L'Essentiel du DSI

Tech & Business

1er trimestre 2026

Facture électronique : ces 42 cas d'usages qui mettent l'IT sous pression

Métiers

Cloud souverain : le défi des intrications IT et juridiques

Business & Tech

EUDI Wallet : d'une économie de l'identité à celle de la preuve

Focus

Hardening : durcir l'IT, l'infra... ?

Les Echos PUBLISHING

oci INFORMATIQUE & DIGITAL

O ' W O R K
groupe OCI

LA FACTURE ÉLECTRONIQUE C'EST O'WORK

Pensé pour, par et avec les clients OCI

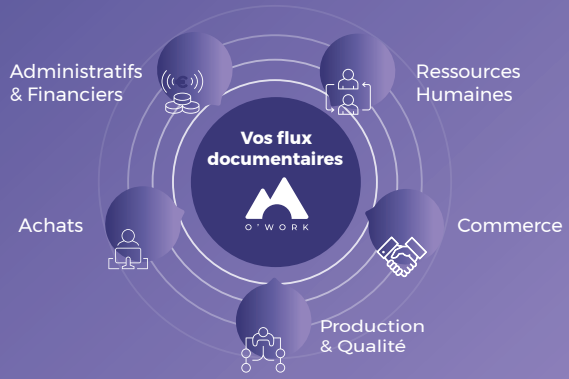
Exclusivement réservé aux clients du Groupe OCI

- **Conforme avec les exigences légales** *(Factur-X, archivage coffre-fort numérique, piste d'audit fiable)*

Plateforme agréée avec ESKER

- **Solution française souveraine**
- **Support en France**
- **Factures clients et fournisseurs**
- **Simple et puissant à la fois**

O'Work, c'est aussi la plateforme qui centralise et automatise tous vos flux documentaires



Édito

Cloud souverain : IT et DSI au centre d'enjeux géopolitiques et juridiques

Romuald VALICHON
Directeur général du Groupe OCI

Vous avez aimé le green washing ? Vous adorez déjà sans doute son équivalent en matière de souveraineté numérique. Quoi de plus trompeur en effet que de nombreuses offres de cloud qui n'ont de souverain que le nom ?

Pour quelle raison ? Quel que soit l'endroit où se trouvent les serveurs, dès lors que vous avez affaire à une entreprise américaine ou une entreprise ayant un lien avec les États-Unis, celle-ci est soumise à des lois extraterritoriales, comme le Cloud Act, qui l'obligent à communiquer au gouvernement américain les données qui s'y trouvent quand on le leur demande.

Et comme la situation géopolitique actuelle est particulièrement tendue, de nombreuses entreprises sont désormais soucieuses de devenir aussi résilientes qu'elles le peuvent face à cette dépendance. L'enjeu est d'autant plus important que se développe le recours à l'IA, à l'IA agentique, qui sont autant de leviers de compétitivité que de sources de dépendance et d'insécurité pour leurs données notamment. Y voir clair est essentiel, avec des informations précises, fiables et digestes.

C'est un des sujets que nous abordons dans ce premier numéro de *L'Essentiel du DSI*, réalisé en partenariat avec Les Echos Publishing. Vous trouverez également un dossier sur la facture électronique et des articles sur le hardening ou les principales erreurs commises en matière de cybersécurité.

Notre objectif est de vous fournir, chaque trimestre, une synthèse éclairée des évolutions économiques, technologiques et business susceptibles d'influencer votre activité. Cette ressource est pensée pour inspirer vos réflexions et nourrir les échanges avec les opérationnels et vos instances dirigeantes.

Nous vous souhaitons une lecture fructueuse !

L'Essentiel du DSI est édité par la société GROUPE OCI SAS, au capital social de 613 500 €, immatriculée au RCS de Strasbourg
sous le numéro 502 770 118
Siège social : 2 rue Ampère, 67450 Mundolsheim
Tél. : 09 69 39 40 60
Directeur de la publication : Frédéric VACHER
Conception et rédaction : Les Echos Publishing filiale du Groupe
Les Echos - Société anonyme au capital de 306 000 000 euros - 349 037 366 RCS Paris

Mis sous presse le 11 mars 2026 - N°01 - Dépôt légal mars 2026
Imprimerie MAQPRINT (87) • Photo couverture : Grady Reese/peopleimages.com - stock.adobe.com

PEFC 10-31-3162
IMPRIM'VERT®
BAC DE TRI

70 000 défaillances d'entreprises en 2025

L'année 2025 s'est conclue sur un triste record avec 69 957 défaillances enregistrées, soit 2 127 de plus qu'en 2024 et 11 944 de plus qu'en 2023. Dans le détail, la situation des PME-ETI d'au moins 100 salariés continue de se dégrader, rappelle l'étude d'Altares. 58 PME-ETI ont ainsi fait défaut au 4e trimestre, soit 18,4 % de plus qu'en 2024 contre une augmentation de seulement 1,7 % pour les entreprises de toutes tailles. Sur l'année 2025, la hausse des défaillances des entreprises de plus de 100 salariés atteint même 18,6 % (contre 3,1 % au global), pour un total de 236 procédures collectives.


REDAKTION83/ADOBE STOCK

Il faut toutefois noter que le pourcentage de liquidations judiciaires n'est que de 11 % sur cette taille d'entreprises contre 67 % sur l'ensemble des structures en 2025.

Les PME employant de 50 à 99 salariés enregistrent, quant à elles, une baisse de 3,3 % du nombre de défaillances sur un an au cours du 4e trimestre 2025, contre des diminutions de 5,3 % pour les PME de 20 à 49 salariés et de 8,3 % pour les PME-TPE employant entre 10 et 19 salariés.

Lithium

Sécuriser les approvisionnements en matières premières critiques est une priorité. Raison pour laquelle l'État vient d'annoncer une prise de participation dans une mine de lithium située dans l'Allier, exploitée par le groupe Imerys. L'investissement de l'ordre de 50 M€ va permettre à Imerys de finaliser l'étude de faisabilité. Une fois en activité, le site devrait garantir l'extraction de 34 000 tonnes d'hydroxyde de lithium par an. Une production suffisante pour équiper plus de 600 000 véhicules électriques.

Nouvelles technologies : quid des entreprises européennes ?

Les entreprises européennes adoptent de plus en plus de nouvelles technologies dans le but d'améliorer leur productivité et, plus largement, leur compétitivité.

Dans son rapport annuel (EIB Investment Survey 2025), la Banque européenne d'investissement (BEI) nous apprend que 77 % des 13 000 entreprises de l'UE interrogées utilisent désormais des technologies numériques avancées telle que l'intelligence artificielle, le big data ou les drones. Un taux d'adoption équivalent à celui des entreprises américaines (78 %).

Côté secteurs, avec un taux d'adoption de 81 %, c'est l'industrie qui est en pointe en Europe devant les entreprises d'infrastructure (énergie, transport… 79 %), le secteur des services (72 %) et celui de la construction (58 %). Dans le détail, l'industrie européenne apparaît même plus investie dans les nouvelles technologies que l'industrie américaine. On note ainsi que le niveau de robotisation des entreprises du Vieux Continent (55 %) est bien supérieur à celui des entreprises américaines (36 %). Les entreprises européennes manufacturières devancent également leurs concurrentes américaines dans l'internet des objets (51 %, contre 47 %), l'utilisation du big data et de l'intelligence artificielle (48 %, contre 28 %), mais aussi celle des dispositifs d'impression 3D (40 %, contre 38 %).

48 %

Près d'un Français sur deux utilise l'IA générative, nous révèle le Baromètre 2026 du Crédoc. Un usage particulièrement répandu chez les 18-25 ans (85 %) qui l'utilisent pour rechercher des informations (73 %), rédiger des textes (58 %), trouver des idées (57 %), créer des contenus (42 %) ou encore faire du codage (30 %). On note que l'utilisation de l'IA est très élevée chez les cadres, réduite chez les ouvriers (38 %) et limitée chez les retraités (17 %). Sans surprise, ChatGPT reste l'IA la plus sollicitée (79 %) devant Gemini (31 %).

L'immigration soutient l'économie européenne

Dans sa note de conjoncture de décembre 2025, l'Insee est revenu sur le poids de la main-d'œuvre née à l'étranger dans les principales économies de la zone euro. Cette étude relève que la population immigrée en âge de travailler représentait en 2024, en France, 14,3 % de l'ensemble des 15-64 ans, 14,8 % en Italie, 22,7 % en Espagne et 23,6 % en Allemagne. D'un point de vue économique, l'immigration dans ces 4 pays européens s'est traduite par une dynamique de croissance en stimulant la demande et en augmentant la population active.

À l'appui de cette analyse, l'Insee cite une étude de la Banque d'Italie réalisée en 2025 qui considère qu'entre 2005 et 2023, « sans immigration, la croissance de l'emploi aurait été au moins deux fois plus faible en Allemagne et en France, nulle en Espagne et négative en Italie ». Et la progression de l'emploi des personnes nées à l'étranger ne résulte pas seulement d'un effet démographique, mais s'explique aussi par une amélioration de leur insertion sur le marché du travail. Le taux d'emploi des personnes nées à l'étranger a ainsi augmenté en France, en Espagne et en Italie entre 2019 et 2024. En France, cette hausse est portée majoritairement par les femmes, à l'inverse des autres pays européens.

Le déficit commercial a reculé en 2025

Après avoir atteint un plus haut historique en 2022 (161,7 Md€), suite à la crise sanitaire, le déficit commercial de la France poursuit son repli. En 2025, selon les Douanes, il a atteint 69,2 Md€, soit 10 Md€ de moins qu'en 2024. Une amélioration dopée par la baisse des prix du pétrole conjuguée à la dépréciation du dollar face à l'euro. Globalement, les exportations ont progressé de 2,5 % en 2025 pour atteindre 614,7 Md€. Ce rebond est dû à la hausse des livraisons de produits aéronautiques et à une bonne dynamique des exportations pharmaceutiques et électroniques.

Les importations, de leur côté, ont atteint 703,6 Md€ en 2025. Elles s'inscrivent en hausse de 0,7 %, portées par l'augmentation de 2,9 % des importations de produits manufacturés, notamment aéronautiques et agroalimentaires.

IBRAVERY/ADOBE STOCK

La stratégie cyber 2026-2030 de la France : un bouclier renforcé pour les PME & ETI

La France lance sa stratégie cyber 2026-2030 pour une cybersécurité partagée, essentielle aux PME et ETI. Face à des menaces sophistiquées, elle vise à transformer leur protection numérique. Le plan insiste sur le développement des compétences cyber, via la formation continue et l'encouragement des entreprises à former leurs équipes IT, reconnaissant que l'ingénierie sociale est responsable de 80 % des incidents.
La résilience est renforcée par l'Observatoire de la résilience cyber, offrant benchmarking et aide à la justification budgétaire. Le nouveau « label PME », inspiré de NIS 2 (cf. p.14), attestera de la robustesse cyber, devenant un atout commercial.
La stratégie anticipe les menaces futures avec l'IA sécurisée et la cryptographie post-quantique (PQC), invitant les PME/ETI à auditer leurs systèmes. Enfin, la systématisation des exercices de crise (PCA/PRA) et l'automatisation via les SOC/SOAR sont des standards désormais incontournables. Cette stratégie valorise également les solutions européennes, offrant un cadre de confiance et des opportunités stratégiques.

DDoS

2025 a été marquée par une recrudescence des attaques DDoS, avec une augmentation de 170 % par rapport à 2024 (Cloudflare), due à la facilité d'accès aux outils d'attaque, aux tensions géopolitiques et à l'émergence de botnets puissants comme Aisuru. Les secteurs stratégiques, tels que les opérateurs télécoms et les services publics, sont particulièrement visés. Face à des attaques volumétriques et des menaces plus discrètes exploitant des failles, il est impératif d'adopter des défenses automatisées, de renforcer la résilience des infrastructures critiques, de diversifier les environnements techniques et de sécuriser des éléments clés comme le DNS.


SEVENTYFOUR/ADOBE STOCK

Le boom des data centers se confirme en France

Les investissements étrangers directs (IED) dans les centres de données connaissent une hausse exponentielle. Notre pays s'arroge un quart des sommes investies dans le monde, soit 58 milliards d'euros en 2025. La France dépasse de loin tous les autres pays, États-Unis inclus, même si les IED n'intègrent pas les capitaux déployés par les multinationales américaines sur leur propre sol. Ce succès est dû au coût abordable et relativement stable de l'énergie.

G7

En janvier 2026, l'ANSSI a pris la tête du groupe de travail sur la cybersécurité du G7, plaçant la France au centre de l'agenda numérique international. Quatre priorités ont été définies pour la rencontre de juin : sécuriser l'IoT industriel par des standards minimaux, préparer la transition vers la cryptographie post-quantique face aux ordinateurs quantiques, garantir la sécurité et l'intégrité de l'intelligence artificielle, et renforcer les partenariats public-privé contre les cybermenaces.
Ces initiatives visent une résilience numérique holistique : les décisions du G7 influencent souvent les futures réglementations européennes.

L'IA agentique source de défis transformateurs

La perspective d'avoir des systèmes autonomes capables de raisonner, planifier et agir sans intervention humaine va entraîner une profonde transformation des systèmes d'information (SI).

Sortir des silos : l'IA agentique doit pouvoir « dialoguer » directement avec les outils métiers et les bases de données de l'entreprise pour être pleinement efficace. L'architecture en silos et le cloisonnement des applications ne permettent pas de répondre à cet enjeu. Le SI doit devenir modulaire, être capable d'intégrer de nouveaux services et des API facilitant les échanges.

S'assurer de la qualité des données : alimentée par des données fausses ou partielles, l'IA pourrait commettre des erreurs dans ses décisions. Cela implique un renforcement drastique des processus de collecte, de validation et d'enrichissement des données et des agents eux-mêmes (cf. p.14).

Renforcer la gouvernance : il est impératif d'établir des cadres clairs et des comités de suivi pour l'éthique, la transparence et la responsabilité des IA, garantissant leur alignement avec les valeurs de l'entreprise et la conformité réglementaire.

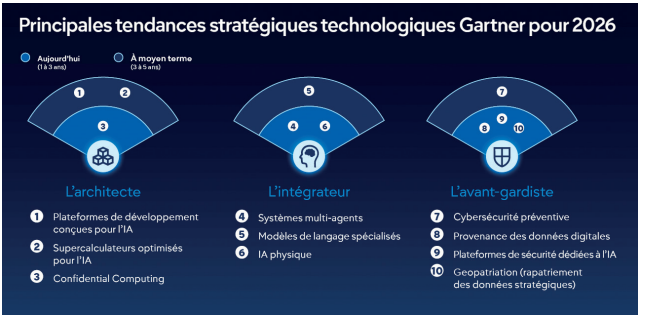
5G en Europe : l'exclusion chinoise, opportunité ou risque maîtrisé ?

L'UE a décidé d'exclure les équipementiers télécoms chinois (Huawei, ZTE), considérés comme « à haut risque », de ses réseaux 5G. Visant à contrer l'espionnage, cette mesure crée une opportunité économique majeure pour Nokia et Ericsson, ouvrant le marché du remplacement des 40 % d'antennes chinoises existantes.
Cependant, cette décision suscite des interrogations.
Malgré le potentiel de milliards d'euros d'investissements, la hausse des commandes n'est pas encore visible, et les opérateurs craignent un « séisme financier et technologique » en raison des coûts induits.
De plus, une critique de « deux poids, deux mesures » est formulée, pointant que l'exclusion se concentre sur la Chine sans aborder les risques similaires liés à certains fournisseurs américains.

MAURICE NORBERT/ADOBE STOCK

10 tendances tech stratégiques en 2026 pour les DSI

À l'occasion de son IT Symposium/Xpo de 2026, Gartner a mis en avant les prochains leviers au service des DSI et de leurs équipes.
Au-delà de l'observation d'innovations émergentes, 10 tendances ont été classées en deux horizons de temps et 6 sont à considérer à court et moyen termes :



• **Le confidential computing,** assurant le traitement sécurisé des données en mémoire et rendant possible le déploiement sécurisé de l'IA et de solutions d'analyse de données sur des infrastructures non approuvées.

• **Les systèmes multi-agents,** favorisant la coopération entre agents d'IA modulaires pour la gestion de tâches complexes, permettant le déploiement à grande échelle d'automatisations.

• **L'IA physique,** avec des robots, des drones, des véhicules et des dispositifs intelligents capables de percevoir leur environnement, de décider et d'agir de manière autonome.

• **Le filtrage via la provenance des données digitales,** afin d'articuler le besoin de données et la sécurisation de celles-ci dans des écosystèmes toujours plus complexes.

• **Les plateformes de sécurité dédiées à l'IA,** dont plus de 50 % des entreprises devraient s'être dotées d'ici 2028.

• **La géopatriation,** soit la relocalisation de charges de travail depuis des clouds hyperscale internationaux vers des environnements souverains ou locaux, dans le but de réduire les risques géopolitiques.

Top 3 des risques business

Si les risques cyber, l'IA et l'interruption des activités dominent le baromètre 2026 de l'assureur Allianz, ce sont les confrontations géoéconomiques, les conflits armés entre États et les phénomènes météorologiques extrêmes qui sont relevés par le Forum économique mondial. Or, les conflits géoéconomiques et les conflits armés débouchent souvent sur des risques tech, de sécurité ou de dépendance.

DC STUDIO/ADOBE STOCK

Cloud souverain : le défi des intrications IT et juridiques

Les fondamentaux : la définition de la souveraineté numérique

1. Maintenir le service sans dépendre d'une puissance étrangère
2. Assurer que la protection des données soit garantie par le système juridique d'un pays membre de l'UE

Les 3 piliers essentiels du cloud souverain

Cloud non souverain — Cloud hybride/de confiance — Cloud souverain

Localisation des données

Sur territoire national/EU, soumises aux lois locales ou en dehors de l'UE

Nationalité du prestataire

(siège dirigeant et capital)

Aucun lien avec un acteur externe à l'UE ; lien encadré par une certification SecNumCloud (version 3.2 ou inférieure) ; autre situation

Maîtrise technologique réelle

Contrôle des technologies sous-jacentes allant jusqu'à la capacité de faire tourner le code dans son cloud grâce à ses seules ressources et compétences propres et sans intervention extérieure

Les exigences clefs

Dans tous les cas, les prestatataires doivent être capables d'assurer :

Contrôle accès / exploitation • Immuabilité / intégrité • Auditabilité / transparence

Le virage vers le cloud souverain exige donc un calcul stratégique.

Habitués à des solutions « non souveraines », nous savons que l'indépendance totale – garantissant la protection de l'accès aux données et la continuité – a un prix. L'essentiel est de calibrer avec précision l'effort financier face au degré de protection recherché, afin de positionner le curseur au juste niveau d'autonomie stratégique adapté à l'entreprise.

GETTYIMAGES-PHIL LEO / MICHAEL DENORA

Facture électronique : ces 42 cas d'usages qui mettent l'IT sous pression

En croisant les approches DSI, métiers et comptabilité, il est possible de dégager principes structurants, questions clefs et bonnes pratiques valorisant les compétences de chacun et assurant une efficace collaboration.

Avec deux ans de retard, la facture électronique s'imposera le 1er septembre 2026 à toutes les entreprises assujetties à la TVA. Derrière l'obligation légale, les entreprises découvrent un projet d'une ampleur certaine mettant en tension et nécessitant la collaboration des équipes IT, opérationnelles et comptables.

Des cas d'usage pour matérialiser les obligations

L'État a eu le souci de bien faire les choses et a fourni aux entreprises une listes de 42 cas d'usage. Ces der-

niers permettent de saisir toutes les situations concrètes concernées par la réforme et de rendre possible leur transformation en flux de données.
Le défi pour chaque entreprise est alors de déterminer comment appliquer ces cadres à ses propres pratiques et/ou comment faire évoluer ses pratiques pour être en accord avec les cadres qui s'imposent à elle. Mais plus l'entreprise est importante, utilise des processus de facturation et des outils variés, et plus son organisation est décentralisée, plus le travail s'avère complexe. Une méthode se dégage pour y faire face, permettant d'élaborer une feuille de route propre à chaque entreprise.

Cartographie et étude d'impact

La première étape consiste à avoir une vision claire et exacte de sa propre réalité au regard de la réforme. Cela commence par une cartographie exhaustive des outils et processus de facturation utilisés dans l'entreprise, mais aussi de ses solutions informatiques. Cette base permettra de réaliser une étude d'impact qui fera ressortir tous les champs nécessaires pour la facture électronique et toutes les adaptations et règles de gestion à mettre en place dans chaque système.

Le choix de l'architecture adaptée

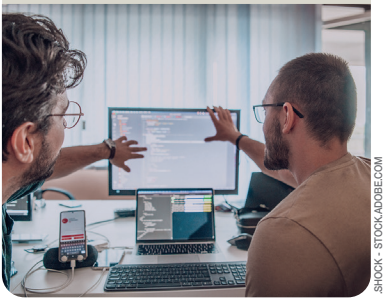
Cette vision claire servira à penser l'architecture cible devant être mise en place. C'est à cette étape que chaque entreprise sera sans doute amenée à choisir entre une solution consistant à rationaliser les différents outils pour n'avoir qu'un seul point de contact avec la plateforme agréée (PA) ou, au contraire, conserver une diversité des outils et construire des interfaces entre chaque système de facturation existant et la PA. Puis sera engagée la rédaction du cahier des charges pour finir par choisir la PA.

L'équipe projet, clef de la réussite

L'une des plus importantes clefs de réussite concerne la création de l'équipe projet. Repousser les approches binaires consistant à faire prévaloir l'approche SI ou l'approche comptable serait la meilleure solution : choisir des personnes des deux mondes, ayant à chaque fois une expérience importante, et les engager sur le long terme. Responsabiliser chacun et déléguer en favorisant l'appropriation du projet est un autre facteur de

Recourir à un conseil externe ?

Utile avec une organisation complexe et décentralisée, des outils et des processus variés. L'enjeu ? Toujours rester en position de comprendre les solutions proposées et de décider par soi-même. Et donc repousser les feuilles de route préconçues.



.SHOCK - STOCK.ADOBE.COM

101

plateformes agréées dans le cadre de la réforme au 16/01/2026,

dont 32

ont déposé un dossier complet et sont en attente d'immatriculation définitive conditionnée à la réussite aux tests d'interopérabilité.

Solution comptable française ou européenne ? C'est un avantage. Les éditeurs ont compris que la conformité à la réforme était indispensable. Les enjeux sont bien pris en compte et les évolutions de leurs systèmes sont faites.

succès. Enfin, la direction du projet, reposant naturellement sur ses sponsors (directeur SI/directeur financier) positionnés en arbitres, distinguera utilement quelques groupes de travail avec des périmètres d'action précis (revue des cas d'usage, évolutions SI, master data, mise en place de la PA…).

Les outils de monitoring

Chaque cas d'usage étant une imbrication de pratiques métiers et d'enjeux technologiques, l'entreprise aura besoin d'un monitoring du pilotage de l'interface et de la bonne réalisation des flux, apporté par la DSI. Mais il lui faudra aussi s'assurer de la bonne conciliation des données de gestion et comptables et de leur bonne arrivée dans la PA et jusqu'à l'administration. Le métier et la comptabilité seront alors à la manœuvre.

Cas d'usage et arbitrages

Tout au long du projet, si la DSI est incontestablement la mieux positionnée pour choisir techniquement les solutions les plus pertinentes en les ayant exposées aux métiers concernés, il est indispensable d'établir des avis métiers sur chacun des cas d'usage qui concernent l'entreprise. Et certains pourront conduire à revoir les solutions business.

Le coût financier du projet

Mais la conduite de ce projet a toujours un coût, qui appelle à adopter une vision très réaliste. Un DSI d'une filiale d'un groupe du CAC40 nous a confié : « Compte tenu de notre maison-mère, beaucoup imaginent que nos moyens sont très conséquents, notamment pour conduire un tel projet. Il est certain que tout aurait été beaucoup plus simple en prenant le module de facture électronique proposé par notre ERP. Mais le coût était tel, que nous avons opté pour des développements spécifiques. Outre le gain financier, le bénéfice a été important en matière d'interfaçage entre les différents métiers concernés.» Une approche dans laquelle se reconnaitront de nombreux DSI d'ETI ou même de PME.

Secret de réussite : se parler

La clé est que les valeurs perçues de l'IT et des équipes compta et métiers soient importantes les unes pour les autres. Bonne pratique : mettre en place une réunion mensuelle questions/réponses, permettant de lever les doutes et d'inspirer les solutions, mais aussi d'aborder un cas précis en 5 à 10 minutes.

FLAMINGO IMAGES/ADOBE STOCK

3 cas d'usage pour illustrer les arbitrages potentiels

1. Les débours

Les débours semblent apparaître hors du cadre de la réforme. Cependant, un cas d'usage (n°15) prévoit la situation dans laquelle des factures sont adressées à un tiers et réglées par un autre tiers, on parle alors de « débours ». Dans ce cas, il faut que le prestataire émettant la facture (A) envoie cette dernière à l'entreprise qui doit la payer (C) puis que celle-ci la mette à disposition par tout moyen à sa convenance à l'entreprise intermédiaire (B). Or il est fréquent que les débours soient utilisés dans des activités de masse où il est quasi impossible de gérer cela opérationnellement. Une solution business est d'abandonner les débours au profit d'un forfait permettant à l'entreprise intermédiaire (B) de recourir à une facturation achat/vente.

2. L'auto-facturation

L'auto-facturation (n°19b) se présente par exemple dans le cas des activités de vente via des plateformes. Une plateforme (A) est alors autorisée à éditer au nom du vendeur (B) une facture destinée à la plateforme elle-même. Cela conduit l'entreprise vendeuse (B) à avoir en factures entrantes ses propres factures émises par des tiers. Afin d'éviter d'avoir une interface descendante vers un système de facturation client, là encore, il peut être envisagé de modifier la manière d'agir du business.

PATPITCHAYA/ADOBE STOCK

3. Les notes de restaurant

Les notes de restaurant (n°28) confrontent deux univers de traitement qui ne se parlent pas, soit les systèmes de notes de frais et de facturation. Au-dessus de 150 euros, quand une note est destinée à une société, il lui faut émettre une facture via e-invoicing, y compris si celle-ci a déjà été payée par le collaborateur. Or, il peut arriver facilement que le statut « payé » ne soit pas correctement rempli ou vérifié et l'entreprise débitrice pourrait se retrouver à régler deux fois la même facture, une fois en remboursant le collaborateur et une fois directement à l'établissement. Là encore, cela peut faire l'objet d'arbitrage de traitement selon les volumes gérés afin de déterminer s'il est préférable d'obtenir une facture au nom de la société et de pouvoir ainsi récupérer la TVA ou s'il serait plus pratique de se contenter d'une facture au nom du collaborateur, sans e-invoicing mais sans récupération de la TVA.

Auditeur IA

L'essor de l'IA fait naître un nouveau rôle essentiel : l'auditeur IA.
Tel un auditeur financier, il garantit la fiabilité et la responsabilité des systèmes IA face aux défis (données, biais). Ses missions incluent supervision technique, surveillance comportementale et application de garde-fous pour prévenir les risques critiques (accès non autorisé, biais cachés).
Ce rôle, encore rudimentaire mais stratégique, exige des compétences pluridisciplinaires et voit l'émergence de cabinets tiers pour assurer une IA éthique et sécurisée.

RAWINTANPIN/ADOBE STOCK

FinOps & IA : optimisation de la valeur technologique

Le FinOps évolue d'une simple optimisation des coûts cloud vers une gestion plus large de la valeur tech, notamment grâce à l'IA. Selon le rapport « State of FinOps 2026 », 98 % des entreprises gèrent leurs dépenses IA via FinOps, et 90 %, celles liées au SaaS. La spécification FOCUS standardise les données de facturation, essentielles pour les grandes entreprises. L'IA, en améliorant la prévision, la détection d'anomalies et l'automatisation des coûts, devient cruciale pour le FinOps. À l'avenir, la surveillance de l'adoption de FOCUS et l'intégration continue de l'IA dans les processus FinOps seront clés pour gérer la complexité croissante des coûts tech.

NIS 2, entre contrainte réglementaire et enjeux business

NIS 2 élargit considérablement le nombre d'entreprises concernées par les exigences en matière de sécurité informatique. Plus de 15 000 entreprises de plus de 50 salariés, ou réalisant plus de 10 millions de CA, dans 18 secteurs d'activité différents doivent désormais répondre aux nouvelles contraintes réglementaires. La directive impose notamment des obligations plus strictes dans la détection des cyberincidents, la gestion des vulnérabilités et la prévention des attaques.
Avec NIS 2 les questions de cybersécurité deviennent des enjeux business. D'abord sur le plan réputationnel : les entreprises conformes renforceront leur résilience et rassureront leurs clients sur leur capacité à assurer la continuité opérationnelle.
La cybersécurité constitue un avantage concurrentiel. À l'assurance de conserver leur part de marché actuel, s'ajoute la perspective de conquérir les clients d'entreprises moins-disantes en la matière.
C'est notamment un sujet primordial pour les sous-traitants. Toutes les entreprises doivent en effet s'assurer que chaque fournisseur ou prestataire est aligné sur leurs contraintes. Un grand nombre de PME sont donc concernées par l'extension du champ réglementaire. En faisant de la cybersécurité un outil stratégique, elles posent les jalons d'un futur prospère pour leur activité.

L'IA vue par les directions financières : de la curiosité à la productivité

Selon les dirigeants de la fonction finance, la technologie est le premier levier de transformation de leurs activités, relève la 14e édition de l'étude « Priorités des directions financières » menée par PwC France et Maghreb, en partenariat avec la DFCG (Association nationale des directeurs financiers et de contrôle de gestion). 72 % déclarent avoir engagé des projets d'adoption de l'IA dans leur entreprise et l'IA agentique est désormais perçue comme étant concrète et déployable. Leurs objectifs : gagner en efficacité pour les collaborateurs (82 %), en réactivité dans la prise de décision (63 %) et améliorer la qualité des processus (60 %).

Les DSI le savent, l'adoption massive de l'IA par la finance — et par toute l'entreprise d'ailleurs — nécessite notamment une intégration fluide avec les systèmes existants (ERP, CRM, outils de reporting), et elle a des conséquences en termes de sécurité et de conformité, mais aussi de gestion des infrastructures et des performances. Autant de sujets qu'il est utile pour une DSI d'examiner dans le cadre des transformations d'une direction majeure pour mettre en lumière sa valeur ajoutée et sa capacité à contribuer à la création de la valeur.

DC STUDIO/ADOBE STOCK

EUDI Wallet : d'une économie de l'identité à celle de la preuve, défis et opportunités

Le règlement sur l'identité numérique européenne et la mise à disposition des citoyens et des entreprises, par les États, du portefeuille d'identité numérique européen (EUDI Wallet) vont provoquer des transformations majeures. Au lieu de partager des données personnelles, l'EUDI Wallet ne transmettra que des attestations vérifiées. Pour les DSI, cela implique une refonte des systèmes d'authentification et de gestion des données, avec un accent sur la sécurité et la conformité.

Pour les entreprises, c'est une opportunité marketing et UX. Elles pourront prendre appui sur cette nouvelle architecture pour proposer des services plus fiables et centrés sur l'utilisateur.

À la clef, une expérience simplifiée et sécurisée, renforçant la confiance des clients et réduisant les frictions liées à la collecte de données.

Si les défis sont nombreux, cela pourrait favoriser l'innovation et la création de nouveaux modèles d'affaires basés sur la confidentialité et le contrôle des données par l'utilisateur. La mise en œuvre devrait intervenir d'ici 2027.

DENPHUM/ADOBE STOCK

Comment durcir et sécuriser son infrastructure IT ?

Plutôt que d'empiler les protections nouvelles, les entreprises doivent réduire la surface d'attaque de leurs systèmes.

Dans un contexte où les entreprises intègrent toujours plus d'outils numériques face à une menace cyber en constante mutation, la sécurité des systèmes d'information est un défi majeur. Plutôt que d'accumuler des solutions de défense qui complexifient l'architecture, une approche stratégique s'impose : le « durcissement » ou « hardening. ». Cette démarche proactive vise à réduire drastiquement la surface d'attaque en sécurisant les fondations mêmes de l'infrastructure numérique. Elle s'articule en différentes étapes.

Faire le ménage dans le SI

La première procédure à appliquer est d'auditer le système d'information pour y supprimer les scories. « *La règle est simple : le système d'information d'une entreprise doit être représentatif de ses réels besoins* », résume Florent Grosso, directeur pôle cybersécurité du groupe OCI.

KHUNKORNSTUDIO/ADOBE STOCK

Limiter les accès réseaux

Les organisations doivent également gérer l'accès à leurs réseaux et appliquer le principe du moindre privilège qui limite le droit d'un utilisateur à ses stricts besoins opérationnels.

« Durcir » également les sauvegardes

« *Les entreprises pensent parfois que les sauvegardes les protègent, alors qu'en réalité elles sont devenues les cibles favorites des pirates* », prévient Jonathan Meraoubi, directeur cybersécurité de groupe OCI. Il est conseillé de mettre en place la double authentification (MFA) pour l'administration des sauvegardes et d'en diversifier le stockage sur des serveurs distincts afin de réduire les risques de perte totale.

Sécuriser les postes de travail

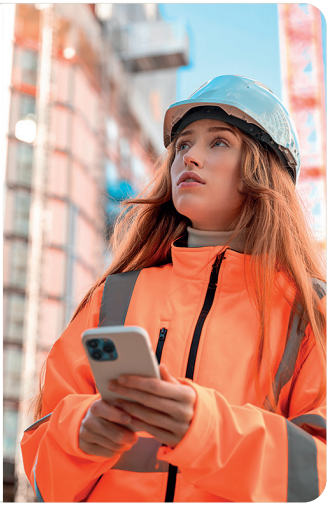
C'est un point essentiel. Par défaut, de nombreuses applications activent des fonctionnalités superflues, tandis que des fonctions de sécurité intégrées peuvent être involontairement désactivées. Une attention toute particulière doit être portée aux suites bureautiques, aux clients mails et aux navigateurs web. « *On doit autant que possible mettre en place des process de sécurité simples et fluides dont les utilisateurs perçoivent la plus-value et qui vont favoriser le réflexe et éviter le shadow IT* », explique Florent Grosso.

Effectuer des mises à jour et des audits réguliers

C'est un processus d'amélioration continue, indispensable pour contrer l'évolution constante des menaces. Des audits réguliers et une application systématique des mises à jour des systèmes sont cruciaux dans un contexte d'évolution permanente de la menace.

FMC, ça vous parle ?

La convergence fixe-mobile (FMC) modernise la téléphonie d'entreprise en fusionnant lignes fixes et mobiles sur une plateforme unique. Chaque employé bénéficie d'un numéro de téléphone unique, accessible sur tout appareil, ce qui garantit une meilleure traçabilité et une gestion informatique simplifiée. Cette solution offre également des gains de productivité et enrichit l'expérience client grâce à des transferts d'appels fluides et un accueil téléphonique constant, sans application spécifique ni dépendance à la data. Techniquement, un système centralisé achemine intelligemment les appels entrants et permet de choisir le numéro affiché pour les appels sortants. Ce regroupement des services chez un fournisseur unique assure une téléphonie continue et résiliente, même en cas d'incident, grâce au routage multi-opérateurs.



IRYNA/ADOBE STOCK

Open source

• **ZORIN OS** – Pour les acteurs du secteur de l'éducation, cette alternative à Windows tournant sous Linux, qui lui ressemble étrangement et ne perturbe donc pas les utilisateurs, offre de nombreuses applications y compris en suite bureautique et se déploie sur une infrastructure classique, en offrant une maîtrise des cycles de mise à jour.

• **HA Proxy, Apache ou NGINX** – Incontournable en matière de reverse proxie, l'open source offre de nombreuses solutions pour s'occuper de l'off-loading SSL et jouer du load balancing.

• **Proxmox** – L'une des alternatives à ESX de Broadcom ou à Azure Hyper-V de Microsoft, fort opportunément compatible avec le format de machines virtuelles ESX : un choix qui ne peut être ignoré quand on souhaite prendre son indépendance.

Vibe coding : un vrai levier de productivité ?

Simplicité, gain de temps, baisse du niveau de compétences requis… Les promesses du vibe coding — faire coder une IA à partir du langage naturel — sont alléchantes. Cependant, l'intégration de ces contributions générées par des LLM peut menacer la viabilité des projets. En effet, ces IA privilégient les résultats statistiquement probables, ignorant l'historique et les spécificités techniques ou opérationnelles. Les développeurs doivent donc exercer une vigilance accrue et une expertise fine pour corriger ces dérives, transformant les gains de productivité initiaux en une phase corrective chronophage et risquée pour la sécurité. Le vibe coding peut donc se révéler utile, notamment dans les phases de conception, mais il exige une forte attention à l'architecture des projets : gouvernance, définition des périmètres et respect de normes claires sont impératifs. Et attention comme le précise le fondateur de Cursor, une application prisée des vibe codeurs : « Si vous laissez les IA construire des choses sur des fondations instables et que vous ajoutez un étage puis un autre […], tout commence à s'effondrer .»

RÉPONSES D'EXPERTS

vos enjeux, vos défis, notre quotidien

GORODENKOFF/ADOBE STOCK

Cybersécurité

Quelles sont les principales erreurs commises même par les équipes aguerries ?

Même les équipes aguerries commettent des erreurs, souvent par excès de confiance. La plus grave ? Sous-estimer l'évolution permanente des menaces.

Une infrastructure sécurisée aujourd'hui peut être vulnérable demain, faute de veille ou d'adaptation.

L'erreur fréquente : négliger l'amélioration continue, en se reposant sur des protocoles figés. Pourtant, la cybersécurité exige une remise en question constante : formation, tests réguliers, analyse des incidents. Sans cette rigueur, le risque d'attaques ciblées ou de fuites de données persiste.

La vigilance ne se décrète pas, elle se cultive. Chaque faille corrigée en révèle d'autres. La cybersécurité n'est pas un état, mais un processus dynamique, où l'humilité et la réactivité font la différence.

Souveraineté

In fine, la souveraineté européenne se résume-t-elle à un lieu d'hébergement en UE opéré par une structure 100 % UE ?

Par-delà la question de l'applicabilité des lois extraterritoriales comme celles adoptées par les États-Unis, la souveraineté recouvre également la problématique de la dépendance stratégique et technologique. Ainsi, si les solutions opérées par la structure sont des solutions propriétaires extra-européennes, des risques de coupure d'accès à la technologie et de l'adhérence unilatérale au modèle commercial persisteront.

WAVEBREAKMEDIA/MICRO/ADOBE STOCK

Intelligence artificielle

Quelle est la différence entre l'IA générative et l'IA agentique ?

L'IA générative est un système réactif : elle produit un contenu (texte, image, code, résumé) à partir d'une instruction précise.
Basée sur des modèles comme les LLM, elle exécute une tâche ponctuelle puis s'arrête. Elle ne poursuit pas d'objectif dans le temps.
L'IA agentique, elle, agit. À partir d'un objectif formulé en langage naturel, l'agent enchaîne des actions concrètes : clics dans une interface, navigation sur un portail, saisie de formulaires, appels API, vérifications et validations. Par exemple, via un simple prompt, vous pouvez lui demander de commander des consommables sur votre portail client BtoB : en lui fournissant vos accès sécurisés, l'agent se connecte, sélectionne les références, valide le panier et finalise la commande de manière autonome.

TEROVESALAINEN/ADOBE STOCK

OCI INFORMATIQUE & DIGITAL

Relevons vos défis du quotidien grâce au digital !

- Sublimez votre informatique
- Propulsez vos équipes
- Enchantez vos clients

www.oci.fr

09 69 39 40 60