Tendances en infrastructures 2025

Enjeux et perspectives

Synapsys

CRiP
PROGRESSER PAR LE PARTAGE

IA, cyber, cloud : l'année de tous les chocs pour les DSI

2024 a été une année intense pour les DSI, marquée par des transformations accélérées et des défis budgétaires. Longtemps perçus comme des garants de la stabilité des SI, ils ont vu leur rôle s'accélérer cette année.

L'IA générative, qui était encore en phase exploratoire en début d'année dernière, s'est immiscée dans les processus, bouleversant les modes de travail. Il ne s'agit plus seulement d'expérimenter, mais de déployer des solutions concrètes capables d'améliorer la productivité tout en restant sous contrôle. Ce défi, bien que prometteur, a placé le DSI face à une question cruciale : comment garantir la souveraineté et la sécurité des données alors que l'IA repose sur des modèles en perpétuelle évolution ?

En parallèle, la menace cyber s'est intensifiée, atteignant un niveau critique. Le terrain de jeu des cybercriminels s'est élargi, obligeant les entreprises à renforcer leurs dispositifs de protection et à adopter une posture Zero Trust. Dans ce contexte, le DSI a dû arbitrer entre performance et sécurité, souvent sous contrainte budgétaire.

L'explosion des coûts du cloud a été un autre coup de tonnerre. Les organisations, qui avaient misé sur le cloud pour sa flexibilité et sa scalabilité, ont découvert avec stupeur des factures difficilement soutenables. L'heure n'est plus à l'expansion débridée, mais à l'optimisation. FinOps, rationalisation des workloads, hybridation entre cloud et on-premise sont devenus des maîtres-mots pour une gestion plus pragmatique des ressources informatiques. Cette remise en question a replacé le DSI au cœur des stratégies financières de l'entreprise.

Ce livre blanc s'attache à décrypter les grandes tendances et priorités des DSI pour l'année à venir, en apportant des éclairages précieux sur les leviers à activer pour relever les défis de la gestion des infrastructures dans un environnement en constante mutation.

Nathalie Hoyos
Directrice Marketing de Synapsys

RENFORCER LA SÉCURITÉ

Face à des cybermenaces toujours plus sophistiquées, **79%** des entreprises jugent indispensable d'investir dans la sécurité numérique pour protéger leurs données et préserver leur activité.

INVESTIR DANS LA DATA & L'IA

L'IA et la valorisation des données ne sont plus une option. **Plus d'une entreprise sur deux** y voit un levier clé pour renforcer son avantage concurrentiel.

Cap sur les priorités d'investissements en 2025

ACCÉLÉRER LA MIGRATION VERS LE CLOUD

46 % des entreprises envisagent une migration vers le cloud afin de gagner en flexibilité et en adaptabilité.

GÉRER L'OBSOLESCENCE ET MODERNISER

56% des entreprises recherchent à moderniser leurs infrastructures IT et réduire leur dette technique pour gagner en agilité et en résilience.

RENFORCER L'AUTOMATISATION

Accélérer les cycles de développement, fiabiliser les déploiements et optimiser les ressources : l'automatisation et le DevOps s'imposent comme des solutions incontournables pour **38%** des entreprises.

MODERNISER LE WORKPLACE

1 entreprise sur 5 souhaite accélérer sa transition vers un environnement de travail moderne, unifié et intégré.

Chaque thématique abordée dans ce livre blanc révèle des enjeux stratégiques, mais aussi des opportunités pour bâtir des infrastructures plus résilientes, agiles et responsables.

DÉVELOPPER LES INITIATIVES GREEN

L'intégration de pratiques plus responsables et durables devient une nécessité pour répondre aux attentes sociétales et limiter l'impact environnemental.

FAIRE ÉVOLUER L'ORGANISATION IT

1 entreprise sur 3 cherche à faire évoluer son organisation pour gagner en agilité, mieux s'adapter aux évolutions et renforcer l'alignement entre les équipes IT et métiers.

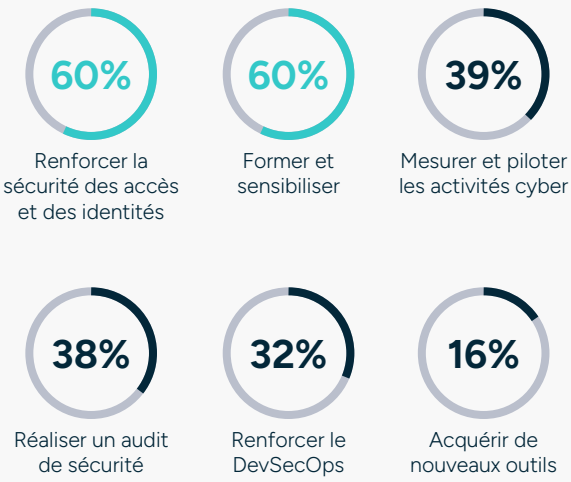
Sommaire

INSIGHT 1

Cybersécurité : de la contrainte à la priorité stratégique

La cybersécurité, priorité n°1 des décideurs en 2025

Principaux enjeux 2025 en matière de cybersécurité



Renforcer la sécurité des accès et des identités

L'IAM (Identity and Access Management) est un rempart essentiel contre les cyberattaques, capable de prévenir la majorité des menaces en entreprise grâce à une gestion rigoureuse des accès.

Former et sensibiliser les collaborateurs

La formation et la sensibilisation des collaborateurs sont une priorité pour 60 % des décideurs, révélant à la fois le rôle clé de l'humain en cybersécurité et un manque de vigilance encore trop présent. La recrudescence des attaques d'ingénierie sociale, qui ciblent directement les employés sans nécessiter d'expertise technique pour les cybercriminels, en est la preuve éclatante.

Mesurer et piloter les activités cyber

Les entreprises cherchent à harmoniser, piloter et évaluer l'efficacité de leur cybersécurité, souvent à l'échelle de toutes leurs entités. Cette approche proactive vise à mieux cerner les risques pour les anticiper et les maîtriser efficacement.

4 sur 5

4 décideurs sur 5 indiquent que le renforcement de la sécurité fera l'objet d'investissements en 2025.

Réaliser un audit de sécurité

Un audit de sécurité est, pour plus d'un tiers des répondants, une étape essentielle pour évaluer la robustesse du SI. Il permet d'identifier les vulnérabilités et de définir une feuille de route pour renforcer la cybersécurité. Perçu comme un prérequis, il assure une stratégie adaptée aux besoins et ressources de l'organisation.

Améliorer la culture DevSecOps

L'intégration de la sécurité dès les premières phases du développement est identifiée comme une priorité par un tiers des répondants. Le DevSecOps (développement, sécurité et opérations) vise à intégrer des pratiques de sécurité directement dans les processus de développement logiciel, afin de réduire les vulnérabilités dès leur conception.

L'approche DevSecOps est particulièrement plébiscitée dans un contexte où les cycles de développement sont de plus en plus courts, augmentant les risques de laisser des failles non détectées.

Acquérir de nouveaux outils

Bien que l'acquisition d'outils de cybersécurité reste une priorité pour certains, elle est considérée comme secondaire par rapport à d'autres initiatives. Cela reflète une prise de conscience : les outils ne peuvent être efficaces que s'ils sont intégrés dans un écosystème global, incluant une gouvernance et des processus.

Les résultats mettent en lumière des tendances claires : une attention particulière est portée à l'humain et aux processus, tandis que les outils technologiques sont perçus comme des compléments nécessaires, mais non suffisants.

L'accent sur la formation, la gestion des identités et l'audit démontre une volonté d'adopter une approche globale et proactive face aux risques.

Pour préparer 2025, les entreprises doivent combiner des solutions technologiques robustes, une gouvernance efficace et une culture organisationnelle axée sur la résilience.

Les défis 2025 en matière de cybersécurité

L'évolution des menaces

Les attaques se sophistiquent, exploitant l'intelligence artificielle et des approches ciblées comme le ransomware-as-a-service. Face à cette évolution, les entreprises doivent renforcer leurs capacités de détection et de réponse pour contrer des menaces toujours plus complexes.

La gestion de la complexité IT

L'augmentation des environnements hybrides et multicloud, associée à la fragmentation des systèmes hérités, complique considérablement la gestion des identités et des accès. Cette complexité augmente les vulnérabilités potentielles.

Le manque de compétences

La pénurie mondiale de talents en cybersécurité persiste, rendant difficile le recrutement de profils qualifiés pour mener des actions stratégiques.

Le pilotage par la valeur

La cybersécurité est devenue une priorité stratégique pour protéger les données, la réputation et assurer la résilience. Le pilotage par la valeur permet de prioriser les investissements ayant un impact significatif et de réallouer les ressources en fonction de l'atteinte des objectifs fixés. Cela aide à optimiser les coûts et à garantir que les initiatives de cybersécurité contribuent réellement à la protection de l'organisation.

Les exigences réglementaires

L'évolution rapide des cadres réglementaires (ex : DORA, NIS2, RGPD) impose aux organisations de se conformer à des normes strictes tout en évitant une surcharge administrative.

L'enquête révèle une volonté accrue de renforcer la posture de sécurité à travers des initiatives prioritaires telles que la formation, la gestion des identités et l'intégration de la sécurité dans les processus. En alignant les efforts de cybersécurité avec leurs objectifs stratégiques, elles pourront non seulement répondre aux menaces actuelles, mais aussi se positionner comme des acteurs résilients et innovants face aux défis futurs.

Conseils de nos experts

Renforcer la sensibilisation et la formation

Investir dans des programmes de sensibilisation continue adaptés aux différents profils des collaborateurs pour réduire les risques liés à l'ingénierie sociale. Simuler des attaques, telles que des campagnes de phishing, pour tester et renforcer la vigilance des équipes.

Mettre en œuvre une stratégie Zero Trust

Face à des menaces de plus en plus sophistiquées et à des environnements distribués (cloud, télétravail, SaaS), le modèle Zero Trust impose une vérification systématique des identités, des appareils et des droits d'accès, tout en appliquant le principe du moindre privilège.

Intégrer le DevSecOps

La mise en œuvre du DevSecOps consiste à intégrer la sécurité dès les premières étapes du cycle de développement logiciel, afin de détecter et corriger les vulnérabilités le plus tôt possible. Le DevSecOps repose sur une collaboration renforcée entre les équipes de développement, d'exploitation et de sécurité, instaurant ainsi une culture où la sécurité est une responsabilité partagée.

Instaurer une politique de gestion des identités et des accès

En adoptant une stratégie IAM, les entreprises s'assurent que chaque partie prenante accède uniquement aux ressources nécessaires à ses fonctions. Cela réduit les risques de fraude, de vol de données et de cyberattaques. De plus, l'IAM permet de suivre et d'auditer les activités des utilisateurs, facilitant ainsi la détection des comportements suspects et la conformité aux réglementations.

Améliorer les capacités de détection et de réponse

Investir dans des solutions comme les systèmes EDR/XDR (Endpoint Detection and Response, Extended Detection and Response) et intégrer des plateformes SIEM et SOAR pour détecter rapidement les incidents et orchestrer des réponses efficaces.

Prioriser la gouvernance et le pilotage par la valeur

Développer des tableaux de bord efficaces pour mesurer les indicateurs clés de performance (KPI) en cybersécurité. Mettre en place un comité cybersécurité pour aligner les priorités sur les objectifs stratégiques et renforcer la communication avec les parties prenantes.

INSIGHT 2

IA : un pilotage par la valeur s'impose

L'IA générative et son potentiel de transformation

Principales priorités en matière d'IA en 2025

Élaboration de la roadmap et recensement des cas d'usage

Les projets d'IA générative en entreprise n'en sont encore qu'à leurs débuts. La priorité principale des décideurs est de construire une feuille de route et de prioriser les cas d'usage en fonction des besoins des différentes directions métiers et des objectifs commerciaux de l'entreprise. Cette étape stratégique est cruciale pour s'assurer que les initiatives lancées apportent une véritable valeur ajoutée.

Réalisation de PoC

Les projets de Proof of Concept (PoC) sont d'actualité pour 46% des répondants. Tester des solutions en conditions réelles avant de les déployer à grande échelle, permet de valider l'efficacité des applications de l'IA générative et de mesurer leur impact potentiel en termes de productivité ou de rentabilité.

Sensibilisation et formation

Vient ensuite l'importance de former et de sensibiliser les équipes. 37% des décideurs jugent primordial de préparer le terrain en formant les collaborateurs sur les enjeux et les usages de l'IA générative. Cette approche permet de mettre un cadre en matière d'usage de l'IA, de sécurité des données, tout en instaurant une culture d'innovation.

Industrialisation

L'industrialisation des solutions IA générative, représentant le déploiement à l'échelle et l'intégration dans les processus business, est perçue comme une priorité par 22% des décideurs. Ils sont encore peu matures pour ce passage à l'action mais cela reste une priorité pour beaucoup d'entre eux.

Les enjeux pour intégrer l'intelligence artificielle générative

La gestion des données, souvent fragmentées ou de qualité insuffisante, représente un défi critique. À cela s'ajoute la difficulté d'évaluer précisément le retour sur investissement (ROI), rendant les directions métiers parfois hésitantes à engager des ressources importantes.

Les entreprises se heurtent à la problématique du « shadow IA », où des initiatives non contrôlées ou non approuvées émergent en dehors du cadre établi par la DSI. Ces pratiques peuvent menacer la sécurité et la confidentialité des données, tout en créant des silos qui nuisent à une stratégie cohérente.

Cela souligne l'importance cruciale de mettre en place un cadre de gouvernance solide pour l'IA, garantissant une utilisation alignée avec les objectifs de l'entreprise, tout en maîtrisant les risques liés à la conformité, la sécurité et l'éthique.

58%

Plus d'un décideur sur deux envisage de réaliser des investissements sur l'IA en 2025.

Les décideurs ne se contentent pas simplement de suivre une tendance technologique, mais cherchent à intégrer l'IA générative de manière stratégique et cohérente avec les objectifs de leur organisation. L'intention est de maximiser l'impact de l'IA sur les activités métiers.

L'IA générative offre un potentiel immense pour les entreprises, mais elle doit être intégrée de manière pragmatique. L'enquête met en lumière l'importance de structurer les initiatives autour de cas d'usage métier clairs et d'assurer un alignement avec les objectifs globaux de l'entreprise. Si les entreprises parviennent à surmonter les défis liés à la formation, à l'industrialisation et à la gestion du changement, elles pourront pleinement exploiter la valeur de l'IA générative pour transformer leurs processus et renforcer leur compétitivité sur le marché.

Les décideurs doivent continuer à être proactifs dans l'élaboration de leur stratégie IA, en plaçant l'humain et la valeur métier au cœur de leurs priorités. C'est ainsi qu'ils réussiront à tirer parti des avancées technologiques pour répondre aux défis de demain.

Conseils de nos experts

L'IA pour les métiers

Les cas d'usage identifiés doivent répondre à des problématiques métier spécifiques, telles que l'optimisation de la productivité, la personnalisation des services ou l'automatisation des tâches répétitives. Cela permet de justifier les investissements dans l'IA, mais aussi d'évaluer concrètement le retour sur investissement.

Évaluer en continu les PoC

La mise en œuvre et l'évaluation des PoC sont cruciales pour valider la faisabilité technique et tester la pertinence des cas d'usage avant un déploiement à grande échelle. Cela permet d'identifier les risques et d'optimiser les ressources en évitant des investissements inutiles. Un PoC bien conçu aide également à affiner les modèles d'IA, à convaincre les parties prenantes et à préparer le passage à la phase de déploiement.

Renforcer l'accompagnement au changement

La formation et la sensibilisation des équipes à l'IA sont cruciales pour favoriser l'adoption de nouveaux usages, améliorer la productivité et garantir une utilisation sécurisée. Une équipe bien formée est plus à même de détecter les risques associés à l'IA, comme les biais ou les problèmes éthiques, et de garantir une utilisation responsable et efficace de ces outils dans les processus métiers.

Mettre en œuvre un cadre de gouvernance robuste

Tandis que les entreprises s'efforcent d'intégrer l'IA dans leurs processus métier, il devient impératif de définir des règles et des pratiques claires pour encadrer l'utilisation de cette technologie. Une gouvernance efficace permet non seulement de maximiser les bénéfices de l'IA, mais aussi de gérer les risques associés, notamment en termes d'éthique, de transparence, de sécurité et de conformité.

Mettre en ordre les données de l'entreprise

Une gestion efficace des données, incluant leur collecte, leur nettoyage et leur structuration, est cruciale pour assurer la performance et la robustesse des solutions d'IA Générative. Sans un chantier data bien structuré, les entreprises risquent de rencontrer des problèmes de fragmentation des données et de qualité insuffisante.

Rendre l'IA plus performante

Les applications généralistes peuvent souffrir de problèmes de performance et de précision, produisant parfois des résultats erronés ou des « hallucinations », ce qui nuit à leur fiabilité et à leur utilité en contexte d'entreprise. Pour y pallier, les entreprises se tournent vers le développement d'applications spécifiques axées sur la productivité et l'efficacité des métiers. Il est envisageable que l'IA s'intègre progressivement dans tous les logiciels où elle apporte une valeur ajoutée en améliorant les tâches et les processus.

INSIGHT 3

Moderniser ses infrastructures et gérer l'obsolescence

Rénover pour innover : l'impératif de la modernisation

Défis en matière de modernisation des infrastructures

Coûts de maintenance élevés

Les systèmes obsolètes nécessitent des ressources importantes pour leur maintenance, ce qui augmente les coûts opérationnels.

Risque de failles de sécurité

Les infrastructures vieillissantes sont souvent plus vulnérables aux cyberattaques, ce qui peut compromettre la sécurité des données et des systèmes.

1 sur 2

Pour la moitié des décideurs, la modernisation des infrastructures et la gestion de l'obsolescence sont des chantiers prioritaires en 2025. Cet investissement est motivé par le fait que près de 25% des décideurs se sentent freinés par des infrastructures obsolètes ou limitées.

Manque d'agilité

Les systèmes obsolètes peuvent freiner l'agilité de l'entreprise, rendant difficile l'adaptation rapide aux nouvelles opportunités et aux changements du marché.

Incompatibilités technologiques

Les anciennes technologies peuvent ne pas être compatibles avec les nouvelles solutions, ce qui complique l'intégration et l'optimisation des processus.

Perte de connaissance

Avec le temps, les connaissances sur les systèmes obsolètes peuvent se perdre, rendant leur gestion et leur mise à jour encore plus difficiles.

Fragmentation des données

La dette technique peut entraîner une fragmentation des données, rendant difficile leur gestion et leur exploitation pour des analyses pertinentes.

Impact sur l'innovation

Les ressources consacrées à la gestion de la dette technique sont autant de ressources qui ne peuvent pas être investies dans l'innovation et le développement de nouvelles solutions.

La modernisation des infrastructures représente un enjeu stratégique aux multiples facettes. D'un côté, elle vise à optimiser la performance des systèmes informatiques et des équipements, contribuant ainsi à une réduction des coûts d'exploitation. De l'autre, elle permet de renforcer la sécurité et d'assurer la conformité aux réglementations, un impératif particulièrement crucial dans les secteurs soumis à des régulations strictes.

La problématique centrale réside dans le fait que, malgré les avantages évidents de la modernisation des infrastructures, de nombreuses entreprises hésitent encore à se lancer, principalement en raison du coût et des risques perçus.

La réussite de la modernisation des infrastructures dépend de la capacité d'une entreprise à concilier innovation et gestion prudente des ressources. Avec une stratégie adaptée et un pilotage efficace, il est possible de transformer ces défis en opportunités pour soutenir la croissance future et l'innovation.

La modernisation des infrastructures SI est un enjeu majeur pour 2025.

Alors que de nombreuses entreprises sont encore en retard dans la gestion de leurs infrastructures, des efforts importants sont nécessaires pour rattraper ce retard et permettre une transformation réussie.

La réduction de la dette technique, l'adoption d'une gouvernance centralisée et l'implication des métiers sont les clés pour réussir cette modernisation. En outre, l'investissement dans les compétences IT et l'accompagnement au changement seront cruciaux pour garantir l'adoption et l'intégration des nouvelles technologies.

Conseils de nos experts

Audit des infrastructures

La gestion de l'obsolescence et la réduction de la dette technique sont des processus complexes qui nécessitent une évaluation complète de l'infrastructure existante pour identifier les systèmes à mettre à jour ou à remplacer.

Réaliser une modernisation progressive

Adoptez une approche progressive en modernisant par le cloud ou en priorisant des transformations à forte valeur ajoutée pour le métier ou des sujets à risque peut-être une manière pragmatique de moderniser l'infrastructure tout en maîtrisant les coûts.

Intégrer des métiers

Impliquez les métiers dans la gestion de la dette en présentant des business cases adaptés et en responsabilisant les équipes. Les infrastructures doivent créer de la valeur ajoutée pour les métiers, en permettant une meilleure collaboration inter-départements, une gestion de projet plus fluide et une prise de décision plus rapide.

Investir dans la formation et l'accompagnement

Investissez dans la formation et l'accompagnement au changement pour assurer l'adoption des nouvelles technologies par les utilisateurs.

Mettre en place l'automatisation et le DevOps

Explorez les solutions cloud et DevOps pour améliorer l'agilité des infrastructures, gérer les ressources de manière plus efficace et réduire les coûts à long terme.

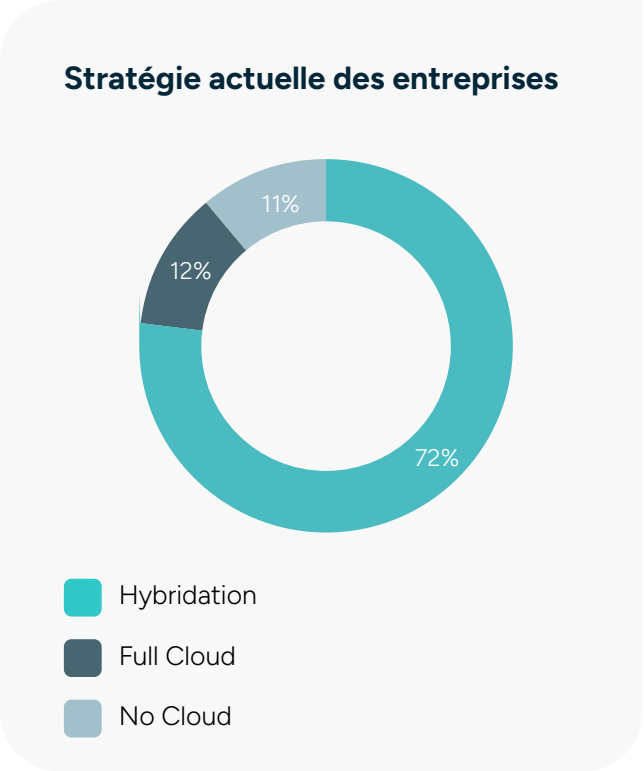
Intégrer des principes de frugalité numérique

Identifiez et conservez uniquement les technologies essentielles, tout en éliminant celles qui ne génèrent pas de valeur. Dans ce contexte, l'objectif est de maximiser la valeur ajoutée tout en limitant les investissements excessifs.

INSIGHT 4

Transformation Cloud : vers un IT hybride

IT hybride : tirer parti du meilleur des deux mondes



Comment les entreprises se positionnent-elles en matière d'infrastructure ?

L'hybridation permet de combiner le meilleur des deux mondes : des solutions cloud public pour leur flexibilité et leurs coûts maîtrisés, et des solutions cloud privé pour des besoins spécifiques de sécurité, de gouvernance et de contrôle. Mais cette complexité engendre aussi des défis d'intégration, de gestion des performances et de surveillance sur plusieurs environnements en même temps.

Infrastructure hybride

77% des répondants ont adopté une approche hybride. Cette tendance confirme que les entreprises privilégient de plus en plus la coexistence des systèmes on-premise, cloud privé et cloud public. L'hybridation permet de bénéficier des avantages du cloud tout en préservant certaines infrastructures locales, souvent pour des raisons de sécurité, de conformité ou de dépendance aux systèmes hérités.

Stratégie Full-cloud

12% des entreprises se positionnent aujourd'hui sur une adoption complète du cloud. Il s'agit pour la plupart des entreprises les plus matures en matière de modernisation des infrastructures, de pilotage et de culture DevOps. Ce chiffre témoigne également de la rareté des organisations ayant choisi une stratégie « all-in », ce qui semble refléter une tendance à privilégier des modèles hybrides et plus nuancés.

No-cloud

11% des décideurs n'a pas encore intégré le cloud dans sa stratégie. Cela peut refléter une certaine prudence ou une absence de besoins immédiats (notamment pour certains secteurs très réglementés).

Les défis en matière de transformation cloud en 2025

Maîtrise des coûts et gouvernance

L'apparition de pratiques telles que le FinOps met en lumière la nécessité de maîtriser la consommation des ressources cloud, notamment les ressources non gouvernées, qui peuvent entraîner des coûts imprévus et des complexités.

45%

Près d'un décideur sur deux pense investir dans leur migration cloud en 2025.

Diversité technologique

Le principal défi réside dans l'intégration des différents environnements cloud au sein d'une architecture hybride. Tandis que le cloud public séduit par sa scalabilité et son optimisation des coûts, le cloud privé demeure indispensable pour les applications stratégiques ou sensibles, nécessitant un contrôle strict de la gouvernance.

Comment concilier cette diversité technologique sans engendrer une complexité excessive, susceptible de freiner l'innovation ou d'accroître les coûts d'exploitation ? La gestion d'une infrastructure hybride et multi-cloud, où coexistent cloud public, privé et on-premise, impose une vigilance accrue sur l'observabilité et la maîtrise des flux de données, devenues des priorités incontournables.

Sécurité

Un autre enjeu majeur concerne la gestion des données et de la sécurité au sein des différents environnements cloud. Les entreprises doivent veiller à ce que cette hybridation ne compromette ni le contrôle sur leurs infrastructures ni leur efficacité opérationnelle. Une complexité excessive pourrait en effet aller à l'encontre de l'agilité recherchée, rendant les bénéfices attendus plus difficiles à concrétiser.

Compétences et ressources internes

La gestion de la complexité des environnements cloud, la sécurité des données et le contrôle des coûts nécessitent des compétences internes avancées. La mise à niveau des compétences des équipes IT est essentielle pour accompagner cette transformation, ce qui nécessite un investissement important en formation et en recrutement.

Dépendances vis-à-vis des éditeurs et technologies obsolètes

L'hybridation est une stratégie qui permet d'éviter la dépendance à un seul fournisseur de cloud en diversifiant les sources et les environnements de stockage et de traitement des données. Elle permet aux entreprises de bénéficier des avantages du cloud tout en conservant certaines infrastructures locales pour des raisons de sécurité, de conformité ou de dépendance aux systèmes hérités.

L'hybridation est la voie privilégiée pour la majorité des entreprises dans leur parcours de transformation cloud pour 2025. Cependant, pour réussir cette transition, les DSI doivent surmonter des défis complexes, notamment en matière de gestion des coûts, de compétences internes et de gouvernance.

Pour relever ces défis, plusieurs leviers peuvent être activés, notamment l'adoption des pratiques FinOps, l'automatisation des processus et le déploiement d'une observabilité avancée. Ces solutions permettent aux entreprises de piloter leur transformation avec efficacité et agilité. Par ailleurs, investir dans le développement des compétences et s'assurer que la transition vers le cloud génère une réelle valeur pour les métiers tout en garantissant la sécurité et la conformité des données est essentiel.

Le succès repose sur une approche stratégique axée sur la maîtrise des coûts, la flexibilité et la résilience des infrastructures. Les organisations capables de naviguer dans cet écosystème hybride seront mieux armées pour anticiper les évolutions à venir et renforcer leur compétitivité sur un marché en constante mutation.

L'hybridation est la tendance dominante pour 2025. Les entreprises adoptent une approche plus pragmatique, en combinant différentes solutions pour répondre à des besoins spécifiques tout en minimisant les risques associés à une migration totale vers le cloud.

Conseils de nos experts

Adopter une approche FinOps robuste

Mettre en place une gestion des coûts proactive et une gouvernance efficace permet d'éviter la prolifération des ressources cloud non gouvernées. Il faut définir des processus clairs pour le suivi des dépenses et l'optimisation des ressources cloud. Une gestion basée sur la valeur permettrait également d'analyser les retours sur investissement et d'aligner les dépenses avec les objectifs métiers.

Automatiser les processus et réduire la complexité

L'automatisation des processus manuels, notamment dans la gestion des ressources cloud et des applications SaaS, permet de réduire les coûts, d'améliorer la sécurité et de limiter les risques opérationnels. Une telle automatisation contribuera à réduire la complexité des environnements cloud hybrides et à simplifier leur gestion.

Investir dans les compétences internes et l'accompagnement au changement

La montée en compétences des équipes IT est essentielle pour maîtriser les enjeux de sécurité, de gestion des coûts et d'architecture dans un environnement hybride. Des programmes de formation dédiés à la gestion des environnements cloud-native et aux nouvelles pratiques DevOps doivent être mis en place pour garantir la réussite de la transformation.

Éviter la dépendance excessive aux éditeurs

Pour limiter les risques associés aux fournisseurs spécifiques, les entreprises doivent envisager des solutions plus flexibles comme Kubernetes ou des environnements multi-cloud. L'indépendance vis-à-vis des fournisseurs permettra une plus grande agilité et résilience dans la gestion des infrastructures.

Mettre l'accent sur l'observabilité avancée

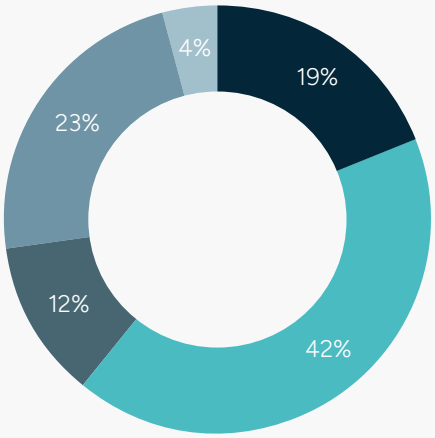
Une visibilité complète sur l'infrastructure hybride est cruciale pour la gestion de la performance, la sécurité et la résilience des systèmes. L'adoption d'outils d'observabilité avancée permettra de mieux comprendre les interactions complexes entre les différents environnements cloud et d'identifier rapidement les goulots d'étranglement ou les risques de sécurité.

INSIGHT 5

Intensification du virage DevOps

Accélérer la maturité DevOps : un enjeu clé

Les différents niveau de maturité en matière d'automatisation (DevOps)



- **Niveau 1 :** Déploiement limités et non structurés
- **Niveau 2 :** Automatisation basique mais reproductible
- **Niveau 3 :** Infrastructure as Code (IaC) standardisée
- **Niveau 4 :** CI/CD entièrement automatisée
- **Niveau 5 :** Automatisation pilotée par l'IA et optimisation continue
- Ne sait pas

NIVEAU 1 : Déploiement limités et non structurés

19% des décideurs indiquent n'être encore qu'au stade préliminaire de l'automatisation. Les déploiements réalisés sont souvent non structurés, limités à des processus manuels ou semi-automatisés. Ils peuvent être ad hoc, sans véritable standardisation ou planification à long terme. Ces organisations font probablement face à des difficultés liées à la fragmentation des outils et à un manque de contrôle sur les processus de développement et de production.

Problématiques rencontrées

- Absence de gouvernance,
- Manque de visibilité sur les processus,
- Risques liés à des déploiements manuels non sécurisés.

Opportunités d'amélioration

- Structurer et automatiser les processus de déploiement de manière plus cohérente.
- Adopter des outils comme les pipelines CI/CD de base pour un premier pas vers une meilleure gestion des déploiements.

NIVEAU 2 : Automatisation basique mais reproductible

42% entreprises ont franchi un cap. Elles ont réussi à automatiser certains processus de manière basique, mais reproductible. Le niveau 2 correspond à un stade où les équipes peuvent automatiser certaines étapes comme les tests, les déploiements ou encore la gestion des configurations, mais cela reste souvent partiel et non complètement intégré dans une chaîne de développement continue.

Problématiques rencontrées

- Automatisation présente mais des processus encore partiels, ce qui peut entraîner des inefficacités et des risques d'erreurs humaines dans certaines parties du pipeline.
- Intégration non fluide avec d'autres outils.

Opportunités d'amélioration

- Étendre l'automatisation à d'autres aspects du processus de développement
- Adopter des pratiques de gestion de l'infrastructure (par exemple avec Infrastructure as Code) pour renforcer la reproductibilité et la sécurité des environnements.

NIVEAU 3 : Infrastructure as Code (IaC) standardisée

12% des décideurs se trouvent au niveau 3, où l'automatisation atteint une étape supérieure grâce à l'intégration de l'Infrastructure as Code (IaC). À ce stade, les entreprises ont réussi à formaliser et standardiser la gestion de leur infrastructure via des outils comme Terraform ou Ansible, permettant ainsi de gérer l'infrastructure de manière versionnée et cohérente, en lien avec les processus de développement logiciel.

Problématiques rencontrées

- Gestion de la complexité des infrastructures multicloud ou hybrides, et la mise en place de l'IaC .
- Peut nécessiter une expertise technique avancée pour assurer la cohérence et la sécurité des configurations.

Opportunités d'amélioration

- Intégration de l'IaC dans tous les aspects de l'automatisation pour améliorer la scalabilité et la flexibilité.
- Adoption de pratiques de CI/CD et d'outils d'automatisation de tests pour renforcer la cohérence entre l'infrastructure et le code.

NIVEAU 4 : CI/CD entièrement automatisée

Le niveau 4 montre que 23% des entreprises ont atteint un stade où leurs processus de développement et de déploiement sont entièrement automatisés grâce à des pipelines CI/CD robustes. Ces entreprises ont probablement mis en place des solutions d'intégration et de livraison continues qui leur permettent de déployer des applications en temps réel avec un haut degré d'automatisation et de sécurité.

Problématiques rencontrées

- Gestion de la complexité des pipelines, surtout lorsqu'ils intègrent de nouveaux services ou outils dans des environnements multicloud.
- Maintien de la qualité et de la sécurité tout au long de ces processus.

Opportunités d'amélioration

- Mieux sécuriser les pipelines en intégrant des pratiques DevSecOps.
- Pousser l'automatisation encore plus loin avec des tests automatisés à tous les niveaux du pipeline.

NIVEAU 5 : Automatisation pilotée par l'IA et optimisation continue

Aucune entreprise n'indique se trouver au niveau 5, ce qui est compréhensible étant donné la complexité de ce stade. L'automatisation pilotée par l'intelligence artificielle (IA) et l'optimisation continue représentent une vision de l'avenir où l'IA analyse en temps réel les processus et ajuste automatiquement les pipelines pour améliorer leur performance, détecter les anomalies et optimiser les ressources.

Problématiques rencontrées

- Forte capacité d'innovation et un investissement technologique important.
- Intégration de l'IA dans les processus de développement et de déploiement (encore en phase de recherche et développement dans de nombreuses entreprises).

Opportunités d'amélioration

- Exploration de l'IA et du machine learning pour optimiser les processus DevOps
- Développer des capacités d'auto-apprentissage et de prendre en charge des processus de prédiction et d'optimisation des déploiements.

1 sur 3

Près de 39 % des décideurs estiment que le renforcement de l'automatisation bénéficiera d'investissements en 2025

Les défis du DevOps en 2025

Complexité croissante des environnements

L'essor des infrastructures hybrides et multicloud, ainsi que la multiplication des outils et des plateformes, entraîne une complexité accrue dans l'intégration des processus. Les équipes doivent gérer un large éventail de technologies et de services tout en maintenant une automatisation cohérente.

Scalabilité et gestion de l'automatisation

Alors que de plus en plus d'entreprises adoptent le DevOps, la gestion de l'automatisation à grande échelle devient un défi. Il est nécessaire de s'assurer que les processus sont scalables et capables de s'adapter aux évolutions des besoins métiers.

Résistance au changement et adoption de la culture DevOps

Beaucoup d'organisations rencontrent des difficultés dans l'adoption de la culture DevOps. Les résistances au changement, qu'elles soient technologiques ou culturelles, ralentissent l'intégration de pratiques DevOps à grande échelle, notamment dans les grandes entreprises avec des équipes silotées.

Sécurité et compliance

L'automatisation et la vitesse des livraisons peuvent entraîner des risques en matière de sécurité et de conformité. Il devient essentiel d'intégrer la sécurité dès les premières étapes du cycle de développement avec des pratiques comme le DevSecOps, pour éviter les vulnérabilités dans les pipelines CI/CD.

Compétences et recrutement

L'adoption du DevOps nécessite des compétences spécialisées, et la pénurie de talents dans ce domaine est un frein pour de nombreuses entreprises. Le recrutement et la formation des équipes DevOps sont des défis majeurs.

Les résultats démontrent des entreprises capables de déployer des services de manière quasi instantanée, d'identifier et corriger des erreurs de manière autonome, et d'offrir des produits toujours plus adaptés aux besoins de leurs clients, tout en augmentant leur sécurité et leur rentabilité. Ainsi, l'automatisation et le DevOps continueront d'évoluer pour offrir des outils toujours plus puissants, intégrés et intelligents, révolutionnant la manière dont les entreprises développent et exploitent leurs solutions informatiques.

Conseils de nos experts

Implémenter la standardisation et la gouvernance de l'automatisation

Pour gérer la complexité des environnements, il faut implémenter des pratiques de gouvernance solide. La mise en place de modèles d'automatisation standardisés, tels que l'utilisation d'Infrastructure as Code (IaC), permet de rationaliser les processus et d'assurer une gestion cohérente à travers différents environnements et plateformes.

Améliorer l'adoption culturelle du DevOps

La culture DevOps doit être encouragée. Cela nécessite une communication claire sur les avantages du DevOps, la mise en place de formations, et des efforts pour encourager la collaboration inter-équipes. La direction doit jouer un rôle clé dans la promotion de cette culture.

Intégrer le DevSecOps

Intégrer la sécurité dès le début du processus de développement via des pratiques DevSecOps permettra de minimiser les risques liés à l'automatisation. Les outils de sécurité automatisée, tels que les scanners de vulnérabilités ou les tests de sécurité dans les pipelines CI/CD, doivent devenir des pratiques courantes pour garantir la sécurité des livraisons rapides.

Investir dans les compétences

La formation des équipes en place est importante pour faire face à la pénurie de talents et maintenir l'agilité dans l'adoption de nouvelles technologies.

Adopter l'IA pour l'automatisation

Les technologies d'IA peuvent aider à optimiser les processus, prédire les défaillances et ajuster les pipelines en temps réel pour une performance maximale.

INSIGHT 6

Moderniser son workplace

Vers des environnements de travail hybrides et intégrés

Les enjeux de modernisation du workplace

La modernisation du workplace s'inscrit aujourd'hui dans une logique de réduction des coûts d'exploitation, de standardisation des environnements utilisateurs, mais aussi d'adaptation aux nouveaux usages professionnels : travail hybride, mobilité, collaboration en temps réel et sécurité renforcée.

Les organisations migrent progressivement vers des environnements cloud-first, portés par des solutions comme Microsoft 365, Intune et Windows 11.

1 sur 3

1 décideur sur 3 envisage d'accélérer sa transition vers un environnement de travail moderne, unifié et intégré.

Réduire les coûts d'infrastructure : en migrant les services Exchange, SharePoint, fichiers et messagerie instantanée vers le cloud, les entreprises allègent les charges liées à la maintenance des serveurs physiques, des solutions de sauvegarde, ou de l'infrastructure réseau interne.

Unifier la gestion des postes de travail et des terminaux mobiles, en s'appuyant sur une stratégie UEM (Unified Endpoint Management). L'intégration d'un MDM permet de gérer des postes Windows, Mac, iOS et Android depuis une console unique, avec des politiques de conformité, des configurations automatisées et une gestion du cycle de vie des devices.

Anticiper les exigences de sécurité dans un contexte BYOD et travail nomade, en adoptant une architecture Zero Trust, basée sur l'analyse du contexte d'accès (type de terminal, état de conformité, localisation, rôle utilisateur).

Challenges opérationnels dans des environnements hétérogènes et hybrides

Hétérogénéité des environnements IT

La modernisation du poste de travail s'effectue rarement dans un environnement homogène. Aujourd'hui, les DSI doivent composer avec une large diversité de terminaux : PC Windows, Mac, smartphones Android et iOS, postes durcis ou VDI. Cette pluralité rend complexe la standardisation des configurations, le suivi des mises à jour et le déploiement applicatif. Il devient alors indispensable d'adopter une approche de gestion unifiée des terminaux (UEM) capable de couvrir tous ces périmètres.

Transition vers la gestion moderne

La plupart des organisations partent d'un modèle on-premise structuré autour de SCCM, des GPO Active Directory et de scripts de déploiement maison. La bascule vers une gestion moderne implique une révision complète des processus. Il faut repenser l'enrôlement des postes avec Windows Autopilot, migrer les politiques de configuration dans Microsoft Intune, et transférer la gestion des identités vers Azure AD / Entra ID. Cette mutation implique une forte montée en compétence des équipes IT.

Sécurisation du BYOD et des usages mobiles

Le BYOD s'est largement démocratisé, mais il représente un véritable défi en matière de sécurité. L'entreprise n'a pas la maîtrise du terminal, mais doit protéger les données et les accès. La stratégie Zero Trust devient incontournable : chaque tentative de connexion doit être vérifiée, contextualisée et autorisée uniquement si le terminal est jugé conforme. Intune permet de combiner des approches MDM (Mobile Device Management) et MAM (Mobile Application Management) pour sécuriser les usages sans gérer physiquement les appareils.

Coexistence SCCM / Intune (co-management)

La gestion hybride, via le co-management SCCM/Intune, est une stratégie transitoire qui permet de tirer parti des forces de chaque solution : SCCM pour le déploiement de packages complexes ou la gestion logicielle sur site, Intune pour la configuration cloud-native, le BYOD et les politiques de conformité.

Migration vers Windows 11

Le passage à Windows 11 n'est pas qu'un simple changement de version. Il nécessite une revue complète du parc matériel, l'adoption de nouvelles normes de sécurité, ainsi qu'une mise à jour des outils de déploiement et de supervision.

Migrations inter-tenant Microsoft 365

Dans les contextes de fusions, acquisitions ou séparations d'activités, la migration d'un tenant Microsoft 365 vers un autre est une opération sensible et complexe. Un projet mal cadré peut entraîner des pertes de données, des interruptions de service ou une mauvaise adoption post-migration. Il est donc crucial de procéder par phases, avec des tests pilotes, une stratégie de coexistence et un accompagnement fort des utilisateurs.

Conseils de nos experts

Structurer les populations et les cas d'usage

Chaque profil utilisateur (terrain, administratif, direction, mobile) présente des besoins et des contraintes différents. Il est essentiel de créer des profils différenciés dans Intune, d'adapter les politiques de sécurité, et de personnaliser les outils selon les usages métiers.

Maintenir une gestion hybride pragmatique

Certaines organisations conservent des outils on-premise comme SCCM pour des raisons spécifiques : gestion logicielle avancée, bande passante locale, applications métiers non compatibles cloud. Il est alors pertinent de maintenir une architecture hybride, avec un socle cloud-first (M365/Intune), tout en conservant des relais locaux si nécessaire.

Déployer une stratégie Zero Trust complète

Au-delà du MFA, une vraie stratégie Zero Trust repose sur l'évaluation en temps réel de la posture de sécurité du terminal, la gestion conditionnelle des accès et le monitoring proactif des comportements anormaux via Defender for Endpoint et Microsoft Sentinel. Cela permet de renforcer la sécurité sans alourdir l'expérience utilisateur.

Industrialiser les déploiements et les mises à jour

Avec Autopilot, il est possible de provisionner automatiquement un poste de travail prêt à l'emploi dès la première connexion Internet, sans intervention IT locale. Combiné à Intune, cela permet de gérer les mises à jour, les applications et les configurations de manière fluide et cohérente.

Piloter les migrations de tenant avec méthode

Une migration Microsoft 365 réussie repose sur une phase de cadrage précise : inventaire, dépendances applicatives, mapping des identités, stratégie de coexistence. Il est recommandé de travailler par lots, utiliser des outils spécialisés (Quest, ShareGate, BitTitan...), prévoir une communication interne structurée et un support renforcé post-bascule.

Investir dans l'accompagnement et la montée en compétences

La modernisation du workplace est aussi un projet humain. Il est indispensable de former les équipes IT à l'administration des outils cloud, de sensibiliser les utilisateurs aux nouveaux usages collaboratifs, et de mettre en place un réseau d'ambassadeurs ou de «champions M365» dans les équipes métiers.

INSIGHT 7

Le numérique responsable : une priorité en devenir

Numérique responsable : un engagement en croissance

Les initiatives actuellement mises en place par les entreprises

Les priorités en matière de numérique responsable

Calcul des émissions

Parmi les premières initiatives en matière de numérique responsable, la mise en place d'un dispositif de calcul des émissions de CO_2 liées à l'IT s'impose comme une priorité. Plus de la moitié des décideurs interrogés déclarent avoir déjà initié cette démarche, signe d'une volonté croissante des entreprises de mieux comprendre l'empreinte carbone de leur système d'information. Cette approche traduit une première étape essentielle : mesurer avant d'agir.

Face à des environnements IT de plus en plus complexes, les organisations cherchent d'abord à établir un diagnostic précis. Cette phase d'évaluation permet de poser les bases d'une stratégie de sobriété numérique plus structurée et plus efficace.

Élaboration d'une feuille de route

39% des décideurs indique avoir formalisé une feuille de route en matière de numérique responsable. Cette démarche traduit une volonté d'inscrire les initiatives dans une vision de long terme, avec des objectifs clairs et alignés sur les ambitions globales de l'entreprise. Elle témoigne également d'une approche progressive et pragmatique : avancer étape par étape, en tenant compte des spécificités de l'organisation, pour construire un numérique plus sobre et durable.

Acculturation au changement

Le processus de sensibilisation et d'acculturation est également important pour 37% des répondants. Ce chiffre montre qu'au-delà des mesures techniques, une dimension culturelle et organisationnelle est jugée indispensable. Sensibiliser les équipes à l'impact environnemental des outils numériques et les former à des pratiques plus responsables est un levier essentiel pour ancrer le numérique responsable dans les comportements au quotidien.

Ce n’est pas une priorité immédiate

Si la prise de conscience autour du numérique responsable est bien présente, le passage à l’action reste encore contrasté selon les organisations. Ainsi, 19 % des décideurs interrogés affirment que ce sujet ne figure pas parmi leurs priorités pour 2025. Ce chiffre révèle une certaine disparité dans la maturité des entreprises face aux enjeux environnementaux du numérique.

Plusieurs facteurs peuvent l’expliquer : pression business plus forte sur d’autres axes stratégiques (performance, cybersécurité, innovation), manque de ressources dédiées ou encore difficulté à mesurer concrètement le retour sur investissement de ces initiatives. Ce constat souligne qu’en dépit des avancées, le numérique responsable peine encore à s’imposer comme un levier structurant dans toutes les feuilles de route IT. Il reste donc un enjeu d’acculturation, de pilotage et de démonstration de valeur pour accélérer son intégration au cœur des priorités technologiques.

1 sur 5

Près de 19 % des décideurs affirment que le numérique responsable n’est pas une priorité pour 2025. Le reste des répondants ont déjà engagé des actions, qu’il s’agisse du calcul des émissions, de l’élaboration d’une feuille de route, de l’acculturation au changement ou encore de la mise en place de nouveaux processus.

L’enquête démontre que de plus en plus de décideurs reconnaissent l’importance du numérique responsable et prennent des mesures pour en réduire l’impact environnemental. Toutefois, des efforts supplémentaires sont nécessaires pour surmonter les obstacles techniques, culturels et organisationnels. En définissant une stratégie claire, en formant les équipes et en adoptant des pratiques responsables, les entreprises pourront non seulement réduire leur empreinte écologique, mais aussi renforcer leur compétitivité et leur attractivité sur un marché de plus en plus sensible aux enjeux environnementaux.

Le numérique responsable est désormais un impératif pour les entreprises qui souhaitent concilier performance économique et respect des valeurs environnementales et sociales. C’est en intégrant ces principes dans la stratégie globale que les entreprises réussiront à se positionner comme des acteurs durables et responsables de demain

Conseils de nos experts

S'aligner avec une démarche FinOps

Intégrer les principes FinOps permet d'optimiser à la fois les coûts et la consommation énergétique des ressources IT. Cette approche favorise une meilleure visibilité sur les usages, tout en identifiant les leviers d'efficacité financière et environnementale.

Former des « évangélistes » internes

Identifier et accompagner des collaborateurs volontaires pour porter la démarche en interne permet de créer un effet d'entraînement. Ces référents jouent un rôle clé dans la sensibilisation, l'animation et la diffusion des bonnes pratiques au sein des équipes.

Adopter une démarche itérative

Plutôt que de viser une transformation radicale immédiate, il est plus efficace d'avancer progressivement. Tester des initiatives à petite échelle, mesurer les impacts, ajuster les actions : cette logique d'amélioration continue favorise l'adhésion et les résultats concrets.

Définir des objectifs atteignables mais ambitieux

Fixer des cibles réalistes, mais engageantes, permet de structurer la démarche tout en générant rapidement des résultats visibles. Ces "quick wins" contribuent à mobiliser les équipes et à démontrer la valeur ajoutée du numérique responsable.

Intégrer le « Green by design »

Penser la sobriété numérique dès la conception des projets (infrastructure, applications, services) permet d'agir en amont plutôt que de corriger a posteriori. Cette approche structurelle est un levier puissant pour limiter durablement l'impact environnemental du SI.

S'appuyer sur une expertise externe

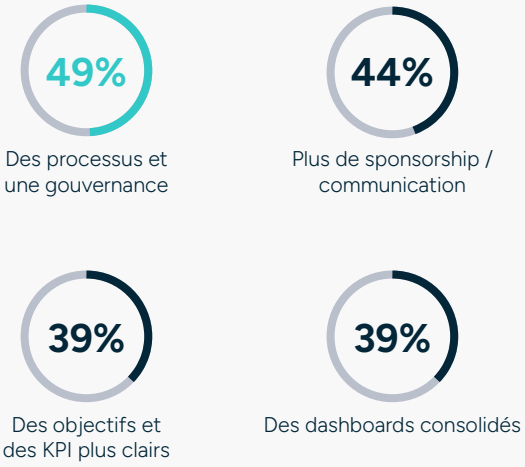
Faire appel à des experts ou à des cabinets spécialisés pour auditer les infrastructures, identifier les postes les plus émetteurs ou construire un plan d'action permet de gagner du temps, de sécuriser les choix techniques et d'accélérer la mise en œuvre.

INSIGHT 8

Gouvernance IT et conduite du changement

Gouvernance IT : entre agilité et transformation

Enjeux prioritaires pour optimiser le pilotage des activités IT



Des processus et une gouvernance renforcée

Près de la moitié des répondants indique que l'amélioration des processus et de la gouvernance représente un axe prioritaire. Cela souligne la nécessité de structurer davantage les activités IT, d'en assurer la conformité et la rigueur dans la gestion des projets.

Plus de sponsorship et de communication

Le sponsoring et la communication autour des projets sont également des leviers clés identifiés par les répondants. Un meilleur accompagnement des équipes et une communication transparente et régulière sont perçus comme essentiels pour garantir le succès des initiatives IT.

Des objectifs et des KPI plus clairs

Les répondants considèrent qu'une des priorités majeures pour l'amélioration du pilotage réside dans la clarification des objectifs et des indicateurs de performance (KPI). Cela reflète un besoin d'alignement stratégique plus fort, de mesure de la performance plus précise et d'une meilleure traçabilité des résultats.

Des dashboards consolidés

L'importance des outils de pilotage, et plus spécifiquement des dashboards consolidés, ressort clairement. Ces outils permettent une vue d'ensemble, facilitent la prise de décision rapide et la communication entre les différents acteurs impliqués dans les projets IT.

Des défis liés à l'évolution de la gouvernance, des processus IT et de la conduite du changement

Complexité de l'intégration des nouvelles technologies

La généralisation de technologies et pratiques nouvelles (IA, cloud, DevSecOps…) nécessite une révision continue des processus IT existants. L'un des principaux défis réside dans l'intégration de ces nouvelles technologies tout en maintenant une gouvernance robuste.

Alignement stratégique et agilité

Les entreprises doivent parvenir à équilibrer agilité et rigueur dans la gestion de leurs projets. Une gouvernance trop rigide peut nuire à la réactivité des équipes, tandis qu'une trop grande flexibilité peut rendre le pilotage difficile. Trouver cet équilibre est crucial.

Adoption de nouveaux modes de travail

Les méthodes agiles, la montée en puissance des équipes distribuées et l'évolution des pratiques de conduite du changement créent de nouvelles dynamiques. La gestion des changements organisationnels et des attentes des parties prenantes devient de plus en plus complexe.

La gestion des données et la consolidation de l'information

Le besoin de dashboards consolidés met en lumière la problématique de la gestion des données, de leur fiabilité et de leur accessibilité. Une gouvernance de données efficace est nécessaire pour fournir des informations précises et à jour, afin de faciliter la prise de décision.

Manque de sponsorship et de communication

Le soutien du top management et une communication fluide au sein des équipes sont des facteurs clés de réussite des projets IT. Sans une vision claire du top management, les initiatives peuvent manquer de direction et d'adhésion.

Les résultats de cette enquête soulignent un besoin fort de structuration et d'amélioration des dispositifs de pilotage, de gouvernance et de conduite du changement au sein des DSI et des équipes projet. Les priorités identifiées par les répondants, telles que la clarification des objectifs, la consolidation des dashboards et le renforcement de la gouvernance, témoignent d'une volonté d'optimiser la gestion des projets IT pour mieux répondre aux exigences stratégiques de l'entreprise.

L'avenir de la gouvernance IT repose sur la capacité des DSI à adopter une vision claire, à intégrer les nouvelles technologies de manière cohérente, et à maintenir une dynamique de changement constante pour répondre aux attentes croissantes des parties prenantes.

Conseils de nos experts pour des solutions court terme

Réaliser un audit des processus existants

Les entreprises doivent cartographier leurs processus IT critiques, identifier les inefficacités et les points de frictions, et évaluer leur alignement avec les objectifs stratégiques. Cela inclut une évaluation complète des systèmes en place pour repérer les goulots d'étranglement et les failles potentielles en matière de cybersécurité.

Définir une stratégie IT alignée avec la vision de l'organisation

La gouvernance doit être adaptée aux besoins de l'époque en adoptant des cadres tels que COBIT ou ITIL, tout en intégrant des approches agiles pour une exécution rapide et flexible. Les métiers doivent être représentés à un niveau stratégique pour garantir que les objectifs technologiques répondent efficacement aux besoins opérationnels sans alourdir les processus décisionnels.

Renforcer la transparence dans la prise de décisions IT

Mettre en place des comités transverses avec une participation active des parties prenantes internes et externes. Cela inclut notamment des échanges réguliers avec les responsables de certains métiers clés, comme les ressources humaines ou la production, pour aligner les initiatives IT avec les besoins du terrain et du marché.

Automatiser ses processus

L'automatisation des processus répétitifs ou chronophages permet de réduire les erreurs, d'améliorer l'efficacité et de libérer des ressources pour des tâches à plus forte valeur ajoutée. Si les métiers ne sont pas directement impliqués dans la configuration technique, il est essentiel de prendre en compte leurs besoins spécifiques pour optimiser les outils et flux de travail.

S'assurer de la conformité réglementaire et éthique

Avec une augmentation des lois sur la protection des données et les régulations technologiques, les processus IT doivent intégrer des mécanismes de surveillance et de conformité continue. Bien que cette tâche relève principalement des équipes IT, les métiers peuvent être formés pour renforcer une application cohérente et éviter les écarts réglementaires.

Favoriser une culture de responsabilité collective

L'adhésion des employés aux nouvelles gouvernances repose sur une communication claire et une implication active de tous les niveaux hiérarchiques. Des initiatives spécifiques peuvent inclure des programmes de sensibilisation pour les métiers les plus concernés par les changements technologiques, afin de maximiser leur adoption et leur implication.

Conclusion

Si les priorités 2025 pour les DSI dessinent clairement les contours des enjeux technologiques actuels - cybersécurité, le cloud, l'IA, l'automatisation des processus - le véritable défi stratégique réside désormais dans la capacité à **sortir d'une posture défensive pour construire une approche véritablement offensive et génératrice de valeur**.

Il s'agit de développer une approche proactive de la performance IT où chaque investissement devient un levier de création de valeur, en repensant les modèles économiques internes et en construisant des architectures IT plus agiles et adaptables.

La DSI doit se positionner comme un partenaire stratégique, capable de placer le changement au cœur de sa démarche. Cela implique de dépasser la pure dimension technologique et devenir un architecte du changement, en développant une culture de la collaboration, en anticipant les résistances et en créant les conditions d'une transformation qui fait sens pour tous.

L'enjeu est de transformer la perception traditionnelle de la DSI : passer d'un service technique contraint à un facilitateur d'innovation, capable de concilier performance technologique et épanouissement collectif.

Remerciements

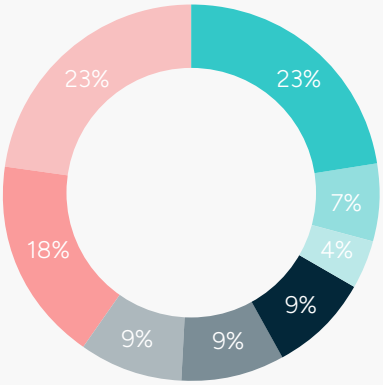
Nous tenons à remercier chaleureusement l'ensemble des décideurs et professionnels IT qui ont contribué à cette enquête. Leur vision, leur expérience et leur engagement ont permis d'enrichir cette étude et de dresser un panorama concret et utile des défis à venir. Grâce à leurs retours, ce rapport se veut un outil de réflexion pour tous ceux qui construisent l'IT de demain.

Noël Cavaliere
Directeur Technique du CRiP

Enquête menée auprès d'un panel de 60 décideurs

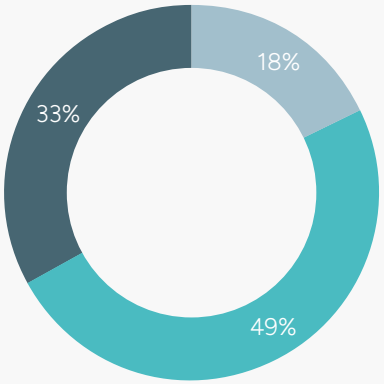
Fin 2024, Synapsys et le CRiP ont lancé une enquête visant à établir un état des lieux des tendances et des priorités en matière d'infrastructures en 2025. Pour approfondir ces orientations, un questionnaire a été adressé à des décideurs pour comprendre leur vision et leurs convictions en matière de gestion et de modernisation des infrastructures informatiques.

Secteurs d'activité représentés



- Banque / Finance / Assurance
- BTP / Immobilier
- Distribution
- Énergies / Utilities
- Industrie
- Retail / Luxe
- Secteur public
- Services

Taille des entreprises interrogées



- Moins de 500 salariés
- De 501 à 5 000 salariés
- Plus de 5 000 salariés

À propos de Synapsys

Synapsys est un acteur de référence spécialisé dans la transformation des infrastructures IT. Depuis plus de 12 ans, nous accompagnons nos clients tout au long du cycle de vie des projets d'infrastructure à travers nos expertises en Digital Workplace, Cloud, DevOps, Cybersécurité, Data/IA et Transformation des SI.

Synapsys propose à ses clients un service technologique de qualité, grâce à l'esprit collectif et engagé de ses 180 talents répartis à Paris, Lille, Lyon et Kuala Lumpur.

Nous sommes fiers d'être considérés comme un partenaire de confiance et plébiscités pour la réalisation de projets de transformation structurants. Nos clients grands comptes nous sollicitent pour bâtir des infrastructures agiles et résilientes afin de relever les défis de transformation digitale de demain.

Convaincus que tout projet doit apporter le progrès et toute collaboration, la confiance, nous avons à cœur de proposer une vision de l'entreprise inclusive et équitable. Nous faisons du développement des hommes un véritable modèle d'entreprise qui guide nos orientations stratégiques, notre culture et notre mode de fonctionnement.

Chez Synapsys, c'est la force du collectif, l'engagement, l'équité et l'authenticité qui priment. Nous mettons tout en œuvre pour que chacun ait l'opportunité de se développer professionnellement dans un climat de confiance autour d'un projet commun.

www.synapsys-groupe.com
Crédit images : Synapsys & Adobe Stock

Contact Synapsys

Nathalie Hoyos
Directrice Marketing
nhoyos@synapsys-groupe.com

À propos du CRiP

Le CRiP, le cercle de confiance des décideurs de l'IT, rassemble 14 000 responsables d'infrastructure, de technologies et de production informatique issus de 350 grands comptes, entreprises et administrations.

Espace d'échange entre pairs, il permet de confronter et de benchmarker ses expériences, ainsi que de partager ses bonnes pratiques de manière agnostique et authentique. Pour accompagner ses adhérents, le CRiP propose plus d'une dizaine de groupes de travail dédiés à des thématiques clés comme la cybersécurité, le cloud, le FinOps ou encore le numérique responsable. Il produit également des livrables et organise plus de 50 événements à Paris et en région afin d'échanger sur les tendances et meilleures pratiques du secteur.

Rejoindre le CRiP, c'est :

- Profiter du partage d'expérience de vos pairs,
- Se créer un réseau solide,
- Disposer d'une veille technologique pertinente et ciblée.

www.crip-asso.fr

Contact CRiP

Sylvie Roche
Directrice Générale
roche.sylvie@crip-asso.fr

Synapsys

www.synapsys-groupe.com

7 rue Scribe 75009 Paris
01 84 16 49 71 - contact@synapsys-groupe.com