# Analyse d'impact « compétences »

20 JANVIER

# Contexte de l'analyse

Cette analyse de risques en matière de traitement de données personnelles a pour objectif d'aider à la construction de traitements respectueux des principes de protection de la vie privée et de permettre la démonstration de conformité au RGPD.

Cette analyse se fonde sur un cas précis d'échange de données personnelles impliquant :

- Un acteur public (Région) et un acteur privé de l'EdTech,
- Des données relatives à l'identité d'une personne et à ses compétences professionnelles
- Le choix en amont de la base légale du consentement afin de pouvoir inclure un rôle d'intermédiaire de données en charge de la gestion du consentement

Cette analyse a pour vocation d'offrir une vision globale des risques liés à ce cas spécifique d'utilisation et de partage de données personnelles. Il pourra être augmenté par des approfondissements complémentaires, en incluant :

- D'autres acteurs de l'EdTech proposant des prestations complémentaires (e-portfolio, matching IA, etc.)
- Des données de mineurs.

Cette analyse se base sur un contexte dans lequel :

- Les mesures de sécurité et organisationnelles nécessaires ont préalablement été définies contractuellement dans l'accord de protection des données,
- Les obligations de chacune des parties et leur qualité ont également été prédéfinies ; une répartition plausible de responsabilité est indiquée infra (sous-traitance et co-responsabilité de traitement).

# Préambule

La Région Ile-de-France, via sa stratégie de bassins d'emploi, a créé un espace de collaboration des acteurs de l'emploi, de la formation et de l'insertion au niveau local. Prometheus-X propose de venir étendre et renforcer cette stratégie par la création d'un écosystème de données de compétences, ouvert à tous les acteurs et centré sur la personne, positionnant la Région comme la première et plus innovante Smart Région d'Europe via une infrastructure numérique en lien avec la stratégie européenne de la donnée.

# Présentation des acteurs :

| Acteur | Rôle |
|---|---|
| **Ile de France** | Orienter les jeunes et les demandeurs d'emplois, leur proposer des formations adaptées, les mettre en relation avec les organismes de formation ou d'accueil (apprentissage) et d'emploi. Suivre l'évolution professionnelle d'une personne, suivre le parcours d'une personne entre les acteurs de l'orientation. Obtenir des statistiques agrégées et des analyses de compétences/offre et demande de formation/emploi sur son territoire. |

| | |
|---|---|
| **Prometheus-X/Vision** | S’assurer que le consentement des personnes soit respecté, s’assurer que les aspects juridiques et de gouvernance du réseau soient respectés, s’assurer que l’identité de la personne concernée est vérifiée, s’assurer de l’interopérabilité des données entre la source de données et l’utilisateur de données |
| **JobReady** | Accompagner les personnes dans l'identification de leurs compétences douces, afin de pouvoir les valoriser et les développer. |

# Interactions :

1. Utiliser le suivi d’évolution professionnelle, l’analyse de compétence de la Région Ile de France pour les envoyer sur JobReady et déterminer les compétences douces.

2. Puis utiliser ces compétences pour les faire matcher avec les offres d’emploi de la région et proposer de la recommandation personnalisée de formations pour développer des compétences.

# Etude du contexte

## Présentation du (des) traitement(s) considéré(s)

| Description du traitement | |
|---|---|
| Parcours de la donnée | • Ile de France > JobReady : transmission d’informations sur la personne et son parcours pour l’identification des compétences de la personne<br>• JobReady > Ile de France : à partir des compétences identifiées orienter, recommander de la formation et des offres d’emploi. |
| Finalité | • Permettre l’identification des compétences douces et dures d’un individu à partie d’un parcours scolaire/professionnel identifié<br>• Permettre à partir des compétences/informations de faire de la recommandation en termes de formation et d’emploi |
| Base légale | • Consentement |
| Responsabilité de traitement | • Coresponsabilité de traitement (IdF et JobReady) |
| Intermédiaire de données/sous-traitant (si accès dans le cadre de la sécurisation/interopérabilité) | • Prometheus-X : Sous-traitance<br><br>Explication complémentaire : par la solution qu'elle propose la société Vision pourrait être |

| | |
|---|---|
| | considéré juste comme intermédiaire (sans accès aux données pour la gestion du consentement). Cependant, dans la description du cas d'usage il est question d'accès aux données pour les sécuriser, pour assurer leur interopérabilité etc. Ce qui relève de la ST.<br>De surcroit, cela laisse la porte ouverte à tous les services que d'autres EdTech au sein de Prometheus-X pourraient proposer (pseudo/anonymisation, ontologies/traducteurs de compétences entre référentiels, matching IA etc.) |

### Description des données, destinataires et durées de conservation

| Typologie des données | Source des données | Destinataires | Durée de conservation |
|---|---|---|---|
| Formation scolaire/universitaire | Région IdF | JobReady | **Option 1** (préférable pour réduire le degré de risque) : une durée à définir par le RT, un délai à calculer à partir de la date de dernière activité (1 an par exemple).<br><br>**Option 2** (moins préférable) : jusqu'au retrait du consentement mais risque de comptes dormants inactifs (et de violation) |
| mail | | | |
| identifiant | | | |
| nom | | | |
| sexe | | | |
| Date de naissance | | | |
| Projets professionnels | | | |
| Expérience professionnelle | | | |
| Loisirs | | | |
| Compétences | JobReady | IdF | Idem supra |

Point de vigilance : l'analyse qui suit s'appuie sur le tableau qui a été communiqué par les porteurs de projet. La typologie des données est à analyser sur la base d'un jeu de données "test" car nous ne maitrisons pas, par exemple, la nature du champ "expérience professionnelle". Des données sensibles pourraient-elles y figurer ? Ex recommandation administrative de la qualité de travailleur handicapé.

En cas d'autres prestataires (CampusSkills etc.) une description équivalente devra être décrite contractuellement en amont, en minimisant l'accès de chacun selon la finalité spécifique du service fourni.
Par exemple, il n'est pas certain que "nom" soit nécessaire pour la prestation fournie par JobReady, ou la date complète de naissance (année pourrait être suffisante).

# Etude des risques

Description et évaluation des mesures contribuant à traiter des risques liés à la sécurité des données (art. 32)

**Analyse et estimation des risques**

- **Focus sur le risque de "Profilage" :**

Le profilage est défini à l'article 4 du RGPD. Il s'agit d'un traitement utilisant les données personnelles d'un individu en vue d'analyser et de prédire son comportement, comme par exemple déterminer ***ses performances au travail, sa situation financière, sa santé, ses préférences, ses habitudes de vie, etc.***
Un traitement de profilage repose sur l'établissement d'un profil individualisé, concernant une personne en particulier : il vise à évaluer certains de ses aspects personnels, en vue d'émettre un jugement ou de tirer des conclusions sur elle.
Tout traitement de profilage doit faire l'objet d'une attention particulière, car il soulève par nature des risques importants pour les droits et libertés des personnes. Les dispositions du RGPD doivent donc être appliquées à ces traitements en tenant compte de cette spécificité, par exemple en assurant la plus grande transparence et le respect des droits des personnes concernées par le profilage réalisé.
Toutes les décisions entièrement automatisées ne sont pas interdites. Par exemple, les décisions fondées sur le consentement explicite des personnes concernées.

**Mesures nécessaires :**

- Mentions d'information adaptées
- Transparence sur les algorithmes utilisés
- Intervention humaine
- Mesures de sécurité adaptées

D'autres risques ont été identifiés (violation, qualité des données) et sont détaillés au paragraphe suivant. Certaines possibilités complémentaires de risque ont été identifiées mais ne sont pas directement liées au cas étudié.

- **Potentiel traitement de profilage faisant appel à des données provenant de sources externes (profilage + croisement de données)** : ce risque pourrait se poser en augmentant le nombre de prestataire EdTech et les services complémentaires proposées. Dans ce cas-là, il serait obligatoire d'ajouter au cadre contractuel une analyse d'impact préalable (La réalisation d'un PIA est obligatoire si le traitement de données personnelles est susceptible d'engendrer des risques élevés sur les droits et libertés des personnes, notamment s'il remplit au moins 2 des neufs critères définis dans les lignes directrices de l'EDPB)

- **Données de mineurs** : à priori, les personnes concernées ont > 15 ans (dans les compétences de la Région il y a aussi l'apprentissage et l'alternance). Toutefois, même dans l'éventualité de traitement de données concernant les « mineurs » (<15 ans) les données traitées ne semblent pas impacter le degré de gravité des risques identifiés, en revanche cela impliquerait une action d'information renforcée (+ gestion de consentement via l'autorité parentale).

# Tableau des risques, gravité, vraisemblance

| Risques | Principales sources de risques | Principales menaces | Principales mesures réduisant la gravité/vraisemblance | Gravité | Vraisemblance |
|---|---|---|---|---|---|

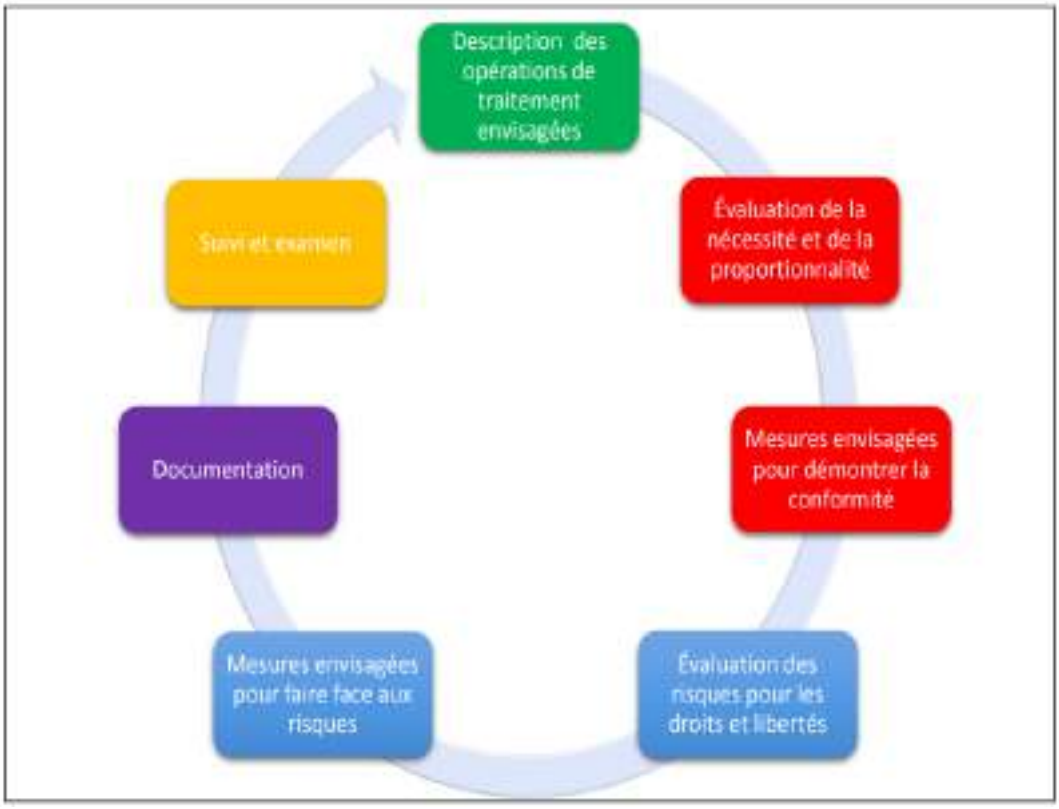
| | | | | | |
|---|---|---|---|---|---|
| **Violation (accès illégitime, Modification non désirée de données etc.)** | | Modifications inopportunes dans une base de données, effacement de fichiers utiles au bon fonctionnement, erreur de manipulation menant à la modification de données | Mesures de sécurité | Négligeable | (Appréciation nécessitant une connaissance des mesures de sécurité proposées) |
| **Qualité des données** | Données incomplètes ou imprécises car non structurées (ex. Projet professionnel) ou adossées à des référentiels à transposer | | Se baser sur un référentiel / utiliser un traducteur entre référentiels / accompagner l'utilisateur dans le renseignement des champs afin de recueillir des informations pertinentes | Négligeable | Vraisemblable<br>• (qualité) : référentiel<br>• (qualité/complétude/exhaustivité) : accompagnement |
| **Profilage** | Récupération de données/biais d'algorithme | Réception de courriers non sollicités (publicité ciblée)<br><br>Erreurs de profilage=> mauvaises recommandations | Mesures de sécurité<br><br>Actions d'information sur l'utilisation d'algorithmes de recommandations (mises à jour, claires, précises) | Négligeable<br><br>(Contrariété, peur de perdre le contrôle de ses données, sentiment d'atteinte à la vie privée) | La vraisemblance s'estime au regard du degré d'explicabilité que le prestataire JobReady peut fournir sur ses processus, de la vulnérabilités des supports et des capacités des sources de risque à les exploiter compte tenu des mesures de sécurités existantes |

A ajouter : descriptif des mesures de sécurité proposées par JobReady et Vision, à compléter avec les exigences complémentaires requises par la Région IdF

## Annexes:

https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf
Prometheus - legal Use case - Google Sheets
Cas d'usage compétences - GAIA X Prometheus - Google Sheets
Mes fichiers - OneDrive (sharepoint.com)

Le schéma suivant illustre le processus itératif générique suggéré pour la réalisation d'une AIPD[25]:



## 1.3 Typologie de sources de risques

Le tableau suivant présente des exemples de sources de risques :

| Types de sources de risques | Exemples |
|---|---|
| Sources humaines internes | Salariés, administrateurs informatiques, stagiaires, dirigeants |
| Sources humaines externes | Destinataires des DCP, tiers autorisés[2], prestataires, pirates informatiques, visiteurs, anciens employés, militants, concurrents, clients, personnels d'entretien, maintenance, délinquant, syndicats, journalistes, organisations non gouvernementales, organisations criminelles, organisations sous le contrôle d'un État étranger, organisations terroristes, activités industrielles environnantes |
| Sources non humaines | Codes malveillants d'origine inconnue (virus, vers...), eau (canalisations, cours d'eau...), matières inflammables, corrosives ou explosives, catastrophes naturelles, épidémies, animaux |

## 1.4 Échelle et règles pour estimer la gravité

La gravité représente l'ampleur d'un risque. Elle est essentiellement estimée au regard de la hauteur des impacts potentiels sur les personnes concernées, compte tenu des mesures existantes, prévues ou complémentaires (qu'il convient de mentionner en tant que justification).

L'échelle suivante peut être utilisée pour estimer la gravité des événements redoutés (**attention : ce ne sont que des exemples, qui peuvent être très différents selon le contexte**) :

| Niveaux | Descriptions génériques des impacts (directs et indirects) | Exemples d'impacts corporels[3] | Exemples d'impacts matériels[4] | Exemples d'impacts moraux[5] |
|---|---|---|---|---|
| 1. Négligeable | Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté | - Absence de prise en charge adéquate d'une personne non autonome (mineur, personne sous tutelle)<br>- Maux de tête passagers | - Perte de temps pour réitérer des démarches ou pour attendre de les réaliser<br>- Réception de courriers non sollicités (ex. : spams)<br>- Réutilisation de données publiées sur des sites Internet à des fins de publicité ciblée (information des réseaux sociaux réutilisation pour un mailing papier)<br>- Publicité ciblée pour des produits de consommation courants | - Simple contrariété par rapport à l'information reçue ou demandée<br>- Peur de perdre le contrôle de ses données<br>- Sentiment d'atteinte à la vie privée sans préjudice réel ni objectif (ex : intrusion commerciale)<br>- Perte de temps pour paramétrer ses données<br>- Non respect de la liberté d'aller et venir en ligne du fait du refus d'accès à un site commercial (ex : alcool du fait d'un âge erroné) |

| Niveaux | Descriptions génériques des impacts (directs et indirects) | Exemples d'impacts corporels[2] | Exemples d'impacts matériels[3] | Exemples d'impacts moraux[4] |
|---|---|---|---|---|
| 2. Limitée | Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés | - Affection physique mineure (ex. : maladie bénigne suite au non respect de contre-indications)<br>- Absence de prise en charge causant un préjudice minime mais réel (ex : handicap)<br>- Diffamation donnant lieu à des représailles physiques ou psychiques | - Paiements non prévus (ex. : amendes attribuées de manière erronée), frais supplémentaires (ex. : agios, frais d'avocat), défauts de paiement<br>- Refus d'accès à des services administratifs ou prestations commerciales<br>- Opportunités de confort perdues (ex. : annulation de loisirs, d'achats, de vacances, fermeture d'un compte en ligne)<br>- Promotion professionnelle manquée<br>- Compte à des services en ligne bloqué (ex. : jeux, administration)<br>- Réception de courriers ciblés non sollicités susceptible de nuire à la réputation des personnes concernées<br>- Élévation de coûts (ex. : augmentation du prix d'assurance)<br>- Données non mises à jour (ex. : poste antérieurement occupé)<br>- Traitement de données erronées créant par exemple des dysfonctionnements de comptes (bancaires, clients, auprès d'organismes sociaux, etc.)<br>- Publicité ciblée en ligne sur un aspect vie privée que la personne souhaitait garder confidentiel (ex : publicité grossesse, traitement pharmaceutique)<br>- Profilage imprécis ou abusif | - Refus de continuer à utiliser les systèmes d'information (whistleblowing, réseaux sociaux)<br>- Affection psychologique mineure mais objective (diffamation, réputation)<br>- Difficultés relationnelles avec l'entourage personnel ou professionnel (ex. : image, réputation ternie, perte de reconnaissance)<br>- Sentiment d'atteinte à la vie privée sans préjudice irrémédiable<br>- Intimidation sur les réseaux sociaux |
| 3. Importante | Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives | - Affection physique grave causant un préjudice à long terme (ex. : aggravation de l'état de santé suite à une mauvaise prise en charge, ou au non respect de contre-indications)<br>- Altération de l'intégrité corporelle par exemple à la suite d'une agression, d'un accident domestique, de travail, etc. | - Détournements d'argent non indemnisé<br>- Difficultés financières non temporaires (ex. : obligation de contracter un prêt)<br>- Opportunités ciblées, uniques et non récurrentes, perdues (ex. : prêt immobilier, refus d'études, de stages ou d'emploi, interdiction d'examen)<br>- Interdiction bancaire<br>- Dégradation de biens<br>- Perte de logement<br>- Perte d'emploi<br>- Séparation ou divorce<br>- Perte financière à la suite d'une escroquerie (ex. : après une tentative d'hameçonnage - phishing)<br>- Bloqué à l'étranger | - Affection psychologique grave (ex. : dépression, développement d'une phobie)<br>- Sentiment d'atteinte à la vie privée et de préjudice irrémédiable<br>- Sentiment de vulnérabilité à la suite d'une assignation en justice<br>- Sentiment d'atteinte aux droits fondamentaux (ex. : discrimination, liberté d'expression)<br>- Victime de chantage<br>- Cyberbullying et harcèlement moral |

| Niveaux | Descriptions génériques des impacts (directs et indirects) | Exemples d'impacts «corporels» | Exemples d'impacts matériels» | Exemples d'impacts moraux» |
|---|---|---|---|---|
| | | | - Perte de données clientèle | |
| 4 Maximale | Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter | - Affection physique de longue durée ou permanente (ex. : suite au non respect d'une contre-indication)<br>- Décès (ex. : meurtre, suicide, accident mortel)<br>- Altération définitive de l'intégrité physique | - Péril financier<br>- Dettes importantes<br>- Impossibilité de travailler<br>- Impossibilité de se reloger<br>- Perte de preuves dans le cadre d'un contentieux<br>- Perte d'accès à une infrastructure vitale (eau, électricité) | - Affection psychologique de longue durée ou permanente<br>- Sanction pénale<br>- Enlèvement<br>- Perte du lien familial<br>- Impossibilité d'ester en justice<br>- Changement de statut administratif et/ou perte d'autonomie juridique (tutelle) |

On retient la valeur dont la description correspond le mieux aux impacts potentiels identifiés, en comparant les impacts identifiés dans le contexte considéré avec les impacts génériques de l'échelle.

Elle peut être augmentée ou diminuée en fonction d'autres facteurs, tels que les suivants :

- le caractère identifiant des données ;
- la nature des sources de risques ;
- le nombre d'interconnexions (notamment avec l'étranger) ;
- le nombre de destinataires (ce qui facilite la corrélation de données initialement séparées).

## 1.5 Échelle et règles pour estimer la vraisemblance

La vraisemblance traduit la possibilité qu'un risque se réalise. Elle est essentiellement estimée au regard des vulnérabilités des supports concernés et de la capacité des sources de risques à les exploiter, compte tenu des mesures existantes, prévues ou complémentaires (qu'il convient de mentionner en tant que justification).

L'échelle suivante peut être utilisée pour estimer la vraisemblance des menaces :

1. Négligeable : il ne semble pas possible que les sources de risques retenues puissent réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge et code d'accès).
2. Limité : il semble difficile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge).
3. Important : il semble possible pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans les bureaux d'un organisme dont l'accès est contrôlé par une personne à l'accueil).
4. Maximal : il semble extrêmement facile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papier stockés dans le hall public de l'organisme).

On retient la valeur dont la description correspond le mieux aux vulnérabilités des supports et aux sources de risques identifiés.

Elle peut être augmentée ou diminuée en fonction d'autres facteurs, tels que les suivants :

- une ouverture sur Internet ou un système fermé ;
- des échanges de données avec l'étranger ou non ;
- des interconnexions avec d'autres systèmes ou aucune interconnexion ;
- l'hétérogénéité ou l'homogénéité du système ;
- la variabilité ou la stabilité du système ;
- l'image de l'organisme.

## 1.6 Menaces qui peuvent mener à un accès illégitime à des données

| Critères tracés | Types de supports | Actions | Exemples de menaces | Exemples de vulnérabilités des supports |
|---|---|---|---|---|
| C | Matériels | Utilisés de manière inadaptée | Utilisation de clefs USB ou disques inappropriés à la sensibilité des informations, utilisation ou transport d'un matériel sensible à des fins personnelles, le disque dur contenant les informations est utilisé pour une fin non prévue (par exemple pour transporter d'autres données chez un prestataire, pour transférer d'autres données d'une base de données à une autre, etc.) | Utilisable en dehors de l'usage prévu, disproportion entre le dimensionnement des matériels et le dimensionnement nécessaire (par exemple : disque dur de plusieurs To pour stocker quelques Go de données) |
| C | Matériels | Observés | Observation d'un écran à l'insu de son utilisateur dans un train, photographie d'un écran, géolocalisation d'un matériel, captation de signaux électromagnétiques à distance | Permet d'observer des données interprétables, émet des signaux compromettants |
| C | Matériels | Modifiés | Piégeage par un keylogger, retrait d'un composant matériel, branchement d'un appareil (ex. : clé USB) pour lancer un système d'exploitation ou récupérer des données | Permet d'ajouter, retirer ou substituer des éléments (cartes, extension) via les connecteurs (ports, slots), permet de désactiver des éléments (port USB) |
| C | Matériels | Perdus | Vol d'un ordinateur portable dans une chambre d'hôtel, vol d'un téléphone portable professionnel par un pickpocket, récupération d'un matériel ou d'un support mis au rebut, perte d'un support de stockage électronique | Petite taille, attractif (valeur marchande) |
| C | Logiciels | Utilisés de manière inadaptée | Fouille de contenu, croisement illégitime de données, élévation de privilèges, effacement de traces, envoi de **spams** depuis la messagerie, détournement de fonctions réseaux | Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées |
| C | Logiciels | Observés | Balayage d'adresses et ports réseau, collecte de données de configuration, étude d'un code source pour déterminer les défauts exploitables, test des réponses d'une base de données à des requêtes malveillantes | Possibilité d'observer le fonctionnement du logiciel, accessibilité et intelligibilité du code source |
| C | Logiciels | Modifiés | Piégeage par un keylogger logiciel, contagion par un code malveillant, installation d'un outil de prise de contrôle à distance, substitution d'un composant par un autre lors d'une mise à jour, d'une opération de maintenance ou d'une installation (des bouts de codes ou applications sont installés ou remplacés) | Modifiable (améliorable, paramétrable), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes), ne fonctionne pas correctement ou conformément aux attentes |
| C | Canaux informatiques | Observés | Interception de flux sur le réseau Ethernet, acquisition de données sur un réseau Wifi | Perméable (émission de rayonnements parasites ou non), permet d'observer des données interprétables |
| C | Personnes | Observées | Divulgation involontaire en conversant, écoute d'une salle de réunion avec un matériel d'amplification sonore/le | Peu discret (loquace, sans réserve), routinier (habitudes facilitant l'espionnage régulier) |
| C | Personnes | Détournées | Influence (hameçonnage, filoutage, ingénierie sociale, corruption), pression (chantage, harcèlement moral) | Influençable (naïf, crédule, altruiste, faible estime de soi, faible loyauté), manipulable (vulnérable aux pressions sur soi ou son entourage) |

| Critères touché | Types de supports | Actions | Exemples de menaces | Exemples de vulnérabilités des supports |
|---|---|---|---|---|
| C | Personnes | Perdues | Débauchage d'un employé, changement d'affectation, stage de test ou partie de l'organisation | Faible loyauté vis-à-vis de l'organisme, faible satisfaction des besoins personnels, facilité de rupture du lien contractuel |
| C | Documents papier | Observés | Lecture, photocopie, photographie | Permet d'observer des données interprétables |
| C | Documents papier | Perdus | Vol de dossiers dans les bureaux, vol de courriers dans la boîte aux lettres, récupération de documents mis au rebut | Portable |
| C | Canaux papier | Observés | Lecture de parapheurs en circulation, reproduction de documents en transit | Observable |

## 1.7 Menaces qui peuvent mener à une modification non désirées de données

| Critères touché | Types de supports | Actions | Exemples de menaces | Exemples de vulnérabilités des supports |
|---|---|---|---|---|
| I | Matériels | Modifiés | Ajout d'un matériel incompatible menant à un dysfonctionnement, retrait d'un matériel indispensable au fonctionnement correct d'une application | Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions) via des connecteurs (ports, slots), permet de détourner des éléments (port USB) |
| I | Logiciels | Utilisés de manière inadaptée | Modifications inopportunes dans une base de données, effacement de fichiers utiles au bon fonctionnement, erreur de manipulation menant à la modification de données | Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées |
| I | Logiciels | Modifiés | Manipulation inopportune lors de la mise à jour, configuration ou maintenance, contagion par un code malveillant, substitution d'un composant par un autre | Modifiable (améliorable, paramétrable), maîtrise (insuffisante par les développeurs ou les intervenants (spécifications incomplètes, pas de compétences internes), ne fonctionne pas correctement ou conformément aux attentes |
| I | Canaux informatiques | Utilisés de manière inadaptée | ***Man in the middle*** pour modifier ou ajouter des données à un flux réseau, rejet (déconnexion d'un flux interceptif) | Permet d'altérer les flux communiqués (interception puis réémission, éventuellement après altération), seule ressource de transmission pour le flux, permet de modifier les règles de partage du canal informatique (protocole de transmission qui autorise l'ajout de nœuds) |
| I | Personnes | Surchargées | Charge de travail importante, stress ou perturbation des conditions de travail, emploi d'un personnel à une tâche une maîtrise ou mauvaise utilisation des compétences | Ressources insuffisantes pour les tâches assignées, capacités inappropriées aux conditions de travail, compétences inappropriées à la fonction<br>Incapacité à s'adapter au changement |
| I | Personnes | Démarchées | Influence (espionnage, désinformation) | Influençable (naïf, crédule, dévoué) |
| I | Documents papier | Modifiés | Modification de chiffres dans un dossier, remplacement d'un document par un faux | Falsifiable (support papier ou contenu modifiable) |
| I | Canaux papier | Modifiés | Modification d'une note à l'insu du rédacteur, changement d'un pamphlet par un autre, envoi multiple de courriers contradictoires | Permet d'altérer les documents communiqués, seule ressource de transmission pour le canal, permet la modification du circuit papier |

## 1.8 Menaces qui peuvent mener à une disparition de données

| Critères touché | Types de supports | Actions | Exemples de menaces | Exemples de vulnérabilités des supports |
|---|---|---|---|---|
| D | Matériels | Utilisés de manière inadaptée | Stockage de fichiers personnels, utilisation à des fins personnelles | Utilisable en dehors de l'usage prévu |
| D | Matériels | Surchargés | Unité de stockage pleine, panne de courant, surexploitation des capacités de traitement, échauffement, température excessive, attaque par déni de service | Dimensionnement inapproprié des capacités de stockage, dimensionnement inapproprié des capacités de traitement, n'est pas approprié aux conditions d'utilisation, requiert en permanence de l'électricité pour fonctionner, sensible aux variations de tension |
| D | Matériels | Modifiés | Ajout d'un matériel incompatible menant à une panne, retrait d'un matériel indispensable au fonctionnement du système | Permet d'ajouter, retirer ou substituer des éléments (cartes, périphériques) via des connecteurs (ports, slots), permet de désactiver des éléments (port USB) |
| D | Matériels | Détériorés | Inondation, incendie, vandalisme, dégradation du fait de l'usure naturelle, dysfonctionnement d'un dispositif de stockage | Composants de mauvaise facture (fragile, facilement inflammable, sujet au vieillissement) ; n'est pas approprié aux conditions d'utilisation ; effaçable (vulnérable aux effets magnétiques ou vibratoires) |
| D | Matériels | Perdus | Vol d'un ordinateur portable, perte d'un téléphone portable, mise au rebut d'un support ou d'un matériel, disques sous dimensionnés amenant à une multiplication des supports et à la perte de certains | Portable, attractif (valeur marchande) |
| D | Logiciels | Utilisés de manière inadaptée | Effacement de données, utilisation de logiciels contrefaits ou copiés, erreur de manipulation menant à la suppression de données | Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées |
| D | Logiciels | Surchargés | Dépassement du dimensionnement d'une base de données, injection de données en dehors des valeurs prévues, attaque par déni de service | Permet de saisir n'importe quelle donnée, permet de saisir n'importe quel volume de données, permet d'exécuter des actions avec les données entrantes, peu interopérable |
| D | Logiciels | Modifiés | Manipulation inopportune lors de la mise à jour, configuration ou maintenance, codage par un code malveillant, substitution d'un composant par un autre | Modifiable (améliorable, paramétrable), maîtrise insuffisante par les développeurs ou les exploitants (spécifications incomplètes, peu de compétences internes), ne fonctionne pas correctement ou conformément aux attentes |
| D | Logiciels | Détériorés | Effacement d'un exécutable en production ou de code source, virus, bombe logique | Possibilité d'effacer ou de supprimer des programmes, exemplaire unique, utilisation complexe (mauvaise ergonomie, peu d'explications) |
| D | Logiciels | Perdus | Non renouvellement de la licence d'un logiciel utilisé pour accéder aux données, arrêt des mises à jour de maintenance de sécurité par l'éditeur, faillite de l'éditeur, corruption du module de stockage contenant les numéros de licence | Exemplaire unique (des contrats de licence ou du logiciel, développé en interne), attractif (rare, novateur, grande valeur commerciale), cessible (clause de cessibilité totale dans la licence) |
| D | Canaux informatiques | Surchargés | Détournement de la bande passante, téléchargement non autorisé, coupure d'accès Internet | Dimensionnement fixe des capacités de transmission (dimensionnement insuffisant de la bande passante, piège de numéros téléphoniques limités) |
| D | Canaux informatiques | Détériorés | Sectionnement de câblage, mauvaise réception du réseau wifi, oxydation des câbles | Altérable (fragile, cassable, câble de faible structure, à nu, gainage disproportionné), unique |

| Critères (axe) | Types de supports | Actions | Exemples de menaces | Exemples de vulnérabilités des supports |
|---|---|---|---|---|
| D | Canaux informatiques | Perdus | Vol de câbles de transmission en cuivre | Attractif (valeur marchande des câbles), transportable (légers, dissimulable), peu visible (cachable, insignifiant, peu remarquable) |
| D | Personnes | Surchargées | Charge de travail importante, stress ou perturbation des conditions de travail, emploi d'un personnel à une tâche non maîtrisée ou mauvaise utilisation des compétences | Ressources insuffisantes pour les tâches assignées, capacités inappropriées aux conditions de travail, compétences inappropriées aux conditions d'exercice de ses fonctions, incapacité à s'adapter au changement |
| D | Personnes | Détériorées | Accident du travail, maladie professionnelle, autre blessure ou maladie, décès, affection neurologique, psychologique ou psychiatrique | Limites physiques, psychologiques ou mentales |
| D | Personnes | Perdues | Décès, retraite, changement d'affectation, fin de contrat ou licenciement, rachat de tout ou partie de l'organisation | Faible loyauté vis-à-vis de l'organisme, faible satisfaction des besoins personnels, facilité de rupture du lien contractuel |
| D | Documents papier | Utilisés de manière inadaptée | Effacement progressif avec le temps, efficacité volontaire de parties d'un texte, réutilisation des papiers pour prendre des notes sans relation avec le traitement, gene faire la liste de course, utilisation des cahiers pour faire autre chose | Modifiable (support papier au contenu effaçable, papier thermique non résistant aux modifications de températures) |
| D | Documents papier | Détériorés | Vieillissement de documents archivés, endommagement des dossiers lors d'un incendie | Composants de nature facture (fragile, facilement inflammable, sujet au vieillissement), n'est pas approprié aux conditions d'utilisation |
| D | Documents papier | Perdus | Vol de documents, perte de dossiers lors d'un déménagement, mise au rebut | Portable |
| D | Canaux papier | Surchargés | Surcharge de courriers, surcharge d'un processus de validation | Existence de limites quantitatives ou qualitatives |
| D | Canaux papier | Détériorés | Coupure du flux suite à une réorganisation, blocage du courrier du fait d'une grève | Instable, unique |
| D | Canaux papier | Modifiés | Modification dans l'expédition des courriers, réaffectation des bureaux ou des locaux, réorganisation du circuit papier, changement de langue professionnelle | Modifiable (remplaçable) |
| D | Canaux papier | Perdus | Réorganisation supprimant un processus, disparition d'un transporteur de documents, vacance de poste | Utilité non reconnue |

## 1.9 Échelles pour le plan d'action

Les échelles suivantes peuvent être utilisées pour élaborer le plan d'action et suivre sa mise en œuvre :

| Critère | Niveau 1 | Niveau 2 | Niveau 3 |
|---|---|---|---|
| Difficulté | Faible | Moyenne | Élevée |
| Coût financier | Nul | Moyen | Important |
| Temps | Trimestre | Année | 3 ans |
| Avancement | Non démarré | En cours | Terminé |