

# PIA 1

---

## Sommaire:

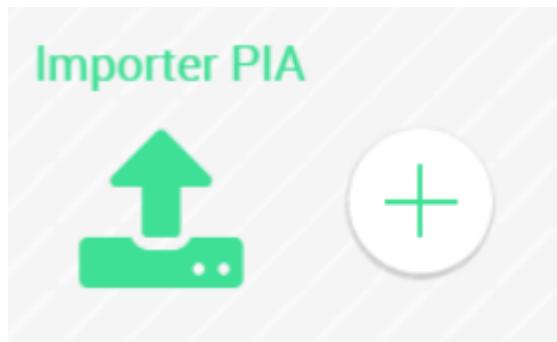
I.Introduction.....	1
II.Exercice 1.....	2
III.Exercice 2.....	11
IV.Exercice 3.....	11
V.Exercice 4.....	12
VI.Exercice 5.....	13
VII.Exercice 6.....	14
VIII.Conclusion.....	14

## I. Introducion

Dans ce TP nous allons découvrir comment vérifier comment est sécurisée l'entreprise et comment faire une expertise afin de savoir quoi améliorer. De plus, nous verrons l'utilisation des données à caractères personnel et leur traitement.

## II. Exercice 1

Importation du travail réalisé par M.Grospire dans l'application PIA en cliquant sur ce bouton :



Le travail de M.Grospire se télécharge dans l'application :



## Pour le risque d'accès illégitime à des données :

Comment estimez-vous la **gravité du risque**, notamment en fonction des impacts potentiels et des mesures prévues ?

(Non définie) Négligeable Limitée Importante Maximale

La gravité du risque est importante car une personne tiers va avoir accès à l'ensemble des informations sur le serveur, chiffre financier, informations secrète, données personnelle...

Une attaque pourrait donc faire fuiter des informations personnelles des salariés.

Enfin, si l'attaque vient d'un concurrent, l'attaque pourrait détruire l'entreprise en divulguant des projets à venir, expériences...

0 commentaire(s)

15/09/2019

Commenter

---

Comment estimez-vous la **vraisemblance du risque**, notamment au regard des menaces, des sources de risques et des mesures prévues ?

(Non définie) Négligeable Limitée Importante Maximale

Il est peu probable d'après les mesures mises en place qu'une personne puisse attaqué

0 commentaire(s)

15/09/2019

Commenter

## Pour le risque modification non désiré de donnée :

Comment estimez-vous la **gravité du risque**, notamment en fonction des impacts potentiels et des mesures prévues ? ^

(Non définie) Négligeable Limitée Importante Maximale

Si un salarié venait à supprimer l'entièreté des données cela aurait un impact dévastateur sur l'entreprise

0 commentaire(s)

15/09/2019

 Commenter ▾

Comment estimez-vous la **vraisemblance du risque**, notamment au regard des menaces, des sources de risques et des mesures prévues ? ^

(Non définie) Négligeable Limitée Importante Maximale

D'après les mesures mises en place il est peu probable qu'un salarié est accès facilement à toutes les données

0 commentaire(s)

15/09/2019

 Commenter ▾

## Pour le risque disparition de données

Comment estimatez-vous la **gravité du risque**, notamment en fonction des impacts potentiels et des mesures prévues ?

(Non définie) Négligeable Limitée Importante Maximale

Perdre les données en étant une entreprise peut potentiellement faire fermer cette dernière.

0 commentaire(s)

15/09/2019

 Commenter ▾

Comment estimatez-vous la **vraisemblance du risque**, notamment au regard des menaces, des sources de risques et des mesures prévues ?

(Non définie) Négligeable Limitée Importante Maximale

Grâce à l'archivage, même en cas de suppression des données, il y aurait quelques sauvegardes.

0 commentaire(s)

15/09/2019

 Commenter ▾

Pour le moment la cartographie des risques est la suivante :



## mesures existantes ou prévus:

**Chiffrement**

Un chiffrement des flux de données est réalisé par le protocole SSL.

0 commentaire(s)

15/09/2019

Commenter ▾

**Évaluation**

✗ À corriger   Améliorable   ✓ Acceptable

02/10/2025

Commentaire d'évaluation

Le protocole SSL est obsolète et présente des failles de sécurité connues.

Plan d'action / mesures correctives

Il faudrait utiliser TLS, idéalement la version 1.2 ou 1.3, pour garantir un chiffrement plus robuste et à jour.

---

**Contrôle des accès logiques**

Seules les personnes habilitées peuvent consulter les données personnelles des salariés. Le login correspond à leur nom de famille et le mot de passe à leur date de naissance.

(MOT DE PASSE FORT ! 12 Caractères

0 commentaire(s)

02/10/2025

Commenter ▾

**Évaluation**

✗ À corriger   Améliorable   ✓ Acceptable

02/10/2025

Commentaire d'évaluation

Le mot de passe basé sur la date de naissance est trop faible et facilement devinable.

Plan d'action / mesures correctives

Il faudrait utiliser des mots de passe forts, uniques et imposer une politique de complexité (longueur minimale, chiffres, lettres, caractères spéciaux), ainsi qu'une authentification à deux facteurs pour renforcer la sécurité.

---

**Archivage**

Les données sont sauvegardées sur un disque dur externe puis celui-ci est amené au service informatique pour le transfert dans une base de données de TESTOP et vers un serveur hébergé par la société OVH.

0 commentaire(s)

15/09/2019

Commenter ▾

**Évaluation**

✗ À corriger   Améliorable   ✓ Acceptable

02/10/2025

Commentaire d'évaluation

Le transfert manuel sur un disque dur externe présente des risques de perte ou de vol.

Plan d'action / mesures correctives

Il serait préférable d'utiliser un transfert sécurisé et automatisé (par exemple via SFTP ou un VPN) et de chiffrer les sauvegardes avant leur envoi vers le serveur hébergé par OVH.

---

**Gestion des postes de travail**

L'ouverture de la session du poste de travail qui sert à la collecte des données à caractère personnel est assurée par un login et un mot de passe uniques pour tout le service de la gestion du personnel.

(UTILISER PLUSIEURS MDP)

0 commentaire(s)

02/10/2025

Commenter ▾

**Évaluation**

✗ À corriger   Améliorable   ✓ Acceptable

02/10/2025

Commentaire d'évaluation

Un login et un mot de passe uniques pour tout le service ne permettent pas de tracer les actions individuelles et augmentent les risques en cas de fuite.

Plan d'action / mesures correctives

Il faudrait attribuer des identifiants personnels à chaque utilisateur et appliquer une politique de mots de passe robustes, éventuellement complétée par une authentification à deux facteurs.

## Accès illégitime à mes données:

**Évaluation**

À corriger    Améliorable    Acceptable

02/10/2025

**Commentaire d'évaluation**

Les deux mesures contribuent à traiter le risque, mais elles ne sont pas suffisantes :

**Plan d'action / mesures correctives**

Contrôle des accès logiques : À corriger → abandonner les mots de passe basés sur la date de naissance et utiliser des identifiants individuels avec des mots de passe forts et, idéalement, une authentification à deux facteurs.

Prenant en compte le plan d'action, comment ré-évaluez-vous la **gravité de ce risque** (Accès illégitime à des données) ?

(Non définie)   Négligeable   Limittée   Importante   Maximale

Prenant en compte le plan d'action, comment ré-évaluez-vous la **vraisemblance de ce risque** (Accès illégitime à des données) ?

(Non définie)   Négligeable   Limittée   Importante   Maximale

## Modifications non désirées de mes données:

**Évaluation**

À corriger    Améliorable    Acceptable

02/10/2025

**Commentaire d'évaluation**

les identifiants partagés permettent à n'importe quel utilisateur du service de modifier les données

les mots de passe faibles ne sécurisent pas l'accès aux données sensibles

**Plan d'action / mesures correctives**

utiliser TLS 1.2 ou 1.3 pour protéger les données en transit, mais cela n'empêche pas les modifications non désirées sur le serveur.

il faudrait des comptes individuels et des droits limités selon le rôle.

il faut des mots de passe forts et, si possible, une authentification à deux facteurs pour limiter les modifications non autorisées.

Prenant en compte le plan d'action, comment ré-évaluez-vous la **gravité de ce risque** (Accès illégitime à des données) ?

(Non définie)   Négligeable   Limittée   Importante   Maximale

Prenant en compte le plan d'action, comment ré-évaluez-vous la **vraisemblance de ce risque** (Accès illégitime à des données) ?

(Non définie)   Négligeable   Limittée   Importante   Maximale

# Disparitions de données

## Évaluation

 À corriger

 Améliorable

 Acceptable

02/10/2025

### Commentaire d'évaluation

les comptes partagés permettent à n'importe quel utilisateur de supprimer des données

### Plan d'action / mesures correctives

limite l'accès aux personnes habilitées, mais des mots de passe faibles ou partagés ne protègent pas efficacement contre la suppression ou la disparition des données.

la sauvegarde existe, mais le transfert manuel sur disque dur présente un risque de perte ou vol ; il faudrait automatiser le transfert et chiffrer les sauvegardes.

il faut des comptes individuels avec droits limités selon le rôle.

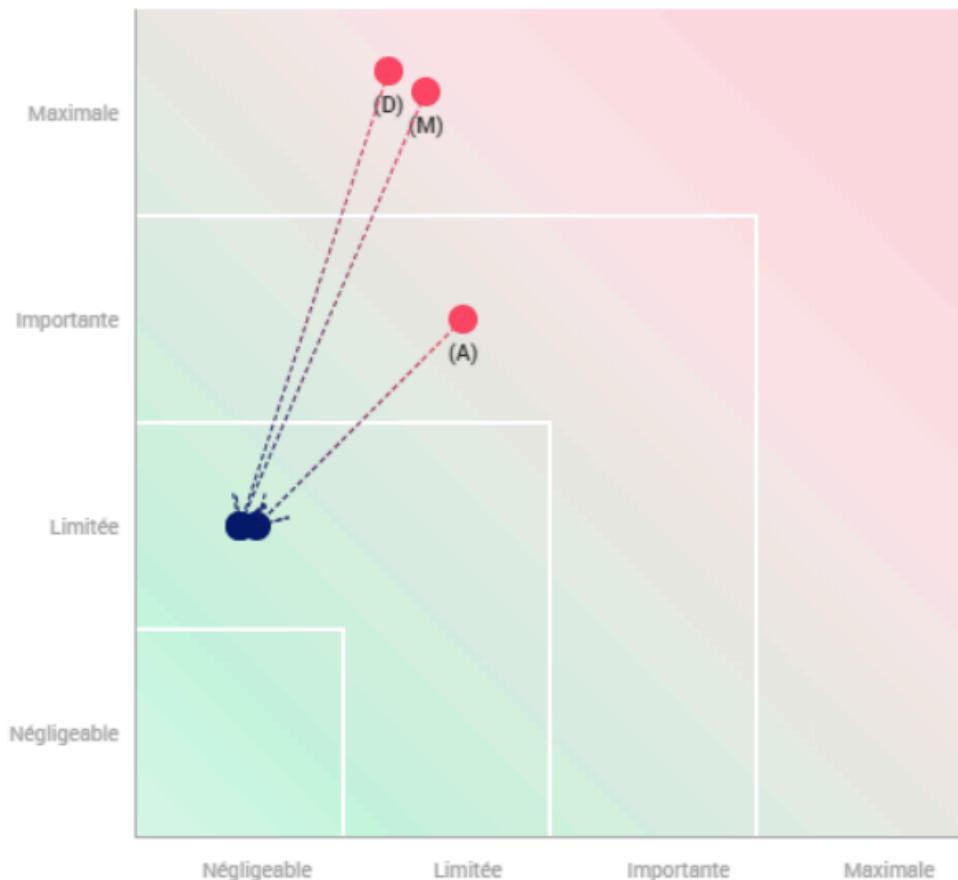
Prenant en compte le plan d'action, comment ré-évaluez-vous la **gravité de ce risque** (Accès illégitime à des données) ?



Prenant en compte le plan d'action, comment ré-évaluez-vous la **vraisemblance de ce risque** (Accès illégitime à des données) ?



Après toutes ces modifications, voici la cartographie des risques :



Nous voyons que les risques sont encore présents mais largement limités.

### III. Exercice 2

La conformité au Règlement Général sur la Protection des Données (RGPD) repose sur l'élaboration rigoureuse d'une cartographie des traitements. Ce processus, qui vise à recenser et qualifier l'intégralité des flux de données personnelles, constitue un outil de pilotage stratégique. Il permet d'anticiper les risques juridiques et techniques tout en définissant une politique de sécurité adaptée.

Il est nécessaire de faire le registre des traitements des données à caractère personnel avant afin de ne pas oublier de risques mais surtout de pouvoir corriger ce qui doit l'être. Cela permet de recenser tous les risques et les mesures au même endroit.

### IV. Exercice 3

Lorsque l'on saisit des données personnelles (nom, email, historique d'achats...) sur castorama.fr, elles peuvent être :

- Utilisés pour nous identifier et gérer notre compte
- Partagé avec d'autres sociétés du groupe
- Utilisé à des fins d'analyse ou d'études

Les données ne restent donc pas uniquement chez Castorama, elles peuvent être partagées avec d'autres entités et utilisées pour des analyses.

Non, la seule lecture de l'extrait ne permet pas de dire que la confidentialité n'est pas assurée. Le texte indique que les données peuvent être partagées avec des tiers, mais il ne précisent pas comment elles sont protégées (ex : chiffrement, contrôle d'accès). Pour affirmer qu'il y a un problème de confidentialité, il faudrait connaître les mesures de sécurité mises en place par Castorama.

## V. Exercice 4

- collecte : formulaire en ligne, cookies, carte de fidélité...
- Stockage : bases de données, serveurs d'entreprise...
- Diffusion : campagnes marketing, partage avec des partenaires commerciaux...

Collecte et enregistrement des données.

- Conservation et organisation (bases de données)
- Analyse statistique et marketing
- Transmission à des tiers -Suppression ou anonymisation des données

-Obtenir le consentement des personnes avant de collecter et d'utiliser leurs données.

- Respecter RGP
- Garantir la confidentialité, l'intégrité et la disponibilité des données.
- Permettre l'accès, la rectification et la suppression des données par les utilisateurs
- Ne collecter que les données nécessaires

-Amendes administratives

-Dommages et intérêts aux victimes

-perte de confiance et atteinte à la réputation de l'entreprise

## VI. Exercice 5

Scénarios	Sécurité	Sûreté	Justifications
L'ensemble des serveurs est hors-service à cause d'une inondation du local technique.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	L'inondation est un événement naturel, donc c'est une menace non intentionnelle
Les données d'un hôpital sont illisibles à la suite d'une attaque de type ransomware.	<input checked="" type="checkbox"/>		L'attaque est délibérée et malveillante
L'apparence du site vitrine d'une entreprise est modifiée pendant le week-end par des personnes malveillantes.	<input checked="" type="checkbox"/>		L'attaque est délibérée et malveillante
Une surcharge électrique temporaire due à des travaux réalisés dans les bâtiments de la société provoque une panne des routeurs.		<input checked="" type="checkbox"/>	Il s'agit d'un incident accidentel lié à l'environnement

## VII. Exercice 6

Données	Caractère personnel	Justifications
Le nom de l'enseigne du magasin carrefour	Non	Ce n'est pas une personne physique mais une entreprise
L'adresse Courriel professionnelle d'un directeur des services informatiques	Oui	Elle permet d'identifier directement une personne physique
Une photo postée sur un réseau social	Oui	l'image peut permettre d'identifier la personne
Une vidéo de présentation de son parcours professionnel envoyée à une entreprise dans le cadre d'un recrutement	Oui	La vidéo peut permettre d'identifier la personne
Les coordonnées GPS de localisation d'un smartphone	Oui	Une personne qui aurait accès aux coordonnées pourrait trouver la personne
Le groupe sanguin d'un patient stocké sur le serveur de base de données de son médecin	Oui	Le groupe sanguin est forcément lié à un dossier avec le nom de la personne
Les enregistrements de vidéosurveillance d'un datacenter	Oui	L'image des personnes filmées est un élément qui permet de les identifier
Le numéro d'enregistrement au registre du commerce et des société d'une entreprise	Non	On parle ici d'une entreprise, pas d'une personne physique
Le numéro de sécurité sociale d'un salarié saisi sur la fiche d'embauche	Oui	Identifiant unique d'une personne physique.

## VIII. Conclusion

Ce tp a été un peu compliqué au début à cause de l'application un peu compliqué à comprendre sur le début mais après avoir analysé le logiciel, on découvre que c'est une application très utile pour les entreprises.