avec ses partenaires AXION (intelligence artificielle & automatisation) et ComputerShop (partenaire local)

OFFRE EN RÉPONSE À L'APPEL D'OFFRES AO-02

Protection des collaborateurs et de leurs appareils contre les cybermenaces

Référence	ABAXINFO-TRAJETS-2026-001-AO02
Date	23 juin 2026
Validité de l'offre	180 jours à compter de la soumission
Périmètre	Ce volet (AO-02), extrait de la réponse consolidée aux 9 appels d'offres — précédé de la Phase 0 (prérequis transversal) — contractualisable séparément
Langue	Français
Contact ABAXINFO	Eric Darien - eric.darien@abaxinfo.com

> *Document confidentiel - établi à l'attention exclusive de la Fondation Trajets. Ce document répond au seul AO-02 ; l'offre complète (Phase 0, 9 volets, dépendances inter-volets, planning global, TCO 3 ans) est disponible dans le document consolidé offre.html.*

Partie I - Contexte & engagements communs

> *Cette partie est commune à notre réponse aux 9 appels d'offres de la Fondation Trajets ; elle est reprise à l'identique dans chacun des 9 documents de volet.*

1. Synthèse exécutive

La Fondation Trajets recherche un partenaire capable de renforcer la sécurité, la résilience et l'efficacité de son système d'information, tout en rendant son Pool Informatique pleinement autonome. C'est exactement notre manière de travailler.

ABAXINFO est votre interlocuteur unique pour l'ensemble des appels d'offres. Pour les sujets d'intelligence artificielle et d'automatisation, nous nous appuyons sur notre partenaire AXION, spécialisé sur ces technologies. Vous gardez un seul point de contact, une seule équipe, une seule responsabilité.

Il s'agit d'une **offre globale**, qui répond aux neuf appels d'offres dans un document d'ensemble cohérent. Elle reste **ajustable à la demande**, selon vos priorités et vos financements.

- **Proximité :** nous restons proches, à taille humaine, avec un support en français.
- **Autonomie :** nous vous rendons autonomes plutôt que dépendants (transfert de compétences à chaque appel d'offres).
- **Souveraineté :** vos données sensibles restent protégées et hébergées en Suisse, dans le respect de la LPD.

2. Qui nous sommes

ABAXINFO - votre partenaire informatique de proximité

ABAXINFO accompagne les organisations de Suisse romande sur l'ensemble de leur informatique : infrastructure, sécurité, environnement Microsoft 365, support et accompagnement des équipes. Nous privilégions une relation directe, dans la durée, et un support réactif en français.

AXION - intelligence artificielle & automatisation

AXION est notre partenaire pour les projets d'IA et d'automatisation (assistant conversationnel, automatisation des processus). Cette complémentarité nous permet de couvrir l'intégralité de votre appel d'offres avec, côté Fondation Trajets, un seul interlocuteur : ABAXINFO.

ComputerShop - partenaire local

Service premium. Revendeur partenaire Apple, spécialisé dans la vente et la maintenance de matériel, en partenariat avec ABAXINFO depuis plus de 18 ans.

Un seul interlocuteur, une équipe que vous rencontrez

Vous ne subirez pas une rotation de consultants. Vous travaillez avec une équipe identifiée, qui connaît votre contexte et que vous rencontrez dès le cadrage.

3. Notre compréhension du contexte

La Fondation Trajets est une organisation genevoise d'intégration sociale et professionnelle dédiée à l'accompagnement de personnes vivant avec des troubles psychiques. Elle compte environ 230 collaborateurs répartis sur 16 sites, et s'appuie sur Microsoft 365 et sur un Pool Informatique dont la double mission - accompagner la Fondation Trajets et former des bénéficiaires - est au coeur de votre démarche.

- des données sensibles (bénéficiaires) qui imposent un haut niveau de protection et la conformité LPD ;
- une organisation multi-sites avec des usages mobiles et du télétravail ;
- un Pool Informatique à la disponibilité variable, qu'il faut outiller et rendre autonome ;
- des financements en partie conditionnels, qui imposent de la souplesse sur les calendriers.

4. Méthodologie et gouvernance de projet

Notre gouvernance de projet s'appuie sur **HERMES 2022**, la méthode de gestion de projet de la Confédération suisse (standard fédéral obligatoire depuis 2023) : des phases claires (Initialisation, Conception, Réalisation, Déploiement) et des **jalons de décision** (go / no-go) à chaque étape, qui donnent à la Fondation Trajets visibilité et contrôle. Sur cette base, nous appliquons une démarche progressive et pédagogique, pensée pour une fondation : cadrer, mettre en oeuvre par étapes (avec une phase pilote quand c'est pertinent), puis transférer. Les AO-05 et AO-06 en détaillent le phasage et les jalons.

Étape	Ce que nous faisons	Implication de la Fondation Trajets
1. Cadrage	État des lieux, besoins par site et par profil, priorisation	Ateliers courts, validation des priorités
2. Pilote	Mise en oeuvre sur un périmètre restreint (souvent le Pool IT)	Retours d'expérience, ajustements
3. Déploiement	Généralisation par vagues, en limitant les interruptions	Points d'étape réguliers
4. Transfert	Formation, documentation en français, accompagnement dégressif	Montée en autonomie du Pool IT

Outils collaboratifs et fluidité

Le pilotage s'appuie sur les outils Microsoft que vous utilisez déjà, notamment Microsoft Teams, pour faciliter la collaboration, le partage de documents et le suivi tout au long du projet.

Planning et flexibilité

Nous intégrons dès le départ la disponibilité variable du Pool Informatique et le caractère conditionnel de certains financements : les calendriers sont jalonnés mais souples, et un démarrage peut être reporté sans pénalité.

5. Engagements : protection des données (LPD) et sécurité

Compte tenu des données sensibles traitées, la conformité à la Loi fédérale sur la protection des données (LPD) est un engagement central de notre offre, et non une simple mention.

- **Données sensibles :** les données de santé de vos bénéficiaires (art. 5 let. c LPD) appellent un niveau de protection renforcé - c'est le fil conducteur de l'ensemble de nos engagements ci-dessous.
- **Localisation :** hébergement des données en Suisse (privilégié/obligatoire selon les appels d'offres).
- **Sécurité :** mesures techniques et organisationnelles (art. 8 LPD).
- **Sous-traitance :** cadre clair de traitement par un tiers lorsque applicable (art. 9 LPD).
- **Privacy by design :** protection des données dès la conception et par défaut (art. 7 LPD).
- **Analyse d'impact :** AIPD (art. 22 LPD) pour les traitements à risque, notamment l'IA.
- **Incidents :** annonce des violations au PFPDT dans les meilleurs délais (art. 24 LPD).

> *Référence : Loi fédérale suisse sur la protection des données (LPD). Engagements détaillés dans le volet AO ci-après et dans les Conditions communes, en fin de ce document.*

6. Transfert de compétences et autonomie du Pool Informatique

Notre objectif n'est pas de vous rendre dépendants de nous, mais de renforcer votre Pool Informatique. Chaque appel d'offres inclut un transfert de compétences : formation, documentation en français, ateliers pratiques et accompagnement qui diminue à mesure que votre autonomie augmente. Ce projet est aussi une occasion de formation pour vos bénéficiaires.

Phase 0 - Découverte terrain (préalable transversal)

Avant d'engager les 9 appels d'offres, nous réalisons une **Phase 0** de découverte terrain sur vos **16 sites** — un prérequis transversal qui fiabilise nos chiffrages et notre séquencement pour l'ensemble du programme. Cette étape, déjà évoquée avec vous, fait l'objet d'un document dédié : Phase 0 - Découverte terrain.

Partie II - Réponse à l'appel d'offres AO-02

AO-02 : Protection des collaborateurs et de leurs appareils contre les cybermenaces

Notre compréhension

Vous ne voulez pas d'un pare-feu de plus qui protège un périmètre, mais une protection qui suit la personne et ses appareils, où qu'ils se trouvent : le principe « connecté = protégé », transparent pour l'utilisateur et simple à gérer pour le Pool Informatique.

Notre approche

- Protection automatique des appareils (PC, Mac, smartphones, tablettes) dès la connexion, sur tout réseau.
- Anti-phishing, anti-malware/ransomware, filtrage web (y compris HTTPS), protection de la vie privée.
- Protection cyber des équipements réseaux (imprimantes, NAS...).
- Gestion centralisée simple, mises à jour automatiques, compatibilité Microsoft 365.

Hébergement en Suisse fortement privilégié, conformité LPD garantie, transparence sur le traitement des données.

Simplicité et protection automatique (votre critère n°1)

Votre priorité première est claire : une protection automatique, transparente, sans configuration. Notre réponse repose sur le principe « connecté = protégé » : dès qu'un appareil se connecte à Internet, quel que soit le réseau (WLAN d'entreprise, WLAN public, réseau mobile 4G/5G, box personnelle), la protection s'active automatiquement. Le collaborateur n'a rien à paramétrer, rien à activer, rien à comprendre.

- Configuration minimale côté utilisateur : une application légère, ou une connexion automatique, qui se met en place une fois et n'exige plus d'intervention au quotidien.
- Protection active dès la connexion, sur tout réseau, sans VPN à lancer ni pare-feu à régler.
- Transparence totale : aucune action quotidienne demandée au collaborateur, aucune friction dans son travail.
- Mises à jour de sécurité automatiques et quotidiennes, sans intervention du Pool Informatique ni de l'utilisateur.
- Gestion centralisée très simple pour le Pool Informatique : pas de configuration par réseau ni par site, une politique unique appliquée partout.

C'est l'inverse d'un pare-feu traditionnel : la protection ne défend pas un périmètre, elle suit la personne et ses appareils, où qu'ils se trouvent.

Cas d'usage concrets

La même protection accompagne le collaborateur dans tous ses contextes de travail, sans qu'il ait à y penser.

Situation	Ce qui se passe	Protection appliquée automatiquement
À domicile	Connexion depuis la box personnelle, navigation web, emails, téléchargement et impression de documents.	Anti-phishing, anti-malware, filtrage des sites malveillants, sans configuration de la box.
Dans un café / lieu public	WLAN public non sécurisé, accès aux applications cloud de la Fondation Trajets, consultation des emails.	Chiffrement des communications, anti-phishing, anonymisation et protection de la vie privée sur réseau non sûr.
En mobilité (train, bus)	Connexion 4G/5G via smartphone, consultation de documents professionnels, réponse aux emails.	Protection mobile native, anti-phishing, accès sécurisé aux données de la Fondation Trajets.
Au bureau	Réseau de la Fondation Trajets, accès aux serveurs locaux et aux applications cloud, impression.	Protection continue, contrôle des accès, prévention de la fuite de données.
Chez un partenaire	WLAN du partenaire, présentation depuis son PC, consultation de données de la Fondation Trajets.	Protection automatique quel que soit le réseau tiers, sans réglage à l'arrivée sur place.

Le point commun : la protection ne dépend ni du lieu, ni du réseau, ni d'une action de l'utilisateur. Elle est déjà là.

Fonctionnalités de protection

La solution couvre l'ensemble des menaces visées par votre cahier des charges, sur PC Windows et Mac, smartphones iOS et Android, et tablettes.

- **Anti-phishing :** blocage des emails et des sites frauduleux avant qu'ils n'atteignent l'utilisateur.
- **Anti-malware et anti-ransomware :** détection et blocage des codes malveillants.
- **Filtrage des sites web malveillants, y compris en HTTPS :** les connexions chiffrées sont elles aussi analysées.
- **Inspection approfondie du trafic (Deep Packet Inspection) :** analyse fine des flux pour repérer les menaces dissimulées.
- **Protection contre les attaques Zero Day :** détection des menaces inconnues, au-delà des signatures connues.
- **Protection contre le social engineering :** défense face aux tentatives de manipulation visant les collaborateurs.
- **Protection contre le tracking :** blocage de la collecte de données et de la traçabilité publicitaire.
- **Chiffrement sur réseaux non sûrs :** les communications sont protégées sur les WLAN publics et autres réseaux non maîtrisés.

Transparence pour l'utilisateur et pour l'administrateur

La transparence va dans les deux sens : rassurer le collaborateur sans le surcharger, et donner au Pool Informatique une vision claire sans exposer la vie privée des personnes.

- **Pour le collaborateur :** notifications des menaces bloquées et tableau de bord personnel des incidents évités, qui rend la protection visible et compréhensible.
- **Pour l'administrateur (Pool Informatique) :** vue agrégée et anonymisée des menaces, statistiques de sécurité par appareil et globales, reporting clair et actionnable - dans le respect de la sphère privée des collaborateurs.

La protection de la vie privée est ainsi assurée : l'administrateur pilote la sécurité sans accéder au détail de l'activité individuelle des personnes.

Protection du matériel fixe des locaux

Au-delà des collaborateurs et de leurs appareils, la même démarche s'étend aux équipements fixes et partagés présents sur vos sites.

- Équipements couverts : imprimantes multifonctions réseau, serveurs NAS, téléphones Microsoft Teams, écrans interactifs des salles de réunion, bornes Wi-Fi et infrastructure réseau.
- Segmentation du réseau lorsque c'est nécessaire, pour isoler ces équipements et limiter la surface d'attaque.
- Détection et blocage des mouvements latéraux suspects (propagation horizontale depuis le réseau interne).
- Surveillance en temps réel des équipements et alertes en cas de comportement anormal.
- Gestion centralisée simplifiée et compatibilité avec votre environnement Microsoft 365.

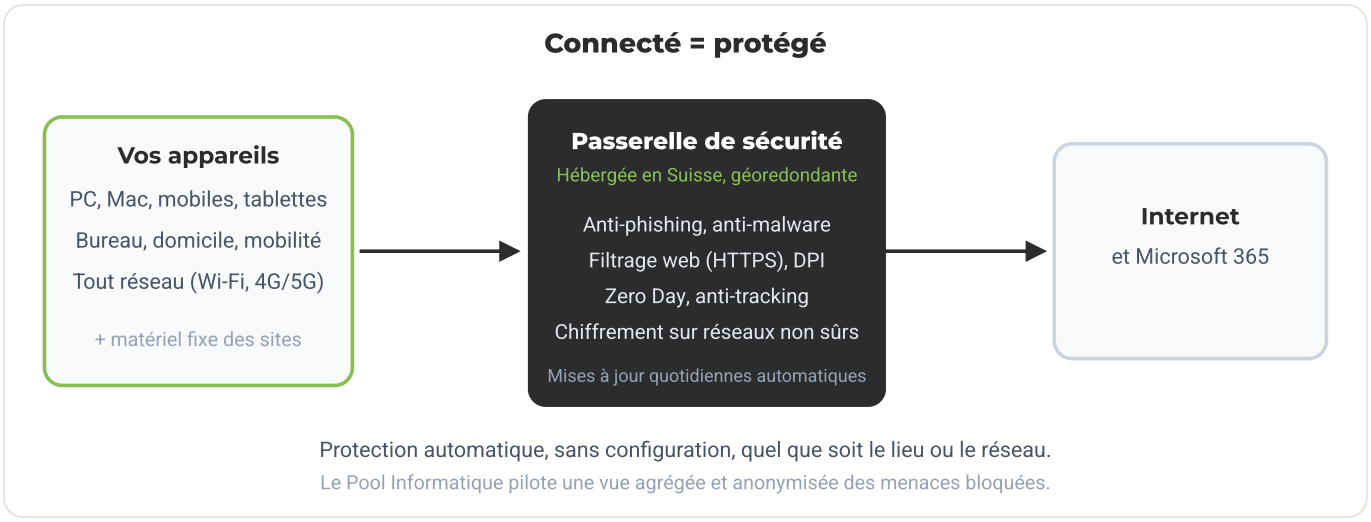
Selon votre contexte, cette couverture est apportée soit par extension de la solution de protection des collaborateurs, soit par une solution complémentaire dédiée au réseau local - l'option retenue est arbitrée au cadrage.

Architecture

L'architecture repose sur une passerelle de sécurité par laquelle transite le trafic Internet de chaque appareil.

- Chaque appareil se connecte automatiquement à une passerelle sécurisée ; tout le trafic y est analysé et filtré.
- Les menaces sont bloquées avant d'atteindre l'appareil, et la protection est maintenue quel que soit le réseau sous-jacent.
- Infrastructure géoredondante, gérée par des experts en cybersécurité, avec mises à jour automatiques quotidiennes.
- Application légère et performante, sans impact significatif sur les performances des appareils.
- Compatibilité Microsoft 365 et support de Windows, macOS, iOS et Android.

Hébergement en Suisse fortement privilégié, conformité LPD garantie, transparence sur le traitement des données.



> *Schéma de principe de l'architecture proposée. Les captures d'écran de l'application utilisateur et de l'interface d'administration sont fournies avec la solution retenue.*

Déploiement et formation

Le déploiement est progressif et pensé pour limiter les interruptions, dans la continuité de notre méthodologie de transfert de compétences.

- Déploiement par phases : phase pilote (souvent le Pool Informatique), puis généralisation par vagues sur les 16 sites.
- Onboarding simplifié des collaborateurs : installation de l'application ou connexion automatique, sans manipulation technique.
- Formation des administrateurs (Pool Informatique) à la gestion centralisée des politiques, au reporting et au suivi des incidents.
- Sensibilisation simple des utilisateurs, pour comprendre la protection et adopter les bons réflexes.
- Documentation en français et support au démarrage, avec un accompagnement dégressif à mesure que l'autonomie du Pool Informatique augmente.

Support et niveaux de service (SLA)

La protection des collaborateurs est un service en continu. Le support en français (un critère de votre évaluation) et les niveaux de service ci-dessous s'appliquent à ce service, avec une procédure d'escalade.

Engagement de service	Niveau
Canaux de support (téléphone, email, chat)	Outil de ticketing
Délai de prise en charge (h ouvrées)	04h00 du lundi au vendredi
Délai de résolution, incident bloquant (h ouvrées)	Diagnostic en 24h00
Disponibilité du support (plage horaire)	Du lundi au vendredi de 08h00 à 17h00
Procédure d'escalade (incident critique)	Création d'un incident critique (P1)
Conditions d'engagement et de sortie	Engagement assuré pendant toute la durée du contrat

Modèle tarifaire du support	Selon Bordereau de prix détaillé

> *Niveaux de service à confirmer par ABAXINFO à la contractualisation. Support assuré en français.*

Planning indicatif - 3 mois, méthode HERMES 2022

Cet appel d'offres est conduit selon **HERMES 2022**, la méthode de gestion de projet de la Confédération suisse. Le planning ci-dessous est **indicatif** et couvre le projet de bout en bout, du cadrage au déploiement généralisé et au transfert au Pool Informatique. Les **jalons de décision** HERMES offrent à la Fondation Trajets un point de validation (go / no-go) à la fin de chaque phase.

Phase HERMES 2022	Période	Activités clés (macro)	Jalon
Initialisation et cadrage	Mois 1	Cadrage du périmètre (appareils, profils, 16 sites, équipements fixes), exigences d'hébergement en Suisse et de protection des données (LPD), définition des politiques de sécurité et des critères du pilote.	Cadrage validé
Conception et architecture	Mois 1	Architecture de la passerelle de sécurité, politiques de protection (anti-phishing, anti-malware, filtrage web, vie privée), segmentation du réseau pour les équipements fixes, intégration Microsoft 365.	Conception validée
Réalisation et pilote	Mois 2	Mise en place de la solution sur un périmètre restreint (Pool Informatique), enrôlement des appareils, tests de protection sur différents réseaux, ajustement des politiques.	Pilote en service
Déploiement	Mois 3	Généralisation par vagues sur les 16 sites, protection des équipements fixes, onboarding des collaborateurs, formation des administrateurs et sensibilisation des utilisateurs.	Mise en service
Déploiement - hypercare et transfert	Mois 3	Accompagnement renforcé après démarrage (hypercare), suivi des menaces bloquées, transfert de compétences au Pool Informatique et documentation en français.	Clôture et autonomie

> *Planning indicatif (mois comptés à partir du lancement, T0), ajustable avec la Fondation Trajets, sans pénalité ; les jalons HERMES 2022 garantissent un go / no-go documenté à la fin de chaque phase.*

Bordereau de prix - modèle par utilisateur

Élément	Base	Prix (CHF)

Mise en place initiale	forfait	**CHF 16'800.-**
Licence par utilisateur	par utilisateur / an	**CHF 242,20**
↳ Total licences / an (230 utilisateurs × tarif annuel)	calculé	**CHF 55'706**
Protection des endpoints	par licence (jusqu'à 5 laptop + 5 tablettes + 5 téléphones)	**-**
Formation et accompagnement	forfait 2j	**CHF 3'360.-**
Support	annuel	**CHF 8'640.-**
↳ Coût projet (ponctuel)		**CHF 20'160**
↳ Coût récurrent (par an)		**CHF 64'346**

> *Dimensionnement : env. 230 collaborateurs, plusieurs appareils par personne. Saisir le **tarif par utilisateur / an** et le **nombre d'utilisateurs** : le total des licences est calculé automatiquement. Licence de type **Non Profit Company** (à confirmer). Conditions d'engagement et de sortie précisées à la contractualisation.*

Récapitulatif financier de ce volet

Protection des appareils « connecté = protégé » + équipements locaux.

Élément	Montant
Coût projet (ponctuel)	**CHF 20'160**
Coût récurrent (par an)	**CHF 64'346**

> *Détail du chiffrage : voir le bordereau de prix d'AO-02 ci-dessus. Le total consolidé (9 volets + Phase 0) et la projection sur 3 ans (TCO) figurent dans l'offre complète.*

Équipe assignée à ce volet

Une équipe identifiée, que la Fondation Trajets rencontre dès le cadrage. Équipe complète du programme (tous les rôles, CV synthétiques) : voir la Synthèse consolidée.

Rôle	Société	Responsabilité
Chef de projet - interlocuteur unique	ABAXINFO + AXION	Pilotage, gouvernance Teams, coordination des appels d'offres
Expert infrastructure & sécurité	ABAXINFO	Résilience, cybermenaces, MDM, endpoints
Référent protection des données (LPD)	ABAXINFO	Conformité LPD, AIPD, hébergement Suisse

Conditions communes

Élément	Engagement
Nature de l'offre	Offre ferme, engageant ABAXINFO pendant toute sa durée de validité (art. 3 al. 1 CO)
Validité de l'offre	180 jours à compter de la soumission
Langue	Français (communications, documentation, livrables)
Protection des données	Conformité LPD suisse ; hébergement en Suisse (privilégié/obligatoire selon l'appel d'offres)
Confidentialité	Stricte, pendant le contrat et 2 ans après son terme
Propriété intellectuelle	Livrables spécifiques propriété de la Fondation Trajets ; savoir-faire et méthodes génériques restent au prestataire

Réversibilité	Récupération des données et portabilité vers un autre prestataire en fin de contrat
Financement	Démarrage adaptable au caractère conditionnel des financements
Support	En français, avec SLA (prise en charge, résolution) précisés à la mise en production
Prix et TVA	Prix en CHF hors taxes ; TVA en sus au taux légal en vigueur ; modalités de paiement et échéancier précisés au contrat
Garantie	Garantie sur les configurations et livrables remis (durée et modalités précisées au contrat)
Responsabilité	Responsabilité limitée au montant des prestations concernées, dans les limites du droit suisse ; assurance responsabilité civile professionnelle
Non-engagement	La Fondation Trajets reste libre de ne pas donner suite à la présente offre, sans frais ni indemnité de préparation
Droit applicable / for	Droit suisse ; for juridique à Genève

Risques, hypothèses & dépendances

Éléments identifiés à la lecture de l'ensemble de vos appels d'offres et notre manière de les gérer (liste commune aux 9 volets ; les dépendances propres à ce volet sont également rappelées dans la Partie II ci-dessus).

Point	Description	Notre approche
Financement conditionnel	Démarrage soumis à l'obtention de financements	Calendrier souple, démarrage reportable sans pénalité, contractualisation AO par AO
Disponibilité du Pool Informatique	Disponibilité variable (nombreux projets en cours)	Phases pilotes, jalons espacés, ateliers courts, documentation pour autonomie
BIA = prérequis (AO-08)	Le bilan d'impact métier conditionne les deux sous-volets de résilience	Réalisé en premier puis réutilisé pour l'IT et l'organisationnel
Accès aux environnements	Microsoft 365 / Entra ID, sites, documentation existante	À mettre à disposition par la Fondation Trajets en début de projet
Données sensibles (bénéficiaires)	Traitement de données de santé, exigences LPD	Cadre LPD (Partie I §5), hébergement Suisse, AIPD pour l'IA
Dépendances entre appels d'offres	Ex. tenant M365 assaini avant MDM et assistant IA	Ordonnancement recommandé proposé lors du cadrage

Structuration documentaire (AO-05)	Une centaine de documents à harmoniser avant l'assistant IA	Chiffrée en option (audit + cadre méthodologique)

> *Ce document constitue la réponse ABAXINFO au volet **AO-02 : Protection des collaborateurs et de leurs appareils contre les cybermenaces**. Il s'inscrit dans une réponse globale portant sur les 9 appels d'offres de la Fondation Trajets, précédée d'une Phase 0 - Découverte terrain (prérequis transversal). Les dépendances entre volets, le planning consolidé et le coût total de possession sur 3 ans figurent dans la Synthèse consolidée. L'offre complète (tous les volets détaillés dans un seul document) reste disponible dans offre.html, ou sur la page des réponses détaillées.*