TP - L’analyse des risques du SI GesVol

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 …) puis 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

Hypothèse et périmètre du traitement GesVol

- 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

L’étude de risque SSI et l’EIVP de GesVol

- Le SI GesVol devra être conforme au RGPD et inscrit au registre de l’UR
- Une étude des risques SSI et IL est demandée au vu des DCP sensibles qui seront manipulées par ce SI et du nombre important de volontaires concernés par ce SI -> EIVP
- Une prestation est réalisée par la société TrucMuche afin d’évaluer si les mesures de sécurisation de GesVol sont adaptées à la sensibilité des données

L’exercice: jeu de rôle autour de l’analyse des risques

- 4 groupes de 10 personnes
- Par groupe :
  - 2 personnes de la société TrucMuche mènent les entretiens et restituent le rapport
  - 4 personnes sont la direction (DU, DU adjoint, scientifique …)
  - 4 personnes sont « l’informatique » (informaticiens UR, DSI …)
- La partie contexte du rapport est distribué et est déjà renseignée
- La partie évaluation du risque SSI et IL du rapport est à compléter. Le canevas est distribué.
- Les restitutions (tableaux d’évaluation et plan d’action) se feront sur les papers board

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

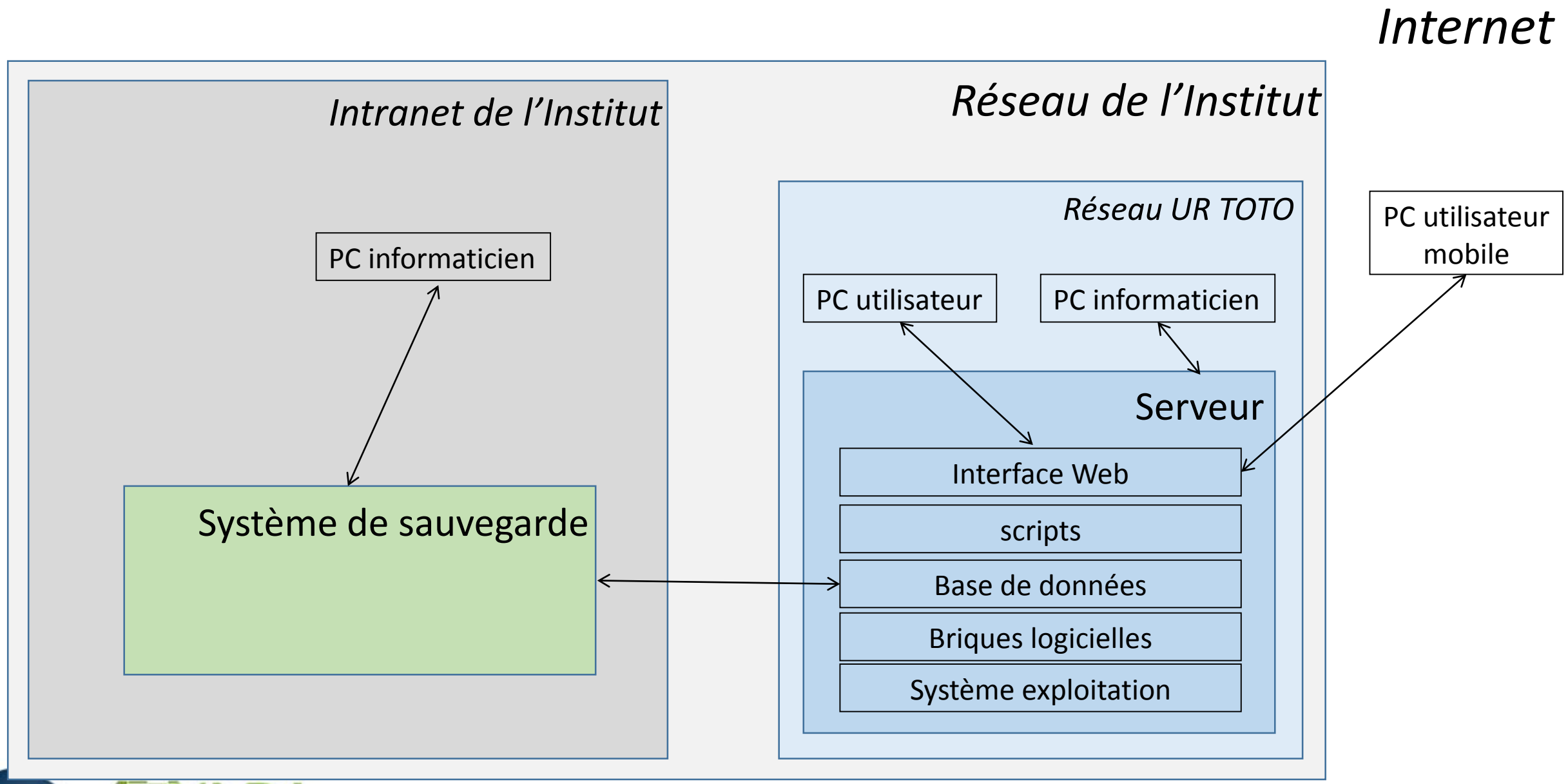
Les données d'état civil peuvent concerner des personnes dites vulnérables (ex : mineurs)

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)

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


Internet
Intranet de l'Institut
Réseau de l'Institut
Réseau UR TOTO
PC informaticien
PC utilisateur mobile
PC utilisateur
PC informaticien
Serveur
Interface Web
scripts
Base de données
Briques logicielles
Système exploitation
Système de sauvegarde

Précisions sur le SI

- 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

- Organisationnelle : Formation à GesVol, Notice d'utilisation, Charte utilisateur GesVol
- Logique : Création de compte, Procédure révocation de compte, Sauvegarde, Environnement test-développement VS production, Traçabilité, Antivirus
- physique : Serveur dans salle machine de l'UR, Matériels de la DSI dans un Datacenter

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

L’exercice: jeu de rôle autour de l’analyse des risques

Évaluation du risque SSI et IL à compléter …

L’exercice: jeu de rôle autour de l’analyse des risques

Restitution …