranet. Elle le seront plutôt à travers des applications SI (BDE, Suivi,...).
  - Pour les autres rapports, l'Intranet présentera une description sous forme de texte et offrira la possibilité de télécharger le rapport. Seront aussi présents les rapports de toutes les années précédentes:
    - Rapports annuels
    - Rapports spéciaux (dans ce cas, des mesures de sécurité additionnelles seront mises en vigueur)
    - Autres types de rapports publiés par l'IGF
    - Statistiques et bilans d'activités
- Formation:
  - L'information suivante sera primordiale et susceptible d'être publiée :
    - Plans de formation (annuels et pluriannuels)
    - Formulaire pour la proposition de thèmes
    - Formulaire pour les demandes de participation à des sessions de formation
    - Calendrier des activités de formations
    - Offres de formations à l'étranger.
- Nouvelles
  - Cet élément offrira un grand dynamisme au site.
  - L'Éditeur et/ou le Webmaster devront publier articles portant sur les événements, collaborations, assises, séminaires, réunions du conseil de direction, informations sur les projets de l'IGF, appels à candidatures, appels d'offres, instructions de l'IGF, notes de services, annonces sur des oeuvres sociales .
  - La date de publication et l'auteur seront toujours mentionnés. Il serait aussi important que des catégories et des "tags" puissent paraître pour permettre de mieux classifier l'article.
- Calendrier des événements
- Forum de l'inspecteur
- RRHH - Gestion de carrière.
  - Dans cette première phase, il n'y aura pas de connection directe avec les systèmes de la DAM. L'Éditeur Intranet devra d'abord obtenir l'information nécessaire de manière hors ligne, pour la publier ensuite dans l'Intranet en format HTML ou PDF. L'information suivante sera importante et susceptible d'être publiée :
  - Répertoire des employés de l'IGF (adresse email et n° de téléphone).
  - Dossiers administratifs du personnel de l'IGF (PV d'installation ; Arrêté de nomination ; Arrêté de détachement ; Décisions d'intérim….etc.) (accès

limité)
    - Situation des inspecteurs (par division/ par inspection régionale) (accès limité)
    - Promotion (passage de grade, échelons….) (accès limité)
    - Information d'ordre normatif (accès libre)
- Accès aux systèmes d'information
    - Catalogue des SI
        - Sera présenté ici un catalogue (par exemple) contenant une ligne dédiée à chaque système d'information disponible à l'IGF.
    - Accès au BDE
        - Connection via la Base des données des entités.
    - Accès au suivi des missions
    - Accès au Programme d'intervention annuel (accès limité selon type d'usager).
- Accès au Centre d'assistance technique. Contact.
- Sitemap - Plan de site

15.6 Site Web de l'IGF[3]

Élaborer un espace web dédié à une organisation régalienne telle que l'IGF est une étape importante du développement de nouvelles capacités d'action et de communication de l'administration publique. Ce document a pour but de spécifier les paramètres entourant le lancement du site web de l'IGF tout en veillant à proposer différentes hypothèses, notamment en ce qui a trait à la nature du domaine qui sera privilégiée ainsi qu'à la maintenance du site avec, par exemple, la possibilité de contracter des services externes.

Ce document se veut aussi un ensemble de recommandations qui devraient être prises en compte en amont du lancement de la page web eu égard à la particularité du statut public de l'IGF, ainsi qu'un résumé des différentes caractéristiques techniques et de design qui devraient s'y retrouver. Ainsi, la finalité de ce processus est de doter l'institution de l'IGF d'un nouvel instrument de rayonnement sur internet tant dans une perspective classique (site web) que moderne avec les nouvelles applications liées aux réseaux sociaux.

15.6.1 Scénarios: Décisions que l'IGF doit prendre

Publier un site web est une décision des plus plus importantes, surtout dans la phase de lancement et particulièrement au niveau du choix du nom du domaine. Ce dernier constitue en effet la principale fenêtre d'accès pour les navigateurs et doit en ce sens pouvoir être distinguable aisément.

Dans le diagramme suivant, nous posons deux questions :

1. Est ce-qu'on peut avoir un nom de domaine different de celui du MdF (mf.gov.dz) ?
2. Est ce-qu'on peut avoir un sous-domaine au sein du domaine du MdF (igf.mf.gov.dz) ?

[3] La version complète de la spécification fonctionnelle du site web de l'IGF est accessible à: https://docs.google.com/document/d/1p5L6Fzs7UjsBy_BxJzf4BWmyprl_oXDuhslRQHdDL_0/edit

Si la réponse à l'une de ces questions est affirmative, nous émettons les recommandations suivantes :

- Utiliser un fournisseur Internet pour l'hébergement du site web
- Utiliser un cabinet de communication pour le dessin, la construction ainsi que pour la mise à jour du site
- L'Éditeur Web enverra au cabinet le document portant sur les spécifications fonctionnelles pour transmettre les orientations concernant la phase du dessin du site. Dans cette première phase, l'Éditeur Web enverra le contenu initial à publier dans la version 1.0.
- L'Éditeur Web enverra par la suite au cabinet, de manière périodique, les articles à publier

Si les deux réponses sont négatives, Il est plutôt recommandé de :

- Utiliser les services de l'unité responsable de la mise à jour du site du MdF
- Veiller à ce que l'Éditeur Web envoie les articles, de manière périodique, audit responsable avec un format préalablement convenu.

16 PLANIFICATION-FEUILLE DE ROUTE

Cette section a pour objectif de servir comme référence aux responsables de l'IGF pour leur permettre d'envisager la relation de projets à mettre en marche avec un calendrier qualitatif/estimatif.

16.1 Relation des projets

16.1.1 Adaptation de la nouvelle salle d'ordinateurs

Objectif: Mise en marche de la nouvelle salle d'ordinateurs pour héberger l'infrastructure TI de l'IGF.
Code: **SALLE**

Sous-tâche	Description	Responsable	Remarques
Specs fonctionnelles	Définir les exigences et caractéristiques de cette salle d'ordinateurs qui hébergera la nouvelle infrastructure TI PRO et PRE	DMNI	Aide externe: Ingénieur des systèmes de la DSI
Adéquation	Travaux pour la mise en adaptation de la salle	DAM/DMNI	
Sécurité	Incorporer mesures de sécurité définies dans les specs fonctionnelles et supervisées par le responsable de la sécurité de l'information	Cabinet externe/RSI/DMNI	Aide externe: Cabinet spécialisé
Réseau	Interconnection au LAN du MdF et de l'IGF	DSI/DMNI	Aide externe: Ingénieur des systèmes de la DSI

16.1.2 Mise à jour des services de réseau (*network services*) de l'IGF

Objectif: Mise en marche l'infrastructure TI de base pour faciliter aux usagers l'accès facile et quotidien aux applications.
Code: **NETWORK**

Sous-tâche	Description	Responsable	Remarques
Diagnostic	Diagnostic de la situation actuelle des services de réseau (*network services*) que la DMNI offre à l'IGF	DMNI	Aide externe: Ingénieur des systèmes

Documentation	Faire la documentation détaillée de la configuration des services de réseau	DMNI	
Configuration des services de réseau	Plan IP, DHCP, DNS, SMTP, NTP, Domain (AD), Windows Server 20xx server, serveur des fichiers, ...	DMNI	Aide externe: Ingénieur des systèmes
Serveur de réseau	Mise en marche du Serveur Réseau	DMNI	Acheter Serveur (appel d'offre DEV)
PC's	Poste de travail: (Re) Configuration des postes de travail pour l'accès facile et prédictif aux services de réseau	DMNI	

16.1.3 Mise en oeuvre du service de support (HelpDesk) à la DMNI

Objectif: Mise en oeuvre d'un service à l'intention des usagers de l'IGF par rapport aux systèmes d'information: Centre d'assistance technique
Code: **HELPDESK**

Sous-tâche	Description	Responsable	Remarques
Procédure	Définir et documenter une procédure qui décrit les processus et fonctionnement de ce Centre d'assistance technique	DMNI	
Formulaire	Configurer un formulaire dans l'Intranet pour que les usagers puissent demander support. Configurer des alertes via courrier électronique	DMNI	
Suivi	Configurer une application de suivi des demandes d'assistance interconnecté avec le formulaire de l'intranet. Elaborer une procédure de suivi des demandes	DMNI	
Formation	Formation au personnel de la DMNI sur l'application de suivi des demandes d'assistance	DMNI	

16.1.4 Mise en oeuvre l'environnement DEV

Objectif: Mise en oeuvre l'environnement DEV (infrastructure pour le développement à la DMNI).
Code: **DEV**

Sous-tâche	Description	Responsable	Remarques
Appel d'offre	Préparer une appel d'offres pour l'acquisition du matériel et du logiciel pour l'environnement de développement (DEV)	DAM/DMNI	
DEV: faire l'analyse et le dessin de la solution finale	Avec la participation du fournisseur externe, analyser et dessiner l'architecture TI de l'environnement de production de l'IGF	DMNI	
DEV: Install & Config	Installation et configuration de l'environnement DEV (serveur physique, machine virtuelle, serveur web (Apache), moteur PHP, serveur de base des données (MySQL),...)	DMNI	Le processus doit être documenté Aide externe: Ingénieur des systèmes
Documentation	Le processus doit être documenté pour faciliter la tâche de support de l'infrastructure	DMNI	
Contrôle de versions	Installer un système de contrôle de versions	DMNI	Par exemple Subversion
Wiki collaboratif	Installer un système wiki collaboratif pour les travaux de développement	DMNI	Par exemple Redmine
DEV Poste	Définir et configurer un poste PC de travail pour un développeur standard	DMNI	

16.1.5 Mise en oeuvre de l'environnement PRO

Objectif: Mise en oeuvre de l'environnement PRO: infrastructure des productions des applications de l'IGF.
Code: **PRO**

Sous-tâche	Description	Responsable	Remarques
Appel d'offres	Préparer une appel d'offres pour l'acquisition du matériel, logiciel et services pour l'environnement de production (PRO)	DAM/DMNI	
PRO: faire l'analyse et le dessin de la solution finale	Avec la participation du fournisseur externe, analyser et dessiner l'architecture TI de l'environnement de production de l'IGF	DMNI	Avec la participation des techniciens du fournisseur externe
PRO: Install & Config	Installation et configuration de l'environnement PRO (serveurs physiques, machines virtuelles, Intégration avec les services de réseau, serveur web (Apache), moteur PHP, serveur de base des données (MySQL),...)	DMNI	Le processus doit être documenté avec la participation des techniciens du fournisseur externe
Documentation	Le processus doit être documenté pour faciliter la tâche de support de l'infrastructure	DMNI	
Procédure	Définir une procédure pour déployer des applications à l'environnement de production	DMNI	Avec la participation des techniciens du fournisseur externe

16.1.6 Mise en oeuvre de l'environnement PRE

Objectif: Mise en marche l'environnement PRE: infrastructure de pré-production des applications de l'IGF.
Code: **PRE**

Sous-tâche	Description	Responsable	Remarques
Appel d'offres	Préparer une appel d'offres pour l'acquisition du matériel, du logiciel et des services pour l'environnement de production (PRE)	DAM/DMNI	
PRE: faire l'analyse et le dessin de la solution finale	Avec la participation du fournisseur externe, analyser et dessiner l'architecture TI de l'environnement de production de l'IGF	DMNI	Avec la participation des techniciens du fournisseur externe

PRE: Install & Config	Installation et configuration de l'environnement PRE (serveurs physiques, machines virtuelles, Intégration avec les services de réseau, serveur web (Apache), moteur PHP, serveur de base des données (MySQL) outils, ,...)	DMNI	
Documentation	Le processus doit être documenté pour faciliter la tâche de support de l'infrastructure	DMNI	
Procédure de déploiement des applications	Définir les procédures de déploiement des applications (DEV->PRE->PRO)	DMNI	Documenter et publier dans l'intranet

16.1.7 Gérer les mesures de sauvegarde

Objectif: Mise en marche du processus de sauvegarde . Assurance de la pérennité des données (systèmes, applications, base des données, documentation) selon un calendrier défini.
Code: **BACKUP**

Sous-tâche	Description	Responsable	Remarques
Procédure de sauvegarde	Définir les besoins de stockage des données de sauvegarde sur le site et hors site qui répondent aux exigences d'affaires	DAM/DMNI	Aide externe: Possible participation externe d'un analyste des systèmes
Appel d'offres	Achat d'équipements pour sauvegarder des données	DAM/DMNI	Inclus dans l'appel d'offres de PRO
Backup Install & Config	Installer et configurer les dispositifs de sauvegarde	DMNI	
Implantation et tests	Implantation d'un système de sauvegarde avec la mise en marche de tests pour actualiser de façon périodique les données archivées et les données sauvegardées.	RSI/DMNI	Aide externe: Possible participation externe d'un analyste des données

16.1.8 Formation des effectifs de la DMNI

Objectif: Renforcer la structure technique du Service des TI de l'IGF.
Code: **FORMATION**

Sous-tâche	Description	Responsable	Remarques
Plan de formation TI	Elaborer un Plan de formation TI pour les effectifs de la DMNI qui leur permettra de renforcer leurs capacités techniques	DAM/DMNI	Le plan de formation peut utiliser des systèmes de formation on-line disponibles sur internet. De manière complémentaire, une formation en présentiel sera mise en oeuvre
Exécution du Plan de formation TI	Exécuter le Plan de formation TI	DMNI	Les participants seront évalués

16.1.9 Accord d'échange de données avec des organisations publiques

Objectif: Signer des accords avec de fournisseurs publics d'informations.
Code: **ACCORDS**

Sous-tâche	Description	Responsable	Remarques
Accord avec l'ONS	Arriver à un accord de collaboration avec l'ONS pour les échanges des données avec la base des données des entités de l'IGF (BDE)	Le Chef de l'IGF/CG's	L'accord doit inclure des annexes avec la précision des données à échanger
Accord avec la CNRC	Arriver à un accord de collaboration avec la CNRC pour les échanges des données avec la base des données des entités de l'IGF (BDE)	Le Chef de l'IGF/CG's	L'accord doit inclure des annexes avec la précision des données à échanger et la périodicité des échanges
Accord avec	Arriver à un accord de	Le Chef de	L'accord doit inclure

la DGI	collaboration avec la DGI pour les échanges de données avec la base des données des entités de l'IGF (BDE)	l'IGF/CG's	des annexes avec la précisions des données à échanger et la périodicité des échanges
Accord avec la DGB	Arriver à un accord de collaboration avec la DGB pour les échanges de données avec la base des données des entités de l'IGF (BDE)	Le Chef de l'IGF/CG's	L'accord doit inclure des annexes avec la précision des données à échanger et la périodicité des échanges
Accord avec la DGC	Arriver à un accord de collaboration avec la DGC pour les échanges des données avec la base de données des entités de l'IGF (BDE)	Le Chef de l'IGF/CG's	L'accord doit inclure des annexes avec la précisions des données à échanger et la périodicité des échanges
Accord avec la DGD	Arriver à un accord de collaboration avec la DGD pour les échanges des données avec la base des données des entités de l'IGF (BDE)	Le Chef de l'IGF/CG's	L'accord doit inclure des annexes avec la précisions des donnés à échanger et la périodicité des échanges

16.1.10 Analyse des données du périmètre

Objectif: Analyser et adapter les données reçues des organisations externes Code: **ANALYSE**			
Sous-tâche	Description	Responsable	Remarques
Définir un modèle d'architecture de l'information	Maintenir un dictionnaire de données d'entreprise qui favorise une compréhension commune et un système de classification qui comprend des détails sur la propriété des données, la définition des niveaux de sécurité appropriés, ainsi que la conservation des données et les exigences en matière de destruction.	DMNI/Chefs de projets	Aide externe: Possible participation externe d'un analyste des données
Analyse des	Analyse des données échangées	DMNI/Chefs de	Aide externe:

données échangés	avec des organisation externes. L'objectif principal est d'adapter l'information reçue au format du modèle des données de la BDE. Et de raffiner et donner de la qualité à l'information stockée	projets	Possible participation externe d'un analyste des données

16.1.11 Mise en marche de l'Intranet de l'IGF

Objectif: Mise en marche l'Intranet de l'IGF.			
Sous-tâche	Description	Responsable	Remarques
Specs fonctionnelles	Elaboration des spécifications fonctionnelles finales	Chef de projet fonctionnel/Editeur Intranet/Web master	
Intégration	Installer et intégrer la plateforme Intranet sur les systèmes de la DMNI en utilisant les services de réseau existants.	DMNI	Le processus doit être documenté
Formation	Former à l'Éditeur Intranet et au Webmaster dans le CMS	Éditeur Intranet/Web master	
Configurer le CMS	Selon les directives du document Specs fonctionnelles de l'Intranet configurer le CMS	Éditeur Intranet/Web master	
Ramasser des informations à publier	Les unités fonctionnelles doivent remettre l'information à publier à l'Éditeur/Webmaster	Éditeur Intranet/Web master Responsables des unités fonctionnelles	

16.1.12 Développer la base de données des entités (BDE)

Objectif: Mise en marche la BDE de l'IGF. Code: **BDE**			
Sous-tâche	Description	Responsable	Remarques

Specs fonctionnelles	Élaboration des spécifications fonctionnelles finales	Chef de projet/DMNI	
Appel d'offres	Obtenir des services professionnels pour le développement de la BDE	DAM/Chef de projet/DMNI	Inclus dans l'appel d'offres de développement des applications de l'IGF (BDE+SM2+PAM)
Gestion du projet	Définir l'organisation et les responsabilités dans la gestion du projet	Chef de projet/DMNI	
Planning	Définir la planification détaillée des tâches à réaliser	Chef de projet/Fournisseur externe/DMNI	
Dessin	Faire le dessin technique de l'application BDE (modèle des données, case d'usage, UML, catalog de classes, API, …)	Fournisseur externe/DMNI	
Documentation	Toutes les phases doivent être bien documentées	Fournisseur externe/DMNI	
Suivi de projet	Faire le suivi et gestion de projet	Chef de projet/DMNI	
Validation partielle	Valider des versions intermédiaires	Chef de projet/Fournisseur externe/DMNI	
Testing	Faire les tests pour vérifier le fonctionnement adéquat des versions livrées	Fournisseur externe/DMNI	
Validation finale	Valider la rémission de la version finale de la BDE	Chefs de projets/Fournisseur externe/DMNI	
Mise en production	Mise en production de la version 1.0 de la BDE	Fournisseur externe/DMNI	
Testing	Faire les tests pour vérifier le fonctionnement adéquat de la version dans l'environnement	Fournisseur externe/DMNI	

	PRO		

16.1.13 Développer l'application Suivi de missions (SM2)

Objectif: Mis en marche de l'application de suivi des missions de l'IGF (SM2).
Code: **SM2**

Sous-tâche	Description	Responsable	Remarques
Specs fonctionnelles	Élaboration des spécifications fonctionnelles finales	Chef de projet/DMNI	
Appel d'offres	Obtenir des services professionnels pour le développement de la SM2	DAM/Chef de projet/DMNI	Inclus dans l'appel d'offre de développement des applications de l'IGF (BDE+SM2+PAM)
Gestion du projet	Définir l'organisation et les responsabilités dans la gestion du projet	Chef de projet/DMNI	
Planning	Définir la planification détaillée des tâches à réaliser	Chef de projet/Fournisseur externe/DMNI	
Dessin	Faire le dessin technique de l'application SM2 (modèle des données, case d'usage, UML, catalog de classes, API, …)	Fournisseur externe/DMNI	
Documentation	Toutes les phases doivent être bien documentées	Fournisseur externe/DMNI	
Suivi de projet	Faire le suivi et a gestion de projet	Chef de projet/DMNI	
Validation partielle	Valider des versions intermédiaires	Chef de projet/Fournisseur externe/DMNI	
Intégration BDE	Intégrer les versions intermédiaires avec la BDE	Fournisseur externe/DMNI	

Testing	Faire les tests pour vérifier le fonctionnement adéquat des versions livrées. Tester aussi l'intégration avec la BDE	Fournisseur externe/DMNI	
Validation finale	Valider la rémission de la version finale de la SM2	Chef de projets/Fournisseur externe/DMNI	
Mise en production	Mise en production de la version 1.0 de la SM2	Fournisseur externe/DMNI	
Testing	Faire les tests pour vérifier le fonctionnement adéquat de la version dans l'environnement PRO (BDE+SM2)	Fournisseur externe/DMNI	

16.1.14 Développer le module PAM

Objectif: Mise en marche du module PAM de l'IGF.
Code: **PAM**

Sous-tâche	Description	Responsable	Remarques
Specs fonctionnelles	Élaboration des spécifications fonctionnelles finales	Chef de projet/DMNI	
Appel d'offres	Obtenir des services professionnels pour le développement du module PAM	DAM/Chef de projet/DMNI	Inclus dans l'appel d'offres du développement des applications de l'IGF (BDE+SM2+PAM)
Gestion du projet	Définir l'organisation et les responsabilités dans la gestion du projet	Chef de projet/DMNI	
Planning	Définir de la planification détaillée des tâches à réaliser	Chef de projet/Fournisseur externe/DMNI	
Dessin	Faire le dessin technique de l'application PAM (modèle des données, case d'usage, UML, catalog de classes, API, …)	Fournisseur externe/DMNI	

Documentation	Toutes les phases doivent être bien documentées	Fournisseur externe/DMNI	
Suivi de projet	Faire le suivi et la gestion de projet	Chef de projet/DMNI	
Validation partielle	Valider des versions intermédiaires	Chef de projet/Fournisseur externe/DMNI	
Intégration BDE+SM2	Intégrer les versions intermédiaires avec la BDE et SM2	Fournisseur externe/DMNI	
Testing	Faire les tests pour vérifier le fonctionnement adéquat des versions livrées. Tester aussi l'intégration avec la BDE+SM2	Fournisseur externe/DMNI	
Validation finale	Valider la rémission de la version finale de la PAM	Chef de projet/Fournisseur externe/DMNI	
Mise en production	Mise en production de la version 1.0 de la BDE+SM2+PAM	Fournisseur externe/DMNI	

16.1.15 Publication du site web de l'IGF

Objectif: Mise en marche du site web de l'IGF.
Code: **WEB**

Sous-tâche	Description	Responsable	Remarques
Scénario	Choisir le scénario de publication du site web, par exemple le nom du domaine, la relation avec le site du Ministère de finances, l'hébergement du site, etc...	Le Chef de l'IGF	
Specs fonctionnelles	Élaboration des spécifications fonctionnelles finales	Chef de projet/Editeur Intranet/Web master	
Documentati	Ramasser le contenu à publier	Chef de	

on initiale	dans la première version du site	projet/Editeur Intranet/Web master	
Appel d'offres	Publier un appel d'offres pour les services d'hébergement, de dessin et de construction du site	DAM/Éditeur Web	
Construction	Dessiner et construire le site web	Fournisseur/Éditeur Web	
Mise à jour	Définir la procédure pour la mise à jour du contenu du site web	Fournisseur/Éditeur Web	

16.1.16 Formation aux nouvelles applications

Objectif: Formation des usagers aux nouvelles applications.
Code: **COURS-APPS**

Sous-tâche	Description	Responsable	Remarques
Plan de formation	Élaboration d'un Plan de formation pour les usagers des nouvelles applications	DAM/Chef de Projet	
Élaboration de matériel didactique	Élaboration d'un matériel didactique	DAM/Chef de Projet	
Exécution du Plan de formation	Exécution des cours planifiés dans le Plan de formation	DAM/Chef de Projet	

16.1.17 Répertoire des rapports de missions: gestion de l'historique

Objectif: Gestion de l'historique des rapports des missions
Code: **HISTORIQUE**

Sous-tâche	Description	Responsable	Remarques
Procédure	Élaboration de procédures pour la gestion de l'historique des rapports de missions.	DPAS	

Appel d'offres	Acheter un appareil de numérisation des documents	DAM/DPAS	Inclus dans l'appel d'offres DEV
Configurer un répertoire RM	Configurer un répertoire pour stocker des fichiers de rapports de missions	DMNI/DPAS	
Numériser RM	Numériser les rapports des années 2016 et 2017 selon les procédures élaborées. Remplir les métadonnées définies pour l'application Suivi de Missions v2 et entretenir un registre	DPAS	Former un groupe d'opérateurs pour faciliter la tâche de la numérisation massive des rapports des missions
Nouvelles demandes de RM	Numériser les nouvelles demandes des rapports des mission. Remplir les métadonnées définies pour l'application Suivi de Missions 2 et maintenir un registre	DPAS	
Stocker RM	À partir de 2018, stocker les rapports des missions dans le répertoire RM	DPAS	

16.1.18 Adaptation de l'organisation de l'IGF

Objectif: Adapter l'organisation interne aux nouveaux besoins. Voir section 11 Nouveaux rôles.
Code: **ORGANISATION**

Sous-tâche	Description	Responsable	Remarques
Réglementation interne	Élaboration d'une instruction pour définir l'adaptation de l'organisation aux nouveaux besoins dérivés de l'implantation des systèmes d'information à l'IGF.	Le Chef de l'IGF/CG's	
Sécurité	Adapter l'organisation selon les nouveaux besoins de sécurité de l'information.	Le Chef de l'IGF/CG's/...	Voir section 9.1 Rôles et responsabilités du Plan Directeur des SI

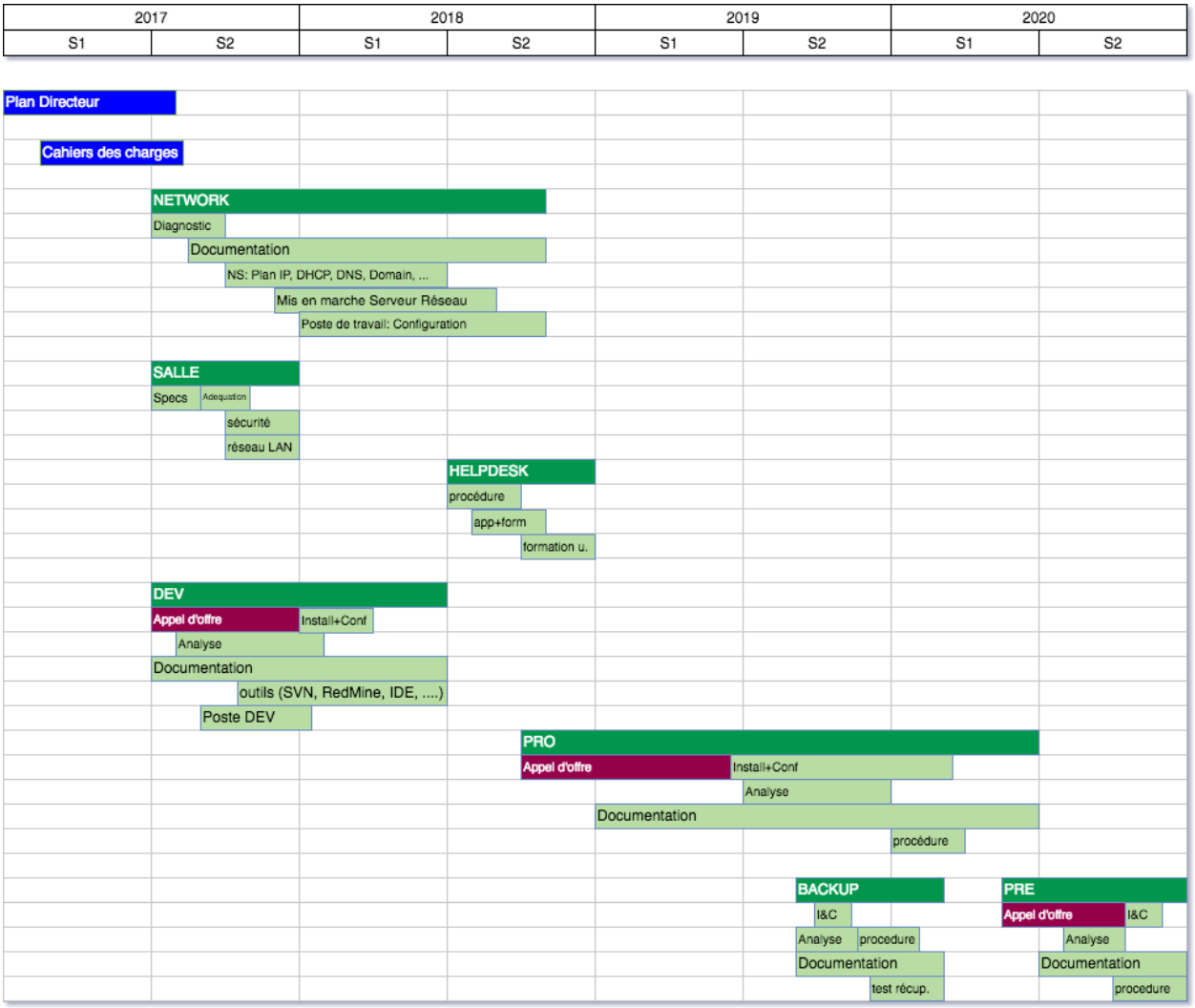
Intranet	Adapter l'organisation selon les nouveaux besoins dérivés de l'implantation de l'Intranet.	Le Chef de l'IGF/CG's/...	voir section 11.1 du Plan Directeur des SI
Site web	Adapter l'organisation selon nouveaux besoins dérivés de la publication du site web de l'IGF.	Le Chef de l'IGF/CG's/...	voir section 11.5 du Plan Directeur des SI
Renforcer la structure technique	Adapter l'organisation de la DMNI aux besoins dérivés de l'implantation des nouveaux systèmes d'information.	Le Chef de l'IGF/CG's/...	voir section 11.2 du Plan Directeur des SI
Chefs de projets fonctionnels	Ajouter aux unités fonctionnelles la figure de Chef de projet fonctionnel	Le Chef de l'IGF/CG's/...	voir section 11.4 du Plan Directeur des SI
Centre d'assistance technique	Adapter l'organisation de la DMNI pour héberger le Centre d'assistance technique	Le Chef de l'IGF/CG's/...	voir section 13: Centre d'assistance technique du Plan Directeur des SI

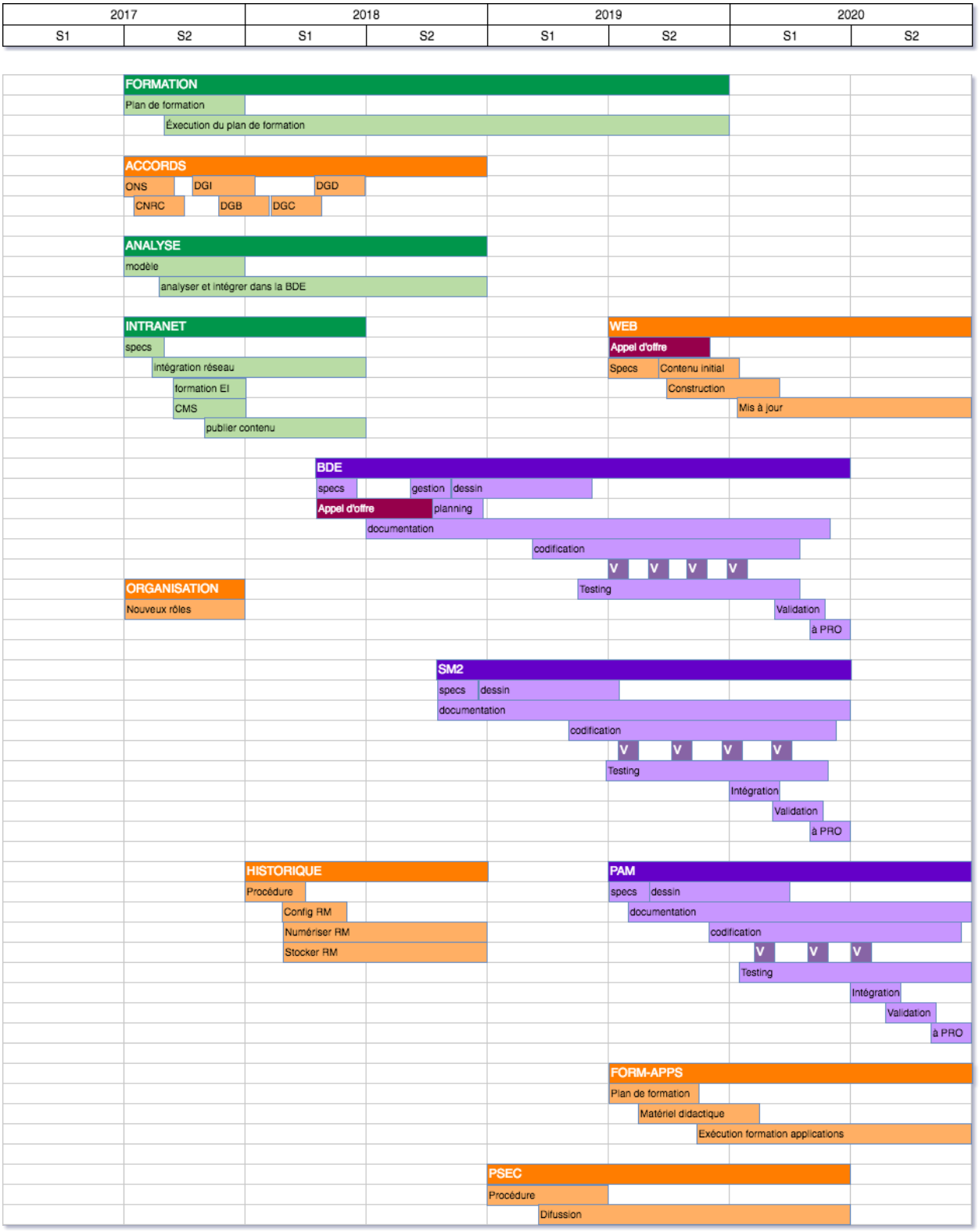
16.1.19 Élaborer un Plan de Sécurité des systèmes d'information

Objectif: Élaborer un Plan de sécurité des systèmes d'information avec l'objectif de définir des procédures et techniques de sauvegarde de l'information de l'IGF gerée par ses systèmes d'information.
Code: **PSEC**

Sous-tâche	Description	Responsable	Remarques
Procédure	Élaborer un Plan de sécurité des systèmes d'information avec l'objectif de définir des procédures et techniques de sauvegarde de l'information de l'IGF gerée par ses systèmes d'information.	RSI/CG's	Aide externe: possible participation d'un expert de sécurité de l'information
Diffusion	Diffuser des mesures de sécurité incluses dans ce Plan	RSI	

16.2 Planification des projets




2017
2018
2019
2020
S1
S2
S1
S2
S1
S2
S1
S2
FORMATION
Plan de formation
Éxecution du plan de formation
ACCORDS
ONS
DGI
DGD
CNRC
DGB
DGC
ANALYSE
modèle
analyser et intégrer dans la BDE
INTRANET
specs
intégration réseau
formation EI
CMS
publier contenu
WEB
Appel d'offre
Specs
Contenu initial
Construction
Mis à jour
BDE
specs
gestion
dessin
Appel d'offre
planning
documentation
codification
V
V
V
V
Testing
Validation
à PRO
ORGANISATION
Nouveux rôles
SM2
specs
dessin
documentation
codification
V
V
V
V
Testing
Intégration
Validation
à PRO
HISTORIQUE
Procédure
Config RM
Numériser RM
Stocker RM
PAM
specs
dessin
documentation
codification
V
V
V
Testing
Intégration
Validation
à PRO
FORM-APPS
Plan de formation
Matériel didactique
Exécution formation applications
PSEC
Procédure
Difussion

17 BUDGET DES SYSTÈMES D'INFORMATION

Il très recommandé de procéder à la mise en oeuvre d'un budget pluriannuel dédié à des nouveaux projets relatifs aux systèmes d'information et à leur maintenance.

ANNEXES

18 ANNEXE I : CADRE LÉGAL (L'ADMINISTRATION ÉLECTRONIQUE EN ESPAGNE, UN CADRE GÉNÉRAL)

18.1 Organisation

Au cours des dernières années, des changements profonds ont été observés dans l'Administration en ce qui concerne l'utilisation des technologies de l'information et des communications (TIC). Des changements caractérisés, dans une première phase, par l'usage de ces technologies pour l'automatisation et les améliorations du fonctionnement des processus internes de l'Administration, avec la conviction que l'épargne dérivée des améliorations de l'efficacité se déplacerait aux citoyens, et dans une deuxième phase, par l'universalisation d'Internet et des technologies associées qui ont favorisé le développement de nouveaux services et formes de relation avec les citoyens et les entrepreneurs sur un chemin sans retour vers l'Administration électronique.

La confluence de nouvelles tendances technologiques comme le sont les services dénommés « sur l'informatique en nuage » (cloud computing), l'apparition de dispositifs mobiles de plus en plus intelligents, la généralisation de l'usage des réseaux sociaux, la capacité d'analyse de grands volumes de données (big data) avec l'universalisation de l'usage d'Internet, ont confirmé l'affirmation d'un nouveau panorama dans lequel les citoyens ont acquis de nouvelles habitudes dans l'utilisation des services numériques dans leur relation avec les entreprises et aussi avec les Administrations Publiques.

La numérisation des services englobe, d'une part, les services électroniques et les technologies de l'information et des communications, qui ont été la base de l'Administration électronique dans laquelle l'Espagne a atteint une progression remarquable.

Mais la numérisation pose de nouveaux défis et opportunités. La convergence de ces nouvelles forces technologiques amène à un nouveau scénario dans lequel l'Administration doit être capable de s'adapter de manière agile aux demandes d'un environnement changeant, de fournir une information et des services digitaux à tout moment, dans n'importe quel lieu et à travers différents canaux, de générer de nouvelles formes de relation avec les citoyens et d'innover de nouveaux services, en profitant les opportunités que fournissent ces technologies. Et tout cela doit être pourvu de manière sûre, agile et avec efficacité et efficience dans l'utilisation des ressources disponibles.

Par conséquent, il ne s'agit pas d'utiliser des TIC dans les processus de l'Administration, mais de créer les dynamiques nécessaires pour pouvoir adapter les services, les processus, les opérations et les capacités de l'Administration à une réalité numérique et qui continuera d'évoluer à grande vitesse.

L'Administration doit adopter une nouvelle culture de l'information et être préparée pour générer et traiter de grands volumes d'information numérique sur ses opérations, processus et résultats, afin qu'ils puissent être mis à la disposition des citoyens par souci de transparence, et aux entreprises et agents sociaux pour la promotion de la réutilisation de l'information du secteur public. De la même manière, le développement des capacités d'analyse transversale de l'information permettra d'optimiser la gestion, d'améliorer la prise de décisions et d'offrir des services interdépartementaux de manière indépendante à

la structure administrative.

Par ailleurs, l'universalisation des services digitaux permet de fonder une Administration plus transparente, où les citoyens peuvent participer à la définition et même à la conception des services publics appelés à être en phase avec leurs nécessités réelles sous un nouveau modèle de gouvernance.

Tout cet environnement implique un nouveau monde d'opportunités, mais aussi des menaces, qui doivent être affrontées dès leur apparition, additionnant les efforts et les ressources disponibles et dessinant une stratégie commune pour la transformation digitale de l'Administration, basée sur les TIC et orientée vers la génération de valeur ajoutée pour les citoyens.

Le rapport élaboré par la **Commission pour la Réforme des Administrations Publiques (CORA)**, créée par l'Accord du Conseil des Ministres du 26 octobre 2012, et présenté au Conseil des Ministres du 21 juin 2013, reconnaît ce rôle fondamental des TIC et conseille un traitement singulier par rapport à d'autres services communs pour obtenir le maximum d'efficacité et d'optimisation de ressources ainsi que pour profiter des opportunités que suscite une stratégie commune.

La reconnaissance du rôle des TIC dans la transformation de l'Administration était déjà prise en compte dans la **Loi 11/2007, du 22 juin, pour l'accès électronique des citoyens aux Services Publics** qui partait de la reconnaissance d'un développement insuffisant de l'administration électronique.

La Loi 11/2007 consacre la relation avec les Administrations Publiques par des moyens électroniques comme un droit des citoyens et comme une obligation pour les Administrations.

Un bon usage des TIC, efficient et intégré, semble aussi indispensable pour s'acquitter des engagements que la **Loi 19/2013, du 9 décembre, de la transparence, de l'accès à l'information publique et du bon gouvernement** établi pour l'Administration.

Le Décret royal 695/2013, du 20 septembre, crée la **Direction de Technologies de l'Information et les Communications de l'Administration Générale de l'État (DTIC)**, avec la volonté de constituer les TIC comme un outil de structuration pour améliorer le fonctionnement des administrations. La DTIC est mise en place, conformément à sa norme de création, comme un organe spécifique, au plus haut niveau, pour pousser et coordonner le processus nécessaire de rationalisation et transformation des diverses facettes de la politique des TIC dans tout le domaine du Secteur Public Administratif de l'État. Par Décret royal 802/2014, du 19 septembre, le dit organe est assigné au Ministère des Finances et les Administrations Publiques.

Le processus de transformation qui se charge de la DTIC implique la révision des approches organisationnelles en vigueur, dont certaines sont mises en évidence dans le rapport CORA. Parmi celles-ci, il faut noter l'existence d'un degré élevé d'atomisation et un haut niveau d'indépendance dans l'agissement des agents qui interviennent dans le domaine des TIC au niveau de l'Administration Générale de l'État et de ses Organismes Publics.

Cette situation favorise une grande autonomie dans la gestion des fonds et des

ressources TIC de la part des différents organes de l'Administration Publique qui prennent les décisions relatives à la gestion des frais et des investissements. Ceci a donné lieu à une dispersion considérable des ressources et des efforts dans l'environnement des TIC, bien que les sous-secrétariats et d'autres organes compétents en matière des technologies de l'information et des communications ont été capables de s'occuper d'une demande croissante de services et de certaines exigences, qui ont situé l'actuelle offre de services à des niveaux équivalents ou supérieurs à la moyenne de l'Union Européenne.

Le modèle de gouvernance sur lequel s'appuyait ce décret royal essaie de surpasser telle situation, afin d'obtenir une politique TIC commune à toute l'Administration Générale de l'État et de de ses Organismes Publics dans un contexte d'austérité de la dépense publique basée sur l'exigence d'efficacité et coresponsabilité. La **Loi Organique 2/2012, du 27 avril, de Stabilité Budgétaire et une Durabilité Financière** est l'un des piliers des principes d'efficacité dans l'allocation et l'utilisation des ressources publiques. Comme un développement de ce qui dispose la Loi Organique 2/2012, du 27 avril, le **Décret royal 806/2014** crée des instruments pour contribuer à une gestion des ressources publiques, axée sur l'efficacité, l'économie et la qualité.

Pour la conception de la nouvelle gouvernance TIC, trois objectifs basiques ont été identifiés depuis la DTIC:

1. Orienter les rôles et les lignes stratégiques des TIC de telle façon qu'ils aient pour objectif principal de satisfaire les nécessités découlant de la stratégie globale du Gouvernement et disposer d'une planification stratégique commune à toute l'Administration Générale de l'État et ses Organismes Publics .

2. Renforcer l'Administration numérique et faire des TIC les instruments qui permettent de rendre durable le processus constant d'innovation et d'amélioration de la qualité des services tout en augmentant la productivité des employés.

3. Rationaliser l'usage des ressources informatiques pour obtenir une plus grande efficacité, en fournissant une économie substantielle de coûts.

La DTIC est chargée d'aligner les investissements TIC avec les objectifs stratégiques établis.

Le nouveau modèle de gouvernance TIC a pour objectif de centraliser les compétences et les moyens dans un seul organe administratif auquel toutes les unités TIC de l'Administration Générale de l'État et ses Organismes Publics seront intégrées. On crée aussi de nouveaux organes associés qui servent comme un canal d'information et de mise en commun des nécessités et des opportunités d'utilisation de moyens informatiques de manière rationnelle et efficiente.

Cela entraînera, donc, une formation pour la prestation de services TIC partagés à toutes les unités de l'Administration Générale de l'État et ses Organismes Publics, et la définition d'une stratégie commune qui définira les lignes d'action en matière des TIC.

À ces effets, on crée la **Commission de Stratégie TIC** et, dans le domaine départemental, les **Commissions Ministérielles d'Administration Numérique**, qui sont des organes associés chargés de pousser la transformation numérique de l'Administration

conformément à une Stratégie commune dans le domaine des TIC.

Le Décret royal 424/2016, du 11 novembre, par lequel a été établie la structure organique basique des départements ministériels, change la dénomination de la Direction de Technologie de l'Information et des Communications pour celle de **Secrétariat Général d'Administration Digitale (SAGD)**, avec les mêmes fonctions, et dépendant du Secrétariat d'État de la Fonction Publique et du Ministère des Finances et de la Fonction Publique.

18.2 Cadre réglementaire actuel

La **Loi 11/2007, du 22 juin, d'accès électronique des citoyens aux Services Publics**, a été la première norme qui a formalisé le droit des citoyens à établir des liens avec les Administrations Publiques de manière électronique. La Loi établit aussi l'obligation pour l'Administration d'être dotée des moyens et des systèmes nécessaires pour que ce droit puisse être exercé.

Cependant, dans l'actuel environnement, une démarche numérique ne peut pas encore être considérée comme une forme spéciale de gestion des procédures. Elle doit plutôt devenir la norme au sein des administrations. Il s'agit de promouvoir une gestion administrative sans papier basée sur un fonctionnement complètement électronique dans le but de se mettre en phase avec principes d'efficacité et d'efficience et ce, en réduisant les coûts pour les citoyens et les entreprises, et en renforçant les garanties des intéressés.

Avec la nouvelle **Loi 39/2015, de la procédure administrative commune des administrations publiques**, l'usage de moyens électroniques se généralise dans la procédure administrative, de telle sorte que l'Administration fonctionne sans papier. Tout cela, sans toutefois préjuger que les intéressés peuvent continuer d'exercer leur droit de traiter sur place avec l'Administration s'ils le décident.

Pour cela, il est nécessaire de simplifier les moyens électroniques à travers lesquels les citoyens peuvent traiter avec les Administrations Publiques et de généraliser la présentation de documents à travers un registre électronique pour chaque Administration qui fonctionnera comme un portail permettant l'accès aux registres électroniques de chaque organisme et à ses archives électroniques.

On règle ainsi, pour la première fois, la possibilité de pouvoir réaliser des remises de pouvoirs « *apud acta* », par voie présentielle ou électronique, ce qui permet d'accélérer les relations du citoyen ou de l'entreprise qui traite avec l'administration à travers un représentant.

Suivant la ligne imposée par le **Règlement européen sur l'identification électronique et des services de confiance pour les transactions électroniques sur le marché intérieur**, l'identification (pour savoir qui réalise la formalité) est séparée de la signature électronique (nécessaire pour l'expression du consentement pour lequel une capacité juridique suffisante est requise).

Les collectifs obligés de traiter électroniquement avec l'Administration sont définis dans la loi, en considérant pour la première fois, pour certaines démarches, le collectif d'employés publics dans les limites établis par les Administrations Publiques, et les

professionnels avec obligation de s'inscrire en corporation.

Toutes les notifications seront préférablement réalisées par des systèmes électroniques (quelques sujets seront obligatoirement notifiés sous forme électronique).

Les ressources suivantes de notification électronique ont été établies : une direction électronique habilitée unique, ou une notification par comparution de l'intéressé dans un siège électronique. De la même manière, il est établi que les intéressés pourront accéder aux notifications depuis le point d'accès général électronique de l'Administration qui fonctionnera comme un portail d'accès.

La loi rend obligatoire le caractère électronique des registres administratifs et des archives de documents administratifs. Si les intéressés présentent un document en format papier, en personne, celui-ci devra être numérisé dans les bureaux d'aide en matière des registres, et il sera automatiquement inscrit dans le registre électronique général de chaque Administration ou organisme. Par la suite le document sera incorporé à l'archive électronique unique (un par chaque Administration).

Les formalités sont simplifiées et les charges administratives sont réduites. La règle générale sera de ne pas apporter de documents originaux sauf, de manière exceptionnelle, lorsqu'on on recueille dans la réglementation régulatrice. L'intéressé ne devra pas apporter les documents qui sont déjà en possession de l'Administration.

Les normes applicables à l'élaboration de copies électroniques de documents sont clarifiées et simplifiées, afin d'accélérer l'action de l'Administration et de pousser l'usage de moyens électroniques entre les Administrations et les intéressés, en égalant les conditions requises pour la présentation de copies sous forme présentielle et avec les conditions requises pour la présentation de copies électroniques.

La réforme intégrale et structurelle des Administrations Publiques, promue par la CORA, a aussi misé sur l'amélioration de l'usage des TIC dans la totalité pratique de ses propositions d'innovation pour l'Administration, en considérant que toute initiative de modernisation et d'amélioration des Administrations doit se baser nécessairement sur l'emploi des technologies.

En ce sens, la **Loi 40/2015, du 1er octobre, du Régime Juridique du Secteur Public**, en sa qualité d'élément de modernisation des structures administratives et d'améliorations du système des relations existantes entre les trois niveaux d'Administration (étatique, régional et local), s'occupe des questions basiques d'Administration Électronique qui sont relatives à son objet: établir et régler les bases du régime juridique, de l'organisation et du fonctionnement des Administrations Publiques, Organismes publics et entités liées ou dépendantes d'elles, pour le développement de leurs activités.

Avec la Loi 40/2015, nous essayons d'accélérer le fonctionnement interne de l'Administration, en établissant avec un caractère général l'obligation de la part des Administrations Publiques de l'usage de moyens électroniques dans leurs relations inter-administrations, au niveau interne et externe. De la même manière, on établit que l'usage de ces moyens électroniques par les Administrations Publiques devra garantir l'interopérabilité des systèmes et solutions adoptés par chacune d'elles. Préférablement, on optera pour la prestation de services conjointe pour le citoyen.

Ces objectifs seront réalisés sous forme graduelle et planifiée, de sorte à permettre de réaliser les adaptations nécessaires, techniques et formatives, pour arriver à un fonctionnement de nature complètement électronique.

Il est aussi intéressant de signaler que les **Décrets Royaux 4/2010, et 3/2010, du 8 janvier**, qui régissent le **Schéma National d'Interopérabilité (ENI)** et le **Schéma National de Sécurité (ENS)** dans le domaine de l'Administration Électronique, ainsi que leurs normes dérivées, sont encore en vigueur.

19 ANNEXE II: Spécifications fonctionnelles de la base de données des entités[4]

19.1 Introduction

Dans le lot APPS, il y a entre autres l'appel d'offres pour le développement de l'application fonctionnelle de l'IGF et la Base de données des entités: Code BDE. Il inclut les services professionnels pour développer cette application.

Dans ce chapitre, on décrit les principales caractéristiques fonctionnelles de l'application que le prestataire doit connaître pour préparer sa proposition de développement de l'application BDE.

19.1.1 Description de l'IGF du point de vue de la BDE

L'IGF a besoin de la création d'une base de données d'entités qui sont objets d'audit. La base de données contiendra l'information sur l'identification des entités, leur classification du point de vue juridique, la composition du capital, le cas échéant, leurs données budgétaires, ressources humaines, etc. On posera aussi l'inclusion d'indicateurs de gestion et financiers qui permettent de générer un tableau de bord pour le suivi des entités de la part de l'IGF, et qui introduit une information additionnelle pour une sélection optimale de l'échantillon d'entités qui fera partie du Plan Annuel d'Audit de l'IGF.

Chaque utilisateur de l'IGF a besoin de plusieurs fonctionnalités selon le poste occupé. En outre, l'utilisateur a besoin de se connecter aux données de certaines entités ou à celles de leur ensemble. Alors, l'application doit fournir à chaque utilisateur les fonctionnalités nécessaires pour effectuer son travail de sorte à ce que soit pris en compte l'ensemble des besoins de l'IGF ainsi que les besoins particuliers de chaque utilisateur.

Ce chapitre est complété par le document "Spécifications fonctionnelles de l'application de BDE".

19.1.2 Besoins et Objectifs principaux de la BDE

19.1.2.1 Besoins

Les principaux besoins de l'IGF à propos de la BdE sont:

1. Avoir la liste de toutes les entités publiques couvertes par le contrôle de l'Inspection Générale des Finances (IGF) : qu'elles revêtent le statut d'établissement à caractère administratif ou économique ;
2. Avoir les informations générales permettant l'identification de chaque entité ;
3. Avoir les informations financières et non financières de chaque entité ;
4. Améliorer la préparation du plan annuel d'audits de l'IGF à travers les informations fournies par la BDE.
5. Améliorer la préparation et le suivi des missions d'audits à travers les informations fournies par la BDE.

[4] La version complete de la spécification fonctionnelle de la base des données des entités est accesible à: https://docs.google.com/document/d/1xAnpVCCPfEkWZitTJGljsy5UqyOk55nDeV4qTQjgPkA/edit

19.1.2.2 Objectifs

L'objectif principal de la base de données est d'assurer le recensement exhaustif et permanent des informations relatives aux entités publiques.

Toutefois, la BDE vise aussi les objectifs suivants :

1. Le développement d'une base de données informatique pour l'hébergement des informations relatives aux entités ;
2. L'amélioration de l'accessibilité des informations relatives aux entités aux différents utilisateurs de l'IGF à travers une application informatique ;
3. La réduction de l'utilisation du papier comme support d'information ;
4. Le développement d'un système d'autorisation d'accès à l'information sensible relative aux entités ;
5. La contribution et l'exploitation des informations relatives aux entités avec les autres dispositifs informatiques (applications) de l'IGF, notamment ; le plan annuel d'audit, le suivi des missions et l'intranet ;

19.2 Description du contexte actuel (l'existant)

19.2.1 Information sur les entités

19.2.1.1 Sources d'Information de l'IGF

Actuellement, l'IGF recense les informations de 2.500 entités. Ce recensement a été utilisé durant la réalisation de l'étude sur la cartographie de risques du contrôle interne et des systèmes d'information dans le cadre du jumelage.

Par ailleurs, les inspecteurs de l'IGF utilisent les programmes fournis par le Secrétariat Général du Gouvernement (SGG) pour la collecte des textes réglementaires (journaux officiels), notamment ;

- Le site internet du SGG ; www.joradp.dz;
- Le logiciel « JO+ » accessible uniquement à l'administration centrale (DMNI) ;
- Le logiciel « SCALER » diffusé à tous les inspecteurs.

Ainsi, par exemple, les programmes du SGG permettent de fournir les informations suivantes :

1. Le texte de création des entités administratives ainsi que de leurs organisations
2. La nomination des responsables des entités administratives ;
3. Les budgets des entités administratives (lois de finances, décrets de répartitions, transferts de crédit,…).

D'autre part, les inspecteurs accèdent aux comptes administratifs ainsi qu'aux bilans des activités des entités durant les missions.

Par ailleurs, l'IGF est destinatrice régulièrement de rapports et de bilans financiers des EPIC, mais, faute d'une structure centralisée de ces rapports, leurs informations ne sont pas exploitées par les inspecteurs de l'IGF.

Enfin, les rapports de l'IGF forment une source importante de données sur les entités, du fait que chaque rapport est structuré de manière à contenir ;

- Les informations générales sur l'entité contrôlée ;
- Les principaux indicateurs financiers et non financiers ;
- Les constats et observations ;
- Les recommandations.

L'exploitation des informations issues des rapports de l'IGF permet d'alimenter les indicateurs sur l'évaluation du contrôle interne ainsi que de la cartographie des risques.

19.2.1.2 Sources d'Information provenant d'autres organisations

Les organisations desquelles l'IGF peut recevoir des informations sur les entités sont les suivantes::

1. Centre National du Registre de Commerce (CNRC)
    a. Les statuts des EPE et EPIC
    b. Bilan et compte de résultats pour les EPE et EPIC
2. L'Office National des Statistique (ONS)
    a. information du périmètre reliée au numéro d'identification statistique
    b. nomenclature et tables auxiliaires (wilayas, communes, secteurs, activités, etc…)
3. Secrétariat Général du Gouvernement (SGG)
    a. Journal Officiel pour le cadre juridique:
        i. Texte de création
        ii. Texte organisationnel
4. Direction Générale des Impôts (DGI)
    a. information du périmètre reliée au numéro d'identification fiscale
5. Direction Générale du Budget (DGB)
    a. Information pour le périmètre
    b. Budget des Entités Administratives
    c. Subventions
    d. CAS
6. Direction Générale de Comptabilité (DGC)
    a. Information pour le périmètre
    b. Comptabilité: Compte de gestion
7. Direction Générale du Douanes (DGD)
    a. Inspections de contrôle
    b. Information du périmètre
8. Algérie Télécom

a. Coordonnées: annuaire téléphonique

9. Cour des comptes
    a. Évaluation du contrôle interne
10. Départements ministériels
    a. Coordonnées: la communication de chaque ministère des coordonnées de ses établissements
11. Inspections des Ministères (IGM)
    a. Évaluation du contrôle interne
12. L'entité elle-même
    a. Cartographie des risques, élaborée par l'entité elle-même
    b. Risques de contrôle identifiés pour les inspecteurs de l'IGF
    c. Évaluation du contrôle interne

19.2.2 Gestion de l'information

19.2.2.1 De manière manuelle

La plus grande partie des informations utilisées par les inspecteurs durant les missions de contrôle est sur support papier.

19.2.2.2 Application informatique

Actuellement, il n'y a aucune application informatique portant sur les entités. Les inspecteurs essayent de chercher l'information dont ils ont besoin de manière manuelle, ainsi qu'à travers les programmes fournis par le SGG en ce qui a trait aux textes juridiques (JO+, SCALER,…).

19.3 Définition du problème

Absence d'une application informatique pour la gestion de l'information des entités qui sont contrôlées par l'IGF.

Le manque d'information suffisante concernant les entités pour réaliser les contrôles.

L'information disponible actuellement sur les entités est sur support papier, ce qui rend difficile une utilisation efficace de cette information tant pour les missions que pour le plan annuel d'audit.

19.4 Analyse de besoins fonctionnels

19.4.1 Acteurs (groupes) et utilisateurs (rôles, …)

19.4.1.1 Externes à l'IGF

Les acteurs externes en relation avec l'IGF dans le cadre de la BDE sont les organisations publiques pouvant envoyer des informations sur les entités.

Ces organisations publiques sont, jusqu'à présent, les suivantes :

1. Office National des Statistique (ONS)
2. Centre national du registre de commerce (CNRC)
3. Secrétariat Général du Gouvernement (SGG)
4. Direction Générale de Budget (DGB)
5. Direction Générale de Comptabilité (DGC)
6. Direction Générale des Impôts (DGI)
7. Direction Générale du Douanes (DGD)
8. Cour des comptes
9. Ministères
10. Inspection des Ministères (IGM)
11. Algérie Telecom
12. Les entités elle-même

19.4.1.2 Internes à l'IGF

Les différents rôles ou acteurs de l'IGF pouvant utiliser la base de données des entités sont:

1. Tous les utilisateurs de l'IGF
2. Le chef de l'IGF
3. Le contrôleur général
4. L'inspecteur régional
5. Le directeur de mission
6. Le chargé d'inspection
7. L'inspecteur
8. L'informaticien
9. L'administrateur
10. L'assistant (la personne qui assure les tâches de secrétariat du chef de l'IGF ainsi que celles des contrôleurs généraux)

Par ailleurs, d'autres applications de l'IGF accèderont à la base de données également, notamment :

- Suivi de mission v2.0
- Plan annuel des missions
- Intranet

19.4.2 Histoires d'utilisateurs (User stories)

19.4.2.1 1Introduction

Les "user stories" ou histoires d'utilisateurs résume en une ou deux phrases ce que recherche l'utilisateur sur la base de données des entités. Elles sont formées par trois parties:

1. Le rôle ou utilisateur à l'IGF (Qui je suis <rôle>)
2. Fonctionnalité exigée par l'utilisateur sur les entités (je veux <fonctionnalité>)
3. Quel est le but de l'utilisateur (pour <but>)

19.4.2.2 Tous les utilisateurs de l'IGF (Niveau 0)

Comme utilisateur de l'IGF, une personne peut :

1. obtenir une liste des toutes les entités, pour connaître leurs données principales (coordonnées, propriétés, secteur et activité);
2. obtenir une liste de toutes les entités, pour savoir les données du budget, du cadre juridique, de la comptabilité et de l'organisation;
3. rechercher par différents filtres, pour obtenir les entités selon: statut juridique, tutelle, secteur, budget, etc;
4. avoir l'organigramme de chaque entité;
5. avoir une carte relationnelle des entités par filtre (tutelle, budget, programme,…);
6. avoir une matrice budgétaire globale du périmètre des entités.

Ces histoires d'utilisateurs sont communes à tous les utilisateurs de l'IGF. En outre, chaque utilisateur a ses propres histoires d'utilisateur (user story) qui sont développées ci-dessous:

19.4.2.3 Le chef de l'IGF et contrôleur general (Niveau 1)

Comme chef de l'IGF ou contrôleur général, il m'est possible d'obtenir une liste de toutes les entités, pour connaître la cartographie des risques et l'évaluation du contrôle interne.

19.4.2.4 L'inspecteur régional et le directeur de mission (Niveau 2)

Comme directeur de mission ou inspecteur régional, il m'est possible de :

1. obtenir un liste des entités qui font partie de mon périmètre d'intervention, pour en connaître la cartographie de risques et l'évaluation du contrôle interne.
2. la capacité d'introduire et de modifier des données manuellement des entités auditées/contrôlées dans le cadre de mon périmètre d'intervention, avec une option de traçabilité (journal des modifications, identification de l'auteur des modifications,…).

19.4.2.5 Le chargé d'inspection et L'inspecteur (Niveau 3)

Comme chargé d'inspection ou inspecteur, il m'est possible de :

1. obtenir une liste des entités qui font partie de mon périmètre d'intervention (mission), pour en connaître la cartographie des risques et l'évaluation du contrôle interne. .
2. la capacité d'introduire et de modifier les données manuellement des entités auditées/contrôlées dans le cadre de mon périmètre d'intervention (mission), avec

une option de traçabilité (journal des modifications, identification de l'auteur des modifications,…).

19.4.2.6 L'informaticien

Comme informaticien, il m'est possible de :

1. importer à la BdE l'information des entités envoyée par les organisations externes, pour que l'administrateur puisse l'examiner.
2. ajouter à la BdE l'information des entités révisée pour l'administrateur, pour que les utilisateurs de l'IGF puissent l'utiliser.

19.4.2.7 L'assistant

Comme assistant, il m'est permis de :

1. obtenir une liste des entités auxquelles j'ai accès, pour en connaître la cartographie des risques et l'évaluation du contrôle interne.
2. la capacité d'introduire et de modifier les données manuellement des entités dont j'ai accès, avec une option de traçabilité (journal des modifications, identification de l'auteur des modifications,…).

19.4.2.8 L'administrateur

Comme administrateur, je peux :

1. examiner l'information des entités que l'informaticien (DMNI) a ajoutées à la BdE pour l'examiner.
2. modifier l'information qui n'est pas bonne, pour l'examiner une nouvelle fois.
3. avoir la capacité d'introduire et de modifier les données manuellement des entités dont j'ai accès, avec une option de traçabilité (journal des modifications, identification de l'auteur des modifications,…).

19.5 Analyse des besoins non fonctionnels

19.5.1 Du produit

19.5.1.1 La securité

Les besoins non fonctionnels de la sécurité sont communs à toutes les applications. Ils sont définis dans le chapitre 3 "EXIGENCES TECHNIQUES".

19.5.1.2 L'utilisation

Les utilisateurs de la BDE peuvent sélectionner l'emploi de la langue arabe ou de la langue française. Une option au premier écran de l'application permettant de basculer entre les deux langues doit être prévue à cet effet.

19.5.1.3 Portabilité

L'application de la BDE doit être utilisée à partir des principaux navigateurs actuels (ex. explorer, chrome, firefox, opera, etc.)

L'application de la BDE doit être compatible avec l'un des systèmes d'exploitation actuels: windows ou linux.

Tout dépend de l'évolution des terminaux (tablette ou smartphone) utilisés par l'IGF à l'avenir. Une compatibilité potentielle doit être prévue pour les systèmes Android ou IOS.

19.5.2 Organisationnel

19.5.2.1 Environnement

Jusqu'à présent, les besoins non fonctionnels organisationnels de ce type n'ont pas été définis.

19.5.2.2 Organisationnel

Les différents rôles ou utilisateurs principaux de l'IGF et leurs fonctions assignées sont définis conformément aux textes réglementaires suivants :

- Décret exécutif n°08-273 du 06 Septembre 2008 portant organisation des structures centrales de l'inspection générale des finances.
- Décret exécutif n°08-274 du 06 Septembre 2008 fixant l'organisation et les attributions des inspections régionales de l'inspection générale des finances.

19.5.2.3 Développement

Jusqu'à présent, les besoins non fonctionnels organisationnels de ce type n'ont pas été définis.

19.5.3 Externes

Jusqu'à présent, les besoins non fonctionnels externes de type juridiques ou réglementaires n'ont pas été définis.

19.6 Description de la solution

La description détaillée et graphique de la solution est dans le livrable "Base des données des entités - Spécifications fonctionnelles". Plusieurs diagrammes UML de type Comportement ou de Structure sont apportés dans cette description. .

19.6.1 19.6.1 Comportement des diagrammes

Pour la description du modèle d'affaires, sont utilisés :

1. Les cas d'utilisation;
2. Les diagrammes d'activités.

19.6.1.1 Cas d'utilisation

Les principaux cas d'utilisation identifiés dans l'application de BDE sont décrits dans cette partie.

Toutefois, le prestataire chargé de l'élaboration de l'application de la BDE peut définir d'autres cas d'utilisation au cours de l'analyse fonctionnelle qu'il effectuera par ses soins.

1. Cas d'utilisation 1 - Identification "Entités"
    a. Acteurs: Source de données et utilisateurs de l'IGF
    b. Type: premier niveau
    c. Références:
        i. Cas d'utilisation principale des systèmes d'information de l'IGF.
        ii. Toutes les cases du deuxième niveau
    d. Conditions préalables.
        i. Les utilisateurs sont identifiés et autorisés.
        ii. Les utilisateurs peuvent se connecter à l'application informatique de la BdE.
    e. Postcondition: uniquement les utilisateurs de l'IGF peuvent passer à d'autres cas d'utilisation
    f. Description
        i. Les utilisateurs de l'IGF peuvent avoir accès à l'application.
        ii. Les organisations avec lesquelles l'IGF a établi des protocoles d'accords pour l'échange d'informations peuvent envoyer des informations sur les entités.
        iii. Dans les protocoles, sont définis les trois niveaux de l'échange d'informations.
2. Cas d'utilisation 2 - Identification "Gestion de la Qualité"
    a. Acteurs:
        i. L'application
        ii. L'administrateur de la Qualité.
    b. Type: principal
    c. Références: diagramme d'activité "L'Échange des données et Qualité Activity Diagram"
    d. Condition préalable: l'informaticien a importé l'information envoyée par une entité à la base de données des entités
    e. Postcondition: l'informaticien ajoute l'information envoyée par une entité après que la qualité ait été révisée par l'application et par l'administrateur.
    f. Description: réviser la qualité des données.
        i. L'application effectue plusieurs contrôles de la qualité des données. Si des erreurs sont détectées, elle les reporte à l'administrateur
        ii. L'administrateur examine les erreurs relatives à la qualité des données que l'application a détectées.
3. Cas d'utilisation 3 - Identification "Gestion des filtres et rapports"
    a. Acteurs: l'Administrateur des filtres et rapports

b. Type: secondaire
c. Références: néant
d. Condition préalable: les utilisateurs de l'IGF ont défini les filtres et les rapports dont ils ont besoin
e. Postcondition: l'administrateur a implémenté les filtres et les rapports de manière dynamique dans l'application.
f. Description: en utilisant l'application, l'administrateur pourrait définir:
    i. Filtres incluant une combinaison des variables suivantes:
        1. Commune
        2. Wilaya
        3. Secteur
        4. Activity
            a. Section
            b. Division
            c. Groupe
            d. Classe
        5. Propriété
        6. Forme juridique
    ii. Une liste avec plusieurs classes de rapports des entités selon une combinaison des variables suivantes:
        1. Commune
        2. Wilaya
        3. Secteur
        4. Activité
            a. Section
            b. Division
            c. Groupe
            d. Classe
        5. Propriété
        6. Forme juridique
    iii. En utilisant l'application, l'administrateur pourra obtenir les rapports les plus utilisés par les utilisateurs de l'IGF. Il pourra donc les situer en première position de la liste.

4. Cas d'utilisation 4 - Identification "Gestion des Utilisateurs"
    a. Acteurs: l'Administrateur des Utilisateurs

b. Type: principal

c. Références: néant

d. Condition préalable:

i. Le nouvel utilisateur dispose d'un code d'utilisateur et d'un mot de pas dans le système des identités de l'IGF (on peut consulter le chapitre trois du Cahier de Charges)

ii. Le Chef de l'IGF ou un des Contrôleurs Généraux envoie à l'administrateur l'autorisation pour accéder à la BdE du nouvel utilisateur.

iii. L'administrateur télécharge l'autorisation d'accès à la BdE.

e. Postcondition:

i. L'application envoie au nouvel utilisateur une communication, par exemple un courrier électronique, pour lui confirmer qu'il a été autorisé à accéder à l'application.

f. Description: l'administrateur entrera le code d'utilisateur et l'application de la BdE accédera au système des identités de l'IGF pour prendre le profil du nouvel utilisateur. L'administrateur définit le rôle du nouvel utilisateur.

5. Cas d'utilisation 5 - Identification "Ajouter des entités"

a. Acteurs:

i. L'administrateur des entités

b. Type: secondaire

c. Références: néant

d. Condition préalable:

i. Le Chef de l'IGF ou un des Contrôleurs Généraux a envoyé à l'administrateur l'information principale de l'entité pour l'ajouter à la BdE.

ii. Un des Contrôleurs Généraux a envoyé à l'administrateur l'autorisation pour ajouter la nouvelle entité à la BdE.

iii. L'administrateur télécharge l'autorisation à la BdE.

e. Postcondition:

i. La nouvelle entité a été ajoutée à la BdE.

f. Description: l'administrateur des entités doit ajouter l'information de la nouvelle entité. Les informations obligatoires sont :

i. Données principaux

ii. Coordonnées

iii. Propriétés

iv. Secteur

v. Activité
vi. Forme juridique

6. Cas d'utilisation 6 - Identification "Échange des données"
    a. Acteurs:
        i. Les organisations envoient des données à l'IGF
        ii. L'informaticien
    b. Type: principal
    c. Références: diagramme d'activité "L'Échange des données et Qualité Activity Diagram"
    d. Condition préalable:
        i. Niveau organisationnel: les protocoles d'accords
        ii. Niveau sémantique: le langage utilisé
        iii. La manière technique de l'échange
    e. Postcondition:
        i. Le fichier des données a été importé à la BdE de manière provisoire.
        ii. Les fonctions de l'application révisant la qualité des données ont été exécutées par l'application révisant la qualité des données.
    f. Description: selon le niveau technique, un nouveau fichier de données des entités parvient à l'informaticien qui l'importe à la BdE et en exécute les fonctions de qualité.
7. Cas d'utilisation 7 - Identification "Consulters des entités"
    a. Acteurs: Utilisateurs de l'IGF
    b. Type: principal
    c. Références:
        i. Cas d'utilisation
            1. Consulter toutes les données de toutes les entités
            2. Consulter les données principales de toutes les entités
            3. Consulter les données sensibles des entités autorisées
            4. Modifier toutes les données des entités autorisées
    d. Condition préalable: l'utilisateur est autorisé à consulter ou modifier les entités.
    e. Postcondition: si l'utilisateur modifie une entité, la nouvelle information lui appartenant est de fait modifiée dans la BdE.
    f. Description:
        i. Tous les utilisateurs peuvent consulter l'information principale de toutes les entités. Le Chef et les contrôleurs peuvent consulter

l'information sensible de toutes les entités. Les autres utilisateurs seulement peuvent consulter l'information sensible des entités pour lesquelles ils sont autorisés.

ii. En utilisant l'application, l'utilisateur pourrait utiliser les filtres et rapports définis par l'administrateur.

iii. En utilisant l'application, l'utilisateur pourrait définir les filtres et les rapports dynamiques incluant une combinaison des variables suivantes:

1. Commune
2. Wilaya
3. Secteur
4. Activité
    a. Section
    b. Division
    c. Groupe
    d. Classe
5. Propriété
6. Forme juridique

19.6.1.2 Diagrammes d'activités

On définit ici le diagramme d'activité "L'Échange des données et Qualité Activity Diagram". Les acteurs et les activités de ce diagramme sont les suivants:

1. L'IGF et la source de données: protocole pour l'échange de données
2. L'IGF: Demander l'information
3. Source de données: Générer et envoyer l'information
4. Informaticien: Importer l'information
5. Application et l'Administrateur: Examiner la qualité
6. l'Administrateur: En cas d'erreur lors de l'examen de la qualité, réviser l'information
7. Informaticien: Ajouter l'information
8. Utilisateurs BdE: Utiliser la nouvelle information

19.6.2 Structure des diagrammes

Pour la description du modèle de domaine, les diagrammes sont présentés comme suit :

1. Diagrammes des classes ;
2. Diagrammes des relations ;
3. Diagrammes des modèles.

19.6.2.1 Diagrammes des classes

Une classe est la description d'un ensemble de données ayant une structure, un comportement et des relations avec d'autres classes. La principale classe de la BdE est l'Entité.

Une approximation initiale de la structure de la classe "Entité" peut être:

1. Les données identifiant l'identité:
    a. Le nom d'entité
    b. L'abréviation ou le sigle
    c. Les coordonnées
    d. La propriété ou autorité de tutelle
    e. L'activité
    f. Le secteur
2. Cadre juridique: Il fait référence aux principaux textes juridiques relatifs à l'entité, notamment ceux relatifs à sa création ainsi que ceux réglementant son activité.
3. Budget: Il renvoie au budget officiel arrêté annuellement, il s'agit du décret de répartition et du fascicule budgétaire pour les EPA, et du budget approuvé par le conseil d'administration pour les EPE et EPIC.
4. Comptabilité: Elle renvoie au résultat de l'exécution du budget de l'entité, il s'agit notamment ; du compte administratif et celui de gestion pour les EPA, du bilan et du compte de résultat pour les EPE et EPIC.
5. Organisation interne (organigramme): Il s'agit d'identifier la structure organisationnelle de l'entité, notamment l'organigramme, ainsi que les établissements liés ; services déconcentrés, sous tutelle ou filiale, d'une part. D'autre part, la connaissance de l'organisation interne de manière nominative permet d'identifier les principaux cadres dirigeants (directeurs et sous directeurs) ce qui conduit à faciliter la prise de contact.
6. Evaluation du contrôle interne. Il s'agit d'avoir un indicateur sur le contrôle interne, à travers l'exploitation des missions de contrôle précédentes réalisées sur l'entité.
7. Cartographie des risques: Il s'agit d'avoir un aperçu sur la cartographie des risques de l'entité, lorsqu'elle existe.
8. Autres: Toute autre information utile et indispensable peut être ajoutée.

19.6.2.2 Diagrammes des relations

Ce diagramme montre les relations entre les tables de données qui représentent et détaillent les classes.

En relation avec les entités, il y a:

1. Coordonnées: Il s'agit des coordonnées basiques qui servent à l'identification de l'entité ainsi qu'aux moyens de contact, à l'instar de : la dénomination, l'adresse, le numéro de téléphone et de fax, le site internet et l'adresse e-mail.
    a. Nom de la rue.
    b. Le nombre et autres informations
    c. Code Postal
    d. Commune (ex. Alger-Centre)
    e. Wilaya (ex. Alger centre) avec le nom et le code officiel (deux chiffres qui forment la première partie du code postal)

2. Propriété ou autorité de tutelle. Elle renvoie à la détermination du propriétaire selon le niveau géographique : État, Wilaya ou Commune, d'une part et à la détermination de la composition en parts (en pourcentage) lorsque la propriété de l'établissement est partagée soit entre plusieurs établissements publics ou entre des établissements publics et privés, d'autres part. L'ONS dispose de ces informations pour chaque entité.
3. Secteur: renvoie au secteur d'activité tel que défini dans la nomenclature du budget d'équipement de l'Etat ;
4. Activité: Les activités sont définies et codifiées par l'ONS, selon la Nomenclature Algérienne des Activités (NAA), dans laquelle, chaque activité est identifiée par : section, division, groupe et classe.

En relation avec le Budget, il y a:

1. Budget des entités publiques
2. Budget des entités administratives
    a. Budget de fonctionnement
    b. Budget d'équipement

En relation avec la Comptabilité, il y a:

1. Comptabilité des entités publiques: les états financiers (le bilan, le tableau de résultat, le tableau des flux de trésorerie, le tableau de variation des capitaux propres et les annexes)
2. Comptabilité des entités administratives : les comptes administratifs

En relation avec la Cartographie des Risques:

1. Risques définis par les entités
2. Risques définis par l'IGF
3. Risques

19.6.2.3 Diagrammes des modelés

Ce diagramme du modèle de déploiement présente un certain degré d'abstraction pour décrire des aspects relatifs à l'architecture, la logique ou le comportement d'un système. Dans l'architecture TI proposée pour l'IGF, nous pouvons distinguer les trois niveaux typiques d'une architecture web:

- couche de présentation
- couche de logique de l'application ou logique des affaires
- couche des données

Les usagers utiliseront toujours des navigateurs web pour se connecter à la couche de présentation. Une interface (un formulaire) sera utilisée pour l'identification et l'authentification de l'usager.

19.6.3 L'échange d'informations

19.6.3.1 Introduction

Dans la structure de l'échange d'information entre l'IGF et les autres organisations, il faut définir trois niveaux:

1. Niveau Organisationnel

2. Niveau Sémantique
3. Niveau Technique

Le prestataire du service du développement de l'application de la base de données des entités doit prendre en compte les trois niveaux et participer à ses développements et définitions.

19.6.3.2 Niveau Organisationnel

Pour l'échange d'information entre l'IGF et les organisations publiques identifiées précédemment, il est nécessaire d'établir un protocole d'accord avec chacune d'elles.

19.6.3.3 Niveau Sémantique

S'il existe un protocole entre l'IGF et l'organisation pour l'échange de l'information concernant les entités de cette organisation, il faudrait définir le langage à adopter. Ce langage serait:

1. XML: pour les données
2. XSD: pour définir la structure des données

D'autres langages peuvent être utilisés tel que XLS ou un autre langage similaire.

19.6.3.4 Niveau Technique

Pour chaque organisation, il faut définir la forme technique à utiliser pour l'échange d'informations. Il est recommandé que la forme technique pour l'échange soit présentée sous forme de lignes de communication sécurisées, privées ou Internet. À défaut, on peut utiliser un support informatique (CD, DVD, USB, etc.) avec des mesures de sécurité appropriées.

20 ANNEXE III: Évolution du Logiciel Suivi des Missions de l'IGF[5]

20.1 Introduction générale

La DMNI (Direction des Méthodes, de Normalisation et de l'Informatique) a développé le Logiciel de Suivi de Missions (LSM), sous forme d'une application Windows (technologie client-serveur), ayant comme objectif le suivi de l'état d'avancement des missions de l'IGF.

Le logiciel LSM est opérationnel mais demeure en état expérimental. Il est utilisé par les Directeurs de Mission, le secrétariat des CGF, la DPAS et le secrétariat du CIGF (environ 20 utilisateurs). L'accès est seulement possible à partir au réseau interne du Ministère de Finances (en incluant aussi les Inspections Régionales liées avec une connexion VPN).

Une mission du projet de jumelage a été consacrée à discuter des possibilités d'amélioration et d'évolution du logiciel actuel. À cette fin, on a organisé des réunions avec des représentants des différents acteurs du système (personnel de la DMNI, personnel de la DPAS, un Directeur de Mission, un Chef d'Inspection et un Contrôleur Général des finances), en analysant les besoins de chacun. Avec les informations reçues, on a préparé une proposition d'évolution du logiciel existant en ajoutant des nouvelles fonctionnalités détaillées dans la présente annexe.

20.2 Évolution Technologique

Voici l'évolution prévue pour l'environnement technologique du logiciel LSM:

- Utilisation des technologies WEB pour le développement du système.
- Implantation d'une architecture trois tiers (couches de présentation, traitement et base des données).
- Intégration avec un sous-système pour stockage, accès sécurisé (https, mécanisme de contrôle d'accès par fichier) et visualisation web des fichiers.
- Dans une première phase, l'interface du système sera monolingue (français). En cas contraire, il faut le prévoir au début du dessin.
- Idéalement, il y aura un déploiement d'une architecture physique avec la redondance des serveurs en parallèle pour assurer la disponibilité et la séparation des environnements (développement, pré-production, production).
- Assurance de backup des données multi-site.

20.3 changements clés de l'évolution fonctionnelle

À l'heure actuelle, le logiciel LSM sert principalement à:

- Stocker le plan annuel des missions sur une base de données.
- Faire la mise à jour de l'état de chaque mission et générer des rapports consolidés automatiquement.
- Faire le suivi de l'activité des inspecteurs.

[5] La version complete de la spécification fonctionnelle de la version 2 de l'application de suivi de missions est accesible à:
https://docs.google.com/document/d/1OmybIYyI5W1xZ9zNoqS6MZGkLqE_bLCJHgQxieL_orw/edit

- Garder la référence des rapports émis.
- Surveiller le temps écoulé dans les missions, ainsi que dans la rédaction, correction et remise des rapports aux destinataires, en activant des alertes quand les temps fixés sont dépassés.

On a identifié les faiblesses suivantes :

- Le logiciel garde seulement l'information pour contrôler l'exécution des missions, mais il ne garde pas l'information produite par la mission (rapports).
- Le système est utilisé par un nombre assez réduit de personnes.
- Le mécanisme d'alertes est faible et est nettement améliorable.
- Le logiciel est orienté vers le contrôle et le suivi de la performance (DPAS, direction) sans inclure les acteurs opérationnels.
- Il y a beaucoup de traitement manuel en parallèle (fiche suivi, rapports).

Les changements clés proposés pour l'évolution fonctionnelle du logiciel LSM sont les suivants:

- La documentation des missions sera stockée en format numérique dans l'application (spécialement les fichiers en format éditable avec les différentes versions des rapports de mission). En conséquence, on pourra offrir la possibilité d'un accès en ligne aux rapports, avec un moteur de recherche implanté sur le logiciel pour trouver des rapports en saisissant le nom de l'entité, le secteur, les dates, etc... Cela sera très utile car le mécanisme actuel pour demander des copies des rapports au Bureau de Conservation des Rapports n'est pas facile et il y a un besoin chez les inspecteurs (spécialement les nouveaux) pour lire des anciens rapports similaires pour apprendre des informations sur l'entité contrôlée ainsi que pour obtenir des bonnes pratiques d'audit, rédaction, analyse….
- Le suivi de mission sera totalement dématérialisé. On évitera ainsi la circulation de la documentation en papier en parallèle (comme par exemple la fiche de suivi), on saisira ce type d'information sur des champs spécifiques sur le logiciel et elles seront stockées pour en faciliter l'exploitation statistique, la gestion automatique des alertes et la programmation des tableaux de bord.

Les principes de sécurité pour le logiciel LSM sont exposés ci-dessous :

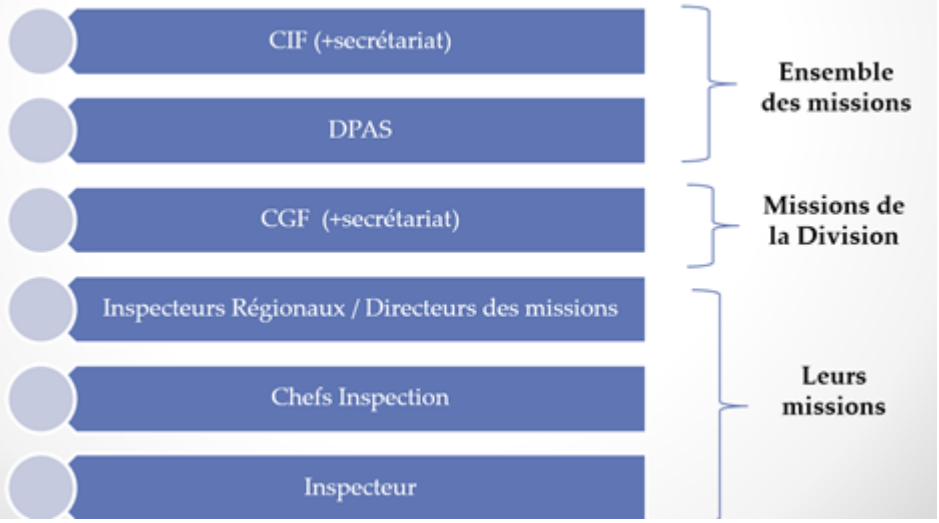
- Le système sera accessible seulement pour les utilisateurs ayant un accès défini pour l'application (réseau interne, accès possible uniquement pour les utilisateurs internes de l'IGF).
- Chaque utilisateur aura un rôle associé au système qui lui donnera des permissions pour accéder exclusivement aux données auxquelles il a droit en fonction de son profil.
- Sécurisation et traçabilité des accès.
- Rédaction des instructions internes de l'IGF pour l'utilisation du système (charte de confidentialité à signer).
- Classification des informations avec des niveaux de sécurité bien définis.

Il y aura différentes interfaces du système en fonction des rôles (profils) associés aux utilisateurs.

En fonction du paramétrage du système et du (des) profil(s) de l'utilisateur, le système

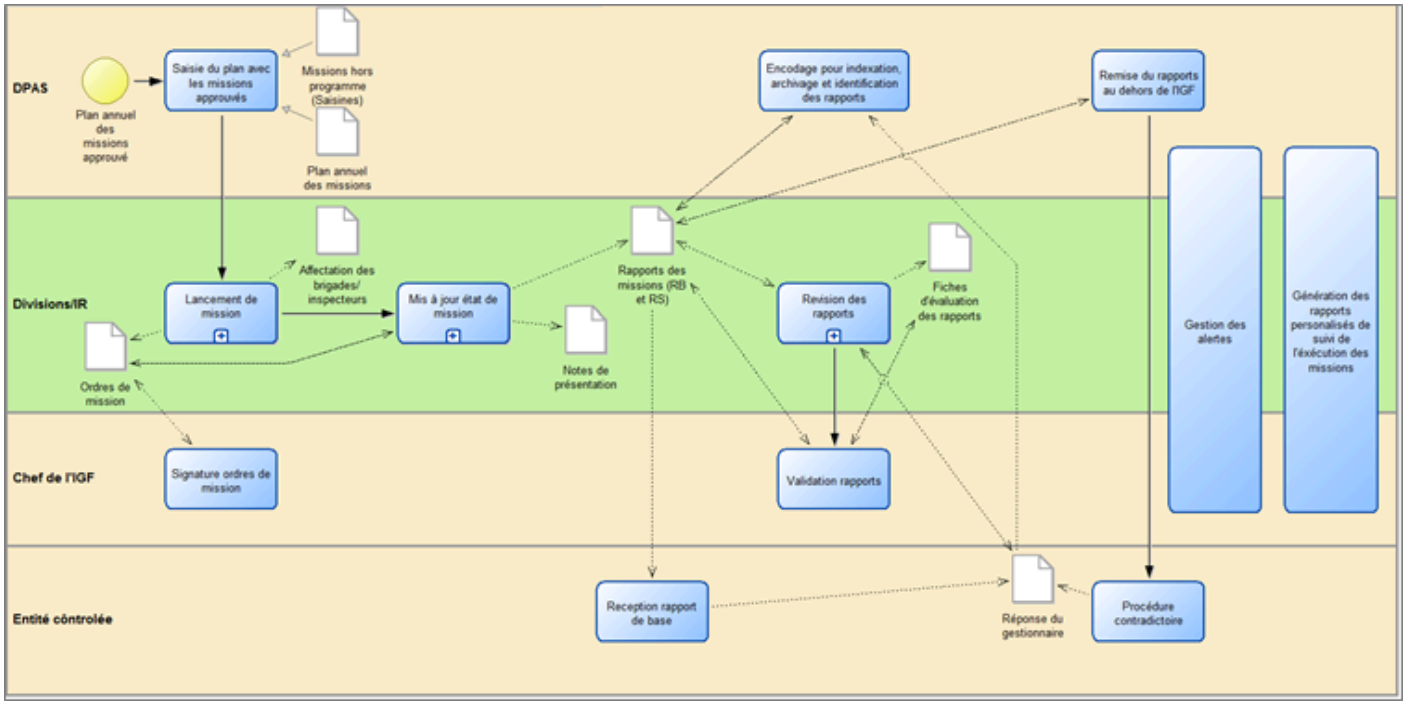
adaptera les menus dynamiquement et proposera différentes fonctionnalités.

Il faudra définir des tableaux profil / fonctionnalités et profil / accès. L'illustration ci-dessous montre un exemple d'accès à l'information en fonction du profil de l'utilisateur.



20.4 Processus et flux principaux

L'illustration suivante les processus et les flux d'information principaux du logiciel LSM :



L'utilisation du logiciel LSM démarre officiellement une fois que le plan annuel des missions et approuvé ; à ce moment, il faut faire la définition de chaque mission sur le système LSM.

> On pourrait envisager dans l'avenir la préparation du plan directement sur le système LSM (élaboration possible par les Divisions des propositions des missions en affectant des brigades et dates prévisionnelles), avec un système de versions qui indiquera s'il s'agit

d'une mission du plan provisoire ou bien d'une mission du plan déjà approuvée.

Le personnel autorisé de la DPAS fait la saisie du plan annuel (février), en entrant les données basiques d'engagement de la mission.

Le logiciel LSM permet aussi d'introduire des missions Hors Programme (saisines).

Au moment du lancement d'une mission, le directeur de la mission saisit sur LSM la date du lancement, la durée prévue et procède à l'affectation du chef de l'inspection et des autres inspecteurs de la brigade.

Le logiciel imprime les formulaires avec les ordres de mission (maximum 30 jours) remplis qui sont traduits en format en papier pour la signature du Chef de l'IGF. Le logiciel peut aussi imprimer le renouvellement des ordres de mission en gardant ainsi une trace de tous les ordres de mission.

On pourrait envisager dans l'avenir la signature électronique des ordres de mission ainsi que le stockage des fichiers numériques signés.

Le directeur de mission (DM) fait la mise à jour de l'avancement de chaque mission, en saisissant l'état de son avancement.

- En cours
- Rapport de Base (RB)en rédaction
- RB en correction
- RB notifié
- En attente de la réception de la réponse du gestionnaire au RB
- RS en rédaction
- RS notifié
- Terminée

Le logiciel LSM actuel ne permet pas de stocker les fichiers avec les rapports numérisés.

Il faudra faire évoluer le logiciel pour stocker les rapports en format éditable.

Le système permet de garder plusieurs dates pour l'exploitation statistique ultérieure:

- Dates début/fin Rédaction du RB
- Dépôt du RB par la brigade au niveau de la Division ou la IR
- Correction du RB au niveau DM/CGF/CIGF
- Notification du RB aux différents destinataires (Gestionnaire, Tutelle, 1er Ministre, Ministre des Finances)
- Date de réception de la réponse du RB

On fera une évolution du logiciel pour informatiser la correction des rapports en gardant de copies avec la version de chaque correction déposée. La fiche de suivi sera informatisée en l'intégrant sur le logiciel.

Le système LSM permet de garder les dates relatives à la rédaction du Rapport de Synthèse pour l'exploitation statistique ultérieure:

- Dates début/fin Rédaction du RS
- Dépôt du RS par la brigade au niveau de la Division ou la IR
- Correction du RS au niveau DM/CGF/CIGF

- Notification du RS aux différents destinataires (Tutelle, 1er Ministre, Ministre des Finances)

On ajoutera des champs pour garder en format texte les recommandations du RS, implémentées ou non, ainsi que des observations.

On pourrait garder plusieurs fichiers associés à une mission (note méthodologique, compte-rendu des missions exploratoires, RB, Fiche de suivi, Réponse du gestionnaire, RS, Décisions du CIGF de convertir le RB en Rapport définitif en cas de non-réception de réponse du gestionnaire, fiche de note de présentation et synthèse pour le 1er ministre, lettres de transmission, Ordres de mission, Documents du Fond de Dossier…).

En ce qui concerne la dématérialisation des documents pour supporter un traitement électronique sans papier, il faudra établir une sécurité équivalente à celle avec le traitement en papier du Bureau de Conservation des Rapports, avec traçabilité et préservation de la confidentialité, en faisant confiance aux inspecteurs.

En ce qui concerne la numérisation des anciens rapports, il est envisagé de numériser un maximum de 10 ans en arrière. Il faudra ajouter un NIVEAU DE CONFIDENTIALITÉ sur les rapports pour avoir des mesures spéciales pour certains rapports. Il faudra aussi définir une politique de backup des données multi-site (par exemple avec des copies sur une IR sans risque sismique).

Le système LSM permet d'exploiter les données des dates d'exécution pour générer des rapports dynamiques avec le détail des missions et l'activité des inspecteurs.

En utilisant ces dates, le système affiche des alertes personnalisées chaque fois qu'on dépasse des limites préfixées.

Il faudra faire évoluer le logiciel pour envoyer des alertes automatiques par courriel aux personnes concernées.

20.5 Fonctionnalité pour la direction (CIF/ DPAS/ CGF/ IR):

Voici la fonctionnalité envisagée pour la direction :

- Chargement/édition des données principales du plan annuel des missions (fiche « engagement de mission »):
  - Structure en charge de la mission: (Division, IR)
  - Secteur
  - Organisme contrôlé
  - Objet de la mission (intitulé)
  - Objectif/motivation de la mission
  - Type de mission
  - Mission du programme annuel /Hors Programme
  - Mission ayant Procédure Contradictoire/mission Sans Procédure Contradictoire
  - Date de la programmation / Date de la saisine
  - Demandeur de la saisine (en cas de saisine)
  - Edition/Modification des données protégées (tableaux de codification; exemple: types de mission, structure IGF, …)
- Génération des rapports de suivi de l'exécution du plan
- Génération des rapports de suivi de l'activité d'un inspecteur/Chef d'inspection

- Génération des rapports d'activité et Tableaux de bord
- Gestion des utilisateurs (profils, permissions basés sur hiérarchies internes)

20.6 Fonctionnalité pour les directeurs de mission:

Voici la fonctionnalité envisagée pour les Directeurs de Mission –phase de lancement de la mission

- Affectation des brigades aux missions, avec souplesse car la composition des brigades peut changer pendant l'exercice
- Gestion des inspecteurs, chefs d'inspection et des brigades
- Saisie de la date de début effectif de la mission
- Gestion des ordres de mission:
    - Lancement des ordres de mission et programmation des alertes avant le jour de renouvellement de l'ordre
    - Téléchargement du document Rapport d'étape (compte-rendu pour le renouvellement des ordres de mission)
- Téléchargement des fichiers avec des documents importants pour la mission:
    - Note méthodologique
    - Compte-rendu des missions exploratoires
    - Documents du Fond de Dossier
- Génération des rapports d'activité et Tableaux de bord

Voici la fonctionnalité des Directeurs de Mission –phase de rédaction, correction et dépôt du RB

- Saisie de l'état d'avancement de la mission ainsi que des dates de l'exécution des activités de contrôle (début de rédaction, correction et dépôt du RB: circuit Unité opérationnelle-CGF/IR-CIF Rapport de Base).
- Génération automatique des lettres de transmission
- Téléchargement des différentes versions des fichiers après chaque niveau de correction:
    - Rapport de Base
    - Note de Présentation et synthèse au 1er ministre
    - Lettres de transmission
- Saisie de la fiche de suivi (texte d'évaluation + note numérique entre 10 et 20) au fur et à mesure qu'on avance avec les corrections
- Génération des rapports d'activités et Tableaux de bord

Voici la fonctionnalité des Directeurs de Mission –phase de rédaction, correction et dépôt du RS

- Saisie de l'état d'avancement de la mission ainsi que des dates de l'exécution des activités de contrôle (réception des réponses du gestionnaire, début de rédaction, correction et dépôt du RS: circuit Unité opérationnelle-CGF/IR-CIF Rapport de Synthèse).
- Génération automatique des lettres de transmission
- Téléchargement des différentes versions des fichiers après chaque niveau de correction:
    - Rapport de Synthèse

- Lettres de transmission

- Saisie de la fiche de suivi (texte d'évaluation + note numérique entre 10 et 20) au fur et à mesure qu'on avance avec les corrections
- Saisie des recommandations, en format texte, registres « intitulé recommandation/ acceptation par l'organe contrôlée / observations »
- Génération des rapports d'activités et Tableaux de bord

Voici la fonctionnalité des Directeurs de Mission –phase de rédaction, du rapport spécial annuel

- Saisie de l'état d'avancement de la mission ainsi que des dates de l'exécution des activités de contrôle (réception des réponses de la tutelle).
- Téléchargement des fichiers avec le plan d'action envoyé par la tutelle et l'analyse du directeur de mission de l'efficacité du plan d'action proposé.
- Consolidation d'un squelette de rapport spécial en tenant compte de l'analyse téléchargée par les directeurs de mission.

20.7 Fonctionnalité pour les inspecteurs

Voici la fonctionnalité envisagée pour les inspecteurs :

- Moteur de recherche de documentation des missions en saisissant le nom de l'entité, le secteur, les dates, etc.
- Le système, en fonction des permissions définies, donnera accès aux documents associés à une mission (par exemple le Rapport de Base)
- Les accès aux documents seront tracés.
- Idéalement, les documents affichés pourront avoir une filigrane avec le nom de l'utilisateur ayant demandé l'accès au document.
- Cette fonction sera aussi disponible pour les profils supérieurs

20.8 Avantages des nouvelles fonctionnalités envisagées:

La solution proposée permettra à l'IGF de:

- Améliorer sa performance en réduisant le traitement manuel
- Partager l'expertise contenu dans les rapports anciens car la simplicité de la consultation on-line des rapports facilite énormément l'accès aux dossiers.
- Réduire le risque de disparition des rapports (en cas de catastrophe dans le Bureau de Conservation des Rapports tout sera perdu).
- Obtenir facilement des tableaux de bord et des rapports pour évaluer la performance de l'IGF et identifier des points faibles.
- L'intégration de la fiche de suivi dans le logiciel permettra de calculer automatiquement des notes moyennes de la performance des inspecteurs et des chefs d'inspection.
- L'intégration des recommandations du RS, (ainsi que son acceptation par le gestionnaire) sur le logiciel permettra d'avoir d'un indicateur précis de l'efficacité des missions.

Les prochaines actions proposées sont:

- Avancer avec les spécifications fonctionnelles de haut niveau, en coopération avec

l'équipe algérienne, avec l'objectif d'élaborer des spécifications plus détaillées qui seront la base d'un futur cahier des charges.

- Se coordonner avec les experts des autres missions pour intégrer le Logiciel de Suivi des Missions avec d'autres systèmes d'information de l'IGF.

21 ANNEXE IV: Spécifications fonctionnelles pour la planification annuelle des missions de l'IGF[6]

21.1 Introduction générale

Le Plan Annuel d'Audit de l'IGF est soumis à une procédure à laquelle participent plusieurs intervenants, et qui est structurée en différentes phases. Le présent document a pour but de proposer les spécifications fonctionnelles pour le développement d'un logiciel, permettant de gérer et coordonner l'ensemble des processus qui, finalement, se matérialisent dans le plan.

Ce projet devrait servir de cadre pour automatiser la grande partie de la procédure, compte tenu des flux de documentation et des différents niveaux de responsabilité des intervenants, avec l'objectif final de rationaliser les processus au moyen de l'exécution d'opérations à travers un système d'information.

La principale source d'information du logiciel est la base de données d'entités, c'est pourquoi ce projet établit une connexion fondamentale entre les deux éléments. D'un autre côté, le résultat final généré par ce logiciel, le plan annuel d'audit, est le point de départ pour le logiciel de suivi des missions.

21.2 Schéma de la procédure

La description des processus répond à une réglementation interne, définie comme suite :

- À la mi-novembre de l'année « n », le Chef de l'IGF invite les Contrôleurs Généraux (CG) et les Inspecteurs Régionaux (IR) à transmettre des propositions pour former un avant-projet de liste d'entités. Les ministères peuvent aussi envoyer des propositions. Ces propositions viennent de trois sources différentes :

    - Les **saisines** (hors programme) parvenues durant l'année « n » et à programmer pour l'année « n+1 ».
    - Les **RAR** sur l'exercice en cours à reconduire.
    - Le **reste d'entités** (nouvelles propositions d'intervention, dûment motivées) qui sont sélectionnées sur la base de critères différents.

Il existe actuellement dix-neuf critères d'élaboration du programme annuel d'action de l'IGF (qui ont été définis pour le programme d'action de l'année 2009) :

> 1. Les reliquats des programmes d'actions antérieurs (après retraitement);
> 2. Les saisines ;
> 3. Les propositions hiérarchisées des membres du gouvernement ;
> 4. Les grandes opérations inscrites au programme de développement ;

[6] La version complete de la spécification fonctionnelle du module de planification annuel des missions est accesible à:
https://docs.google.com/document/d/16wmLxlxtS53GcchvEaiNn-79eSd71Wo1dkWRcK9ecDE/edit

5. La mise en œuvre des politiques publiques;

6. Les comptes d'affectation spéciale (suivant leur importance);

7. Les saisines du secteur économique et des autres établissements publics entrant dans le champ d'intervention de l'IGF ;

8. Les thèmes d'actualité ;

9. L'importance au plan financier ;

10. Les opérations clôturées ;

11. Les présomptions ;

12. La périodicité des contrôles ;

13. Les affaires récurrentes (audits de prêts extérieurs, mises en application des résolutions des AGO et AGE au niveau des banques et assurances publiques) ;

14. Les secteurs gisements;

15. Les actes des investigations antérieures ;

16. L'Aide à la décision ;

17. La réglementation des changes;

18. L'obligation de contrôle périodique des administrations et organismes placés sous l'autorité ou la tutelle du ministre chargé des finances (article 11 du décret nº 08-272 du 06/09/2008 fixant les attributions de l'IGF) ;

19. Les recommandations des cadres et inspecteurs de l'IGF.

Les structures opérationnelles ont un délai maximal de quinze jours pour fournir leurs propositions.

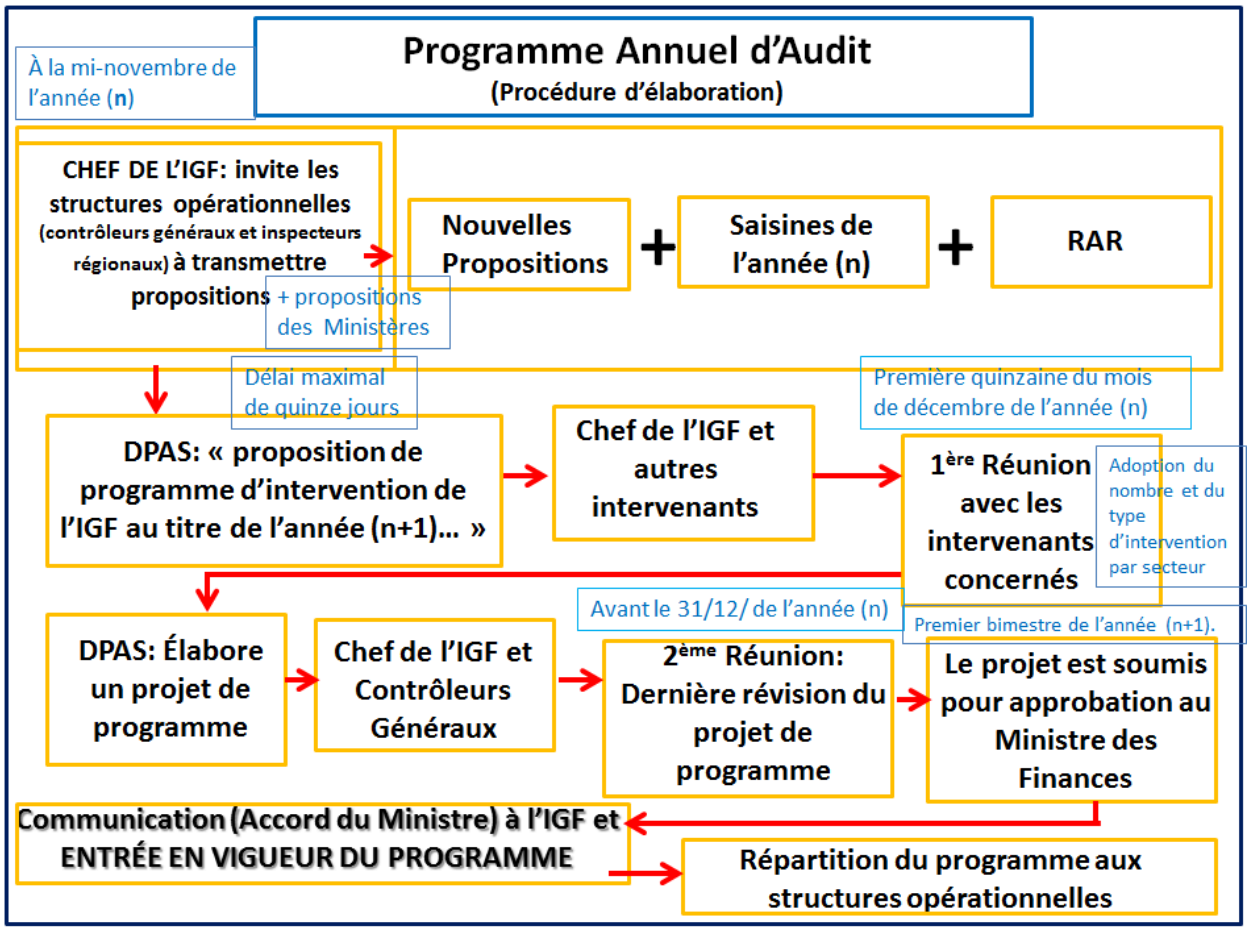
- Avec l'information reçue, la DPAS élabore un premier document, « Proposition de programme d'intervention de l'IGF au titre de l'année n+1 », qui est envoyé au Chef de l'IGF et à d'autres intervenants pour lecture et avis. Ce document synthétique (un tableau consolidé) reprend par secteur d'activité les RAR, les saisines à engager ainsi que les propositions (CG et IR).

- Au cours de la première quinzaine du mois de décembre de l'année « n », le Chef de l'IGF organise une première Réunion avec les intervenants concernés (les Contrôleurs Généraux, les Directeurs de Missions, les directeurs de structures et les Inspecteurs Régionaux), au cours de laquelle on adopte le nombre et les types d'intervention par secteur.

- À partir des documents dérivés de cette réunion-là, la DPAS élabore un projet de programme, qui est transmis au Chef de l'IGF puis aux Contrôleurs Généraux, dans lequel seront reprises toutes les opérations retenues lors de la première réunion en indiquant les structures susceptibles de les prendre en charge.

- Avant le 31/12/ de l'année « n », le Chef de l'IGF organise une seconde réunion pour faire une dernière révision du projet de programme.

- Au cours du premier bimestre de l'année « n+1 », le projet est soumis pour approbation au Ministre des Finances.
- Une fois approuvé, l'Accord du Ministre est communiqué à l'IGF.
- Finalement, le Chef de l'IGF procède, après avoir consulté éventuellement les Contrôleurs Généraux des Finances, à la répartition du programme sur les structures opérationnelles Centrales et Régionales, pour son exécution.



21.3 Structure du logiciel

Le logiciel est conçu comme un système intégré, dans un environnement de type web, composé de trois modules distincts mais complémentaires:

- **MODULE 1: SÉLECTION DE L'ÉCHANTILLON D'ENTITÉS.**

Ce module est préparé pour la sélection des entités qui constituent les nouvelles

propositions. Il y a plus de 11.000 entités qui peuvent potentiellement être auditées par l'IGF et qui sont déjà intégrées dans la base de données des entités (BDE).

Il s'agit de choisir un échantillon relativement modeste par rapport à la population initiale. Dans ce cas, une sélection qui utilise des critères exclusivement statistiques peut s'avérer insuffisante car l'échantillon ne pourra probablement pas répondre à des critères stratégiques.

Il faut donc prendre en compte des critères qui ont été définis par l'IGF (dix-neuf critères). Le Module 1 disposera ainsi d'une fonctionnalité pour la sélection d'une population cible, plus réduite, qui peut être configurée à partir de critères stratégiques, et qui permettra de définir des différents scénarios selon les critères choisis.

Limites de la démarche actuelle :

- Méthode de sélection non formalisée.
- A l'exception de l'obligation imposée aux DM de justifier leurs propositions, il n'y a aucun critère favorisant un choix judicieux des propositions : fréquences d'intervention, couverture maximale de la BD des entités
- Risque de subjectivité des propositions.

Réponses :

- Construction pour chaque secteur d'une fonction de risque des entités.
- Mise en place de certains critères : fréquences d'intervention, fonction de risques, couverture des entités du portefeuille.
- L'échantillon de base est établi par la DMNI, suivant une approche statistique, et communiqué au DM. Cet échantillon représente pour ce dernier le domaine de définition de ses propositions.

Fonction de risque par secteur

On estime nécessaire la mise en place d'une fonction de risque par secteur, qui doit permettre d'attribuer à chaque entité un score qui sera sauvegardé dans un champ de la base de données des entités. Le valeur de ce score sera comprise entre 0 et 5, avec 5 comme maximum de risques (5 étant aussi la valeur par défaut).

Sélection de la population cible (N)

En s'inspirant du concept d'intelligence économique, les utilisateurs pourront indiquer les critères pour faire une première sélection d'entités. Chaque combinaison de critères établit un scénario différent.

Il est indispensable que les critères stratégiques puissent être définis sur les champs de la base de données. Par conséquent, il faut considérer ces critères au moment de configurer la base de données d'entités (BDE).

La population cible est un sous-ensemble de la population initiale, qui est formée au moyen d'une sélection basée sur des critères stratégiques.

Sélection de l'échantillon d'entités (n)

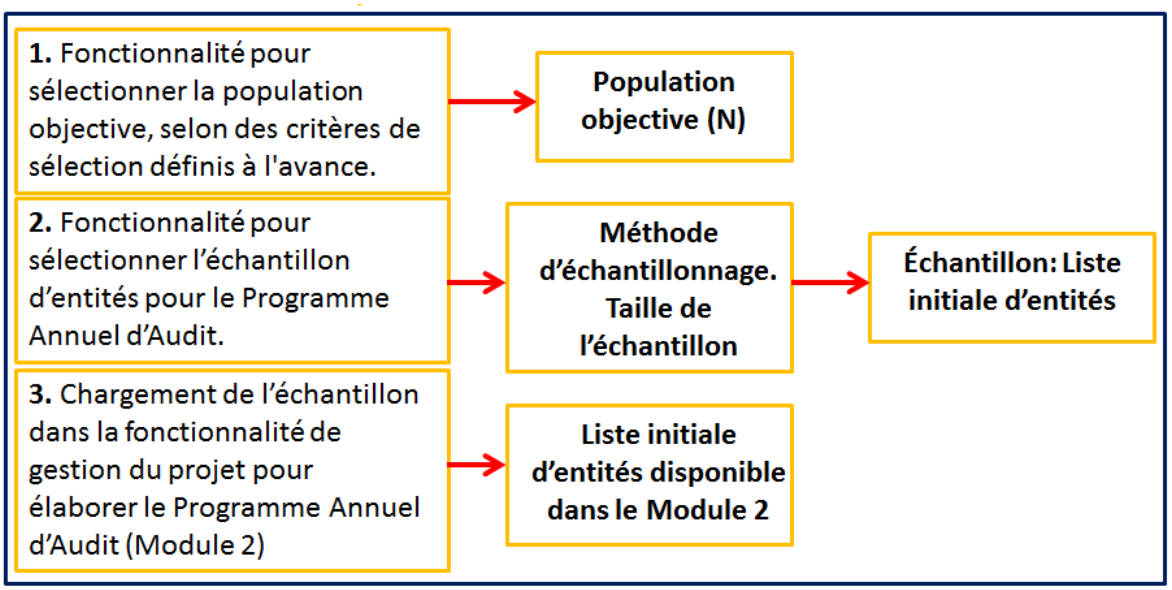
Il faut tenir compte du fait que la liste finale d'entités du plan annuel ne dépasse pas les 200 éléments (par exemple), et qu'il est donc probable qu'une nouvelle sélection soit nécessaire. Cette valeur sera sauvegardée dans un champ de la BDE et pourra être ajustée selon les besoins. Après l'emploie de critères stratégiques, on peut appliquer des critères statistiques pour obtenir un échantillon représentatif du scénario choisi.

Cela pourrait se faire en utilisant l'échantillonnage aléatoire simple, mais pour avoir un échantillon qui soit plus représentatif de la population cible (scénario), il est recommandé d'utiliser un échantillonnage aléatoire stratifié.

Il faut identifier au moins un critère de stratification. La variable « secteur » est considérée comme le principal critère de stratification, mais peut aussi être utilisée la variable « zone géographique » pour faire une double stratification (voir livrable de l'activité A1.2).

Caractéristiques techniques du Module 1

- Une connexion à la base de données d'entités doit être activée.
- Incorporer une fonctionnalité de type « intelligence économique », qui permet de faire une première sélection (population cible) basée sur des critères à partir des champs de la base de données d'entités. Cette fonctionnalité doit être conçue pour une utilisation intuitive par les usagers.
- Intégrer dans le module des algorithmes statistiques pour la sélection d'échantillons au moyen de l'échantillonnage stratifié. La fonctionnalité doit permettre la sélection des variables de stratification de l'échantillonnage dans chaque strate.
- Définir les fonctions de risque sectorielles et créer un algorithme pour ces fonctions.



Téléchargement de la liste d'entités dans le Module 2

Une fois la liste d'entités élaborée, elle est téléchargée (elle peut être déjà utilisée) dans la fonctionnalité de gestion du projet pour élaborer le Programme Annuel d'Audit (Module 2).

- **MODULE 2: GESTION DU PROJET DE PROGRAMME ANNUEL.**

L'objectif de ce module est de mettre en place un système pour gérer les différentes phases de l'élaboration du programme. C'est un module dynamique, qui informe les utilisateurs (via courrier électronique) lorsqu'ils doivent faire une révision de la documentation. La documentation est toujours traitée en format numérique.

Lorsque le Chef de l'IGF invite les Contrôleurs Généraux et les Inspecteurs Régionaux à transmettre leurs propositions pour le programme de l'année « n+1 », la communication du Chef est téléchargée dans le module 2, et le logiciel envoie un courrier électronique aux intervenants.

Dès que les CG et les IR sont alertés, ils accèdent à la documentation numérisée (la liste des entités choisie), ajoutent leurs propositions et téléchargent le document, qui est adressé à la DPAS.

La DPAS, gestionnaire de cette application, met le document synthétique à la disposition du Chef de l'IGF et des différents intervenants pour lecture et avis.

La documentation générée à l'issue des réunions de planification, organisées par le Chef de l'IGF, est mise à la disposition de l'IGF, qui élabore un projet de programme et qui le joint au module, en informant les intervenants par courrier électronique.

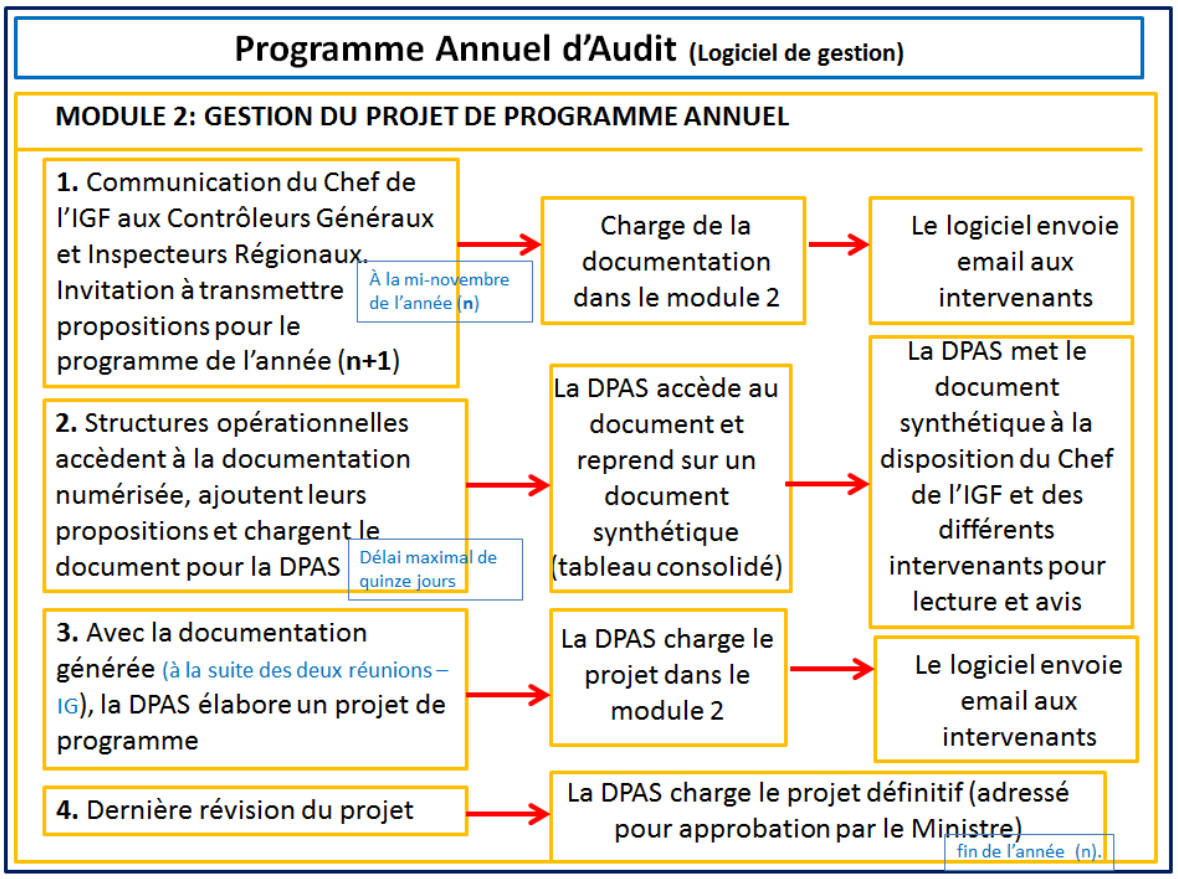
Lors de la dernière révision par les intervenants, la DPAS télécharge le projet définitif qui est adressé, pour approbation, au Ministre des Finances.

Fonctionnalités techniques du Module 2

- Automatiser toutes les phases de la gestion du projet du plan annuel, en s'appuyant sur des modèles de *workflow*.
- Gérer des processus cohérents qui garantissent la fiabilité et accélèrent la distribution de la documentation entre les intervenants.
- Incorporer la fonctionnalité de notification automatique par courrier électronique.
- Permettre le chargement de la version finale du PPA.
- Permettre l'impression des états de sortie du PPA (avant et après discussion finale).
- Fonctionnalités supplémentaires :

    - Chargement de la lettre du chef de l'IGF et du canevas sur le logiciel.
    - Sélection de la population « cible » par DMNI.
    - Sélection de l'échantillon de contrôle par Directeur de Mission (DM) ou IR.
    - Choix du mode d'intervention : CG, Audit, évaluation.
    - Choix de l'étendue d'intervention : globale ou thématique.

- Chargement des nouvelles propositions.
- Chargement de la justification du DM en cas d'écartement de la population de cible.
- Chargement des RAR.
- Chargement des saisines de l'année « n ».
- Donner la possibilité de choisir entre une intervention générale et une intervention thématique
- Proposer, à toute fin utile, une liste de thématiques de contrôle.
- Donner la possibilité aux utilisateurs de charger (ou saisir) les informations /documents relatifs à ces tâches.
- Permettre au DM d'envoyer les états sectoriels au CG.
- Permettre aux CG d'envoyer les états sectoriels à la DPAS.
- Permettre une consolidation automatique des états sectoriels de proposition (format à définir).
- Possibilité d'imprimer l'état consolidé (état de sortie).
- Permettre de charger le projet de programme adopté après discussion sur le Module GESTION DU PROJET DU PROGRAMME.



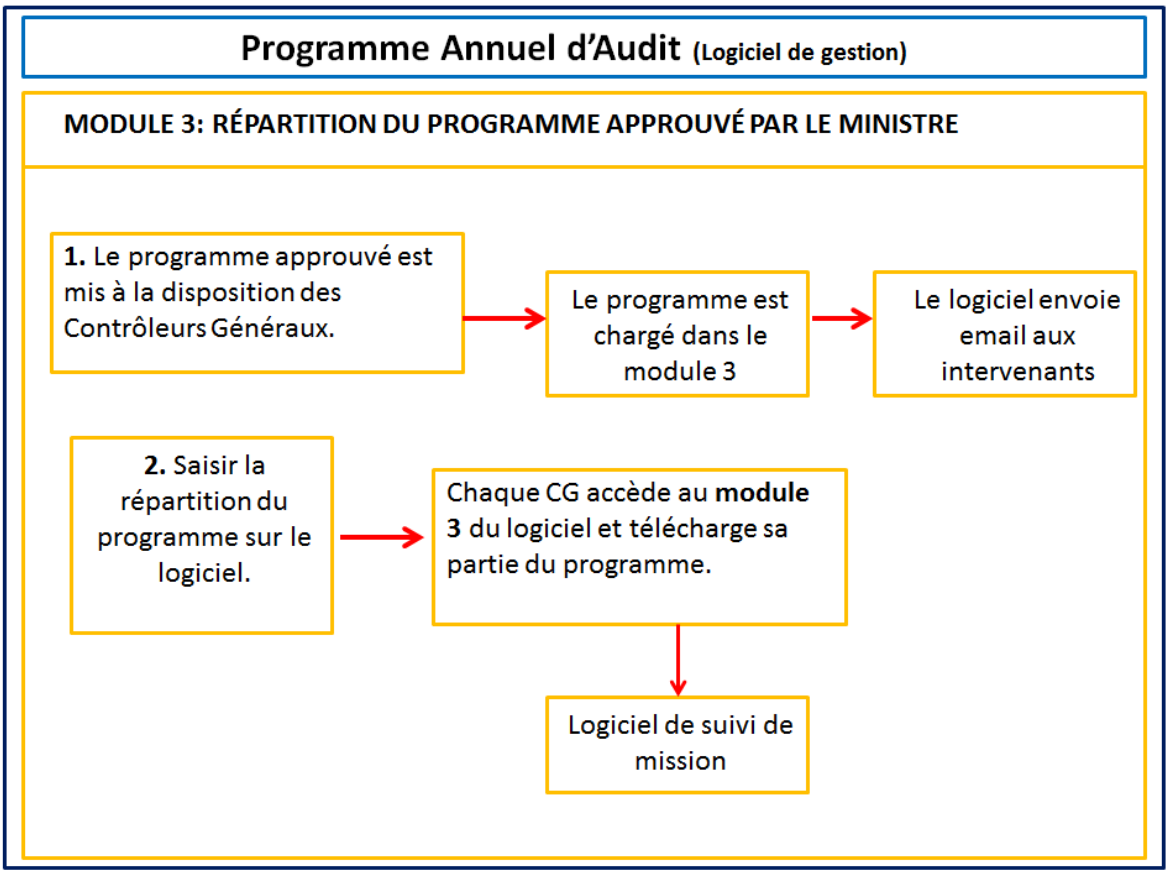
- **MODULE 3: RÉPARTITION DU PROGRAMME APPROUVÉ PAR LE MINISTRE.**

L'objectif de ce module est de mettre à disposition des responsables des structures opérationnelles leur partie du programme, pour la télécharger et la mettre exécution.

Le programme approuvé est mis à la disposition des Contrôleurs Généraux dans le module 3, qui envoient notification par e-mail aux intervenants.

Chaque Contrôleur Général accède au module 3 du logiciel et télécharge sa partie du programme, pour son exécution.

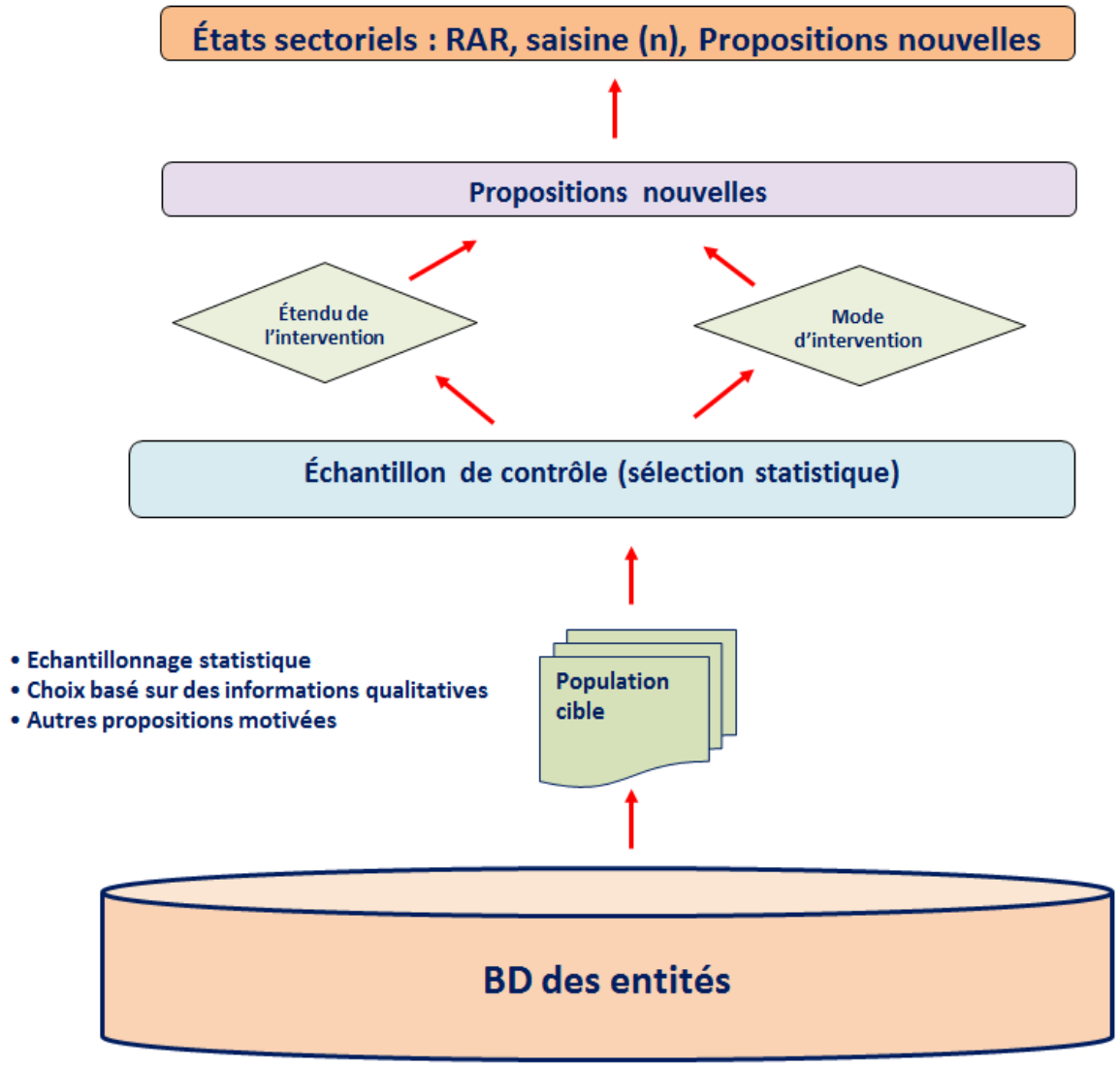
Finalement, les unités opérationnelles exécutent le plan au moyen du logiciel de suivi de mission.



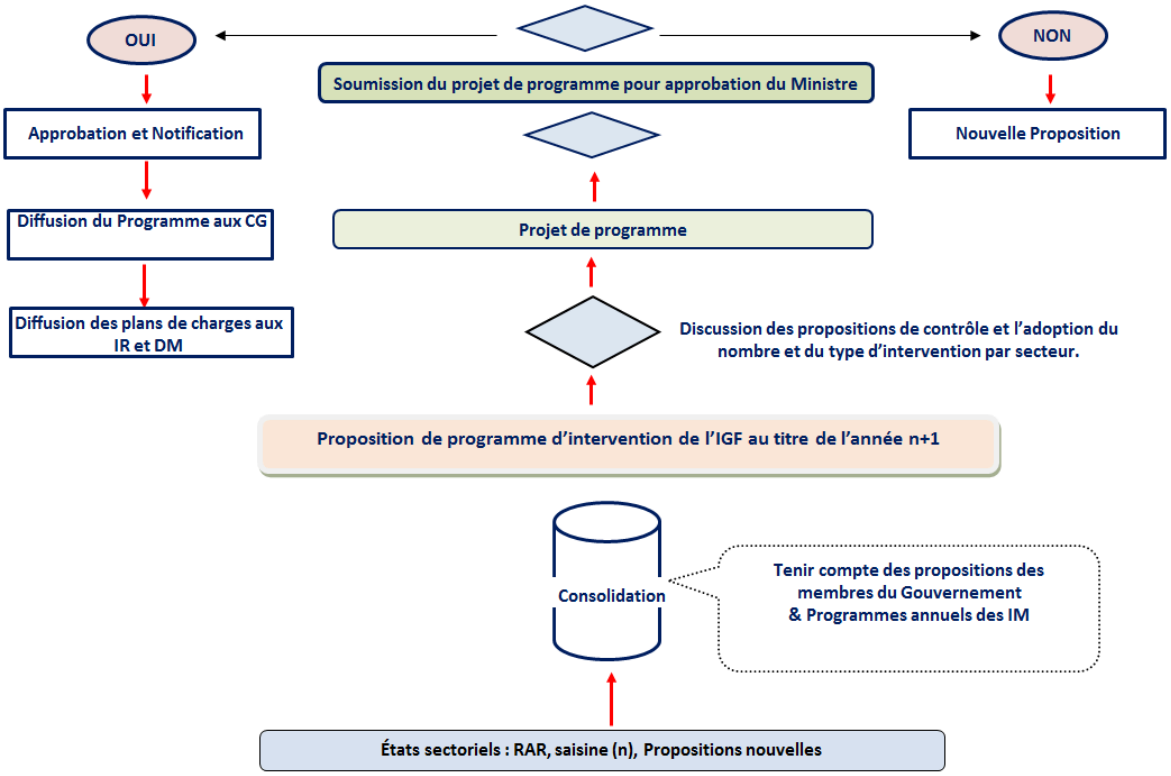
Fonctionnalités techniques du Module 3

- Donner la possibilité de télécharger le programme (approuvé et notifié) sur le module «Répartition du programme approuvé »
- Permettre la diffusion du programme sur les CG.
- Permettre la saisie de la répartition du programme sur les structures opérationnelles.

21.4 Propositions (liste d'entités).



21.5 Programme Annuel d'Audit (Flux d'information)



22 ANNEXE V: Spécifications fonctionnelles de l'INTRANET[7]

22.1 Introduction

L'Intranet est le point d'accès des employés de l'IGF à leur organisation.

Ce document dresse une proposition de structure de contenus pour le "prototype" de l'Intranet à mettre en oeuvre par l'IGF le plus tôt possible.

La section 2 "**sections principales**" doit donc servir comme référence pour envisager les différents volets à inclure dans ce prototype. Parmi elles, tout ce qui est relatif au **Guide de fonctionnement et de l'Organisation de l'IGF** à savoir le manuel d'organisation, le manuel d'intervention, le code de déontologie, mais aussi la liste de textes légaux, des documents modèles d'usage quotidien pour les télécharger, des nouvelles, des widgets pour l'accès aux applications à développer ou déjà développées et finalement, l'accès aux informations d'intérêt par rapport à la Formation des ressources humaines de l'IGF.

Lors des missions de l'activité du projet de jumelage, les experts espagnols ont animé des ateliers techniques concernant **l'implantation d'un CMS** (Content Management System) pour aider l'équipe technique de l'IGF à démarrer les travaux pour ce prototype-intranet.

Les concepts de catégories et "tags" sont très importants pour permettre une classification du contenu qui facilitera par la même occasion sa localisation et/ou sa récupération. Dans l'annexe 7, il y a une première relation établie entre les **catégories**, **tags** et nom de **pages**.

Par rapport à la **sécurité**, le prototype-intranet doit être conçu en tenant compte des recommandations de sécurité publiées dans le Plan Directeur des Systèmes d'information.

Néanmoins, il faut souligner que le prototype-intranet n'est pas accessible à partir d'Internet. Tous les systèmes d'information installés à l'IGF peuvent uniquement être accessibles localement ou à travers d'une passerelle VPN sécurisée (DSI).

En plus, la plupart des répertoires proposés sont d'accès public pour les employés de l'IGF; il pourrait cependant avoir des sections plus sensibles dont l'accès n'est autorisé qu'à certains types d'usagers (voir 4.1 **rôles et usagers**).

Pour la rédaction, l'édition et la publication du contenu sur l'Intranet, il est proposé de suivre un **circuit d'approbation** (voir section 4 **Organisation**).

Finalement, les applications à développer par l'IGF doivent être accessibles à travers l'Intranet, pour faciliter *l'utilisation* du système tel que décrit dans la section 3 réservée à l'**accès aux systèmes d'information**.

[7] La version complète de la spécification fonctionnelle de l'Intranet est accesible à: https://docs.google.com/document/d/1oBUEPVn2MgYSxcOfswwz5-vHz2AVy3cdbwv_DfUj0SM/edit#

22.2 Sections principales

22.2.1 Accueil

Il s'agit de la page principale de l'intranet.

Elle doit donner accès de manière facile et intuitive à toute la fonctionnalité offerte par l'IGF. Elle doit aussi se positionner comme une interface dynamique incitant les usagers à lui porter une attention particulière.

La structure de cette page (le *layout*) changera en fonction des besoins de publications dans l'Intranet.

L'Éditeur Intranet et le Webmaster doivent faire en sorte que les pages les plus importantes de l'Intranet soient facilement visibles et accessibles.

22.2.2 Accès à la législation

Il y sera aussi possible d'accéder à toute la législation (lois, ordonnances, avis et instruction, différents codes…) que l'Éditeur Intranet pense être d'utilité pour les inspecteurs, y compris les :

- Réglementation
  - Textes de création et statut particulier
  - lois, décrets, arrêtés, ordonnances, …
  - avis,
  - différents codes,
  - notes internes émanant du Ministre des Finances.
  - …
- Actes administratifs internes
  - Manuel des procédures,
  - Notes internes émanant du Chef de l'IGF,
  - Instructions du Chef de l'IGF,
  - Décisions du Chef de l'IGF
  - Conventions et protocoles d'accord avec des fournisseurs d'information.
  - ...

Il pourrait aussi contenir une petite description du document toujours avec la possibilité de télécharger le fichier en format pdf.

22.2.3 Guide de fonctionnement et de l'organisation

Le guide de fonctionnement est la compilation de toute l'information pertinente pour les inspecteurs et qui leur permet de réaliser leur travail et de mener leurs interventions.

Il est à noter que la structure du Guide de fonctionnement est en phase d'élaboration et qu'il y aura donc des changements qui y vont être apportés dans l'avenir.

Ce guide est décliné en plusieurs chapitres/sections qui se présentent comme suit :

22.2.3.1 Le Manuel d'Organisation

- Mission: Qui sommes-nous?
- Vision
- Cadre normatif
- Organisation interne
  - Le cadre organique présentant l'organigramme,
  - le tableau des emplois,
  - des compétences et qualification des agents,
  - les fiches fonction, les fiches département,
  - etc …
- Comité d'audit
- Comités de travail
- Procédures de travail
- ...

22.2.3.2 Le Manuel d'Intervention de l'IGF et guides spécifiques

- Programme des missions annuelles
  - Plan de réalisation
- Ordre de mission
- Étude préliminaire
- Note d'orientation. Programme de travail (note méthodologique)
- Réunion d'ouverture
- Étude de terrain
- Présentation des conclusions
- Projet de rapport. Réunion de clôture
- Rapport de base
- Rapport définitif avec recommandations (rapport de synthèse)
- Programme d'actions de progrès
- Suivi des recommandations et des actions de progrès
- Guides spécifiques:
  - Notes d'organisations par type de missions.
  - Fiches techniques de contrôle (dépense publique ; marché public…etc.)
  - ...

22.2.3.3 Le Code de déontologie

22.2.4 Les Comités de travail de l'IGF

Cette section présentera les travaux d'amélioration, de normalisation et d'adaptation aux normes internationales des différents Comités de travail de l'IGF :

- La liste des inspecteurs et leurs responsables
- Le calendrier des activités
- Les propositions
- Des nouvelles

22.2.5 Modèles de documents de travail

Le système d'information de l'IGF doit inclure un nombre important de documents indispensables au bon déroulement des missions et à l'amélioration de la communication au sein de l'institution. Cependant, eu égard à la particularité de certains de ces documents, notamment leur caractère confidentiel, l'accès à ces derniers peut être limité à une certaine catégorie, en fonction des prérogatives.

Dans l'Intranet paraîtra la liste des documents-modèles disponibles, avec la description et les recommandations pour leur utilisation. En tout temps, l'usager pourra télécharger le document-modèle:

- Modèles de plans relatifs aux différents documents de missions : (accès libre)
  - Note de présentation et de synthèse ;
  - Note méthodologique;
  - Compte rendu d'étape ;
  - Rapport d'étape ;
  - Rapport de base (contrôle de la gestion et/ou évaluation) ;
  - Rapport d'expertise judiciaire ;
  - Rapport d'enquête ;
  - Rapport particulier ;
  - Rapport de synthèse.
- Fiches révisées figurant sur le manuel des procédures : (accès libre)
  - Demande de renseignement ;
  - Mises en demeure ;
  - PV de carence ;
  - PV de vérification de caisse ;
  - PV d'infraction à la législation de change ;
- Fiches de suivi et d'évaluation de la mission. (accès limité)
- ...

22.2.6 Rapports de l'IGF

- Rapports annuels
- Rapports spéciaux
- Autres types de rapports publiés par l'IGF
- Statistiques et bilans d'activité

Les rapports de mission ne seront pas accessibles directement via l'intranet mais plutôt à travers des applications SI (BDE, Suivi,...). Ici, sera offerte la possibilité de montrer de l'information générale sur le rapport des missions et, au besoin, renvoyer le lecteur à un rapport spécifique.

Pour les autres rapports, l'Intranet présentera une description sous forme de texte et offrira la possibilité de télécharger le rapport. Seront aussi présents les rapports de toutes les années précédentes.

Dans le cas de rapports spéciaux, des mesures de sécurité additionnelles seront mises en vigueur.

La page des statistiques sera quant à elle dédiée à des études relatives à l'activité de l'IGF.

22.2.7 Formation

L'information par rapport à la Formation est de la responsabilité de la DAM.

Dans cette première phase, il n'y aura pas de connection directe avec les systèmes de la DAM. L'Éditeur Intranet devra d'abord obtenir l'information nécessaire hors ligne, pour ensuite pouvoir la publier dans l'Intranet en format HTML ou PDF.

L'information suivante sera primordiale et susceptible d'être publiée :

- Plans de formation (annuels et pluriannuels)
- Formulaire pour la proposition de thèmes
- Formulaire pour les demandes de participation à des sessions de formation
- Calendrier des activités de formations
- Offres de formation à l'étranger.
- ...

Les formulaires et le calendrier seront sous forme widget et devront être intégrés dans le système.

22.2.8 Nouvelles

Cet élément offrira un grand dynamisme au site.
L'Éditeur et/ou le Webmaster devront publier des articles portant sur les :

- evénements,
- collaborations

- assises
- séminaires
- réunion du conseil de direction
- informations sur les projets de l'IGF
- appels à candidatures
- appels d'offres
- instructions de l'IGF
- notes de services
- annonces sur des oeuvres sociales

La date de publication et l'auteur seront toujours mentionnés. Il serait aussi important que des catégories et des "tags" puissent paraître pour permettre de mieux classifier l'article.

22.2.9 Calendrier des événements

Un widget montrera le calendrier des activités et des événements.

22.2.10 Forum de l'inspecteur

Un espace sera réservé au signalement des problèmes et des questionnements liés aux missions.

22.2.11 RRHH - Gestion de carrière

L'information par rapport aux Ressources humaines est de la responsabilité de la DAM.

Dans cette première phase, il n'y aura pas de connection directe avec les systèmes de la DAM. L'Éditeur Intranet devra d'abord obtenir l'information nécessaire de manière hors ligne, pour la publier ensuite dans l'Intranet en format HTML ou PDF.

L'information suivante sera importante et susceptible d'être publiée :

- Répertoire des employés de l'IGF (adresse email et n° de téléphone). (accès libre)
- Dossiers administratifs du personnel de l'IGF (PV d'installation ; Arrêté de nomination ; Arrêté de détachement ; Décisions d'intérim….etc.) (accès limité)
- Situation des inspecteurs (par division/ par inspection régionale) (accès limité)
- Promotion (passage de grade, échelons….) (accès limité)
- Information d'ordre normatif (accès libre)
- …

22.3 Accès aux systèmes d'information

22.3.1 Catalogue des SI

Sera présenté ici un catalogue (par exemple) contenant une ligne dédiée à chaque système d'information disponible à l'IGF.

En cliquant sur une ligne, une fiche descriptive du système apparaîtra :

- Description brève et concise du système
- Procédure d'accès (niveau de sécurité, identification, autorisation, type d'accès par rôle, etc…)
- Manuel d'utilisation du système
- Version en élaboration de ce système, avec les changements inclus dans cette version
- Un lien pour accéder au système ou pour accéder à certaines fonctionnalités.

22.3.1.1 Accès au BDE

Connection via la Base des données des entités.

22.3.1.2 Widget BDE

Demander une information basique d'une entité en particulier.

22.3.1.3 Accès au suivi des missions

Accès au Programme d'intervention annuel. (accès limité selon type d'usager).

22.3.1.3.1 Droit d'accès aux rapports de missions

Concernant l'accès aux rapports de mission, il y aura un hiérarchie établie en fonction de la catégorie des postes de travail :

1. L'inspecteur accèdera à ses propres rapports
2. Le chef de brigade accèdera en plus à tous les rapports des inspecteurs de sa brigade
3. Le chef de l'inspection régionale accèdera en plus à tous les rapports réalisés par les brigades liées à son inspection
4. Le chef de mission accèdera en plus à tous les rapports réalisés par les brigades sous sa direction
5. Le contrôleur général accèdera à tous les rapports réalisés par les brigades liées à sa division
6. Le Chef de l'IGF accèdera à l'intégralité des rapports réalisés.

22.3.1.4 Widget Suivi

Demander de l'information sur les missions d'une entité en particulier

22.3.2 Accès au Centre d'assistance technique. Contact.

22.3.2.1 Formulaire pour signaler un incident technique

Ce formulaire exigera le mail de l'usager, son nom/prénom et proposera un champ textuel afin que la description précise du problème technique puisse être saisie.

Il serait aussi préférable que les informations de l'usager (nom, prénom, mail, …) puissent être entrées de manière automatique.

Un mail sera envoyé au responsable du Service de support TI en mode alerte. Ce responsable lancera les actions pertinentes pour régler le problème.

22.3.2.2 Formulaire pour demander des renseignements fonctionnels

Ce formulaire exigera le mail de l'usager, son nom/prénom et un champ textuel pour saisir la demande précise tout en mentionnant l'unité fonctionnelle à laquelle elle devra être redirigée.

Il serait préférable que les informations de l'usager (nom, prénom, mail, …) puissent être entrées de manière automatique.

Un mail sera envoyé à l'Éditeur Intranet qui se chargera de transférer le mail au destinataire fonctionnel correspondant. Le destinataire final lancera les actions pertinentes pour répondre à l'usager.

22.4 Organisation

22.4.1 Rôles et usagers

Sont proposés les groupes suivants d'usagers:

- L'Éditeur Intranet: (rôle Chef du Projet du système d'information.
  - responsable de valider, approuver et publier les articles sur l'Intranet
- Webmaster (rôle: Administrateur du Système d'information)
  - responsable de la gestion de l'Intranet
  - collabore avec l'Éditeur de l'Intranet sur les tâches d'approbation de contenu
  - Il est en charge de la maquettisation et publication des articles et aussi de maintenir le système de mise à jour.

- Administrateur technique de l'Intranet (rôle: Développeur du Système d'information)
  - responsable de l'installation et maintenance technique du système
  - maintenance technique: les techniciens des systèmes, les administrateurs des bases des données, des "front-end" développeurs, des "back-end" développeurs le cas échéant, appuient le Webmaster dans la résolution des problèmes techniques associés à l'infrastructure technique de l'Intranet.

- Usager 1: (rôle Usager)
  - L'usager pourra accéder à l'information publiée dans l'Intranet de niveau de sécurité bas. Il sera question de la grande partie du contenu publié en termes quantitatifs.
- Usager 2: (rôle Usager)
  - Les usagers de ce groupe accéderont à tout le contenu de niveau de sécurité bas et moyen.
- Usager 3: (rôle Usager)
  - Les usagers de ce groupe accéderont à tout le contenu de niveau de sécurité bas, moyen et haut.
- Rédacteur: (rôle Usager)
  - Les usagers qui appartiennent à ce groupe accéderont directement au site pour lancer directement la rédaction des articles sur l'Intranet.
  - L'Éditeur et/ou le Webmaster doivent approuver l'article avant sa publication.

22.4.2 Intégration avec directory corporatif

Le système CMS proposé pour ce prototype a son propre système d'usagers.

Pour éviter la duplicité de systèmes des usagers, il est préférable que l'Intranet utilise le

directory corporatif.

Néanmoins, pour le prototype, le Service TI peut utiliser le système inclus dans la CMS.

22.4.3 Circuit d'approbation

22.4.3.1 Rédacteur

Ce sont des usagers fonctionnels qui préparent l'information et l'envoient à l'Éditeur pour son approbation.

22.4.3.2 Éditeur intranet

L'Éditeur Intranet révise l'information reçue. S'il approuve, il la fait parvenir au Webmaster pour sa publication sur l'Intranet.

22.4.3.3 Webmaster

Une fois l'article approuvé par l'Éditeur Intranet, le Webmaster procédera à son adaptation au format adéquat et à sa publication dans l'Intranet.

22.5 Sécurité

Le prototype-intranet doit suivre les recommandations de sécurité publiées dans le Plan Directeur des Systèmes d'information.

Néanmoins, il faut rappeler que le prototype-intranet n'est pas accessible à partir d'Internet. En effet, l'ensemble des systèmes d'information installés par l'IGF peuvent seulement être accessibles de manière locale, ou à travers une passerelle VPN sécurisée (DSI).

En plus, la plupart des répertoires proposés sont publics; il pourrait par contre y avoir une partie de l'information dont l'accès n'est autorisé qu'à certains types d'usagers (voir 4.1 Rôles et usagers).

L'accès aux rapports de missions se fera à travers l'application de suivi des missions. Dans la section 3.1.3.1 du Droit d'accès aux rapports des missions, est décrit avec précision le droit d'accès.

22.6 Format, périodicité et responsable de l'information publiée

22.6.1 Périodicité de la mise à jour de l'information

Il faut bien définir la périodicité de la mise à jour.

Il sera nécessaire d'éliminer des éléments obsolètes, par exemple, tout ce qui n'est plus en vigueur.

22.6.2 Format d'origine

Le processus d'alimentation des répertoires sera nécessaire. Par exemple, nous allons prendre les informations en format numérique (PDF) sur internet et les télécharger dans le répertoire.

22.6.3 Niveau de sécurité

Conformément aux recommandations de sécurité incluses dans le Plan Directeur, il y aura trois niveaux de sécurité:

- Bas
- Moyen
- Haut

22.6.4 Responsable de l'information

Section	Format	Périodicité	Niveau de sécurité	Responsable information
Accueil	HTML	minimum hebdomadaire	Bas	Editeur Intranet (avec délégation au Webmaster)
Guide de fonctionnement	HTML + PDF	Dans les actualisations des versions	Bas	CG Divx
Modèles	Office (Word, Excel, …)	chaque mise à jour des modèles	Bas	Chef de projet modèles
Accès à la législation	HTML + PDF	chaque mise à jour des documents	Bas	CG Div1
Formation	HTML + PDF	chaque mise à jour des	Bas	DAM

		documents		
Nouvelles	HTML	minimum hebdomadaire	Bas	Editeur Intranet (avec délégation au Webmaster)
Forum	Application	dépend des usagers	Bas	
Gestion de carrière	PDF + HTML	trimestriel	Haut	Directeur DAM
Accès aux SI	Widget + Application	Selon les changes des applications	Haut	Resp. Sécurité
Contact incident SI	Widget + HTML	dépend des usagers	Bas	Chef de Service TI
Contact question fonctionnelle	Widget + HTML	dépend des usagers	Bas	Editeur Intranet

23 ANNEXE VI: Infrastructure technique: information supplémentaire

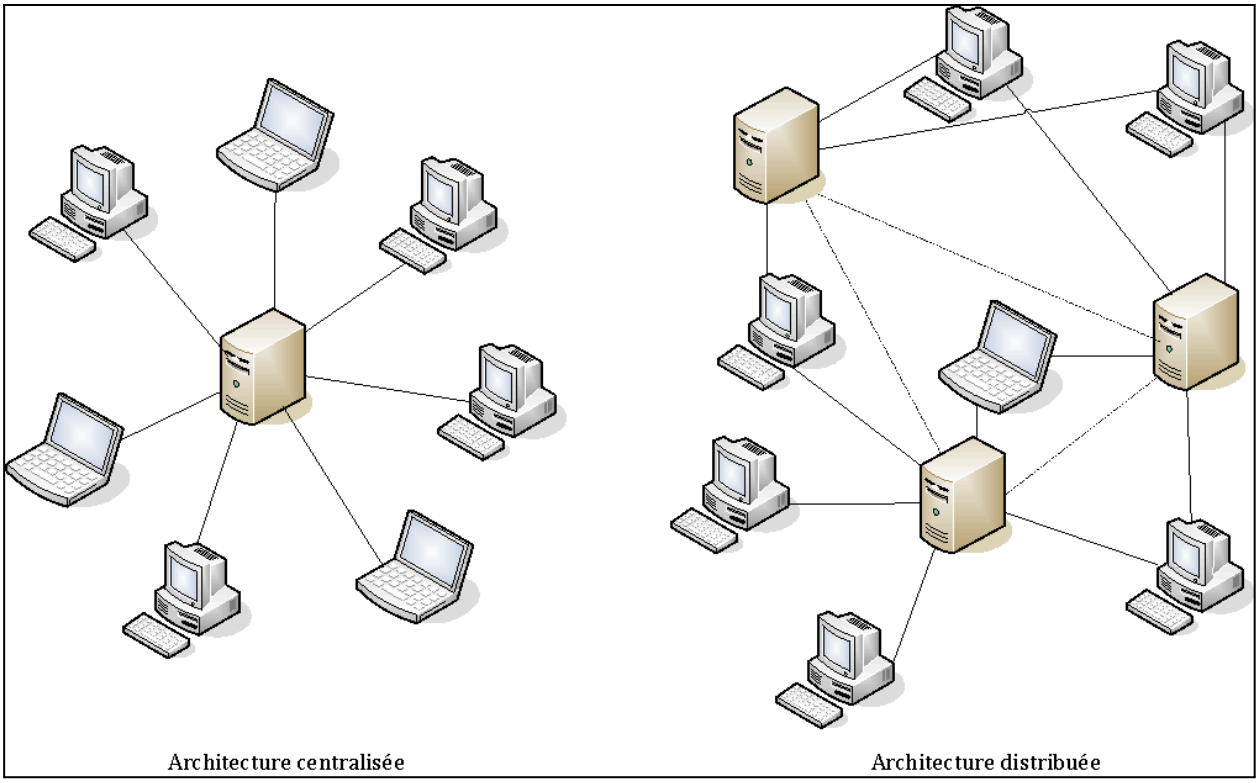
23.1 Architecture centralisée par rapport à l'architecture distribuée

Parmi les avantages de choisir une architecture centralisée, on trouve:

- Toutes les données sont centralisées sur les serveurs centraux, physiques ou virtuels, ce qui simplifie les contrôles de sécurité, l'administration, la mise à jour des données et des logiciels.
- Toute la complexité du traitement et la puissance de calculs sont à la charge du ou des serveurs, les utilisateurs utilisant simplement un client léger sur un ordinateur terminal qui peut être simplifié au maximum.
- En ce qui concerne la recherche d'information, cette architecture est particulièrement adaptée et véloce pour retrouver et comparer de vastes quantités d'informations (par exemple, un moteur de recherche sur le Web), par rapport à l'architecture distribuée beaucoup plus lente.

Bien sûr, il convient de mentionner qu'il y a certains inconvénients liés à ce type d'architectures centralisées, mais comme on le verra, ils ne sont pas décisifs dans le contexte de l'IGF.

- Si trop d'utilisateurs veulent communiquer avec le serveur au même moment, ce dernier risque de ne pas supporter la charge alors que les architectures distribuées fonctionnent mieux en ajoutant de nouveaux participants. Néanmoins, on a remarqué dans le volet 1.1 que le nombre des utilisateurs est relativement petit.
- Si le serveur n'est plus disponible, plus aucun des utilisateurs ne fonctionne tandis que les architectures distribuées continuent de fonctionner, même si plusieurs serveurs tombent en panne. Nous verrons plus loin comment réduire ce risque en introduisant la redondance nécessaire, de façon à ce que les coûts de mise en place et de maintenance ne soient pas élevés.



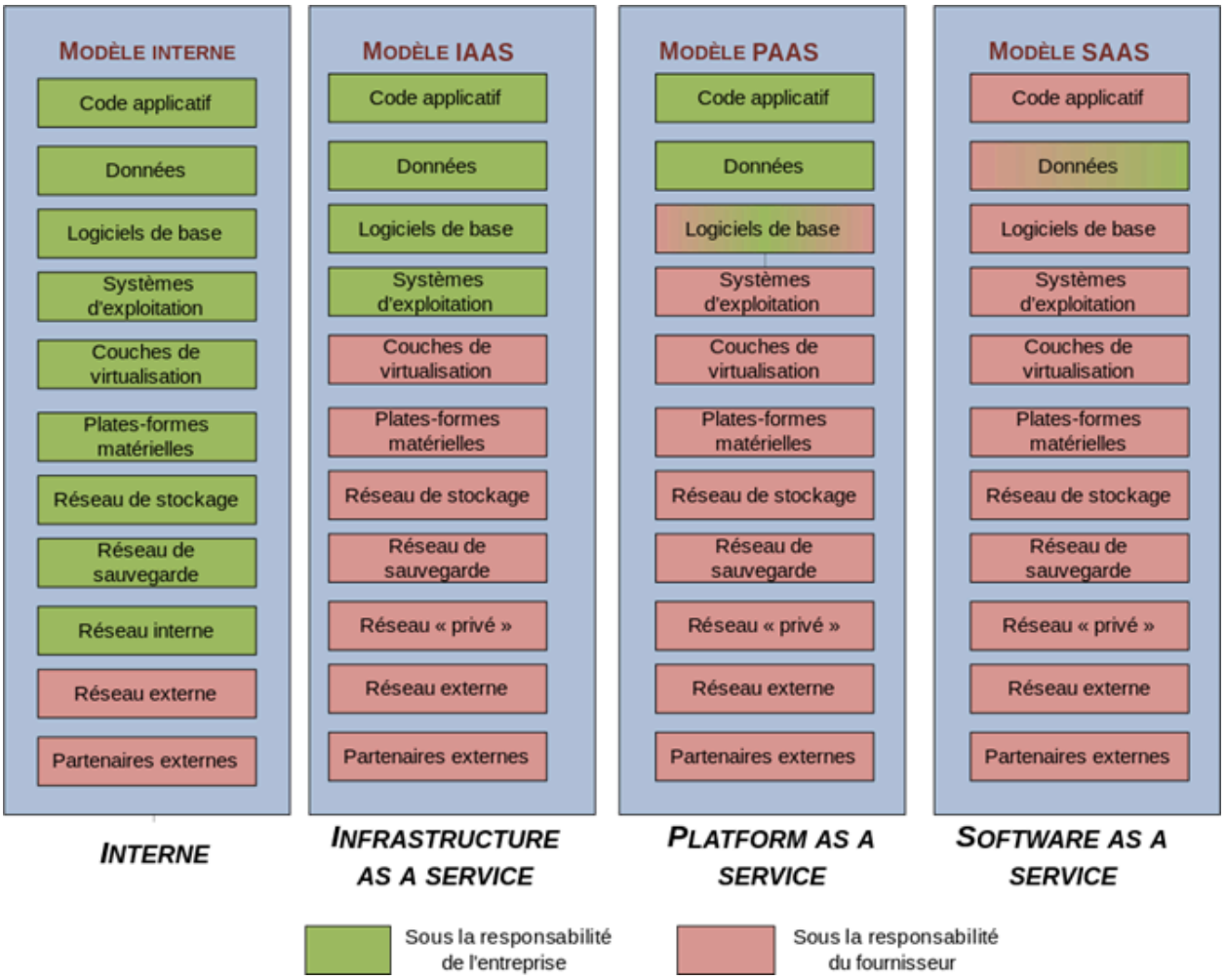
23.2 Cloud Computing

Plusieurs termes désignent actuellement ce nouveau concept en français : « informatique en nuage », « informatique dans les nuages », « infonuagique » ou encore « informatique dématérialisée ». La référence aux nuages (cloud en anglais) vient du fait qu'Internet est souvent représenté sous la forme de nuages dans les schémas qui illustrent l'interconnexion de réseaux.

Wikipedia définit le "cloud computing" comme l'exploitation de la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement internet. Ces serveurs sont loués à la demande, le plus souvent par tranche d'utilisation selon des critères techniques (puissance, bande passante, etc.) mais également au forfait. Le cloud computing se caractérise par sa grande souplesse : selon le niveau de compétence de l'utilisateur client, il est possible de gérer soi-même son serveur ou de se contenter d'utiliser des applications distantes en mode SaaS.

- Le cloud computing peut permettre d'effectuer des économies, notamment grâce à la mutualisation des services sur un grand nombre de clients. Certains analystes indiquent que 20 à 25 % d'économies pourraient être réalisées par les gouvernements sur leur budget informatique s'ils migrent vers le cloud computing. Comme pour la virtualisation, l'informatique dans le nuage peut être aussi intéressante pour le client grâce à son évolutivité. En effet, le coût est en fonction de la durée de l'utilisation du service rendu et ne nécessite aucun investissement préalable (homme ou machine). L'élasticité du nuage permet de fournir des services évolutifs et peut permettre de supporter des montées en charge.

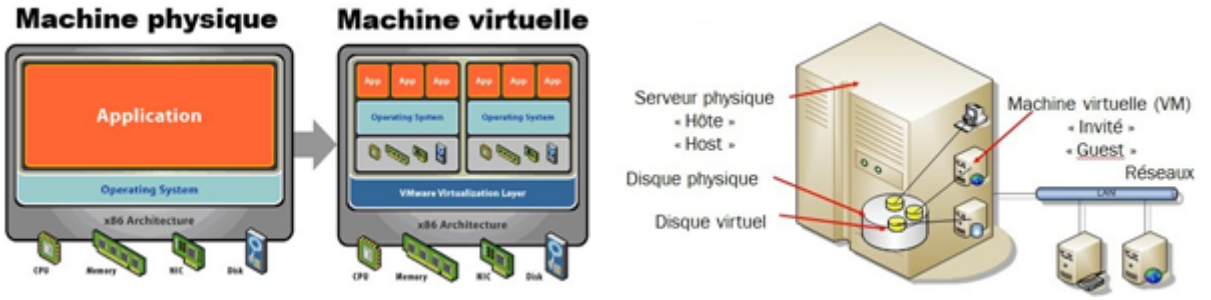
- La maintenance, la sécurisation et les évolutions des services étant à la charge exclusive du prestataire, dont c'est généralement le cœur de métier, elles ont tendance à être mieux réalisées et plus rapidement que lorsqu'elles tombent sous la responsabilité du client.



23.3 Serveurs physiques versus serveurs virtuels

L'architecture d'un serveur physique est simple, chaque serveur a ses propres ressources: la mémoire, le stockage, processeurs, cartes réseau, etc. Sur ce matériel, le système d'exploitation du serveur est chargé. À partir du système d'exploitation, la mise en exécution des applications est possible.

Avec une infrastructure virtuelle, vous disposez du même serveur physique avec toutes les ressources, mais au lieu du système d'exploitation du serveur, il existe un hyperviseur tel que vSphere ou Hyper-V chargé. L'hyperviseur est l'endroit où se créent réellement les machines virtuelles. Tel que présenté sur le diagramme, chaque machine virtuelle possède ses propres ressources virtuelles: processeur virtuel, mémoire virtuelle, cartes d'interface, réseau virtuel et son propre stockage virtuel. Sur ces ressources , il est possible de charger un système d'exploitation invité, puis les applications serveur traditionnelles.



Les avantages de la virtualisation sont évidents: au lieu d'avoir une seule application par serveur, il est possible maintenant d'exécuter plusieurs systèmes d'exploitation invités et une poignée d'applications avec le même matériel physique, apportant beaucoup plus de solutions sans investissement supplémentaire.

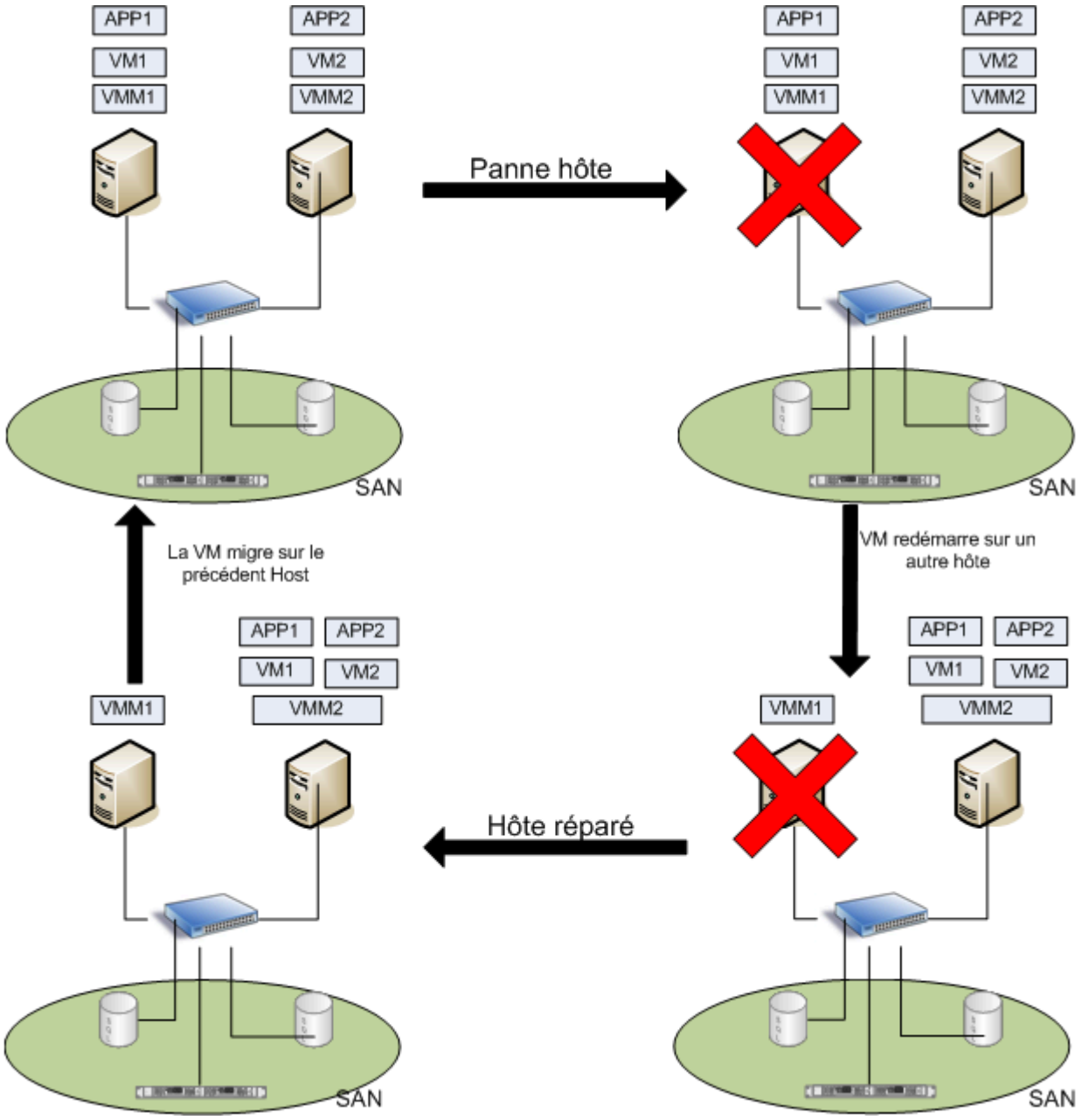
23.4 Disponibilité

Les machines virtuelles sont dotées de plus en plus d'applications qui sont fondamentales pour les entreprises. Les différents acteurs du marché ont alors développé des services de haute disponibilité permettant aux applications de toujours fonctionner car le crash d'un élément est, en principe, transparent.

Le principe de fonctionnement est illustré par le schéma suivant:

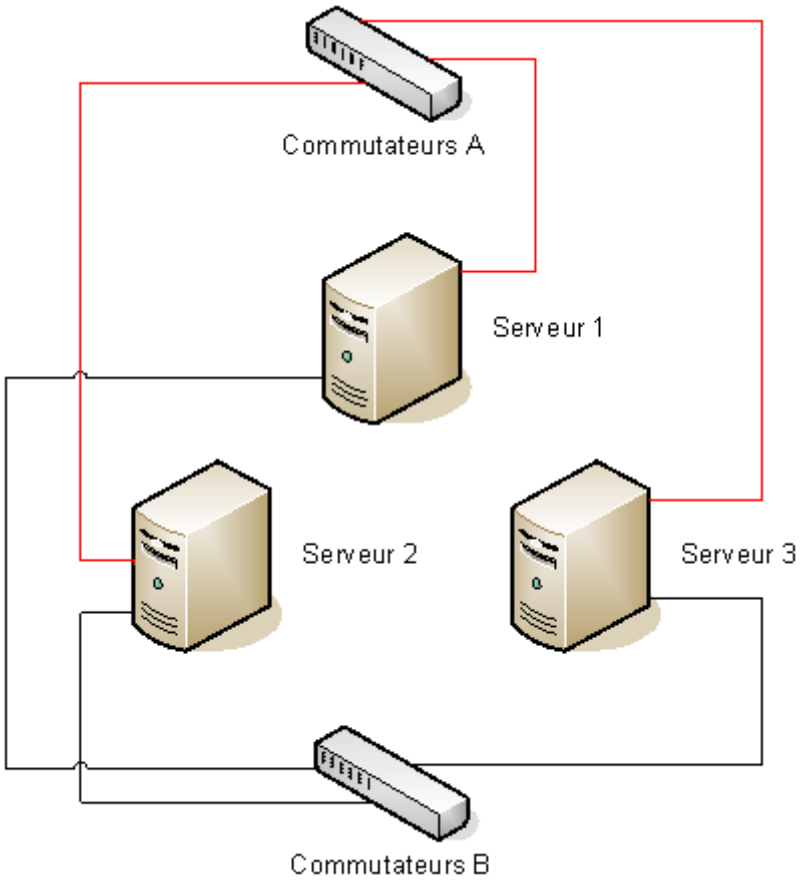
En haut à gauche de l'illustration, deux machines hôtes sont actives et exécutent des applications (APP1 et APP2) au-dessus, respectivement, de deux machines virtuelles (VM1 et VM2). Elles sont régulées par les hyperviseurs (VMM1 et VMM2). Un SAN est utilisé pour garantir la disponibilité des données pour les deux applications.

Quand une panne est détectée, la machine virtuelle (VM1) redémarre instantanément sur le second hôte (VMM2). Cet hôte exécute les deux machines virtuelles(VM1 et VM2) jusqu'à ce que le premier soit réparé. Une fois réparé, le système reprend dans son état initial sans qu'aucun arrêt de fonctionnement ne soit initialisé. La migration de la machine virtuelle se fait à chaud, c'est ce que l'on appelle "la migration à chaud".

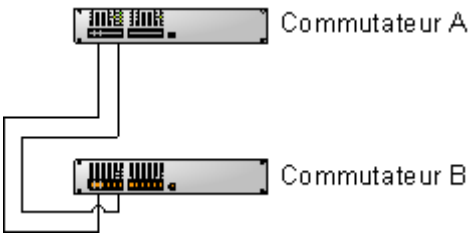


23.5 Réseau LAN

L'infrastructure LAN proposée comprend deux commutateurs. Idéalement, tous les serveurs devraient disposer d'une double interface réseau et il est conseillé de connecter simultanément tous les serveurs aux deux commutateurs, afin de fournir une sauvegarde en cas de panne d'un des commutateurs.



Les deux commutateurs seront connectés aux pare-feu qui fournissent la connectivité Internet. Les commutateurs devraient également être interconnectés l'un avec l'autre afin de fournir une redondance de connectivité sur Internet.



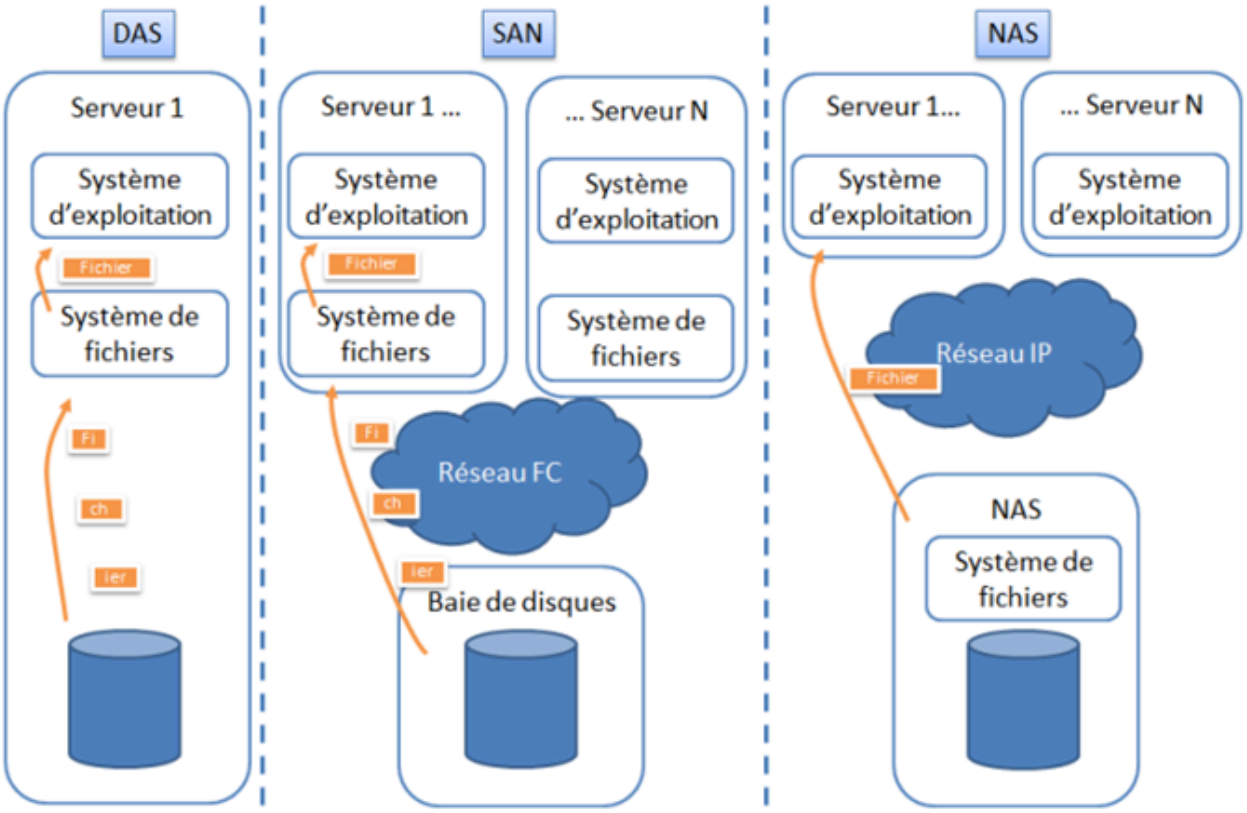
23.6 Solution de stockage

Il existe différentes technologies de stockage de données à des fins professionnelles.

1. DAS: De l'anglais Direct Attached Storage. C'est un système de disque en attachement direct, qui fait en sorte que le système disque ainsi installé n'est accessible directement qu'aux ordinateurs auquel il est raccordé. Ceci ne convient pas pour les applications critiques, puisque si le disque tombe en panne le service est interrompu. Pour la construction de solutions de haute disponibilité, le stockage de données doit être partagé en réseau entre plusieurs serveurs.
2. NAS: De l'anglais Network Attached Storage est un serveur de fichiers autonome, relié à un réseau dont la principale fonction est le stockage de données en un volume

centralisé pour des clients réseau hétérogènes. NAS est souvent fabriqué sous la forme d'un appareil d'ordinateur qui contient un ou plusieurs disques de stockage, fréquemment disposés dans des récipients de stockage logiques, redondants ou RAID. NAS fournit à la fois le stockage et un système de fichiers.

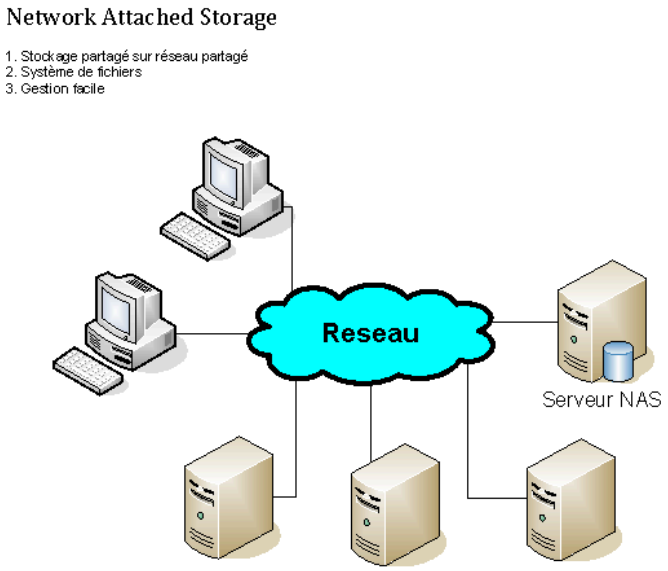
3. SAN: De l'anglais Storage Area Network, est un réseau spécialisé permettant de mutualiser des ressources de stockage. Ces ressources n'apparaissent pas comme des volumes partagés sur le réseau, elles sont directement accessibles en mode bloc par le système de fichiers des serveurs.

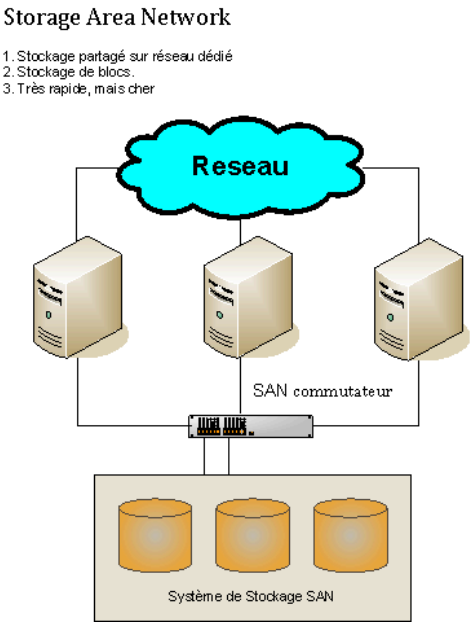


Le tableau et le diagramme suivants résument la différence entre un NAS et un SAN

NAS	SAN
Presque toute machine qui se connecte au réseau local peut utiliser les protocoles NFS, CIFS, FTP ou HTTP pour se connecter à un serveur NAS.	L'accès à un SAN se fait traditionnellement selon le protocole FC, mais on peut utiliser aussi le protocole iSCSI.
Un serveur NAS identifie les données par nom de fichier.	Un SAN adresse les données par blocs logiques et les transfère en blocs de disque.

Un serveur NAS permet de partager facilement des informations. En particulier, parmi les différentes machines.	Pour accéder au SAN, un client (serveur) devra obligatoirement être équipé d'une carte HBA (Host Bus Adapter) spéciale. Une fois connecté le volume de donnée du SAN est présenté au client comme un nouveau disque dur local.
Le système de fichiers est géré par le serveur NAS.	Les clients (serveurs) gèrent le système de fichiers
Les sauvegardes et les miroirs sont générés sur les fichiers.	Les sauvegardes et des miroirs sont générés sur des blocs.





23.7 Architecture de déploiement

Dans le déploiement du logiciel, un environnement ou un niveau est un système informatique dans lequel un programme informatique ou un composant logiciel est déployé et exécuté. En ce qui concerne l'architecture de déploiement, il est proposé d'avoir un minimum de trois environnements opérationnels séparés différents:

1. L'environnement de développement est l'environnement dans lequel on réalise les modifications sur le logiciel et les nouveaux développements. Cet environnement comprendra des outils de développement comme un compilateur, un environnement de développement intégré, des versions différentes ou complémentaires de bibliothèques et des logiciels de support, etc., qui ne sont pas présents dans l'environnement d'un utilisateur.
2. L'environnement de pré-production, pour les tests de fin immédiatement avant le déploiement à la production. Il vise à refléter l'environnement de production actuel le plus fidèlement possible, et peut se connecter à d'autres services de production et

de données, telles que les bases de données. Par exemple, les serveurs seront exécutés sur des machines distantes, plutôt que localement (comme sur le poste de travail d'un développeur), qui teste l'effet de la mise en réseau sur le système.

3. L'environnement de production. Dans l'environnement de production, l'application est mise à la disposition des utilisateurs. En d'autres termes, il s'agit ici de l'environnement qui interagit directement avec les utilisateurs. Le déploiement en production est l'étape la plus sensible.

Il est également conseillé d'avoir les environnements suivants:

1. L'environnement de qualification ou test, sur lequel sont testés les programmes de l'application.
2. L'environnement de formation, sur lequel les utilisateurs sont formés à l'application.

Les trois premiers environnements doivent être séparés et isolés; ils doivent utiliser différentes bases de données; les données réelles de production ne doivent pas être utilisées pour les opérations de test.