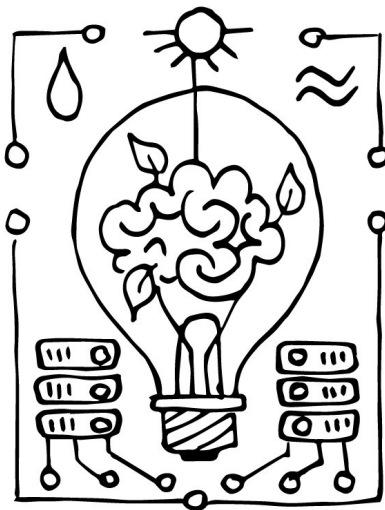


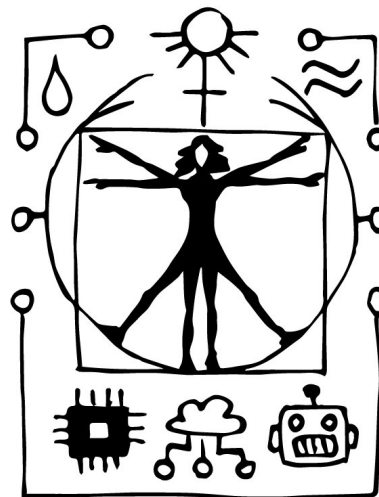
INFRA BASSE

Référentiel opérationnel pour une désescalade numérique choisie et maîtrisée

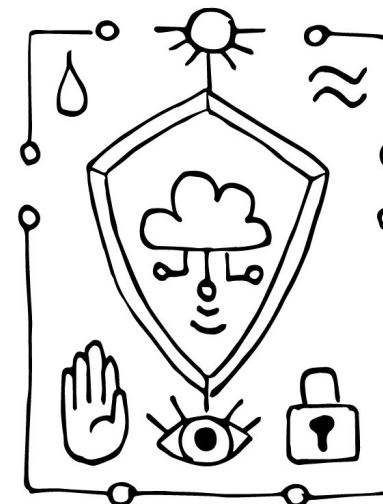
Le guide de gouvernance



La sobriété éclairée prime sur toute décision technologique



L'Humain prime sur la technologie



Toute technologie doit être limitée, maîtrisée et justifiée

Remerciements

Nous remercions l'ensemble des équipes du programme Alt IMPACT, porté par l'ADEME, le CNRS et l'INRIA, dont le soutien financier a permis la réalisation de ce travail.

Merci à Pauline et Dylan qui ont cru en Infrabasse alors qu'elle n'était encore qu'une simple idée.

Nous remercions l'association DeuxFleurs, porteuse initiale du projet, pour son soutien et sa confiance tout au long de cette démarche, ainsi que l'association Syst-A, qui assurera la pérennité du projet.

Merci également à Frédéric et Dylan pour leur regard attentif lors de la relecture, leurs retours exigeants et leur contribution à l'amélioration de ce référentiel.

Nous remercions bien sûr TRIBU, la coopérative (SCOP) accompagnée dans le cadre de cette démarche, et plus particulièrement Mélanie, Laura, Héloïse, Paul et Clément dont les questionnements, les contraintes et les réflexions ont largement contribué à ancrer ce guide dans des réalités concrètes.

Merci à Esther, Laetitia et Vaite, les exceptionnelles graphistes et illustratrices d'InfraBasse.

Ce guide complète le guide de réflexion "InfraBasse, Visibiliser les infrastructures numériques pour les comprendre", afin de rendre actionnables les idées qui y sont développées.

Le référentiel opérationnel InfraBasse a été créé et rédigé par le collectif InfraBasse, constitué de Perrine Letellier, Quentin Dufour et Oriane Saint-Cyr. Si le fond de ce guide de gouvernance est unique; sa forme s'inspire de méthodes existantes, notamment le guide de 2019 co-porté par le CIGREF, l'IFACI et l'ISACA, mais on y retrouve aussi de l'inspiration EBIOS, ISO 27000 et ISO 26000.

Il reflète une démarche construite à travers une volonté partagée de proposer une nouvelle approche du numérique en entreprise, centrée sur l'humain et la sobriété.

Sommaire

Intro

Guide de lecture

Partie 1 - Les fondations

Axe 1 – Stratégie de la gouvernance du numérique

Axe 2 – Désescalade numérique

Axe 3 – Âme de l'organisation

Partie 2 - Les piliers

Axe 4 – Pérennité du système d'information

Axe 5 – Cybersécurité

Axe 6 – Données

Axe 7 – Infrastructures

Partie 3 – La gouvernance opérationnelle

Axe 8 - Projets

Axe 9 – Prestataires et fournisseurs

Axe 10 – Services numériques

Axe 11 – Maîtrise du budget

Axe 12 – Partage de la démarche de désescalade numérique

Conclusion et Lexique

INTRODUCTION

1. Pourquoi ce référentiel de gouvernance du numérique ?

Dans de nombreuses organisations, notamment celles ne disposant pas de compétences internes dédiées, la gestion du système d'information (SI) souffre d'un manque de vision stratégique claire et partagée.

Les projets numériques s'empilent souvent sans être pensés dans une logique d'ensemble, fragilisant progressivement le socle technique et organisationnel.

Cela augmente la dépendance aux prestataires, dont les organisations peinent à comprendre le jargon technique, ainsi que le périmètre d'action et de responsabilités. Un fossé se creuse, entraînant une perte de maîtrise de son système d'information (SI).

Suivre la démarche InfraBasse, c'est autonomiser les équipes, intégrer les enjeux de sobriété et de sécurité, maîtriser la relation aux prestataires, et ainsi reprendre le contrôle de ses infrastructures numériques.

2. L'appropriation du système d'information, un long chemin à suivre

La gouvernance du système d'information (SI) ne se limite pas aux phases de transformation ou aux projets structurants.

Elle s'inscrit dans une démarche continue, qui consiste à questionner en priorité l'infrastructure du système d'information (SI), afin d'en maîtriser les usages, les outils et les évolutions.

La conduite de projets numériques nécessite une méthodologie précise, adaptée à l'organisation.

InfraBasse propose cette méthodologie mais dépasse le seul cadre des projets : elle constitue une grille de lecture mobilisable au quotidien pour interroger la pertinence, la cohérence et les impacts des choix numériques.

À l'issue de l'(auto-)évaluation proposée par InfraBasse, l'organisation sera en capacité de structurer sa démarche, de répondre concrètement aux enjeux identifiés, tout en assumant un positionnement de sobriété. Dans de nombreux cas, cette étape conduira à la réalisation d'un audit technique préalable afin de disposer d'un état des lieux fiable du système d'information.

InfraBasse s'appuie sur un déroulé de gouvernance éprouvé, qu'il adapte à ses principes de maîtrise, de sobriété et d'autonomisation des organisations.

Les étapes présentées ci-après constituent des repères pouvant être activés de manière non linéaire selon les besoins de l'organisation.

COMPRENDRE

- Comprendre les effets délétères du numérique
- Clarifier ses objectifs de gouvernance du numérique (audit de gouvernance)
- S'approprier l'existant (audit technique)

CIBLER LE BESOIN

- Définir une architecture cible globale en adéquation avec la gouvernance (sur la base de l'audit)
- Définir le périmètre d'action dans lequel l'organisation est prête à s'engager

MOBILISER L'ÂME DE L'ORGANISATION (Les équipes)

- Définir les responsabilités de chacun-e en adéquation avec les appétences et les compétences
- Prévoir un plan de formation des équipes le plus en amont possible des projets

ÉVALUER & APPRENDRE

- Vérifier et consigner l'avancement du projet, en évitant ou corrigeant rapidement les dérives
- Évaluer les premiers temps d'exploitation
- Évaluer le déroulé du projet, les prestataires, les manques en interne et faire un bilan qui prend en compte ces retours d'expérience
- Mettre en place un processus d'amélioration continue
- Recommencer jusqu'à clôture du périmètre défini au départ

ÉVOLUER PROGRESSIVEMENT

- Accompagner le changement auprès des équipes tout au long du projet
- Documenter l'ensemble des actions : audit, relation avec les prestataires, sécurité, gestion des données, procédures techniques...
- Décomposer les projets en tâches, qui seront parfois concomitantes
- Se lancer dans la réalisation de la première tâche. Le projet sera minutieusement planifié
- Apporter une attention particulière à la mise en production (le jour de la migration, du changement de serveur,...)

DÉFINIR UNE TRAJECTOIRE

- Identifier les forces et faiblesses du périmètre défini
- S'entourer d'un réseau et de partenaires de confiance
- Utiliser des outils en adéquation avec la stratégie de gouvernance adoptée
- Identifier la pertinence de chaque prestataire pour chaque tâche, ainsi que leur capacité à travailler en commun. Définir ensuite un contrat de niveau de service précis. (Par exemple : niveau de support après le déploiement)

3. Le périmètre du guide InfraBasse

En intervenant en amont des décisions techniques, InfraBasse clarifie le cadre stratégique des évolutions du système d'information (SI) et des relations avec les prestataires.

InfraBasse se distingue par une approche qui place "l'âme de l'organisation" au cœur de la gouvernance du numérique. En impliquant l'ensemble des membres de l'organisation, qu'ils souhaitent ou non participer directement à cette gouvernance, elle crée les conditions d'une désescalade numérique choisie et maîtrisée.

Le guide s'adresse :

- Aux organisations souhaitant maîtriser leurs choix numériques tout en s'inscrivant dans une démarche de désescalade. Il leur permettra d'éviter des erreurs stratégiques énergivores, chronophages et coûteuses
- Aux prestataires qui souhaitent les accompagner dans ce sens, en adoptant un positionnement fort et en repensant leurs préconisations

Pour constituer un référentiel complet, ce guide sera complété par :

- Le guide de réflexion "Visibiliser les infrastructures numériques pour les comprendre"
- Un outil d'(auto-)évaluation
- Une boîte à outils regroupant des modèles de documents
- Un annuaire de prestataires de confiance

Comment lire ce guide ?

Ce guide est divisé en trois parties, composées d'axes :

1. **Les fondations (3 axes)** : Elles définissent le cadre de gouvernance d'InfraBasse. Elles constituent le socle du référentiel et reposent sur trois principes structurants : l'humain, la sobriété, ainsi que la compréhension et la maîtrise du SI et de ses enjeux.
2. **Les piliers (4 axes)** : Ils traduisent les fondations en une lecture transversale du SI. Les axes de cette partie sont interdépendants et permettent d'analyser l'architecture globale du SI afin d'identifier les interactions et les dépendances.
3. **La gouvernance opérationnelle (5 axes)** : Elle s'appuie sur les fondations et les piliers pour guider la gouvernance du SI au quotidien. Ses cinq axes constituent des leviers d'action qui peuvent être mobilisés différemment selon les priorités et le contexte de l'organisation.

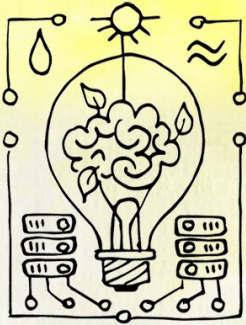
Chaque axe présente :

- Les enjeux liés à sa maîtrise
- Les menaces : situations ou facteurs susceptibles de compromettre la maîtrise des enjeux
- Les risques : conséquences éventuelles pour l'organisation en cas de non maîtrise des enjeux
- Les bonnes pratiques répondant aux enjeux identifiés, en fonction des risques et menaces

L'organisation est invitée à identifier ses enjeux prioritaires afin d'assurer la cohérence de son plan d'action.

InfraBasse repose sur une approche systémique : ce guide doit être appréhendé dans son ensemble afin de comprendre les interdépendances entre ses composantes, puis d'effectuer des choix éclairés et contextualisés.

Il ne s'agit donc pas d'appliquer exhaustivement chaque bonne pratique, mais de construire une trajectoire adaptée aux valeurs et au contexte de l'organisation



La sobriété éclairée prime sur toute décision technologique



L'Humain prime sur la technologie



Toute technologie doit être limitée, maîtrisée et justifiée

Axes 1 à 3
Les Fondations

Axes 4 à 7
Les Piliers

Axes 8 à 12
La Gouvernance Opérationnelle



Partie 1 : LES FONDATIONS

Axe 1 – Stratégie de la gouvernance du numérique

La manière dont l'organisation décide et arbitre

Axe 2 – Désescalade numérique

Les limites que l'organisation choisit de se fixer

Axe 3 – Âme de l'organisation

La réalité humaine dans laquelle s'incarnent ces choix

La gouvernance du numérique ne peut se limiter à une succession de choix techniques ou d'outils. Elle repose avant tout sur une vision structurée, assumée et partagée par l'ensemble de l'organisation.

Cette première partie pose les bases de la démarche InfraBasse. Elle définit les principes directeurs qui orienteront l'ensemble des décisions, des plus stratégiques aux plus opérationnelles.

Loin d'être indépendantes, les fondations s'articulent et se renforcent mutuellement pour construire une gouvernance maîtrisée, sobre et réellement adaptée aux besoins de l'organisation.

1. STRATÉGIE DE GOUVERNANCE DU NUMÉRIQUE

Objectifs :

- Intégrer les enjeux numériques dans le plan stratégique de l'organisation, en définissant une infrastructure cible pérenne, robuste, fiable, sécurisée, résiliente et maîtrisée (ou comprise en interne)
- Garantir que chaque nouvel outil numérique apporte une valeur durable et alignée sur les objectifs de l'organisation

Enjeux	Menaces	Risques
• Maîtrise et compréhension de son SI Comprendre les outils utilisés, leurs usages et leurs limites, même lorsqu'ils sont gérés par des prestataires • Respect des personnes Éviter la surcharge cognitive et favoriser une réflexion sur la surconsommation numérique • Maîtrise des coûts globaux Réduire les coûts humains, environnementaux et financiers des infrastructures et usages numériques (ex : allonger la durée de vie des équipements, éviter les dispositifs inutiles ou sous-exploités comme un ERP surdimensionnés) • Simplicité et clarté décisionnelle Mettre en place un cadre de décision clair, avec des rôles identifiés, permettant des arbitrages collectifs cohérents • Robustesse face aux changements Construire une stratégie numérique fiable et sécurisée, basée sur des choix limités • Alignement avec les valeurs de l'entreprise Intégrer la désescalade numérique comme principe de gouvernance, dans le cadre d'une limitation volontaire	• Pression externe à l'innovation constante Résister au techno-solutionnisme peut s'avérer difficile, notamment sans compétence métier en interne • Surconsommation technologique ○ Succomber à l'appel de l'IA et d'outils émergents ou attractifs ○ Déploiement d'outils non justifiés, entraînant gaspillage (humain, énergétique, économique), coût et complexité inutiles • Dépendance excessive aux outils numériques ○ Oubli du droit/besoin à la déconnexion. ○ Perte de capacités cognitives et de compétences • Non maîtrise des données ○ Le stockage externe, notamment en data-center, invisibilise la matérialité et favorise l'accumulation ○ Une mauvaise gestion des sauvegardes, des accès ou des partages peut entraîner des pertes, des doublons ou une altération de l'intégrité des données ○ Une gouvernance insuffisante des données peut entraîner des pratiques non conformes au RGPD	• Absence de stratégie numérique L'organisation ne définit pas ses besoins réels, ce qui entraîne un déploiement inadapté de solutions • Manque de souplesse Ne pas anticiper les évolutions possibles du SI, rendant les changements futurs plus complexes et coûteux • Responsabilité partagée mal définie Une mauvaise définition des rôles de gouvernance du numérique favorise les dérives dans l'exercice des responsabilités et les choix d'outils et d'usages numériques : décisions descendantes, concentration du pouvoir, multiples outils surdimensionnés... • L'urgence au détriment de la cohérence Privilégier une prise de décision rapide aux dépens d'une solution adaptée • Manque de visibilité sur les impacts réels L'organisation peine à mesurer les effets de ses choix numériques sur les coûts humains, environnementaux et économiques, limitant sa capacité d'arbitrage éclairé

Bonnes pratiques

1. Approche globale

- **Définir l'infrastructure cible dès le départ**
Identifier les outils, fonctionnalités et capacités nécessaires au système d'information, en cohérence avec les besoins réels de l'organisation
- **Adopter une philosophie d'auto-limitation**
Chaque nouveau projet doit répondre à une exigence de désescalade numérique, impliquant une compréhension systémique du SI

2. Processus de sélection et d'arbitrage

- **Poser les bonnes questions**
 - Chaque nouveau besoin doit être questionné au regard de sa nécessité, de sa durabilité et de sa cohérence globale
 - Structurer la prise de décision l'aide d'outils et critères simples et explicites (ex : arbre de décision)
- **Appliquer un cadre d'évaluation basé sur la désescalade numérique**
Coûts humains, sociaux, impact environnemental, simplicité d'utilisation (appropriation), durée de vie utile
- **Accepter de ne pas tout résoudre immédiatement**
Prioriser les actions en fonction des capacités réelles de l'organisation

3. Maîtrise des décisions

- Mettre en place un comité ou un rôle stratégique chargé de veiller à la désescalade numérique, afin de garantir la cohérence globale des choix numériques dans le temps
- Prendre en compte la cybersécurité pour intégrer les exigences d'intégrité, disponibilité et confidentialité

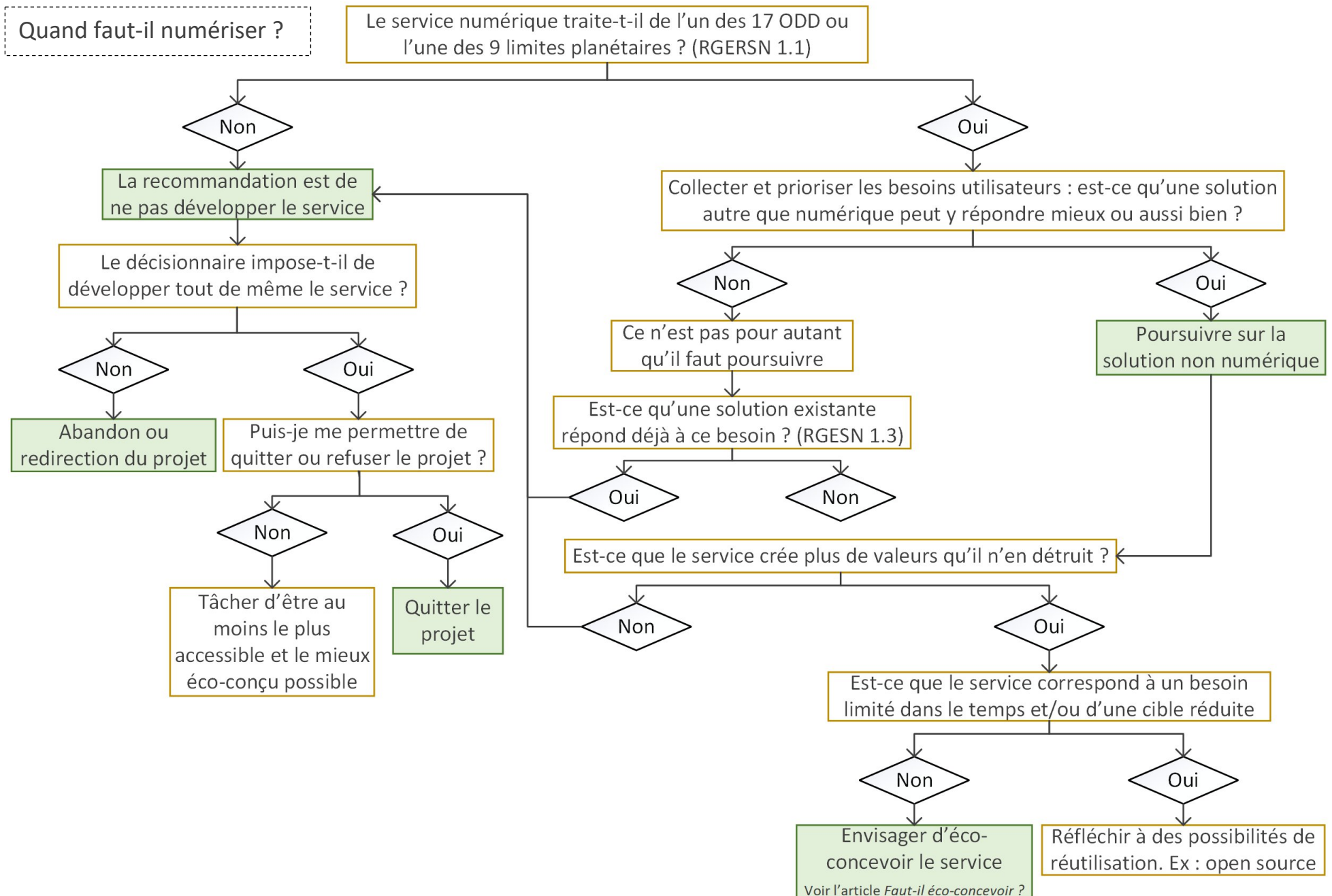
4. Suivi, audit et amélioration continue

- Suivre régulièrement les impacts du numérique au sein de l'organisation sur :
 - La charge cognitive des utilisateurs
 - La qualité des données collectées
 - Les coûts directs et indirects
- Documenter les évolutions du SI au regard des enjeux de désescalade numérique

5. Partager la vision avec les membres

- Fédérer l'ensemble des membres l'organisation autour de la désescalade numérique
- Promouvoir une vision où le refus d'un outil est aussi légitime que son adoption
- Rendre enviable les gains obtenus grâce à la désescalade (économie, gain de temps, satisfaction des utilisateurs...)

Exemple d'Arbre décisionnel : Les Designers Éthiques s'interrogent sur le fait de développer ou non un service numérique



2. DÉSESCALADE NUMÉRIQUE

Objectifs :

- Comprendre le numérique et ses effets délétères, pour fixer des limites cohérentes dans l'usage du numérique
- Refuser les outils numériques inutiles, privilégier les alternatives non numériques

Enjeux	Menaces	Risques
• Compréhension des impacts du numérique ○ Identifier les coûts humains, environnementaux et financiers cachés derrière chaque étape du cycle de vie des outils numériques ○ Prendre conscience de la matérialité des infrastructures, qui hébergent les données • Réduction de la surconsommation Éviter les déploiements inutiles ou inadaptés, et favoriser les solutions simples, durables et réutilisables • Robustesse face à la surconsommation technologique Adopter des choix cohérents avec la stratégie de gouvernance du numérique, basée sur la limitation volontaire • Favoriser la déconnexion ○ Encourager une culture de pause numérique, de reconnexion à la réalité humaine et physique ○ Réduire la surcharge cognitive et favoriser la créativité en limitant l'usage des outils numériques • Alignement avec les valeurs de l'organisation Assurer que chaque outil numérique déployé reflète les valeurs de l'organisation	• Dépendance aux fournisseurs externes ○ Les petites organisations dépendent des conseils de professionnel·les, qui devront appréhender ces enjeux ○ L'essor des services cloud et "SaaS" a entraîné une perte de conscience de la matérialité des usages, une perte de contrôle sur les données ○ Des conditions d'utilisation imposées et complexes laissent parfois à l'utilisateur la responsabilité de la sécurité des données • Inertie des processus de sélection et de décision Les critères d'évaluation et de décisions restent centrés sur la fonctionnalité, au détriment de la durabilité ou de l'éthique du produit ou service • Stagnation des pratiques face à la sobriété L'organisation continue à adopter des outils numériques par habitude, sans questionner leur vrai nécessité, impact ou coût • Diminution de l'ergonomie et de la disponibilité des outils Le taux de disponibilité peut être diminué et l'ergonomie des outils libres ou auto-hébergés est moins bien appréhendée	• Mobilisation accrue de ressources La (ré)internalisation du SI génère un besoin accru en matériel, en compétences, et en temps de formation • Déconnexion du contexte métier Par leur manque d'envergure, les solutions adoptées ne répondent pas aux besoins réels du métier • Mécontentement des utilisateurs et "Shadow IT" ○ La sobriété est perçue comme une limitation ○ La frustration génère des conflits internes, une baisse de motivation ou l'utilisation de ressources numériques non autorisées (Shadow IT), entraînant fragmentation, risques juridiques et incohérence stratégique • Perte de compétitivité Acceptation d'un possible renoncement à certaines opportunités en refusant le techno-solutionnisme, en cohérence avec le positionnement stratégique de limitation volontaire et de stabilité sur son marché • Vulnérabilité réglementaire Écarts avec les obligations légales applicables à la gestion des données personnelles (RGPD)

Bonnes pratiques

1. Approche globale

- **Définir précisément la vision de la sobriété numérique en lien avec la vision stratégique**
Fixer une zone d'action limitée et cohérente : ne pas revenir à des pratiques obsolètes (Non, on ne se remettra pas à envoyer des lettres timbrées pour correspondre !) ou des pratiques trop dissonantes (Non, on ne laissera pas les IA rédiger nos mails !)
- **Évaluer chaque outil selon son impact environnemental, son coût humain, son utilité et son utilisation réelle**
- **Utiliser des outils d'aide à la décision comme un arbre décisionnel ou une matrice RACI qui définit les rôles et responsabilités de chacun (les outils peuvent être utilisés à différentes échelle par ex gouvernance ou projets)**

2. Autonomisation

- Acculturer l'ensemble de l'organisation à la désescalade numérique
- Se réapproprier le SI : comprendre sa matérialité, ses coûts, ses impacts, et ses limites
- Transmettre les connaissances sur la gouvernance du numérique à toute personne qui le souhaite, en définissant des rôles clairs et en assurant la cohérence avec la stratégie globale

3. Gestion des relations prestataires

- Ne pas succomber aux discours des prestataires qui orientent vers des solutions cloud ou SaaS sans justification
- Ne pas succomber à la facilité de l'ergonomie des produits des géants du numérique (Big Tech)
- Challenger activement les prestataires en fonction des obligations légales et des objectifs de sobriété

4. Co-construction avec les équipes

- Impliquer les membres de l'organisation dans la conception et la sélection des outils numériques permet de répondre à leurs aspirations et aux besoins métiers.
- Définir clairement les rôles, avec le comité de surveillance chargé de veiller au respect de la vision stratégique

5. Vigilance juridique

- Assurer que chaque outil déployé respecte les obligations légales (RGPD, RGESN, RGAA,...)
- Se référer à des juristes spécialisé·es dans le numérique, si besoin

6. Privilégier les alternatives non numériques

Droit au refus d'outils numériques pour des raisons de sobriété, si des alternatives sobres et viables sont clairement établies

7. Rendre enviable les gains de la sobriété

Mettre en avant les bénéfices : économie, gain de temps, satisfaction, réduction de la surcharge cognitive, résilience, maîtrise du SI

Extrait de la matrice de responsabilités "RACI", de la boîte à outils InfraBasse

Axe	Mission	Responsable (Responsible)	Décisionnaire (Accountable)	Personnes consul- tées (Consulted)	Personnes infor- mées (Informed)
1. Stratégie	Définir la stratégie numérique				
	Suivre son évolution				
	Piloter la gouvernance du numé- rique				
2. Désescalade	Identifier les usages non essen- tiels				
	Proposer et choisir des alterna- tives sobres ou non numériques				
3. Appropriation	Cartographier les compétences et appétences internes				
	Planifier formations et transfert de compétences				
4. Pérennité	Réaliser et suivre les audits or- ganisationnels et techniques				
	Anticiper les risques d'obsoles- cence (outils, formats, compé- tences)				
5. Cybersécurité	Maintenir à jour la documenta- tion de sécurité et veiller à l'ap- plication des règles définies				
	Assurer la veille réglementaire				
	Prévenir et gérer les incidents de sécurité				

3. L'ÂME DE L'ORGANISATION

Objectif :

- Garantir que la gouvernance reste alignée avec les vrais besoins des membres, pour leur permettre de s'en approprier les usages
- Embarquer les équipes dans la mise en place des nouveaux projets en prenant en compte leurs compétences et leur **appétence**

Enjeux	Menaces	Risques
• Créer un climat de confiance en permettant une participation active dans les décisions stratégiques ○ Favoriser les processus de co-construction et de co-décision structurés par la stratégie de gouvernance du numérique ○ Intégrer les membres dans la culture de la désescalade numérique • Valoriser les appétences puis les compétences ○ Identifier les motivations, les attentes et les compétences des membres de l'organisation pour concevoir les projets en cohérence avec leurs considérations ○ Créer des mécanismes où chaque apport pertinent est reconnu et pris en compte • Création d'un sentiment d'appartenance Impliquer les membres de l'organisation en amont et favoriser un dialogue continu dans le chemin de la désescalade numérique pour susciter une adhésion durable et éviter la perception d'une sobriété imposée • Alignement avec les valeurs de l'ESS et de la RSO (Responsabilités Sociétales des Organisations) Adopter une gouvernance partagée permet de s'aligner sur des modèles valorisés dans l'ESS ainsi que dans les démarches RSO et NR (Numérique Responsable)	• Concertation symbolique Processus participatifs sans réel pouvoir d'influence sur les décisions structurantes • Désengagement Des processus longs ou peu conclusifs favorisent un manque d'implication des membres de l'organisation • Manque de cadre clair Sans un cadre décisionnel et opérationnel clairement structuré, une participation active de l'ensemble des équipes peut rendre le processus chaotique • Conflit entre compétences et appétences ○ Le désir d'acquérir de nouveaux savoirs nécessite un besoin en formation ○ Tension entre motivations individuelles et capacités réelles de mise en œuvre • Résistance au changement Blocage de projets ou inertie organisationnelle • Frustration liée aux outils choisis	• Tension entre gouvernance partagée et efficacité opérationnelle ○ Allongement des délais de prise de décision en l'absence de processus décisionnel clairement structuré ○ La complexité de la coordination pourrait ralentir la réalisation des projets • Fragmentation Concentration informelle du pouvoir décisionnel autour de certains profils, malgré un cadre participatif affiché • Rotation importante Perte de compétences et d'engagement liés à la gouvernance participative en cas de départ de membres clés : les appétences et compétences annexes ne dépendent pas de la fiche de poste initiale. • Fatigue décisionnelle Les membres pourraient se sentir épuisées par la multiplicité des consultations ou des ateliers, ce qui peut nuire à la qualité des contributions

Bonnes pratiques

1. Approche globale

- **L'âme de l'organisation au cœur de toutes les décisions**
 - Intégrer la participation des membres de l'organisation comme principe fondamental de la gouvernance numérique
 - Assurer que chaque décision stratégique ou opérationnelle prenne en compte les compétences, les appétences et les valeurs des équipes
 - Structurer les décisions selon les principes InfraBasse (cf lois InfraBasse, page suivante)
 - Veiller à ce que les membres soient impliquées en amont et accompagnées tout au long du projet

2. Sincérité de la démarche

- Assurer que la participation soit utile, clairement cadrée, et proportionnée au niveau réel d'influence, afin qu'elle puisse impacter la décision finale
- Éviter la rupture des projets en s'engageant à hauteur de ses possibilités

3. Communication et accompagnement en interne

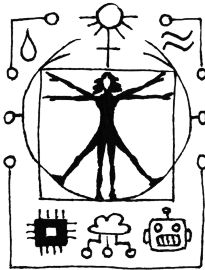
- Mettre en place un cadre de communication clair et régulier pour informer
- Collecter et valoriser les retours des équipes pour améliorer le processus et les projets futurs, transformant ainsi le dialogue en boucle d'amélioration continue
- Acculturer les membres de l'organisation à la désescalade numérique
- Favoriser un dialogue continu entre les équipes et les décideurs, afin de maintenir l'adhésion et éviter la perception d'une sobriété imposée
- Assurer un suivi régulier du fonctionnement des processus participatifs pour ajuster et améliorer la gouvernance

4. Vigilance accrue quant à la gestion des risques

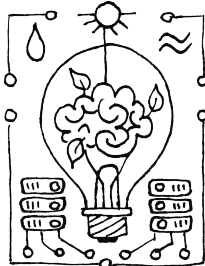
- Anticiper la continuité en cas de départ ou d'absence, en prévoyant des doublons et transferts de compétences
- Éviter les déséquilibres de pouvoir en assurant le respect de l'opinion de chaque membre et en mettant en place des mécanismes de conciliation
- Si besoin, solliciter un soutien externe spécialisé dans la gouvernance ou médiation des organisations

Les autres axes s'appuieront sur ces trois premiers, qui constituent les fondations de la gouvernance du numérique d'InfraBasse.

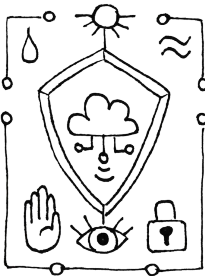
De ces fondations émergent trois lois qui irriguent l'ensemble du référentiel :



L'humain prime sur la technologie



La sobriété éclairée prime sur toute décision technologique



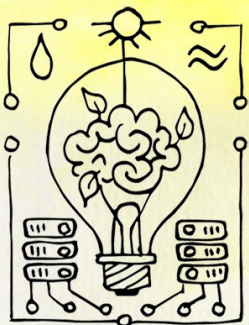
Toute technologie doit être limitée, maîtrisée et justifiée

Comme l'arbre inversé de l'illustration, InfraBasse emprunte une voie différente de celle de la croissance infinie.

À l'image des racines qui portent le tronc, les fondations d'InfraBasse portent ses piliers.

La gouvernance opérationnelle, ne peut se déployer durablement que dans cet équilibre global.

La partie opérationnelle s'appuie sur des choix de gouvernance structurés (Les fondations) et sur la lecture transversale du SI qui en découle (Les piliers).



La sobriété éclairée prime sur toute décision technologique



L'Humain prime sur la technologie



Toute technologie doit être limitée, maîtrisée et justifiée

Axes
1 à 3
Les
Fondations

Axes
4 à 7
Les
Piliers

Axes
8 à 12
La
Gouvernance
Opérationnelle

Partie 2 : LES PILIERS

Axe 4 – Pérennité du système d'information

Axe 5 – Cybersécurité

Axe 6 – Maîtrise des données

Axe 7 – Les infrastructures : la porte d'entrée d'InfraBasse

Une fois les fondations posées, la gouvernance du numérique se traduit dans la structure même du SI.

Cette deuxième partie aborde les piliers techniques et organisationnels qui soutiennent concrètement la stratégie InfraBasse.

Elle vise à construire un SI pérenne, maîtrisé et aligné avec les principes définis précédemment.

InfraBasse fait le choix d'une approche par les infrastructures, qui permet de rendre visible la matérialité du numérique et les dépendances qu'elle implique. (cf. le guide de réflexion "InfraBasse, Visibiliser ses infrastructures numériques pour les comprendre")

Ces piliers interagissent en permanence et doivent être pensés comme un ensemble cohérent et interdépendant.

4. PÉRENNITÉ DU SYSTÈME D'INFORMATION

Objectif

- Disposer d'un SI fiable et robuste, conçu pour durer, et gérer ses ressources afin de limiter les évolutions nécessaires.

Enjeux	Menaces	Risques
• Ressources stables ○ Choisir équipements, logiciels, et méthode de gestion de données en fonction de leur durée de vie ou de leur origine ○ Privilégier l'auto-hébergement ou des prestataires alignés sur les principes d'InfraBasse ○ Éviter les dépendances vers des fournisseurs ou technologies émergentes (cloud, IA SaaS, etc.) • Maîtrise du SI Autonomiser les membres de l'organisation, même sans service informatique, par l'internalisation ou participation active à l'administration du SI • Pertinence des choix Maîtriser son SI permet de faire des choix objectifs, et ne plus dépendre exclusivement de conseils externes • Maîtrise des usages ○ Comprendre l'usage des outils (fréquence, intensité, contexte) pour anticiper les besoins ○ Encourager une culture de sobriété numérique dans l'usage des outils — pas seulement dans leur déploiement	• Coûts de déploiement La (ré)internalisation du SI peut entraîner des coûts supplémentaires en termes de déploiement, de maintenance, et d'adaptation des équipes • Mauvaise appropriation interne ○ Manque de formation aux outils déployés ○ Mauvaise communication de la vision • Évolution rapide des technologies Nouvelles dépendances à des technologies émergentes, auxquelles certaines infrastructures ne pourront pas répondre • Manque de gouvernance de la pérennité ○ Mauvaise gestion des changements ○ Manque de mécanismes de suivi et d'évaluation des coûts et des usages • L'obsolescence programmée Logicielle et matérielle • Dépendance aux constructeurs ou fournisseurs Les fournisseurs de cloud, de logiciels ou de produits numériques peuvent imposer des conditions d'utilisation ou de fin de vie • Pertes de compétences Si les procédures d'administration et d'utilisation ne sont pas documentées, les compétences peuvent se perdre en cas de départ d'un·e membre clé	• Manque d'évolutivité ○ Le SI ne s'adapte plus aux évolutions des besoins métier et se déconnecte progressivement de son contexte. ○ Les outils perdent progressivement leur adéquation avec les usages réels et leur valeur pour l'organisation • Perte de disponibilité ○ Diminution de la productivité ○ Des services non disponibles entraînent non seulement une perte de confiance des membres, mais aussi une surcharge pour les équipes de support • Perte de praticité des usages Les changements d'usage peuvent entraîner une perte de repères • Charge de gestion accrue (Ré)Internalisation et pérennisation augmentent le besoin de compétences et en coordination

Bonnes pratiques

1. Approche globale

- **Faire un audit technique pour dimensionner de façon adaptée son SI**
 - Réaliser un audit de gouvernance puis un audit technique
 - Respecter les lois InfraBasse
 - Faire des choix éclairés sur le SI
- **Accepter les contraintes techniques liées à la désescalade numérique tant qu'elles garantissent le bon déroulement des processus métiers**

2. Maintenir un système d'information adapté aux besoins de l'organisation en condition opérationnelle

- Valoriser la maintenance technique et la maintenance physique du matériel et des locaux

3. Former et autonomiser les membres de l'organisation

- **Administration** : former les équipes pour qu'elles assurent la gestion du SI et réalisent les interventions techniques les plus simples
- **Utilisation** : organiser des formations et développer le transfert de compétences internes pour maîtriser une utilisation efficace des outils

4. Maîtrise de la démarche de pérennité

- Appropriation et autonomisation sur le SI
- Limiter les usages aux capacités et contraintes matérielles du SI
- Challenger les prestataires qui proposent une assistance à la (ré)internalisation et contractualiser une obligation de résultats
- Choisir le matériel en fonction de son évolutivité et sa réparabilité, et des fins de vie programmée (EOL/EOS – End of Life/End of Support)

5. Procédures et documentation

- Élaborer et mettre à jour les procédures d'administration et d'utilisation (Matrice des responsabilités, matrice compétences/appétences pour identifier les besoins en formation...)
- La gestion de la documentation et de ses accès doit être clairement établie pour que les documents soient consultables par tous les membres concernés

6. Assurer des doublons dans les fonctions de gouvernance pour anticiper les départs ou changement d'aspiration

Extrait tableur compétences, appétences et dynamique de formation, de la boîte à outils InfraBasse

Théma- tiques	Architecture & compréhension du SI		Infrastructures & exploitation		Cybersécurité & gestion des risques		Gouvernance & gestion des données		Outils & services numériques (usage)		Pilotage des prestataires & de l'écosystème		Pilotage économique & TCO		Conduite du changement & culture numérique		Gestion de projet	
Perti- nence pour l'or- ganisa- tion	5		5		3		4		4		3		3		4		2	
Per- sonnes	Appé- tence	Compé- tence	Appé- tence	Compé- tence	Appé- tence	Compé- tence	Appé- tence	Compé- tence	Appé- tence	Compé- tence	Appé- tence	Compé- tence	Appé- tence	Compé- tence	Appé- tence	Compé- tence	Appé- tence	Compé- tence
Pierre	4	5	4	4	2	4	2	4	5	5	4	5	4	4	3	4	2	4
	Formateur·ice		Formateur·ice		Doit transférer ses compétences		Doit transférer ses compétences		Formateur·ice		Formateur·ice		Formateur·ice		Référent·e		Doit transférer ses compétences	
Pauline	4	3	3	3	3	4	4	3	3	3	3	4	4	4	3	4	2	2
	Référent·e		Référent·e		Référent·e		Référent·e		Référent·e		Référent·e		Formateur·ice		Référent·e		/	
Jackie	2	4	4	4	4	3	4	4	3	3	2	4			4	3	2	2
	Doit transférer ses compétences		Formateur·ice		Référent·e		Formateur·ice		Référent·e		Doit transférer ses compétences		/		Référent·e		/	
Maï	4	4	2	4	2	2			2	3					2			
	Formateur·ice		Doit transférer ses compétences		/		/		/		/		/		/		/	
Nahel	4	2							2	3								
	Envie de formation		/		/		/		/		/		/		/		/	
Actions	Transfert de compétences interne - Moyen terme		Maintenir et à réévaluer à moyen ou long terme		Transfert de compétences interne - Court terme		Transfert de compétences interne - Court terme		Transfert de compétences interne - Long terme		Transfert de compétences interne - Long terme		Maintenir et à réévaluer à moyen ou long terme		Formation externe ou temps d'auto-formation - Court terme		Transfert de compétences interne - Court terme	
Criticité	1 - Pas urgent		1 - Pas urgent		5 - Très urgent		4 - Urgent		3 - Urgence modérée		2 - Peu urgent		1 - Pas urgent		5 - Très urgent		5 - Très urgent	

5. CYBERSÉCURITÉ

Remarque

- La sécurité du SI doit être pensée en fonction des besoins et usages de l'organisation. InfraBasse ne se substitue pas à un référentiel de cybersécurité. Elle propose un cadre de gouvernance permettant d'intégrer la cybersécurité dans une démarche cohérente et proportionnée.

Objectif

- Prendre en compte la cybersécurité en adoptant une démarche de protection adaptée aux enjeux réels et alignée sur les valeurs, la stratégie de désescalade numérique et les usages de l'organisation.

Enjeux	Menaces	Risques
● La cybersécurité selon InfraBasse ○ Penser la cybersécurité comme un équilibre entre protection et sobriété ○ Éviter l'escalade technologique sécuritaire en privilégiant la maîtrise interne et des dispositifs simples et robustes ● Confidentialité, Intégrité et Disponibilité Inscrire ces piliers de la sécurité des données dans le respect du triptyque InfraBasse (humain, sobriété, maîtrise) ● Fiabilité et résilience du SI ○ Assurer la continuité des processus métier en cas d'incident ou d'attaque ○ Mettre en place des mécanismes de sauvegarde et de récupération adaptés ○ Éviter les dépendances critiques vers des technologies ou fournisseurs externes peu fiables ● Gouvernance des risques et des menaces ○ Identifier et hiérarchiser les risques et menaces spécifiques à l'organisation ○ Mettre en place des mécanismes d'évaluation régulière (évaluations, tests...) ● L'âme de l'organisation au cœur des enjeux de cybersécurité	● La sobriété au détriment de la sécurité ○ Réduction excessive des dispositifs de protection ○ Sous-estimation des menaces réelles ● La sécurité au détriment de la sobriété Multiplication d'outils spécialisés complexes et coûteux, et dépendance accrue aux solutions propriétaires ● Élargissement de la surface d'exposition ○ Usage d'équipements personnels pour des usages professionnels ○ Objets connectés et services externes non maîtrisés ● Manque de compétences internes ○ Difficulté à identifier l'ensemble des risques ○ Absence de culture de cybersécurité, pouvant induire un manque de maintenance et de mises à jour de sécurité ○ Dépendance aux conseils externes sans capacité de discernement ● Lassitude des équipes Accumulation de contraintes perçues comme excessives ● Non-respect des contraintes réglementaires Méconnaissance des exigences légales	● Déséquilibre sécurité / sobriété Perte de cohérence stratégique en cas de sur-sécurisation ou de sous-protection ● Inadéquation de la politique de sécurité aux usages réels ○ Perte de vigilance, de motivation et de confiance des membres qui ne se sentent pas impliqués dans des dispositifs trop complexes ou mal adaptés, pouvant générer contournement (shadow IT) et une fatigue cognitive ○ Retour à des pratiques peu contrôlées si les dispositifs deviennent trop contraignants ● Perte d'efficacité ou de disponibilité Une mauvaise maîtrise des menaces augmente les risques de cyber-malveillance ou de perte de données ● Fragilité des conditions physiques et environnementales Disponibilité perturbée si les risques liés au contrôle d'accès, aux incendies, à la non redondance électrique ou de climatisation sont négligés ● Risque financier et juridique Sanctions financières, perte de productivité et atteinte à la réputation en cas d'incident ou de non-conformité réglementaire

Bonnes pratiques

1. Approche globale

- **Intégrer la cybersécurité dans la stratégie InfraBasse**
 - Définir les rôles de gestion de la cybersécurité au sein du comité de gouvernance du numérique (RACI)
 - Définir les menaces et risques pour sa structure et adapter le niveau de sécurité à mettre en place
 - Penser à la matérialité des infrastructures
 - Accepter certaines contraintes liées à la préférence d'un plan de reprise d'activité (PRA) numérique robuste face à un plan de continuité d'activité (PCA) plus sobre. Exemple : accepter une demi-journée d'indisponibilité planifiée dans un PCA sobre. Le PRA assurera une reprise d'activité rapide.

2. Définir une Politique de Sécurité des Systèmes d'Information

- La PSSI doit être simple, compréhensible, proportionnée et alignée sur la stratégie InfraBasse
- La PSSI doit définir un certain nombre de choses telles que les rôles et responsabilités, les règles d'accès aux données, la gestion des mots de passe et méthode d'authentification, la gestion des incidents, les politique de sauvegarde, continuité et reprise d'activité, etc. Selon les cas, un·e expert·e en cybersécurité devra vous accompagner pour réaliser ce travail
- La PSSI doit être validée par la gouvernance et connue de tous

3. Établir des Plan de Continuité d'Activité (PCA) et Plan de Reprise d'Activité (PRA) en cohérence avec la stratégie de gouvernance

- Le PCA organise le fonctionnement dégradé alors que le PRA organise le retour au fonctionnement normal
- Le PCA identifiera les processus métiers essentiels et définira des alternatives non numériques temporaires. Il formalisera les priorités du PRA
- Le PRA a pour objectif d'assurer un retour maîtrisé au fonctionnement normal du SI après un incident majeur :
 - Il formalise les priorités de reprise en cohérence avec les processus métiers essentiels
 - L'organisation doit pouvoir absorber une perturbation sans perte de maîtrise
- Dans l'esprit InfraBasse, le PCA **accepte la contrainte**, le PRA **restaure la stabilité**

4. Formation et sensibilisation

- Sensibiliser à la cybersécurité
- Former l'ensemble de l'organisation aux pratiques de sécurité mises en place en interne

5. Établir et mettre à jour une charte informatique

La charte doit :

- Être co-construite avec les équipes, régulièrement mise à jour et adaptée aux nouvelles menaces et pratiques
- Être courte, agréable à lire et compréhensible
- Définir les usages autorisés, y compris des équipements personnels dans le cadre professionnel
- Être signée et actualisée (+ autres contraintes réglementaires en fonction de la taille de la structure)

Modèle de fiche pratique de l'usage et la sécurité du numérique, de la boîte à outils InfraBasse

Objet

Le présent document définit les règles d'usage des outils numériques, des données et des infrastructures de l'organisation. Elle vise à garantir un usage sobre, sécurisé, compréhensible et maîtrisé du système d'information.

Principes généraux

L'organisation s'engage à un numérique :

- utile uniquement lorsqu'il apporte une valeur réelle
- sobre par conception (limitation des outils et des données)
- maîtrisé en interne autant que possible
- respectueux des personnes et des usages
- compatible avec la désescalade numérique

Le saviez-vous ?

Une donnée personnelle est une donnée qui permet d'identifier une personne : nom, mail, téléphone, adresse, CV, etc.

L'usage et le traitement des données personnelles est strictement encadré par le RGPD (règlement général sur la protection des données)

Le numérique, une responsabilité collective

Chacun contribue à améliorer le système d'information en :

- Exprimant son point de vue
- Proposant des améliorations
- Participant à la sobriété numérique

Données

Les données sont un patrimoine commun.

Elles doivent être :

- Nécessaires et uniques
- Correctement stockées
- Classées selon leur sensibilité
- Supprimées ou archivées quand elles ne sont plus nécessaires
- Confiées avec prudence à des tiers (IA, logiciels web gratuit type Notion...). Il faut bannir la saisie de données personnelles en ligne

La sobriété numérique

- Limiter les outils redondants, les données inutiles et les usages non essentiels
- Privilégier la simplicité et les formats ouverts
- Tout usage doit rester simple, compréhensible et justifié

Sécurité

La sécurité du système d'information passe par une vigilance quotidienne :

- Respecter les rôles attribués à la cybersécurité au sein du comité de gouvernance du numérique
- Vérifier l'expéditeur et le contenu avant de cliquer sur une pièce jointe ou un lien
- Verrouiller sa session
- Respecter la confidentialité
- Ne pas brancher de périphériques tiers
- Signalement des anomalies (cf contact)

Accès aux outils

- Chaque personne dispose des accès nécessaires à ses besoins.
- Les accès sont personnels, non partagés et contrôlés.
- Les comptes d'administration sont nominatifs

Outils, services et matériel

- Seuls les outils validés par l'organisation sont utilisés.
- Toute exception doit être signalée et justifiée.
- Le matériel est utilisé avec soin et conservé le plus longtemps possible.
- Le remplacement n'intervient qu'en cas de nécessité réelle.

Mot de passe

Il doit être :

- Unique pour chaque compte important
- Confidentiel : ne pas le partager par mail, messagerie instantanée ou téléphone. Ne pas l'écrire sur papier en clair sur papier ou fichier

Communication

- Les outils collaboratifs sont utilisés de façon cohérente et structurée.
- On évite la dispersion des canaux et des informations.

En cas de doute ou d'incident

Pour toute question ou doute (mail suspect, problème de mot de passe, incident de sécurité, perte ou vol de matériel) : contact principal : support / DSI / RSSI (mail, téléphone)

6. MAÎTRISE DES DONNÉES

Objectifs

- Gérer, organiser, valoriser et maîtriser le cycle de vie des données comme un patrimoine informationnel, en assurant le triptyque de sécurité : Confidentialité, Intégrité, Disponibilité
- Optimiser leur volume en maîtrisant la production et en adoptant des pratiques de limitation des collectes, d'archivage et de suppression

Enjeux	Menaces	Risques
• Gouvernance des données ○ Gérer les droits d'accès ○ Classifier et marquer les données selon leur niveau de protection, criticité et étape de leur cycle de vie ○ Disposer d'un document descriptif de l'espace numérique commun • Ressources fiables et accessibles ○ Garantir la précision, la cohérence et la mise à jour des données utilisées dans les processus métier ○ Prévoir des mécanismes d'accès simples aux versions précédentes des documents, sans démultiplier la capacité de stockage • Efficacité et durabilité ○ Évaluer de façon fiable la quantité de données à gérer ○ Estimer la croissance des données ○ Réduire les volumes inutiles • Expertise interne ○ Préférer des solutions internes ou maîtrisées ○ Limiter les dépendances vis-à-vis de services externes sur les données critiques ○ Pratiquer l'archivage définitif et la suppression de données	• Accès non autorisé ou mal géré ○ Mauvaise définition ou attribution des droits d'accès aux données ○ Risque d'actions non tracées ou non auditées • Croissance des données non maîtrisée ○ Accumulation continue de données sans tri, archivage ou suppression • Dépendance aux prestataires externes ○ Externalisation du traitement et du stockage des données, reposant sur des engagements contractuels (SLA, CGU) souvent complexes ou peu lisibles, ce qui peut donner une illusion de protection sans garanties réellement maîtrisées • Non appropriation des solutions choisies en interne ○ Manque d'adhésion et d'acculturation des membres de l'organisation • Difficulté d'usage ○ La multiplication des outils, l'absence de consignes partagées et l'hétérogénéité des pratiques complexifient leur appropriation • Obsolescence des formats ou des systèmes de données ○ Absence de mises à jour ou abandon des solutions utilisées	• Déséquilibre entre sobriété et sécurisation des données ○ Une politique de sauvegarde insuffisante ou inadaptée peut entraîner une perte irréversible d'informations stratégiques • Enfermement technologique des données ○ Difficultés ou impossibilité d'extraire ou migrer des données vers d'autres solutions • Surcharge et complexité de l'environnement numérique ○ L'excès de données nuit au bien-être, à l'efficacité et à la prise de décision ○ La multiplication des espaces de stockage et des applications pour y accéder développe le 'stress numérique' (fatigue informationnelle) • Mauvaise structuration documentaire ○ Une organisation incohérente des espaces et fichiers entraîne des erreurs, une fatigue émotionnelle, une perte de temps • Dégradations de la qualité des données ○ Des données obsolètes, incohérentes ou non à jour entraînent des décisions inadaptées • Non-respect des obligations légales et contractuelles (RGPD...)

Bonnes pratiques

1. Approche globale

- **Adopter une gestion des données sobre et résiliente**
 - Définir une stratégie de données alignée sur la sobriété, les contraintes légales et réglementaires et les besoins métiers
 - Cartographier les flux de données et leur cycle de vie (création, stockage, utilisation, archivage, destruction), en assurant des mises à jour qui intègrent les évolutions et les nouvelles exigences
 - Classifier les données
 - Gérer les accès et leur traçabilité

2. Gouvernance et gestion de la documentation

- Mettre en place un comité de gouvernance des données avec des rôles clairs et charger de la veille réglementaire
- Tenir un registre de traitement des données personnelles
- Documenter les règles d'accès, de responsabilité et de conformité
- Créer et mettre à jour un document descriptif de l'espace numérique commun, en classifiant les données (niveau de protection, criticité, cycle de vie)
- Rendre disponible et facile d'accès les procédures

3. Sécurité et conformité

- Compléter la PSSI par une politique spécifique de gestion et de protection des données

4. Maîtrise du cycle de vie des données

- Définir des durées de conservation adaptées à la nature des données, en évaluant leur besoin réel de conservation
- Mettre en place des règles claires d'archivage et suppression définitive

5. Qualité des données

- Mettre en place des règles de nommage et marquage communes
- Limiter les doublons ou le "versioning manuel"
- Centraliser les référentiels critiques

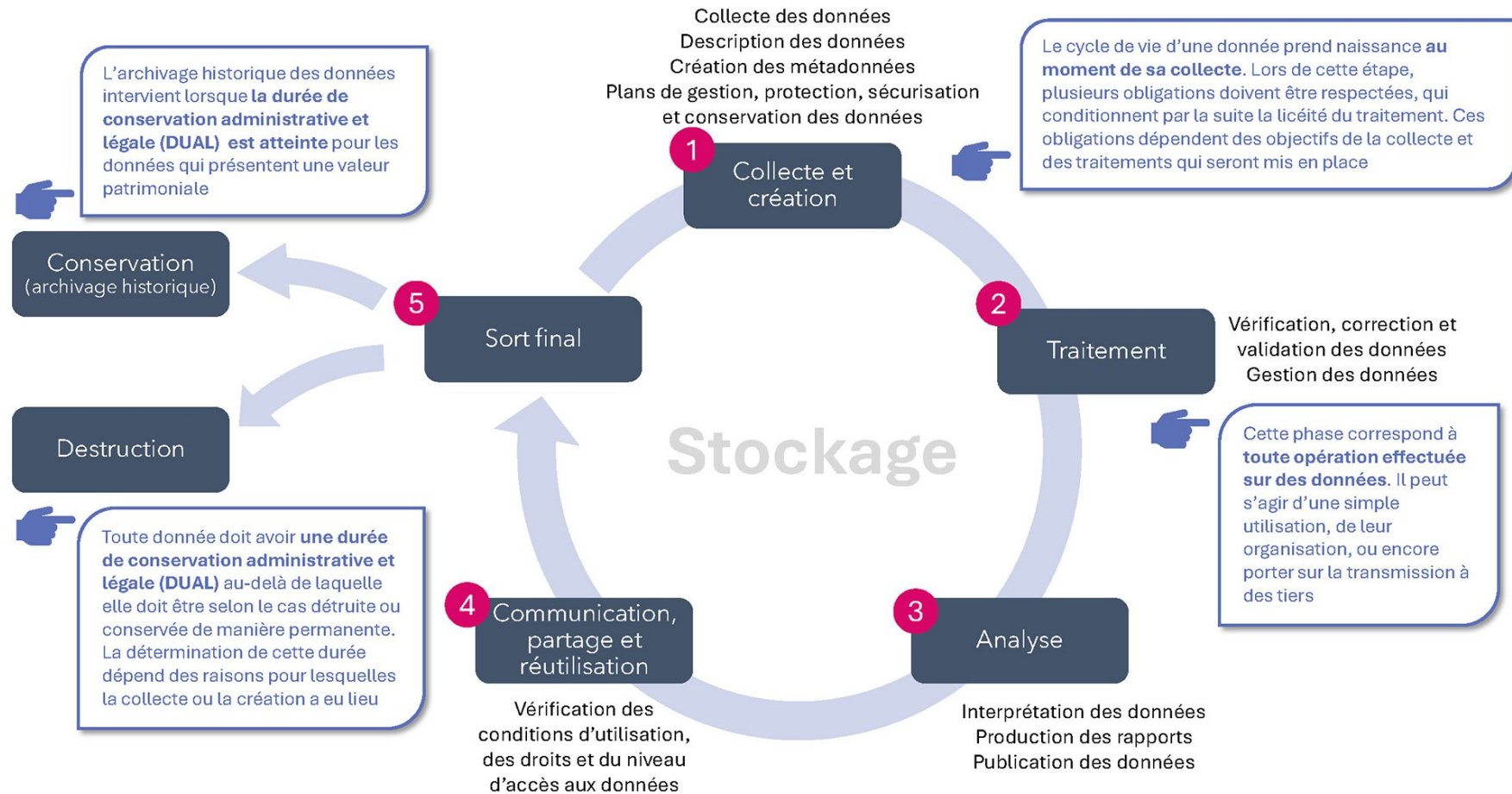
6. Sensibilisation à la sobriété informationnelle

- Former les équipes à produire seulement l'essentiel
- Encourager le nettoyage régulier des espaces communs
- Valoriser les bonnes pratiques de gestion documentaire

7. Interopérabilité et pérennité

- Privilégier les formats ouverts et standards, pour assurer la portabilité des données
- Tester les exports et les migrations, anticiper les éventuels problèmes de compatibilité, sauvegarder les outils d'installation des applications

Le cycle de vie de l'information numérique



7. LES INFRASTRUCTURES : LA PORTE D'ENTRÉE D'INFRABASSE

Objectif

- Penser l'architecture de ses infrastructures dans un principe de limitation volontaire

Enjeux	Menaces	Risques
• Juste dimensionnement* ○ Définir des capacités suffisantes mais limitées pour éviter le sur-dimensionnement et les coûts cachés ○ Concilier sobriété, performance et coût avec les besoins métiers réels • Autonomisation* ○ Doter les équipes des compétences pour comprendre, dépanner et maintenir l'infrastructure ○ Réduire les dépendances externes tout en garantissant le niveau de sécurité et de disponibilité adapté à l'organisation • Compréhension des liens entre Infrastructure et usages* Cartographier l'infrastructure, les flux, les dépendances applicatives et les besoins de données • Soin, surveillance et durabilité du matériel* ○ Superviser et contrôler ses infrastructures ○ Prolonger la durée de vie du matériel et favoriser son réemploi en interne ○ Définir une politique d'achat responsable	• Coûts de maintenance lié à un SI internalisé ○ Mises à jour matérielles et logicielles, pouvant entraîner une indisponibilité ○ Surcharge de travail et mise en difficulté lié à un temps de maintenance trop important • Passer à côté d'innovations technologiques Ne pas tirer parti des innovations, des offres de produits et services et des opportunités technologiques • Infrastructures mal dimensionnées Capacités insuffisantes de l'infrastructure face à de nouveaux besoins • Environnement inadapté Manque d'entretien des infrastructures • Perte du contrôle du SI ○ Shadow IT généralisé ○ Utilisation anarchique des offres cloud et SaaS • Dépendance aux prestataires pour le matériel critique ou le réseau La multiplicité des prestataires peut entraîner une difficulté de compréhension et une redondance inutile du matériel	• Manque d'évolutivité Bridier la capacité d'évolution du SI par manque de rationalisation • Manque de compétences internes Forte dépendance aux prestataires pour conseils et support technique • Organisation de la gestion du SI obscure L'absence de méthodologie de gestion du SI peut entraîner manque d'efficacité, stress et erreurs en cas de problème • Fragmentation des outils et composants Trop de solutions disparates peuvent complexifier la maintenance, le dépannage et le transfert de compétence en interne • Pannes ou interruptions de services liées à l'infrastructure Accepter une perte de productivité en cas de "panne sèche" • Problèmes de compatibilité

Bonnes pratiques

1. Approche globale

- Définir une architecture cible alignée sur les lois InfraBasse et les besoins métiers
- Documenter les liens entre composants (serveurs, stockage, réseau, sécurité) et les usages qu'ils supportent
- Mettre en place une politique d'achat favorisant le réemploi, la compatibilité et l'interopérabilité ainsi que le matériel re-conditionné lorsque cela est pertinent

2. Gouvernance et traçabilité

- Clarifier les responsabilités et assurer la traçabilité des choix et des coûts, en établissant des contrats de niveau de service (SLA) précis et compréhensibles
- Mener une analyse de risques de l'infrastructure et avoir un process de détection et traitement des vulnérabilités
- Avoir des prévisions d'évolutions à la hausse ou à la baisse réalistes
- Mettre en place un suivi régulier des mises à jour et correctifs critiques
- Garantir la bonne gestion et l'alignement de l'infrastructure avec les orientations définies en évaluant disponibilité, coût total de possession (TCO), temps moyen de restauration, nombre d'incidents, taux de conformité...

3. Matériel et hébergement

- Privilégier l'auto-hébergement, avec du matériel qui supporte les conditions environnementales du local prévu
- Prévoir du matériel évolutif et réparable
- Définir des configurations minimales suffisantes pour les usages
- Avoir une politique de fin de vie du matériel clairement définie et en lien avec des opérateurs de confiance

4. Autonomie

- Former les équipes à l'administration de l'infrastructure, suivant les rôles clairement établis dans la gouvernance du SI
- Mettre en place des procédures simples de dépannage
- Mettre en place des règles claires pour l'évolutivité et la conservation des configurations

5. Procédures et documentation

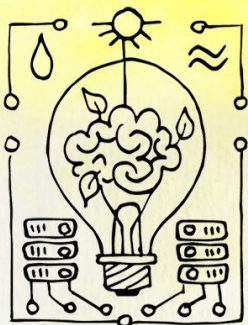
- Chaque outil numérique doit faire l'objet d'une procédure (même si la procédure est "contacter tel prestataire")
- Documenter les dépendances critiques et interactions entre composants pour faciliter maintenance et évolution
- Les procédures doivent être facilement accessibles à l'ensemble des membres concerné-es

Les piliers présentés dans cette partie structurent la dimension technique et organisationnelle du système d'information.

La méthodologie InfraBasse propose une entrée par les infrastructures et repose sur un principe d'auto-limitation.

L'interdépendance de ces piliers souligne toutefois que ces infrastructures ne peuvent être pensées indépendamment des usages. Les choix opérationnels, de sécurité ou de gestion des données influencent directement les pratiques, les comportements et l'autonomie des équipes.

Même si l'entrée se fait par le matériel, les usages restent au centre des décisions.



La sobriété éclairée prime sur toute décision technologique



L'Humain prime sur la technologie



Toute technologie doit être limitée, maîtrisée et justifiée

Axes 1 à 3 Les Fondations

Axes 4 à 7 Les Piliers

Axes 8 à 12 La Gouvernance Opérationnelle



Partie 3 : LA GOUVERNANCE OPÉRATIONNELLE

Axe 8 - Projets

Axe 9 – Prestataires et fournisseurs

Axe 10 – Services numériques

Axe 11 – Maîtrise du budget

Axe 12 – Partage de la démarche de désescalade numérique

Après la mise en place des fondations et des piliers, la gouvernance du numérique s'incarne dans l'action quotidienne.

Cette troisième partie explore les dimensions opérationnelles : gestion de projet, relation avec les prestataires, pilotage des services, le budget et le partage de la démarche.

Elle vise à garantir que les principes InfraBasse se traduisent en pratiques concrètes, suivies et évaluées, à hauteur des enjeux de l'organisation.

8. PROJETS

Objectif

- Maîtriser la réalisation des projets de modification du système d'information en respectant la stratégie de gouvernance d'InfraBasse

Enjeux	Menaces	Risques
• Projets équilibrés ○ Couvrir de façon équilibrée les besoins métiers et stratégiques de l'organisation ○ Trouver un équilibre optimal entre création de valeur, désescalade numérique, risques et ressources • Projets réalistes, réalisables, réalisés Ne lancer que des projets nécessaires, assumés et qui pourront être menés à terme • L'âme de l'organisation ○ Impliquer les membres de organisation selon leur appétence et compétence, dès la conception et tout au long du projet ○ Favoriser l'engagement en sélectionnant des projets motivants • Gestion des risques et des coûts ○ Gestion des risques contractuels si le projet est soumis à une réglementation (RGPD...) ○ Maîtriser les coûts, les délais et les risques opérationnels et de cybersécurité ○ Éviter les dérives technologiques et les fuites hors périmètre	• Passer à côté des projets stratégiques pour l'entreprise Absence de priorisation claire pouvant conduire à négliger des projets à impact structurant • Gaspiller les ressources de l'entreprise sur des projets peu engageants Perte de ressources humaines et financières sur des projets qui n'auront pas su mobiliser • Accroître les coûts par manque de maîtrise Accumulation de décisions techniques ou fonctionnelles sans vision globale, générant une hausse progressive des dépenses • Manque d'outils de suivi et d'évaluation Difficulté à piloter, arbitrer et mesurer la performance du projet • Dérive en cours de projet Élargissement du périmètre ou des fonctionnalités, entraînant dérives et coûts supplémentaires	• Absence d'une vision stratégique pour le numérique Absence de feuille de route du numérique formalisée et validée par l'ensemble des équipes • Manque d'organisation ○ Absence de méthodologie pour la gestion des priorités de lancement des projets ○ Manque de définitions des responsabilités (pilotes et acteur-ices) • Sous-estimation des coûts du projet ○ Mauvaise gestion du changement qui génère du mécontentement ○ Absence de budget prévisionnel précis d'analyse de rentabilité • Perte de connaissances lors de la rotation des équipes projets Absence de capitalisation et transmission du savoir entraînant erreurs et retards • Se focaliser sur la mesure Rechercher exclusivement une conformité mesurable (par exemple, le bilan carbone) invisibilise d'autres externalités négatives non quantifiables • Arrêt non maîtrisé d'un projet Interruption brutale d'un projet sans dispositif qui permette de prévenir les impacts humains, techniques, et financiers

Bonnes pratiques

1. Approche globale

- **Chaque projet devra respecter la philosophie InfraBasse**
 - Définir précisément les périmètres
 - Appliquer la sobriété en fil rouge du projet en se référant aux arbres décisionnels de la stratégie de gouvernance

2. Référentiel des projets

- Mettre en place un référentiel unique pour la gestion globale, le suivi et l'archivage des projets
- Documenter les projets à l'aide d'un document modèle (Objectifs, rôles et responsabilité, budget / moyens, analyse des risques, échéances et indicateurs de suivi...)
- Concevoir les projets de manière à pouvoir les adapter, redimensionner voire interrompre sans fragiliser l'organisation

3. Gouvernance et rôles

- Définir les rôles et se référer à l'arbre décisionnel
- Assurer une traçabilité complète des décisions
- Définir dès le début du projet, la fin de vie des produits ou services numériques
- Assurer la continuité des connaissances et la documentation technique et fonctionnelle

4. Déploiement et conduite du changement

- Mettre en place un planning réaliste, des jalons clairs et des tests utilisateurs
- Prévoir dès le début du projet les livrables attendus, supports de formation utilisateurs / administrateurs, documents d'architectures techniques, maintenances à réaliser...
- Vérification avec des tests utilisateurs et validation des livrables
- Préparer des plans de communication et des supports d'accompagnement pour les utilisateurs

5. Bilan de projet

- Évaluer les effets réels du projet dans le temps au regard des objectifs, usages et équilibres recherchés
- Documenter les enseignements et partager les retours d'expérience

Tableau de gestion du changement, de la boîte à outils InfraBasse

Quelle évolution ?	Qui l'a demandé / proposé ?	Équipe en charge du changement	Équipes impactées par le changement	Partenaires impactés par le changement	Menaces ou risques principaux liés à la mise en œuvre du changement
EX : Mise en place d'une station de travail	Audit InfraBasse	GT numérique	L'ensemble des équipes qui ont des rendus à faire	/	Sous-estimation du besoin quotidien

Communication des intentions/objectifs	Prise en compte des retours	Phase projet (Déploiement, tests, production, évaluation)	Communication continue	Formation
Mail + framaforms	8 questionnaires remplis - 6 favorables au projets	cf gestion et suivi de projets	Mail pendant la mise place + retour site test + comm de fin de projet	Former les membres aux nouveaux usages et suivre les avancées (tableaux de suivi des formations)

9. PRESTATAIRES ET FOURNISSEURS

Objectifs

- Piloter les relations avec les fournisseurs de solutions ou services numériques en orientant les choix et en valorisant la désescalade numérique, et évaluer le niveau de relation
- Garantir des prestations conformes à la stratégie InfraBasse et favoriser l'autonomisation au sein des organisations
- Assurer la traçabilité des décisions, des incidents et des coûts, et limiter les dépendances externes non justifiées

Enjeux	Menaces	Risques
• Choisir entre faire et faire faire Disposer d'un processus efficace et des éléments nécessaires avant d'externaliser une tâche ou un service • Alignement stratégique et sobriété ○ S'assurer que chaque prestation soutient la désescalade numérique et les objectifs métier ○ Favoriser des solutions simples, compréhensibles et faciles à faire évoluer en interne • Qualité du service et pérennité ○ Vérifier la capacité des prestataires à former et déléguer les tâches les plus simples aux membres de l'organisation ○ Évaluer la pérennité des fournisseurs et leur alignement avec les lois InfraBasse • Transparence et coût total Obtenir des objectifs clairs, des contrats de service (SLA) adaptés et une visibilité sur le coût total de possession (TCO) • Gouvernance et responsabilité ○ Bien définir et comprendre le partage des responsabilités avec le prestataire ○ Définir les rôles et les mécanismes de contrôle dans la relation fournisseur	• Prestataires non formés à la vision InfraBasse Risque d'erreurs répétées • Non-adhésion à l'internalisation Les fournisseurs peuvent refuser de prendre en charge certaines tâches ou solutions demandées • Perte de contrôle et dépendance ○ Perte de la maîtrise de son SI ○ Dépendance à un prestataire unique trop important ○ Manque de transparence sur les dépendances • Non-respect des obligations légales et contractuelles et des enjeux de sécurité Le fournisseur pourrait ne pas respecter les obligations légales, de sécurité ou contractuelles, générant litiges ou coûts imprévus • Dégradation de l'image de marque Une collaboration inadéquate ou la dépendance à certains fournisseurs (GAFAM) peut nuire à la réputation de l'organisation	• Pas de prestas capables de répondre à la demande Méconnaissance de l'écosystème de prestataires répondant aux critères d'InfraBasse • Manque de méthodologie dans le pilotage Relations non suivies, difficultés de communications entre prestataires, décisions dispersées, absence de traçabilité • Fragmentation du SI Multiplication de solutions hétérogènes compliquant la maintenance et la cohérence globale • Succomber à une fausse injonction Externaliser une tâche inutile ou mal priorisée, contraire aux principes InfraBasse • Manque de continuité en cas de défaillance du fournisseur Absence de plan de réversibilité ou de continuité peut bloquer des processus critiques • Perte de connaissances Transmission insuffisante des informations lors des changements de prestataires

Bonnes pratiques

1. Approche globale

- **Définir précisément la stratégie et la gouvernance des relations avec les prestataires**
 - Définir une stratégie qui permet de faire respecter sa vision
 - Établir un suivi régulier de la qualité des relations et du niveau de service

2. Gestion des connaissances internes

- Former plusieurs membres à la gestion des prestataires et fournisseurs clés
- Centraliser les documents relatifs à la qualité et au suivi des prestations

3. Étude d'opportunité ou de faisabilité

- Se référer à la liste de prestataires InfraBasse
- Évaluer l'opportunité de déléguer en fonction de son impact sur l'autonomisation
- Identifier les risques liés à l'activité à déléguer

4. Pilotage

- Définir les rôles dans le suivi de la relation aux prestataires, conformément aux rôles définis au sein du comité de gouvernance du numérique
- Documenter les périmètres, objectifs, SLA et responsabilités et les mettre en perspective avec le suivi de la pérennité
- Concevoir les projets de manière à pouvoir adapter, redimensionner ou interrompre la prestation sans fragiliser l'organisation

5. Fin de contrat et réversibilité

- Définir les modalités de clôture et de transfert des services, ressources, données ou tout autre documentation inhérente au SI (configuration d'équipement par exemple)
- Inclure les interdépendances de la prestation avec le SI de l'organisation (interfaces, autres applications concernées, etc) dans le Plan de Continuité d'Activités (PCA)
- Revoir régulièrement les modalités de réversibilité et de transfert de connaissances

Extrait du tableur de gestion des prestataires et identification des dépendances opérationnelles, de la boîte à outils InfraBasse

Nom	Nature du service	Contact	Statut	Date de début de contrat	Existe-t-il des menaces ou risques liés à l'activité déléguée ?	Criticité du service De 1 Très peu critique à 5 Très critique	Le niveau de contrat de service (SLA) est établi, rangé et accessible
Ex: MonPresta	Administration système et réseau	David - commerce : david@monpresta.fr 07 Tara - technique: tara@monpresta.fr 06	En cours	01/01/2026	Instabilité générale du SI	5	Oui
	Hébergement du Site vitrine				Site inaccessible	2	Oui

Le SLA est compréhensible et couvre tout le périmètre attendu	Le SLA définit clairement les responsabilités	Les modalités de fin de contrat et transfert de services sont clairement définies	Localisation géographique de l'hébergement des données	Qualité du service De 1 Insatisfaisant à 5 Très satisfaisant	La prestataire est alignée avec les valeurs et le fonctionnement de l'organisation	Le service peut être repris en interne ou remplacé facilement	Il existe une volonté de formation en interne
Non	Oui	Non	France	3	Non	Non	Oui
Oui	Oui	Non	Europe	3	Non	Oui	Non

10. SERVICES NUMÉRIQUES

Objectifs

- Comprendre et structurer ses services numériques, et en réaliser une cartographie
- Identifier les services numériques conformes aux aspirations des membres de l'organisation et qui répondent à leurs besoins
- Garantir la cohérence entre services, infrastructures et stratégie de désescalade numérique

Enjeux	Menaces	Risques
• Autonomiser les membres ○ Permettre une compréhension claire des services utilisés ○ Favoriser une montée en compétence sur les outils essentiels • Garantir le niveau de service requis ○ Assurer disponibilité, performance et fiabilité ○ Adapter le niveau d'exigence au caractère critique du service • Rendre simple et lisible l'environnement numérique ○ Permettre à chaque membre d'identifier rapidement les outils et services utilisés par l'organisation et leur rôle ○ Réduire la complexité perçue du SI • Offrir des services cohérents ○ Éviter les doublons fonctionnels ○ Clarifier les usages autorisés et recommandés • Sobriété fonctionnelle ○ Limiter les fonctionnalités activées à celles réellement nécessaires ○ Éviter la complexification progressive des outils • Préserver le droit au non numérique	• Non maîtrise des outils ○ Services déployés sans formation suffisante ○ Fonctionnalités avancées inconnues ou mal comprises • Multiplication et adoption non contrôlée des services ○ Ajout d'outils sans suppression des anciens ○ Maintien simultané d'outils redondants par absence d'arbitrage ○ Shadow IT : Adoption d'outils non validés pour compenser une insatisfaction • Augmentation des besoins en matériel Services gourmands en ressources, imposant un renouvellement accéléré des postes utilisateurs • Pression du marché Attractivité des solutions dominantes au détriment de la stratégie InfraBasse • Responsabilités contractuelles peu claires • Absence de dispositif structuré de remontée des besoins	• Mauvaise compréhension des priorités des membres Décalage entre choix stratégiques et besoin ou volonté des équipes • Manque de puissance du matériel et augmentation des coûts Déséquilibre entre infrastructure et services Renouvellement prématuré du parc • Fragmentation du système d'information ○ Aucun membre de l'équipe n'utilise les mêmes outils, entraînant une individualisation du travail ○ Données dispersées, multiplication des interfaces et perte de cohérence globale • La désescalade numérique au détriment du confort Initiée par les équipes ou la gouvernance, trop dénumérer peut entraîner une frustration • Surcharge cognitive Trop d'outils entraînent une fatigue informationnelle et une baisse d'efficacité (ex : Multiplication des canaux de communication) • Perte d'alignement avec la vision stratégique

Bonnes pratiques

1. Approche globale

- **Entendre et comprendre les membres en respectant leurs priorités**
 - Arbitrer ensemble entre dépendance aux géants du numérique, désir de sobriété et praticité
 - Démocratiser l'utilisation de questionnaires anonymes
- **Maintenir une cartographie vivante des services numériques**
 - Identifier les services critiques, secondaires et facultatifs
 - Lier chaque service à un besoin métier clairement identifié
 - Lier les interdépendances entre les services

2. Cohérence entre infrastructure et usages

- Vérifier la compatibilité entre services numériques et capacités matérielles
- Privilégier des stations de travail, dont les composants peuvent être remplacés, pour des tâches occasionnelles et qui demandent beaucoup de ressources

3. Documentation des services

- Formaliser les procédures d'ajout ou de retrait d'un service en définissant un process clair
- Documenter et classer les services numériques
 - Identifier à quoi sert le logiciel, dans quelles circonstances l'utiliser, et quel·les en sont les principaux usager·es
 - Préciser le prestataire associé, dont le contrat de service (SLA) est suivi et accessible
 - Définir le niveau de criticité du service pour prioriser sa reprise d'activité (PRA) et les alternatives en cas d'indisponibilité (PCA)

4. Formation et appropriation

- Former les équipes aux usages essentiels et organiser les retours d'expérience et enquête de satisfaction
- Identifier des référents internes par service critique
- Encourager le partage d'astuces et bonnes pratiques

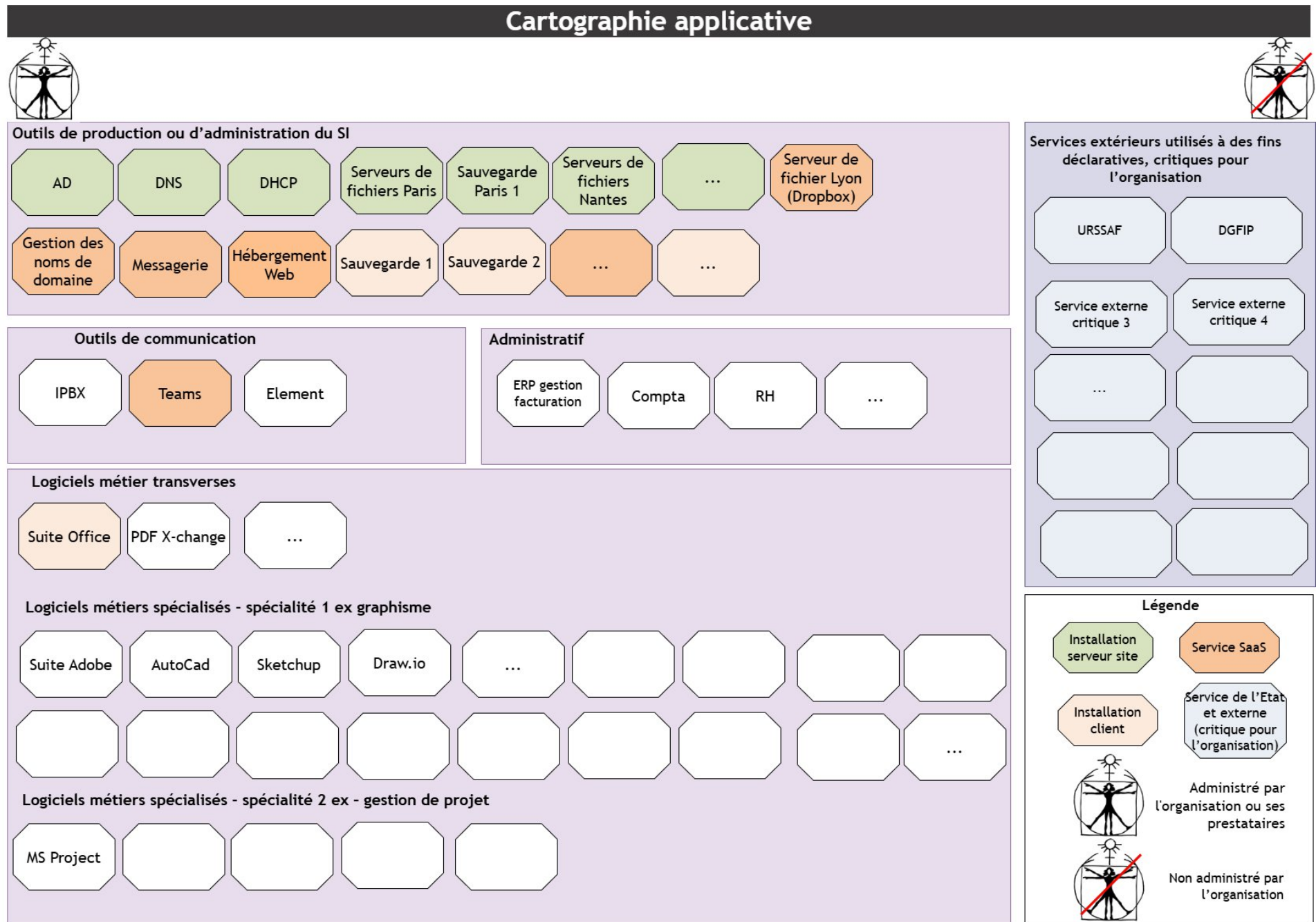
5. Évaluation continue

- Évaluer régulièrement :
 - Le coût total de possession (TCO)
 - Le nombre de services redondants
 - Le coût total (licences + matériel + formation + support)
- Mettre en évidence les services peu utilisés ou redondants afin d'éclairer les décisions de gouvernance
- Réaliser un audit annuel de pertinences des services

6. Gestion du confort et de la sobriété

Suivre les effets réels des services numériques sur le confort d'usage, la charge mentale et les équilibres de sobriété du système

Exemple de cartographie applicative, de la boîte à outils InfraBasse



Services extérieurs utilisés à des fins déclaratives, critiques pour l'organisation

URSSAF

DGFiP

Service externe critique 3

Service externe critique 4

...

Légende

Installation serveur site

Service SaaS

Installation client

Service de l'Etat et externe (critique pour l'organisation)



Administré par l'organisation ou ses prestataires



Non administré par l'organisation

11. MAITRISE DU BUDGET

Objectifs

- Adapter les ambitions numériques aux capacités financières réelles de l'organisation
- Garantir une allocation cohérente, transparente et soutenable des ressources liées au système d'information

Enjeux	Menaces	Risques
• Aligner le budget du SI avec les valeurs de l'organisation ○ Assumer que certaines collaborations éthiques ne sont pas les plus économiques à court terme ○ Ne pas dissocier les choix techniques de leur implication systémique • Allouer les ressources au juste équilibre ○ Assurer l'atteinte des objectifs de performance du SI par une répartition adaptée ○ Éviter la sur-dotation comme la sous-dotation • Associer l'âme de l'organisation à la gestion du SI ○ Écouter les besoins réels permet souvent de simplifier et de réduire les coûts ○ Adapter les choix budgétaires aux usages, aux habitudes et aux objectifs de sobriété • Rendre visible le coût réel du numérique ○ Identifier l'ensemble des postes de dépenses directs et indirects ○ Intégrer les coûts cachés : formation, temps interne, dépendance, maintenance	• Décisions budgétaires prises sans vision globale ○ Manque de connaissance technique ○ Méconnaissance des coûts complets ○ Absence de projection à moyen et long terme • Incompréhension de l'âme de la coop ○ Augmentation du budget pour financer des services peu utiles ou peu alignés avec les besoins réels ○ Réduction excessive du budget alors que le niveau de sobriété est déjà élevé • Cadrage insuffisant d'un projet Ne pas maîtriser les facteurs de dérapage peut considérablement augmenter les coûts • Illusion du "gratuit" ○ Ce n'est pas parce que cela ne coûte rien que c'est gratuit ○ Adoption de solutions sans coût apparent ○ Dépendance créée en échange de données ou de verrouillage technique • Pression du marché et effet de mode Renouvellement prématuré du matériel Multiplication d'abonnements non essentiels	• Méconnaissance des attentes métiers ○ Décalage entre budget alloué et besoins réels des équipes ○ Investissements réalisés sur des priorités mal identifiées • Budget mal intégré à la feuille de route numérique ○ Absence de cohérence entre stratégie SI et capacité financière ○ Projets engagés sans sécurisation des moyens nécessaires • Absence de processus structuré de suivi du budget ○ Manque de visibilité sur les écarts entre prévisionnel et réalisé ○ Décisions correctives tardives ou inadaptées • Manque de culture économique et de compétences en contrôle de gestion du SI ○ Difficulté à évaluer un coût complet ○ Arbitrages fondés sur l'intuition plutôt que sur des données consolidées • Dépendance financière accrue Poids croissant de certains prestataires ou abonnements

Bonnes pratiques

1. Approche globale

- **Intégrer le budget du SI dans la stratégie générale de l'organisation**
- **Rendre explicites les arbitrages budgétaires**
 - Partager les hypothèses de coûts
 - Expliquer les choix de renoncement ou d'adoption

2. Mettre en place un suivi annuel formalisé

- Réaliser un budget prévisionnel lié au numérique
- Formaliser le budget réel
- Analyser les écarts

3. Le coût complet des produits et services

- Évaluer le coût de possession (TCO), qui comprend licences, matériel, formation, maintenance, temps interne et coûts cachés
- Intégrer dans les coûts indirects : le temps passé devant une complexité d'utilisation accrue, la dépendance aux prestataires, la perte d'autonomie, mais aussi la surcharge cognitive et le mécontentement des équipes
- Accepter un coût de déploiement peut-être plus important (matériel, logiciel, prestation de service et formation)
- Comparer les scénarios à moyen et long terme plutôt qu'évaluer seulement le coût immédiat

4. Pilotage de l'économie du numérique

- Désigner un référent budgétaire SI
- Développer une culture partagée des coûts
- Réévaluer régulièrement la pertinence des dépenses
 - Supprimer les services peu ou pas utilisés
 - Renégocier les contrats
 - Réaffecter les économies réalisées dans l'autonomisation de l'organisation

Tableau d'identification des coûts, issu de la boîte à outils InfraBasse

Objectif de l'outil

Cette matrice de lecture des coûts du système d'information permet de :

- Interpréter les coûts
- Révéler les effets indirects des choix techniques
- Identifier les dépendances structurelles
- Faire émerger des arbitrages

Elle ne produit pas de score, ne calcule rien.

Elle sert à visibiliser les effets cumulés des choix techniques sur les coûts, l'organisation interne et la dépendance.

Bien ou Service	Coûts directs	Coût d'exploitation	Coûts cachés/indirects	Coût de dépendance	Enjeu économique
EX : Mise en place d'une station de travail	Acquisition du matériel	Contrat de maintenance	Temps perdu lors des mises à jour obligatoires et interruptions de service	Dépendance au fournisseur matériel et aux OS propriétaires	Réduire la fréquence de renouvellement des postes de travail
	Installation et configuration initiale	Support utilisateur et assistance quotidienne	Surcharge cognitive si changement mal accompagné (cf matrice de gestion du changement)	Dépendance aux prestataires externes	Augmenter l'autonomie d'utilisation et de maintenance
	Déploiement des logiciels standards	Mise à jour logicielle régulière	Incompatibilités entre logiciels entraînant des contournements (Shadow IT)	Dépendance aux éditeurs logiciels pour les évolutions et corrections	Limitier la complexité logicielle
	...				

12. PARTAGE DE LA DÉMARCHE

Objectifs

- Permettre l'appropriation et la diffusion participative de la méthodologie InfraBasse
- Adopter une stratégie de sobriété éditoriale

Enjeux	Menaces	Risques
• Appropriation interne et engagement des membres de l'organisation Élaborer les projets en équipe pour favoriser leur appropriation et fluidifier la communication interne • Valoriser l'acculturation interne dans la communication externe Mettre en avant l'autonomisation des équipes dans le premier niveau de maintenance du système d'information • Valoriser l'efficience atteinte dans le respect de la méthodologie InfraBasse Illustrer que sobriété et efficacité sont compatibles et bénéfiques pour l'organisation • Transparence sur les freins rencontrés Partager ouvertement les difficultés permet de crédibiliser la démarche et d'anticiper les incompréhensions • La communication en situation critique Préparer les messages et les supports permet de réagir rapidement et de maintenir la confiance	• Manque de transparence Les informations partielles ou filtrées nuisent à la crédibilité de la démarche • Manque d'attractivité interne Une communication peu engageante ou trop tardive réduit l'adhésion et l'intérêt des membres, entraînant désintérêt ou résistance • Manque d'adhésion à la philosophie InfraBasse La démarche peut être perçue comme idéologique • Contenus trop longs, mal ciblés ou sur-communication L'attention se perd, les messages clés ne sont pas retenus et la démarche peut être perçue comme envahissante	• Sous-estimer l'impact culturel des projets de transformation Les initiatives peuvent échouer si les habitudes et valeurs des équipes ne sont pas prises en compte • Messages mal compris ou mal relayés Le manque de clarté entraîne des interprétations erronées et des attentes non satisfaites • Perte de marchés Une communication externe mal dosée ou mal comprise peut nuire à certaines relations • Greenwashing La communication superficielle ou exagérée peut décrédibiliser la stratégie de désescalade numérique • Récupération ou déformation de la démarche Simplification excessive ou interprétation partielle pouvant dénaturer les principes d'InfraBasse

Bonnes pratiques

1. Approche globale

- **Valoriser les apports de la méthodologie InfraBasse pour l'organisation**
 - Adopter une stratégie de sobriété éditoriale
 - Adopter un langage clair et accessible

2. Communication interne

- Informer l'ensemble des équipes à chaque étape du projet, y compris sur la communication externe prévue
- Valoriser et intégrer les retours des membres de l'organisation pour renforcer la confiance, l'adhésion et l'appropriation

3. Communication externe

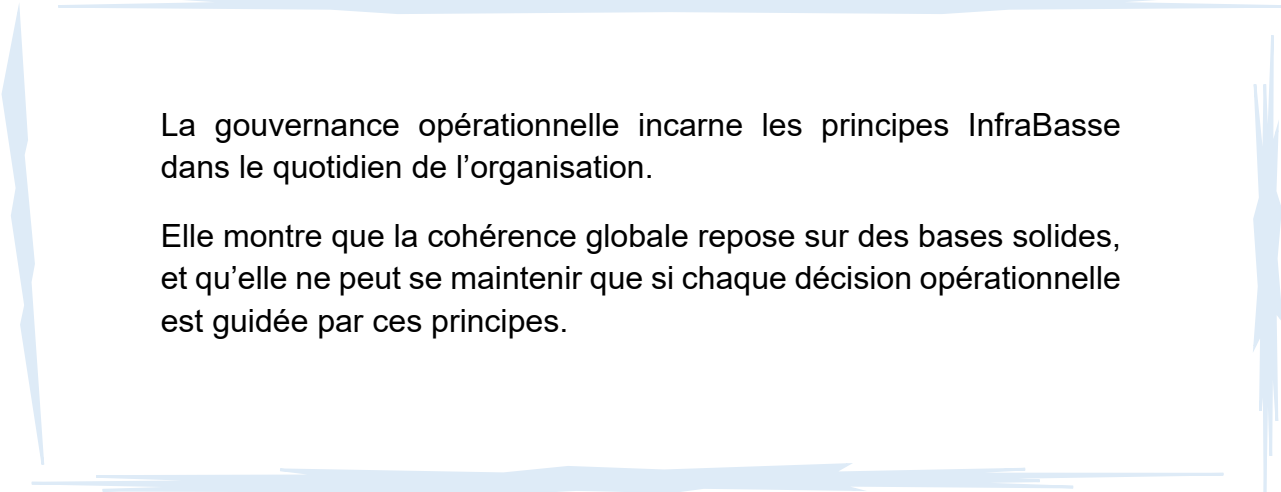
- Élaborer un plan de communication clair et partagé
 - Transparence sur les résultats et les freins rencontrés
 - Sincérité dans la présentation des améliorations

4. Suivi et valorisation des retours d'expérience

- Collecter et documenter les retours d'expérience sur la mise en œuvre et l'évolution de la communication
- Mettre en évidence les bonnes pratiques et les enseignements tirés
- Réajuster les pratiques de communication en fonction des retours pour améliorer l'engagement et renforcer la pertinence de la stratégie

5. Boucler la démarche avec l'appropriation et le partage d'idées

- Reconnaître et valoriser l'engagement des équipes
- S'appuyer sur le partage d'expérience pour pérenniser la stratégie InfraBasse



La gouvernance opérationnelle incarne les principes InfraBasse dans le quotidien de l'organisation.

Elle montre que la cohérence globale repose sur des bases solides, et qu'elle ne peut se maintenir que si chaque décision opérationnelle est guidée par ces principes.

CONCLUSION

InfraBasse est un référentiel complet : sa mise en œuvre opérationnelle, actionnable avec la boîte à outils, ne peut être dissociée des choix de gouvernance qui la structurent (les Fondations) ni de la compréhension systémique du système d'information portée par les Piliers.

Les décisions techniques, organisationnelles et humaines découlent de cette cohérence globale.

Sa force réside dans sa capacité à s'adapter aux spécificités de chaque organisation, tout en plaçant la désescalade au cœur des priorités.

Elle propose une gouvernance du numérique qui remet l'humain au centre des décisions, renforce l'autonomie, permet de maîtriser les ressources, limite les dépendances structurelles et veille à maintenir l'alignement entre usages, infrastructures et objectifs de sobriété.

InfraBasse est une démarche d'amélioration continue, dans laquelle fondations, piliers et pratiques opérationnelles sont régulièrement réévaluées et ajustées afin de rester pertinentes face à l'évolution de l'organisation.

LEXIQUE

Les définitions proposées dans ce lexique sont adaptées au cadre InfraBasse. Elles ne constituent pas des définitions juridiques ou normatives.

Terme	Définition	Remarque
Architecture du système d'information (SI)	Organisation globale des outils, serveurs, logiciels, réseaux et données	C'est "comment tout est construit et relié"
Audit (technique / de gouvernance)	Analyse de l'existant pour comprendre : – ce qui fonctionne – ce qui pose problème – ce qui peut être amélioré	Un état des lieux avancé qui permet de prioriser et prendre les bonnes décisions
Auto-hébergement	Fait d'héberger ses services (site web, fichiers, outils...) sur ses propres serveurs ou via un prestataire local maîtrisé	Permet de garder le contrôle plutôt que de dépendre d'un service externe
Big Tech	Grandes entreprises du numérique (cloud, logiciels, plateformes) qui occupent une position dominante sur le	Elles influencent fortement les choix technologiques des organisations, notamment via leurs stratégies commerciales et de lobbying, ce qui oriente les

	marché mondial	usages et crée des dépendances difficiles à remettre en question
Cloud	Utilisation de services numériques accessibles via Internet (stockage de fichiers, logiciels, applications...) Ces services reposent sur des datacenters, souvent éloignés des usagers finaux et gérés par de grandes entreprises	Pratique, mais souvent moins maîtrisé (données, coûts, dépendance), le cloud donne l'impression que les données sont "dans le nuage", alors qu'il s'appuie sur de lourdes infrastructures
Comité de gouvernance du numérique	Groupe de personnes qui prennent ou valident les décisions importantes liées au numérique	Son action doit permettre de répondre aux enjeux identifiés, grâce à la définition de rôles clairs
Cycle de vie des données	Les étapes par lesquelles passent les données : – création – utilisation – stockage – archivage – suppression	Toutes les données n'ont pas vocation à être conservées indéfiniment. La suppression de certaines d'entre elles entre même dans le cadre réglementaire
Datacenter (Centre de donnée)	Lieu physique où sont regroupés des serveurs qui stockent des données et font fonctionner des services numériques. Un datacenter contient :	C'est la principale infrastructure matérielle derrière "le cloud", qui a de forts coûts environnementaux

	– des ordinateurs (serveurs) – des systèmes de refroidissement – une alimentation électrique importante – des dispositifs de sécurité	
Désescalade numérique	Principe consistant à : – Interroger son rapport au numérique – En comprendre les liens systémiques (géo-politique, économique, droits humains...) – Adopter une posture de limitation volontaire – Refuser le non nécessaire – Privilégier des outils simples, accessibles et indépendants	Améliorer son quotidien, grâce à un usage plus modéré du numérique
Données	Information stockée sous forme numérique (fichier, email, base de données...)	Elles font partie du patrimoine de l'organisation
ERP (progiciel de gestion intégré)	Logiciel central qui regroupe plusieurs fonctions (compta, RH, gestion...)	Souvent puissant, mais complexe et parfois surdimensionné
ESS (Économie Sociale et Solidaire)	Ensemble d'organisations qui cherchent à concilier activité économique et utilité sociale. Elles privilégient la coopération, la gouvernance partagée et la limitation des	C'est un cadre d'acteurs et d'actrices souvent en cohérence avec la démarche InfraBasse

	impacts sociaux et environnementaux	
Fournisseur	Acteur externe fournissant un bien, un service ou une ressource utilisée par le système d'information, sans nécessairement intervenir directement dans sa gestion ou son exploitation	
Hébergement (informatique)	Lieu où sont stockées et exécutées les données et les services numériques	Peut être interne (auto-hébergement) ou externe (cloud)
Infrastructures	Ensemble des éléments techniques qui font fonctionner le SI : – Serveurs – Réseau – Terminaux utilisateurs – Stockage	C'est la "base physique et technique". InfraBasse s'efforce de rendre visible cette base pour aller vers une limitation volontaire des usages
Intégrité des données	Fait que les données restent fiables, complètes et non modifiées de manière incorrecte au cours du temps	Une donnée intègre est une donnée sur laquelle on peut se baser sans risque d'erreur
Interopérabilité	Capacité de différents outils à fonctionner ensemble et à échanger des données	Évite d'être bloqué avec un outil fermé dont les données ne peuvent être exportées ou transférées dans un autre
Logiciel libre / open source	Logiciel dont le code est accessible, modifiable et réutilisable selon les conditions	Favorise la transparence et l'indépendance aux "big techs"
Logiciel propriétaire	Logiciel dont le code source n'est pas	Peut offrir des fonctionnalités ou un

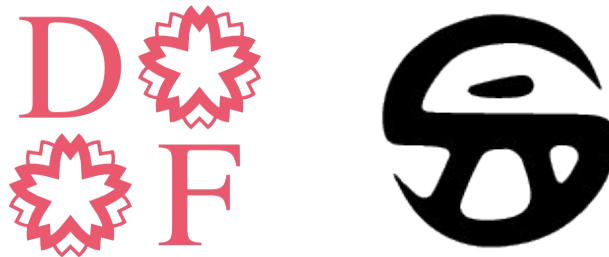
	accessible et dont l'utilisation, la modification et la diffusion sont encadrées par son éditeur	support adaptés à certains besoins, mais crée une forte dépendance envers l'éditeur
Maintenance	Actions permettant de garder un système fonctionnel : entretien physique du matériel et des locaux, mises à jour, corrections, surveillance, etc	Indispensable pour la sécurité et la durée de vie
Matrice RACI	Outil simple pour clarifier les rôles : R : Qui réalise ? A : Qui décide ? C : Qui est consulté·e ? I : Qui est informé·e ?	Permet d'éviter les zones floues et les conflits
PCA (Plan de Continuité d'Activité)	Organisation prévue pour continuer à fonctionner en cas de problème	
PRA - Plan de Reprise d'Activité	Plan pour remettre en route le système d'information après un incident	
Prestataire	Acteur externe intervenant activement dans le fonctionnement, l'exploitation, l'administration, le support ou l'évolution du système d'information	Dans InfraBasse, certains acteurs peuvent être à la fois fournisseurs et prestataires selon leur niveau d'implication et de dépendance fonctionnelle
PSSI (Politique de Sécurité des Systèmes d'Information)	Document qui définit les règles de sécurité : – accès – mots de passe – sauvegardes	Doit être simple et comprise de tous

	– gestion des incidents	
RGPD - Règlement Général sur la Protection des Données	Règles européennes pour protéger les données personnelles	Obligation légale pour toute organisation
RSO - Responsabilité Sociétale des Organisations	Démarche qui vise à intégrer les impacts sociaux, environnementaux et éthiques dans le fonctionnement d'une organisation	Cela consiste à prendre en compte les effets de ses décisions au-delà du seul aspect économique
SaaS (Software as a Service)	Modèle de fourniture d'un logiciel dans lequel l'application est hébergée et administrée par un prestataire externe, et accessible par l'utilisateur via internet (souvent sous forme d'abonnement).	Simplifie l'accès et la maintenance, mais déplace la gestion matérielle, des données et des évolutions techniques vers un tiers, avec une visibilité limitée sur les infrastructures mobilisées.
Serveur	Ordinateur qui fournit des services (stockage, site web, applications...)	Peut être interne ou distant
Shadow IT	Utilisation d'outils numérique non validés par l'organisation	Souvent lié à un manque de solutions adaptées
SI (Système d'Information)	Ensemble des outils, données, processus et personnes qui gèrent l'information	Selon InfraBasse, le SI ne repose pas seulement sur de la technique, mais aussi sur l'âme et les capacités organisationnelles des structures. Il s'agit donc d'un ensemble sociotechnique complexe
SLA (Service Level Agreement)	Contrat qui définit le niveau de service attendu (ex : disponibilité, délais d'in-	Permet de cadrer la relation avec un prestataire

	tervention, support...)	
Sobriété numérique	Réduction de l'ivresse numérique : – moins d'outils – moins de ressources – plus de simplicité Il s'agit de transformer ses pratiques pour réduire la dette cognitive liée au numérique et ainsi améliorer sa qualité de vie, mais aussi réduire ses coûts humains et environnementaux.	La sobriété numérique est la traduction opérationnelle de la démarche de désescalade numérique. Si la désescalade donne la direction réflexive, la sobriété permet quant à elle de la mettre en œuvre.
TCO (Coût Total de Possession)	Coût réel d'un outil sur toute sa durée de vie : – achat – maintenance – formation – temps passé – ...	Permet d'évaluer correctement le coût de l'appropriation du numérique par l'organisation
Versioning (gestion des versions)	Fait de conserver différentes versions d'un fichier ou d'un outil	Il peut être manuel (ce qui n'est pas forcément idéal) ou automatique

INFRA BASSE

InfraBasse est un projet porté initialement par l'association DeuxFleurs, puis l'association Syst-A, et financé par le programme Alt IMPACT



Co-porté
par



Inria

