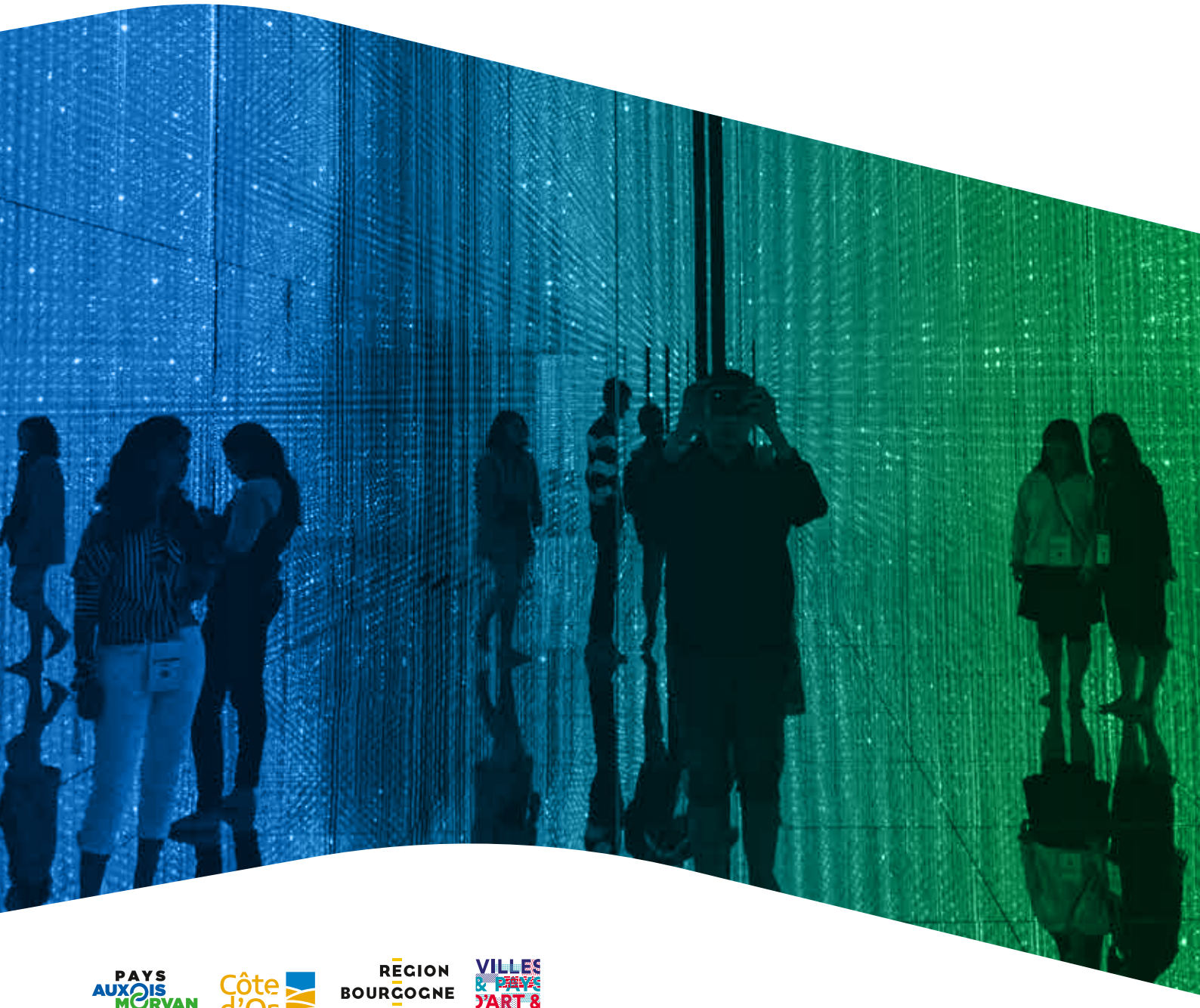
# Portrait NUMÉRIQUE
# DE L'AUXOIS MORVAN



PAYS AUXOIS MORVAN infiniment Bourgogne

Côte d'Or LE DÉPARTEMENT

RÉGION BOURGOGNE FRANCHE COMTE

VILLES & PAYS D'ART & D'HISTOIRE

# PORTRAIT NUMÉRIQUE
de l'Auxois Morvan

## ÉDITO

Face à la multiplication des attaques cyber impactant les collectivités territoriales et afin que chacun puisse appréhender les bonnes pratiques à adopter, j'ai souhaité vous proposer ce « *Portrait numérique de l'Auxois Morvan* ».

L'objectif de cette démarche est de dresser un état des lieux de la maturité numérique des collectivités de Haute Côte-d'Or. Ce « Portrait » résulte d'un travail de collecte d'informations effectué auprès des EPCI et communes du territoire. L'enquête présentée dans les dernières pages de ce fascicule est le fruit d'une collaboration avec les Services de Gestion Comptables de Venarey-Les Laumes et de Pouilly-en-Auxois.

En plus de l'aperçu de l'environnement numérique des collectivités de l'Auxois Morvan, ce livret détaille les parades et préconisations face aux éventuelles attaques cyber. L'Agence Nationale pour la Sécurité des Systèmes d'Informations (ANSSI), le site CyberMalveillance.gouv.fr, la Commission Nationale Informatique et Libertés (CNIL) émettent régulièrement des recommandations techniques vulgarisées dans ce document. Vous trouverez également des solutions proposées par l'Agence Régionale du Numérique et de l'intelligence artificielle (ARNia) et le Centre régional de cybersécurité de Bourgogne-Franche-Comté (CSIRT-BFC) dans ces pages : qu'il s'agisse d'outils ou des services, les tarifs négociés auprès des éditeurs de solutions numériques permettent au GIP ARNia et au Centre régional de cybersécurité d'offrir aux collectivités des solutions de sécurisation, d'appui et de remédiation pour pallier tout incident cyber.

Alexandre GARDAVOT, Chargé de mission Développement des Usages du Numérique du Pays Auxois Morvan, se tient à votre disposition pour vous appuyer et vous accompagner sur la compréhension et la mise en œuvre de ces recommandations : n'hésitez pas à le solliciter au 06 38 38 13 26 ou alexandre.gardavot@auxoismorvan.fr.

Patrick MOLINOZ
Président du PETR Pays Auxois Morvan
Vice-Président du Conseil Régional de
Bourgogne Franche-Comté

## Sommaire

## La Mission numérique

### Accompagnement numérique en Auxois Morvan

La Mission numérique du PETR se tient à disposition des EPCI et des communes pour les accompagner, les conseiller ou les appuyer dans leurs projets numériques. L'aide de la Mission porte sur des préconisations et des recommandations d'**équipements** informatiques et multimédias, sur des **logiciels** mais également sur les **usages** liés au numérique.

Toute structure, commune, établissement public, syndicat, association qui souhaite être accompagnée peut solliciter l'appui de la Mission numérique du Pays Auxois Morvan :

courriel : **alexandre.gardavot@auxoismorvan.fr**

téléphone : **06 38 38 13 26**

Pour dresser ce premier « *Portrait numérique de l'Auxois Morvan* » et afin d'avoir une photographie significative en termes d'équipements, les six Communautés de communes du territoire et les six anciens chefs-lieux de canton ont été expertisés. Par ailleurs, la Mission numérique a réalisé une trentaine d'audits auprès des collectivités du territoire et 123 communes ont répondu à l'enquête « Usages numériques », préparatoire à la rencontre cybersécurité du 13 décembre 2023.

## Collectivités sollicitées

### EPCI

- CC du Montbardois (CCM),
- CC Ouche et Montagne (CCOM),
- CC du Pays Arnay Liernais (CCPAL),
- CC du Pays d'Alésia et la Seine (COPAS),
- CC de Saulieu (CCS),
- CC des Terres d'Auxois (CCTA).

### Communes

- Arnay-le-Duc (CCPAL),
- Montbard (CCM),
- Saulieu (CCS),
- Semur-en-Auxois (CCTA),
- Sombernon (CCOM),
- Venarey-Les Laumes (COPAS).

## Illustrations

Couverture : note thanun sur Unsplash - Page 2 : Conseil Régional de Bourgogne Franche-Comté - Pages 4 et 8 : Daniel Agrelo de Pixabay - Pages 6 et 10 : Lucent_Designs_dinoson20 de Pixabay - Page 3 : StartupStockPhotos de Pixabay, Rodrigo Pignatta de Pixabay, Jan Vašek de Pixabay - Page 4 : StartupStockPhotos de Pixabay - Page 11 : VIN JD de Pixabay

# PORTRAIT NUMÉRIQUE
de l'Auxois Morvan

## Nombre de postes

Le nombre de postes informatiques n'est pas corrélé à la taille de la CC, au nombre de communes ou d'habitants. Ce sont les compétences prises en charge par la collectivité et son degré de maturité numérique qui font varier cette somme.

## Mobilité

Le poste de travail fixe reste la norme dans la moitié des cas : à l'exception des services excentrés ou pour les besoins des responsables de services, l'ordinateur portable n'est pas l'équipement le plus représenté. Post-Covid, il sera intéressant de suivre, sur les années à venir, les taux de répartition fixe-mobile, afin de déterminer si une évolution apparaît, et dans quel sens.

**Disposer d'un parc d'ordinateurs portables ajoute une souplesse dans les usages quotidiens du numérique**

## Connexion Internet

La fibre n'équipe pas encore toutes les structures. 2 sièges sur 6 EPCI sont reliés à la fibre. Dans le meilleur des cas, le reste des services est connecté en VDSL2, voire en ADSL. Certains sites excentrés exploitent une connexion 4G faute de raccordement. Dans les locaux, la plupart des structures partagent un réseau filaire et un réseau Wi-Fi. Pour la majorité, l'entité proposant un accès Wi-Fi l'a couplé à un système de gestion d'accès et de sécurisation. Le Wi-Fi n'est pas ouvert au visiteur sans contrôle d'accès.

**Arnay-le-Duc** :
... ... ... ... plus de 80%
**Saulieu** :
... ... ... ... plus de 80%
**Montbard** :
... ... ... ... plus de 80%
**Semur-en-Auxois** :
... ... ... ... plus de 80%
**Sombernon** :
... ... ... ... plus de 80%
**Venarey-Les Laumes** :
... ... ... ... plus de 80%

Taux de déploiement fibre
au 1è trimestre 2024 selon l'ARCEP
*https://cartefibre.arcep.fr/*

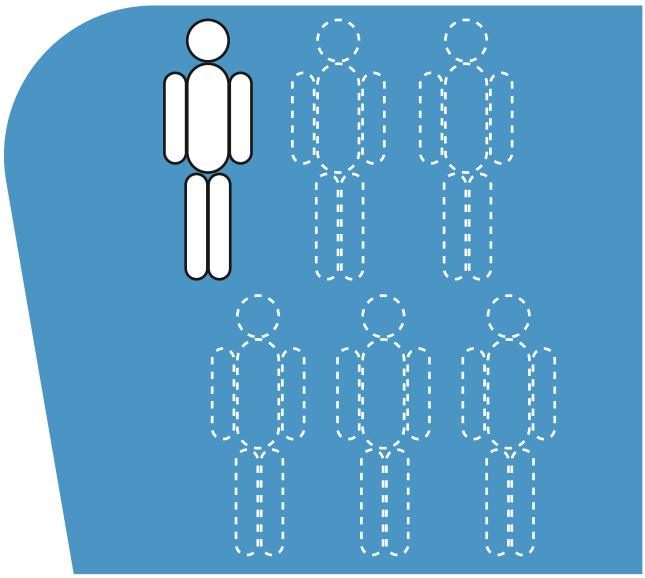
# PORTRAIT NUMÉRIQUE
## de l'Auxois Morvan

### Téléphonie fixe et mobile

L'équipement en téléphonie fixe et mobile est assez homogène : les agents en situation de mobilité ou les responsables de services possèdent en complément des lignes mobiles.

Une information sur la sécurité en mobilité, portant tant sur les ordinateurs que les smartphones est proposée aux structures en faisant la demande.

**Il est recommandé d'équiper son smartphone d'un antivirus ou d'une solution de sécurité : la plupart des éditeurs proposent maintenant une offre antivirus ordinateur + antivirus téléphone**



Sur 6 EPCI de l'Auxois Morvan, seule la COPAS mutualise un Responsable informatique avec le bourg-centre.

### Politique d'achat

Dans la majorité des cas, l'équipement est acheté neuf. À noter : la CCTA, pour le rééquipement de ses Espaces Publics Numériques a procédé à un achat de plusieurs postes d'occasion.

**Le Guichet Vert propose un accompagnement pour faciliter l'ajout des critères de réemploi dans la commande publique**

### Gestion des parcs

Pour la moitié des établissements, c'est un prestataire extérieur qui se charge de l'informatique. Ensuite, les agents faisant office de... Enfin, une seule CC a un agent dédié à la gestion, maintenance de son parc informatique. À noter : cet agent est mutualisé avec le bourg-centre.

Selon Statscounter, fin 2022, la version 10 de Windows équipait environ 69% des postes, suivi de la version 11 avec environ 16 %.
Malgré l'arrêt de la prise en charge par Microsoft, ce sont encore 10 % des postes qui sont équipés de Windows 7.
**Le support de Windows 7 ayant pris fin le 14 janvier 2020, il convient de remplacer toute version 7 par une plus récente.**

# PORTRAIT NUMÉRIQUE
de l'Auxois Morvan

## Actualisation des Systèmes d'Exploitation

Les dernières versions de Windows constituent en quasi intégralité le système d'exploitation du parc informatique des agents publics en Auxois Morvan. La majorité de ordinateurs fonctionnent avec des versions récentes de Windows (11 ou 10).

Quelques postes Mac ou Linux existent à la marge.

## Suites bureautiques

Microsoft Office a la part belle des suites bureautiques disponibles pour les agents de l'Auxois Morvan. Avec des installations s'étalant des versions 2010 aux dernières versions Microsoft 365, les versions des suites bureautiques sont disparates. Les EPCI bénéficient de versions récentes, là où les communes conservent d'anciennes versions. À l'instar d'anciennes installations de Windows, la conservation de vieilles éditions d'Office pose un problème de sécurisation des postes de travail, du fait des failles de sécurité et des vulnérabilités connues.

## Solutions de sécurité

Si les Systèmes d'Exploitation présentent un ensemble homogène, les suites de sécurité sont quant à elles plus disparates.

Cohabitent les suites de marque ESET en installation média, des antivirus Bitdefender gérés par un prestataire (dit « managé »), ou une simple installation de la suite de sécurité Windows Defender, proposée par Microsoft avec son système d'exploitation.

On parle ici d'antivirus, le pare-feu étant couplé avec le VPN fourni par le prestataire de logiciel métiers. Certaines CC se contentent du pare-feu de la box internet pour toute solution de filtrage. Les solutions de type Détection et réponse des terminaux (en anglais EDR Endpoint Detection et Response) n'apparaissent pas dans les réponses. Ces solutions exploitent la surveillance en temps réel, le partage de connaissance via le Cloud (nuage) et l'Intelligence Artificielle pour déterminer si un comportement est suspect.

**L'achat en volume permet de simplifier la commande de licences logicielles : un groupement de commande à l'échelle de l'intercommunalité ou par une centrale d'achat comme celle de l'ARNia permet de conserver des logiciels à jour, pour un coût réduit**

CSIRT
BOURGOGNE-FRANCHE-COMTÉ

**Le CSIRT (Centre de Réponse à Incident Cyber) propose à ses adhérents des solutions de nouvelle génération pour sécuriser les postes de travail.**

**Contact : 0970 609 909**

# PORTRAIT NUMÉRIQUE
de l'Auxois Morvan

## VPN

L'utilisation du VPN est favorisée par les offres SAAS des grands éditeurs. Son installation est rarement la volonté de la collectivité elle-même. Ces contraintes de connexion sont propres à chaque prestataire : par exemple, JVS propose ses outils accessibles via le navigateur web, là où Cosoluce exploite une connexion RDP pour joindre le serveur distant.

## Politique de sauvegarde des données

Chaque Communauté de communes de l'Auxois Morvan a mis en place une solution de sauvegarde. Ce sont principalement les prestataires qui assurent cette sauvegarde. Il s'agit ici de la sauvegarde des fichiers de travail en général et pas seulement des fichiers liés aux applications métiers (Berger-Levrault, Cosoluce...).

Une exception toutefois : une CC assurant sa sauvegarde dans le nuage (Cloud). Avec cette solution le risque de perte de documents persiste, par erreur interne ou malveillance.

## Lieu de stockage des données

Avec les offres SAAS et Cloud des éditeurs nationaux, la majorité des structures hébergent leurs données métiers chez un prestataire.

Les autres données sont stockées sur site, sur un serveur de données. Ce serveur peut être répliqué ou sauvegardé.

## Quelques définitions

**VPN :** Virtual Private Network, réseau privé virtuel, solution technique permettant d'établir une connexion sécurisée entre deux points.

**SAAS :** Software As A Service, logiciel en tant que service, accès à un logiciel à distance, sur abonnement.

**RDP :** Remote Desktop Protocol est une solution de connexion à un poste distant proposée par Microsoft.

**Cloud :** littéralement « nuage », désigne le stockage et l'accès distant aux données ou aux services.

**BYOD** : Bring Your Own Device, littéralement « amène ton propre matériel » désigne la tendance à exploiter des solutions (matérielles ou logicielles) appartenant à l'agent pour effectuer ses missions.
Par exemple, un téléphone portable personnel servant à recevoir ou passer des appels professionnels.

Ce type de solution pose la question de la sécurisation des données et de leur éventuelle fuite.

| | ComCom | Collectivités |
|---|---|---|
| Sauvegarde éditeurs | ●●● | ●●○ |
| Sauvegarde locale | ●○○ | ●●● |
| Sauvegarde distante | ●●● | ●○○ |
| Accès distant | ○○○ | ●○○ |
| Accès Cloud | ●●○ | ●○○ |

Légende *Tableau de stockage des données*

Usage courant ●●●
Usage modéré ●●○
Usage rare ●○○

# PORTRAIT NUMÉRIQUE
de l'Auxois Morvan

## Rétention de données

La rétention des données correspond à la période jusqu'à laquelle il est possible de récupérer des informations : 1 semaine en arrière, 3 mois etc.

Si les EPCI partagent une bonne hygiène de sauvegarde, la notion de rétention de données reste floue : certains, pour raison d'espace de stockage, ont une rétention de 15 ou 30 jours. Mais malheureusement, la majorité ne sait pas jusqu'à quelle date ils peuvent récupérer leurs données.

On peut déduire qu'aucun EPCI n'a été confronté à la problématique de récupérer ses données. Cela laisse supposer également que des tests réguliers de viabilité des sauvegardes ne sont pas effectués.

## Charte ou règlement informatique

Selon leur déclaration, la majorité des EPCI n'a pas de Règlement Intérieur, un seul établissement travaille actuellement à sa rédaction. Selon les articles 2121-8 et L5211-1 du Code Général des Collectivités Territoriales (CGCT) c'est un élément obligatoire pour les EPCI, qui autorise ensuite la mise en place d'un Règlement ou d'une Charte Informatique.

**La Mission numérique du Pays Auxois Morvan propose de mettre en place un groupe de travail rassemblant toutes les entités intéressées afin d'établir un Règlement ou une Charte informatique commune, que chacun pourra ensuite adapter à ses besoins.**

## 3·2·1

Rapportée à la politique de sauvegarde, la règle 3, 2, 1 est une astuce mnémotechnique visant à mémoriser facilement les principes suivants :

- **3 copies** du fichier à protéger, la version primaire + deux versions supplémentaires
- ces versions supplémentaires sont stockées sur **2 supports différents** permettant de retrouver la donnée si l'un d´eux est illisible
- un des supports est stocké dans **1 site externe**, afin de parer aux risques de vol, incendies, dégâts des eaux, etc. sur le site principal.

**Le Président ou le Maire peuvent voir leur responsabilité engagée lors d'un incident cyber.**
**En effet, de nombreuses informations, nécessaires à l'exercice des missions de service public, transitent par les ordinateurs des Communautés de communes ou des Collectivités.**
**Il convient de prendre conscience de cet aspect de la numérisation des procédures.**

# PORTRAIT NUMÉRIQUE
de l'Auxois Morvan

## Désignation d'un Délégué à la Protection des Données (DPD)

Face à la contrainte de la désignation d'un Délégué à la Protection des Données (DPD), la majorité des Établissements ont choisi d'adopter la solution proposée par le Centre de Gestion de Côte-d'Or (CDG) : prendre la prestation externalisée proposée par ce dernier. L'autre moitié a soit botté en touche, soit peine à mettre en œuvre sa conformité.

Les Établissements ayant missionné le CDG n'ont pas de nouvelles de ce dernier : le RGPD nécessite pourtant un suivi régulier, qui concourt à la mise en œuvre d'une informatique sécurisée. En effet, en cas de compromission, c'est la responsabilité du Président de l´EPCI comme responsable de traitement et non du DPD qui est engagée.

Afin d'aider les communes dans leur mise en conformité, L'ARNia propose un outil « Super Chef RGPD » qui simplifie la procédure. L'Agence propose également l'accompagnement d'un agent pour :

- la rédaction du registre des traitements,
- la rédaction de procédures en cas de contrôle,
- l'élaboration d'analyses d'impacts,
- la conformité de contrat avec les sous-traitants,
- la conformité des sites web.

**Faites-vous accompagner par l'ARNia et ses recettes du « Super Chef RGPD » pour faciliter la mise en place de votre conformité :**

**Contact au 0 970 609 909**

Le Règlement Général sur la Protection des Données (RGPD) - au delà de son aspect contraignant - permet d'interroger la sécurisation des données détenues par les EPCI et collectivités.

Il vise à amener le responsable du traitement à une prise de conscience de l'importance de la donnée et de sa sécurisation.

**Quelques points clés du RGPD :**

- identifier les jeux de données à caractère personnel en possession de la structure,
- se limiter aux données nécessaires à la réalisation de la mission ayant mené à la collecte,
- en cas de compromission et selon le type de données collectées, administrés et CNIL devront être informés,
- lors de la collecte d'informations à caractère personnel, le consentement doit être explicite : la personne a le choix entre « accepter » et « refuser » la collecte.
- renforcement du droit des personnes : portabilité, oubli, recours juridictionnel contre le responsable du traitement.

# PORTRAIT NUMÉRIQUE
de l'Auxois Morvan

## Connaissance des risques cyber

L'information sur les risques cyber semble être correctement reçue par les répondants : seul l'un d'eux a indiqué n'être pas suffisamment informé. Responsables informatiques ou Directeurs Généraux assurent être au fait de l'actualité cyber. La mise en œuvre de mesures de sécurité efficaces reste liée au degré de maturité et au choix budgétaire des structures.

Les répondants s'accordent à privilégier les formats numériques et plus précisément la lettre d'information pour suivre l'actualité de la cybersécurité.

La Mission numérique préconise de s'abonner aux listes de diffusion de Cybermalveillance.gouv.fr, de la CNIL et de l'AMF pour avoir un panel d'informations compréhensibles et régulières sur les risques.

CYBER MALVEILLANCE .GOUV.FR

Assistance et prévention en sécurité numérique

Retrouvez les fiches et le contenu mis à disposition sur : Cybermalvaillance.gouv.fr

## Les sources auprès desquelles s'informer

Cybermalveillance.gouv.fr : consultez le site web et ses kits de sensibilisation,

CNIL.fr : retrouvez de nombreux conseils liés à la cybersécurité,

AMF.asso.fr : diffusez dans votre structure la « *Méthode clés en main pour sensibiliser les agents des collectivités* » et consultez le guide « *Cybersécurité : toutes les communes et intercommunalités sont concernées* »,

La Mission numérique du Pays Auxois Morvan peut vous aider à mettre en place des séances de prévention pour vos agents.

# PORTRAIT NUMÉRIQUE
## de l'Auxois Morvan

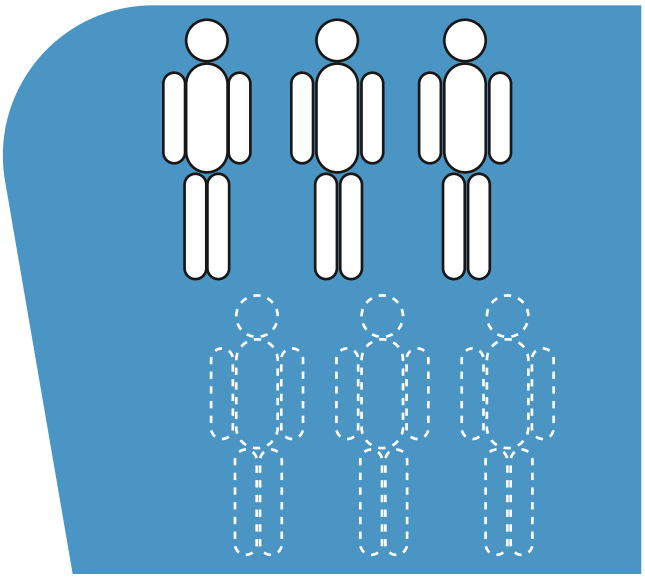
### COMMUNES : L'ÉQUIPEMENT

L'équipement informatique des communes peut être classé en deux ensembles :

- Le poste unique d'une petite commune (moins de 500 habitants), accessible par le Maire, la secrétaire de Mairie et l'équipe municipale ; le poste est partagé.

- Les postes multiples, pour les communes plus peuplées, où l'équipement est associé à un agent ou une fonction : le poste est individualisé.

À ce dernier cas de figure s'ajoutent les flottes d'ordinateurs des écoles, musées, CCAS selon les cas.



Montbard, Semur-en-Auxois et Venarey-Les Laumes ont un Responsable informatique.

### La Centrale d'achat

Les postes informatiques sont dans l'ensemble plutôt récents : les Systèmes d'Exploitation (SE) installés sont Windows 10 et 11.

En effet, les communes de moins de 1 000 habitants ont pu bénéficier du financement proposé, dans le cadre du plan France Relance, par la Région Bourgogne Franche-Comté pour le rééquipement de leur informatique.

En complément de ces financements, les communes peuvent également se rapprocher de l'ARNia pour formuler des demandes d'évolutions, qui seront prochainement déployées dans la Centrale d'achat du Groupement d'Intérêt Public (GIP).


La Centrale d'achat est ouverte aux adhérents du GIP. Retrouvez sa présentation à l'adresse :

https://centrale-achat.ternum-bfc.fr/

# PORTRAIT NUMÉRIQUE
de l'Auxois Morvan

## ENQUÊTE « USAGES NUMÉRIQUES DES COMMUNES EN AUXOIS MORVAN »

En préparation de la « *Rencontre cybersécurité en Auxois Morvan* » du 13 décembre 2023, le Pays Auxois Morvan et les Services de Gestion Comptable de Venarey-Les Laumes et de Pouilly-en-Auxois se sont associés pour diffuser une enquête conjointe portant sur les usages numériques des communes.

123 communes répondantes ont complété les 10 questions portant sur les usages liés à la sécurité et au numérique au quotidien.

Les résultats de l'enquête présentés dans les pages suivantes sont accompagnés des préconisations de la Mission numérique afin d'appuyer les collectivités de l'Auxois Morvan dans le renforcement de leur sécurité numérique.

### Questions 01. Avez-vous connaissance de ce qu'est un FOVI ? et 02. Connaissez-vous les procédures pour l'éviter ?

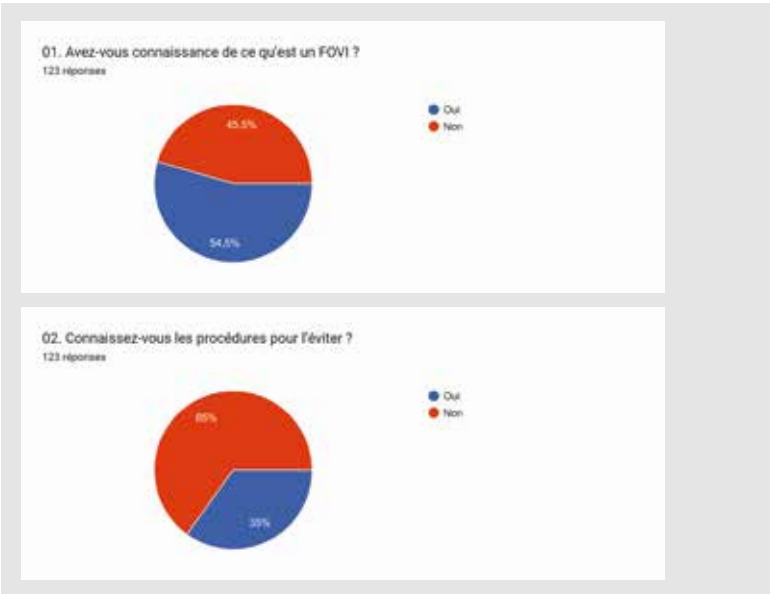
L'acronyme FOVI signifie Faux Ordre de Virement. C'est une arnaque qui consiste, pour le malfaiteur, à détourner la destination d'un paiement administratif vers un compte auquel il a accès. Pour arriver à ses fins, le malfaiteur peut pirater la messagerie d'une commune et détourner un courriel. Ce courriel demande de modifier les coordonnées bancaires d'un fournisseur ou d'un prestataire. Les nouvelles coordonnées bancaires sont celles du pirate.

**La parade** consiste à :

1) ignorer les demandes de modifications de coordonnées bancaires adressées par courriel ;

2) utiliser exclusivement CHORUS-Pro pour le circuit facturation-paiement ;

3) en cas de doute, téléphoner – via des coordonnées connues - à l'émetteur de la facture pour demander des précisions.

# PORTRAIT NUMÉRIQUE
## de l'Auxois Morvan

### Question 03. Les éléments suivants (nom de la commune, code postal, nom du maire, aucun des éléments ci-dessus) sont-ils présents dans le mot de passe de la messagerie de la commune ?

Les mots de passe de messagerie des communes de l'Auxois Morvan contiennent plus de 35 % le nom de la commune et à plus de 17 % le code postal de la collectivité.

Un mot de passe facilement déductible permet à l'attaquant d'accéder à la messagerie de la commune, lui assurant ainsi une large liberté d'action pour détourner des courriels, imiter des messages, obtenir des informations à caractère personnel ou des accès à d'autres services. En effet, l'accès à la plupart des services numériques s'appuie sur la messagerie électronique de la commune.

**La parade** : élaborez des mots de passe complexes (lettres majuscules et minuscules, chiffres, symboles… ) n'ayant aucun rapport avec votre activité. En complément, vous pouvez utiliser un coffre-fort numérique, qui va rassembler et créer vos mots de passe. L'ARNia propose un outil connecté simple d'utilisation nommé UpSignOn.




### Questions 04. Le maire ou un autre membre de l'équipe municipale accède-t-il à la messagerie de la commune sur son téléphone portable ? et 08. Travaillez-vous à distance, en télétravail ?

Hérité de l'acronyme BYOD (Bring Your Own Device), UYOD (Use Your Own Device) désigne l'utilisation d'un équipement personnel à des fins professionnelles. Le téléphone portable d'un maire rentre dans cette catégorie. Avec l'augmentation du télétravail, ce sont également les secrétaires de mairie qui rejoignent ces pratiques, avec comme nuance l'usage de l'ordinateur personnel à des fins professionnelles. C'est donc l'ordinateur du domicile qui sert à administrer les affaires de la commune. Cet usage reste marginal, mais il faut toutefois l'inclure parmi les mauvais usages à réduire pour renforcer la sécurité des communes. S'il n'est pas envisageable de proposer des interventions sur les postes personnels des agents, l'adoption de sessions utilisateurs restreintes en droits, la mise en place d'un antivirus sur le smartphone du maire et la diffusion de quelques précautions de bases semble la piste la plus simple et efficace à mettre en place.

**La parade** : créez et utilisez des sessions séparées. La session correspond au profil de l'utilisateur et aux droits dont il dispose sur l'ordinateur. Une session consacrée au secrétariat de la Mairie dans le cas du télétravail permet d'isoler les documents, informations de connexion et activités des autres utilisateurs de l'ordinateur.

Concernant les appareils personnels (téléphones portables ou ordinateurs), il convient d'être très prudent lorsqu'on installe une application ou un logiciel gratuit. Certains éditeurs malveillants exploitent la popularité des applications présentes dans les magasins d'applications, pour diffuser des outils vérolés. Ceux-ci prennent la main ou aspirent les informations présentes sur l'appareil de l'utilisateur. Parmi les types d'applications les plus souvent détournées, on trouve les applications d'ajout de filtres photos, les lecteurs PDF, des jeux, des applications pour personnaliser son smartphone (fonds d'écrans, icônes d'application, émojis etc.).

# PORTRAIT NUMÉRIQUE
## de l'Auxois Morvan

### 05. Pour vos logiciels métiers, effectuez-vous une sauvegarde locale ou distante ? et 06. Pour vos divers documents numériques (photos, plans, documents, copies de courrier...), effectuez-vous des sauvegardes (locales ou distantes) ?

Plus de 74 % des répondants sauvegardent les données métiers. C'est un bon réflexe, qui permet de retrouver rapidement ses données en cas de dysfonctionnement. Pour être efficace, cette sauvegarde doit être isolée des équipements informatiques habituels. En effet, si le support de sauvegarde reste dans les lieux, en cas de vol, d'incendie, de choc électrique, la commune s'expose à une perte complète des fichiers. Selon la nature de ceux-ci, cela peut être des documents uniques définitivement perdus (numérisation des parcelles du cimetière, archives de la commune...) ou des documents qu'il faut redemander aux administrés (30 % des répondants indiquent que les documents de travail sont enregistrés sur l'ordinateur de la commune, sans autre copie).

Plus de 58 % de répondants assurent disposer d'une copie des documents de travail sur clés USB ou sur un disque dur externe. C'est une première étape pour assurer une éventuelle récupération des documents en cas d'incidents sauf si :

• le disque dur ou la clé USB restent branchés sur l'ordinateur.

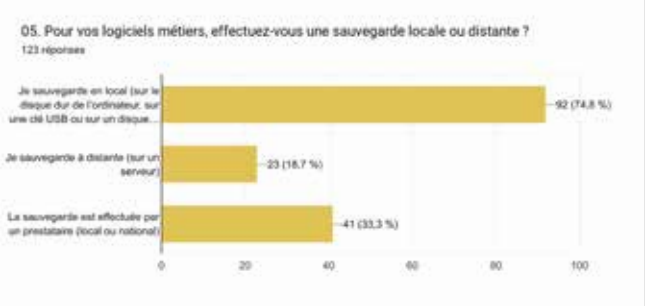
• le disque dur ou la clé USB sont stockés à proximité de l'ordinateur (tiroir du bureau...).

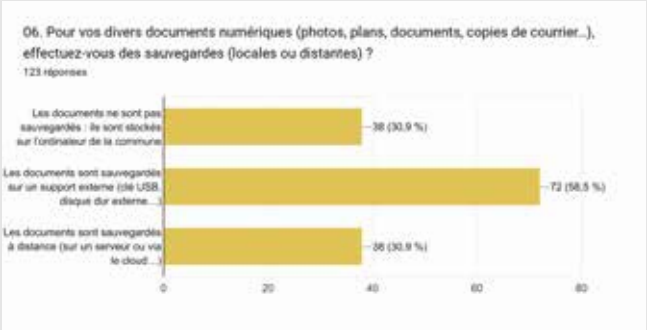
L'inconvénient de ce dispositif est qu'il implique la manipulation des supports de sauvegarde rendant difficile l'automatisation du procédé.

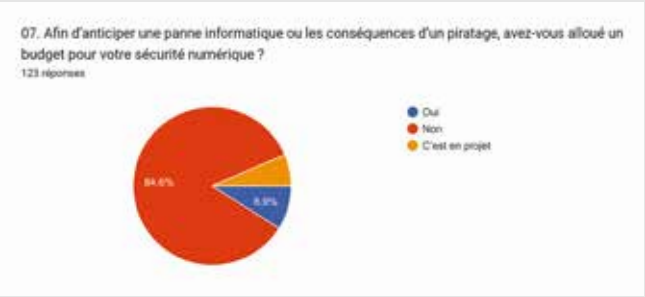
Enfin, c'est un peu plus de 30 % des répondants qui sauvegardent leurs documents sur un disque réseau ou via le cloud.

Ces solutions de sauvegardes présentent l'avantage de permettre l'automatisation de la copie et le stockage des données hors du bâtiment (dans le cas d'un disque réseau distant). Selon les systèmes et le mode de sauvegarde, l'enregistrement de différentes versions est également possible.

**La parade** : déployez des solutions de sauvegarde. À minima, optez pour une sauvegarde régulière sur un disque dur, stocké en dehors de la Mairie. Pour une automatisation des sauvegardes, consultez l'offre du CSIRT-BFC à l'adresse www.csirt-bfc.fr.




### Question 07. Afin d'anticiper une panne informatique ou les conséquences d'un piratage, avez-vous alloué un budget pour votre sécurité numérique ?

Plus de 84 % des répondants n'ont pas prévu de budget cybersécurité. Lors des réunions de sensibilisation, l'aspect financier de la cybersécurité n'est pas souvent évoqué. C'est pourtant un élément primordial : si les bonnes pratiques n'engagent pas systématiquement de frais, l'équipement et les services nécessaires (sauvegardes, antivirus, pare-feu) ont un coût. Ce coût est à relativiser, puisqu'il convient de dimensionner l'équipement et les services à hauteur de la structure à sécuriser.

Presque 9 % des répondants ont réservé une part budgétaire à la sécurité. 6,5 % des répondants vont allouer une part notable du budget communal au renforcement de la sécurité.

**La parade** : la Mission numérique peut vous aider à identifier les solutions et élaborer un budget consacré à la sécurité informatique. L'ARNia et le CSIRT proposent également des solutions clés en main à découvrir sur le site www.arnia-bfc.fr.

# PORTRAIT NUMÉRIQUE
## de l'Auxois Morvan

### Question 09. Pensez-vous que votre commune puisse être la cible d'une attaque cyber, d'un piratage ou d'un rançonnage ?

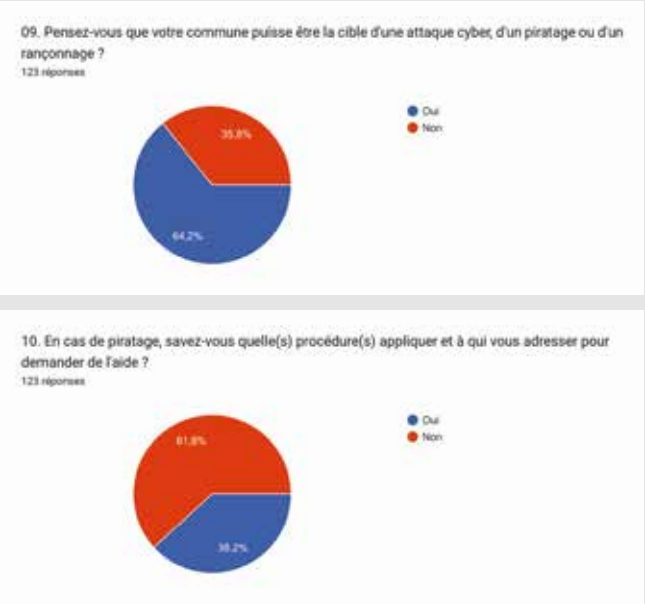
Plus de 64 % des répondants se considèrent comme cible potentielle. Ce taux est une bonne nouvelle. En effet, les petites structures considèrent souvent que leur taille leur permet de passer sous les radars. C'était peut-être le cas il y a quelques années. Actuellement, la menace cyber est une industrie avec des fournisseurs (de virus) et des prestataires exploitants. Ces prestataires louent des programmes informatiques malveillants en reversant une commission aux pirates qui proposent le programme à la location. Ces sous-traitants vont exploiter le programme malveillant sans cibler précisément une commune, une entreprise, un service public. Ceux qui ne sont pas suffisamment sécurisés se font avoir. Ce type d'attaque diffère de celles qui visent les grandes entités publiques : la revendication politique joue un rôle dans ce cas, même si l'extorsion monétaire n'est jamais loin.

**La parade** : renforcez vos mots de passe, installez les mises à jour dès leur publication, mettez en place une sauvegarde. En cas de doute, interrogez les différents interlocuteurs qui peuvent vous accompagner : la Mission numérique, votre fournisseur informatique, le CSIRT-BFC.

### Question 10. En cas de piratage, savez-vous quelle(s) procédure(s) appliquer et à qui vous adresser pour demander de l'aide ?

Plus de 61 % des communes ayant répondu ne savent pas quoi faire en cas d'attaque réussie. Dès l'attaque constatée, un compte-à-rebours se met en place : en effet, selon la portée de l'attaque, il sera nécessaire de contacter certains organismes dans des délais impartis. La liste au dos de ce livret détaille ces étapes.

**La parade** : en cas d'attaque, vous devrez avoir anticipé le blocage de votre système d'information. Il y a de grandes chances que vous ne disposiez plus de l'accès à vos contacts habituels, numéro direct de la gendarmerie, ligne directe de l'assureur, coordonnées du prestataire informatique... Préparez ici un « plan B » qui vous permettra de fonctionner a minima, sans vos outils habituels. Cela prend la forme de documents au format papier, de liste de contacts à jour imprimées. Ces listes rassemblent les personnes pouvant vous aider dans la gestion de la crise. Dans l'idéal, vous aurez identifié au préalable




l'emplacement de vos équipements, comment y accéder, quelle est la personne référente... Il s'agit d'établir une cartographie de votre environnement numérique.

Le plan de secours est désigné sous le terme de Plan de Continuité de l'Activité (PCA) ; il précède le Plan de Reprise de l'activité (PRA).

## POUR RÉSUMER...

**Les résultats de l'enquête permettent d'identifier deux notions, à retenir :**

**La première est qu'il reste une marge d'amélioration pour les communes de l'Auxois Morvan en ce qui concerne la sécurité numérique.**

**La seconde est que cette progression s'appuie sur la politique des « petits pas » : c'est la somme de petites actions, facilement applicables, qui crée la sécurité informatique. Seul, un logiciel ne suffit pas à sécuriser un environnement numérique.**

**La Mission numérique se tient à l'écoute des communes de l'Auxois Morvan qui souhaitent être accompagnées et découvrir ces bonnes pratiques de sécurité numérique.**

# Réflexes
# en cas d'attaque

Anticiper et connaître dès à présent les réflexes à adopter en cas d'attaque cyber vous permettra de faire face à cette épreuve. Préparez un document de référence au format papier, contenant les étapes à suivre et les partenaires à contacter en cas de compromission.

1. **Alertez votre responsable informatique ou votre prestataire** si vous en avez un ;
2. **N'éteignez pas l'ordinateur mais isolez-le du réseau**. Pour cela, coupez le Wi-Fi de l'appareil ou débrachez la prise réseau (RJ-45) de la carte réseau ;
3. **Alertez la Gendarmerie** ;
4. **Contactez le CSIRT au 0 970 609 909, choix 1** ;
5. **Alertez la trésorerie et votre banque** au cas où des transferts des fonds auraient été initiés ;
6. **Déposez plainte** ;
7. **Dans les 72 heures**, vous devrez :
   A. **déclarer le sinistre à votre assureur**,
   B. **notifier la CNIL** si des données à caractères personnels ont pu être consultées, modifiées ou détruites.
8. **Informez** vos administrés, fournisseurs, partenaires de l'attaque subie et de ses conséquences.

## CONSTITUEZ LE DOCUMENT DE RÉFÉRENCE DÈS AUJOURD'HUI

Notez les procédures dans l'ordre d'exécution ;

Partagez cette procédure avec vos collaborateurs : répartissez les rôles de chacun ;

Notez coordonnées et contacts : en cas de compromission, vous n'aurez peut-être plus accès à ces informations.