Green communications

La résilience des infrastructures numériques pour les données critiques

Mariam Maréchal

Exemple concret

La résilience en trois points

La résilience est un processus cyclique,

La résilience repose sur une architecture décentralisée et interopérable (Cloud et Edge),

La résilience est un projet de gouvernance.

Définissons résilience, infrastructure numérique et données critiques.

Définissons les termes

Infrastructure numérique

Ensemble des ressources matérielles, logicielles, réseaux et services qui permettent le fonctionnement numérique d'une organisation.

Données critiques

Données dont la perte ou l'indisponibilité entraîne un impact majeur.

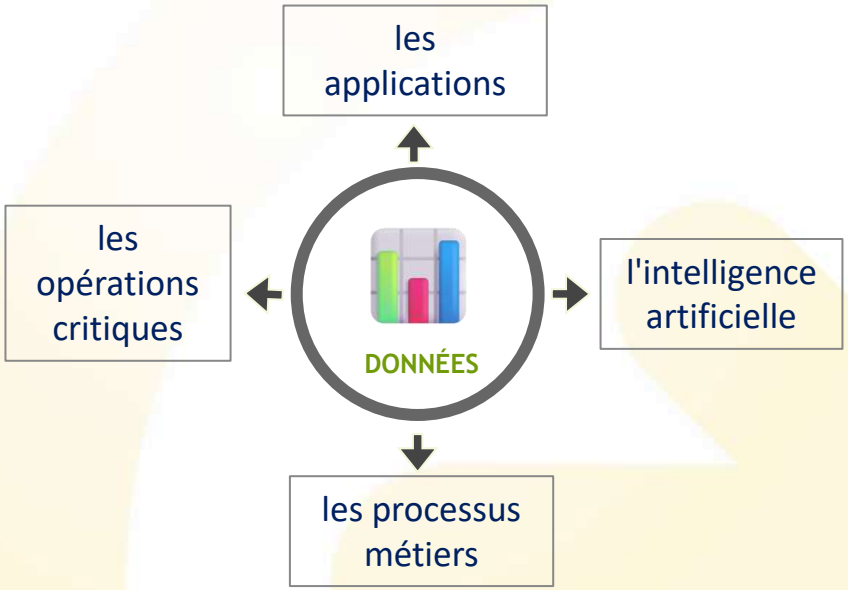
La résilience des données critiques

C'est la capacité d'une organisation à garantir la disponibilité, l'accessibilité, l'intégrité et la récupérabilité de ses données critiques, même quand un incident majeur affecte son infrastructure numérique.

Les données critiques n'ont de valeur que si elles sont accessibles et exploitables.

Des données vitales

Les données alimentent :



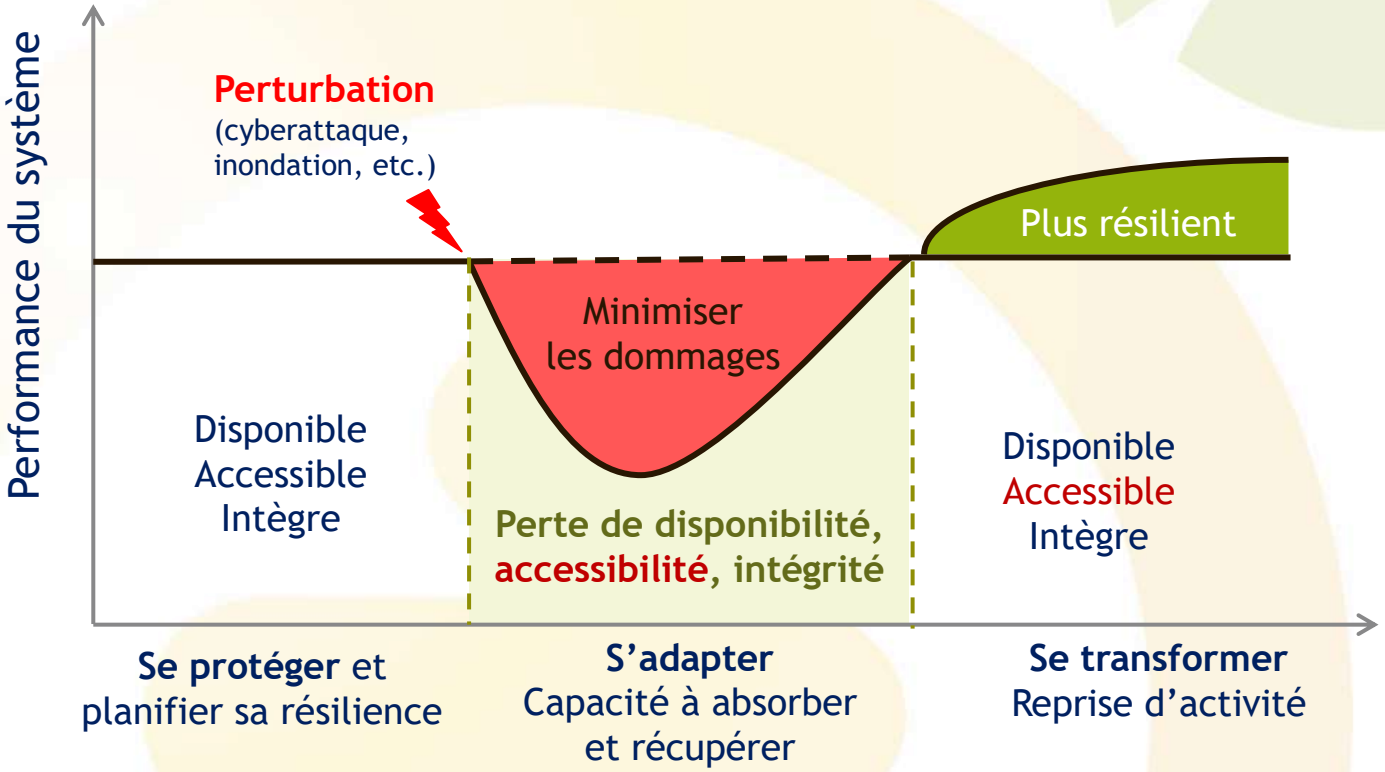
Les données sont au cœur de la transformation numérique.

Elles conditionnent la prise de décision, l'innovation et la continuité des activités.

Une donnée indisponible, inaccessible, altérée ou perdue peut paralyser une organisation entière.

Si les données sont le nouveau carburant de l'économie numérique, comment garantir qu'elles restent disponibles, accessibles, fiables et récupérables malgré les incidents majeurs ?

La résilience : un processus cyclique



Une organisation résiliente n'est pas celle qui évite tous les incidents, mais celle qui continue à fonctionner malgré tout.

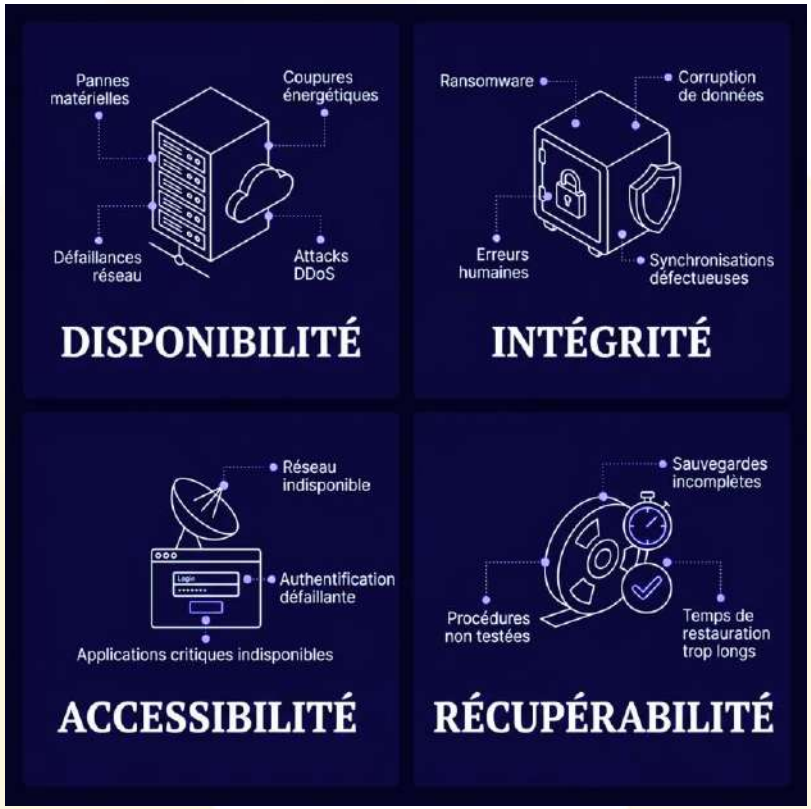
Les 4 objectifs de la résilience

Propriété	Question
Récupérabilité > Disponibilité	Peut-on les restaurer rapidement après un incident ?
Accessibilité	Les utilisateurs autorisés peuvent-ils y accéder ?
Intégrité	Les données sont-elles fiables et non altérées ?

Une défaillance sur une seule de ces dimensions suffit à compromettre l'activité.

Pourquoi est-ce si difficile ?

Garantir simultanément ces quatre propriétés implique de répondre à des risques différents :



Données indisponibles
→ arrêt d'activité

Données altérées ou perdues
→ mauvaises décisions

Données perdues
→ pertes irréversibles

Données inaccessibles
→ paralysie opérationnelle

Architecture de résilience

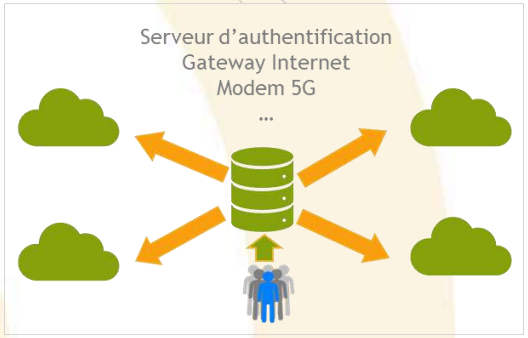
1) Retirer les maillons faibles

Connexion réseau

2) Relocaliser

Cloud

- Données centralisées
- Redondance
- Scalabilité,
- Mutualisation etc.



Organisation

- rapproche les services du terrain,
- conserve l'autonomie locale,
- réduit la dépendance aux réseaux,
- la distribution améliore la continuité.

EDGE
(local)
- Services critiques

EDGE
(local)
- Services critiques

La meilleure résilience ne se fait qu'avec des services totalement distribués !

Si le centre (Cloud) devient indisponible, le terrain (Edge) doit continuer à fonctionner.

Maintenir l'accès aux données

Pyramide de résilience des données critiques

La résilience vise un objectif plus ambitieux : permettre à l'organisation de poursuivre sa mission malgré la dégradation de son environnement numérique.

Projet de gouvernance

Continuer malgré l'incident passe par

La coordination interne : l'enjeu actuel est de passer d'un empilement de solutions techniques à un plan de coordination global qui prend en compte le sinistre avant, pendant et après son apparition.

La transversalité : un plan de résilience efficace doit faire collaborer la DSI, les directions métiers, le juridique et les RH.

Le jour « J » un écosystème d'acteurs pour accéder aux données critiques permettant de continuer et de reprendre ses activités rapidement fait la différence.

Notre résilience dépend de l'écosystème dans lequel on évolue. La gouvernance est interne et externe.

Projet de gouvernance

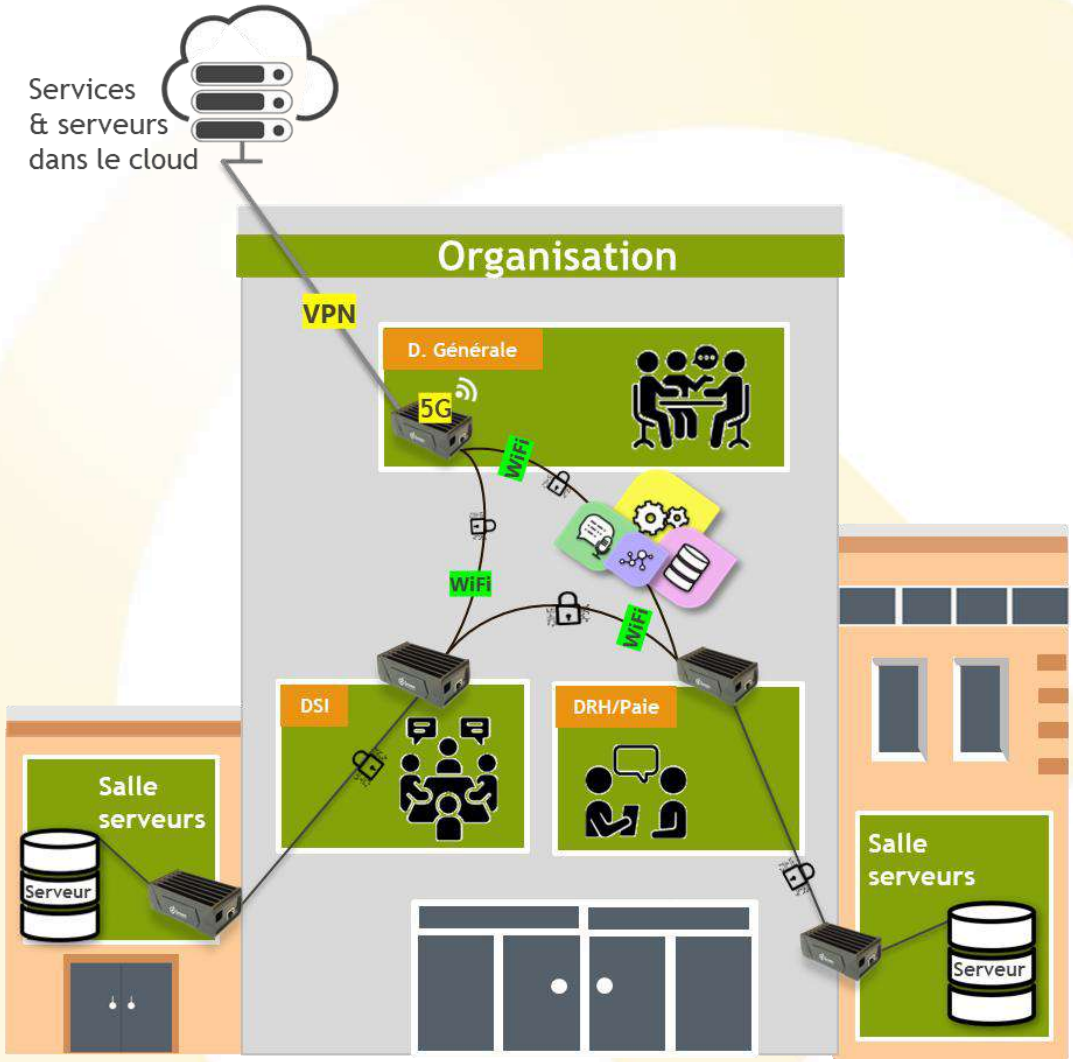
Continuer malgré l'incident grâce à ces piliers

Aucun pilier ne suffit seul.

1. **Technologie**
   Disponibilité – Récupérabilité
2. **Cybersécurité**
   Intégrité – Disponibilité
3. **Humain & organisation**
   Exercise - Réaction – Procédures
4. **Gouvernance**
   Stratégie – Arbitrages – Pilotage
5. **Écosystème**
   Fournisseurs – Experts - Dépendances

Exemple concret

Un exemple concret



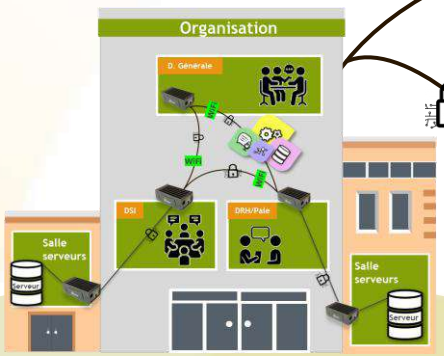
Une solution permettant de rendre disponibles les données critiques d'une organisation en cas de sinistre sur le même site.

Un exemple concret

Des sites autonomes

Synchronisation des services

Site 1



5G

VPN

Site 3

Connexion de plusieurs sites

Site 2

Centre de commandement :
site référent, cellule de crise.

Une responsabilité collective

La résilience est une responsabilité collective

Objectif ultime : ***permettre aux organisations d'avoir accès a leurs données critiques quel que soit le sinistre subi.***

Green Communications, votre partenaire en résilience

contact@green-communications.fr

https://www.green-communications.fr

Mariam Maréchal

Experte en Cyber Résilience et
Responsable Commerciale et Innovation