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.
GesVol est sous la responsabilité de l'UR TOTO. 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'importation des données des volontaires retenus
- L'utilisateur scientifique pourra corriger ponctuellement des données
- L'utilisateur scientifique responsable d'une étude sélectionnera et exportera les données d'un lot de volontaires pour l'expérimentation concernée

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.

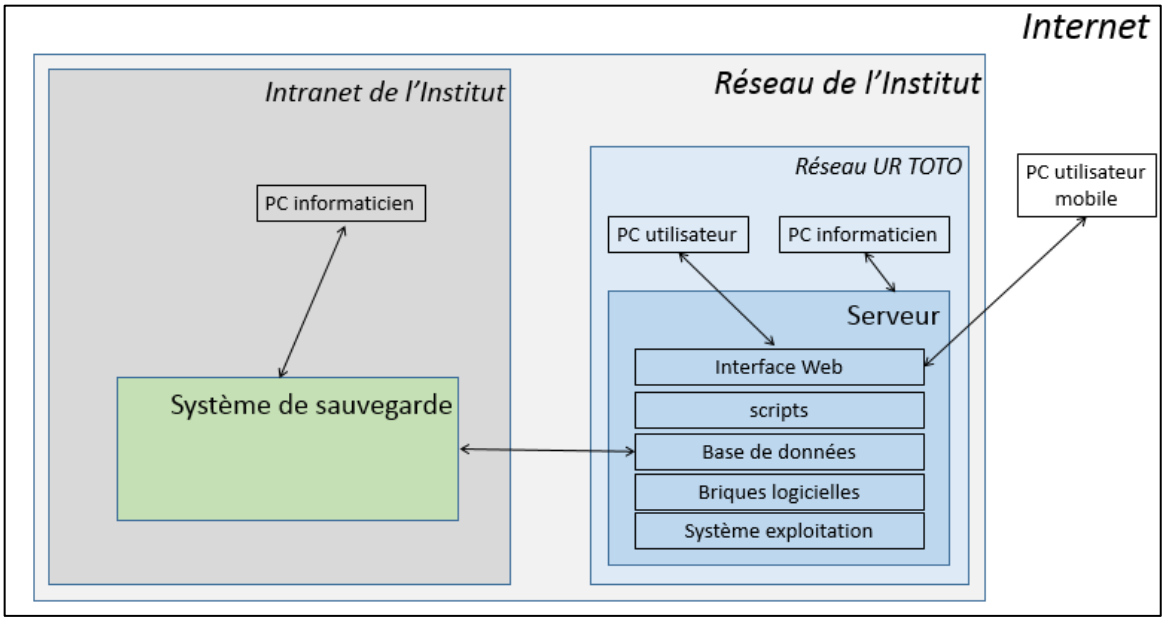
Données à protéger

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

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

Description du SI GesVol



Les éléments qui peuvent supporter (stocker) les données :

- Les postes de travail des administrateurs et des développeurs
- Les postes de travail des utilisateurs (scientifiques) 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 qui peuvent accéder aux données (en lecture et/ou en écriture) :
- Informaticiens (administrateurs et développeurs) de l'UR TOTO
- Les utilisateurs (scientifiques de l'UR TOTO)
- Les informaticiens administrateurs de la DSI (réseau et sauvegarde)

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

Mesure	Type	Description
Formation à GesVol	organisationnelle	Une formation est dispensée par les informaticiens à tous les nouveaux utilisateurs
Notice d'utilisation	organisationnelle	Une notice d'utilisation est disponible pour les utilisateurs (document Assurance Qualité Recherche)
Charte utilisateur GesVol	organisationnelle	Les utilisateurs doivent signer une charte d'utilisation décrivant leurs engagements. Les informaticiens s'assurent que tous les utilisateurs ont bien signé la charte GesVol
Création de compte	Logique	À l'issue de la formation, sont attribués aux utilisateurs un login et un mot de passe.
Procédure révocation de compte	Logique	Lorsqu'un utilisateur quitte l'unité, son compte est automatiquement révoqué
Sauvegarde	Logique	La BD est sauvegardée régulièrement par le service SV de la DSI de l'Institut
Environnement test-développement VS production	Logique	Les environnements de développement (PC des développeurs) et de production sont distincts (serveur)
Traçabilité	Logique	La traçabilité des accès au serveur est assurée via les logins de connexion ou les @IP des journaux des serveurs
Antivirus	Logique	L'antivirus est présent sur tous les PC de l'UR
Liaison serveur	Logique	Le serveur supportant GesVol est accessible depuis l'Internet, la liaison se fait avec chiffrement (https)
Serveur dans salle machine de l'UR	physique	Fermeture par badges du bâtiment de l'UR. La salle machine est protégée par un digicode.
Matériels de la DSI dans un Datacenter	physique	Les équipements de la DSI sont dans un Datacenter certifié ISO 27000

Évaluation des risques

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.

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.

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.

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 si exploitation d'un défaut de confidentialité, intégrité, disponibilité

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

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.