Baptiste Gaillard *BTS SIO*

Cybersécurité : Thème 1 - PIA2

Étape 1 – Installation et analyse du paramétrage de l'outil

Les 4 phases du PIA (telles qu'affichées dans l'application)

1. **Décrire le traitement et le contexte**
   On précise la finalité, les acteurs (responsable, sous-traitants, DPO), les personnes concernées, les catégories de données, les flux, la durée de conservation et le périmètre.

2. **Analyser la nécessité et la proportionnalité**
   On vérifie la base légale (ex. consentement), la minimisation des données, l'information des personnes et le respect des principes RGPD (finalité, limitation, transparence).

3. **Apprécier les risques sur les droits et libertés**
   On identifie les menaces (accès illégitime, modification, perte/disparition), on évalue **gravité** et **vraisemblance**, puis on cartographie les risques.

4. **Déterminer et valider les mesures de maîtrise**
   On définit les mesures techniques/organisationnelles (chiffrement, journalisation, sauvegardes, contrôle d'accès, MFA), on arrête un **plan d'action**, puis on décide de l'**acceptabilité du risque** et de la conformité.

Étape 2 – Saisie des informations utiles pour le PIA

4. Délimitation du contexte (Document 1)

- Les données sont collectées avec le consentement explicite des personnes interrogées.

- Seules les données nécessaires à l'étude sont enregistrées.

- Les données sont stockées dans des serveurs sécurisés appartenant à CentreCall ou à ses prestataires.

- Aucune donnée n'est transférée en dehors de l'Union européenne.

- Les droits des personnes (accès, rectification, opposition, effacement) sont garantis via le site de CentreCall.

5. Dispositif mis en place pour le respect des principes fondamentaux

- Collecte loyale et transparente.
- Limitation des finalités à la seule étude de marché.
- Conservation limitée dans le temps.
- Mesures de sécurité : chiffrement SSL, sauvegardes redondantes, traçabilité des accès.
- Journalisation des accès au serveur.
- Sensibilisation des employés à la protection des données.

6. Mesures existantes pour la protection de la vie privée (Document 2)

Principe	Mesure appliquée
Chiffrement	Protocole SSL pour le transfert des données.
Journalisation	Enregistrement des identifiants des utilisateurs dans un journal sécurisé.
Archivage	Sauvegardes redondantes sur plusieurs serveurs et supports.

7. Catégories de risques et exemples

Catégorie de risque	Exemple identifié
Accès illégitime à des données	Piratage du serveur ou mot de passe faible d'un opérateur.
Modifications non désirées	Suppression accidentelle ou altération d'un fichier de réponses.
Disparition de données	Perte des sauvegardes à cause d'une panne matérielle.

Étape 3 – Analyse des résultats de l'étude des risques

8. Cartographie des risques

Risque	Gravité	Probabilité	Niveau de risque	Mesures complémentaires
Accès illégitime	Élevée	Moyenne	**Important**	Authentification forte, mot de passe complexe, double facteur.
Modification non désirée	Moyenne	Moyenne	**Modéré**	Sauvegarde quotidienne automatique, contrôle d'accès.
Disparition de données	Élevée	Faible	**Modéré**	Sauvegardes hebdomadaires externes, test de restauration.

9. Plan d'action proposé

- **Sécurité technique :**
    - Renforcer la politique de mots de passe (12 caractères min., rotation semestrielle).
    - Mettre en place une authentification à deux facteurs pour les opérateurs.
- **Organisation et gouvernance :**
    - Former les employés à la sécurité des données et aux obligations RGPD.
    - Mettre à jour le registre de traitement tous les six mois.
- **Suivi et évaluation :**
    - Audits internes de conformité tous les ans.
    - Rapports d'incident à transmettre au DPO.

Résumé global

- **Niveau de conformité RGPD :** satisfaisant avec un faible risque résiduel.
- **Décision finale :** le traitement est autorisé sous réserve de la mise en œuvre du plan d'action.