



PARTENAIRE PRIVILÉGIÉ
DES COMMUNES POUR
UNE CYBERSÉCURITÉ DURABLE

**Wéi digital resilient ass
de Gemengesecteur ?**

BISSEN - 7 MAI 2024



SOMMAIRE

- 01** **Le Mot du Président**
Philippe Meyers
- 02** **Les missions des Communes**
Philippe Mathieu
- 03** **Notre rôle de fournisseur de services**
Philippe Mathieu
- 04** **Notre partenariat avec les Communes**
Philippe Mathieu

01 LE MOT DU PRÉSIDENT



Philippe Meyers

Président du SIGI
Echevin Dippach

02 LES MISSIONS DES COMMUNES

Le SIGI supporte les missions des Communes en proposant un panel de solutions couvrant leurs besoins métiers

Missions Obligatoires



Administration



Aménagement



Entretien



Alimentation en
Eau Potable



Evacuation des
Eaux Usées



Enseignement



Gestion des
Déchets



Ordre et Sécurité



Hygiène et
Salubrité Publique



Protection Civile



Tenue Registre
Etat Civil et Population



Assistance Sociale

Missions Non-Obligatoires



Culture et Loisirs



Social, Familial : crèches,
maisons relais, retraites



Transport



Sport



Tourisme



Santé Publique



Environnement

Nos communes et administrations



99 Communes
membres



537 Crèches et
maisons relais



60 Syndicats



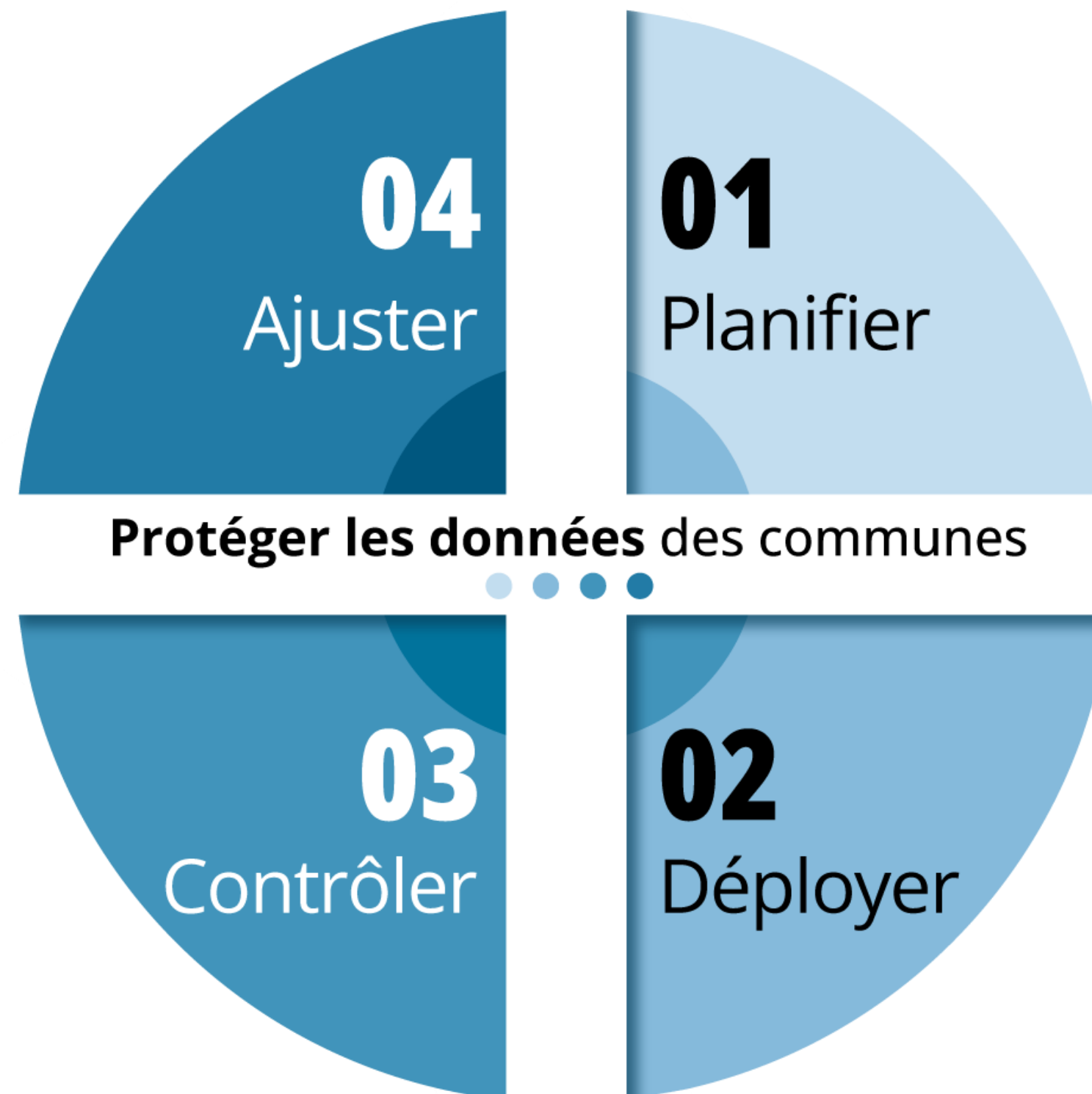
30 Offices
sociaux



**Partenaires
Membres
au total**

03 NOTRE RÔLE DE FOURNISSEUR DE SERVICES

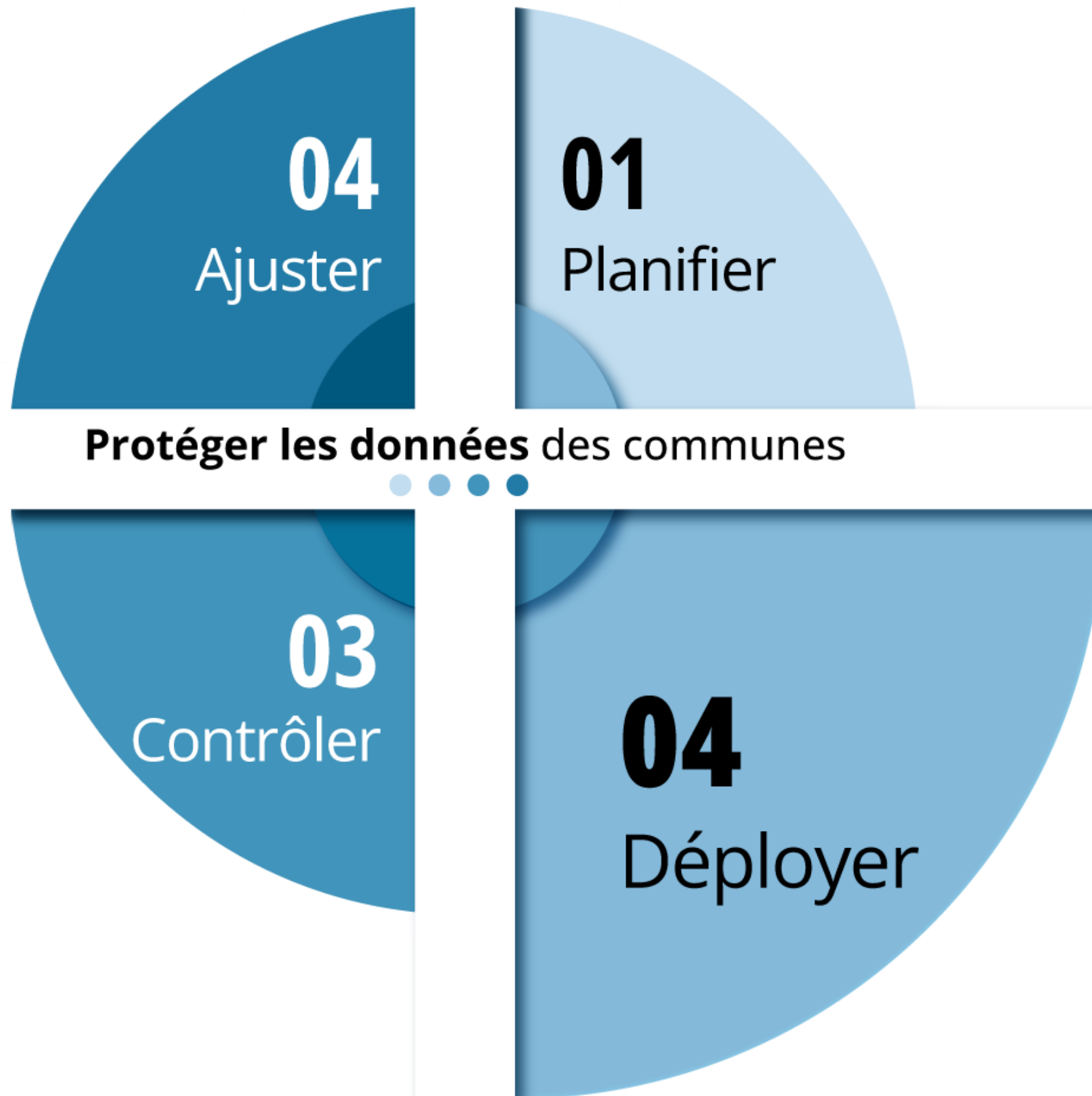
Le SIGI héberge l'ensemble des données des Communes.





Planifier

- Définir une **politique et un objectif de sécurité** avec les rôles et responsabilités de chacun
- **Analyser et évaluer** les risques
- Définir **une équipe** en charge de la sécurité
- Mettre en place un **plan d'action** permettant de :
 - **Mitiger** le risque
 - **Accepter** le risque
 - **Éliminer** le risque
 - **Transférer** le risque
- Assurer une **veille légale** et sa **conformité** (ex : NIS2)
- S'appuyer sur des **frameworks de type ISO27001** pour les normes et **ISO27005** pour l'analyse de risque



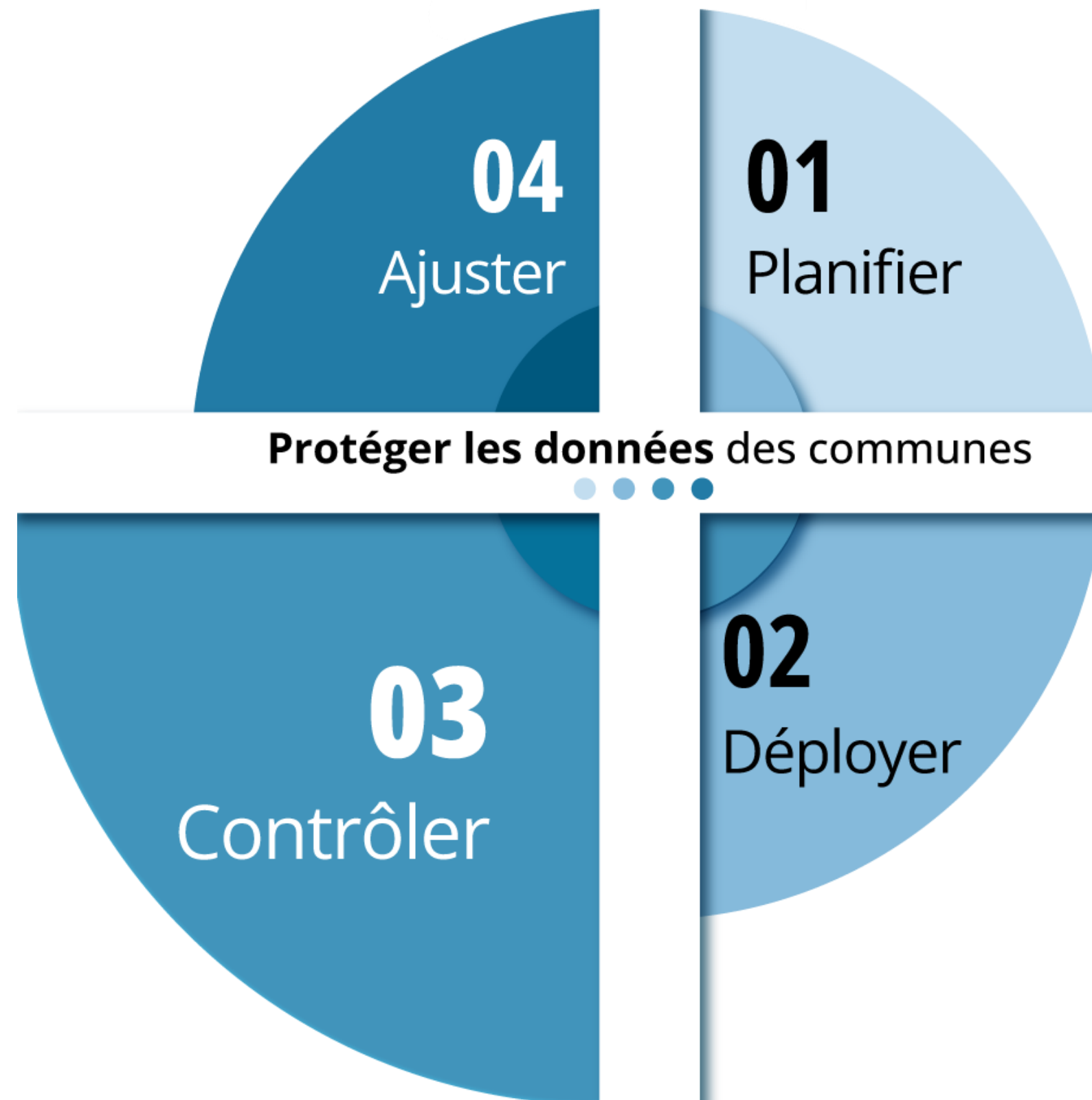
Déployer

Déployer et implémenter des contrôles opérationnels :

- **Maintenir un inventaire** de ses actifs (matériels, logiciels)
- **Sécuriser ses actifs** (*firewall, hardening*, bonnes pratiques utilisateurs, gestion des vulnérabilités)
- **Gérer les comptes** et les accès aux différents actifs (logs, authentification multi-facteur, processus de révocation)
- Maintenir des solutions **anti-malware** sur l'ensemble des actifs
- Assurer une **politique de backup** en ligne avec la criticité des données
- **Sécuriser** l'architecture réseau
- Identifier les fournisseurs de services
- Centraliser les événements de sécurité
- Mettre en place une **procédure de gestion d'incident**

Sensibiliser le personnel :

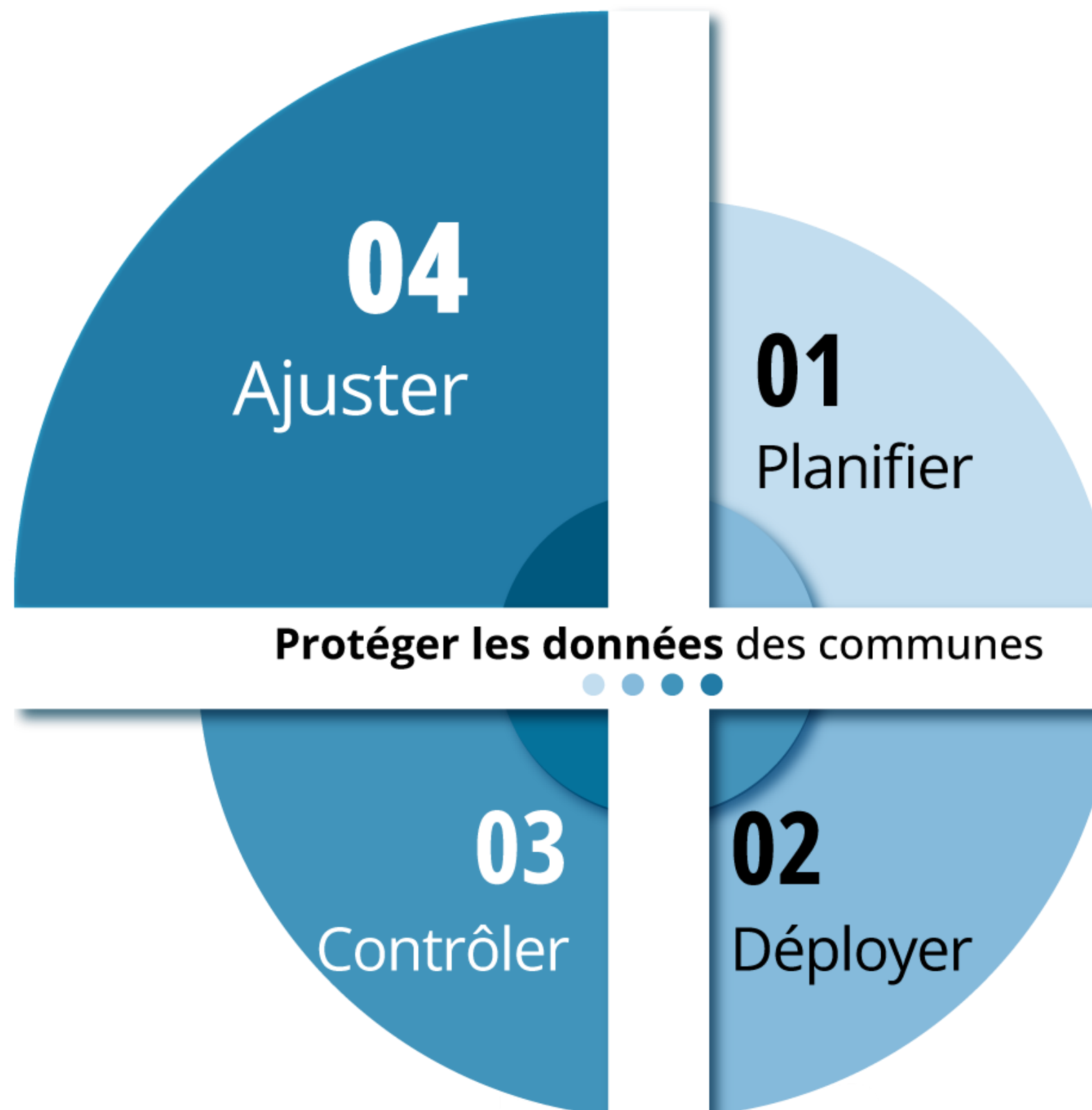
- Campagnes de **formations / sensibilisation**
- Campagnes de **tests**



Contrôler

Assurer une vue 360 degrés des contrôles opérationnels:

- Vérifier hebdomadairement les actifs en lien avec **l'inventaire**
- Vérifier les comptes **inactifs** et les **désactiver** (systèmes, applicatifs)
- Monitorer les **évènements** et **incidents** de sécurité
- Monitorer le temps de réaction sur un incident de sécurité afin d'en limiter l'impact
- Lancer régulièrement des **scans de vulnérabilités** sur les actifs exposés
- Lancer régulièrement des **tests de restore** des données
- Lancer régulièrement des **tests d'intrusions** (physiques, réseau, applicatifs)
- Maintenir des **tableaux de bord** automatisés (ex: % de PC ayant les dernières mises à jour)



Ajuster

- **Analyser l'ensemble des anomalies** remontées du terrain ou dans la phase de contrôle
- **Prioriser et planifier des remédiations** sur base de la criticité de l'anomalie et de son impact métier
- Adapter les **politiques de sécurité**, les procédures de sécurité avec les menaces émergentes et les évolutions d'exigences du métier
- Travailler à **automatiser** au maximum la **détection d'évènement** de sécurité ainsi que leur reporting
- Sur base des écarts de sécurité observés, fournir des **formations** et des **campagnes de sensibilisation** adaptées
- Être proche des experts locaux afin de suivre les tendances en matière de Cybersécurité (**LHC, CIRCLE, ILR, HCPN**)

04 NOTRE PARTENARIAT AVEC LES COMMUNES

Le SIGI agit comme un partenaire au travers de différents canaux

01

Partage des expériences communales

Nous échangeons à travers la **commission micro-informatique**, les **forums** et nous sensibilisons nos partenaires

02

Facilitateur pour NIS2

Nous sommes **facilitateurs** pour l'implémentation de l'application de la **future Directive NIS2**

03

Fourniture d'un accès privilégié

Nous **facilitons l'accès** aux partenaires importants dans le domaine de la Cybersécurité

04

Retour d'expériences

Nous fournissons des **résultats d'analyse de risques**

05

Clarification des responsabilités

Nous informons les communes des **rôles de chacun** en termes de cybersécurité

Ensemble, renforçons la résilience numérique de nos communes pour garantir une cybersécurité durable et efficace face aux défis de demain