Thème 1 Chapitre 1

Activité 3.1: Protéger des données à caractère personnel

C3.1-2 Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel

Mission 2

Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel

Mission

Mmer Azri souhaite maintenant identifier les risques liés au traitement des données à caractère personnel dans le cadre du processus d'études de marché.

Pour réaliser ce travail, vous devez prendre appui sur la méthode PIA (Privacy Impact Assessment, en français « analyse d'impact relative à la protection des données ») proposée par la CNIL et présentée dans le document 1.

© Delagrave

Travail à faire

La première phase de La méthode PIA repose sur La compréhension du contexte.

1 - Identifiez, dans la description du contexte, les éléments permettant d'identifier les vulnérabilités liées au traitement des données à caractère personnel.

Documents 1 et 2 Fiche savoir techn. 1

Les données sont partagées au téléphone par les clients et entrées manuellement sur un ordinateur, les donnes sont stockes par Centre-Call sur leurs serveurs, les données sont partagées avec les différents clients.

2 - Complétez le tableau d'analyse des scénarios de menaces présenté dans le document 4. Justifiez les niveaux de vraisemblance retenus pour chaque menace.

Documents 3 et 4 Fiches savoir techn. 1 et 2

Source de menace	Type de menace	Bien support	Niveau de vraisemblance	Critères de sécurité		
				C	D	I
Scénario de menace lié au **risque 1** : attaquant extérieur	Espionnage	Ordinateur de l'opérateur	**2 : limité** (les données ne sont présentes que sur le serveur de base de données.)	X (L'authentification n'est plus limitée aux personnes habilitées)		
Scénario de menace lié au risque 2 : attaquant intérieur	**Attaque intérieur**	**Base de données**	**3 : important**		**X**	
Scénario de menace lié au risque 3 : attaquant extérieur	**Erreur de configurations**	**Base de données**	**1 : négligeable**			
Scénario de menace lié au risque 4 : attaquant extérieur	**Attaque extérieur**	**Serveurs**	**4 : maximale**			
Scénario de menace lié au risque 5 : attaquant extérieur	**Attaque**	**Serveurs**	**1 : négligeable**			

C : confidentialité – D : disponibilité – I : intégrité.
Mesures de la vraisemblance : 1 négligeable – 2 limitée – 3 importante – 4 maximale.

© Delagrave

3 - Retrouvez, pour chaque risque mentionné, l'événement redouté et son niveau de gravité estimé en complétant le document 5.

Documents 3 à 5 Fiche savoir techn. 1

Exemple : scénario 1	Usurpation d'identité	**Niveau de gravité : 3 (important)** Les données confidentielles peuvent être exploitées par une entité malveillante.
Scénario 2	Suppression ou vol de données	Niveau de gravite : 4 (maximale) C'est le niveau de gravite le plus important, il signifie l'échec complet des deux principaux objectifs de l'entreprise, le stockage de données et sa protection.
Scénario 3	Consultation des donnes sans habilitation (par des employés)	Niveau de gravite : 2 (limitée) Cela révèle de failles de configurations (qui pourrait reveler des failles dans le système) ainsi que d'un problème de confidentialité pour les clients
Scénario 4	Altération des données sur le serveur	Niveau de gravite : 3 (importante) Cela dépends de la situation, une altération des données peut être permanente et signifier un accès total au serveur mais pas dans tout les cas.
Scénario 5	Arrêt du serveur par attaque repetees	Niveau de gravite : 1 (négligeable) Le serveur serait inaccessible un moment mais les fichiers et disques resteraient protégés.

Mesures de la gravité : 1 négligeable – 2 limitée – 3 importante – 4 maximale.

4 - Cartographiez les risques liés au traitement des données à caractère personnel par un schéma croisant les niveaux de vraisemblance et de gravité déterminés précédemment.

Fiche savoir techn. 1

	Vraisemblance	Gravité
Risque 1		
Risque 2		
Risque 3		
Risque 4		
Risque 5		

5 - Rédigez une note de synthèse à l'intention de Mme AZRI pour l'informer des risques identifiés et de leur hiérarchisation. Cette note doit énumérer des propositions pour garantir la confidentialité et l'intégrité des données à caractère personnel dans le cadre du processus d'études de marché.

Fiche savoir techn. 2

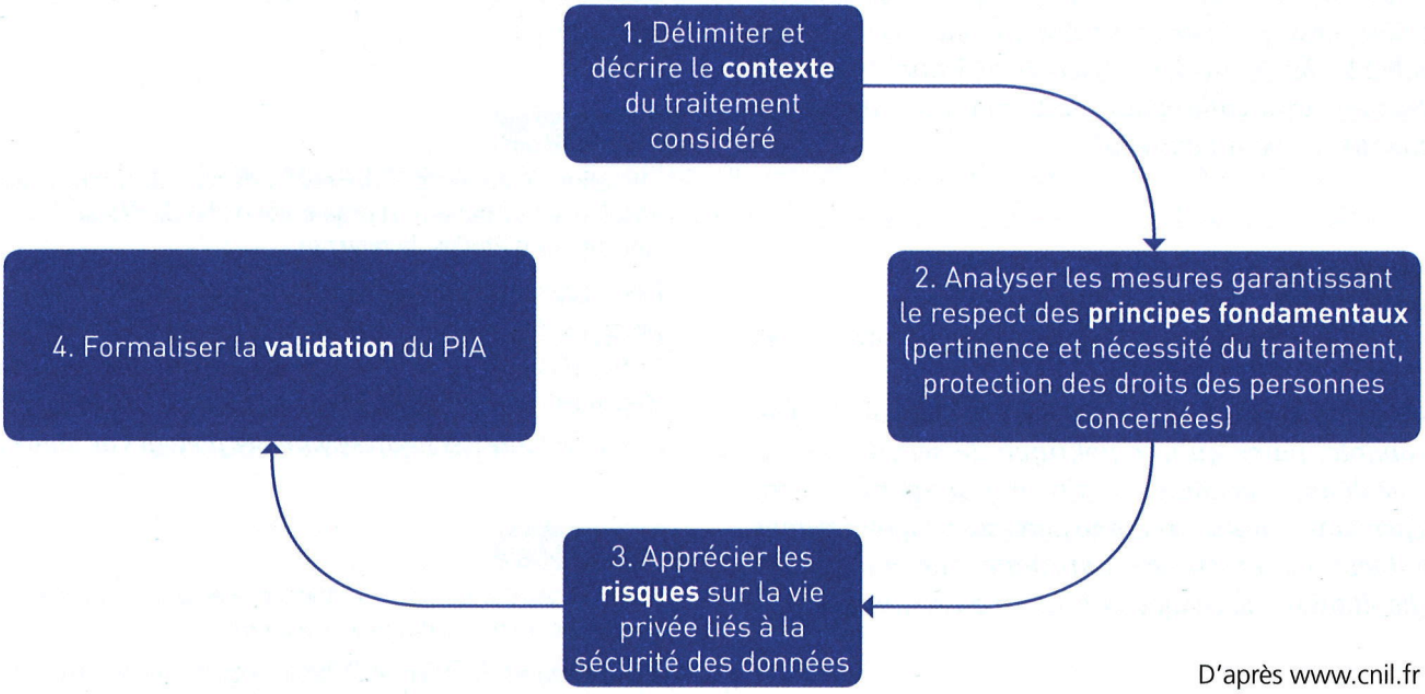
© Delagrave

Document 1

Démarche PIA (Privacy Impact Assessment)

Une «analyse d'impact relative à la protection des données» (voir article 35 du **RGPD**), plus communément appelée Privacy Impact Assessment (PIA) décrit la manière d'employer la méthode **EBIOS** (Expression des besoins et identification des objectifs de sécurité) préconisée par l'**ANSSI**.

Quatre phases permettent de mener un PIA :



Document 2

Contexte du PIA relatif au traitement d'une étude de marché chez CentreCall.

Le PIA porte sur le processus d'étude de marché mis en œuvre par Centre-Call. M"° Azri est responsable du traitement des données manipulées dans le cadre de ce processus. L'objectif des études de marché est de collecter et d'analyser des informations qui identifient les caractéristiques d'un marché. Les données traitées sont ensuite mises à disposition des différents clients.

Cycle de vie des données

- Demande d'enregistrement de l'appel : la personne contactée notifie son acceptation ou non de l'enregistrement de l'entretien, et elle est informée des conditions de traitements de ses données à caractère personnel.
- Collecte des réponses aux questionnaires : les données sont collectées par l'opérateur par saisie sur son ordinateur de bureau, puis enregistrées sur un serveur de base de données hébergé par CentreCall.
- Vérification de l'enregistrement audio de l'entretien : l'enregistrement audio est vérifié puis sauvegardé sur un serveur de fichiers hébergé par CentreCall.
- Analyse des résultats de l'étude de marché.

Supports des données

- Un téléphone IP (Internet Protocol) est utilisé pour la conversation.
- Un ordinateur de bureau est mobilisé lors de l'enregistrement des réponses et de l'entretien.
- Plusieurs serveurs de base de données redondants stockent les réponses aux questionnaires, et un serveur de fichiers stocke l'enregistrement audio de l'entretien.

Données traitées
Informations personnelles, réponses au questionnaire, enregistrement audio de l'entretien, analyse des résultats de l'étude de marché.
Destinataires
- CentreCall. - Clients de l'étude de marché.
Durée de conservation
Les données sont conservées 1 an.

© Delagrave

Document 3

Risques identifiés sur Les données à caractère personnel

Scénario 1

Usurpation d'un compte d'authentification d'un opérateur par un intervenant extérieur lors d'une opération de maintenance sur un ordinateur, pour récupérer des données confidentielles.

Les données se situent sur le serveur de base de données et non sur le poste de l'opérateur; la menace reste peu probable. Par contre, les données confidentielles peuvent bénéficier à une entité malveillante avec des conséquences importantes pour CentreCall.

Scénario 2

Suppression ou vol de données dans la base de données par un salarié mécontent, dans l'objectif de nuire à CentreCall, voire de les communiquer à un concurrent.

L'action est facile à mener avec des conséquences importantes.

Scénario 3

Consultation de données par un employé non-habilité due à une erreur de manipulation.

La consultation de données sans habilitation est peu probable, parce qu'une politique de sécurité rigoureuse dans ce domaine est mise en place par Mme Azri. Cependant, dans le cas d'une faiblesse temporaire dans ce domaine, les risques sont limités car le périmètre d'habilitation de chaque utilisateur est restreint.

Scénario 4

Altération de données sur le serveur de base de données par un attaquant extérieur à l'organisation afin de déstabiliser les campagnes d'études de marché.

Les serveurs de base de données sont actuellement peu protégés des menaces qui viendraient de l'extérieur de l'organisation. Une attaque de ce type provoquerait d'importantes conséquences, notamment sur la qualité et la crédibilité des futures synthèses d'études de marché.

Scénario 5

Arrêt du serveur de base de données par une attaque extérieure due à une multitude de requêtes.

Actuellement, le serveur de base de données pourrait être arrêté pour cette raison. Le risque serait alors maximal, car le travail de tous les opérateurs et des Call managers dépend de l'accès aux données hébergées sur le serveur.

Document 4

Analyse des scénarios de menaces

Source de menace	Type de menace	Bien support	Niveau de vraisemblance	Critères de sécurité		
				Confidentialité	Disponibilité	Intégrité
Scénario de menace lié au risque 1 : attaquant	Espionnage	Ordinateur de l'opérateur	**2** : limité (les données ne sont présentes que sur le serveur de base de données)	L'authentification n'est plus assurée aux seules personnes habilitées.		
…	…	…				

Mesure de la vraisemblance : **1** négligeable – **2** limité – **3** important – **4** maximal.

Document 5

Événements redoutés

Exemple : scénario 1	Usurpation d'identité	Niveau de gravité : **3** (important). Les données confidentielles peuvent être exploitées par une entité malveillante.
…	…	

Mesure de la gravité : **1** négligeable – **2** limité – **3** important – **4** maximal.

© Delagrave