SCHÉMA DIRECTEUR des SYSTÈMES D'INFORMATION NUMÉRIQUES 2025-2030

Sud Roussillon
COMMUNAUTÉ DE COMMUNES

SOMMAIRE

POURQUOI UN SCHÉMA DIRECTEUR DES SYSTÈMES D'INFORMATION ?

Le Schéma directeur des systèmes d'information numériques s'appuie sur une feuille de route Transformation numérique. Celle-ci donne un cap à des projets techniques souvent cloisonnés par nature mais qui nécessitent de s'articuler autour d'une **dimension stratégique et transversale**.

Ce schéma est d'autant plus important pour intégrer le système d'information (SI) dans la stratégie de Sud Roussillon qui souhaite aller vers une société qui entreprend et modernise ses services en s'appuyant sur de nouveaux outils technologiques.

Cette démarche, pour tendre vers le un succès, doit évoluer sur au moins trois points :

- FOCUS : aller à l'essentiel, et rester sur les axes directeurs,
- AGILE : devenir plus dynamique dans son actualisation pour s'adapter à l'environnement actuel,
- DESIGN DES SERVICES : prendre en compte le plus en amont possible les utilisateurs de la communauté de communes ainsi que les communes membres qui pourraient bénéficier des services numériques de l'EPCI.

Un schéma directeur a d'autant plus de valeur qu'il permet d'**anticiper** et de **se restructurer**. Il constitue donc une formidable opportunité d'établir en amont un dialogue réel entre la Direction des systèmes d'information numériques et les contributeurs, transformant ce document en une démarche de fédération des équipes autour de lui.

Ce schéma directeur, prévu pour la période 2025-2030, prendra une démarche itérative et participative. Il ira donc moins dans la définition du « comment » et reviendra à ses fondamentaux : être un « schéma » et être « directeur », sans nécessairement préciser tous les détails.

Par son Schéma directeur agile, la DSI prépare l'avenir et repositionne les systèmes d'information en leur donnant une nouvelle ambition.

NOTRE STRATÉGIE DES SYSTÈMES D'INFORMATION NUMÉRIQUES

Notre société actuelle est en pleine **mutation numérique**.

Cela passe par :

- Une prise de conscience des risques tant matériels qu'humains
- Une accélération des performances technologiques :
  - Évolution des pratiques « projets » vers des approches agiles et plus largement DevOps,
  - Explosion des besoins et évolution des usages numériques…
- L'arrivée de nouveaux métiers et services autour de la donnée et de la mobilité
- Des crises type Covid avec une transformation du travail.

Cette transformation numérique doit s'inscrire autour de documents phares (PSSI, Schéma directeur des SI numériques, feuille de route Transformation numérique…).

Aujourd'hui, face à ces transformations engagées dans nos collectivités pour y répondre, les fondamentaux de la DSI restent identiques. Si ces mandats restent les mêmes, le contexte, les contenus, les moyens d'**être performant et d'atteindre ces objectifs** ont sensiblement évolué avec des effets majeurs sur la collectivité, sur ses métiers, sur son système d'information et par conséquent sur sa gouvernance.

Grâce à ce schéma directeur AGILE, Sud Roussillon prépare l'avenir. Il repositionne les systèmes d'information en leur donnant une nouvelle ambition au travers de 3 enjeux.

L'enjeu 1 concerne la poursuite de la modernisation des systèmes d'information, le renforcement de leurs efficiences et de leurs performances avec :

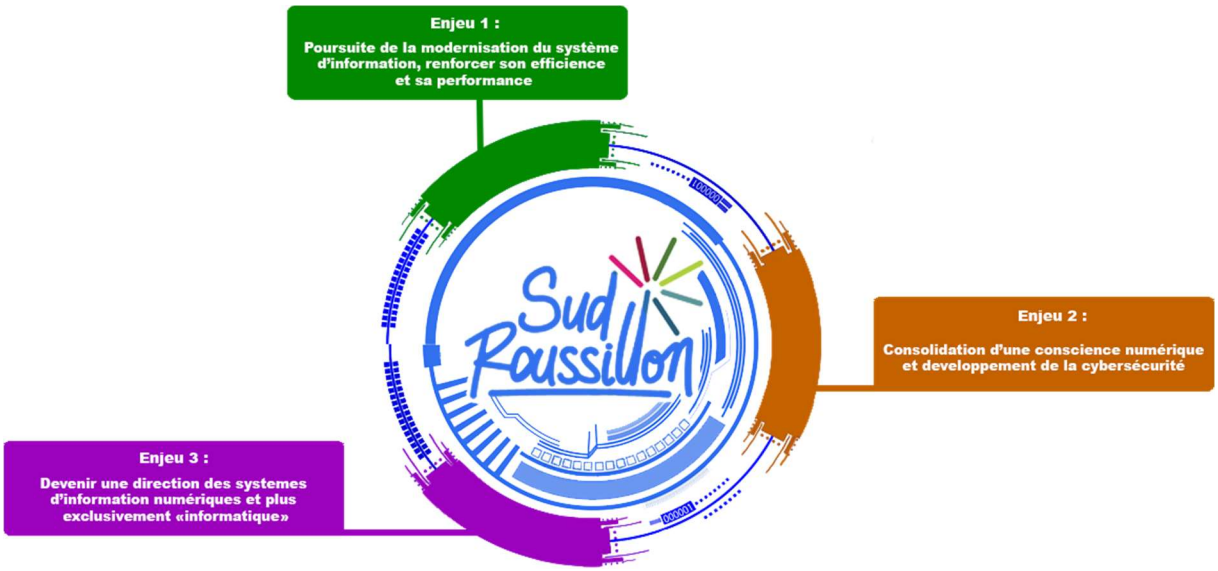
- Axe1 : Refonte récurrente des éléments du SI
- Axe2 : Besoins immobiliers spécifiques
- Axe3 : Moyens de la DSI

L'enjeu 2 porte sur le volet sécurité et englobe la consolidation d'une conscience numérique et le développement de la cybersécurité :

- Axe1 : Uniformisation de la sécurité
- Axe2 : Segmentation des réseaux et des données
- Axe3 : Formations renforcées des agents aux risques numériques
- Axe4 : Informations transverses dès la conception des projets

L'enjeu 3 porte sur un élargissement des attributions de la DSI, pour devenir une DSI numérique et plus seulement informatique :

- Axe1 : Mutualisation d'outils
- Axe2 : Développement d'une nouvelle mobilité
- Axe3 : S'orienter vers le futur

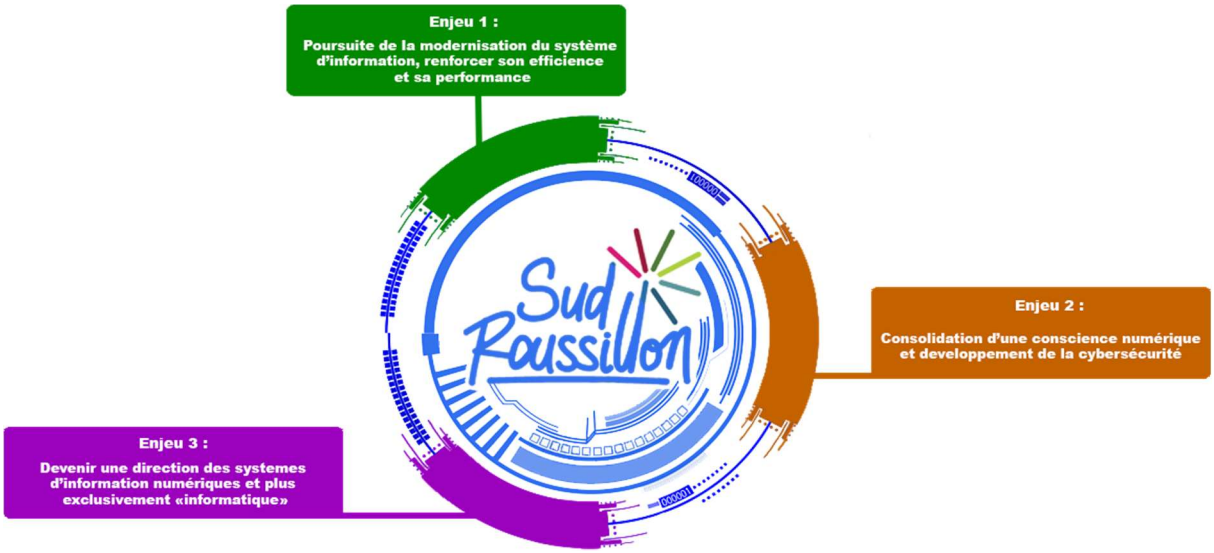


ENJEU 1

POURSUITE DE LA MODERNISATION DES SYSTÈMES D'INFORMATION, RENFORCER LEURS EFFICIENCES ET LEURS PERFORMANCES

OBJECTIF :

Maintien des solutions technologiques de la DSI et accentuation de ses capacités humaines.



1 – CONTEXTE

Le système d'information (SI) regroupe un ensemble de ressources humaines, technologiques et matérielles permettant de collecter, stocker, gérer et transmettre des informations. Il représente la colonne vertébrale de la gestion des données et des processus d'une entreprise.

Son architecture joue un rôle central dans la productivité. Parmi les enjeux majeurs, la sécurité de l'information occupe une place prépondérante. Face à l'augmentation des cyberattaques, il est indispensable de protéger les données sensibles collectées. Également, un **système d'information étant en constante évolution**, il est nécessaire que celui-ci soit **évolutif et innovant** pour rester compétitif. L'intégration de nouvelles technologies est donc un facteur majeur d'un SI performant.

Au sein de la DSI, l'efficacité des opérations IT reste un sujet clef, dont dépend la crédibilité du service. Optimiser les pratiques reste avant tout un processus d'**amélioration continue**, qui se doit d'intégrer les dernières pratiques et technologies, comme l'AIOps.

Aucun DSI ne souhaite diriger une organisation informatique inefficace. Pourtant, par manque d'attention ou en s'en tenant à des pratiques dépassées, l'IT peut devenir progressivement inefficace et peu productive. Selon Robert Orshaw, leader cloud chez Deloitte Consulting, l'amélioration de l'efficacité informatique doit être un processus continu, et non un projet ponctuel. Tout repose sur l'amélioration continue est essentielle, dit-il.

« *Les environnements informatiques sont dynamiques et en constante évolution, c'est pourquoi les indicateurs clés tels que les mesures d'efficacité doivent être examinés et revus régulièrement afin de garantir des performances optimales* », explique-t-il. Cette surveillance continue permet d'identifier et de corriger rapidement les problèmes, et de parvenir à une amélioration constante de l'efficacité au fil du temps.

Au cœur de l'entreprise, le système d'information assure la mise en œuvre de divers processus. L'intérêt de procéder à son amélioration est multiple :

- **Améliorer sa productivité :** l'optimisation d'un système d'information permet d'accroître l'efficacité des processus. En automatisant les tâches répétitives et en optimisant les flux de travail, les entreprises peuvent réduire leurs délais et leurs coûts, tout en augmentant leur productivité. Un SI optimisé facilite également l'accès à l'information, ce qui permet aux équipes de travailler plus efficacement.

- **Garantir la disponibilité et la sécurité des données :** la sécurisation est devenue une préoccupation majeure pour toutes les entreprises, des PME aux multinationales. Améliorer son SI implique de prendre des mesures de sécurité destinées à protéger l'organisation contre les cyberattaques, les pertes de données et les interruptions de service. En outre, un SI solide garantit la disponibilité des données essentielles pour le bon fonctionnement de l'activité.

- **Améliorer la motivation des équipes** : un système d'information en phase avec son époque et avec les attentes des utilisateurs favorise une plus grande satisfaction au travail et une augmentation réelle de la motivation, de l'engagement, et donc de la productivité.

Pour cela, il faut comprendre quels éléments analyser et leur importance dans le fonctionnement d'un SI optimal. Voici, pour nous, les éléments majeurs à diagnostiquer lorsque l'on souhaite améliorer son Système d'Information :

Voici trois pistes essentielles ou axes stratégiques ayant fait leurs preuves pour optimiser les performances des opérations IT :

- **Fiabilité de l'environnement de production**

Un SI doit garantir la disponibilité des ressources et une infrastructure robuste.

Le maintien en état optimal de celui-ci est un préambule essentiel à cette sécurisation. Cette conservation passe nécessairement par des renouvèlements récurrents de ces actifs.

- **Locaux**

Une architecture bien conçue est essentielle pour un SI performant. Elle doit être modulable, évolutive et capable de s'adapter aux besoins changeants de l'entreprise. Des salles cohérentes permettent également de faciliter l'intégration de nouvelles technologies et d'assurer la pérennité des systèmes.

- **Organisation des équipes, compétences et processus**

L'optimisation d'un SI commence par une évaluation des compétences internes. Il est essentiel d'identifier les lacunes et les ressources nécessaires au bon fonctionnement du système. Une organisation fluide et des processus adaptés maximisent l'efficacité du SI.

Voici quelques chiffres illustrant l'importance et l'impact de la modernisation des infrastructures systèmes informatiques :

1. Investissement et Budget

- En moyenne, les entreprises consacrent 16,5 % de leurs budgets IT à la modernisation de leurs infrastructures
- En France, 57 % des décideurs IT sont prêts à investir dans des évolutions importantes pour moderniser leurs systèmes

2. Productivité et Efficacité

- Les entreprises ayant modernisé leurs systèmes d'information voient une augmentation de la productivité de 25 % en moyenne
- La modernisation des infrastructures permet de réduire les coûts de fonctionnement de 15 à 20 % en moyenne

3. Flexibilité et Réactivité

- 51 % des responsables informatiques ont adapté leur infrastructure pour répondre aux exigences du travail hybride ou à distance
- Les entreprises avec des infrastructures modernes réagissent 33 % plus vite aux risques cyber

4. Adoption et Préparation

- 54 % des entreprises sont actuellement en pleine modernisation de leurs systèmes, et 29 % prévoient de s'y lancer prochainement

Ces chiffres montrent clairement que la modernisation des infrastructures systèmes informatiques est non seulement une nécessité stratégique, mais aussi un **levier important** pour améliorer la productivité, réduire les coûts et augmenter la flexibilité des entreprises.

Chiffres clés

« Productivité :

Les entreprises ayant modernisé leurs systèmes d'information voient une augmentation de la productivité de 25 % en moyenne »

« Temps de Réponse :

La modernisation permet de réduire les temps de réponse des systèmes de 30 %, améliorant ainsi l'efficacité des processus métiers »

« Sécurité :

Les systèmes modernisés sont 68 % moins susceptibles de subir des incidents de sécurité majeurs »

2 - AXES STRATEGIQUES

ENJEU N°1 – AXE 1 : Refonte récurrente des éléments du SI

Comme évoqué précédemment, l'attention portée à l'obsolescence des différents éléments actifs du SI est un enjeu pour Sud Roussillon.

Dans un environnement technologique en constante évolution, les systèmes d'information (SI) jouent un **rôle crucial** dans la performance et la compétitivité des entreprises. Les refontes ou évolutions récurrentes des éléments d'un SI sont essentielles pour maintenir l'efficacité, la sécurité et l'innovation. Voici pourquoi il est important de procéder régulièrement à ces mises à jour :

Importance des Refontes ou Évolutions Récurrentes

1. **Performances optimales :** Systèmes d'information doivent être régulièrement mis à jour pour tirer parti des nouvelles améliorations en termes de vitesse, de capacité et de fonctionnalité. Cela permet d'assurer une performance optimale des systèmes et d'éviter les ralentissements qui peuvent affecter la productivité des employés.

2. **Renforcement de la Sécurité** : Les cybermenaces évoluent constamment, et les anciens systèmes peuvent devenir vulnérables aux nouvelles formes d'attaques. Les mises à jour régulières des SI permettent d'intégrer les dernières mesures de sécurité et de protéger les données sensibles contre les violations.

3. **Adaptation aux Nouveaux Besoins** : Les besoins de l'entreprise et des utilisateurs évoluent avec le temps. Les refontes et évolutions permettent d'ajuster les systèmes pour répondre aux nouvelles exigences, qu'il s'agisse de nouvelles fonctionnalités, de l'intégration de nouveaux processus métier ou de l'amélioration de l'expérience utilisateur.

4. **Conformité Réglementaire** : Les régulations et les normes évoluent également. Maintenir les systèmes d'information à jour est essentiel pour garantir la conformité avec les législations en vigueur (NIS v2), évitant ainsi les risques légaux et les amendes potentielles.

5. **Favoriser l'Innovation** : Les évolutions technologiques offrent de nouvelles opportunités pour innover et améliorer les processus internes. En intégrant régulièrement ces innovations, les entreprises peuvent rester compétitives et répondre rapidement aux changements des besoins. Une infrastructure moderne permet d'intégrer plus facilement de nouvelles technologies et innovations, comme l'intelligence artificielle, l'Internet des objets (IoT) et le cloud computing, ce qui peut offrir un avantage significatif

Cependant, la mise en œuvre de refontes ou d'évolutions récurrentes peut poser plusieurs problématiques. Les coûts élevés associés aux mises à jour fréquentes peuvent être un obstacle majeur, car elles nécessitent des investissements financiers importants. Les interruptions d'activité liées aux mises à jour peuvent également perturber les opérations quotidiennes et entraîner une perte de productivité temporaire. De plus, la résistance au changement de la part des employés habitués aux anciens systèmes peut ralentir l'adoption des nouvelles technologies. La complexité de l'intégration des nouvelles solutions avec les systèmes existants représente un autre défi, nécessitant une planification minutieuse et des compétences techniques spécialisées. Enfin, le manque de compétences internes pour gérer et maintenir les nouvelles technologies peut nécessiter le recours à des consultants externes, ce qui peut augmenter les coûts.

Pour surmonter ces problématiques, plusieurs solutions peuvent être envisagées. Planifier soigneusement les mises à jour en définissant un calendrier précis et en communiquant efficacement avec les équipes permet de minimiser les interruptions d'activité. Allouer **un budget dédié pour les évolutions technologiques** et justifier l'investissement par les bénéfices à long terme peut aider à surmonter les contraintes financières. Mener des programmes de formation pour accompagner les employés dans l'adoption des nouvelles technologies et atténuer la résistance au changement est également crucial. Pour gérer la complexité de l'intégration, il est recommandé de faire appel à des experts internes ou externes qui possèdent les compétences nécessaires. Enfin, mettre en place un support technique continu pour assurer la maintenance et le bon fonctionnement des nouveaux systèmes renforce la sécurité et la performance.

Les refontes ou évolutions récurrentes des éléments d'un système d'information sont indispensables pour **assurer la performance, la sécurité et l'innovation** au sein d'une entreprise. Bien que ces processus puissent présenter des défis, une planification rigoureuse, une formation adéquate et un soutien technique approprié permettent de surmonter les obstacles et de maximiser les bénéfices. En adoptant une approche proactive et stratégique, Sud Roussillon peut maintenir ses systèmes à jour, rester compétitive et répondre efficacement aux besoins changeants de son environnement.

➔ ***OBJECTIF***

Mise à niveau des éléments actifs de notre infrastructure lors de plusieurs étapes :

Phase 1 : Remplacement de notre pare-feu (*2026*)

Phase 2 : Actualisation de notre centre de données (*2027*)

ENJEU N°1 – AXE 2 : Besoins immobiliers spécifiques

La gestion du risque en salle informatique impose de tenir compte de ses principales fonctions et caractéristiques associées, au rang desquelles on peut citer la forte concentration d'actifs IT fédérés (matériels et immatériels) d'importance cruciale pour le fonctionnement du Système d'Information :

- Serveurs,
- Zones de stockage de la donnée,
- Équipements actifs de réseau,
- Câbles,
- Données ;

La salle informatique comporte également des éléments d'infrastructure indispensables à la bonne marche de l'IT, destinés par exemple à assurer l'apport énergétique aux équipements informatiques, à offrir un espace de distribution cohérent et lisible pour le courant faible, à **assurer et optimiser** la gestion thermodynamique de la salle.

En plus de former un ensemble complexe de composants interconnectés, la salle informatique constitue souvent une zone de convergence de concentration des flux et transactions entre les utilisateurs, les fournisseurs de service et les partenaires. Les missions de la salle peuvent couvrir simultanément plusieurs besoins.

Par référence aux principaux modèles de gestion des risques, l'impact d'un sinistre en salle informatique s'avère par conséquent particulièrement élevé, coûteux avec une résolution non-immédiate. D'où la nécessité, en premier lieu, déjà mise en place, d'anticiper ce cas de figure en inscrivant la salle informatique au sein d'un ensemble multi-actifs en réseau à même de garantir la **continuité du service**, ou bien de disposer d'un plan de secours, activable *a posteriori* si la rupture occasionnelle du service est envisageable (Plan de Reprise Informatique).

En matière de typologie des menaces (lesquelles se distinguent notamment par leur grande diversité), une attention toute particulière doit être portée sur l'omniprésence de l'énergie en salle, soit la densité et la puissance du courant fort acheminé depuis les tableaux électriques ondulés jusqu'en face arrière des équipements IT. Cette caractéristique pose le problème des risques induits par la manipulation des réseaux électriques (qui ne devrait être réalisée que par des personnels disposant des habilitations d'usage), les éventuelles erreurs de conception dans la répartition de puissance et la segmentation de la disjonction, et génère de multiples contraintes additionnelles à gérer sous peine de panne ou de départ de feu : évacuation de la chaleur produite par dissipation thermique, restriction de l'impact des phénomènes électrostatiques et électromagnétiques.

Chiffres clés

***« Pannes Fréquentes** :*

Les serveurs dans des environnements mal ventilés ont 50 % plus de chances de tomber en panne »

***« Performance Dégradée** :*

Les entreprises avec des salles serveurs sous-dimensionnées signalent une réduction de 15 % de la performance des systèmes »

***« 20 % des incendies dans les centres de données** sont liés à des installations électriques surchargées »*

Une salle serveur exiguë présente plusieurs risques importants :

1. Surchauffe

Les équipements informatiques génèrent beaucoup de chaleur. Dans une salle exiguë, il peut être difficile de gérer efficacement la dissipation thermique, ce qui peut entraîner une surchauffe des serveurs et des pannes

2. Incendie

La concentration élevée d'équipements électriques et électroniques dans un espace restreint augmente le risque d'incendie. Une mauvaise gestion de la chaleur et des câbles peut provoquer des courts-circuits et des départs de feu

3. Accès et Maintenance Difficiles

L'espace limité rend l'accès aux équipements pour la maintenance et les réparations plus compliqué. Cela peut entraîner des temps d'arrêt prolongés et des difficultés à intervenir rapidement en cas de problème

4. Problèmes de Sécurité

Une salle exiguë peut compliquer la mise en place de mesures de sécurité adéquates, comme les systèmes de contrôle d'accès et les dispositifs de surveillance

5. Risque Électromagnétique

Les équipements électroniques concentrés dans un espace restreint peuvent générer des interférences électromagnétiques, affectant la performance des serveurs et d'autres équipements

6. Capacités d'évolutions limitées

Une salle exiguë limite la capacité d'ajouter de nouveaux équipements, freinant ainsi la croissance et l'évolution des infrastructures IT

Enfin, nos centres de données sont **les cœurs du fonctionnement numérique** de Sud Roussillon, leurs sécurités physiques doivent faire partie intégrante de la sécurité des systèmes d'information et être à l'état de l'art afin de s'assurer qu'ils ne puissent pas être contournés aisément. Il convient donc d'identifier les mesures de **sécurité physique adéquates** et de sensibiliser continuellement les utilisateurs aux risques engendrés par le contournement des règles.

Les accès aux salles serveurs et aux locaux techniques doivent être contrôlés à l'aide de serrures ou de mécanismes de contrôle d'accès par badge. Les accès à ces salles pour d'autres motifs que les besoins numériques ou les accès non accompagnés des prestataires extérieurs aux salles serveurs et aux locaux techniques sont à proscrire.

En résumé, fort de ce constat, une attention devra être portée à la mise en conformité des salles serveurs de Sud Roussillon. En effet, celle-ci ne présentent pas les prérequis essentiels à la sécurité de notre collectivité.

Il est convenu que des transformations sont prévues durant la restructuration des bureaux prévue dans les mois à venir devant amener des espaces plus sécurisants et pratiques assurant ainsi la sécurisation physique des systèmes d'information.

➔ ***OBJECTIF***

- Transformation de la salle « serveur de production » solutionnant les problématiques actuelles (2025)
- Mise en place d'éléments de sécurisation physique sur l'accès de la salle « serveur de PRA »

ENJEU N°1 – AXE 3 : Moyens de la DSI

La DSI accompagne depuis plusieurs années la collectivité dans sa **démarche de modernisation et d'efficience**.
Aujourd'hui, elle doit garder un coup d'avance dans le domaine technologique et anticiper les **évolutions du numérique et du collaboratif** pour promouvoir des idées et des solutions.

Malgré tous les efforts d'adaptation du personnel et son engagement avec un grand sens du service, la DSI est malgré tout contrainte par **le manque de ressources humaines** dans la mise en place de nouveaux projets ou d'évolution de projets existants mais aussi dans sa capacité à faire évoluer ses architectures pour être en conformité avec l'état de l'art. En effet, une part importante de son activité est consacrée au maintien en condition opérationnelle des applications déjà déployées.

Dans les prochaines années, pour faire face et mettre en place les grands projets, les compétences de la DSI vont devoir évoluer tout en veillant à ne pas négliger la **montée en compétences** et la formation nécessaire de certains agents pour occuper de nouveaux métiers. Renforcer ses compétences dans certains domaines, ainsi que sa capacité à faire pour maintenir la qualité de service rendue aux utilisateurs. Incontestablement, la DSI devra également mettre en œuvre de nouveaux projets de ce schéma directeur et bien d'autres.

Chiffres clés

« Les équipes IT sous-dimensionnées consacrent 70 % de leur temps à la maintenance et au support, laissant peu de temps à l'innovation au de nouveaux projets »

« 95 % des incidents de sécurité sont liés à des erreurs humaines, souvent exacerbées par une surcharge de travail et un manque de formation continue »

La DSI a été, et est encore, soumise à une forte pression en termes d'exigences de sécurité, de maintien en production, règlementaires (dématérialisations, sécurité, RGPD…), de besoins de la Direction, des services, dans un contexte de calendriers contraints.

Cela s'est accompagné également d'une évolution de son périmètre :

- Demandes de subventions,
- Démarrage de la stratégie sécurité et de la sensibilisation des agents,
- Proposition de solutions innovantes : LORA, CloudComputing, interconnexion rapides, …,
- Transformations de solutions hébergées en interne (GF, RH, Régie des eaux, …),
- Mise en place des documentations techniques de son infrastructure,
- Simplification des démarches des agents (fonctionnement quotidien, développement du télétravail…),
- Mise en œuvre de solutions nomades sécurisées,
- Conception et dispense de formations à la cybersécurité

Dans un contexte plus récent, la pandémie a accéléré l'essor des outils numériques et a fait **émerger d'autres perspectives** nécessitant de nouveaux moyens.

Enfin, des évolutions techniques rapides nécessitent un développement des connaissances et des profils à la DSI telles que :

- Innovation,
- Hypermobilité,
- Explosion des données (infrastructures à déployer, protection des données de la collectivité…),
- Sécurité, accompagnement des utilisateurs ;

Aujourd'hui, ce bilan fait émerger plusieurs problématiques :

1. **Surcharge de Travail**

- Le personnel est souvent surchargé, ce qui peut entraîner du stress, des erreurs et une baisse de la qualité du service

Chiffres clés

« Les équipes IT sous-dimensionnées sont 40 % moins efficaces dans la gestion des infrastructures et ont signalé des symptômes de burnout en raison de la charge de travail excessive »

2. **Réactivité Réduite**

- Avec des ressources limitées, la DSI peut avoir du mal à répondre rapidement aux incidents et aux demandes des utilisateurs, affectant ainsi la continuité des opérations

3. **Innovation Limitée**

- Un manque de personnel freine l'innovation et la mise en œuvre de nouveaux projets technologiques, car trop occupées par les tâches quotidiennes

4. **Risque de Burnout**

- Un sous-effectif peut entrainer des burnout en raison de la charge de travail excessive, ce qui peut entraîner une augmentation du turnover

5. **Sécurité Compromise**

- La gestion de la sécurité peut être négligée en raison du manque de personnel, augmentant ainsi les risques de cyberattaques et de violations de données

6. **Conformité et Réglementation**

- Avec des ressources humaines limitées, il peut être difficile de suivre et de se conformer aux nouvelles réglementations et normes de l'industrie

Les objectifs de la démarche seront les suivants :

1. **Améliorer l'Efficacité**

- Optimiser les processus internes pour maximiser l'efficacité des équipes existantes

2. **Renforcer la Sécurité**

- Assurer une gestion proactive de la sécurité pour protéger les données et les systèmes

3. **Favoriser l'Innovation**

- Libérer du temps pour que les équipes puissent se concentrer sur des projets innovants

4. **Prévenir le Turnover**

- Améliorer les conditions de travail pour réduire le stress et le burnout

En résumé, augmenter les moyens humains de la DSI permet non seulement **d'améliorer la réactivité et la sécurité**, mais aussi de **favoriser l'innovation**, de réduire le stress des employés et d'améliorer la qualité du service. Cela contribue à la **performance globale** et a l'efficacité opérationnelle de la collectivité.

Pour répondre à ces problématiques, une évolution des moyens humains est à envisager en plusieurs étapes pour atteindre une capacité cohérente.

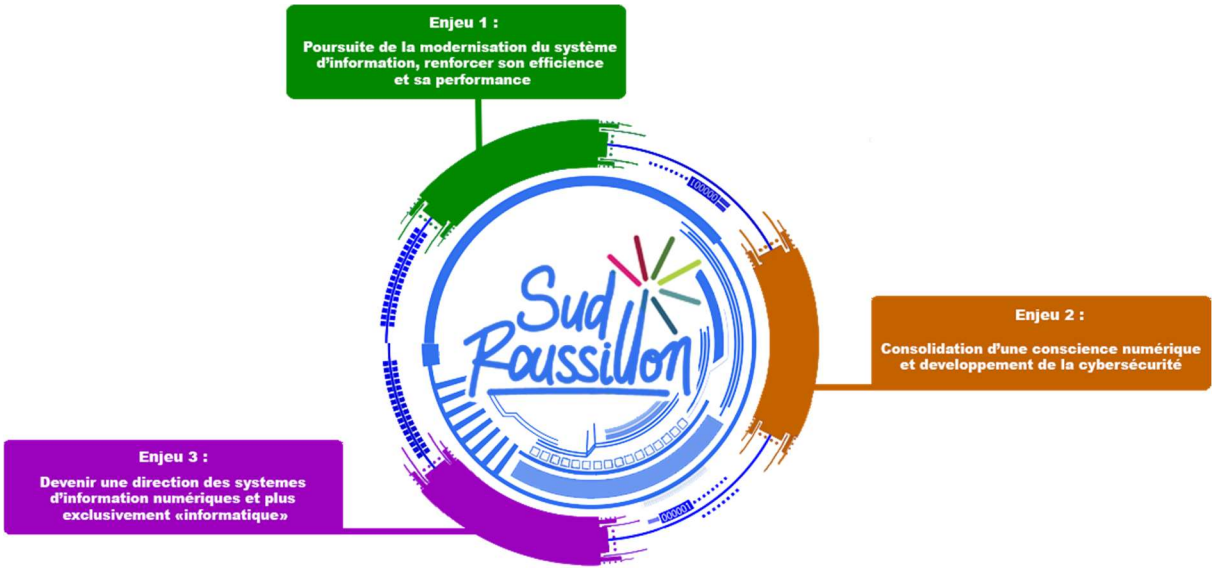
➔ ***OBJECTIF***

Faire évoluer les moyens humains de la DSI

CONSOLIDATION D'UNE CONSCIENCE NUMÉRIQUE ET DÉVELOPPEMENT DE LA CYBERSÉCURITÉ

OBJECTIF :

Renforcer la politique de sécurisation face aux risques.



1 – CONTEXTE

Notre collectivité est de plus en plus connectée, ouverte (portails, télétravail, smartphones…), dématérialisée et agrège des données personnelles des citoyens comme l'identité, les coordonnées bancaires, des consommations… Une manne financière pour les hackers.

État des lieux des attaques *(source : ANSSI)*

La cybersécurité est devenue un enjeu de **souveraineté nationale**.

Il revient à chaque organisation de « trouver l'équilibre entre la défense de ses principaux actifs face à des attaques cybercriminelles et le coût des mesures de cybersécurité »

Les cybermenaces (vol de données, ransomwares, hameçonnage…) doivent être intégrées à une politique de gestion des risques et de gouvernance de la collectivité qui dépasse largement le périmètre informatique. S'agissant du risque cyber, les systèmes d'information sont en évolution permanente (ouverture, mobilité), complexes à appréhender globalement (chaine de sous-traitance, externalisation de tout ou partie des systèmes d'information, téléphonie…) et pas uniquement techniques (humains, organisationnels…). Dès lors, les risques associés le sont également et cela impose d'innover en termes de moyens et de réponses pour faire face à ces nouveaux risques, y compris réglementaires.

Les solutions de **réduction du risque** sont autant techniques (firewall, sauvegardes, chiffrement des données…) que liées à la mise en place de processus (analyse des risques, règles de développement, normes de sécurité…). Elles doivent également être humaines (formation et sensibilisation de tous les utilisateurs) et financières.

Les cybercriminalités en augmentation

- Les attaques par logiciels rançon et autres logiciels malveillants modulaires ou à plusieurs niveaux / couches vont devenir la norme, car cette technique d'évitement devient plus répandue. Les attaques modulaires utilisent des chevaux de Troie et des virus pour lancer l'attaque avant le téléchargement et le lancement du véritable ransomware ou programme malveillant.
- 70 % des attaques exploitant des programmes malveillants utiliseront le chiffrement pour contourner les mesures de sécurité (attaques par logiciel malveillant chiffré). Il va devenir de plus en plus difficile de réunir les **compétences de sécurité indispensables en interne**.

Chaque année apporte son lot de nouveautés en matière de menaces de sécurité, de violations de données et de défis opérationnels, ce qui signifie que les entreprises, les collectivités et les consommateurs doivent constamment rester sur leur garde. Les 5 prochaines années ne seront pas différentes, notamment avec la transition vers les réseaux mobiles 5G et la généralisation de l'IoT. Le risque de cyberattaques massives et généralisées s'est accru de façon exponentielle.

Les prises en compte de cette situation imposent à la collectivité de prendre des mesures essentielles à sa sécurité à travers 4 axes stratégiques :

- **Uniformisation de la sécurité**

L'état des lieux des différents sites montre un déséquilibre entre les moyens mise en œuvre.

L'état de l'art énonce des mesures essentielles au maintien de la cybersécurité qui ne sont pas mises en œuvre sur certains de nos établissements.

Au-delà d'une prise de risque pour la structure cible, une compromission pourrait s'étendre sur la totalité des SI de par leurs imbrications.

- **Segmentation des réseaux et des données**

Les nouvelles techniques cyber malveillantes fonctionnent souvent par rebonds pour atteindre toutes les machines interconnectées.

Comme nous l'avons évoqué précédemment, ces attaques sont de plus en plus sophistiquées, efficaces et difficile à endiguer.

L'ANSSI préconise, dans ses différents guides, la sectorisation des machines et des données pour restreindre autant que faire ce peu les surfaces atteintes.

- **Formations des agents aux risques numériques**

Le **1er rempart étant humain**, la DSI a lancé dès 2021 une sensibilisation des agents par des formations, un règlement d'usage des systèmes d'information ainsi que des rencontres avec les agents. Cet axe propose de poursuivre cette sensibilisation pour devenir une activité récurrente.

- **Informations transverses dès la conception des projets**

Jadis, l'outil informatique n'était qu'un support. Les études menées au cours des dernières années, montrent une part grandissante du numérique dans tous les sujets métiers. Il devient aujourd'hui la solution a part entière. Cela implique une **vision IT** dès la conception des projets pour garantir interopérabilité, sécurité et faisabilité.

2 - AXES STRATÉGIQUES

ENJEU N°2 – AXE 1 : Uniformisation de la sécurité des sites

Dans le monde interconnecté d'aujourd'hui, les systèmes d'information (SI) jouent un rôle crucial dans les opérations quotidiennes des entreprises. Assurer la sécurité de ces systèmes est essentiel pour protéger les données sensibles, maintenir la continuité des activités, et respecter les réglementations en vigueur. L'uniformisation de la sécurité de tous les sites d'un SI au sein d'une entreprise est une pratique fondamentale pour garantir une protection cohérente et efficace contre les cybermenaces. La cybersécurité homogène consiste à appliquer des mesures de **sécurité uniformes et cohérentes** sur l'ensemble des sites d'une entreprise. Cela inclut non seulement les bureaux et les infrastructures physiques, mais également les plateformes numériques, et les sites distants.

Importance d'une Cybersécurité Homogène

1. **Protection Unifiée** : En appliquant des politiques de sécurité homogènes, toutes les parties de l'entreprise bénéficient du même niveau de protection contre les cybermenaces. Cela réduit le risque de vulnérabilités exploitables par des attaquants.

2. **Réduction des Points Faibles** : Une cybersécurité uniforme permet de minimiser les failles de sécurité potentielles. Si chaque site applique les mêmes normes, il est moins probable que des failles apparaissent dans des sites moins sécurisés.

3. **Gestion Centralisée** : Une approche homogène facilite la gestion centralisée des politiques de sécurité. Les administrateurs peuvent déployer des mises à jour et des correctifs à travers l'ensemble des sites sans devoir ajuster les configurations pour chaque lieu individuellement.

4. **Conformité Réglementaire** : Les entreprises doivent souvent se conformer à diverses réglementations de sécurité des données (comme le RGPD). Une stratégie de cybersécurité homogène assure que tous les sites respectent ces lois, évitant ainsi les amendes et les sanctions.

Chiffres clés

***Investissements en sécurité** : Les entreprises dépensent en moyenne **15% de leur budget IT** en sécurité informatique, selon une étude de Gartner*

5. **Réponse aux Incidents** : En cas de cyberattaque, une sécurité homogène permet une réponse plus rapide et coordonnée. Les équipes de sécurité peuvent identifier et contenir les menaces plus efficacement lorsqu'elles travaillent avec des systèmes et des procédures uniformes.

6. **Optimisation des Ressources** : L'uniformité dans les pratiques de cybersécurité permet d'optimiser l'utilisation des ressources. Les formations, les outils de sécurité, et les procédures opérationnelles peuvent être standardisés, réduisant ainsi les coûts et les efforts redondants.

En première ligne, un **pare-feu** en tête de réseau joue un rôle crucial dans la protection des réseaux contre les menaces extérieures et intérieures. Il agit comme une **barrière de sécurité** en surveillant et contrôlant le trafic réseau entrant et sortant selon des règles de sécurité prédéfinies.

Importance d'un Pare-feu en Tête de Réseau

1. **Protection Maximale** : En étant placé en tête de réseau, un pare-feu filtre tout le trafic entrant avant qu'il n'atteigne les autres parties du réseau. Cela empêche les attaques potentielles et les accès non autorisés dès la périphérie du réseau.

2. **Contrôle du Trafic** : Il permet de gérer et de contrôler le trafic réseau de manière plus efficace. Les administrateurs peuvent définir des règles spécifiques pour autoriser ou bloquer certains types de trafic, en fonction des besoins de sécurité de l'organisation.

3. **Détection et Prévention des Intrusions** : Un pare-feu en tête de réseau intègre souvent des systèmes de détection et de prévention des intrusions (IDS/IPS) qui analysent le trafic pour détecter des comportements suspects et des tentatives d'intrusion, bloquant ainsi les menaces en temps réel.

4. **Sécurité Renforcée** : En bloquant les connexions non sécurisées et en surveillant les activités suspectes, le pare-feu protège les données sensibles et prévient les fuites d'informations.

5. **Gestion des Politiques de Sécurité** : Il facilite l'application centralisée des politiques de sécurité, permettant une gestion cohérente et efficace des règles de sécurité à travers l'ensemble du réseau.

6. **Surveillance et Reporting** : Les pare-feu en tête de réseau offrent des capacités avancées de surveillance et de génération de rapports. Cela permet aux administrateurs de réseau de suivre les activités, de détecter les anomalies et de prendre des mesures correctives rapidement.

7. **Mise en Conformité** : En assurant la protection et la confidentialité des données, les pares-feux aident les entreprises à se conformer aux réglementations et aux standards de sécurité, tels que le RGPD (Règlement Général sur la Protection des Données), réglementation DORA et NISv2.

La mise en place d'une cybersécurité homogène sur tous les sites d'une entreprise est cruciale pour garantir une protection robuste et cohérente contre les cybermenaces. Elle simplifie la gestion de la sécurité, assure la **conformité réglementaire**, et renforce la confiance des parties prenantes. En fin de compte, une approche unifiée de la cybersécurité contribue à la résilience et à la continuité des activités de l'entreprise.

Un pare-feu en tête de réseau est un élément essentiel de **la stratégie de sécurité informatique** d'une organisation. Il offre une protection robuste contre les cyberattaques et les accès non autorisés, améliore la gestion du trafic réseau. En somme, il constitue une **première ligne de défense indispensable** pour maintenir la sécurité et l'intégrité des réseaux.

➔ ***OBJECTIF***

- Mise à plat et évolution des sécurités des sites distants

Chiffres clés

Réduction des risques de sécurité : *Environ **70%** des cyberattaques exploitent des vulnérabilités internes. La segmentation permet de limiter la propagation de ces attaques en isolant les différents segments du réseau*

***Temps de récupération** : Le temps moyen de récupération après une attaque est réduit de **50%** avec une segmentation efficace*

ENJEU N°2 – AXE 2 : Segmentation des réseaux et des données

Lorsque le réseau est « à plat », sans aucun mécanisme de cloisonnement, chaque machine du réseau peut accéder à n'importe quelle autre machine. La compromission de l'une d'elles met alors en péril l'ensemble des machines connectées. Un attaquant peut ainsi compromettre un poste utilisateur et ensuite « rebondir » jusqu'à des serveurs critiques. Il est donc crucial, dès la conception de l'architecture réseau, de raisonner par segmentation en zones composées de systèmes ayant des besoins d'interconnexions et de sécurité homogènes. Par exemple, il est pertinent de regrouper distinctement des serveurs d'infrastructure, des serveurs métiers, des postes de travail utilisateurs, des postes de travail administrateurs, des postes de téléphonie sur IP, des outils d'impression, etc.

Sans segmentation, la gestion d'un réseau large et complexe peut devenir ingérable, rendant difficile la surveillance et la mise en œuvre des **politiques de sécurité**. Les réseaux non segmentés sont plus vulnérables aux attaques, car une fois qu'un attaquant pénètre dans le réseau, il peut se déplacer latéralement sans entrave. De plus, les réseaux non segmentés présentent un risque accru de **propagation rapide des menaces**, comme les malwares et les ransomwares. La difficulté à isoler les incidents de sécurité peut entraîner des interruptions de service étendues.

Il est primordial d'assurer la confidentialité, l'intégrité et la disponibilité des données sensibles en limitant les mouvements latéraux des attaquants. La segmentation permet de réduire le risque de fuites de données et de violations de la vie privée. Elle aide également à se conformer aux réglementations en matière de protection des données, comme le RGPD, en limitant l'accès aux données sensibles et en évitant les sanctions et les amendes liées à la non-conformité. Enfin, la segmentation contribue à préserver la réputation de l'entreprise en évitant les incidents de sécurité majeurs.

La segmentation réduit la surface d'attaque et limite les points d'entrée pour les cybercriminels. Si un segment est compromis, l'impact est contenu, ce qui empêche l'attaquant de compromettre l'ensemble du réseau. En segmentant le réseau, on empêche les attaquants de se déplacer librement d'un segment à l'autre, limitant ainsi la propagation des menaces. En cas d'incident, les segments non affectés continuent de fonctionner normalement, ce qui améliore la résilience. La segmentation simplifie également la gestion du réseau. Les équipes IT peuvent se concentrer sur des segments spécifiques, facilitant ainsi la surveillance et la maintenance. Moins de pannes et de temps d'arrêt se traduisent par des économies significatives. De plus, la segmentation permet de contrôler le flux de trafic et de réduire la congestion, améliorant ainsi les performances globales du

réseau. En isolant les segments, les ressources peuvent être allouées plus efficacement en fonction des **besoins spécifiques** de chaque segment.

Enfin, une infrastructure sécurisée permet à l'entreprise de se concentrer sur l'innovation et le développement de nouveaux services, tout en facilitant l'adoption de nouvelles technologies et de la transformation numérique.

Pour segmenter les réseaux informatiques, il est possible d'utiliser plusieurs méthodes, la segmentation physique, en implémentant des routeurs, commutateurs et pare-feu pour créer des segments distincts. Chaque segment est physiquement séparé, ce qui permet un contrôle granulaire du trafic. Par exemple, un réseau d'entreprise peut être divisé en segments pour les départements RH, finance et IT, chacun ayant ses propres équipements de sécurité.

La segmentation logique peut également être utilisée, en créant des VLANs (Virtual Local Area Networks) pour segmenter logiquement le réseau au sein d'un même réseau physique. Cela permet de séparer le trafic sans nécessiter de matériel supplémentaire.

Les sous-réseaux peuvent également être utilisés pour diviser le réseau en segments distincts, chacun avec ses propres adresses IP et politiques de sécurité.

Enfin, la micro-segmentation permet d'appliquer des politiques de sécurité spécifiques à des charges de travail et des applications individuelles, souvent à l'aide de logiciels de gestion de réseau. Par exemple, dans un environnement cloud, chaque application peut être isolée dans son propre segment, avec des règles de sécurité adaptées à ses besoins spécifiques.

En résumé, la segmentation des réseaux informatiques est essentielle pour **protéger les données, assurer la conformité réglementaire**, et maintenir la réputation de l'entreprise. Elle permet également de réduire les risques, d'améliorer l'efficacité opérationnelle et de favoriser l'innovation. Elle est une mesure également pour limiter les problématiques lorsque le vecteur d'infection est dû à une défaillance humaine comme dans 90% des cas. Une transformation comme le cloisonnement a posteriori ne serait pas aisée, il est recommandé d'intégrer cette démarche dans toute nouvelle extension du réseau ou à l'occasion d'un renouvellement d'équipements.

➔ ***OBJECTIF***

- Étude de restructuration de l'infrastructure en réseaux séparés
- Mise en application des segmentations

Chiffres clés

90% des cyberattaques nécessitent une interaction humaine *: Cela signifie que des actions simples comme cliquer sur un lien de phishing ou utiliser des mots de passe faibles peuvent entraîner des violations de sécurité*

ENJEU N°2 – AXE 3 : Formations des agents aux risques numériques

Dans le monde numérique actuel, les cybermenaces sont en constante augmentation et deviennent de plus en plus sophistiquées. La cybersécurité n'est plus seulement une question de technologie mais une **responsabilité partagée** par tous les membres d'une organisation.

C'est pourquoi la formation et la sensibilisation à la cybersécurité des collaborateurs sont cruciales pour protéger l'entreprise contre les attaques potentielles et **garantir la sécurité** des informations sensibles.

Chaque utilisateur est un maillon à part entière de la chaîne des systèmes d'information. À ce titre et dès son arrivée dans l'entité, il doit être informé des enjeux de sécurité, des **règles à respecter et des bons comportements** à adopter en matière de sécurité des systèmes d'information à travers des actions de sensibilisation et de formation.

Ces dernières doivent être régulières et adaptées aux utilisateurs ciblés, peuvent prendre différentes formes (mails, affichage, réunions, espace intranet dédié, etc.).

Importance de la Formation et Sensibilisation

1. **Réduction des Risques** : Les employés bien informés sont moins susceptibles de commettre des erreurs qui pourraient compromettre la sécurité de Sud Roussillon, telles que cliquer sur des liens de phishing ou utiliser des mots de passe faibles.

2. **Détection Précoce des Menaces** : Les collaborateurs formés peuvent identifier les signes d'activités suspectes et signaler rapidement les incidents, permettant une intervention rapide et limitant les dommages potentiels.

3. **Culture de Sécurité** : La sensibilisation continue renforce une culture de sécurité au sein de l'entreprise, où chaque employé se sent responsable de la protection des actifs numériques.

4. **Conformité Réglementaire** : De nombreuses réglementations exigent des formations en cybersécurité régulières. Une formation adéquate aide la collectivité à rester conforme et à éviter des sanctions légales.

La mise en place d'un programme de formation et de sensibilisation à la cybersécurité peut rencontrer plusieurs problématiques. **La résistance au changement est souvent un défi**, car certains employés peuvent être réticents à suivre de nouvelles directives ou à investir du temps dans des

formations. La diversité des compétences des collaborateurs est également une problématique, car il peut être difficile de concevoir des **programmes adaptés** à tous les niveaux de connaissances et d'expertise. En outre, la mise à jour continue des connaissances est nécessaire pour suivre **l'évolution rapide des menaces et des technologies**, ce qui peut représenter un défi logistique et financier. Enfin, il peut être difficile de mesurer l'efficacité des formations en cybersécurité et de s'assurer que les compétences acquises sont appliquées correctement au quotidien.

Pour surmonter ces problématiques, plusieurs solutions peuvent être mises en place. Adopter une approche personnalisée de la formation permet de mieux répondre aux besoins individuels des collaborateurs en fonction de leurs rôles et de leurs compétences. Utiliser des méthodes interactives et engageantes, telles que des simulations de phishing, des jeux sérieux ou des ateliers pratiques, peut augmenter l'engagement et l'adhésion des employés. Mettre en place une formation continue et régulière, en utilisant des plateformes en ligne, des sessions en présentiel ou des webinaires, permet de maintenir les connaissances à jour et d'adapter les contenus aux nouvelles menaces. De plus, il est crucial de mesurer l'efficacité des formations en cybersécurité en utilisant des évaluations, des tests et des simulations pour s'assurer que les compétences sont bien acquises et appliquées. Enfin, impliquer la direction et les leaders de l'entreprise dans la promotion et le soutien des initiatives de cybersécurité renforce l'importance de ces actions et motive les collaborateurs à les suivre.

La formation et la sensibilisation à la cybersécurité des collaborateurs sont essentielles pour protéger l'entreprise contre les **menaces croissantes et complexes du monde numérique**. En investissant dans des programmes de formation adaptés et continus, les entreprises peuvent réduire les risques de cyberattaques, renforcer leur culture de sécurité et garantir la conformité avec les réglementations. Adopter des solutions pour surmonter les problématiques associées à la mise en œuvre de ces programmes est crucial pour leur succès et leur efficacité à long terme.

Exemples de réussites

Airbus a développé un programme de sensibilisation à la cybersécurité qui inclut des formations obligatoires pour tous les employés, des campagnes de communication internes et des exercices de simulation d'attaques.

AXA a lancé une initiative globale de sensibilisation à la cybersécurité, incluant des formations en ligne, des ateliers en présentiel et des campagnes de communication. L'entreprise utilise des vidéos, des infographies et des quiz pour rendre la formation plus accessible et interactive

➔ ***OBJECTIF***

- Poursuite et approfondissement des formations a la cybersécurité des agents

ENJEU N°2 – AXE 4 : Informations transverses dès la conception des projets

Dans le monde de l'entreprise d'aujourd'hui, la technologie est un élément central qui influence presque tous les aspects de l'activité d'une entreprise. La Direction des Systèmes d'Information (DSI), responsable de la gestion et de l'optimisation des technologies de l'information, joue un rôle crucial dans la réussite des projets. Intégrer la DSI dès la phase de conception de chaque projet est donc indispensable pour plusieurs raisons clés.

Alignement Stratégique

Impliquer la DSI dès le départ permet de garantir que les projets sont en **adéquation avec la stratégie technologique globale de l'entreprise**. Cela assure que les initiatives sont alignées avec les objectifs à long terme et les priorités de l'organisation, réduisant ainsi les risques de redondance et de conflits entre les différents projets technologiques.

Sécurité et Conformité

La sécurité des données et la conformité aux réglementations sont des préoccupations majeures pour toutes les entreprises. La DSI, en tant qu'expert en sécurité informatique, peut intégrer des mesures de sécurité robustes dès la conception des projets. Elle veille également à ce que toutes les solutions soient conformes aux législations en vigueur, évitant ainsi les potentielles amendes et atteintes à la réputation.

Optimisation des Ressources

Une implication précoce de la DSI permet une meilleure planification et utilisation des ressources technologiques. Cela inclut la sélection des plateformes appropriées, la prévision des besoins en infrastructure, et l'allocation optimale des équipes techniques. Cela contribue à éviter les surcoûts et les retards, tout en maximisant l'efficacité des projets.

Innovation et Compétitivité

La DSI se doit d'être à la pointe des innovations technologiques. En intégrant la DSI dès le début, les entreprises peuvent bénéficier de solutions innovantes qui non seulement améliorent les processus internes mais aussi offrent des avantages compétitifs. Cela permet de rester à jour avec les tendances technologiques et d'adopter rapidement de nouvelles technologies pertinentes.

Gestion des Risques

Les projets d'entreprise sont souvent accompagnés de divers risques, notamment technologiques. La DSI, avec son expertise, est capable d'identifier et de mitiger ces risques dès la phase de planification. Une gestion proactive des risques permet de minimiser les interruptions et les imprévus qui pourraient compromettre la réussite du projet.

Amélioration de la Collaboration

L'intégration de la DSI dès le début favorise une meilleure communication et collaboration entre les différentes parties prenantes. Cela permet de s'assurer que les besoins et les contraintes technologiques sont bien compris et pris en compte dans la planification du projet. Une collaboration étroite entre la DSI et les autres services facilite également la résolution rapide des problèmes qui pourraient survenir au cours du projet.

Cependant, l'intégration de la DSI dès la conception des projets peut rencontrer certaines problématiques. Les silos organisationnels peuvent rendre difficile la collaboration entre la DSI et les autres services, freinant ainsi l'alignement des projets. De plus, il peut y avoir une résistance au changement de la part des équipes qui sont habituées à leurs propres processus de travail. La **complexité technologique** est également une préoccupation, car les projets peuvent nécessiter des compétences spécifiques et une intégration complexe avec les systèmes existants. Enfin, il y a des contraintes budgétaires qui peuvent limiter les ressources disponibles pour inclure la DSI dans toutes les phases des projets.

Pour surmonter ces problématiques, il est crucial de mettre en place plusieurs stratégies. Premièrement, démanteler les silos organisationnels en favorisant une culture de collaboration interfonctionnelle peut faciliter l'intégration de la DSI. Deuxièmement, mener des programmes de gestion du changement pour préparer les équipes à adopter de nouvelles pratiques et technologies. Troisièmement, investir dans la formation continue pour doter les membres de la DSI des compétences nécessaires pour gérer la complexité technologique. Enfin**, allouer des ressources humaines suffisantes** en démontrant les bénéfices à long terme de l'intégration précoce de la DSI.

En somme, intégrer la DSI dès la conception de tous les projets d'entreprise est **un facteur clé de succès**. Cela permet de garantir un alignement stratégique, une sécurité renforcée, une optimisation des ressources, une capacité d'innovation accrue, une gestion efficace des risques, et une collaboration améliorée. En faisant de la DSI un partenaire stratégique dès le début Sud Roussillon peut non seulement **améliorer la qualité et l'efficacité de ses projets**, mais aussi renforcer sa position compétitive dans un environnement numérique en constante évolution.

➔ ***OBJECTIF***

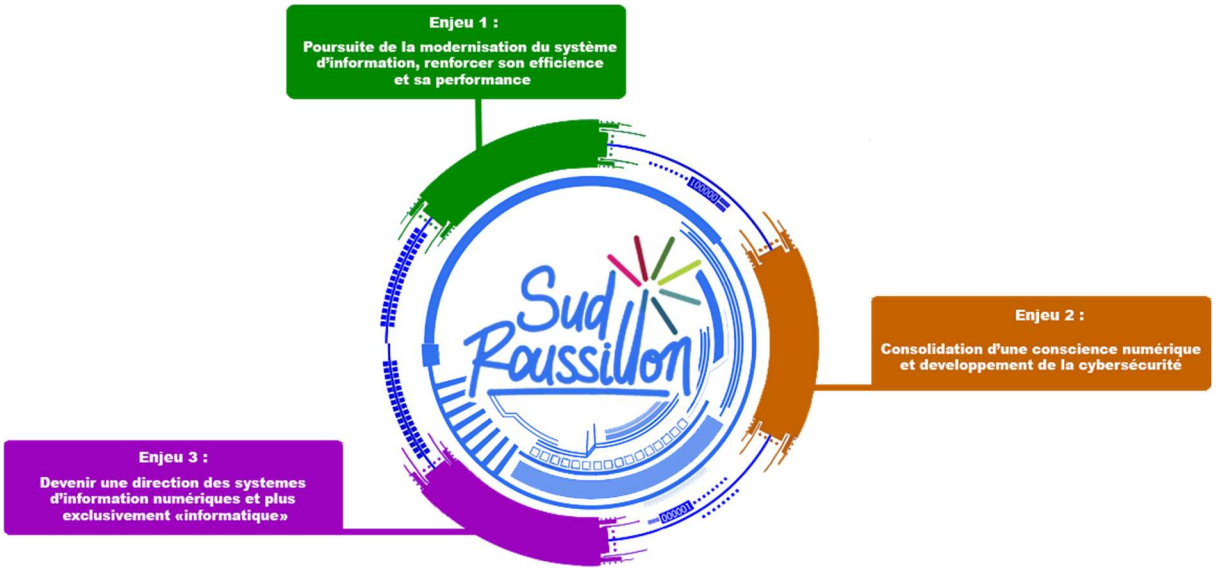
- Intégrer la DSI dès la conception des projets.

ENJEU 3

DEVENIR UNE DIRECTION DES SYSTÈMES D'INFORMATION NUMÉRIQUES ET PLUS EXCLUSIVEMENT « INFORMATIQUE »

OBJECTIF :

Amener sereinement la DSI dans son rôle transversal.



1 – CONTEXTE

À l'ère du numérique, les entreprises sont confrontées à des changements rapides et profonds qui transforment la manière dont elles opèrent et se développent. La Direction des Systèmes d'Information (DSI), traditionnellement centrée sur la gestion des infrastructures informatiques et le support technique, doit évoluer pour répondre à ces **nouvelles exigences**. Cette transformation vers une DSI numérique plus large représente une **opportunité stratégique majeure** pour les organisations cherchant à rester compétitives et innovantes.

La DSI numérique ne se limite plus à la gestion des systèmes informatiques. Elle englobe désormais des responsabilités plus vastes telles que la transformation digitale, l'innovation technologique, la gestion des données, la cybersécurité et l'amélioration de l'expérience utilisateur. En adoptant une approche numérique, la DSI devient un **catalyseur de changement**, capable de conduire des initiatives qui transforment les processus internes, améliorent les services et soutiennent la croissance de la collectivité.

Cette transition s'accompagne de nombreux avantages. Une DSI numérique permet une plus grande agilité, facilitant une adaptation rapide aux **évolutions des pratiques et aux besoins**. Elle offre également une meilleure intégration des technologies émergentes comme l'intelligence artificielle, le cloud computing et l'Internet des objets, ouvrant ainsi la voie à des innovations continues. De plus, en mettant l'accent sur la gestion des données et la sécurité, la DSI numérique contribue à protéger les actifs informationnels critiques de Sud Roussillon tout en garantissant la conformité avec les réglementations en vigueur.

Cette transition s'accompagne toutefois de plusieurs problématiques. Les coûts initiaux élevés représentent un obstacle majeur, car la mise en place des nouvelles infrastructures numériques et la formation des employés nécessitent des investissements importants. De plus, la résistance au changement est souvent rencontrée au sein des équipes habituées aux anciennes méthodes de travail, ce qui peut ralentir la mise en œuvre des nouvelles technologies. Les défis liés à l'intégration des systèmes sont également considérables, car les nouvelles solutions numériques doivent s'interfacer de manière fluide avec les systèmes existants. Enfin, la sécurité des données et la conformité aux réglementations représentent des défis permanents, nécessitant une vigilance constante pour protéger les informations sensibles et éviter les infractions légales.

Pour surmonter ces problématiques, plusieurs solutions peuvent être mises en œuvre. Tout d'abord, il est essentiel de définir une vision stratégique claire, alignée sur les objectifs de la collectivité, et de mobiliser le soutien de la direction pour garantir une adhésion totale à la transformation. L'adoption de méthodologies agiles permet de gérer les projets de transformation de manière itérative et flexible, facilitant ainsi l'adaptation rapide aux changements. Investir dans des technologies émergentes telles que l'intelligence artificielle et le cloud computing offre des opportunités d'innovation et d'amélioration des processus. De plus, il est crucial de former et d'accompagner les équipes pour les préparer aux nouvelles compétences requises et atténuer la résistance au changement. Enfin, la mise en place de mesures de sécurité renforcées et le suivi régulier des conformités garantissent la protection des données et le respect des lois en vigueur.

En somme, passer d'une DSI purement informatique à une DSI numérique est une évolution nécessaire pour toute organisation souhaitant tirer pleinement parti des opportunités offertes par la transformation digitale. Cela nécessite une **vision stratégique**, un **engagement fort** de la part de la direction, et une culture d'innovation et d'adaptation continue. Cette transformation positionne la DSI comme un partenaire clé dans la réalisation des objectifs stratégiques de l'entreprise, tout en renforçant sa capacité à innover et à prospérer dans un environnement numérique en constante évolution.

2 - AXES STRATÉGIQUES

ENJEU N°3 – AXE 1 : SIG mutualisé / LORA

Dans un contexte économique et technologique en constante évolution, les collectivités territoriales sont confrontées à des défis de plus en plus complexes. La nécessité de fournir des services publics de qualité, de maîtriser les dépenses et de répondre aux attentes croissantes des citoyens exige une gestion plus efficiente et innovante des ressources. C'est dans ce cadre que la mutualisation des ressources et des outils entre les collectivités territoriales prend tout son sens.

La mutualisation, en permettant le partage de ressources technologiques, offre de nombreux avantages. Elle favorise des **économies d'échelle significatives**, réduit les coûts d'acquisition et de maintenance, et optimise l'utilisation des infrastructures existantes. De plus, elle permet aux collectivités de bénéficier des meilleures pratiques et innovations en matière de gestion publique, en tirant parti des expériences et des expertises de chacune.

En mutualisant leurs ressources, les collectivités peuvent également renforcer la qualité et la cohérence des services publics offerts aux citoyens. Elles peuvent partager des systèmes d'information intégrés, faciliter la **collaboration entre les différents services**, et garantir une meilleure accessibilité et transparence des informations. Cette approche collaborative est essentielle pour répondre efficacement aux **enjeux de modernisation de l'administration publique** et pour soutenir le développement durable des territoires.

En somme, la mutualisation des ressources et des outils entre collectivités territoriales est une stratégie gagnant-gagnant qui permet de conjuguer efficacité, innovation et qualité des services publics. Elle constitue une réponse adaptée aux contraintes budgétaires actuelles et aux besoins croissants des citoyens, tout en renforçant la solidarité et la coopération entre les territoires.

Dans ce contexte, Sud Roussillon dispose de deux outils qui pourraient répondre à ces préoccupations.

Un SIG mutualisé

Dans un contexte où la gestion des ressources et l'optimisation des services publics sont des enjeux cruciaux, la mutualisation d'un Système d'Information Géographique (SIG) entre les collectivités territoriales apparaît comme une solution stratégique et efficiente. Un SIG mutualisé permet aux collectivités de **partager des données géographiques**, des outils, et des infrastructures, offrant ainsi de nombreux avantages pour la gestion territoriale.

La mutualisation d'un SIG favorise d'abord des économies substantielles. En partageant les coûts d'acquisition, de maintenance et de mise à jour des logiciels et matériels nécessaires à un SIG, les collectivités peuvent réduire significativement leurs dépenses. Cela permet également d'allouer les ressources financières économisées à d'autres projets prioritaires. De plus, un SIG mutualisé offre un accès équitable à des **technologies avancées**, même pour les collectivités de plus petite taille qui pourraient ne pas avoir les moyens de développer et de maintenir un SIG complet de manière autonome.

Un autre avantage majeur réside dans l'amélioration de la qualité et de la **précision des données géographiques**. En mutualisant leurs efforts, les collectivités peuvent créer une base de données géographiques commune, régulièrement mise à jour et enrichie par les contributions de chaque partenaire. Cette collaboration renforce la fiabilité des données utilisées pour la planification urbaine, la gestion des infrastructures, la protection de l'environnement, et bien d'autres domaines.

Les SIG mutualisés contribuent également à la transparence et à la participation citoyenne. En rendant les données géographiques **accessibles au public**, les collectivités peuvent renforcer la confiance des citoyens et encourager leur participation aux processus décisionnels. Cela permet une meilleure communication avec le public et une plus grande implication des habitants dans les projets locaux.

Un réseau LORA privé du territoire intercommunal

Dans un monde de plus en plus connecté, les technologies de l'Internet des Objets (IoT) jouent un rôle crucial dans la gestion des services publics et l'optimisation des ressources. Le réseau LoRa (Long Range) est une technologie de communication sans fil qui permet de connecter une multitude d'appareils IoT sur de longues distances avec une faible consommation d'énergie. La mutualisation d'un réseau LoRa privé entre les collectivités territoriales offre des avantages significatifs pour la gestion territoriale et le développement durable.

La mutualisation d'un réseau LoRa permet de réaliser des économies substantielles. En partageant les coûts d'installation, de maintenance et de mise à jour des infrastructures nécessaires, les collectivités peuvent réduire considérablement leurs dépenses. Cela permet aussi d'accéder à une **technologie de pointe**, même pour les collectivités de plus petite taille qui pourraient avoir des budgets limités. En outre, un réseau LoRa mutualisé assure une couverture étendue et homogène sur l'ensemble des territoires participants, garantissant ainsi une connectivité fiable et continue pour les dispositifs IoT.

Un autre avantage majeur de la mutualisation d'un réseau LoRa réside dans l'amélioration de la gestion des ressources et des services publics. Par exemple, les capteurs IoT connectés via le réseau LoRa peuvent surveiller en temps réel la qualité de l'air, la gestion des déchets, l'éclairage public, ou encore la consommation d'eau et d'énergie. Ces données précises et en temps réel permettent aux collectivités de prendre des **décisions éclairées**, d'optimiser l'utilisation des ressources et d'améliorer la qualité des services offerts aux citoyens.

La mutualisation d'un outil permet également de renforcer la collaboration entre les collectivités territoriales. En travaillant ensemble sur des projets communs, elles peuvent partager leurs expériences, leurs bonnes pratiques et leurs expertises, ce qui conduit à une meilleure coordination et à une gestion plus efficace des territoires. Cela favorise également une **approche cohérente et harmonisée** de l'aménagement du territoire, évitant les doublons et les conflits entre les différentes collectivités.

Toutefois, la mise en place d'un réseau LoRa mutualisé peut présenter des défis. La coordination entre les différentes collectivités participantes peut être complexe, nécessitant une gouvernance claire et une communication efficace. Les questions de standardisation des protocoles et des

données peuvent également poser des problèmes, car il est crucial de s'assurer que les systèmes de chaque collectivité sont compatibles entre eux. Enfin, la gestion de la sécurité et de la confidentialité des données collectées par les logiciels et par les dispositifs IoT est une préoccupation majeure, nécessitant des mesures de protection robustes pour éviter toute compromission.

Pour surmonter ces problématiques, il est essentiel de mettre en place une structure de gouvernance solide, définissant clairement les rôles et les responsabilités de chaque collectivité participante. L'adoption de standards et de protocoles communs pour la gestion des données et des communications IoT est également cruciale pour garantir l'interopérabilité et la compatibilité des systèmes. De plus, il est nécessaire d'investir dans des solutions de sécurité avancées pour protéger les données sensibles et assurer la confidentialité des informations échangées. La formation continue des équipes techniques et la sensibilisation des parties prenantes à la sécurité des données sont également des éléments clés pour garantir le succès de la mutualisation.

La mutualisation de tels outils entre collectivités territoriales offre de nombreux avantages, notamment en termes d'économies, d'amélioration de la gestion des ressources et des services publics, et de renforcement de la **collaboration intercommunale**. Bien que des défis existent, une approche structurée et bien planifiée permet de les surmonter et de maximiser les bénéfices. En adoptant cette stratégie, les collectivités peuvent non seulement optimiser leur gestion territoriale, mais aussi contribuer au développement durable et à l'innovation technologique.

Il est important également de signaler que la communauté de communes Sud Roussillon dispose déjà de ces outils fonctionnels dans ses services.

Enfin, cette mutualisation ne doit pas s'arrêter là et doit accompagner les actions de transformation numérique du territoire pour fluidifier les process et rendre l'action publique plus souple et réactive, définir des communs numériques souverains, durables et sécurisés pour les acteurs institutionnels du territoire.

➔ ***OBJECTIF***

- Relancer la mutualisation du SIG mutualisé avec les communes membres
- Établir une discussion intercommunale sur les capacités d'ouverture de notre réseau LORA privé

ENJEU N°3 – AXE 2 : Téléphonie sur IP

Les tendances montrent des nouvelles solutions de communication sont devenus essentielle pour les entreprises modernes, amenant **flexibilité, sécurité et des fonctionnalités avancées** pour répondre aux besoins croissants de mobilité et de collaboration à distance.

La VoIP (Voice over Internet Protocol), ou téléphonie sur IP, est une technologie qui permet de transmettre des communications vocales via Internet plutôt que par des lignes téléphoniques traditionnelles. Cette méthode de communication offre de nombreux avantages pour les entreprises, améliorant à la fois la productivité et l'efficacité.

L'un des principaux avantages de la VoIP est la réduction des coûts. Contrairement aux systèmes téléphoniques traditionnels, la VoIP utilise l'infrastructure Internet existante, ce qui élimine le besoin de lignes téléphoniques dédiées et permet de réaliser des économies importantes sur les appels, notamment les appels longue distance et internationaux. De plus, les coûts de maintenance sont généralement inférieurs, car le système repose sur des mises à jour logicielles plutôt que sur des équipements matériels coûteux.

La VoIP offre également une **flexibilité accrue**. Les employés peuvent passer et recevoir des appels depuis n'importe où dans le monde, à condition d'avoir une connexion Internet stable. Cela facilite le travail à distance et permet une meilleure mobilité des agents. Les fonctions avancées telles que la messagerie vocale, les transferts d'appels, les conférences téléphoniques, et l'intégration avec d'autres outils de communication et de collaboration, améliorent encore plus la productivité et la réactivité des équipes.

Un autre avantage majeur de la VoIP est **sa scalabilité**. Les entreprises peuvent facilement ajuster leur capacité de communication en fonction de leurs besoins, ajoutant ou supprimant des lignes et des extensions sans avoir à investir dans de nouveaux équipements. Cela est particulièrement bénéfique pour les entreprises en croissance ou celles qui connaissent des fluctuations saisonnières de leurs activités.

La qualité des appels est également améliorée grâce à la VoIP, surtout si elle est couplée à une connexion Internet de haute qualité disponible aujourd'hui à travers la fibre et les réseaux 5G. Les technologies de compression et de transmission avancées permettent de fournir une clarté vocale supérieure à celle des systèmes téléphoniques traditionnels.

Cependant, la mise en place de la VoIP peut présenter quelques problématiques. Par exemple, la qualité de service dépend fortement de la connexion Internet et de la bande passante disponible. Les pannes de courant ou les interruptions de service Internet peuvent également affecter la disponibilité des communications vocales. De plus, la VoIP nécessite des mesures de sécurité supplémentaires pour protéger contre les menaces telles que le piratage et les écoutes illégales.

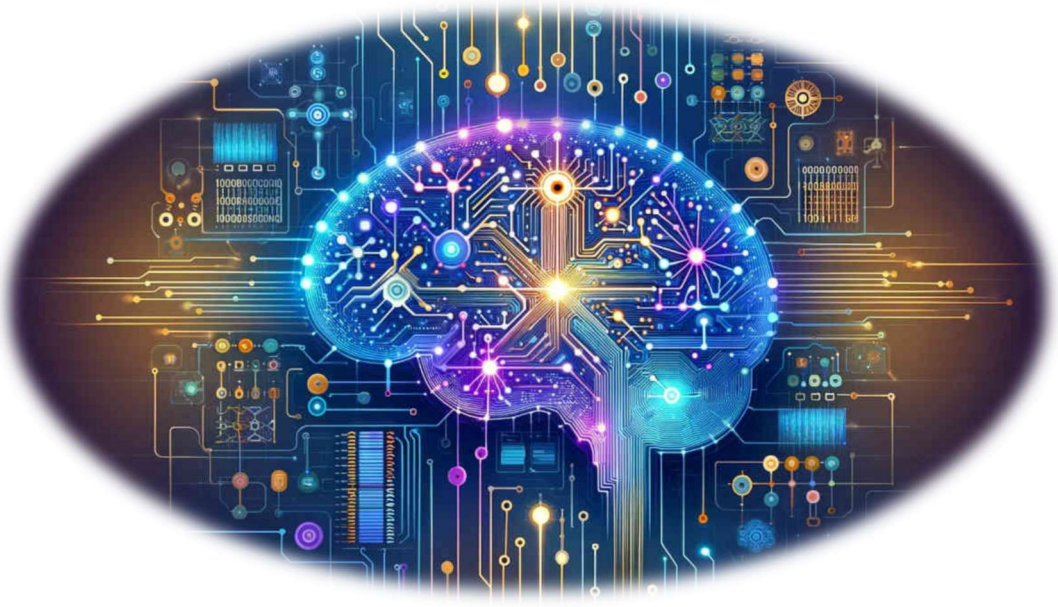
Pour surmonter ces problématiques, il est essentiel de choisir un fournisseur de services VoIP fiable et de garantir une connexion Internet robuste et stable. La mise en place de règles de qualité de service (QoS) peut aider à prioriser le trafic VoIP sur le réseau, assurant ainsi une qualité d'appel constante. Investir dans des solutions de sécurité avancées, telles que le chiffrement des communications et les pare-feu VoIP, est également crucial pour protéger les données sensibles. Enfin, la formation des employés sur l'utilisation des systèmes VoIP et les meilleures pratiques de sécurité peut contribuer à maximiser les bénéfices de cette technologie.

En conclusion, la VoIP offre de nombreux avantages pour les entreprises, notamment en termes de réduction des coûts, de flexibilité, de scalabilité et de qualité des appels. Bien que des défis existent, des solutions adaptées permettent de les surmonter et de tirer pleinement parti de cette technologie. En adoptant la VoIP, les entreprises peuvent améliorer leur **efficacité opérationnelle**, **favoriser la mobilité** de leurs employés et offrir une meilleure expérience de communication à leurs clients.

➔ ***OBJECTIF***

- Faire évoluer le système de téléphonie interne vers une technologie ToIP

ENJEU N°3 – AXE 3 : IA



Dans un monde de plus en plus digitalisé, les collectivités territoriales doivent s'adapter aux évolutions technologiques pour rester **pertinentes et efficaces**. Se tourner vers les métiers liés au numérique du futur est essentiel pour répondre aux attentes croissantes des citoyens et pour optimiser la gestion des services publics. Cette transformation numérique joue un rôle clé dans la modernisation des collectivités territoriales, en leur permettant de tirer parti des innovations technologiques pour améliorer leurs opérations et leurs services.

Les métiers du numérique du futur englobent une diversité de domaines, tels que l'intelligence artificielle, la cybersécurité, la gestion des données, le développement de logiciels, l'Internet des objets (IoT), et bien d'autres. En intégrant ces compétences, les collectivités peuvent moderniser leurs infrastructures et améliorer la qualité des services offerts. Par exemple, l'intelligence artificielle peut être utilisée pour optimiser la gestion des ressources, prévoir les besoins en infrastructure, et améliorer les services à la population et de sécurité publique. La cybersécurité est essentielle pour protéger les données sensibles et garantir la **continuité des services publics** en évitant les cyberattaques.

La transition vers les métiers numériques permet également de favoriser une meilleure gestion des ressources et une prise de décision plus éclairée. Les technologies de gestion des données, comme le Big Data et l'analytique, offrent aux collectivités la possibilité d'analyser de vastes quantités d'informations en temps réel. Cela permet d'identifier des tendances, de prévoir des besoins futurs, et d'optimiser les services en fonction des données recueillies. Par exemple, la gestion des déchets, la consommation d'énergie, et la qualité de l'air peuvent être surveillées et optimisées grâce à des capteurs IoT et des analyses de données.

Cette transition est aussi cruciale pour améliorer la relation entre les collectivités et les citoyens. Les outils numériques facilitent la communication et l'interaction avec les administrés, offrant des plateformes pour les retours d'expérience, les demandes de services, et la participation citoyenne. Les applications mobiles et les portails en ligne permettent aux citoyens d'accéder facilement aux informations et services publics, améliorant ainsi la satisfaction et l'engagement civique.

Cependant, cette transformation numérique présente des défis. Les collectivités doivent surmonter la résistance au changement et sensibiliser les employés à **l'importance des métiers numériques.** Les programmes de formation continue et de reconversion professionnelle sont essentiels pour doter les agents des compétences nécessaires. Il est aussi crucial d'allouer des **ressources adéquates** pour l'acquisition de technologies et la mise en place d'infrastructures numériques.

Pour réussir cette transition, les collectivités doivent adopter une stratégie claire et intégrée. Cela inclut l'identification des métiers numériques les plus pertinents, la création de partenariats avec des institutions éducatives et des entreprises technologiques, et la mise en œuvre de politiques favorisant l'innovation. En outre, la **promotion de la culture numérique** au sein de l'administration territoriale est essentielle pour garantir une adoption réussie et durable des nouvelles technologies.

En conclusion, se tourner vers les métiers du numérique du futur est indispensable pour les collectivités territoriales qui souhaitent rester compétitives, innovantes et efficaces. Cette transition permet non seulement d'améliorer la qualité des services publics, mais aussi de renforcer la résilience des collectivités face aux défis actuels et futurs. En adoptant une approche proactive et bien planifiée, les collectivités peuvent tirer pleinement parti des avantages offerts par les technologies numériques et contribuer à un développement durable et inclusif de leurs territoires.

➔ ***OBJECTIF***

- Faire évoluer les liens de la collectivité avec le numérique et s'ouvrir vers les nouveaux domaines

GLOSSAIRE

A

AGILE : méthode de gestion de projet qui prône une démarche collaborative, itérative et incrémentale. Elle est dite « agile », car elle permet de prendre en compte à la fois les besoins initiaux et ceux générés par les changements futurs

AMOA ou AMO : assistance à maîtrise d'ouvrage

ANSSI : Agence nationale de la sécurité des systèmes d'information

API : solution informatique qui permet à des applications de communiquer entre elles et de s'échanger mutuellement des services ou des données

B

BAN : Base adresse nationale, base de données ayant pour but de référencer l'intégralité des adresses du territoire français

Big Data : ressources d'informations dont les caractéristiques en termes de volume, de vélocité et de variété imposent l'utilisation de technologies et de méthodes analytiques particulières pour générer de la valeur

BIM : processus intelligent basé sur un modèle 3D qui offre aux professionnels de l'architecture, ingénierie et construction les informations et les outils nécessaires pour planifier, concevoir, construire et gérer plus efficacement des bâtiments et des infrastructures

Briques techniques : ensemble d'outils ayant des fonctions très précises (authentification par exemple), communiquant avec les autres afin de créer un ensemble cohérent répondant à une problématique métier, sécurité…

Byod ou Bring your own device : utilisation de matériel informatique personnel à des fins professionnelles moyennant en général l'ajout d'un logiciel de contrôle par l'entreprise

C

Chatbot : outil permettant à un utilisateur de demander des renseignements auprès d'un robot en s'exprimant en langage courant

Cloud : recouvre l'ensemble des solutions de stockage distant. En clair, vos données, au lieu d'être stockées sur vos disques durs ou mémoires, sont disponibles sur des serveurs distants et accessibles par internet

CNFPT ou Centre national de la fonction publique territoriale : établissement public paritaire déconcentré doté de trois missions principales : la formation, l'observation et l'organisation des concours des cadres d'emplois A+

Collaboratif : qui permet de travail ensemble (partage de documents ...)

Connecteurs : lien entre différents outils permettant la transmission ou l'enrichissement d'informations

CPOM ou Contrat pluriannuel d'objectifs et de moyens : engagement pluriannuel sur des objectifs d'activité et des moyens d'action

CSIRT ou Computer Security Incident Response Team : centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises ou aux administrations, mais dont les informations sont généralement accessibles à tous

Cyber'Occ : portail de la cybersécurité en Occitanie, créé par le Conseil régional d'Occitanie et son agence de développement économique Ad'Occ. Il centralise un ensemble d'informations liées à la cybersécurité (métiers, aides, documentation, alertes...)

D

Data : données

Data analyst : il met en œuvre des outils informatiques, techniques et méthodes statistiques pour permettre d'organiser, synthétiser et traduire efficacement des données. Bac + 5 en informatique

Data scientist : il exploite, analyse et évalue la richesse, de données structurées ou non pour établir des scénarios permettant de comprendre et d'anticiper de futurs levier métiers ou opérationnels pour l'entreprise. Bac + 5 École d'ingénieur, commerce, statistiques

Datavisualisation : représentation graphique de données statistiques

Décisionnel : outils dont l'objectif est l'aide à la décision (indicateurs, tableaux de bord...)

Design de service : façon de concevoir un service centré sur l'utilisateur de manière à ce qu'il soit utile et facilement utilisable

DEVOPS : pratique technique visant à l'unification du développement logiciel (dev) et de l'administration des infrastructures informatiques (ops), notamment l'administration système. En général, demande également un rapprochement des équipes opérationnelles et des développeurs pour une plus grande réactivité et une réponse aux besoins plus précise

DPO : Data protector officer, traduit en français par Délégué à la protection des données. Personne chargée, dans le cadre du RGPD, de veiller à la protection des données personnelles au sein des entreprises, collectivités...

DUA ou Durée d'utilité administrative : durée pendant laquelle les documents, données ou informations archivées doivent être conservés et gardés en état d'être consultés et utilisés, soit par ceux qui les ont produits, soit par des services d'archives

DSI : Direction des systèmes d'information

DOCK : dispositif informatique conçu pour accueillir, à la manière d'un socle, un appareil informatique portable en le branchant, lui offrant ainsi du courant électrique. Dans le cas d'un ordinateur portable, elle permet de l'utiliser de façon semblable à un ordinateur de bureau

E

EDR ou Endpoint detection and response :

Catégorie d'outils et de solutions qui mettent l'accent sur la détection d'activités suspectes directement sur les hôtes du système d'information (ordinateurs, serveurs…). Combiné avec un moteur basé sur de l'intelligence artificielle, le logiciel EDR est très réactif dans la détection et l'arrêt de menaces

EMM ou Entreprise mobile management :

Outil de gestion de flotte de téléphones portables

E-inclusion : concept de donner l'accès et la compréhension du numérique au plus grand nombre

Entrepôt (de données) : zone de stockage d'un maximum d'informations, qui pourront être consultées par différents logiciels afin de les exploiter au mieux

EPCI : Etablissement public de coopération Intercommunale

ETP : équivalent temps plein

F

Firewall : logiciel et/ou matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique

G

GED ou Gestion électronique des documents : procédé informatisé visant à définir, concevoir, produire, organiser, diffuser et gérer des informations et des documents papier ou des documents électroniques au sein d'une organisation

Géomaticien : à la croisée de la géographie et de l'informatique, le géomaticien exploite les données pour modéliser le territoire. Il intervient dans tous les secteurs qui ont besoin d'analyse spatiale : urbanisme, environnement, transport, énergie, marketing…

GMP : logiciel de suivi des mouvements de personnel

GPEC : Gestion prévisionnelle des emplois et des compétences

Green IT : a pour objectif de réduire l'empreinte carbone générée par les systèmes d'information tout en permettant de réaliser des économies

I

IA : intelligence artificielle

IoT ou Internet of things : Internet des objets. Regroupe les objets et équipements connectés (à Internet) et les technologies qui s'y rapportent

IIoT ou Industrial internet of things : Internet industriel des objets ou IOT dans l'industrie

Interopérable : le fait d'avoir des outils capables de communiquer entre eux (ayant des interfaces par exemple)

Itrust : éditeur de solutions de cybersécurité

L

Label ExpertCyber : label destiné à valoriser les professionnels en sécurité numérique ayant démontré un niveau d'expertise technique et de transparence dans les domaines de l'assistance et de l'accompagnement de leurs clients. Le label ExpertCyber est issu d'une collaboration entre cybermalveillance.gouv.fr, ses membres et AFNOR Certification

Lean : appliqué aux systèmes d'information, le lean est l'élimination du superflu afin de rendre leur gestion plus flexible. Le Lean IT amène notamment l'utilisation d'une démarche structurée dans le recueil des besoins, l'amélioration continue…

LIDAR : méthode de télédétection et de télémétrie semblable au radar, mais qui émet des impulsions de lumière infrarouge au lieu d'ondes radio, puis en mesure le temps de retour après avoir été réfléchies sur des objets à proximité

Logiciel métier : outil dont l'objectif est de répondre aux besoins d'un métier particulier

Loi « numérique » : cf. loi Lemaire ci-dessous

Loi « Lemaire » : la loi pour une République numérique (abr. Loi numérique) est une loi française initialement proposée par la secrétaire d'État au numérique Axelle Lemaire et promulguée le 7 octobre 2016. L'objectif est double : « donner une longueur d'avance à la France dans le domaine du numérique en favorisant une politique d'ouverture des données et des connaissances » et « adopter une approche progressiste du numérique, qui s'appuie sur les individus, pour renforcer leur pouvoir d'agir et leurs droits dans le monde numérique ». Pour ce faire, la loi s'organise autour de trois axes : la circulation des données et du savoir, la protection des individus dans la société du numérique et l'accès au numérique pour tous

Loi « NOTRe » : la loi n° 2015-991 du 7 août 2015 portant nouvelle organisation territoriale de la République, fait partie de l'acte III de la décentralisation mis en œuvre sous la présidence de François Hollande et vise notamment à renforcer les compétences des Régions et des Établissements publics de coopération intercommunale

M

Mindmap : carte mentale, représentation graphique d'une arborescence d'idées

Monitoring : suivi et affichage de statistiques en direct (consommation électrique ou volume de données occupé par exemple)

O

Occitanie Data : association de préfiguration d'un pôle d'économie de la donnée (entreprises, institutions publiques, collectivités territoriales, acteurs académiques). Occitanie Data consiste à construire un cadre de confiance, éthique et souverain, destiné à permettre aux acteurs de partager et de croiser leurs données tout en respectant les intérêts des individus et des propriétaires des données

On Premise : installation en interne

Opendata : Ouverture de données, obligation règlementaire de diffuser les données non sensibles des collectivités à des fins de transparence et de possible réutilisation par toute personne morale ou physique

P

PCA ou Plan de continuité d'activité : plan regroupant un ensemble de mesures ayant pour objectif de poursuivre au mieux l'activité en cas de problème majeur. Pour cela, il présente de la sécurisation (redondance par exemple), des moyens de contournements ou une priorisation

PCRS ou Plan de corps de rue simplifié : représentation graphique permettant d'améliorer la précision du repérage des réseaux et fiabiliser l'échange d'informations entre les acteurs concernés (collectivités, exploitants de réseaux, maîtres d'ouvrages et entreprises de travaux)

Phishing ou Hameçonnage : technique frauduleuse utilisée pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité, consistant notamment à envoyer des messages en se faisant notamment passer pour une organisation légitime, mais contenant un lien vers un site malveillant

POC ou Proof of concept : prototype d'expérimentation d'un logiciel sur un périmètre restreint dont l'objectif est de montrer sa bonne adéquation avec les besoins. L'évaluation du POC permet d'éclairer la décision de généraliser ou non la solution

PRA ou Plan de reprise d'activité : ensemble de mesures permettant de reprendre l'activité au plus vite et au mieux suite à un incident majeur ayant occasionné une interruption (ex : mise en place de sauvegardes sécurisées)

Prédictif : outil d'aide à la décision simulant une situation future en fonction de données, tendances ou de paramètres (ex : accroissement de la population sur un territoire ou estimation des recettes en cas de facturation des déchets au poids)

Programme TNT : en 2021, le programme Transformation numérique des territoires a pris le relais du programme de Développement concerté de l'administration numérique territoriale (DCANT 2018-2020). Véritable feuille de route de la transformation numérique des territoires, ce programme a été entièrement co-écrit par les associations d'élus et les représentants des

services de l'État autour d'une ambition partagée : construire ensemble des services publics numériques fluides et performants

Q

QQOQCCP : le QQOQCCP (Quoi, Qui, Où, Quand, Comment, Combien, Pourquoi), appelé aussi méthode du questionnement est un outil d'aide à la résolution de problèmes comportant une liste quasi exhaustive d'informations sur la situation

QuickCapture : module du SIG permettant la collecte d'observations sur le terrain

R

Ransomwares : logiciels malveillants ayant pour objectif de demander une rançon à leurs victimes

RGPD ou Règlement général de protection des Données : règlement européen de 2016 (entré en vigueur en 2018), qui constitue le texte de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne

RGS ou Référentiel général de sécurité : cadre réglementaire qui contraint les autorités administratives à garantir la sécurité de leurs systèmes d'information en charge de la mise en œuvre de téléservices et des échanges électroniques entre l'administration et les usagers

RSSI ou Responsable de la sécurité des systèmes d'information : personne qui a la charge de la rédaction de la PSSI, de sa mise en application et de son respect

S

SaaS ou Software as a service : modèle de distribution de logiciel au sein duquel un fournisseur tiers héberge les applications et les rend disponibles pour ses clients par l'intermédiaire d'internet

SI : Système(s) d'information

SIG : Système d'information géographique

Smart-city : « ville intelligente ». Il s'agit d'améliorer la qualité de vie des citadins en rendant la ville plus adaptative et efficace, à l'aide de nouvelles technologies qui s'appuient sur un écosystème d'objets et de services. Le périmètre couvrant ce nouveau mode de gestion des villes inclut notamment : infrastructures publiques (bâtiments, mobiliers urbains, domotique, etc.), réseaux (eau, électricité, gaz, télécoms), transports (transports publics, routes et voitures intelligentes, covoiturage, mobilités dites douces - à vélo, à pied, etc.), les e-services et e-administrations

Smart mobility ou mobilité intelligente : désigne les services de transports qui intègrent les solutions des technologies de l'information et de la communication pour améliorer la qualité du service rendu à l'usager

SO ou Système ouvert : système informatique interopérable entre différents fournisseurs et normes, permettant une modularité entre les matériels et les logiciels

Softphone : logiciel utilisé pour faire de la téléphonie par Internet depuis un ordinateur plutôt qu'un téléphone

Spam : courriel (mail) indésirable (ou pourriel), communication électronique non sollicitée. Il s'agit en général d'envois en grande quantité de courriels effectués à des fins publicitaires

SWOT ou Strengths (forces)**, Weaknesses** (faiblesses)**, Opportunities** (opportunités)**, Threats** (menaces) **:** technique d'analyse visant à préciser les objectifs d'un projet et à identifier les facteurs internes et externes favorables et défavorables à la réalisation de ces objectifs

T

Téléservices : services en ligne permettant à l'utilisateur de réaliser diverses opérations (paiement, inscription à la cantine, etc.)

Ticketing (outil de) : outil de suivi de demandes permettant à un utilisateur d'adresser une demande qui sera dirigée vers les bonnes personnes, de suivre son traitement et d'afficher des statistiques liées

To : téraoctet