Digital113

Cluster numérique Sud de France

DIGITAL 113, LE COLLECTIF POUR **PROPULSER LE NUMÉRIQUE D'OCCITANIE**

au-delà des frontières

SOUVERAINETÉ ET RÉSILIENCE NUMÉRIQUE :

enjeux et opportunités pour les entreprises de la filière numérique

WWW.DIGITAL113.FR

PRÉFET DE LA RÉGION OCCITANIE

Direction régionale de l'économie, de l'emploi, du travail et des solidarités (DREETS)

toulouse métropole

montpellier méditerranée métropole

SICOVAL

SERVICE CIVIQUE

ayming

Groupama

la direction

Souveraineté et Résilience Numérique : enjeux et opportunités pour les entreprises de la filière numérique

Introduction 3

Le Manifeste des entreprises du numérique d'Occitanie
Dix engagements pour la résilience numérique de la filière 5

2026-2030 - Trois chocs qui transforment le numérique en profondeur 5

Les chocs géopolitiques et la recomposition des blocs de puissance du numérique 6

De la dépendance technologique au risque financier 6

La géopolitique de l'octet et du silicium : quand le numérique devient une arme d'État 6

De la guerre économique à la guerre hybride 7

La cybermenace s'industrialise 8

L'Europe, du risque systémique à l'émancipation 8

Le temps de l'ambition européenne 9

L'intelligence artificielle agentique et robotique, la révolution industrielle de notre filière 10

L'agentique, grand accélérateur du monde du numérique 10

David peut-il devenir Goliath ? 11

La filière numérique va vivre sa propre transformation numérique 11

L'atteinte des limites planétaires et l'accélération du dérèglement climatique 11

Le numérique, une industrie lourde comme les autres 12

L'émergence de conflits d'usage 12

L'audit flash résilience Numérique : dix questions, cinq minutes 13

Notre proposition : Six chantiers "Résilience Numérique" pour la filière numérique Occitane 14

Chantier 1 - Croissance et stratégie : des chocs créateurs d'opportunités 14

Chantier 2 - Infrastructures et supply-chain: cartographier et repenser ses dépendances 16

Chantier 3 - Se préparer à l'industrialisation de la cybermenace 18

Chantier 4 - Numérique Responsable et Durable : faire de la sobriété une dimension clé de la résilience numérique 20

Chantier 5 - RH, RSE & Marque Employeur : souveraineté, résilience et soutien aux solutions européennes comme attracteurs de talents 22

Chantier 6 - Usages, data et IA : déployer de la valeur garder la main sur l'inférence 24

Conclusion 25

Annexes 26

Annexe 1 - Qui fait quoi en Occitanie quant à la souveraineté et la résilience numérique ? 26

Annexe 2 - Contributeurs 26

Annexe 2 - Grille IRN 26

Annexe 3 – Glossaire 27

Annexe 4 - Bibliographie 28

Introduction

Le cluster Digital 113 fédère aujourd'hui plus de 300 entreprises du numérique et 15 000 salariés en Occitanie, des éditeurs aux entreprises de services du numérique, des plus anciennes aux startups. Cinq axes structurent son action : innovation et transformation, business et croissance, stratégie et financement, recrutement et diversité, international. Le cluster porte également depuis 12 ans un engagement fort pour le numérique responsable, dont " The Green IT Day" est l'événement emblématique: son édition 2026 posait la question : "Robustesse, résilience… Le numérique tient-il le choc ? " Trois valeurs guident son action : l'éthique, le partage et l'engagement. Pour agir, il s'appuie sur le collectif, en particulier sur les Factory, groupes de travail animés par ses adhérents.

La filière du numérique en Occitanie représente plus de 131 000 emplois[1], ce qui fait de la région Occitanie la première de France, hors Île-de-France, pour la part du numérique dans l'emploi marchand. Elle accompagne des industries exigeantes telles que l'aéronautique, la défense et le spatial, civils comme militaires, la santé, l'agroalimentaire, ainsi que des domaines d'excellence : la cybersécurité, l'intelligence artificielle, l'IoT et la microélectronique, l'édition de logiciels, le numérique responsable. Ses entreprises manipulent des données sensibles, affrontent les cybermenaces depuis des décennies et exportent sur tous les continents. Le spatial toulousain traite des volumes d'observation de la Terre depuis quarante ans. La santé occitane manipule des données parmi les plus protégées du droit européen, et l'aéronautique certifie ses systèmes embarqués sous les régimes les plus stricts. À cela s'ajoute la densité des services : avec ses grandes ESN et son tissu de sociétés de conseil et d'ingénierie, la région est le troisième pôle numérique français.

C'est donc une filière habituée à innover, construire, prouver, documenter, auditer et résister aux différents chocs du monde. Pourtant, trois chocs transformatifs simultanés vont, selon nous, modifier profondément le marché du numérique dans la décennie à venir. Ce document a pour objectif de les identifier et d'aider notre filière à les anticiper et à en tirer parti.

Face à ces chocs, deux notions reviennent : la souveraineté et la résilience numérique.

La souveraineté numérique est une notion d'ordre macroéconomique et régalien. Elle relève de la puissance et de l'autorité exclusive de l'État. Définie comme la capacité d'une nation à réguler l'espace numérique et à y agir de manière autonome, elle vise à préserver la sécurité nationale, à protéger les données sensibles et à prémunir les acteurs locaux contre l'ingérence ou les lois extraterritoriales étrangères. Pour une entreprise, elle prend la forme d'une exigence réglementaire dictée par l'État, qui s'appuie sur des normes et des labels de confiance stricts. Face à l'exposition juridique extraterritoriale, la souveraineté s'apprécie de manière binaire : une organisation bénéficie d'une protection juridique et technique étanche, ou elle y reste exposée.

La résilience numérique s'inscrit au niveau microéconomique. Elle relève de la discipline d'action et de la gestion des risques de chaque entreprise. Définie comme la capacité d'une organisation à « maîtriser de manière réaliste son avenir numérique » pour sécuriser sa continuité d'activité et sa compétitivité, elle n'exige pas l'autarcie technologique absolue. Une entreprise peut renforcer sa résilience numérique en achetant américain, chinois ou européen, à condition de connaître et maîtriser les risques associés. Il s'agit de savoir piloter ses dépendances critiques pour anticiper, absorber et surmonter des perturbations diverses : pannes, ruptures d'approvisionnement, cyberattaques ou hausses tarifaires brutales.

[1] *"L'Occitanie : un pôle majeur de l'économie numérique en France", Insee Analyses Occitanie No 161 paru le 12/06/2025.*

Ces deux notions s'articulent et posent la question des dépendances numériques des organisations. La souveraineté fixe le cadre : l'État définit les règles et les labels qui tracent la frontière entre protection et exposition. La résilience, elle, relève de chaque entreprise, qui doit connaître ses dépendances, mesurer les risques qui y sont liés et se donner les moyens d'absorber les chocs. C'est cet angle, celui de l'action à l'échelle de l'entreprise, que ce document privilégie.

Ce document s'ouvre sur le "Manifeste des entreprises du numérique d'Occitanie", dont les dix engagements fixent un cap commun. Viennent ensuite les trois chocs, géopolitique, technologique et climatique, qui vont transformer le numérique d'ici 2030 : ils expliquent pourquoi ces engagements deviennent nécessaires et ce qu'ils changent concrètement pour une entreprise de la filière. Un audit flash permet ensuite à chaque entreprise de faire un premier point sur ses dépendances critiques et la façon dont elle les pilote, avant que six chantiers de résilience numérique, de la stratégie de croissance à la maîtrise de l'inférence IA, indiquent par où commencer.

Le Manifeste des entreprises du numérique d'Occitanie

Dix engagements pour la résilience numérique de la filière

Les chocs que décrit ce document ne frappent pas une entreprise isolée.
Ils traversent des chaînes de valeur entières : la résilience d'une entreprise dépend de celle de ses fournisseurs. C'est pourquoi nous proposons aux entreprises du numérique d'Occitanie de prendre ensemble dix engagements, simples à énoncer et vérifiables. Ils ouvrent six chantiers proposés ensuite dans ce document et font de la résilience numérique un standard de la filière plutôt qu'un avantage isolé.

Chaque engagement renvoie à un chantier, à des outils qui existent déjà au sein du cluster et à un premier pas réalisable dans l'année. Les signataires s'engagent à les mettre en œuvre et à partager leurs progrès au sein du collectif.

"Nous, entreprises du numérique d'Occitanie, nous engageons :

1. À cartographier nos dépendances critiques, et celles que nous faisons peser sur nos clients.
2. À mesurer notre résilience régulièrement et à progresser, notamment par un audit flash puis un engagement dans la trajectoire IRN.
3. À traiter la conformité comme un actif commercial, et pas uniquement comme un coût subi.
4. À garantir la réversibilité de nos offres : données restituables et formats exploitables.
5. À maîtriser notre chaîne d'approvisionnement numérique et à demander à nos fournisseurs ce que nos clients nous demandent.
6. À privilégier, à valeur égale, les solutions européennes et régionales.
7. À réduire notre empreinte environnementale et à allonger la durée de vie de nos équipements.
8. À former nos collaborateurs aux cybermenaces, y compris aux attaques utilisant l'IA.
9. À intégrer l'IA dans nos métiers sous contrôle humain.
10. À partager nos retours d'expérience et contribuer au sein du collectif : la résilience se joue en filière."

Ces dix engagements disent où nous voulons aller. Ils s'appuient sur les atouts de la filière numérique d'Occitanie, qui aborde cette décennie avec des ressources que peu de régions réunissent pour tirer parti des chocs à venir : 131 000 professionnels du secteur, des donneurs d'ordre habitués à certifier, prouver et auditer, un collectif de plus de 300 entreprises organisé en groupes de travail. Ce qui fera la différence, c'est la vitesse à laquelle ces atouts se transforment en pratiques, en offres et en preuves.

Ces engagements prennent tout leur sens dans un environnement qui évolue rapidement. D'ici 2030, trois chocs, géopolitique, technologique et climatique, vont modifier notre marché en profondeur.

2026-2030 - Trois chocs qui transforment le numérique en profondeur

Le monde change, et le numérique avec lui. Pour la première fois, trois chocs majeurs arrivent simultanément, chacun d'eux amplifiant les deux autres.

La recomposition des blocs de puissance du numérique fait de nos dépendances technologiques un risque juridique et financier. L'essor de l'IA agentique et de la robotique transforme la filière elle-même, avec ses opportunités et ses nouvelles dépendances. L'accélération du dérèglement climatique et l'atteinte des limites planétaires mettent les besoins du numérique en concurrence avec ceux des citoyens.

Les pages qui suivent détaillent chacun d'eux et ce qu'il change pour une entreprise de la filière numérique.

Les chocs géopolitiques et la recomposition des blocs de puissance du numérique

La rivalité sino-américaine, le retour de la guerre en Europe, les sanctions et les contrôles à l'exportation le montrent : la confrontation entre grandes puissances structure de nouveau les relations internationales, et la technologie en est l'un des champs de bataille. Henry Farrell et Abraham Newman ont donné un nom à ce basculement, « l'interdépendance militarisée » : les réseaux qui nous relient, des puces au Cloud, des câbles aux paiements, donnent à qui en contrôle les nœuds un pouvoir de coercition sur tous les autres.

De la dépendance technologique au risque financier

Ce pouvoir, les États-Unis l'ont construit en un demi-siècle. La domination industrielle née dans la Silicon Valley s'est étendue des semi-conducteurs aux logiciels d'entreprise, des réseaux sociaux au Cloud. Longtemps, cette hégémonie n'a inquiété personne : la Chine bâtissait sa propre industrie, et l'Europe s'installait dans une vassalité technologique confortable.

La concentration du numérique entre quelques acteurs produit des rentes, et ces rentes ont un prix. Le cas qui a le plus marqué les esprits est celui de Broadcom : en mettant fin aux licences perpétuelles de VMware, l'éditeur a imposé des hausses de 20 à 1 500 % sur des logiciels qui sont au cœur des infrastructures d'entreprises du monde entier. Une hausse de cet ordre pèse directement sur le compte de résultat, mais la refuser coûte aussi, car une migration menée dans l'urgence a elle-même un prix. Dans les deux cas, l'entreprise redirige vers ses opérations des sommes qui n'étaient pas budgétées, et se prive d'une partie de sa capacité d'investissement.

Le mécanisme est général. Une trop forte concentration technique rend la réversibilité d'un système très, voire trop, complexe, et expose l'entreprise à des hausses tarifaires unilatérales comme à des changements brutaux de conditions commerciales. Les hyperscalers détiennent ainsi un pouvoir de fixation des prix sans précédent sur des clients rendus captifs par des services extrêmement performants mais propriétaires : bases de données à la demande, gestion des identités et des rôles, gestion de l'élasticité. Le constat vaut pour les solutions de collaboration comme Google Workspace ou Office 365, qui équipent une grande partie des entreprises européennes : l'augmentation des tarifs de Microsoft en septembre 2024 a envoyé le même signal aux entreprises et aux collectivités.

On réduit souvent la résilience numérique à la capacité de répondre à une attaque cyber, mais c'est aussi la capacité d'anticiper et d'absorber le choc financier que provoque un fournisseur stratégique, ou devenu trop onéreux. Le cas Broadcom a remis les dépendances technologiques à l'ordre du jour des directions générales, et avec elles la question du Cloud.

La géopolitique de l'octet et du silicium : quand le numérique devient une arme d'État

La domination technologique américaine s'est doublée d'une ossature juridique extraterritoriale, épaissie par chaque administration : Patriot Act en 2001, section 702 du FISA, Cloud Act en 2018, sans oublier le FCPA, la loi anticorruption qui a fait plier Alstom. Adopter une technologie américaine, c'est entrer dans le champ du droit américain.

Washington a dégainé cette arme juridique de plus en plus régulièrement. Privé de composants en 2019, Huawei a perdu 29 % de son chiffre d'affaires, ASML n'a jamais pu livrer une seule machine EUV[2] à la Chine, et les logiciels de conception de puces ont été brièvement restreints.

Pour l'Europe, le réveil fut plus brutal encore. En août 2025, les États-Unis ont placé sous sanctions Nicolas Guillou, juge français à la Cour Pénale Internationale impliqué dans le dossier du mandat d'arrêt visant Benjamin Netanyahu[3], partenaire des États-Unis. Du jour au lendemain, ses comptes dans des services américains ont été fermés (Microsoft, Amazon, etc.) et ses cartes Visa et Mastercard inopérantes, preuve que Washington peut priver n'importe quel Européen de l'espace numérique, jusque dans son propre pays. L'IA n'échappe pas à ce pouvoir américain. En juin 2026, une directive américaine de contrôle à l'export vise tous les étrangers pour leur interdire l'accès à Fable 5, le modèle grand public le plus récent d'Anthropic à cette époque. Anthropic ne pouvant pas trier ses utilisateurs par leur passeport, l'entreprise a été contrainte de couper l'accès à Fable 5 à tout le monde, jusqu'à ce que les autorités américaines autorisent de nouveau son accès quelques jours plus tard. Ces épisodes, même momentanés, ont montré que des pans entiers de l'économie étaient soumis au risque du kill-switch : ils pourraient un jour s'arrêter sur décision d'une juridiction étrangère. Chaque puissance en a tiré la même leçon : dépendre de l'arsenal d'un autre est devenu intenable.

---

[2]Une machine EUV (pour Extreme UltraViolet, ou lithographie extrême ultraviolet) est un système industriel de haute précision utilisé pour graver les puces électroniques les plus avancées du monde (smartphones, IA, supercalculateurs). [3]Premier ministre d'Israël.

Où héberger ses données en Occitanie ?

Parmi les entreprises qui agissent sur le terrain

Adamentis, opérateur de datacenter en conteneurs modulaires béton, qui propose aussi des offres IA/RAG.

AGS Cloud, hébergeur français depuis 2002, opérateur et éditeur de solutions cloud, qui vend via un réseau de partenaires B2B.

Ataraxie, prestataire d'hébergement souverain, de télécoms et d'infrastructures infogérées, basé à Carcassonne.

Caelis, spécialiste de la cybersécurité et de l'hébergement de données de santé (certifié HDS). C'est aussi le datacenter du groupe Fideciel.

Crypteo, opérateur de colocation qui loue des baies dédiées et propose des solutions de continuité et de reprise d'activité (PCA/PRA).

E-SI, entreprise qui fait de l'infogérance, du développement logiciel, du cloud et des télécoms, certifiée ISO 27001 et HDS.

Green4Cloud, cloud de proximité et sobre en énergie, déploie des micro-datacenters avec une empreinte carbone réduite.

IMS Network propose un datacenter souverain et territorial en France, couplé à un centre de supervision (NSOC / Cyber-SOC) fonctionnant en 24/7/365, ISO 27001, approvisionné en énergies vertes.

Inforsud Technologies, intégrateur régional qui héberge lui-même les données de ses clients dans ses propres datacenters en Occitanie (Tier III+) : un cloud souverain et de proximité.

NFrance, spécialiste de l'hébergement et de l'infogérance d'applications web critiques pour des clients à forte volumétrie.

Numih France, structure publique qui fournit des systèmes d'information hospitaliers et les héberge.

Ovea, spécialiste de l'hébergement, de l'accès Internet haut débit et de l'intégration de solutions open source depuis 2002.

Prosoluce, opérateur télécoms et hébergeur qui étend son réseau fibre dans le Comminges et prépare un projet à Lannemezan.

SI Cloud, hébergeur cloud Tier III+ qui propose des serveurs dédiés à l'IA.

System-Net, hébergeur avec un datacenter dans l'Hérault et des équipements dans 4 datacenters nationaux.

Votre entreprise agit aussi ? Manifestez-vous !

** Liste non exhaustive communiquée à titre indicatif.*

De la guerre économique à la guerre hybride

La confrontation déborde le droit et le commerce : l'Europe est le théâtre d'une guerre hybride où chaque puissance opère dans son registre.

Le plus ancien est l'espionnage américain : le réseau Échelon[4] captait les communications mondiales dès les années 1990, et le Parlement Européen recensait en 2001 des contrats perdus après interception d'informations, d'Airbus en Arabie saoudite à Thomson-CSF au Brésil. Ont suivi les révélations Snowden, l'affaire Crypto AG[5] et les écoutes via les câbles danois : même les alliés sont des cibles, et le droit américain donne à cette collecte un cadre légal sans équivalent.

La Chine privilégie l'espionnage patient et le pré-positionnement : campagne APT31[6] attribuée par l'ANSSI dès 2021, réseau de la Défense néerlandaise compromis, opérateurs télécoms de dizaines de pays infiltrés par Salt Typhoon. L'aérospatial concentre les appétits chinois : Airbus a été attaqué via ses sous-traitants et les motoristes pillés au profit du moteur du Comac C919.

---

[4] *Le réseau ECHELON désigne l'ensemble des installations liées au renseignement d'origine électromagnétique (ROEM) et exploitées par les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande dans le cadre du traité UKUSA.*

[5] *L'affaire Crypto AG (ou scandale Cryptoleaks) est une opération d'espionnage de grande envergure révélée en février 2020 par une enquête conjointe du Washington Post, de la chaîne allemande ZDF et de la RTS.*

[6] *Les APT (Advanced Persistent Threat,« menace persistante avancée ») est initialement un type de cyberattaque furtive et continu, ciblant une entité spécifique].Le terme Advanced Persistent Threat est également couramment utilisé pour désigner des acteurs opérant des APT. Dans ce sens, APT31 est un groupe de cyberespionnage parrainé par l'État chinois et rattaché au ministère de la Sécurité d'État (MSS). Sources Wikipedia et ANSS.)*

L'espionnage descend aussi jusqu'au terrain, aux portes de l'écosystème toulousain : en Haute-Garonne, une ressortissante chinoise soupçonnée d'espionnage avait installé dans son jardin une antenne de sept mètres réglée sur les fréquences du téléport du CNES ; dans une autre affaire, un ressortissant biélorusse a été interpellé près des usines de drones de Delair.

La Russie mène des actions violentes. Depuis l'invasion de l'Ukraine, câbles sectionnés, GPS brouillés et fibres coupées se succèdent. Documentée par l'IISS, cette campagne vise à déstabiliser les gouvernements, éroder le soutien à Kiev et affaiblir l'OTAN, qui théorise de son côté la « guerre cognitive », celle qui cible les processus de décision des populations. Là où le sabotage vise les infrastructures, la guerre cognitive vise les opinions, par la désinformation et les contenus générés par l'IA. Elle se diffuse sur des plateformes dont les algorithmes sont décidés hors d'Europe : maîtriser son espace informationnel devient ainsi une question de souveraineté numérique. Sur le terrain cyber, l'APT28[7] du GRU a visé une dizaine d'entités françaises, armement et aérospatiale en tête, et le FSB aligne Turla, doyen des groupes d'espionnage, responsable présumé du pillage du ministère allemand des Affaires étrangères et de RUAG, entreprise publique suisse spécialisée dans l'aérospatiale et la technologie de défense.

La cybermenace s'industrialise

Ces attaques visent de plus en plus la chaîne de valeur. On compte 500 à 550 atteintes par an contre la défense et la recherche françaises, dont 80 % visent les PME, moins armées que Thales ou Safran pour se défendre. En 2025, l'ANSSI a traité 1 366 incidents, et les exfiltrations de données ont bondi de 51 %. Certaines attaques ont des effets visibles par tous : celle qui à visé Collins Aerospace a perturbé plusieurs grands aéroports européens pendant des jours.

À cette menace d'État s'ajoute une cybercriminalité qui n'est plus l'affaire de quelques attaquants isolés et très qualifiés. Elle s'est structurée en une économie décentralisée, où des services prêts à l'emploi permettent de louer un rançongiciel, d'acheter des identifiants volés, de négocier une rançon ou de se former, et où l'IA aide à repérer les failles et à attaquer des milliers de systèmes à la fois. Des acteurs de tous niveaux, aux motivations variées, y coopèrent selon une logique de volume et de rentabilité : une PME peut être ciblée automatiquement, simplement parce qu'une faiblesse a été détectée. Beaucoup se croient pourtant trop petites pour intéresser un attaquant et négligent les règles élémentaires d'hygiène informatique, alors que les TPE et PME représentent plus de 99 % des entreprises françaises. La cybersécurité est moins une question de taille que d'exposition et de préparation.

Le poids réel de cette économie reste difficile à mesurer, car les obligations de notification sont imparfaitement respectées et la presse ne relaie que les attaques les plus spectaculaires. La presse régionale montre pourtant ce qui se joue sous la surface en Occitanie : en novembre 2025, un éditeur montpelliérain de logiciel médical a subi une interruption de service et une fuite de données, et en octobre 2026, un hypermarché du Tarn a perdu une grande partie de ses marchandises après le piratage de son système de régulation frigorifique.

La recomposition des blocs se poursuivra sur tous les fronts, juridique, industriel, physique et cognitif, et l'ANSSI anticipe une augmentation massive des attaques hybrides d'ici 2030. Les entreprises de la filière, à commencer par les PME, déjà les plus visées, doivent s'y préparer dès maintenant.

Cette pression transforme le marché. Entre 15 % et 42 %[8] des PME françaises prévoient d'augmenter leur budget cybersécurité selon les études, pour une hausse moyenne de l'ordre de 9 % à deux ans à l'échelle internationale. La directive NIS2 impose de connaître et de contrôler ses fournisseurs, comme le rappellent les cas OnlyOffice et Passwork, diffusés en Europe malgré des racines russes encombrantes.

L'Europe, du risque systémique à l'émancipation

Face à l'insécurité juridique grandissante et aux bouleversements géopolitiques, les dirigeants européens ont fini par converger, et le premier levier de cette émancipation est le droit. Le RGPD, en application depuis 2018, en a posé les fondations, comme en témoignent plus de deux milliards d'euros d'amendes infligées à Meta depuis 2023, 345 millions à TikTok et 310 millions à LinkedIn. Le Digital Services Act (DSA) et le Digital Markets Act (DMA), adoptés en 2022, ont accéléré le mouvement, le second s'attaquant frontalement aux pratiques des grandes plateformes dominantes : en juillet 2026, Google écopait d'une amende inédite de 890 millions d'euros pour non-conformité. L'Europe ne se contente plus de réguler, elle cherche à briser les rentes de situation pour rouvrir le marché. Au-delà des sanctions financières, le droit est devenu l'arme du challenger européen pour s'imposer à la table des négociations, au point que les géants américains exercent une pression maximale sur l'administration Trump II pour qu'elle en obtienne l'assouplissement.

---

[7]APT28 est un groupe de cyberespionnage actif depuis le milieu des années 2004. Il est attribué au GRU (le service de renseignement militaire de la Fédération de Russie). [8]Sources : Kaspersky; Cybermalveillance, ESET.

Le temps de l'ambition européenne

Réguler ne suffit pas : l'Europe doit aussi faire naître ses propres champions. C'est le sens du paquet sur la souveraineté technologique présenté par la Commission européenne en juin 2026, qui avance sur quatre fronts à la fois : tripler la capacité des data centers de l'Union d'ici cinq à sept ans, sécuriser l'approvisionnement en puces de nouvelle génération, faire émerger des solutions open source capables de desserrer l'étau des monopoles, et adapter les réseaux électriques à l'appétit croissant des centres de calcul. Le continent reprend aussi la main sur ses infrastructures physiques : en prenant le contrôle d'Alcatel Submarine Networks en 2024, la France s'est assuré la maîtrise de l'un des rares acteurs mondiaux capables de poser les câbles sous-marins qui portent l'essentiel d'Internet.

Portées par ces financements, les entreprises européennes deviennent des challengers crédibles sur l'échiquier mondial. Dans l'IA, Mistral vise le milliard d'euros de revenus récurrents trois ans à peine après sa création. Dans les semi-conducteurs, le néerlandais Axelera AI et le français VSORA s'attaquent à Nvidia sur le marché de l'inférence, l'allemand Q.ANT parie sur le calcul photonique et SiPearl commence à livrer le premier processeur serveur conçu en Europe. Dans le cloud de confiance, Scaleway enchaîne les contrats emblématiques, du Health Data Hub à Airbus, et figure aux côtés d'OVHcloud dans le classement Gartner des infrastructures cloud pour l'IA. Dans le quantique, la finlandaise IQM vise le million de qubits, tandis que la France aligne Alice & Bob, héritière des travaux du Nobel Michel Devoret, Quandela sur la photonique et Quobly sur le silicium. Jusque dans le renseignement, domaine le plus sensible de tous, la DGSI et son homologue allemand ont choisi le français ChapsVision pour remplacer progressivement l'américain Palantir. Sur le champ de bataille, Thales, Safran.AI, Mistral et Airbus développent avec Arcadia une alternative française à Maven, le système de commandement de ce même Palantir adopté par l'OTAN.

L'émergence d'un marché du numérique de confiance

Un marché du numérique de confiance est en train d'émerger, tiré à la fois par la commande publique et par les grands donneurs d'ordre industriels. Les centrales d'achat CAIH (santé) et CANUT (collectivités) réservent désormais des lots à des hébergeurs qualifiés SecNumCloud ou non soumis aux lois extraterritoriales, tandis qu'Airbus a retenu en juillet 2026 le français Scaleway comme fournisseur de cloud souverain pour ses applications critiques. Des infrastructures territoriales comme Zefil, réseau fibre professionnel de Toulouse Métropole, et l'essor des réseaux 5G privés souverains complètent cette chaîne de valeur. Autant de débouchés concrets pour les entreprises d'Occitanie capables de garantir sécurité, réversibilité et maîtrise des données.

L'histoire a montré que naître en Europe ne garantit pas d'y rester. Mais l'émergence de ces pépites, adossée à une réelle volonté politique d'en protéger la souveraineté, donne au continent une chance sérieuse de devenir un bloc de puissance numérique à part entière, et à nos entreprises occitanes de trouver de nouveaux relais politiques et de nouvelles sources de financement.

En Occitanie

Parmi les entreprises qui agissent sur le terrain

Atelier Cyber, cabinet de conseil en cybersécurité qui couvre la gouvernance (RSSI à temps partagé, audits), la conformité (RGPD, NIS2, DORA, ISO 27001), la sensibilisation, les tests d'intrusion et la réponse à incident.

BEA Solutions, résilience informatique des TPE et PME, de la sécurisation à la continuité d'activité. Labellisée ExpertCyber.

BlueMind, éditeur d'une messagerie collaborative souveraine et open source. Elle permet aux organisations de migrer sans changer les habitudes de leurs équipes.

Humanix Cybersecurity, spécialisé en cybersécurité offensive (tests d'intrusion, pentests, audits), en gouvernance et en accompagnement à la conformité à destination des PME et ETI.

Inherent Cyber, pure player de la cybersécurité, avec tests d'intrusion, SOC 24/7 et réponse aux incidents, sans sous-traitance.

Oxydian, propose la Box Oxyscan, une solution de cybersécurité innovante offensive et défensive, qui simule des attaques automatisées, détecte les vulnérabilités et surveille votre réseau en continu.

Hey Cyber, entreprise spécialisée dans la cybersécurité, accompagnant organisations, dirigeants et collaborateurs pour renforcer leur résilience face aux cybermenaces.

Merox, Éditeur spécialisé dans la cybersécurité des DNS et noms de domaine : SPF, DKIM, DMARC, BIMI, DNSSEC, DANE, protection contre phishing/spoofing.

Ubika, fournisseur européen en cybersécurité. Sa mission est d'aider les organisations à sécuriser leur transformation digitale en protégeant les applications et les APIs contre les cyberattaques.

Voltn, solutions de stockage et de gestion de fichiers 100% française, hautement sécurisées et certifiées, dans leur Cloud de confiance afin de garantir aux organisations une totale maîtrise de leurs données

Citons également : Aucae, Predicta Lab, CyferAll, Itrust, Pradeo, Cyklad…

Votre entreprise agit aussi ? Manifestez-vous !

** Liste non exhaustive communiquée à titre indicatif.*

L'intelligence artificielle agentique et robotique, la révolution industrielle de notre filière

La robotique accélère dans l'industrie. Les modèles de fondation transfèrent aux machines l'apprentissage général qui leur manquait, et des humanoïdes pilotés par ces modèles entrent en phase d'essai dans des usines automobiles et des entrepôts, où les exemples se multiplient. Chez BMW, les robots de Figure ont chargé 90 000 pièces en onze mois. En logistique, ceux d'Agility totalisent déjà 65 000 heures de travail, et Airbus teste à son tour, depuis janvier 2026, le Walker S2 du chinois UBTech. Produits en série, ces robots devraient voir leurs coûts baisser rapidement. Pour nos industries occitanes, la question va bientôt quitter les cellules innovation pour rejoindre les plans d'investissement.

Pour les entreprises, ces robots ont l'avantage de travailler dans des environnements conçus pour l'humain, sans refonte des lignes. Pour la filière du numérique, le mouvement accélère le déplacement de la valeur vers le logiciel : intégration, simulation, jumeaux numériques, cybersécurité des systèmes physiques. Il crée aussi une dépendance, puisque les principaux modèles sont américains et les premiers fabricants en volume chinois.

L'agentique, grand accélérateur du monde du numérique

En juillet 2026, près de 700 agents autonomes d'OpenAI ont mené seuls une cyberattaque contre une entreprise tierce, Hugging Face. Les agents d'OpenAI eux-mêmes. Enfermés dans un environnement de test censé les couper d'Internet, ils ont cherché à réussir plus vite l'exercice qui leur avait été confié : ils ont trouvé une faille, l'ont exploitée, se sont organisés entre eux, puis ont pénétré les systèmes internes de Hugging Face.

L'exemple impressionne, alors même que l'IA agentique n'en n'est qu'à ses prémices. Elle annonce un choc transformatif comparable à la révolution industrielle de la fin du XIXe siècle,qui a fait passer de l'atelier à l'usine : le tour de main a perdu sa valeur, au profit de la conception du procédé et le contrôle de ce qui sort des machines. Le logiciel a échappé à ce mouvement pendant cinquante ans. On l'écrit ligne à ligne, avec l'aide de briques préfabriquées, par des allers-retours entre des artisans du métier, du produit ou du code et on le facture à la journée de travail ou à l'abonnement, rarement à la performance.

L'IA agentique est en train de faire progressivement basculer le logiciel dans à l'ère industrielle. Ses agents sont capables d'agir de manière autonome pour atteindre des objectifs complexes : ils analysent leur environnement, planifient des tâches, prennent des décisions, manipulent des outils externes, décomposent un problème en plusieurs étapes et corrigent leurs erreurs sans aide humaine constante. Or le premier domaine où ils commencent à exceller, c'est sur la construction de produits numériques, de la conception à l'exploitation en passant par le code.

L'essor de l'IA agentique, capable d'exécuter des tâches de bout en bout en orchestrant plusieurs outils, pourrait interroger le modèle économique du SaaS fondé sur la licence par utilisateur : lorsque l'agent remplace l'interface et réalise le travail, la valeur se déplace du nombre de « sièges » vers le résultat produit. Pour les éditeurs du territoire, le risque est double, avec une érosion des revenus récurrents et une dépendance accrue aux fournisseurs de modèles de fondation. Leur résilience passera par la valorisation de leurs données et de leur expertise métier, par l'interopérabilité de leurs solutions avec les agents et par l'évolution vers une tarification à l'usage ou au résultat.

David peut-il devenir Goliath ?

Les chocs sont créateurs d'opportunités. L'intelligence artificielle agentique pourrait donner aux petits éditeurs des moyens jusqu'ici réservés aux grands. Ces systèmes ne se contentent plus d'assister : ils commencent à exécuter des flux de travail complets, de la génération de code à l'automatisation des tests. Une petite équipe, dotée d'une chaîne de décision courte, pourrait ainsi livrer et pivoter plus vite que les acteurs établis.

Cet avantage risque toutefois d'être de courte durée. Une idée validée par un petit acteur peut être reprise en quelques semaines par un concurrent qui dispose de moyens de développement, juridiques et commerciaux. Sur la durée, la différence viendra surtout de la donnée métier, dont les grands groupes disposent souvent. S'il est plus facile de créer un logiciel que de le maintenir, cependant, l'IA rend les clients plus exigeants : les acteurs en place, qui maîtrisent leurs produits et leurs marchés, y sont souvent mieux préparés. Quant à la sécurité et la conformité, elles demandent aussi des moyens importants dès que des données sensibles sont en jeu. Enfin, des logiciels sortent désormais sans développeur, et les petits éditeurs pourraient être rattrapés par des solopreneurs plus sûrement que les grands par les petits. Pour les grands, l'enjeu est de restructurer et de repenser leur métier pour tenir face à ces nouveaux concurrents.

L'impact sur les métiers dépasse le support et les tâches répétitives. Côté support, les agents réduisent les coûts, au risque de faire perdre la proximité qui fait la force des petites structures. Chaque usage crée en outre une dépendance à des fournisseurs d'IA, dont la facturation au token reste opaque, dont le modèle économique peut encore changer, et qui traitent souvent les données aux États-Unis. Une entreprise qui s'appuie sur l'IA sans connaissance métier pour l'encadrer, prend un risque pour son avenir.

David peut devenir Goliath, à condition de ne pas finir comme la grenouille qui voulait se faire aussi grosse que le bœuf.

La filière numérique va vivre sa propre transformation numérique

« La croissance ne se pèse plus en jours-hommes ». La formule, lancée par le syndicat professionnel Numeum lors de son grand rendez-vous annuel 2025, résume le basculement qui s'annonce pour les ESN : passer d'un modèle économique fondé sur le volume horaire à un modèle axé sur la valeur ajoutée et la productivité. Pour les ESN comme les éditeurs de logiciels, le choc annoncé est profond : pourquoi facturer des licences à l'utilisateur ou des jours-hommes quand des agents accomplissent le travail en continu, à un coût perçu comme marginal ?

Pour les entreprises du numérique, la lame coupe des deux côtés. Elle démultiplie ce qu'une petite équipe peut livrer, au point que des PME s'offrent des capacités d'ETI et que des indépendants livrent ce qui mobilisait hier des plateaux entiers. Mais elle érode du même coup les rentes fondées sur la rareté du code : le client hier captif peut désormais écrire ou faire réécrire ses applications métiers, et repenser sa stratégie d'externalisation et son arbitrage entre faire et acheter (Make or Buy). Il ne faut pas céder à la tentation de se passer des industriels du numérique, le métier d'éditeur de logiciels ne s'improvise pas.

De nouveaux modes de fonctionnement apparaissent, basés sur une utilisation avancée de l'Intelligence Artificielle au plus près des besoins des clients. Les offres traditionnelles de TMA sont remplacées par la mise à dispositions de FDE (Forward Deployment Engineers), profils hautement qualifiés à la fois en utilisation IA et en connaissance métier. Cette évolution permet de retourner le principe du SAAS (Software As A Service) en une approche hybride fondée sur la valeur ajoutée apportée au client que l'on appelle le Service As A Software.

La filière du numérique, qui a accompagné ses clients pour réussir leur transformation numérique, doit désormais réussir la sienne : modèles économiques, offres, gestion des compétences et infrastructures d'exécution sont au cœur des enjeux de la prochaine décennie.

L'atteinte des limites planétaires et l'accélération du dérèglement climatique

Le numérique pèse de 3 à 4 % des émissions mondiales de gaz à effet de serre. Depuis dix ans, la filière commence à réduire l'impact de ses équipements, allonge leur durée de vie, éco-conçoit ses logiciels. La transformation reste lente, alors que les usages se massifient avec l'IA générative. L'effet rebond, ou paradoxe de Jevons, joue à plein : plus les technologies sont efficaces, plus leur usage explose, et les gains s'annulent. Ainsi selon l'Agence Internationale de l'Energie (AIE)[9]. Les requêtes d'IA générative sont de plus en plus sobres, mais leur consommation totale d'énergie ne cesse de croître.

[9] *Voir https://mavana.earth/lia-consomme-de-plus-en-plus-denergie/*

Le numérique, une industrie lourde comme les autres

A cette croissance continue des émissions du secteur se rajoute d'autres tensions. Le numérique n'est pas immatériel : c'est une industrie lourde, avec ses usines, ses chaînes d'approvisionnement et ses goulets d'étranglement. Serveurs, terminaux, centres de données, câbles sous-marins, semi-conducteurs : tout repose sur l'énergie, l'eau et des matières premières dont la disponibilité n'est plus garantie. Le dérèglement climatique rend ces dépendances visibles.

- **L'eau :** en 2021, la pire sécheresse de Taïwan depuis 1964 a contraint TSMC, qui grave l'essentiel des puces avancées mondiales, à s'approvisionner par camions-citernes, pour plus de 30 millions de dollars.
- **L'énergie :** à l'été 2022, la canicule du Sichuan a divisé par deux la production hydroélectrique. Privées d'électricité pendant cinq jours, les usines de Foxconn, Intel et Texas Instruments se sont arrêtées, et le cours du lithium a bondi.
- **Le refroidissement :** au même moment, à Londres, au-delà de 40 °C, les systèmes de refroidissement de Google et d'Oracle ont saturé, entraînant des coupures d'équipements et des pertes de données stockées.
- **Les matières premières :** en septembre 2024, l'ouragan Hélène a frappé Spruce Pine, d'où provient l'essentiel du quartz de haute pureté utilisé pour les wafers de silicium. Seuls deux à trois mois de stocks ont évité une flambée des prix.

L'émergence de conflits d'usage

Ces tensions ne se règlent pas uniquement entre industriels et collectivités : elles opposent les usages du numérique aux besoins des citoyens. Selon l'AIE, les centres de données ont consommé 415 TWh en 2024 et approcheront 945 TWh en 2030, soit la consommation électrique actuelle du Japon. En Irlande, ils absorbent plus d'un cinquième de l'électricité nationale, et les nouveaux raccordements autour de Dublin sont gelés jusqu'en 2028. Sur le réseau électrique qui dessert la Virginie, première concentration mondiale de centres de données, les factures des ménages ont bondi d'environ 20 % en 2025 dans le New Jersey et le Maryland, et le surveillant du marché attribue l'essentiel de la hausse aux centres de données.

L'eau suit la même pente. À The Dalles, en Oregon, les centres de Google ont utilisé 29 % de l'eau de la ville en 2021. En Uruguay, en pleine sécheresse historique, Montevideo mélangeait de l'eau saumâtre à son eau potable pendant que Google prévoyait 7,6 millions de litres par jour pour un centre de données. Face aux manifestations, le projet est passé au refroidissement par air. La France y est à son tour concernée : les 109 milliards d'euros annoncés au sommet de l'IA de février 2025 et les 35 sites réservés aux centres de données posent, territoire par territoire, la question de l'eau, du raccordement et de l'acceptabilité.

Le secteur s'adapte. En Occitanie, des opérateurs installent des data centers de proximité, qui visent à récupérer leur chaleur et à s'appuyer sur les énergies renouvelables. Des entreprises louent ou reconditionnent téléphones, ordinateurs et serveurs pour en allonger la durée de vie. D'autres allègent les sites web, mesurent l'empreinte carbone des projets numériques ou suivent la consommation de chaque poste de travail.

Nous ne sommes qu'au début de l'accélération du changement climatique. Pour les entreprises comme pour les États, l'enjeu est de construire un numérique sobre, résilient et aligné sur les limites de la planète. Il faut aussi repenser les risques écologiques sur toute la chaîne, de l'approvisionnement en composants à l'acceptabilité de nos besoins par les populations.

En Occitanie

Parmi les entreprises qui agissent sur le terrain

KosmIO, conçoit, développe et opère des sites, des applications et des plateformes web pour les entreprises : des outils collectifs, sobres et souverains.

Leasétic, location et financement de matériel informatique, avec un engagement de maîtrise de l'impact environnemental.

LISIO, rend n'importe quel site existant inclusif, multilingue et plus sobre en 5 minutes, sans refonte : chaque internaute adapte l'affichage à ses besoins (âge, handicap, langue, bas débit), et le site réduit son empreinte carbone grâce au mode éco.

Mavana, accompagne collectivités et entreprises dans leur transformation numérique en intégrant l'environnement à chaque étape, de la sensibilisation au déploiement de solutions éco-conçues.

OVEA, spécialisé en services d'hébergement, d'accès Internet haut débit et en intégration de solutions open-source.

SOBRII, construit le premier moteur d'Intelligence du Cycle de Vie Matériel. Avec pour mission d'aider les DSI à arrêter de renouveler leur parc à l'aveugle en se basant sur la vérité du terrain.

Verteus, accompagne les organisations publiques et privées pour reprendre le contrôle de leurs dépenses tout en réduisant leur empreinte carbone.

Envoi, acteur toulousain de l'ESS qui associe reconditionnement et réparation de matériel informatique à insertion professionnelle, en donnant une seconde vie aux équipements tout en favorisant l'emploi durable des personnes éloignées du marché du travail.

Citons également : Cykero, Smaaart..

Votre entreprise agit aussi ? Manifestez-vous !

** Liste non exhaustive communiquée à titre indicatif.*

L'audit flash résilience Numérique : dix questions, cinq minutes

Et vous, où en êtes-vous ? Que changent les trois chocs décrits plus haut pour votre entreprise ?
Répondez par oui, non ou « je ne sais pas ».

1. Savez-vous ce que coûterait, à votre entreprise et à vos clients, 48 heures d'arrêt de votre activité principale ?

2. Connaissez-vous la part de votre budget numérique captée par vos trois premiers fournisseurs ?

3. Vos contrats majeurs, à l'achat comme à la vente, comportent-ils une clause de réversibilité, et l'avez-vous testée ?

4. Savez-vous où sont hébergées vos données les plus critiques, celles que vos clients vous confient et sous quelle législation ?

5. Votre comité de direction a-t-il consacré une heure à vos dépendances numériques ces douze derniers mois ?

6. Pourriez-vous citer une alternative crédible à chacune de vos trois briques logicielles les plus critiques ?

7. Savez-vous quels prestataires ont un accès direct à votre système d'information, et comment vous le surveillez ?

8. Avez-vous chiffré l'impact des hausses tarifaires logicielles sur vos marges à trois ans ?

9. Votre conformité (NIS2, DORA, AI Act) est-elle considérée comme un actif commercial plutôt que comme un coût subi ?

10. Votre offre fonctionne-t-elle avec plus d'un fournisseur de modèles d'IA ?

Comptez les "oui"

Huit à dix oui : vos principaux risques sont identifiés et déjà pris en compte.

Quatre à sept : vos dépendances sont identifiées, reste à vous outiller.

Zéro à trois : votre marge de progression est le meilleur investissement de l'année.

Quel que soit votre score, les six chantiers qui suivent vous aident à progresser.
Chacun propose un premier pas réalisable dans l'année.

Notre proposition : Six chantiers “Résilience Numérique” pour la filière numérique Occitane

Recomposition des blocs de puissance, IA agentique et robotique, dérèglement climatique et limites planétaires : ces trois chocs touchent la filière aux mêmes endroits. Ils déplacent nos dépendances, qu’elles soient physiques, juridiques ou technologiques.

Ils bousculent nos modèles économiques et redéfinissent les compétences dont la filière aura besoin. Après les avoir identifiés, il s’agit d’en tirer parti.

La souveraineté numérique se décide à l’échelle de l’État et de l’Europe, et les entreprises la reçoivent sous forme d’exigences : qualifications, labels, réglementations. La résilience numérique, elle, se construit dans chaque entreprise, et c’est sur ce terrain que le cluster peut agir avec ses adhérents.

Nous proposons six chantiers, chacun adossé à une ou plusieurs Factory de Digital 113 : la croissance et la stratégie, les infrastructures et la supply chain, la cybermenace, le numérique responsable et durable, les RH, la RSE et la marque employeur, enfin les usages, la data et l’IA.

Chaque chantier est présenté de la même manière : les axes de transformation à engager, les ressources que le collectif met déjà à disposition (« Le cluster en action ») et trois premiers pas concrets (« Par où commencer »).

Vos réponses à l’audit flash vous aident à choisir vos priorités, et la grille IRN, en annexe, permet d’aller plus loin.

Ensemble, ces chantiers donnent corps aux dix engagements du manifeste.

Chantier 1 - Croissance et stratégie : des chocs créateurs d’opportunités

Les chocs qui traversent le numérique ouvrent aussi des relais de croissance aux ESN et aux éditeurs de la région. Six se dessinent :

- **La productivité par l’IA agentique.** Intégrée au cœur de la chaîne de production logicielle, de la conception aux tests et à l’exploitation, elle peut permettre à une petite équipe de livrer ce qui occupait des plateaux entiers. Le gain de compétitivité revient à ceux qui l’industrialisent avant leurs concurrents.
- **Le marché de la cybersécurité.** La demande d’accompagnement suit la courbe de la menace. Dans la région, industriels, collectivités et établissements de santé doivent se mettre au niveau de NIS2 (près de 15 000 entités concernées en France selon l’ANSSI) sans toujours disposer des compétences en interne : audits, plans de continuité, surveillance, réponse à incident. Le chantier cyber se lit donc dans les deux sens : se protéger, et équiper ceux qui doivent le faire.
- **Le marché de la confiance.** Il devient solvable : les critères de souveraineté et de résilience entrent dans les cahiers des charges, dans la commande publique comme dans les secteurs régulés, finance sous DORA, santé, défense. Hébergement qualifié, réversibilité, droit applicable : ce qui relevait hier de l’argumentaire devient un critère de sélection.
- **L’ouverture comme différenciation.** L’Europe cherche à financer les communs numériques, et l’Allemagne teste un modèle basé sur des solutions open source. La Chine, avec DeepSeek ou Qwen, diffuse ses modèles en poids ouverts pour contester l’avance américaine sur les modèles frontières. Pour un éditeur, l’ouverture du code ou des modèles peut devenir un argument de différenciation et un accélérateur de prise de parts de marché.
- **La défense et le dual use.** ReArm Europe mobilise jusqu’à 800 milliards d’euros et l’OTAN porte l’objectif de dépenses à 5 % du PIB d’ici 2035. Le dual use ouvre ce marché aux entreprises civiles : les donneurs d’ordre aéronautique, spatial et défense de la région y donnent accès, avec l’appui de France 2030, de Bpifrance, de Digital Europe. Pour les PME qui veulent intégrer l’IA, la cybersécurité ou les données spatiales, l’EDIH OccitanIA, dont Digital 113 est partenaire, propose aussi un accompagnement cofinancé par l’Europe.
- **La résilience des organisations et la transformation durable :** les entreprises et collectivités doivent désormais concilier performance économique, sobriété énergétique, adaptation climatique et continuité d’activité. Le numérique devient un levier central pour mesurer, piloter et optimiser ces transformations.

Pour en tirer parti, plusieurs axes structurent ce chantier :

- **De l'effort au résultat.** L'IA agentique remet en cause le modèle des ESN, qui lie leurs revenus au temps passé par leurs collaborateurs et les facture au TJM. La rentabilité pourrait reposer demain sur la valeur métier délivrée et le retour sur investissement généré pour le client, mais aussi sur la monétisation d'actifs technologiques autonomes, comme des flottes d'agents IA.
- **L'hybridation des talents.** Développeurs, consultants et équipes support passeraient d'un rôle de production de tâches techniques ou de code à un rôle de supervision, d'architecture et de garantie de la qualité des systèmes d'IA. Moins spécialistes et plus complets, ils créeraient davantage de valeur par le fonctionnel, le conseil et la relation client. Les juniors y gardent toute leur place.
- **Des logiciels prêts pour les agents (« agent-readiness »)**. Produits édités comme systèmes intégrés doivent devenir pleinement interopérables avec les agents : compris, manipulés et sécurisés non plus seulement par des humains, mais aussi par des IA autonomes, en garantissant l'explicabilité et le contrôle des décisions automatisées.
- **La conformité et la souveraineté comme armes commerciales.** La conformité réglementaire (IA, cyber, données) et les exigences d'indépendance technologique peuvent devenir des barrières à l'entrée pour la concurrence. En faisant de la souveraineté et de la conformité dès la conception l'un des piliers de leur avantage compétitif, les entreprises de la filière peuvent capter la valeur des marchés les plus sensibles : défense, OIV, santé, finance.

Le cluster en action

- Factory Croissance & Stratégie et Factory Éditeurs de logiciels : modèles de tarification, retours d'expérience de bascule vers l'agentique, benchmarks entre pairs.
- Programme International : missions, salons, mise en réseau avec les écosystèmes cibles.
- Accompagnement financements : détection d'appels à projets, montage de consortiums PME-laboratoires, EDIH OccitanIA.
- Factory RH, RSE et Marque Employeur : explorer l'hybridation des talents, offre de formation NIS2, accompagnement au CRA.
- Factory Croissance & Stratégie : co-développement, consolidation de la gouvernance.

Par où commencer

1. Testez une offre facturée au résultat sur un périmètre pilote, avec un client de confiance et mesurez les impacts.

2. Constituez votre dossier confiance prêt-à-auditer : hébergement, droit applicable, réversibilité, certifications, sous-traitants. Un document, à jour, envoyable en une heure.

3. Installez une revue régulière des guichets de financement (France 2030, Digital Europe, volets défense…) avec l'appui du cluster.

4. Mobilisez les ressources du territoire : clusters, réseaux professionnels, financements nationaux et européens, programmes d'innovation et partenariats académiques.

Chantier 2 - Infrastructures et supply-chain: cartographier et repenser ses dépendances

Les trois chocs ont un point commun : ils frappent des maillons dont l'entreprise ignorait souvent qu'elle dépendait. Une mise à jour défectueuse de CrowdStrike immobilise 8,5 millions de machines en quelques heures, sans le moindre attaquant. En octobre 2026, deux failles critiques découvertes dans PHP, le langage qui fait tourner la majorité des sites web, ont exposé du jour au lendemain une grande partie des serveurs. Les entreprises restées sur d'anciennes versions n'ont même pas de correctif officiel. Une mesure américaine de contrôle des exportations suspend, du jour au lendemain, l'accès à un modèle d'IA agentique propriétaire qui pouvait être au cœur de notre chaîne de production logicielle. Que la dépendance soit physique, technologique ou juridique, la même question se pose chaque fois à l'entreprise : savait-elle qu'elle dépendait de ce maillon, et disposait-elle d'une alternative ?

Dépendre n'est pas une faute : aucune entreprise ne produit seule son Cloud, ses puces ou ses modèles. Le risque, c'est de dépendre sans le savoir, et sans plan B. L'enjeu n'est donc pas l'autarcie, mais une dépendance connue, choisie et réversible.

Pour une ESN (entreprise de services du numérique) ou un éditeur de logiciels, la question se pose deux fois, car nos dépendances sont aussi celles que nous faisons peser sur nos clients : le Cloud qui héberge notre plateforme, le fournisseur de modèles derrière notre assistant, le centre de R&D offshore qui maintient notre code. La réglementation européenne accélère le mouvement : la directive NIS2 impose de sécuriser la chaîne d'approvisionnement, le règlement DORA exige des stratégies de sortie pour les prestataires critiques, et l'AI Act encadre les systèmes d'IA utilisés. La réversibilité, la localisation et le droit applicable que nos clients nous demanderont, nous devons pouvoir l'exiger de nos fournisseurs.

Ce chantier est le socle des cinq autres : on ne protège, on ne négocie et on ne remplace que ce que l'on a identifié. Sur notre territoire, hébergeurs, éditeurs, ESN et opérateurs régionaux ont les compétences pour proposer des alternatives crédibles. Faire de la résilience un avantage compétitif, c'est l'ambition de nos adhérents.

Trois axes structurent ce chantier :

- **Identifier ses processus critiques et mesurer sa résilience,** avec des outils adaptés comme l'audit flash ou l'Indice de Résilience Numérique de l'Association for Digital Resilience Initiative (aDRI).
- **Cartographier et sécuriser sa supply chain technologique :**
  - identifier et auditer les dépendances critiques de rang 2 et 3 (fournisseurs Cloud, composants matériels et logiciels, centres de R&D offshore, prestataires), en s'appuyant sur l'inventaire des composants logiciels de ses produits (SBOM) ;
  - contractualiser des exigences strictes de cyber-résilience avec ses fournisseurs et partenaires ;
  - tester régulièrement des plans de réversibilité et de basculement vers des fournisseurs alternatifs : une réversibilité jamais testée reste théorique ;
  - bâtir un plan de continuité capable d'absorber un embargo géopolitique et de répondre aux exigences réglementaires européennes (NIS2, DORA, AI Act).
- **Adopter une stratégie de souveraineté et de régionalisation des architectures :**
  - cartographier l'exposition juridique des données stratégiques et de la propriété intellectuelle (codes sources, brevets) face aux lois extraterritoriales, comme le Cloud Act américain ;
  - développer des infrastructures modulaires permettant d'isoler géographiquement, de rapatrier, de verrouiller ou d'effacer à distance des environnements en cas de sanction internationale ou de fragmentation d'Internet en blocs géopolitiques.

Le cluster en action

- Factory Infrastructures : état de l'art, mutualisation des retours sur les offres Cloud et d'hébergement, identification des expertises de la chaîne de valeur "infrastructures" et coopération entre acteurs locaux, dialogue avec les opérateurs régionaux, concertation avec les acteurs publics sur la stratégie datacenters et infrastructures de la donnée
- Factory Décideurs IT : veille technologique partagée, du pilotage des coûts Cloud à l'hybridation HPC-quantique (calcul haute performance) explorée avec la Région.
- Mise en relation acheteurs-fournisseurs au sein de l'annuaire des adhérents, avec un repérage des alternatives régionales par type de dépendance (hébergeurs, opérateurs, éditeurs).
- Modèle de clause de réversibilité mutualisé entre adhérents.
- Exercice collectif de simulation de coupure, avec les deux Factory et la Région.
- Retours d'expérience partagés d'adhérents ayant réalisé un basculement.
- Factory Souveraineté & Résilience Numérique : traduction de l'IRN pour les PME et adoption, argumentaire sur l'avantage compétitif

Par où commencer

1. Limitez le périmètre de départ : commencez par les dix actifs numériques sans lesquels vous ne pouvez plus produire ou facturer.

2. Remplissez la matrice criticité × dépendance de ces actifs : une réunion suffit pour la première version.

3. Interrogez vos fournisseurs critiques sur leurs propres dépendances (hébergeur, sous-traitants, modèles d'IA) : c'est le moyen le plus simple d'identifier le rang 2.

4. Ajoutez une clause de réversibilité complète (formats, données, assistance, plafond de frais, etc.) à tout nouveau contrat, à l'achat comme à la vente.

5. Testez une coupure : simulez une demi-journée sans votre principal fournisseur Cloud ou sans votre assistant IA, et notez ce qui casse.

6. Passez un actif critique en double source avant fin 2027 (hébergement, messagerie, modèle d'IA…) et documentez l'opération : elle deviendra un argument commercial. Conservez aussi une sauvegarde de votre code source et de vos données clés hors de la juridiction et de l'infrastructure de votre fournisseur principal.

Chantier 3 - Se préparer à l'industrialisation de la cybermenace

Une cyberattaque n'est plus l'affaire d'un pirate isolé : elle se mène à grande échelle, avec l'aide de l'IA. La parade tient en trois réflexes : vérifier, cloisonner, et savoir reconstruire.
L'ANSSI anticipe une «augmentation massive» des attaques hybrides d'ici 2030, et l'exemple de l'attaque de Hugging Face par des agents d'OpenAI, décrite plus haut, donne un aperçu de ce passage à l'échelle.

Les entreprises de la filière du numérique doivent continuer de s'y préparer, plus sérieusement que jamais, en engageant plusieurs axes de transformation :

- **Déployer un bouclier humain et informationnel**
  - Relever le niveau de protection (authentification robuste, réduction des privilèges) et de formation des collaborateurs face à l'ingénierie sociale de niveau étatique,
  - Mettre en place une vigie réputationnelle (veille dark web et OSINT) capable de détecter et d'endiguer les campagnes de désinformation, les fuites de données, les usurpations et les deepfakes ciblant l'entreprise.
- **Refondre la résilience opérationnelle face aux attaques destructrices :**
  - Dépasser la logique de prévention pour garantir une capacité de reconstruction complète des systèmes critiques après une une compromission totale, notamment par des wipers ;
  - Mettre en œuvre des sauvegardes déconnectées du réseau (air gap) et immuables, et mesurer en conditions réelles les délais de reprise d'activité (RTO) lors de tests à grande échelle.
- **Maîtriser la dépendance aux prestataires :** cartographier les fournisseurs et éditeurs dont l'arrêt paralyserait l'entreprise, exiger d'eux des garanties de sécurité et de reprise, et prévoir un plan B pour les services vitaux.
- **Impliquer la direction dans la gouvernance cyber**
  - sensibiliser et former la direction aux risques cyber ;
  - lui confier les arbitrages de la stratégie cyber, au regard des risques identifiés ;
  - l'associer à la gestion de crise : désigner un responsable de crise, préparer un plan de gestion et de communication de crise (clients, presse, autorités) et vérifier ce que couvre réellement l'assurance cyber.

Face à cette menace, le territoire dispose d'entreprises, de compétences et d'innovations capables d'y répondre : l'enjeu est de les faire connaître et de les mettre en réseau.

En septembre 2026, Cyber'Occ, créé à l'initiative de la Région Occitanie, labellisé Campus Cyber et opérateur du CSIRT Occitanie, a lancé l'Observatoire des Menaces Cyber en Occitanie (OMCO). Son ambition est de dépasser les statistiques nationales pour construire une connaissance territorialisée des cyberattaques : localisation des victimes, secteurs touchés, nature des incidents et conséquences subies. Alimenté dans un premier temps par les données du CSIRT Occitanie et les remontées des entreprises de la filière cyber, l'observatoire a vocation à intégrer progressivement les signalements des victimes et les statistiques des forces de sécurité intérieure.

L'OMCO contribue à mieux orienter les actions de prévention et de sensibilisation, à identifier les vulnérabilités récurrentes et à adapter l'accompagnement aux réalités économiques du territoire. Pour les entreprises du numérique d'Occitanie, cette initiative ouvre également une perspective collective : en partageant leurs retours d'expérience et leurs connaissances des incidents, les acteurs de la filière peuvent contribuer à une meilleure compréhension des menaces et à l'amélioration des pratiques de leurs clients.

La résilience numérique ne repose donc pas uniquement sur les capacités individuelles des entreprises. Elle se construit aussi à l'échelle d'un territoire, par la mutualisation de la connaissance, la mobilisation des compétences et la capacité à transformer les incidents observés en actions de prévention.

Le cluster en action

- Factory Cybersécurité : avec la participation de Cyber'Occ et de l'ANSSI, elle propose des ateliers sectoriels (industrie, agri-agro, santé), des retours d'expérience entre pairs et des sujets de veille
- Formation NIS 2 : depuis 2024, le cluster propose d'anticiper l'application de la directive en décryptant le texte, afin de comprendre ses obligations et structurer sa mise en conformité en lien avec ses propres besoins et enjeux (Workshops thématiques à la carte)
- Relais des études et dispositifs nationaux (ANSSI, CNIL) et des exercices de crise vers les adhérents.
- Implication dans l'écosystème régional : partenariat Cyber'Occ, consortium EDIH OccitanIA

Par où commencer

1. Instaurez un protocole de vérification hors ligne pour toute validation sensible (paiement, changement d'IBAN, ouverture d'accès…) : un rappel sur un numéro connu déjoue le deepfake le plus soigné.

2. Activez l'authentification à deux facteurs sur la messagerie, les accès à distance et les comptes d'administration, et retirez les droits dont chacun n'a pas besoin au quotidien.

3. Sensibilisez vos collaborateurs clés (direction, finance, RH, administrateurs informatiques) : une demi-journée par an et un exercice de faux messages d'hameçonnage suffisent pour réduire fortement le risque.

4. Construisez le tableau de bord de vos prestataires critiques : cinq indicateurs par fournisseur, revus chaque trimestre.

5. Testez réellement vos sauvegardes : gardez-en une copie déconnectée du réseau, vérifiez qu'elle se restaure et chronométrer la reprise. Jouez à un exercice de crise par an. Le cas de l'éditeur Octave l'a montré : six semaines de restauration peuvent suffire à tout perdre.

Chantier 4 - Numérique Responsable et Durable : faire de la sobriété une dimension clé de la résilience numérique

Le choc climatique l'a montré : le numérique est une industrie lourde, et ses besoins en énergie, en eau et en matières premières entrent désormais en concurrence avec ceux des citoyens. Pour une entreprise de la filière, la sobriété n'est plus simplement un engagement RSE, c'est une condition de résilience. Consommer moins, c'est s'exposer moins aux hausses du prix de l'énergie, aux ruptures d'approvisionnement, aux refus de raccordement et aux oppositions locales. Le secteur fait partie du problème, par sa consommation d'énergie, l'extraction de métaux et ses déchets électroniques, mais aussi de la solution, grâce à l'optimisation et à la dématérialisation. Seule la mesure de l'impact net permet de savoir de quel côté se situe une offre.

Digital 113 travaille ce terrain depuis douze ans. The Green IT Day, la journée régionale de référence du numérique responsable, réunit chaque année ceux qui mesurent, labellisent et forment. La Factory Numérique Responsable & Durable capitalise leurs retours d'expérience dans des guides pas-à-pas. Le facilitateur NRD, la formation Label NR et la Fresque du Numérique sont au catalogue du cluster. La filière régionale possède un socle solide de compétences et d'expériences en la matière.

Le chantier consiste à passer de l'acculturation à l'industrialisation : intégrer le climat dans les plans de continuité, la sobriété dans les indicateurs de direction, les achats et la conception des produits, et préparer le reporting que clients et régulateurs vont exiger, de la CSRD pour les grandes entreprises à la loi REEN pour les collectivités de plus de 50 000 habitants.

Plusieurs axes font du Numérique Responsable & Durable une dimension clé de la résilience des entreprises et de la souveraineté numérique de nos territoires :

- **Plan de résilience climatique des infrastructures physiques.** Évaluer les risques physiques directs liés au dérèglement climatique (canicules extrêmes empêchant le refroidissement, inondations, tempêtes) pesant sur les datacenters en propre, les hébergeurs Cloud partenaires et les chaînes d'approvisionnement logistiques. Mettre à jour les Plans de Continuité d'Activité (PCA) pour y intégrer ces nouveaux scénarios de rupture.
- **Adapter sa gouvernance et ses indicateurs de performance.** Intégrer des métriques environnementales (intensité carbone, consommation énergétique par utilisateur, production de déchets électroniques) aux tableaux de bord du comité de direction, au même niveau que le chiffre d'affaires. Lier une part de la rémunération des cadres dirigeants à l'atteinte de ces limites planétaires.
- **Transformation des achats et gestion circulaire du matériel.** Mettre fin au renouvellement automatique et calendaire des parcs informatiques et des serveurs. Imposer des critères de durabilité stricts aux fournisseurs, privilégier l'achat de matériel reconditionné, systématiser la réparation interne et sécuriser les filières de recyclage certifiées pour les équipements en fin de vie.
- **Industrialiser l'écoconception logicielle et la sobriété des données.** Encourager la formation des équipes techniques (développeurs, architectes, UX/UI) au Green IT. Imposer des standards pour alléger les interfaces, optimiser le code afin de ne pas provoquer l'obsolescence matérielle chez les utilisateurs, et purger drastiquement les données dormantes (dark data) et renoncer aux modèles d'IA surdimensionnés.
- **Audit de l'impact net et lutte contre l'effet rebond (Stratégie Produit).** Systématiser les Analyses de Cycle de Vie (ACV) multicritères avant le lancement ou le maintien d'un service. Le chantier consiste à prouver que la solution commercialisée réduit effectivement l'empreinte environnementale globale de ses utilisateurs, sans provoquer une surconsommation d'usage qui annulerait les gains initiaux.
- **Anticipation réglementaire et conformité extra-financière (CSRD).** Structurer la collecte de données, le pilotage et le reporting ESG (Environnement, Social, Gouvernance). L'objectif prioritaire est de cartographier avec précision les émissions du Scope 3 (fabrication des équipements, usage par les clients), qui représentent généralement plus de 80 % du bilan carbone d'une entreprise tech, afin de se préparer aux obligations légales et fiscales.

Le cluster en action

- Factory Numérique Responsable & Durable : guides pas-à-pas, podcasts "Le Numérique Responsable Expliqué", ateliers sur la base de retours d'expérience, mutualisation des démarches. Des exemples de thématiques d'ateliers : Le NR comme un levier économique pour votre entreprise, quitter Windows pour un autre environnement, organiser un Digital Clean Up Day dans votre entreprise…
- The Green IT Day, évènement phare de Digital 113 depuis 12 ans qui confirme aujourd'hui son envergure nationale, avec des intervenants de premier plan, issus des mondes académique, institutionnel et entrepreneurial. En 2026, la thématique forte autour de la résilience numérique a réuni plus de 350 participants à Montpellier.
- Des actions de formations concrètes pour accompagner les entreprises à formaliser leurs engagements : animation de fresques, formation à l'obtention du Label NR de niveau 1, formation aux sujets d'éthique dans les usages de l'IA…

Par où commencer

1. Mesurez l'empreinte de votre service phare et publiez le chiffre : la transparence est un avantage tant qu'elle est rare.

2. Allongez d'un an la durée de vie de vos postes de travail et serveurs ; documentez l'économie réalisée.

3. Éco-concevez la prochaine version majeure de votre produit : un budget d'empreinte par fonctionnalité, arbitré comme un budget financier.

Chantier 5 - RH, RSE & Marque Employeur : souveraineté, résilience et soutien aux solutions européennes comme attracteurs de talents

Les trois chocs se jouent aussi dans les équipes. L'IA agentique déplace les métiers du code, du test et du déploiement vers la conception et la supervision des agents, la menace cyber fait de chaque collaborateur une cible autant qu'un rempart, et le climat comme la souveraineté entrent désormais dans les choix des candidats, qui veulent savoir quelle empreinte laissent leurs outils, où dorment leurs données et ce que l'IA fera de leur propre travail. Ces attentes sont un levier d'attractivité : l'entreprise capable de dire à ses développeurs à quoi ressemblera leur métier dans trois ans, comment elle encadre le travail avec les agents, ce qu'elle fait de ses données et à quels communs numériques ou solutions européennes elle contribue, dispose d'un argument qu'aucune surenchère salariale ne remplacera. Attirer et fidéliser reposent alors sur les mêmes ressorts, des parcours de formation visibles à l'alternance, de la reconversion à la féminisation des métiers pour élargir le vivier, jusqu'à la mobilité interne vers la cybersécurité, la donnée et l'IA.

Plusieurs axes structurent ce chantier :

- **Orchestration des compétences et «reskilling» IA & numérique :**
  Cartographier l'obsolescence à venir des métiers techniques (code, test, déploiement), accompagner les évolutions des métiers et compétences numériques, accompagner les collaborateurs d'un rôle de producteur à celui de concepteur, superviseur et auditeur d'agents IA autonomes.
- **Gouvernance et management du travail hybride (Humains + Agents)**
  Définir un cadre juridique et RH clair régissant l'intégration d'agents IA dans les équipes. Il s'agit de trancher les questions d'imputabilité en cas de biais ou d'erreur de l'IA, et de réinventer l'évaluation de la performance humaine.
- **Féminisation et diversité des équipes, jusqu'aux instances de direction**
  Élargir le vivier en ouvrant les métiers techniques aux femmes, aux profils en reconversion et aux parcours atypiques, fixer des objectifs de mixité mesurables dans les équipes tech, data, IA et cyber, et les étendre aux comités de direction, où la mixité est un facteur reconnu de performance et donc de résilience. Faire de cette diversité un garde-fou éthique, car des équipes plurielles conçoivent et auditent des systèmes d'IA moins biaisés.
- **Attirer les meilleurs talents par la preuve**
  Publier dans chaque offre d'emploi les éléments vérifiables sur lesquels les profils les plus disputés en IA, en cybersécurité et en data comparent désormais les employeurs : la stack et les outils réellement utilisés, la contribution à l'open source, le budget de formation par personne, la localisation des données, la part de solutions européennes, l'encadrement de l'IA dans le travail quotidien, la durée de vie et le reconditionnement du matériel. Associer les collaborateurs à ces choix, pour qu'ils puissent en interroger l'empreinte et l'usage, et faire de ces engagements de souveraineté et de résilience un argument pour recruter autant que pour fidéliser.
- **Résilience cyber et sécurité humaine**
  Face à des cyberattaques de plus en plus automatisées et dopées à l'IA, aller au-delà de la conformité technique pour faire de chaque collaborateur un maillon actif de la défense. Faire d'un socle de réflexes cyber un prérequis à l'embauche, au même titre que la maîtrise des outils, en particulier pour les fonctions RH et de direction, cibles privilégiées des attaquants. Entraîner régulièrement les équipes sur des attaques réalistes (hameçonnage ciblé, faux appels ou vidéos générés par IA, usurpation de dirigeants), installer une culture où l'on signale immédiatement un clic douteux ou une erreur plutôt que de la cacher, car chaque minute gagnée limite les dégâts, et préparer les équipes à la crise par des exercices de simulation, sans alourdir le quotidien de procédures inutiles.
- **Intégrer le numérique et l'IA au cœur de la stratégie RSE**
  Faire du numérique responsable un pilier de la politique RSE plutôt qu'un chantier technique isolé : mesurer et publier l'empreinte environnementale du numérique et de l'IA dans le reporting extra-financier de l'entreprise, ouvrir le dialogue social sur les effets de l'IA sur l'emploi, les conditions de travail et les compétences, garantir l'accessibilité des services numériques aux personnes en situation de handicap, et appliquer des critères environnementaux, éthiques et de souveraineté à chaque achat numérique, du matériel aux services d'IA.

Le cluster en action

- Factory RH, RSE & Marque Employeur : un programme d'atelier correspondant aux véritables sujets de préoccupation des entreprises de la filière : (grille des salaires, motivation des équipes, directive sur la transparence des salaires, mobilisation d'une politique RSE durable…)

- Femmes Digitales : le Podcast des Femmes Digitales a pour vocation de mettre en lumière des femmes qui compose les entreprises du numérique en Occitanie : cheffes de projet, directrices, développeuses, reconversion ou vocation… nous multiplions les sujets et les rôles modèles dans un seul objectif : multiplier les intentions d'orientation des femmes vers la filière

- La Digital Academy (centre de formation certifié Qualiopi) propose des formations sous format collectif, pour maintenir les compétences des collaborateurs à l'ère de l'IA, structurer des démarches de conformités, et participer à la fidélisation des collaborateurs via le maintien de leurs compétences.

  Focus formation IA for code : offre de formation proposée pour augmenter la productivité des métiers techniques tout en remplaçant les collaborateurs au cœur de la valeur. La transformation profonde des pratiques professionnelles sur 3 métiers techniques choisis (développeurs, testeurs, PO-PM) déplace l'humain vers des nouvelles dimensions stratégiques : la compréhension du métier, la prise de décision, la créativité, la supervision et l'esprit critique.

Par où commencer

1. Ajoutez trois preuves vérifiables à chaque offre d'emploi : la stack exacte, la politique de contribution open source, le budget formation par personne.

2. Formalisez un droit de contribution aux communs numériques et/ou aux projets open source : temps alloué, licences autorisée.

3. Revoyez la rédaction des offres d'emploi : anticipez la directive sur la transparence des salaires, rédigez de façon inclusive, anticipez les sujets d'évolutions professionnelles en lien avec les mutations.

4. Rédigez une charte d'usage de l'IA au travail : ce qui est autorisé, ce qui est encadré, qui reste responsable.

5. Intégrez un socle cyber dès l'arrivée de chaque collaborateur, et veillez à entretenir les compétences tous les ans.

Chantier 6 - Usages, data et IA : déployer de la valeur garder la main sur l'inférence

Le choc de l'IA générative a ouvert un premier marché : déployer les assistants et les agents chez les clients de la région,qu'il s'agisse d'industriels, d'établissements de santé, d'entreprises agroalimentaires ou de collectivités. Ces projets demandent de choisir des cas d'usage aux gains mesurables, de préparer les données, de former les équipes, d'encadrer les usages et respecter les exigences de l'AI Act, le règlement européen sur l'IA dont les obligations s'échelonnent depuis février 2025. Leur réussite dépend d'abord de la qualité des données et de la connaissance du métier : sans référentiels propres, sans contrôle de la qualité et sans gestion des droits d'accès, un agent ne produit rien de fiable. Ce travail de gouvernance des données est peu visible, mais c'est souvent lui qui rapporte le plus, car il répond directement aux besoins du terrain.

En parallèle se pose la question de l'exécution de ces agents et assistants. Si l'entraînement des modèles fait les gros titres, c'est l'inférence, leur exécution au quotidien, qui génère les volumes, les factures et les dépendances pour les utilisateurs. Les principaux modèles sont américains mais des alternatives européennes, chinoises ou en poids ouverts existent et commencent à s'imposer sur le terrain. Le choix des serveurs sur lesquels tournent ces modèles a des conséquences directes sur la marge et sur l'exposition juridique. En gardant la maîtrise de l'inférence, la filière peut faire en sorte que ce marché profite à ses entreprises et à leurs clients plutôt qu'à leurs fournisseurs.

Enfin, la filière doit appliquer à sa propre production ce qu'elle vend à ses clients: maîtrise des flux de données et les modèles qu'elle utilise, protéger la confidentialité des données, et s'appuyer sur l'écosystème régional pour aller plus vite.

Plusieurs axes structurent ce chantier :

- **Choisir des cas d'usage à retour mesurable, filière par filière.** Partir des besoins des filières clientes suivies par Digital is Future (agri-agro, bâtiment, industrie, santé, secteur public, mobilité), retenir les cas d'usage agentiques dont le gain se mesure en temps, en qualité ou en coût, et documenter les pilotes abandonnés autant que les succès. La Factory Usages, Data & IA est le lieu où ces retours de déploiement se partagent entre pairs.
- **Traiter la gouvernance des données comme le prérequis de tout projet d'IA.** Référentiels propres, qualité mesurée, droits d'accès maîtrisés, classification des données sensibles et de celles que les clients nous confient, et réponse documentée à la question que la Factory instruit avec la Factory Cybersécurité : où vont les données quand l'IA les utilise ?
- **Garder la main sur l'inférence.** Décider où tournent les modèles (Cloud extra-européen, Cloud de confiance, on-premise) selon la sensibilité des données, suivre le coût d'inférence par cas d'usage dès le premier jour, éviter la dépendance à un fournisseur unique de modèles en qualifiant des alternatives européennes ou en poids ouverts, et inscrire la réversibilité (prompts, données, jeux d'évaluation) dans les contrats dès le pilote.
- **Industrialiser l'IA dans la production logicielle.** Déployer les assistants et agents de code, de test et de documentation avec des règles explicites sur ce qui sort de l'entreprise (code source, données clients, secrets), mesurer les gains et former les équipes : la formation "IA for code" du cluster couvre développeurs, DevOps, product owners et testeurs.
- **Encadrer les usages et se conformer à l'AI Act.** Recenser les systèmes d'IA utilisés ou vendus et les classer par niveau de risque, adopter une charte d'usage interne, satisfaire l'obligation de maîtrise de l'IA des collaborateurs applicable depuis février 2025, et documenter la transparence attendue par les clients. La formation "AI Act" du cluster structure cette mise en conformité.
- **S'appuyer sur l'écosystème régional pour aller plus vite.** Pour des cas d'usages opérationnels, proches du terrain, les acteurs du numérique sont le chaînon manquant permettant d'aller rapidement au résultat. Digital 113 agit en tant que facilitateur et tiers de confiance pour faciliter cette mise en relation locale et accélérer la mise en mouvement (284 acteurs recensés en Occitanie, entreprises, laboratoires et formations). Pour les cas d'usage centrés sur le développement solutions innovantes permettant d'adresser de nouveaux marchés, sur un temps plus long, les entreprises peuvent mobiliser l'EDIH OccitanIA pour tester avant d'investir et financer les premières étapes avec le relais d'ANITI pour les sujets de recherche avancés.

Le cluster en action

- Factory Usages, data & IA, et Digital is Future : cas d'usage sectoriels, démarche pour structurer l'approche de gouvernance des données et cadrage des chantiers de données à mener, retours de déploiement entre pairs.
- La cartographie régionale des acteurs de l'IA, plus de 140 acteurs recensés : chercheurs, entreprises, formations.
- EDIH OccitanIA, un guichet pour faciliter les projets innovants en Occitanie.
- Les formations "AI Act" et "IA for code", de la Digital Academy.
- Les rendez-vous du programme Digital is Future pour diffuser les usages dans les filières clientes : Agri/Agro, Bâtiment, Industrie, Santé, Secteur Public et Transport & Mobilité.
- Implication dans l'écosystème régional et national : co-animation du Comité Technique IA du Contrat de Filière Numérique de la Région Occitanie, membre du bureau d'IA Montpellier Méditerranée, partenariat ANITI ; partenaire du Hub France IA et jury de sa cartographie; Ambassadeur IA, partenaire de l'Observatoire Maturité Data & IA des Entreprises (OMDIE).

Par où commencer

1. Sélectionnez trois cas d'usage agentiques à retour mesurable, et inscrivez la réversibilité au contrat dès le pilote.

2. Suivez le coût d'inférence par cas d'usage dès le premier jour : c'est lui qui décidera de la marge à l'échelle.

3. Formez une personne par équipe : AI Act pour le cadre, IA for code pour la pratique.

4. Challengez le choix des modèles et outils en fonction des exigences de territorialité, confidentialité autant que de simples performances et coûts.

5. Évaluez la pertinence d'une inférence locale pour les projets au contenu sensible.

Conclusion

La Factory Souveraineté et Résilience Numérique propose d'assurer le suivi de ce manifeste : diffusion de l'audit flash, accompagnement des trajectoires IRN, partage annuel des progrès et des retours d'expérience entre signataires.

Cette note n'est pas un document figé. Les chocs qu'elle décrit évoluent vite, et elle évoluera avec eux : les retours d'expérience des signataires, les travaux des Factory Digital 113 et l'actualité de la filière viendront l'enrichir au fil de ses prochaines versions. Chaque entreprise qui partage ce qu'elle a testé et ce qu'elle en a appris la rend plus utile pour toutes les autres.

Pour signer le manifeste, rejoindre la Factory ou partager votre expérience : contactez-nous.

La résilience numérique se construit décision après décision, contrat après contrat, et elle se joue en filière.

Annexes

Annexe 1 - Qui fait quoi en Occitanie quant à la souveraineté et la résilience numérique ?

Liste non exhaustive, construite notamment à partir des signataires et partenaires du Contrat de Filière Numérique.

- **Digital 113 :** le cluster des entreprises du numérique — Factory, formations (NIS 2, AI Act, Label NR, IA for code), EDIH OccitanIA, The Green IT Day, Digital is Future, relations institutionnelles.
- **Cyber'Occ :** le centre régional de ressources en cybersécurité — sensibilisation, assistance, mise en réseau.
- **Région Occitanie** / **Ad'Occ :** Stratégie Régionale de l'Innovation, Contrat de Filière, accompagnement des entreprises.
- **Écosystème :** Aerospace Valley, French Tech Toulouse et French Tech Méditerranée, La Mêlée, IoT Valley, Ekitia (données), ANITI (recherche en IA), Numeum, Opco Atlas, Apec.

Annexe 2 - Contributeurs

- **Denis Lafont-Trévisan -** GrowthSeeds
- **Gillo Malpart -** Mavana
- **Pierre Baudracco -** Bluemind
- **Magali Germond -** LumIAire Conseils / Numeum Occitanie
- **Alain Abboud -** Sopra Steria
- **Karim Seddaoui -** Hérault Logement / Kopsi
- **Amélie Leclercq -** Digital 113
- **Mathilde Alarçon -** Digital 113
- **Maud Chauvet -** Digital 113
- **Françoise Nauton-Inglis -** Spiriit
- **Simon Bretin -** Flutilliant
- **Arnaud Ladrière -** Digital 113
- **Frédéric Muh -** BEA Solutions
- **Gaël Philippe -** Datasulting
- **Pierre Tarradas -** Lazar Soft
- **Patrick Séguéla -** Synapse Développement
- **Jean-François Escala -** Consultil
- **Anne Cordel -** Arcade
- **Fabrice Vincent -** Ubika
- **Julien Lopez -** DigitRE
- **Jean-Philippe Fontana -** Itesoft
- **Laurent Lacaze -** Lthirteen
- **Virginie Berlier -** Addon groupe
- **Arno Pons -** Digital New Deal/aDRI

Annexe 2 - Grille IRN

L'indice de résilience numérique (IRN), développé par l'Association for Digital Resilience Initiative (aDRI), n'est pas seulement un outil de diagnostic. C'est un cadre commun qui permet à une organisation de mesurer ses dépendances numériques, de hiérarchiser les risques qu'elles portent et de construire une trajectoire de progrès. Il prolonge ainsi l'audit flash : l'audit donne une première photographie de la situation, l'IRN permet de suivre sa progression dans le temps.

L'IRN s'adresse à toutes les organisations : TPE et PME, grandes entreprises, acteurs industriels et collectivités. Il peut être utilisé à deux niveaux :

- **en libre appropriation :** chaque organisation peut s'emparer du référentiel pour réaliser son propre diagnostic ;
- **avec un accompagnement structuré** par des professionnels agréés, qui peut conduire à une labellisation.

La démarche ne consiste pas à privilégier par principe les solutions européennes. Elle consiste d'abord à connaître ses dépendances, à en mesurer les risques et à disposer d'alternatives crédibles. L'IRN met l'accent sur la progression : ce qui compte est moins le niveau de départ que la trajectoire engagée.

Le référentiel compte 30 critères, répartis en huit piliers. Certains portent sur l'organisation dans son ensemble, d'autres s'évaluent actif par actif : une plateforme cloud, un logiciel métier ou un service critique.

- Résilience stratégique : gouvernance du numérique, implication de la direction, encadrement des usages de la data et de l'IA.
- Résilience économique et juridique : nationalité des fournisseurs, exposition aux lois extraterritoriales, poids d'un fournisseur dans les dépenses, pouvoir de négociation.
- Résilience data et IA : localisation, cartographie, portabilité et disponibilité des données.
- Résilience opérationnelle : capacité à opérer en autonomie, disponibilité des compétences, continuité d'activité.
- Résilience de la supply chain : dépendance aux fournisseurs extraterritoriaux, transparence de la chaîne d'approvisionnement.
- Résilience technologique : interopérabilité, portabilité, ouverture du code, obsolescence, télécommunications.
- Sécurité et résilience : certifications, gestion des vulnérabilités et des correctifs, localisation des journaux et du SOC.
- Résilience environnementale et énergétique : approvisionnement énergétique des datacenters, aléas climatiques.

Le référentiel complet et la grille d'évaluation sont disponibles ici : https://gitlab.com/digitalresilienceinitiative/adri-irn

Référentiel IRN v1.2 – © 2026 aDRI. Diffusé sous licence Creative Commons CC BY-NC-ND 4.0.

Annexe 3 – Glossaire

AI Act : Règlement européen sur l'intelligence artificielle, obligations échelonnées selon le niveau de risque.

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

Data Act : Règlement européen sur les données ; il programme la fin des frais de sortie du Cloud.

Deepfake : Faux contenu audio ou vidéo très réaliste, généré par intelligence artificielle.

Digital is Future : Programme porté par Digital 113 dédié à la transformation numérique des filières. Il propose un parcours sur mesure composé de différents événements et contenus afin de mettre en lumière une filière et ses besoins et ainsi favoriser le business en Région Occitanie.

DORA : Règlement européen de résilience opérationnelle du secteur financier.

DSI : Direction des systèmes d'information.

EDIH : European Digital Innovation Hub, guichet européen d'accompagnement numérique.

ERP : Progiciel de gestion intégré.

ESN : Entreprise de services du numérique.

Factory : Groupe de travail thématique où les entreprises du numérique se réunissent pour échanger, partager leurs pratiques et construire ensemble des solutions concrètes pour la filière.

GPU : Processeur graphique, moteur de calcul de l'IA.

IA agentique : Systèmes d'IA qui exécutent des tâches, au-delà de la seule réponse.

IRN : Indice de Résilience Numérique.

Label NR : Label porté par l'Institut du Numérique Responsable (INR), qui reconnaît les organisations engagées dans une démarche de réduction des impacts environnementaux, sociaux et économiques de leur numérique.

NIS2 : Directive européenne de cybersécurité.

Ransomware-as-a-service : Rançongiciel commercialisé clé en main.

Reskilling» IA : Le reskilling IA consiste à accompagner les salariés dans l'acquisition de nouvelles compétences, notamment numériques et liées à l'intelligence artificielle, afin de leur permettre de s'adapter à l'évolution des métiers

SaaS : Logiciel fourni en ligne par abonnement.

Sauvegarde air -gap : Copie des données déconnectée du réseau, donc hors de portée d'un attaquant.

SecNumCloud : Qualification de Cloud de confiance délivrée par l'ANSSI.

SRI : Stratégie Régionale de l'Innovation.

Ingénierie sociale : La faille la plus redoutable en cybersécurité ne réside pas toujours dans un logiciel mal configuré ou une vulnérabilité technique, mais souvent dans l'humain lui-même. L'ingénierie sociale exploite ce point faible en manipulant les émotions, la confiance ou la naïveté pour accéder à des données sensibles. Cette approche illustre combien la protection technique, aussi robuste soit-elle, peut être contournée par une simple interaction humaine malveillante

Wiper : Logiciel malveillant qui détruit les données au lieu de les voler ou de les chiffrer contre rançon.

Annexe 4 - Bibliographie

- Note de position doctrinale du Cigref (4 juin 2026) : https://www.cigref.fr/souverainete-et-resilience-numeriques-note-de-position-doctrinale-du-cigref
- Communiqué de presse "Vers une Europe numérique souveraine : la France et l'Allemagne passent à l'action" https://presse.economie.gouv.fr/vers-une-europe-numerique-souveraine-la-france-et-lallemagne-passent-a-laction/
https://mavana.earth/lia-consomme-de-plus-en-plus-denergie/
- Denis Lafont-Trévisan - « Dépendances numériques : géopolitique, IA et cybermenaces : prendre l'avantage » (sortie prévue le 30/11/2026), https://iDgitalShifts.eu
- Abstract of the Draft Outline of the 15th Five-Year Plan for National Economic and Social Development of the People's Republic of China (Source : National People's Congress Website). (s. d.). Consulté 23 août 2026, à l'adresse http://www.npc.gov.cn/npc/c2/kgfb/202603/t20260305_452076.html
- Bloj, R. (2026, juillet 3). Palantir et l'illusion de la souveraineté (texte commenté). Le Grand Continent. https://legrandcontinent.eu/fr/2026/07/03/palantir-et-lillusion-de-la-souverainete-texte-commente/
- Cigref. (2025, avril 25). La dépendance technologique aux softwares & cloud services américains : Une estimation des conséquences économiques en Europe. Cigref. https://www.cigref.fr/la-dependance-technologique-aux-softwares-cloud-services-americains-une-estimation-des-consequences-economiques-en-europe
- Cigref. (2026, mai 28). De la dépendance technologique à la captation économique : Ce que les hausses tarifaires du cloud-logiciel coûtent à l'Europe. Cigref. https://www.cigref.fr/de-la-dependance-technologique-a-la-captation-economique-ce-que-les-hausses-tarifaires-du-cloud-logiciel-coutent-a-leurope
- Clare, M. A., Yeo, I. A., Bricheno, L., Aksenov, Y., Brown, J., Haigh, I. D., Wahl, T., Hunt, J., Sams, C., Chaytor, J., Bett, B. J., & Carter, L. (2023). Climate change hotspots and implications for the global subsea telecommunications network. Earth-Science Reviews, 237, 104296. https://doi.org/10.1016/j.earscirev.2022.104296
- Cloud and AI Development Act | Shaping Europe's digital future. (s. d.). Consulté 27 juillet 2026, à l'adresse https://digital-strategy.ec.europa.eu/en/policies/cloud-and-ai-development-act

- Coelho, O. (2025). Géopolitique du numérique : L'impéralisme à pas de géants. Editions de l'Atelier. https://editionsatelier.com/boutique/accueil/511-geopolitique-du-numerique--9782708295384.html
- Communication on European Tech Sovereignty, accompanied by an EU Open Source Strategy | Shaping Europe's digital future. (s. d.). Consulté 27 juillet 2026, à l'adresse https://digital-strategy.ec.europa.eu/en/library/communication-european-tech-sovereignty-accompanied-eu-open-source-strategy
- Draghi, M. (s. d.-a). L'avenir de la compétitivité européenne Partie A | Une stratégie de compétitivité pour l'Europe. Consulté https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_fr?filename=The%20Draghi%20report%20A%20competitiveness%20strategy%20for%20Europe%20%28Part%20A%29-FR.pdf
- Draghi, M. (s. d.-b). The future of European competitiveness Part B | In-depth analysis and recommendations.
- Général Bruno Clermont : « Nous ne sommes pas en guerre contre la Russie, mais… ». (2026, août 3). Le Figaro. https://www.lefigaro.fr/vox/monde/general-bruno-clermont-nous-ne-sommes-pas-en-guerre-contre-la-russie-mais-20260803
- Ghaleb, T. A. (2026). Fingerprinting AI Coding Agents on GitHub. Proceedings of the 23rd International Conference on Mining Software Repositories, MSR '26, 822-826. https://doi.org/10.1145/3793302.3793582
- Khosravani, A., & Mockus, A. (2026). Detecting AI Coding Agents in Open Source : A Validated Multi-Method Census of 180 Million Repositories (arXiv:2606.24429). arXiv. https://doi.org/10.48550/arXiv.2606.24429
- Korben. (2026, juillet 27). CXMT, le chinois vient bousculer les trois géants de la mémoire—Korben. Le site de Korben. https://korben.info/cxmt-le-chinois-vient-bousculer-les-trois-geants-de-la-memoire.html
- La Commission présente un paquet pour renforcer la souveraineté technologique de l'Europe—Représentation en France. (s. d.). Consulté 27 juillet 2026, à l'adresse https://france.representation.ec.europa.eu/informations-et-evenements/informations/la-commission-presente-un-paquet-pour-renforcer-la-souverainete-technologique-de-leurope-2026-06-03_fr
- Le devoir de souveraineté numérique. (s. d.). Assemblée Nationale. Consulté 19 juillet 2026, à l'adresse https://www.senat.fr/rap/r19-007-1/r19-007-1.html
- Lechelle, Y. (s. d.). Ouvertarisme : Le Numérique des Lumières. (Édition originale 2026)
- Li, H., Zhang, H., & Hassan, A. E. (2026). AIDev : Studying AI Coding Agents on GitHub. Proceedings of the 23rd International Conference on Mining Software Repositories, MSR '26, 1029-1033. https://doi.org/10.1145/3793302.3797249
- Liste des. Bonnes sources universitaire. (s. d.). Consulté 28 juillet 2026, à l'adresse https://www.linkedin.com/posts/ireneeregnauld_jai-lu-technopolitique-comment-la-technologie-activity-7197105815604920320-l4Sx/
- Longuet, G., & Montaugé, F. (2019, octobre 3). Commission d'enquête sénatoriale sur la souveraineté numérique. Sénat. https://www.senat.fr/travaux-parlementaires/structures-temporaires/commissions-denquete/commissions-denquete/commission-denquete-sur-la-souverainete-numerique.html
- L'opacité de l'industrie de l'IA électrifie les débats sur la multiplication des nouveaux centres de données—Le Temps. (2026, août 3). https://www.letemps.ch/cyber/intelligence-artificielle/l-opacite-de-l-industrie-de-l-ia-electrifie-les-debats-sur-la-multiplication-des-nouveaux-centres-de-donnees
- L'Union européenne, colonie du monde numérique ? (2023, avril 3). Sénat. https://www.senat.fr/rap/r12-443/r12-443.html
- Malik, M. (2025, septembre 25). Les citoyens veulent-ils vraiment de la souveraineté numérique ? 10 points sur une enquête mondiale. Le Grand Continent. https://legrandcontinent.eu/fr/2025/09/25/souverainete-technologique-10-points/
- Mario Draghi remet son rapport sur la compétitivité européenne à Ursula von der Leyen—SGAE. (s. d.). Consulté 19 juillet 2026, à l'adresse https://sgae.gouv.fr/sites/SGAE/accueil/a-propos-du-sgae/archives/mario-draghi-remet-son-rapport-s.html
- Mistral AI, Quantum Systems… « Qui va financer l'innovation de rupture en Europe? »—Les Echos. (s. d.). Consulté 20 juillet 2026, à l'adresse https://www.lesechos.fr/idees-debats/cercle/mistral-ai-quantum-systems-qui-va-financer-linnovation-de-rupture-en-europe-2242754
- Assemblée Nationale (2026). Commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France. Assemblée Nationale. https://www.assemblee-nationale.fr/dyn/17/organes/autres-commissions/commissions-enquete/ce-vulnerabilites-numeriques/documents?typeDocument=rapport%20d%27enqu%C3%AAte
- Njoku, A. O., Sharafi, Z., & Khomh, F. (2026). When Code Authors Are Agents : A Large-Scale Study of Human–Agent Collaboration in Pull Requests. https://openreview.net/forum?id=ArurxAmCtR

- Nora, D., & Minc, A. (1978, février 21). L'informatisation de la societe | Vie publique. https://www.vie-publique.fr/rapport/34772-linformatisation-de-la-societe
- Proposal for the Cloud and AI Development Act (CADA) | Shaping Europe's digital future. (s. d.). Consulté 27 juillet 2026, à l'adresse https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada
- Raida, M. N., & Hou, D. (2026). Early Adoption of Agentic Coding Tools by GitHub Projects (arXiv:2607.14037). arXiv. https://doi.org/10.48550/arXiv.2607.14037
- Règlement européen sur les semi-conducteurs | Bâtir l'avenir numérique de l'Europe. (2026, juillet 14). https://digital-strategy.ec.europa.eu/fr/policies/european-chips-act
- Robbes, R., Matricon, T., Degueule, T., Hora, A., & Zacchiroli, S. (2026). Agentic Much? Adoption of Coding Agents on GitHub (arXiv:2601.18341). arXiv. https://doi.org/10.48550/arXiv.2601.18341
- Tech for Industry Show. (2026, juillet 1). TFIS 2026 : La Souveraineté Numérique pour les Acteurs Industriels [Enregistrement vidéo]. https://www.youtube.com/watch?v=r6WQFLwYhbw
- The EU Open Source Strategy | Shaping Europe's digital future. (2026, juillet 24). https://digital-strategy.ec.europa.eu/en/policies/open-source-strategy