Table des matières

Étude du contexte

Le besoin et le contexte

L'Unité de Recherche (UR) TOTO souhaite construire un SI qui permettra de constituer des Panels de personnes disponibles pour participer aux recherches de l'UR TOTO.

Les données contenues dans cette base seront stratégiques pour l'UR car à l'avenir ses activités de recherches dépendront du contenu de cette base.

Après étude, il s'avère qu'il n'existe pas de logiciel (en SAAS ou dans d'autres organisme) répondant à leurs besoins.

Ce SI se nommera GesVol, il sera entièrement sous la responsabilité de l'UR. C'est-à-dire développé, hébergé et maintenu par les agents informaticiens de l'unité. L'utilisateur de GesVol est un scientifique de l'unité TOTO.

Finalités du traitement GesVol

L'UR validera les candidatures ou non pour les recherche (étude, questionnaire, expérience …).

Le SI GesVol permettra :

- L'importation des données des volontaires retenus
- L'utilisateur scientifique pourra corriger ponctuellement des données
- Le scientifique responsable d'une étude sélectionnera et exportera les données d'un lot de volontaires pour l'expérimentation concernée

Le fondement juridique de cette base est nécessaire à l'exécution de la mission d'intérêt public de l'unité TOTO.

Références à respecter

Le traitement est soumis uniquement au respect de la Loi Informatique et Libertés (Règlement européen sur la protection des données - mai 2018).

Dans le cadre de l'open science, l'ouverture des données sur l'Internet n'est pas envisageable. Par ailleurs, la Protection du Potentiel Scientifique et Technique ne s'applique pas ici.

Pas de transfert de données vers un pays situé hors de l'Union européenne.

Hypothèse et périmètre de l'étude

Le périmètre de l'étude est l'accès aux données à caractère personnelles de GesVol.

Les demandes des volontaires et la gestion de leurs échanges avec les scientifiques ne rentrent pas dans le périmètre de cette étude, cette gestion est réalisée par un autre outil.

Les données sélectionnées de la base sont exportées par les utilisateurs scientifiques sur leur poste puis elles sont cumulées avec les données récoltées pendant l'étude scientifique.

Éléments à protéger

Les éléments immatériels

Les grands ensembles de données traités sont :

- État civil : Nom, prénom, date de naissance, adresse postale, adresse email, téléphone, sexe
- Données sociologiques : situation familiale, pays de naissance, niveau d'étude, situation d'activité profession, religion
- Données « santé » : fumeur, problèmes de santé
- Données liées à la participation aux études : indemnisations versées par l'UR TOTO, RIB

Leur nature est du texte.

Par ailleurs, les données d'état civil peuvent venir de personnes dites vulnérables (ex : mineurs).

Les éléments matériels

C'est-à-dire les éléments qui peuvent supporter (stocker) les données du SI GesVol.

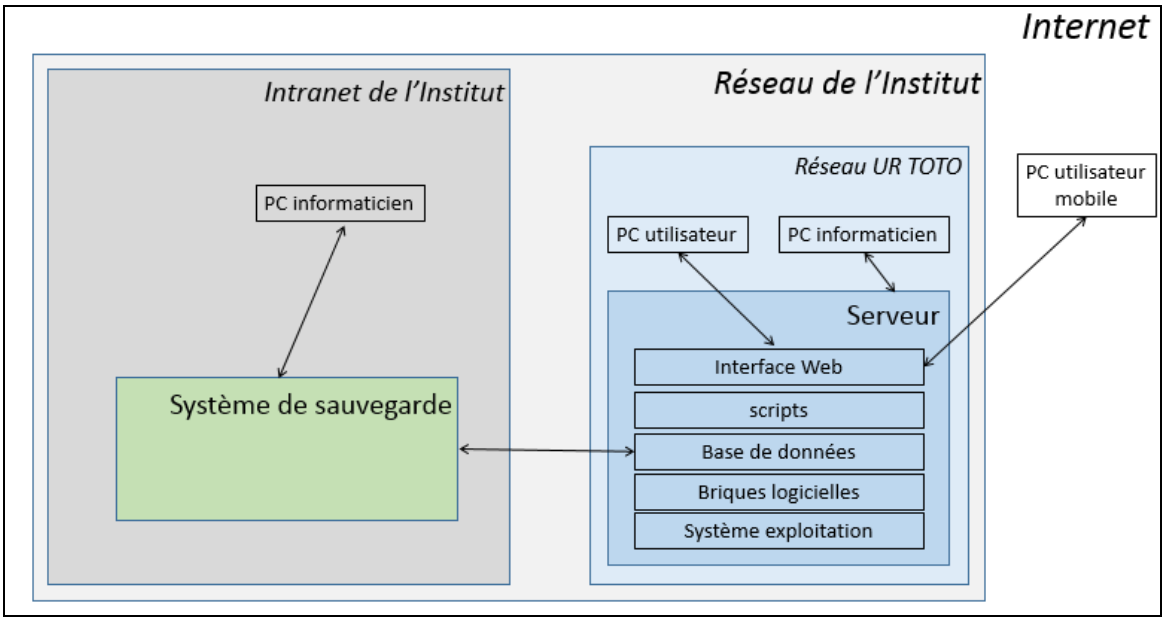
- Les postes de travail des administrateurs et des développeurs
- Les postes de travail de l'UR TOTO
- Le serveur supportant les données et les applications
- Le réseau de l'Institut
- Les serveurs de sauvegarde de l'Institut

Les personnes

C'est-à-dire les personnes qui peuvent accéder aux données (en lecture et/ou en écriture) du SI GesVol.

- Informaticiens (administrateurs et développeurs) de l'UR TOTO
- Les utilisateurs (scientifiques de l'UR TOTO)
- Les informaticiens administrateurs de la DSI (réseau et sauvegarde)

Schéma d'architecture



Les informaticiens de l'UR TOTO installent et maintiennent : le système d'exploitation, les briques logicielles (par ex : MySQL, phpMyAdmin, Apache, PHP …) et l'application GesVol qui comprend une base de données type MySQL, une interface Web écrite en PHP à destination des utilisateurs et plusieurs logiciels et scripts de traitement de données (par ex en PHP et JavaScript).

Les comptes et l'authentification sont propres à l'application GesVol. Il n'y a pas de système de gestion des droits dans l'application GesVol.

Les postes de travail de l'UR TOTO sont tous des PC portables.

Le réseau informatique est entièrement géré par les équipes de l'Institut dont dépend l'UR TOTO. Ce réseau héberge les PC de l'unité et son serveur, il est constitué d'adresses IP publiques.

La gestion des sauvegardes est assurée par la DSI de l'Institut.

Mesures de sécurité existantes

Mesures organisationnelles

Une formation est dispensée par les informaticiens à tous les nouveaux utilisateurs (attestation de formation enregistrée). Une notice d'utilisation est disponible pour les utilisateurs (document Assurance Qualité Recherche). Les utilisateurs scientifiques doivent signer une charte d'utilisation décrivant leurs engagements. Les administrateurs s'assurent que tous les utilisateurs ont bien signé cette charte.

Mesures de sécurité logique

À l'issue de la formation, sont attribués aux utilisateurs un login et un mot de passe. Lorsqu'un utilisateur quitte l'unité, son compte est automatiquement révoqué

La BD est sauvegardée régulièrement par le service SV de la DSI de l'Institut.

Les environnements de développement (PC des développeurs) et de production sont distincts (serveur).

La traçabilité des accès au serveur est assurée via les logins de connexion ou les @IP des journaux des serveurs.

L'antivirus est présent sur tous les PC de l'UR.

Le serveur supportant GesVol est accessible depuis l'Internet, la liaison se fait avec chiffrement (https)

Mesures de sécurité physique

Fermeture par badges du bâtiment de l'UR. Les bureaux sont quasiment tous fermés à clefs. La salle machine est protégée par un digicode.

Les équipements de la DSI sont dans un Datacenter certifié ISO27000.

Évaluation du risque

Les facteurs à considérer

L'impact ou la conséquence

Les impacts peuvent toucher plusieurs périmètres (Institut, unité, projet …) et être de plusieurs ordres, par exemple :

- Perturbation du fonctionnement interne (ex : cout humain de reconstruction)
- Fuite intelligence économique
- Pertes financières pour l'établissement
- Engagement de responsabilité, conséquences juridiques
- Atteinte à l'image de l'établissement
- Sur les personnes (stress voire maladie …)
- Etc.

Un impact peut être produit par la réalisation d'une menace exploitant un défaut de sécurité (vulnérabilité) sur un ou plusieurs des critères confidentialité, intégrité et disponibilité.

Si le risque se produisait, les principaux impacts sont :

Concernant	**l'entité (unité)**	**Les personnes**
la confidentialité	Perte de confiance des volontaires, retrait des expériences, arrêt potentiel des recherches de l'UR	Données très sensibles (problèmes de santé, profession, religion) exposées sur Internet -> exploitation malveillante
l'intégrité	Remise en cause des résultat des recherches	Dysfonctionnement (ex : pas de dédommagement financier)
la disponibilité	Pertubation du fonctionnement des recherches	Pas d'impact

La menace et les sources de risque

Menace : mode opératoire composé d'une ou plusieurs actions unitaires sur des supports de données. La menace peut être utilisée, volontairement ou non, par des sources de risques, et peut alors provoquer un événement redouté.

Les principales menaces qui pourraient permettre la réalisation du risque sont :

Concernant	
la confidentialité	Intrusion sur serveur ; vol d'un PC avec données de la base exportée

l'intégrité	Mauvaise manipulation (en écriture) d'un utilisateur
la disponibilité	Restitution sauvegarde non fiable ; PB techniques (logiciel ou matériel)

Source de risque : personne, interne ou externe à l'organisme, agissant de manière accidentelle ou délibérée (ex : administrateur informatique, utilisateur, attaquant externe, concurrent), ou source non humaine (ex : eau, matériaux dangereux, virus informatique non ciblé) qui peut être à l'origine d'un risque.

Les principales sources de risques pouvant en être à l'origine sont :

Concernant	
la confidentialité	Pirates, ancien employé malveillant, utilisateur non attentif à son PC
l'intégrité	Les utilisateurs
la disponibilité	Les informaticiens (DSI et unité)

Risque de non-conformité RGPD :

Les risques de non-conformité RGPD non liés à la sécurité informatique ont déjà été traités avec le Délégué à la Protection des Données qui accompagne l'unité TOTO :

Non-conformité RGPD	* Travailler sur la durée de conservation : Penser en termes d'activité du volontaire. Quels critères pour considérer qu'un volontaire ne participe plus aux études ? Et si inactivité : script automatique pour anonymiser les données ou détruire les données le concernant *La BDD doit supporter l'effacement des données d'un volontaire en cas d'exercice des droits de celui-ci * Refaire une notice d'information, incluant l'exercice des droits et revoir sa diffusion

Estimation des risques si exploitation d'un défaut de confidentialité, intégrité, disponibilité

Définitions

Confidentialité - accès illégitime à des données : propriété selon laquelle l'information n'est pas rendue disponible ni divulguée à des personnes, des entités ou des processus non autorisés (ISO 27000).

Intégrité - modification non désirées de données : propriété d'exactitude et de complétude (ISO 27000).

Disponibilité - disparition de données : propriété d'être accessible et utilisable à la demande par une entité autorisée (ISO 27000).

Tableaux de l'évaluation des risques

Pour chaque risque, la **gravité du risque**, est estimée en fonction des impacts potentiels et des mesures de sécurité actuelles, ceci pour les impacts concernant l'unité puis pour les impacts concernant les personnes dont l'unité détient les données à caractères personnels.

Pour chaque risque, la **vraisemblance du risque** (sa probabilité), est estimée au regard des menaces, des sources de risques et des mesures de sécurité actuelles.

Échelles pour les estimations *(1 : Négligeable ; 2 : Limité ; 3 : Important ; 4 : Maximal)* en annexe.

Gravité des risques SSI

Risque	Risque (Défaut de sécurité)	Gravité du risque	Justification de la gravité
C-A	Confidentialité - accès illégitime à des données	4	Pourrait aller jusqu'à fermeture de unité

I-M	Intégrité - modification non désirées de données	3	Mauvaise image de l'UR cout humain important de reconstruction
D-D	Disponibilité - disparition de données	2	Gène non bloquante pour les utilisateurs

Gravité des risques IL (RGPD)

Risque	Risque (Défaut de sécurité)	Gravité du risque	Justification de la gravité
C-A	Confidentialité - accès illégitime à des données	4 (ou 3 ?)	Les pb de santé exposés, récupérés puis exploités peuvent pousser au divorce, suicide etc.
I-M	Intégrité - modification non désirées de données	2	Les dysfonctionnements ne généreront pas de conséquence bloquante
D-D	Disponibilité - disparition de données	1	Les personnes ne sont pas concernées

Vraisemblance des risques

Défaut de sécurité	**Vraisemblance du risque**	**Justification de la vraisemblance**
Confidentialité - accès illégitime à des données (risque C-A)	4	Exposition sur Internet. Base totale potentiellement sur PC portable.
Intégrité - modification non désirées de données (risque I-M)	4	Modification autorisée aux utilisateurs
Disponibilité - disparition de données (risque D-D)	3	Les PB techniques sont courants

Cartographies des risques

Risque SSI

Gravité	4				C-A
	3				I-M
	2			D-D	
	1				
Vraisemblance		1	2	3	4

Risque IL (RGPD)

Gravité	4				C-A
	3				
	2				I-M
	1			D-D	
Vraisemblance		1	2	3	4

Plan action

Listez ci-dessous les mesures à mettre en place pour diminuer de façon significative les risques notés.

Risque SSI et IL	Mesure / Action	Qui	Échéance
C-A	Déplacer la BD dans l'Intranet de l'institut + utilisation d'un VPN pour les utilisateurs en mobilité	Informaticiens (UR + DSI)	Dans 3 mois
C-A	Chiffrer les disques durs des PC	Informaticiens (UR + DSI)	Dans 6 mois
C-A	Supprimer l'exportation de la base totale pour les utilisateurs	Informaticiens (UR + DSI)	Dans 1 mois
I-M	Supprimer la modification des données pour les utilisateurs	Informaticiens (UR + DSI)	Dans 1 mois
D-D	Procédure de tests réguliers des SV	Informaticiens (UR + DSI)	Dans 1 an

Estimation des risques résiduels après réalisation du plan d'action

Risque SSI

Gravité	4		C-A		
	3	I-M			
	2		D-D		
	1				
Vraisemblance		1	2	3	4

Risque IL (RGPD)

R*isque C-A, I-M et D-D à placer à l'intérieur*.

Gravité	4		C-A		
	3				
	2	I-M			
	1		D-D		
Vraisemblance		1	2	3	4

Acceptation du risque

Validation par le responsable du système d'information

1.Le commanditaire (décisionnel) valide ou non, et dans ce cas indique pourquoi (par exemple : coût financier trop élevé, moyens humains insuffisants, etc.), le plan d'action :

Plan d'action validé.

2.Le commanditaire indique éventuellement tout commentaire sur les propositions (par exemple : revu des scenarios, des niveaux de gravité, etc.) :

3.Compte tenu des risques résiduels et du plan d'action associé, le système GesVol est proportionnel et nécessaire à l'activité de recherche de l'unité TOTO conformément à l'intérêt légitime du responsable du système d'information.

L'étude de sécurité est validée par Jeanine Dupont, DU de l'unité TOTO (et si pertinent : indiquez : au cours de la réunion (mettre la date) en présence de (mettre les noms)).

Jeanine Dupont

Annexe

Échelles pour les estimations

La gravité

La gravité représente l'ampleur d'un risque. Elle est essentiellement estimée au regard de la hauteur des impacts potentiels. L'estimation de la gravité doit donc être réalisée par les porteurs d'enjeux (MOA, financeur, responsable de traitement, coordinateur du projet …)

La gravité est estimée dans les deux cas sur une échelle de 1 à 4 :

		Sécurité du SI	Sécurité de la personne concernée
1	Négligeable	Les impacts peuvent être surmontés sans difficultés	Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments qu'elles surmonteront sans difficulté
2	Limité	Les impacts peuvent être surmontés avec quelques difficultés	Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés
3	Important	Les impacts peuvent être surmontés avec de sérieuses difficultés	Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives
4	Maximal	Les impacts sont potentiellement insurmontables	Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter

La vraisemblance, la probabilité

La vraisemblance traduit la possibilité qu'un risque se réalise. Elle dépend essentiellement des vulnérabilités des supports face aux menaces et des capacités des sources de risques à les exploiter. La maîtrise d'œuvre (informatique) étudie les scénarios de menaces et propose des mesures de sécurité. L'évaluation de la vraisemblance doit donc être réalisée par la MOE.

La vraisemblance des menaces est estimée sur une échelle de 1 à 4 :

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