Mai 2025

Les bonnes pratiques en matière d'Intelligence Artificielle

Le point de vue de l'utilisateur sur la Gouvernance des Systèmes d'information

La réussite d'une application informatique repose, en grande partie, sur la mise en œuvre des bonnes pratiques. C'est, notamment, le cas des systèmes à base d'Intelligence Artificielle. Ils ne sont pas fondamentalement différents des autres applications mais ils sont plus complexes et surtout leurs résultats sont parfois étonnants. Souvent ils semblent relever du miracle. Mais, au-delà de leurs spécificités ce sont des systèmes d'information reposant sur des architectures informatiques comme les autres et à ce titre il est important qu'ils respectent un certain nombre de bonnes pratiques communes à tous les systèmes d'information ; c'est la gouvernance des systèmes d'information.

Les domaines concernés sont :

- La conception et les fonctionnalités du système,
- La réalisation et les tests,
- La production et la MCO (maintenance en conditions opérationnelles).

Les bonnes pratiques des applications à base d'Intelligence Artificielle doivent respecter celles de l'informatique classique tel que les recense COBIT mais aussi les référentiels de qualité : CMMI et ITIL. Elles concernent en particulier la gouvernance des Systèmes d'Information et une la liste de ces bonnes pratiques a été établie par le Club européen de la gouvernance des Systèmes d'Information (voir annexe ci-dessous). A ces listes de s'ajoutent quelques bonnes pratiques spécifiques à l'Intelligence Artificielle. Attention : elles portent sur l'ensemble des systèmes à base d'Intelligence Artificielle mais ne portent pas sur les applications d'IA génératives. Elles feront l'objet d'un autre document que nous établirons quand nous aurons le recul suffisant.

Importance des bonnes pratiques générales concernant notamment la conception et la mise en œuvre de l'Intelligence Artificielle

Comme tous les développements importants les systèmes à base d'Intelligence Artificielle représentent des efforts conséquents de conception et de mise en place, de plus ils comprennent des risques qu'il faut maîtriser. A cela s'ajoute le fait que la plupart de ces opérations concernent plusieurs entités de l'entreprise. Pour ces raisons il est nécessaire de gérer ces opérations comme des projets d'entreprise.

Or, l'observation montre que trop souvent les opérations concernant l'Intelligence

Artificielle ne sont pas gérées en mode projet. Cette attitude est probablement dû à la croyance que ces développements sont simples, faciles à mettre en œuvre et rentables à tous les coups. C'est oublier que ce sont toujours des opérations complexes, concernant une multiplicité de personnes ou de services, que les temps de réalisations et de mise en œuvre sont souvent longs, enfin qu'il est souvent nécessaire d'organiser les déploiements et notamment la formation des futurs utilisateurs. Comme on le voit, le niveau de risques est assez élevé.

Ces dispositifs concernent trois points clés :

- Un projet d'Intelligence Artificielle est toujours un projet d'entreprise. Il doit être gérer en mode projet, un dispositif de pilotage doit être mis en place et un contrôle suffisant des opérations doit exister.
- Avant de décider la mise en œuvre d'un système à base d'Intelligence Artificielle il est impératif d'effectuer une étude permettant d'apprécier le périmètre du futur système, sa faisabilité et sa rentabilité.
- L'étude économique doit permettre d'apprécier la création de valeur induite par le système à base d'Intelligence Artificielle. Elle doit pour ce cela être complète. Elle doit au moins comprendre :
  - L'impact du futur système sur la productivité (faire la même chose avec moins de ressources) et l'efficacité (faire plus d'opérations avec les mêmes ressources).
  - Evaluer le montant de l'investissement notamment en études, réalisation et mise en place.
  - Estimer les coûts de fonctionnement du système en phase de fonctionnement régulier.
  - Calculer la rentabilité de l'investissement.

La conception, la réalisation et la mise en œuvre d'un système à base d'Intelligence Artificielle est toujours un investissement même lorsqu'il concerne la simple mise en œuvre de fonctions apparemment simples.

Sécuriser l'utilisateur de l'Intelligence Artificielle

Le FutureTech du CSAIL du Massachusetts Institute of Technologie (MIT) a créé une base de données dans l'AI Risk Repository recensant plus de 700 cas de systèmes d'Intelligence Artificielle ayant rencontrés des difficultés et permettant d'évaluer de manière objective les risques potentiels de ces applications. Les trois facteurs de risques les plus fréquents sont :

- La sécurité et à la robustesse des systèmes d'Intelligence Artificielle (76 %),
- Les préjugés injustes et la discrimination (63 %),
- La compromission de la vie privée (61 %).

Un effort particulier doit être porté à la mise en œuvre de bonnes pratiques permettant de réduire significativement l'importance de ces trois facteurs de risques.

Fiabiliser les relations avec les utilisateurs

1. Informer l'utilisateur qu'il est en contact avec une Intelligence Artificielle

   Dès que l'utilisateur se connecte à un système à base d'Intelligence Artificielle, quel qu'il soit, un message clair doit l'informer qu'il est en contact avec un système d'Intelligence Artificielle. Cette information est indépendante de la nature de l'application et du système sur laquelle elle fonctionne : PC, tablette, smartphone, serveur local ou à distance, cloud, …. Le message doit être écrit dans la langue de l'utilisateur et un message audio doit être disponible pour les mal-voyants.

2. Contrôle humain des systèmes à base d'Intelligence Artificielle

   L'utilisateur doit pouvoir interrompre à tout moment un traitement basé sur l'Intelligence Artificielle grâce à un bouton rouge accessible à tout moment. L'état du système est alors sauvegardé et, si l'utilisateur le souhaite, il peut reprendre le traitement quand il veut à l'endroit où il s'est arrêté. Il doit aussi être possible de lancer un nouveau traitement avec de nouveaux paramètres.

3. Respect de la vie privée concernant notamment les informations communiquées au système à base d'Intelligence Artificielle

   Les informations personnelles confiées à un système à base d'Intelligence Artificielle, notamment les informations d'identité et les renseignements bancaires, doivent être inaccessibles à toute autre personne. Ces données doivent être stockées sur un site sécurisé et elles doivent être cryptées.

   Un audit de sécurité et le cas échéant des tests de résistance du système à base d'Intelligence Artificielle doivent être effectués périodiquement. Le dernier certificat de l'auditeur de sécurité doit être accessible en ligne.

   Si les données personnelles doivent être transmises par le système à un tiers elles ne peuvent l'être qu'avec l'accord explicite de l'utilisateur.

   Lorsque les données personnelles saisies passent du poste de travail de l'utilisateur au système à base d'Intelligence Artificielle elles doivent aussi être cryptées de bout en bout. Il en est de même des données transmises à des tiers. Un message de confirmation de la réception de ces données doit être envoyé par ce tiers.

   Si les données personnelles ne sont pas sécurisées ou ne le sont que partiellement, de même si les tests de sécurité n'ont pas été faits ou s'ils ont fait apparaître des fragilités, le système doit être déclaré non-fiable et, dans ce cas, il

ne doit pas être mis à la disposition d'un large public non-averti.

4. Transparence des opérations.

   À tout moment l'utilisateur d'un système à base d'Intelligence Artificielle doit pouvoir savoir où il en est et pour cela il doit pouvoir consulter l'historique des transactions qu'il a effectué. Il est nécessaire que toutes les transactions de saisie antérieure et les résultats obtenus doivent pouvoir être consulté par l'utilisateur. Seul l'utilisateur qui a saisi les données peut les consulter. Il peut modifier les données qu'il a saisies et le cas échant un nouveau traitement peut être relancé. En aucun cas un tiers peut consulter ces informations.

   En terme technique il est pour cela nécessaire de disposer d'un log des transactions : voir point le 19 ci-dessous.

5. Possibilité du recours à un traitement par un humain

   En cas de difficulté l'utilisateur doit avoir la possibilité de demander l'assistance d'un humain, voir à la prise en main de l'application à distance. Bien entendu, il est pour cela nécessaire que le poste de travail et le système à base d'Intelligence Artificielle soit connecté à un réseau.

   L'utilisateur doit pouvoir s'exprimer dans sa langue et recevoir des réponses de manière claire et distincte. Le système doit lui proposer plusieurs langues en audio ou à défaut proposer un échange écrit avec traduction automatique.

   Si c'est un système autonome un numéro d'appel doit être affiché et appelable à l'aide d'un simple téléphone (fixe ou portable) au tarif d'un appel local. Si ceci n'est pas possible cela doit être signalé dans le message initial indiquant que le système ne dispose pas de numéro d'appel.

   Cette assistance doit être systèmatiquement évalué ex-post et notamment les temps de réponse aux demandes des utilisateurs (décroché, durée du dialogue, redémarrage effectif) et la qualité de l'assistance fournie.

6. Explicabilité des décisions prises

   La plupart des systèmes à base d'Intelligence Artificielle sont amenés à prendre des décisions. Celles-ci doivent pouvoir être expliquées par le système. S'il ne peut pas justifier ses décisions il doit être déclaré non-fiable et ne pas être mis à la disposition d'un large public non-averti.

   En cas de litige l'utilisateur doit avoir accès à une procédure de réclamation

offrant la possibilité d'échanger avec un être humain.

7. Explicabilité des algorithmes

Un système à base d'Intelligence Artificielle repose sur un certain nombre d'algorithmes. Ils doivent être clairs et compréhensibles et une documentation suffisante doit être disponible et accessible à tous utilisateur. Celle-ci doit être périodiquement mise à jour.

Certains algorithmes peuvent être couverte par le secret des affaires surtout s'ils ne sont pas protégés par des brevets. Dans ce cas la partie de la documentation concernée n'est accessible qu'aux développeurs, aux décideurs et aux auditeurs autorisés et une documentation simplifiée doit être accessible par l'ensemble des utilisateurs.

De manière générale il est recommandé d'avoir, à côté d'une documentation technique, une documentation légère et facile à lire destinés aux utilisateurs.

8. Egalité de traitement des personnes sans discriminations possibles

Il est fondamental de s'assurer que le système à base d'Intelligence Artificielle traite toutes les personnes de la même manière quel que soit leur origine, leur sexe, leur religion, … Il doit être conforme à la charte des droits fondamentaux de l'Union européenne (1) et les législations nationales non-discriminatoire en vigueur.

Des tests d'absence de biais doivent être régulièrement effectués (voir point 20 ci-dessous).

Une attention particulière doit être portée aux réclamations faites par des utilisateurs se plaignant d'être discriminé par le système.

9. Former les utilisateurs à avoir un œil critique sur les résultats

Il est nécessaire d'informer les utilisateurs qu'un système à base d'Intelligence Artificielle peut commettre des erreurs et qu'il est souhaitable d'effectuer des vérifications.

Des messages clairs doivent figurer dans les écrans affichés par le système

1 - Article 21 : « Est interdite toute discrimination fondée notamment sur le sexe, la race, la couleur, les origines ethniques ou sociales, les caractéristiques génétiques, la langue, la religion ou les convictions, les opinions politiques ou toute autre opinion, l'appartenance à une minorité nationale, la fortune, la naissance, un handicap, l'âge ou l'orientation sexuelle ».

notamment lors de la présentation des résultats.

Le fournisseur du système doit mettre à disposition des utilisateurs une vidéo apprenant aux utilisateurs de s'assurer de l'exactitude des résultats affichés en se basant sur des exemples simples leur montrant que des vérifications simples leur permet de s'assurer de la qualité des réponses. En cas de résultat jugé douteux par les utilisateurs il est important de leur dire d'envoyer un message à l'administrateur du système avec une copie des résultats litigieux.

Dans le cas où le système à base d'Intelligence Artificielle est intégré dans un système plus complexe comme par exemple une voiture autonome ou un robot industriel les neufs points ci-dessus doivent être adaptés à ces contextes particuliers.

Un système fiable et piloté

Il est important de s'assurer que tout système d'information, quel qu'il soit, est fiable et piloté. De même l'architecture informatique permettant son fonctionnement doit être maîtrisée. Dans le cas des systèmes à base d'Intelligence Artificielle, compte tenu des enjeux et des risques, le niveau d'exigence est plus élevé que les systèmes de gestion classiques. Ceci justifie que les bonnes pratiques à mettre en œuvre soient renforcées.

10. Gouvernance des données alimentant le système à base d'Intelligence Artificielle

Les systèmes à base d'Intelligence Artificielle ont besoin de données pour fonctionner en particulier les systèmes reposant sur l'apprentissage profond (« deep learning »). Pour cela on va constituer une ou plusieurs bases de données afin de paramétrer le futur système.

La qualité de ces données est fondamentale. Pour s'en assurer il est nécessaire d'effectuer quelques vérifications :

- S'assurer de la provenance de ces données. Ceci permet souvent d'apprécier leur qualité et d'être prudent lorsque leur provenance est suspecte.
- Vérifier que le fichier ou la base de données est exhaustive et si elle ne l'est pas se demander pour quelle raison il ne l'est pas.
- Ces données sont ensuite nettoyées. Toutes les informations suspectes ou réputées tels ont été éliminés et certaines valeurs peuvent avoir été remplacées par des estimations. Ce nettoyage peut être fait de manière manuelle ou automatique. Il faut s'assurer que ce nettoyage a été fait de manière raisonnable sans dégrader la qualité des données.

Pour être paramétrer le système ces données doivent souvent être indexées. Ainsi dans le cas d'un système de reconnaissance de forme à partir de photos il est nécessaire de rédiger un intitulé pour chaque image. Ce travail peut être fait

manuellement ou de manière plus ou moins automatique.

La qualité et l'efficacité des systèmes à base d'Intelligence Artificielle en dépendent directement de la bonne qualité des données d'apprentissage.

11. Avoir une procédure claire de qualification des données d'apprentissage et de tests

Il est très important de s'assurer que le jeu de données servant à l'apprentissage du système ne sert pas aux tests. Si c'est le cas les tests ne seront pas efficaces car ils ne permettront pas de détecter d'éventuelles anomalies.

Les bases de données servant à l'apprentissage des systèmes à base d'Intelligence Artificielle et celles servant aux tests doivent être qualifier. Pour cela il est nécessaire de mettre en place un processus efficace et rigoureux. Une procédure écrite doit décrire ce processus et permet de s'assurer de la qualité de ces opérations.

12. Avoir des équipes de développement et de tests diversifiées

L'expérience montre que les équipes « mono color » commettent parfois des erreurs car tous leurs membres pensent et réagissent de la même manière. Pour éviter cela il est recommandé de constituer des équipes de développement et de tests comprenant des personnes ayant des profils différents. Ceci concerne notamment la présence dans l'équipe projet de femmes, d'utilisateurs, de « littéraires », ….

13. Avoir une procédure de remontée et de traitement des anomalies et des erreurs

Des anomalies et des erreurs peuvent survenir même dans des systèmes à base d'Intelligence Artificielle bien rôdés. Les utilisateurs constatent que le système donne une réponse curieuse, inadéquate ou franchement fausse. Il doit leur être possible de signaler l'anomalie qu'ils constatent au responsable chargé de l'exploitation du système. Il est pour cela utile de pouvoir sauvegarder le ou les écrans, le contexte informatique (le log des précédentes transactions) et les observations ou les questions de l'utilisateur.

Cette procédure de détection des remontées utilisateurs a plusieurs avantages. Elle permet d'abord de connaître les difficultés rencontrées par les utilisateurs. Il est ainsi possible de repérer des améliorations possibles. Et, bien entendu, elle est aussi utile pour détecter les bugs à corriger. Une statistique des incidents et de leurs causes doit être périodiquement établie.

Parmi les réclamations faites par les utilisateurs il y a des plaintes de personnes qui s'estime victime de biais de genre, de race, … Une attention toute particulière

doit être portée à ces plaintes et des vérifications doivent être effectués pour s'assurer si elles sont réelles ou imaginaires.

Point important : il est important de répondre à tous les messages utilisateurs, quel qu'ils soient. Ce peut être fait dans le cadre de l'application ou par mail.

14. S'assurer de la robustesse technique du système

Il est important de vérifier la robustesse du système. Ceci se fait par le biais de l'analyse de la fréquence des incidents et leur degré de gravité. Mais ce n'est pas suffisant notamment lors de la mise en production d'un nouveau système à base d'Intelligence Artificielle. Pour évaluer la robustesse du système il est recommandé d'effectuer des tests du type « stress tests ».

Pour cela on va faire subir à l'application :

- Des saisies de données aberrantes qui doivent toutes être rejetées,
- Des dégradations des bases de données des paramètres pour s'assurer que le système les détecte automatiquement et les rejette,
- La possibilité de lancer simultanément des volumes importants de transactions normales car l'expérience montre que certaines anomalies apparaissent lorsque le système est proche de la saturation,
- Des arrêts inopinés des opérations en cours de traitement pour observer dans quelles conditions le système redémarre,
- ….

Il est recommandé d'effectuer ces tests de manière automatique sur une machine de tests et d'éviter de les faire sur le système de production. Il est de bonne pratique de refaire périodiquement les tests de façon à constater que l'application ne se dégrade pas.

15. Avoir un poste de contrôle en temps réel de l'ensemble de l'activité de chaque système à base d'Intelligence Artificielle

Pour suivre l'activité d'un système à base d'Intelligence Artificielle il est recommandé d'avoir un PC permettant de suivre en temps réel son fonctionnement et permettant, le cas échant, d'intervenir. De nombreux indicateurs peuvent être suivis, notamment :

- Le nombre d'utilisateurs connectés à un instant donné,
- Le temps moyen de réponse,
- La longueur des files d'attentes,
- Le nombre de transactions traitées par seconde,
- Les anomalies détectées,
- Le nombre de tâches laissées pendantes,
- Le nombre de messages utilisateurs reçus,
- ….

En cas de blocage du système l'opérateur doit disposer sur le poste de contrôle de toutes les informations permettant de comprendre ce qui se passe et, si c'est nécessaire, il doit pouvoir lancer des actions permettant de revenir à une situation normale.

Une personne responsable et compétente doit être désignée pour surveiller le système et intervenir en cas de nécessité. Si le système fonctionne 24 heures sur 24 il est nécessaire de s'organiser en conséquence. Pour faciliter la surveillance et ces interventions il doit être possible de déporter le poste de contrôle sur un PC portable ou une tablette sous 5G.

Dans le cas d'un système à base d'Intelligence Artificielle mono-utilisateur un poste de contrôle est sans objet, par contre il est utile de disposer de quelques statistiques pour comprendre en cas de dégradation ou de panne du système ce qui se passe.

16. Evaluer périodiquement le niveau de sécurité pour s'assurer qu'il est suffisant

Compte tenu des enjeux liés à l'application et du degré de confidentialité des informations qui lui est confié il est nécessaire de s'assurer périodiquement que le niveau de sécurité objectif est respecté.

Ces contrôles peuvent être effectués par l'exploitant du système mais pour des raisons de prudence il est préférable de les confier à un tiers extérieur. Il est nécessaire de s'assurer qu'il a des compétences en matière d'audit informatique.

Les points à vérifier sont, entre autres :

- La gestion des habilitations d'accès au système,
- L'efficacité des contrôles lors de la connexion,
- La possibilité de contourner ces contrôles (existence de by-pass, de codes d'accès largement diffusés et connus de tous, …),
- L'existence d'un historique des connexions,
- Le cryptage des transactions notamment des postes distants,
- Le cryptage des données stockées, notamment les informations personnelles,
- L'impossibilité de visualiser les transactions effectuées par un tiers,
- La sauvegarde des données sur un système informatique à distance,
- La capacité de reprise du système après incident,
- …

Il est recommandé d'effectuer ces contrôles de sécurité au moins une fois par an.

17. Avoir un planning de tests périodiques de l'ensemble du système

La maintenance doit être mise sous contrôle car il arrive que ces informations se traduisent par des dégradations des performances du système. Pour cette raison il est de bonne pratique de mettre sous contrôle les opérations de maintenance et les interventions faites en urgence. Pour cela il est recommandé de disposer d'une procédure d'enregistrement des demandes de maintenance, un suivi des opérations de modifications et l'existence de tests préalables à la mise en production.

Il est de plus nécessaire de prévoir périodiquement une série de tests permettant d'apprécier la qualité des contrôles et des traitements ainsi que sur les performances du système afin de détecter une éventuelle dégradation du système.

Pour cela il est nécessaire de disposer d'un jeu d'essais standard, stocké sur une machine de tests sur la quelle sont préalablement recopiées les programmes à tester et les données opérationnelles. Si c'est possible la machine de tests doit avoir la même configuration que les machines de production. Dans la mesure du possible les tests doivent pouvoir s'exécuter de manière automatique. Autre précaution : pendant les tests la machine de tests doit être déconnectée du réseau.

18. Avoir un programme d'audit à moyen terme

Un système basé sur l'Intelligence Artificielle, en particulier s'il a une large diffusion et s'adresse à un public non-avertis doit faire l'objet d'un audit périodique.

Il est prudent d'effectuer un audit avant que l'application soit mise en production et puis il est ensuite recommandé de réaliser périodiquement un audit de suivi. Celle-ci dépend de plusieurs facteurs : le niveau des enjeux, l'importance des risques, le nombre d'utilisateurs potentiels, le degré de visibilité de l'application, l'aversion au risque et le niveau de réputation de l'entreprise mettant en production l'application, … En règle générale ce type d'audit général est effectué tous les 2 ou 3 ans.

Il est recommandé que ces audits soient confiés à un auditeur informatique professionnel et connaissant, si possible, les bonnes pratiques de l'Intelligence Artificielle. En fin de mission il remettra un rapport comprenant des recommandations permettant d'améliorer le fonctionnement du système à base d'Intelligence Artificielle.

19. Nécessité d'avoir un log des transactions

Pour avoir un suivi des opérations et, en cas de difficulté, comprendre ce qui s'est passé, il est indispensable de les tracer. Ceci repose sur un enregistrement

de toutes les transactions. Les techniciens appellent ce type de dispositif un log. On peut se limiter à n'enregistrer que les données saisies et les résultats restitués mais il est possible d'aller plus loin d'enregistrer les traitements intermédiaires. Mais il faut être raisonnable car, dans ce cas les volumes à stocker peuvent devenir très importants.

Pour consulter l'historique il est souhaitable de disposer d'un programme de mise en forme de ces données. Il doit être possible de rechercher les informations d'une transaction particulière ou d'un groupe de transactions spécifiques.

Pour éviter d'avoir des historiques trop volumineux il est nécessaire de prévoir une fonction de purge de ces données.

20. Disposer d'outils de détection des biais

Tout système a des biais. Même les humains ont des biais et certains sont inconscient. Cependant, dans le cas des systèmes à base d'Intelligence Artificielle ils peuvent entrainer des dérives qui peuvent avoir des conséquences importantes. Les plus redoutables sont les biais de genre ou les biais de race. Pour les éviter il est nécessaire de mettre en place des outils de détection de biais.

Ce sont pour l'essentiel des programmes statistiques permettant de comparer les pourcentages de résultat de deux populations distinctes par exemple les embauches des hommes et des femmes pour une fonction donnée. Il suffit ensuite de comparer les taux d'embauche des uns et des autres pour apprécier l'importance du biais de genre.

Comme on le voit il est indispensable de s'assurer que les bonnes pratiques soient mises en œuvre faute de quoi les systèmes à base d'Intelligence Artificielle dérivent. Mme Virgina Dignum, professeur d'informatique en Suède et consultante de l'ONU sur le développement de l'Intelligence Artificielle, constate : « *L'Intelligence Artificielle est une voiture sans freins, conduite par un conducteur sans permis, dans une rue sans panneaux de signalisation* »

Liste des bonnes pratiques générales en matière de gouvernance des systèmes d'information

1 – La gouvernance en matière de conception des systèmes d'information

1 . 1 S'assurer l'intégration du futur système d'information dans la stratégie de l'entreprise.
1 . 2 Evaluer la création de valeur par le système d'information.
1 . 3 Concevoir l'architecture du système d'information.
1 . 4 S'intégrer dans l'architecture existante.
1 . 5 Gérer le projet en mode projet.
1 . 6 Accorder une grande importance à l'organisation.
1 . 7 Définir la conception globale en deux étapes.
1 . 8 Rédiger un document de référence.
1 . 9 Identifier des fonctions et des processus.
1 . 10 Prendre en compte le rôle particulier joué par le système informatique.
1 . 11 Faire participer les personnes concernées par le futur système d'information à sa conception.
1 . 12 Partir de l'existant et le faire évoluer.
1 . 13 Désigner un responsable du système d'information.
1 . 14 Choisir une architecture adaptée.
1 . 15 Respecter les règles de contrôle interne.
1 . 16 Evaluer et suivre les risques.
1 . 17 Définir des dispositifs de sécurité adaptés.
1 . 18 Chiffrer le montant de l'investissement.
1 . 19 Suivre l'avancement du projet.
1 . 20 Assurer le suivi des dépenses investies.
1 . 21 Estimer les coûts prévisionnels de fonctionnement du système d'information.
1 . 22 Evaluer la rentabilité de l'investissement.
1 . 23 Accorder au management de l'entreprise un rôle clé.
1 . 24 Faire valider le projet par toutes les parties prenantes.
1 . 25 Mettre en place un tableau de bord du projet de système d'information.

Chapitre 2 – La gouvernance en matière de fonctionnement des systèmes d'information

2 . 1 Désigner un responsable du système d'information.
2 . 2 Contrôler l'ensemble du système d'information.
2 . 3 Alimenter une base de données mémorisant l'ensemble des opérations de façon à établir un tableau de bord de l'activité du système d'information.
2 . 4 Suivre le détail des opérations.
2 . 5 Garantir la sécurité des opérations et des bases de données.

2 . 6 Auditer périodiquement le système d'information.
2 . 7 Enregistrer tous les incidents et les tentatives de forçage.
2 . 8 Enregistrer toutes les anomalies qui surviennent.
2 . 9 Effectuer un suivi des anomalies constatées.
2 . 10 Vérifier le contenu des bases de données.
2 . 11 Gérer les actifs informationnels.
2 . 12 Mettre en place des contrôles suffisants.
2 . 13 Effectuer des contrôles particuliers des transactions délicates.
2 . 14 Etablir un tableau de bord du contrôle interne du système d'information.
2 . 15 Documenter le système d'information.
2 . 16 Disposer d'une procédure écrite.
2 . 17 Mesurer des indicateurs de performances significatifs.
2 . 18 Mesurer des indicateurs de productivité.
2 . 19 Suivre le coût global du système d'information.
2 . 20 Calculer le coût moyen par unité produite.
2 . 21 Travailler les coûts unitaires.
2 . 22 Analyser le détail des opérations effectuées.

Chapitre 3 – La gouvernance en matière de pilotage des systèmes d'information

3 . 1 Désigner un pilote du système d'information.
3 . 2 Avoir un décideur consensuel, reconnu par les autres décideurs concernés.
3 . 3 Veiller à ce que le pilote ait des pouvoirs suffisants.
3 . 4 Nommer une personne réactive.
3 . 5 Disposer d'un organe de pilotage adapté.
3 . 6 Rendre périodiquement des comptes.
3 . 7 Mettre en place un tableau de bord.
3 . 8 Mettre en place une procédure d'escalade des problèmes.
3 . 9 Prévenir l'apparition des conflits et les traiter dès qu'ils se manifestent.
3 . 10 Suivre les incidents.
3 . 11 Consulter périodiquement les utilisateurs et les décideurs pour recenser les demandes d'évolution qu'ils souhaitent mettre en œuvre.
3 . 12 Sélectionner les demandes en fonctions de critères simples.
3 . 13 Planifier les changements.
3 . 14 Pratiquer la délégation de pouvoir.
3 . 15 Suivre le planning et mesurer l'avancement.
3 . 16 Prévoir et suivre la charge de travail.
3 . 17 Fixer et suivre le budget des opérations.
3 . 18 Vérifier l'impact des changements.
3 . 19 Effectuer périodiquement une évaluation du système d'information.
3 . 20 Evaluer la valeur créée par le processus.
3 . 21 Gérer les risques.
3 . 22 Gérer la sécurité.
3 . 23 S'assurer du respect des règles de contrôle interne.

Chapitre 4 – La gouvernance en matière de gestion de l'évolution des systèmes d'information

4 . 1 Désigner un pilote des évolutions du système d'information.

4 . 2 Avoir une vision à moyen terme du système d'information.
4 . 3 Rédiger un document d'orientation.
4 . 4 Faire valider ces orientations.
4 . 5 Définir un cycle et une périodicité d'évolution du système d'information.
4 . 6 Stabiliser le périmètre du système d'information.
4 . 7 Validation des extensions ou des réductions du périmètre du système d'information.
4 . 8 Consulter périodiquement les utilisateurs et les décideurs pour recenser les demandes d'évolution qu'ils souhaitent mettre en œuvre.
4 . 9 Sélectionner les demandes d'évolution en fonction de critères simples.
4 . 10 Planifier les changements.
4 . 11 Suivre le planning et mesurer l'avancement.
4 . 12 Prévoir et suivre la charge de travail.
4 . 13 Fixer et suivre le budget des opérations.
4 . 14 Gérer les évolutions importantes en mode projet.
4 . 15 Préparer le travail à effectuer.
4 . 16 Evaluer la charge de travail nécessaire et fixer le budget.
4 . 17 Fixer des priorités.
4 . 18 Fixer des échéances.
4 . 19 Améliorer le système informatique.
4 . 20 Faire tester les changements effectués par des personnes utilisant habituellement le système d'information.
4 . 21 Disposer d'une plateforme de tests.
4 . 22 Mettre à jour la documentation du système informatique.
4 . 23 Améliorer l'organisation en place.
4 . 24 Mettre à jour la note de procédure.
4 . 25 Donner des instructions écrites aux personnes utilisant le système d'information.
4 . 26 Former les personnes intervenant dans le cadre du système d'information.
4 . 27 Evaluer ultérieurement le système d'information.
4 . 28 Fixer la date de la prochaine révision.

Pour plus de détail, lire le document : https://www.cegsi.org/index.php/documents/les-bonnes-pratiques-en-matiere-de-gouvernance-de-systemes-d-information/les-bonnes-pratiques-en-matiere-de-gouvernance-des-systemes-d-information

Pour télécharger le texte complet : https://www.cegsi.org/index.php/documents-a-telecharger/category/autres-documents