



*Faisons équipe*

# ACTUALITÉ 6 DUOTECH 2025

*Simplifiez la gestion de la paie avec Silae Paie.*

*La solution idéale pour les entreprises à la recherche de performance et d'efficacité.*

*Profitez dès maintenant d'un **tarif compétitif** à partir de 4,50 € par bulletin de paie, un prix imbattable pour un service de qualité. Grâce à une interface intuitive et des fonctionnalités complètes, Silae Paie vous permet de **gérer facilement la paie** de vos salariés tout en garantissant la conformité légale.*

À partir de  
**4.50€\***  
le bulletin  
de paie



*Fini les erreurs et les pertes de temps, avec Silae Paie, vous optimisez votre gestion de la paie tout en **réduisant vos coûts**. Découvrez dès aujourd'hui pourquoi de plus en plus d'entreprises choisissent Silae Paie et bénéficiez d'un tarif flexible et **adapté à vos besoins** !*

\* Prix indicatif basé sur un nombre de salariés standard. Le tarif réel peut varier en fonction de la taille de votre entreprise, des options choisies et des spécificités de votre dossier. Les prix sont hors taxes et sous réserve de conditions particulières.



*Pour plus d'informations, contactez-nous [contact@duotech.fr](mailto:contact@duotech.fr)*

# Victime de cybermalveillance ?



**DUOTECH vous guide pour agir.**

Pour se **protéger efficacement des attaques** cyber au quotidien, votre entreprise doit adopter une approche globale de la cybersécurité.

Voici les points clés préconisés à mettre en place pour renforcer la sécurité de vos systèmes :

**1. Formation continue des employés :** Sensibiliser les collaborateurs aux risques de cybersécurité, notamment le phishing, les ransomwares et les pratiques de sécurité essentielles (mots de passe robustes, méfiance envers les courriels suspects, etc.). Découvrez nos **SÉMINAIRES FORMATION DUOTECH\***.

**2. Mise en place d'une politique de mots de passe :** Utiliser des mots de passe complexes et les changer régulièrement. Envisager l'authentification multi-facteurs **KEEPER\*** pour un niveau de sécurité renforcé.

**3. Antivirus et anti-malware :** Installer des solutions antivirus EDR / XDR et anti-malware **BITDEFENDER\*** performantes et les mettre à jour régulièrement pour détecter et éliminer les menaces potentielles.

**4. Filtrage des courriels (Anti-spam) :** Mettre en place des filtres anti-spam **VADE SECURE\*** pour prévenir l'arrivée de courriels malveillants. Assurez-vous que les liens et les pièces jointes soient vérifiés avant toute ouverture.

**5. Pare-feu et sécurité réseau :** Configurer un pare-feu solide **WATCHGUARD\*** pour surveiller et contrôler les flux entrants et sortants. Utiliser un VPN pour sécuriser les connexions à distance, notamment pour les employés en télétravail.

**6. Sauvegardes régulières :** Effectuer des sauvegardes fréquentes et automatisées des données sensibles via **BEEMO TECHNOLOGIE\***. Conservez-les à la fois sur site et dans le cloud, pour garantir leur restauration en cas de perte ou de ransomware.

**7. Mises à jour régulières des systèmes et logiciels :** Assurer la mise à jour régulière via **LA SUPERVISION DUOTECH\*** des systèmes d'exploitation, logiciels, et applications afin de corriger les failles de sécurité connues. Installez les patches de sécurité dès qu'ils sont disponibles.

**8. Contrôles d'accès et gestion des privilèges :** Limiter les accès aux données et systèmes sensibles en fonction des rôles et responsabilités des employés. Appliquer le principe du moindre privilège (les utilisateurs ne doivent avoir accès qu'aux informations nécessaires à leur travail).

**9. Gestion des vulnérabilités :** Identifier, évaluer et corriger régulièrement les vulnérabilités de votre infrastructure. Utilisez des outils d'analyse des vulnérabilités pour détecter les failles potentielles avant qu'elles ne soient exploitées.

**10. Plan de réponse aux incidents :** Élaborer un plan d'intervention en cas d'incident de cybersécurité, incluant des procédures pour détecter, répondre et récupérer après une attaque. Assurez-vous que tout le personnel soit formé pour savoir comment réagir.

**11. Sécurisation des connexions à distance :** Mettre en place des protocoles sécurisés pour les connexions à distance (ex. : VPN, chiffrement SSL/TLS) afin de garantir que les employés puissent accéder en toute sécurité aux ressources de l'entreprise depuis l'extérieur.

En adoptant ces pratiques avec les conseils de **DUOTECH**, et en maintenant une vigilance constante, votre entreprise pourra réduire significativement son exposition aux cybermenaces et renforcer sa posture de sécurité. La cybersécurité étant un processus continu, il est essentiel d'effectuer des audits réguliers et de réévaluer les stratégies de sécurité face aux nouvelles menaces.

**Et c'est pour cela que nous vous accompagnons au quotidien sur toutes ces questions.**

\* solutions partenaires préconisées par DUOTECH.



# La BI DUOTECH (Business Intelligence) à partir de 30 € / mois !

Boostez la performance de votre entreprise avec la **BUSINESS INTELLIGENCE DUOTECH (BI)**, à partir de seulement 30 € HT par mois. Offrez à vos équipes un accès en temps réel à des indicateurs clés, permettant un suivi précis et une prise de décision éclairée.

Grâce à la **BI DUOTECH**, vous pouvez piloter vos finances en toute simplicité, en identifiant rapidement les opportunités d'amélioration et en anticipant les risques. Suivez l'évolution de vos revenus, vos dépenses, vos marges et bien plus encore, pour prendre des décisions stratégiques basées sur des données fiables et actualisées.

**Demandez votre essai gratuit 30 jours !**



À partir de  
**30€/mois\***

## Les Événements à venir chez DUOTECH

Ateliers , matinales , ...

Rendez-vous sur :

<https://festivalduotech.com/>  
pour en savoir plus !



\* Prix d'une BI DUOTECH Standard.