DES SERVICES PUBLICS PLUS SÛRS GRÂCE AU CLOUD

Capgemini

Solution sélectionnée par UGAP

CLOUD ET SECTEUR PUBLIC,
LES CLÉS D'UN MARIAGE PROMETTEUR

La révolution numérique s'organise autour des plateformes, qui mettent en relation des clients ou des usagers et des fournisseurs de biens et de services.

Elles créent de la valeur en connaissant les besoins des premiers et les capacités des seconds à y répondre.

Pour cela, elles doivent capter, brasser, analyser d'énormes quantités de données afin d'orienter, anticiper, optimiser les choix des uns et des autres.

Le cloud s'est naturellement imposé comme l'architecture technologique privilégiée de ce modèle grâce à ses capacités presque sans limite et à son aptitude à se reconfigurer.

Ayant vocation à fournir un large éventail de services à des citoyens qui attendent des réponses toujours plus rapides et personnalisées, les organisations publiques sont elles aussi incitées à adopter le modèle de la plateforme, et donc le cloud.

Cependant, les données qu'elles manipulent sont particulièrement sensibles, et elles ont donc, en termes de sécurité, de confidentialité, de traçabilité et de conformité, de très fortes exigences.

Par ailleurs, cette évolution reste soumise à l'obligation de continuité et d'universalité du service public, ce qui ajoute des impératifs supplémentaires de sûreté, d'accessibilité et de résilience.

Les acteurs publics sont donc tiraillés entre les attentes de dématérialisation des services exprimées par les citoyens, les agents et les décideurs politiques, et des exigences renforcées de sécurité dans un contexte où les menaces se multiplient.

Entre 2019 et 2020, avant même la crise sanitaire, l'ANSSI faisait ainsi déjà état d'une hausse de 255 % des attaques par rançongiciels, lesquelles visent plus particulièrement les collectivités et les secteurs de la santé et de l'éducation.

Les organisations publiques peuvent aussi être la cible d'attaques d'activistes, de malfaiteurs ou d'États cherchant à voler des informations, à paralyser les systèmes ou à les détruire.

Dans tous les cas, aux coûts techno-logiques et financiers, s'ajoutent de lourdes conséquences humaines pour le personnel et la population.

Dans ces conditions, le basculement vers le cloud suscite, au sein du secteur public, des craintes légitimes.

On redoute de perdre le contrôle sur ses données, de moins maîtriser ses systèmes, d'être davantage exposé aux cyberattaques, de ne pas se conformer à la réglementation…

La souveraineté et la réversibilité, qui garantissent l'autonomie d'action et de décision, sont des préoccupations majeures.

Si l'on ajoute qu'il a longtemps été difficile de faire entrer le modèle du paiement à l'usage du cloud dans le cadre strict des achats publics, tout ceci explique que le mariage prometteur entre cloud et secteur public a pu tarder à se concrétiser.

Aujourd'hui, pourtant, ces craintes n'ont plus lieu d'être. Des solutions techniques, organisationnelles, juridiques existent pour faire du cloud une plateforme à la fois adaptée aux enjeux des organisations publiques et plus sûre face aux cybermenaces que ne le seraient leurs propres infrastructures.

Mais une certaine méconnaissance de ces solutions et du cadre réglementaire dans lequel elles s'inscrivent reste un frein à leur adoption.

Clarifier les points essentiels pour aider les acteurs publics à choisir leur voie vers un cloud sécurisé et maîtrisé au service des citoyens et des agents, tel est l'objectif de ce document.

LE CADRE
NORMATIF ET RÉGLEMENTAIRE

Les acteurs publics sont particulièrement vigilants à la conformité des solutions qu'ils mettent en œuvre ainsi qu'au risque juridique qui peut peser sur leurs systèmes et sur les données qu'ils contiennent.

C'est pourquoi les incertitudes qui entourent parfois le cadre normatif et réglementaire, national et international, ont pu être un frein à l'adoption du cloud dans le secteur public.

Afin d'y voir enfin clair, voici très succinctement les principaux textes et labels à connaître et prendre en compte.

En France

SecNumCloud

SecNumCloud est une qualification de sécurité définie par l'ANSSI (Agence nationale de la sécurité des systèmes d'information) à destination des opérateurs proposant, dans le cloud, des services PaaS (Platform as a Service), IaaS (Infrastructure as a Service) et SaaS (Software as a Service).

Pour être qualifié SecNumCloud, le prestataire doit prouver auprès d'auditeurs agréés que son service respecte les bonnes pratiques de sécurité physique, organisationnelle et juridique établies par le référentiel.

SecNumCloud s'appuie notamment sur les exigences de sécurité issues des normes internationales du secteur, comme l'ISO 27001, l'ISO 27017 et l'ISO 27018.

Dans sa version 3.2, SecNumCloud fixe des exigences supplémentaires sur la localisation des services et la nationalité du fournisseur afin de garantir « l'immunité au droit non communautaire » :
héberger les données en France ; gérer les services depuis un pays européen ; être une entreprise européenne, détenue en majorité par des acteurs européens.

Cette nouvelle version de SecNumCloud servira de base au label « Cloud de confiance » (voir le chapitre « La stratégie de l'État »).

HDS

Les données de santé font l'objet d'une réglementation particulière et renforcée.

Depuis le 1er avril 2018, il faut, pour héberger des données de santé, obtenir une certification HDS (Hébergeur de Données de Santé) auprès d'un organisme certificateur indépendant.

Il existe deux types de certificats, « Hébergeur d'infrastructure physique » et « Hébergeur infogéreur ».

Le premier couvre les sites physiques et les infrastructures matérielles ; le second, les plateformes d'hébergement, l'infrastructure logicielle, l'administration et l'exploitation des systèmes,
et la sauvegarde des données.

En Europe

RGPD

Entré en vigueur en mai 2018, le RGPD (Règlement général sur la protection des données) encadre la collecte, l'utilisation et la conservation de données personnelles des citoyens européens.

Est considérée comme une donnée personnelle toute information qui se rapporte à une personne physique, identifiée ou identifiable.

L'organisation est tenue de recenser les données personnelles qu'elle détient (sur ses clients, fournisseurs, salariés, agents…), de lister les traitements qu'elle leur applique, de recueillir le consentement des personnes concernées, et, si celles-ci le demandent, d'effacer ou de leur restituer leurs données.

Les implications de tout nouveau projet doivent également être évaluées en amont afin de prendre d'emblée les mesures de protection appropriées (privacy by design).

Enfin, le RGPD portant sur les données elles-mêmes, il s'applique de la même façon où qu'elles se trouvent, dans un data center, un cloud privé ou un cloud public.

Gaia-X

Gaia-X est une initiative privée soutenue par l'Allemagne et la France, dont l'objectif est de proposer des standards pour la création de services cloud et de promouvoir la création d'espaces de données sectoriels mutualisés.

Les participants à Gaia-X doivent adhérer à des principes d'interopérabilité, de portabilité, de réversibilité et de transparence.

Ceci n'exclut donc pas les acteurs extraeuropéens, qui ne peuvent cependant pas intégrer la gouvernance du projet.

Dans le monde

Normes iso/cei 27000

La famille de normes ISO/CEI 27000 regroupe les normes internationales en matière de sécurité de l'information et constitue un référentiel de bonnes pratiques.

La norme ISO 27001, révisée en 2013, établit en particulier une liste d'exigences permettant la certification.

Publiée en 2015 et spécifiquement dédiée au cloud, la norme ISO 27017 apporte des garanties sur les sécurités techniques, juridiques et organisationnelles – offertes par les prestataires.

La norme ISO/CEI 27701, publiée en 2019, complète quant à elle l'ISO/CEI 27001 avec des exigences spécifiques sur la protection des données personnelles.

Audits SOC

Les rapports SOC (Service Organisation Controls), déclinés en SOC 1, SOC 2 et SOC 3, sont des cadres de référence établis par l'American Institute of Certified Public Accountants (AICPA) pour rendre compte des dispositifs de contrôle internes mis en place dans une entreprise. Ils sont rédigés suite à des audits indépendants réalisés par des tiers reconnus.

En particulier, le rapport SOC2 couvre la sécurité, la confidentialité, l'intégrité et la disponibilité, et le rapport SOC3 couvre la sécurité, la confidentialité, l'intégrité et la disponibilité.

Les audits SOC constituent un élément important de la surveillance réglementaire, des programmes de gestion des fournisseurs, de la gouvernance interne et de la gestion des risques.

C.L.O.U.D. Act

Adopté en 2018, le C.L.O.U.D. (Clarifying Lawful Overseas Use of Data) Act est une loi américaine qui permet aux autorités munies d'un mandat judicaire de demander à une entreprise fournissant des services de communication électronique, sous le contrôle d'un juge, la transmission des données nécessaires à la conduite d'enquêtes criminelles ou terroristes.

Le C.L.O.U.D. Act s'impose à tous les fournisseurs de cloud, quelle que soit leur nationalité, dès lors qu'ils ont une activité aux Etats-Unis ou qu'ils entretiennent une relation avec les Etats-Unis.

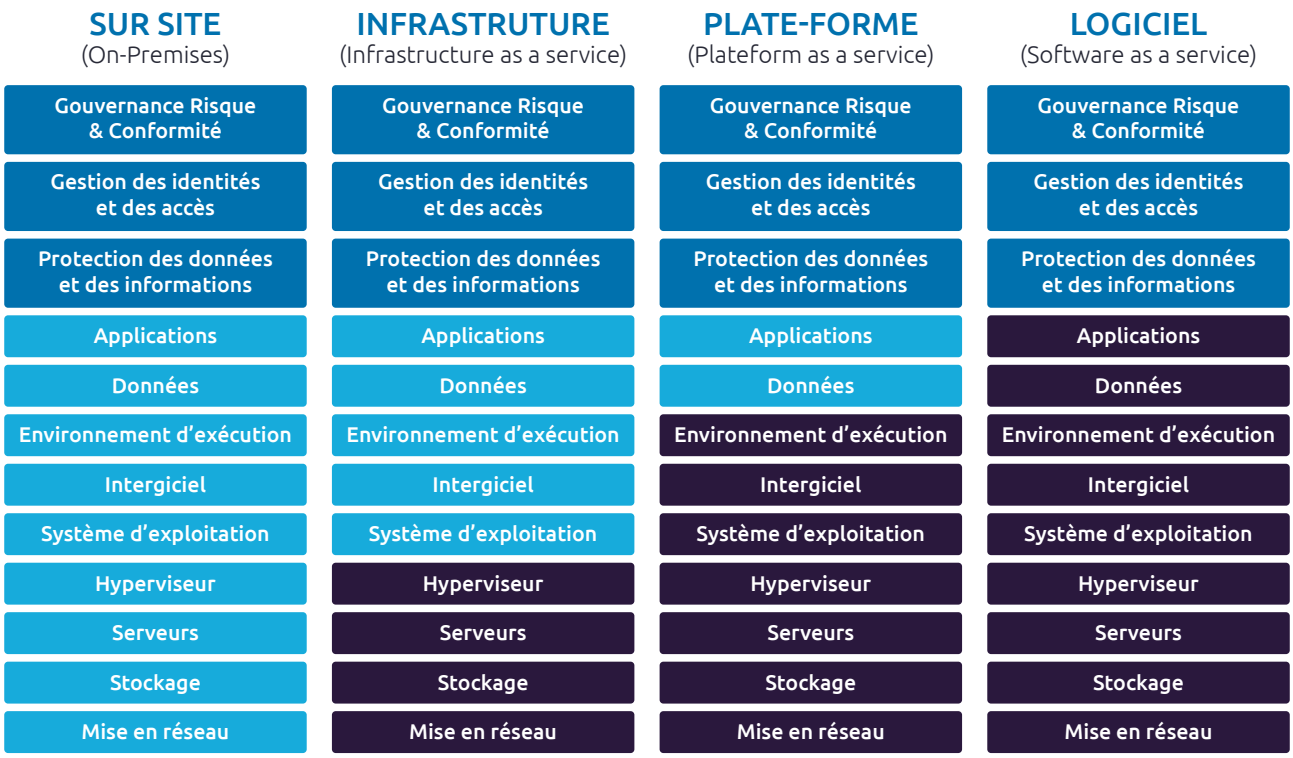
Il est important de noter que le C.L.O.U.D. Act reconnaît la possibilité pour les entreprises de contester les demandes des autorités, en particulier lorsqu'elles ne respectent par la législation du pays où sont stockées les données. Ainsi, le RGPD offre un moyen juridique de contestation pour les données hébergées en Union Européenne.

LE CLOUD,
UN SOCLE ULTRA- SÉCURISÉ

Forme d'externalisation de ressources techniques, le cloud repose, en matière de sécurité, sur un principe de responsabilités partagées. Il revient au prestataire de sécuriser les systèmes qu'il met à la disposition de son client et à celui-ci de sécuriser tout ce qui lui est propre. On parle de sécurité du cloud pour le premier et de sécurité dans le cloud pour le second.

La frontière – et donc l'étendue du périmètre qui incombe au client – dépend du type de service souscrit, IaaS, PaaS ou SaaS (respectivement Infrastructure, Platform et Software as a Service). Dans le cas de l'IaaS, l'opérateur de cloud ne fournit que des ressources « brutes », matérielles (processeurs, mémoire…) et réseau (routeurs, pare-feux…). La responsabilité du client est maximale car il doit gérer toute la pile technique depuis le système d'exploitation. Ajoutant à l'IaaS des couches d'infrastructure logicielle (système d'exploitation, base de données…), les offres PaaS fournissent un environnement d'exécution complet. Le client peut y déployer ses applications à sa guise, à charge pour lui d'en sécuriser les accès et le fonctionnement. Enfin, dans le cas d'un logiciel en mode SaaS, il n'a qu'à se préoccuper de ses données. Les obligations respectives découlant de ce partage des responsabilités en matière de sécurité sont clairement énoncées dans le contrat de services qui lie les deux parties.

Qui est responsable de la sécurité ?



La gouvernance, les risques, la conformité, la gestion des identités et des accès ainsi que la protection des informations et des données relèveront **toujours** *de la* **responsabilité** *du* **propriétaire des données.**

●● Géré par le client ● Géré par le fournisseur cloud

Dans tous les cas de figure, le prestataire de services cloud est à minima responsable de la sécurité physique des installations (data center), des machines et du réseau. La sécurité est par conséquent un sujet qui est au cœur de son métier et de sa proposition de valeur, et sur lequel il est en mesure d'investir beaucoup plus que chacun de ses clients pris individuellement. Ceci lui permet de mettre en œuvre les technologies de sécurité les plus à la pointe et de recruter les meilleurs spécialistes. C'est pourquoi peu d'organisations, publiques ou privées, peuvent aujourd'hui rivaliser avec la sécurité qu'offrent les data centers et les infrastructures des grands prestataires de cloud.

Pour le client, pouvoir se reposer sur un tel socle est un gage de confiance et cela le soulage d'une importante charge opérationnelle. Pour autant, cela ne l'exonère pas de sa part du travail, à savoir la sécurité dans le cloud. Quel que soit le modèle, il lui revient en particulier de garantir la confidentialité, l'intégrité et la conformité de ses données. Il lui faut donc en gérer les accès et les droits, les chiffrer si besoin, les sauvegarder… Exactement comme si elles se trouvaient dans son propre data center ! Pour cela, il est généralement possible d'utiliser les outils de son choix, mais les fournisseurs de cloud proposent souvent des solutions clé en main, d'excellente qualité, optimisées pour leurs environnements et rigoureusement maintenues à jour. Elles représentent un atout supplémentaire du cloud en matière de sécurité.

À bien des égards, le cloud offre donc un environnement beaucoup plus sécurisé que ce que pourraient mettre en œuvre seules la plupart des organisations, a fortiori de taille moyenne comme des collectivités ou des établissements publics. La richesse des outils de supervision et de contrôle, la rapidité de détection et d'intervention, la régularité des mises à jour, le nombre et la compétence des effectifs, tout cela est incomparable.

LA STRATÉGIE
DE L'ÉTAT

Le cloud est aujourd'hui le principal vecteur de diffusion et de consommation de l'innovation numérique. L'État le considère de ce fait comme un puissant levier de développement de l'économie et un outil incontournable de la modernisation et de l'efficience des entreprises et des services publics, sans toutefois ignorer l'écrasante mainmise qu'ont aujourd'hui les acteurs américains sur ce domaine. Ceci a conduit le gouvernement à adopter en mai 2021 une stratégie nationale qui concilie plusieurs objectifs :

Favoriser l'adoption du cloud par les entreprises et les administrations françaises

Leur permettre de bénéficier des technologies les plus avancées

Leur apporter de solides garanties en matière de sécurité technique et juridique

Soutenir le développement des acteurs français et européens, et les aider à rattraper leur retard technologique et commercial

Cette stratégie repose sur trois piliers :

CLOUD DE CONFIANCE

La création d'un label « Cloud de confiance » indiquant aux acteurs publics et privés les services cloud offrant un niveau satisfaisant de sécurité technique et juridique. Cette approche n'exclut pas totalement les acteurs extra européens, dont l'avance technologique est jugée indispensable, mais elle les contraint à se plier aux exigences strictes énoncées dans la version actualisée du référentiel SecNumCloud. Capgemini et Orange ont notamment formé une co-entreprise, Bleu, pour créer l'un de ces « clouds de confiance ».

CLOUD AU CENTRE

Une politique dite « Cloud au centre », qui invite les administrations françaises à basculer massivement vers le cloud et à en privilégier l'utilisation dans tous leurs nouveaux projets numériques. Les applications essentielles et les données sensibles devront néanmoins être hébergées sur l'un des clouds internes de l'État, comme ceux développés par la Direction générale des Finances publiques (Nubo) et le ministère de l'Intérieur (PI), ou sur des clouds commerciaux qualifiés SecNumCloud.

ÉCONOMIE EUROPÉENNE DE LA DONNÉE

Une politique industrielle destinée à soutenir l'offre afin de poser les bases d'une économie européenne de la donnée. Cette politique, financée par le 4e Programme d'Investissement d'Avenir et France Relance, visera en particulier à valoriser les offres françaises innovantes, à aider les acteurs nationaux à passer à l'échelle et à soutenir la recherche, l'innovation et la formation.

Le plan de relance est également mis à contribution pour soutenir la demande, tout particulièrement sur le volet cybersécurité, identifié comme un enjeu prioritaire pour le secteur public.
Pour aider les collectivités territoriales, les établissements de santé et les établissements publics à renforcer la sécurité de leurs systèmes et de leurs données, l'État propose des « parcours de cybersécurité » conçus et financés par l'ANSSI. Ces parcours comportent un pré-diagnostic, puis un accompagnement en deux temps par des prestataires qualifiés PASSI (Prestataires d'audit de la sécurité des systèmes d'information) :

PACK INITIAL

Subventionné à 100%, qui inclut un état des lieux, des actions de sensibilisation et de formation, la mise en œuvre des mesures les plus urgentes et l'élaboration d'un plan de sécurisation.

PACKS RELAIS

En partie subventionnés, destinés à mettre en œuvre les préconisations du plan de sécurisation.

RECOMMANDATIONS
ET SOLUTIONS CLÉS

Malgré des budgets contraints, les services publics ont la double obligation de se moderniser et de renforcer la sécurité de leurs systèmes face à la recrudescence des cyberattaques. Le cloud apparaît comme la meilleure des options car il leur permet de bénéficier de ressources flexibles et performantes tout en offrant les plus hauts niveaux de fiabilité et de sécurité. Basculer vers le cloud constitue en outre une excellente occasion de remettre à plat sa politique de sécurité face à l'évolution des usages (mobilité, télétravail…), de la réglementation (RGPD…) et des menaces (rançongiciels…).

Voici quelques recommandations et solutions clés qui doivent absolument figurer au menu de la réflexion :

1. Une approche par le risque

Autant pour des raisons financières que pratiques, il n'est pas possible, ni même souhaitable, d'appliquer un niveau de sécurité maximal à tout le système d'information. Pour définir partout le juste niveau de sécurité, il convient d'aborder le sujet sous l'angle des risques, c'est-à-dire d'évaluer chaque menace au double prisme de sa probabilité et des dégâts qu'elle occasionnerait. Ceci permet de fixer des priorités, de sélectionner les réponses les plus efficientes et d'instaurer la confiance nécessaire à l'adoption des services numériques par les utilisateurs finaux, agents et citoyens.

2. Une classification des données pour une protection optimale

Cette approche différenciée commence par une connaissance précise de ses données. Des données d'état civil ou de santé n'ont ni la même valeur, ni le même cycle de vie, ni le même cadre réglementaire, que des données de gestion. Établir une classification des données permettra de déterminer les règles et les dispositifs de sécurité applicables à chacune : localisation, stockage, chiffrement, droits d'accès, prévention des fuites, archivage…

3. Des dispositifs de détection et de réponse

Malgré ces protections, des intrusions exploitant des vulnérabilités encore inconnues restent possibles. C'est pourquoi il est indispensable de mettre en place un système de surveillance et d'analyse des informations et des évènements de sécurité (SIEM), et de le coupler à un centre d'intervention (SOC) où des experts, disponibles 24h/24h et 7j/7j, pourront être avertis, prendre la mesure de la situation et intervenir au plus vite.Pandémie, incendie, inondations…

4. PRA, PCA et réversibilité pour parer à toute éventualité

Les data centers du cloud ne sont pas à l'abri des catastrophes du monde réel. Minimiser les conséquences de telles situations, cela s'anticipe en mettant en place des plans de continuité (PCA) et de reprise d'activité (PRA), avec par exemple une réplication des données sur un site distant. Et si l'incident devait se prolonger, avoir organisé la réversibilité permet de ne pas se retrouver prisonnier d'un prestataire défaillant.

5. La sécurité dès la conception

Dans les modèles IaaS et PaaS, le client reste responsable de la sécurité de ses applications. Or, l'expérience montre qu'il est beaucoup plus efficace et moins coûteux d'envisager leur sécurité le plus en amont possible (on parle de « shift left »). Pour les applications destinées au cloud, on mettra donc en place des méthodes et des pratiques de conception, de développement et de test tenant compte des enjeux de sécurité et appliquant, si possible de façon automatisée, les règles en la matière.

6. Ne pas négliger la dimension humaine

L'un des freins qui demeure à l'adoption du cloud est la défiance qu'il peut encore susciter. La première cause des incidents de sécurité, ce sont les négligences ou les imprudences des utilisateurs. Et la priorité absolue des acteurs publics est de conserver la confiance des citoyens en assurant quoi qu'il arrive la continuité de leurs missions. Bref, l'humain est au centre de l'équation cloud et cybersécurité, et, en parallèle des projets techniques, il est fondamental de veiller à accompagner l'évolution des compétences et de la culture des agents comme des usagers.

7. L'UGAP, un catalogue complet de solutions, la sécurité juridique en plus

Le modèle de consommation à l'usage du cloud n'a pas toujours été facilement intégré par les acheteurs publics dans leurs marchés, ce qui a sans doute freiné son adoption dans le secteur public. Grâce aux centrales d'achats publics (UGAP, RESAH, CAIH…), cette difficulté appartient au passé et les ministères, collectivités et établissements publics peuvent accéder facilement aux services « IaaS et PaaS » des principaux fournisseurs de cloud (AWS, Clever Cloud, Google Cloud, IBM, Microsoft Azure, Oracle, Orange Business Services, 3DS Outscale, OVHcloud, Scaleway) adaptés aussi bien aux données sensibles et aux services essentiels qu'à des usages moins critiques.
La procédure d'achat s'en trouve à la fois simplifiée, accélérée, et parfaitement sécurisée du point de vue juridique.

Via les lots AMOA, conseil et SSI du marché PII de l'UGAP dont il est titulaire, et fort de son expertise sur l'ensemble des briques de la cybersécurité et du cloud, Capgemini peut accompagner les organisations publiques de bout en bout dans leur démarche de sécurisation.

Cela inclut les « parcours de cybersécurité » de l'ANSSI qui pour plus de commodité, de rapidité et une totale sécurité juridique, peuvent être mises en place via le lot SSI du marché PII de l'UGAP, dont Capgemini Cyber sécurité, anciennement Sogeti, est titulaire.

En savoir plus sur nos offres :

CYBERSÉCURITÉ | PII AMOA | CLOUD

Evènements, infos, webinaires, sur notre site dédié au marché cloud de l'UGAP:

CLOUDTOUR

Nous contacter :

CONTACTCLOUD.FR@CAPGEMINI.COM

Capgemini

GET THE FUTURE YOU WANT*

Capgemini est un leader mondial, responsable et multiculturel, regroupant 325 000 personnes dans plus de 50 pays. Partenaire stratégique des entreprises pour la transformation de leurs activités en tirant profit de toute la puissance de la technologie, le Groupe est guidé au quotidien par sa raison d'être : libérer les énergies humaines par la technologie pour un avenir inclusif et durable. Fort de 55 ans d'expérience et d'une grande expertise des différents secteurs d'activité, Capgemini est reconnu par ses clients pour répondre à l'ensemble de leurs besoins, de la stratégie et du design jusqu'au management des opérations, en tirant parti des innovations dans les domaines en perpétuelle évolution du cloud, de la data, de l'Intelligence Artificielle, de la connectivité, des logiciels, de l'ingénierie digitale et des plateformes.
Le Groupe a réalisé un chiffre d'affaires de 18 milliards d'euros en 2021.

*Capgemini, le futur que vous voulez

www.capgemini.com