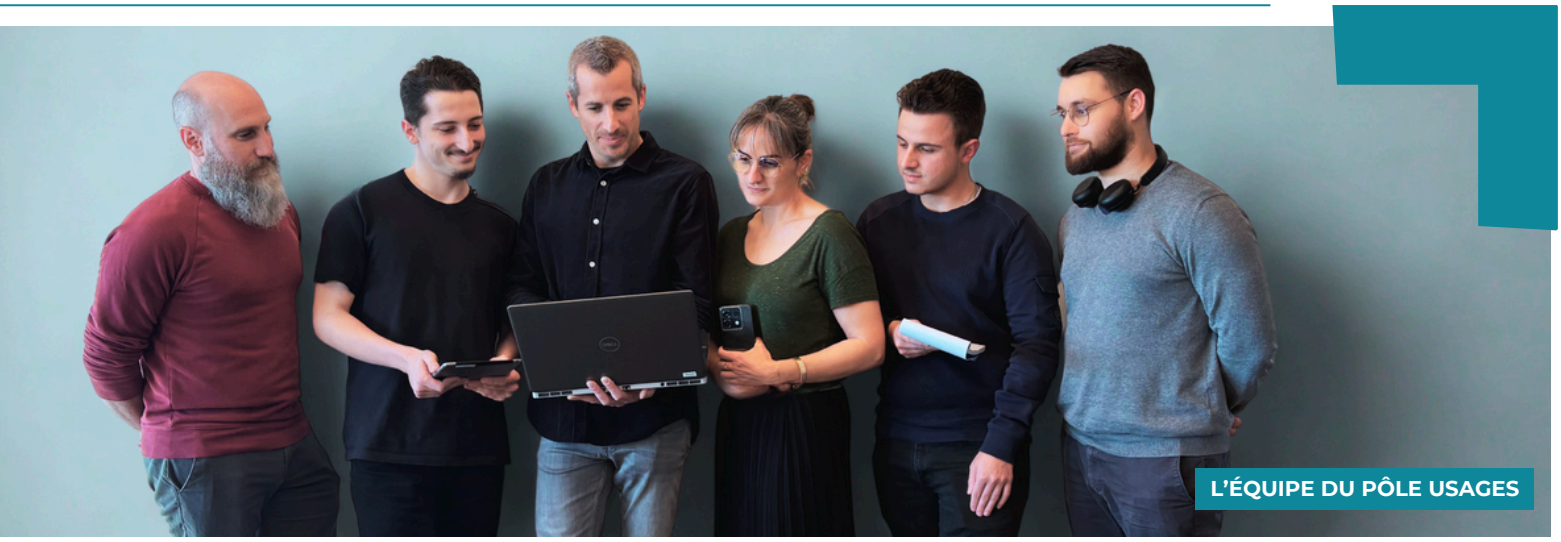
Le pôle usages Gers Numérique

L'expertise informatique au service des collectivités locales



L'ÉQUIPE DU PÔLE USAGES

Vos interlocuteurs privilégiés vous accompagnent au quotidien dans votre transformation numérique.

Le bouquet de services, une offre informatique globale adaptée aux collectivités.

Notre équipe d'experts optimise les coûts de fonctionnement de votre collectivité et intervient dans différents domaines numériques :

- Hotline dédiée aux mairies,
- Sécurité des environnements informatiques,
- Mutualisation des services,
- Gestion de l'obsolescence matériel/logiciel,
- Optimisation budgétaire des abonnements télécoms et des coûts de fonctionnement...

Gagnez en efficacité, maîtrisez votre budget et bénéficiez d'un suivi personnalisé et de proximité.

Financées par le Conseil départemental du Gers et votre communauté de communes, nos prestations ne vous seront pas facturées.

Le bouquet de services c'est aussi :

L'application INTRAMUROS
Gers Numérique offre aux collectivités un accès à ce nouveau moyen de communication avec les citoyens.

Les conseillers Gers Numérique :
Organisez gratuitement des permanences numériques dans votre commune pour permettre à vos administrés d'être plus à l'aise avec le numérique.

L'adressage communal :
Gers Numérique accompagne de nombreuses communes gersoises dans leur démarche d'adressage.

Votre Hotline dédiée
05 67 24 00 96

usages@gersnumerique.fr

www.gersnumerique.fr

47 Avenue Sambre et Meuse 32000 AUCH

Mes cyber réflexes

LES MOTS DE PASSE

Les mots de passe constituent la première ligne de défense contre les cyberattaques.
Il est donc essentiel de ***définir un mot de passe fort et unique*** pour votre session et pour tous vos logiciels. Pour éviter tout accès non autorisé,
Ne partagez pas et ne diffusez **pas votre mot de passe !**

UpSignOn

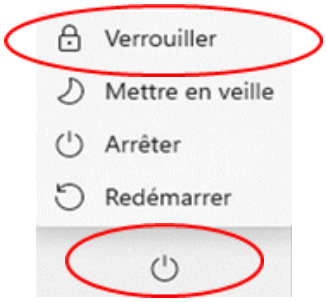
LE COFFRE-FORT DE MOTS DE PASSE

Notre bouquet de services vous propose la mise en place d'un coffre-fort numérique appelé «UpSignON», une solution 100% française et hébergée en France qui apporte une gestion sécurisée de vos mots de passe.
Cette application renforce la sécurité de vos appareils en générant elle-même des mots de passe forts et uniques.

Nous sommes à votre disposition pour configurer votre application si vous souhaitez en bénéficier et nous vous accompagnerons pour appréhender cet outil numérique.

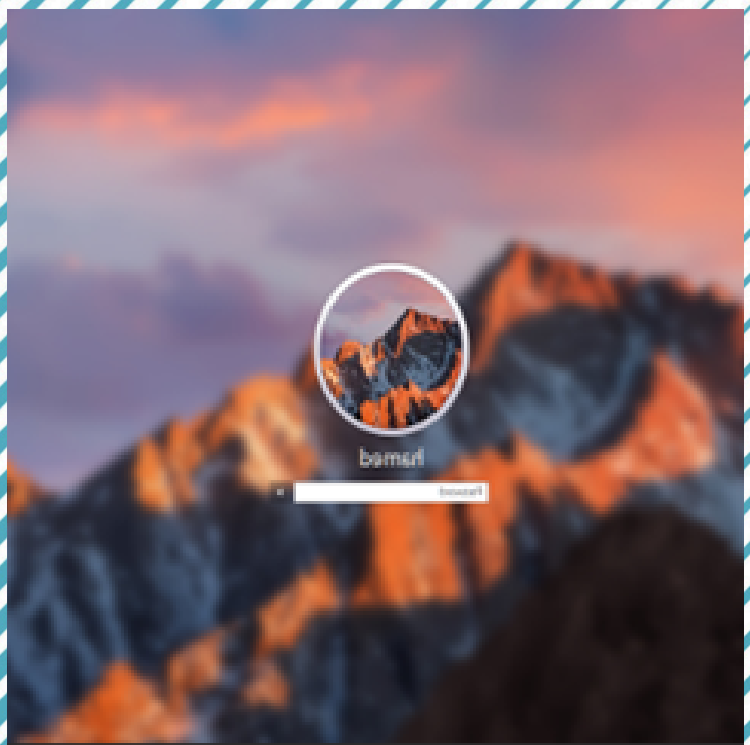
LE VERROUILLAGE DE SESSION

Lorsque vous vous absentez quelques minutes, prenez l'habitude de verrouiller votre poste de travail.
Verrouiller vos données et les crypter vous protège un maximum de collectes pirates.
Pour verrouiller votre session, plusieurs possibilités s'offrent à vous :



La plus rapide est d'appuyer simultanément sur la touche « Windows+L »

Ou cliquez sur le menu "Démarrer"



LES MISES À JOUR

L'importance des mises à jour

Les mises à jour de logiciels et systèmes d'exploitation (OS) sont essentielles pour ***corriger les vulnérabilités de sécurité et protéger les systèmes des menaces***.
C'est pourquoi il est important de bien réaliser les mises à jour régulièrement afin de garantir un système plus performant et sécurisé.

Le pôle usages collabore avec le CDG32 pour s'assurer que les mises à jour soient compatibles avec les logiciels métiers.
La fin du support de windows 10 est prévu pour octobre 2025 ; de ce fait le passage à windows 11 est obligatoire.

LA SAUVEGARDE DES DONNÉES

Les sauvegardes régulières des données **vous *protègent contre la perte d'informations*** cruciales en cas de défaillance du matériel ou de cyberattaque.

C'est pourquoi nous vous proposons, en plus de vos sauvegardes actuelles locales, d'***externaliser la sauvegarde automatique de votre environnement de travail dans le DataCenter à Auch, que nous exploitons en direct***.

Le **RGPD**, obligatoire depuis le 25 mai 2018, permet de mieux encadrer le traitement des données persnnelles. Nous ne proposons pas cette prestation dans le bouquet de services mais vous pouvez vous rapprocher de prestataires expérimentés dans le domaine comme le CDG32 par exemple. Informations : dpd-asm@cdg32.fr

Le pack cybersécurité inclus dans le bouquet de services Gers Numérique

ANTIVIRUS ET LOGICIELS ANTI-MALWARE

Les logiciels antivirus et anti-malware sont essentiels pour ***détecter et éliminer les menaces*** sur les systèmes informatiques. A minima, nous vous recommandons d'activer l'antivirus de Microsoft « Windows defender » intégré à votre ordinateur.

FIREWALLS (PARE-FEU)

Les firewalls sont utilisés pour ***surveiller et contrôler le trafic réseau, protégeant ainsi les systèmes des intrusions*** non autorisées. Il est primordial de vérifier que ces derniers sont activés.

OUTILS DE SURVEILLANCE

Les outils de surveillance permettent de ***détecter les activités suspectes et de garantir la sécurité des systèmes informatiques en temps réel***.
Nous travaillons en collaboration avec CT-Square expert français en cybersécurité, qui supervise tous les postes de travail référencés dans notre base de données afin d'analyser en permanence les flux. En cas d'activité suspecte, nous sommes prévenus sans délais.

CT-Square associé à notre solution antivirus Harfanglab nous permettent de protéger les postes de travail et les serveurs contre les cybermenaces.

LIENS UTILES
www.cyber.gouv.fr/bonnes-pratiques-protegez-vous
www.cybermalveillance.gouv.fr/17cyber
www.cnil.fr

Que faire en cas de cyber attaque?

Contactez :
- **le Pôle Usages Gers Numérique**
- **le délégué à la protection des données**
- **la trésorerie ou la paierie départementale**

Déposez plainte à la gendarmerie

Comment remonter un incident ?
Afin d'apporter une réponse adaptée et efficace, les divers intervenants ont besoin de renseignements précis pour effectuer un diagnostic initial.

Répondez de la manière la plus complète possible aux questions suivantes :
Quoi ? Décrire tous les évènements suspects constatés.
Quand ? Horodater le plus précisément possible les différents constats.
Qui ? Détailler les utilisateurs, boîte mail et comptes impliqués.
Où ? Détailler les machines, services, sites web et ressources impliquées.
Comment ? Détailler les actions qui ont menées à effectuer le ou les constat(s) d'incident(s)
Ex: MAJ serveur, réception d'un email, ouverture de PJ d'un mail, renseignement d'un formulaire, clic sur un lien, etc.