AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

RESULTATS DE L'ANALYSE DES RISQUES SSI

Modèle de présentation pour les MOA Territoriales

« ASIP Santé / Pôle Référentiels, Architecture et Sécurité »

Identification du document	
Référence	Outillage-Risques-SSI-V1.0.0
Date de création	19/11/09
Date de dernière mise à jour	08/07/10
Etat	Validé
Rédaction	ASIP Santé / PRAS
Version	V 1.0.0
Classification	Non sensible public
Nombre de pages	11

Historique du document			
Version	Date	Auteur	Commentaires
V 1.0.0	08/07/10	ASIP Santé / PRAS	Version pour publication

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard - 75015 Paris
T. + 33 (0)1 58 45 32 50
www.asipsante.fr
Agir ensemble pour soigner mieux

Sommaire

1 Objet du document

L'ASIP Santé souhaite répondre à l'un des enjeux majeurs identifiés pour la réussite des projets de partage de données de santé : « garantir la confiance des utilisateurs ». Pour ce faire, il a été demandé à chaque maîtrise d'ouvrage territoriale de fournir les résultats de l'analyse des risques SSI pour les systèmes d'information sous sa responsabilité.

Le présent document a pour objet de proposer un modèle de restitution des résultats de cette analyse et de structurer leur présentation.

Le choix de la méthode utilisée pour cette analyse des risques SSI reste de la libre initiative de la maîtrise d'ouvrage territoriale.

Pour autant, l'ASIP Santé souhaitant recommander aux maîtrises d'ouvrage l'utilisation des outils méthodologiques gouvernementaux, la méthode EBIOS [1] publiée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI [2]) est préconisée.

Les informations renseignées en italique dans la suite du document sont données à titre d'exemple ou d'illustration.

[1] Expression des Besoins et Identification des Objectifs de Sécurité.

[2] http://www.ssi.gouv.fr, rubrique Publication.

2 Présentation des résultats de l'analyse

2.1 Méthodologie d'analyse de risques utilisée

Le tableau ci-après identifie la méthodologie utilisée pour l'analyse de risques SSI du système.

Nom de la méthode	Editeur/Promoteur	Référence documentaire
EBIOS	*Agence Nationale de la Sécurité des Systèmes d'Information*	*http://www.ssi.gouv.fr rubrique Publication.*

2.2 Périmètre du système-cible de l'analyse

Le tableau ci-après présente de manière synthétique le périmètre fonctionnel du système pris en compte dans le cadre de cette analyse de risques SSI.

Périmètre du système d'information considéré	*Description macroscopique des principales fonctions du système et inventaires des catégories d'informations manipulées*
Enjeux et finalités	*Description des bénéfices attendus de la mise en œuvre du système-cible, en particulier en réponse aux attentes du promoteur et des utilisateurs.*

2.3 Expression des besoins de sécurité

Le tableau ci-dessous présente pour les fonctions et les informations les plus sensibles une évaluation de l'impact d'une perte totale ou partielle pour chacun des critères DICA [3].

Evènement redouté DICA	Fonction / Informations	Impact
Perte de Disponibilité	*Fonction de téléconsultation.*	*Perte de chance pour les patients.*
Perte d'Intégrité	*Informations médicales contenues dans les dossiers patient.*	*Erreur de diagnostic.* *Perte de chance pour les patients.*
Perte de Confidentialité	*Fonction d'accès aux dossiers des patients.*	*Atteinte à la vie privée, non respect des obligations légales et réglementaires.*
Perte Auditabilité	*Fonction d'archivage de l'historique des accès aux dossiers des patients.*	*Impossibilité de fournir des éléments de preuves lors d'un contentieux.*

[3] Une proposition de définition pour les critères de sécurité DICA (Disponibilité, Intégrité, Confidentialité, Auditabilité) est fournie en annexe.

2.4 Inventaire des types de menace considérés

Le tableau ci-après présente la liste exhaustive des types de menaces issue de la méthodologie utilisée [4], est détermine pour chaque type de menace s'il a été retenu dans l'analyse. Dans le cas où un type de menace n'a pas été retenu, ce choix doit être justifié.

Libellé type de menace	**Description du type de menace**	**Retenu Oui / Non**	*Si Non retenu* **Eléments de justification**
27 - GÉOLOCALISATION	*Localisation géographique d'une personne à son insu, à partir des informations contenues dans le système*	*Non*	*Pas d'information manipulée par le système qui permettrait une géolocalisation.*
42 - ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL	*Indisponibilité du personnel d'exploitation ou d'administration ou impossibilité pour celui-ci d'accéder au système effectuer les actions nécessaires (exemples : pandémie, évacuation d'un site, mouvement social)*	*Oui*	*Sans objet*

[4] Le référentiel des types de menace EBIOS est fourni à titre d'illustration en annexe.

2.5 Présentation des risques pesant sur le système

2.5.1 Inventaire exhaustif des risques SSI

Le tableau présente les caractéristiques des risques SSI identifiés en appliquant la méthodologie d'analyse mise en œuvre sur le périmètre du système-cible. Les impacts sur le système de la réalisation des risques sont exprimés suivants les critères traditionnels DICA.

Libellé du risque	**Description détaillée du scénario du risque**	**Impact**				**Mesures de couverture du risque mise en œuvre**	*Si risque partiellement couvert* **Eléments justifiant l'acceptation du risque résiduel**
		D	**I**	**C**	**A**		
Arrêt du système par manque de personnel	*A la suite d'une pandémie, le personnel d'exploitation ou d'administration est indisponible pour effectuer les actions nécessaires pour maintenir le système en fonctionnement.* *Type de menace prise en compte :* *42 - ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL*	*X*				***Sensibilisation du personnel aux mesures d'hygiène.*** ***Fourniture de solution hydro-alcoolique.*** ***Plan de continuité d'activité prenant en compte la gestion des ressources humaines.***	***Le risque ne peut être totalement couvert.*** ***Le risque résiduel est accepté par la MOA au regard des dispositions prises pour garantir la continuité des fonctions vitales du système.***

2.5.2 Synthèse des risques résiduels

Exposé synthétique des risques résiduels acceptés par la MOA.

Ces risques résiduels pourront être présentés en les regroupant par critère D, I, C, A impacté.

3 Annexes

3.1 Les critères de sécurité

Disponibilité, Intégrité, Confidentialité et Auditabilité

Une proposition de définition des critères Disponibilité, Intégrité, Confidentialité et Auditabilité est présentée ci-dessous :

Sigle	Critère	Définition
D	**Disponibilité**	Propriété d'accessibilité en temps utile d'un élément essentiel, par les utilisateurs autorisés. Pour une fonction : garantie de la continuité du service offert ; respect des temps de réponse attendus. Pour une information : garantie de l'accès aux données dans les conditions prévues de délai ou d'horaire.
I	**Intégrité**	Propriété d'exactitude et de complétude d'un élément essentiel. Pour une fonction : assurance de conformité de l'algorithme ou de la mise en œuvre des traitements, automatisés ou non, par rapport aux spécifications ; garantie de production de résultats corrects et complets par la fonction (sous réserve d'informations correctes et complètes en entrée). Pour une information : garantie d'exactitude et d'exhaustivité des données vis-à-vis d'erreurs de manipulation, de phénomènes accidentels ou d'usages non autorisés ; non-altération de l'information.
C	**Confidentialité**	Propriété d'un élément essentiel de ne pouvoir être connu que des utilisateurs autorisés. Pour une fonction : protection des algorithmes décrivant les règles de gestion et les résultats dont la divulgation à un tiers non autorisé porterait préjudice ; absence de divulgation d'un traitement ou mécanisme à caractère confidentiel. Pour une information : protection des données dont la connaissance par des tiers non autorisés porterait préjudice ; absence de divulgation de données à caractère confidentiel.
A	**Auditabilité**	Propriété d'un élément essentiel permettant de retrouver, avec une confiance suffisante, les circonstances dans lesquelles cet élément évolue. Pour une fonction : capacité à déterminer la personne ou le processus automatisé à l'origine de la demande de traitement et à déterminer les autres circonstances utiles associées à cette demande. Pour une information : capacité à déterminer la personne ou le processus automatisé à l'origine de l'accès à l'information et à déterminer les autres circonstances utiles associées à cet accès.

3.2 Les types de menace EBIOS (extrait de la méthode EBIOS)

Type de menace référentiel EBIOS
01- INCENDIE Destruction ou altération de ressources techniques, de supports de stockage, de documents ou de locaux du système, liée à un incendie dans ou à proximité des locaux du système
02- DÉGÂTS DES EAUX Destruction ou altération de ressources techniques, de supports de stockage, de documents ou de locaux du système, liée à des infiltrations ou des écoulements d'eau dans ou à proximité des locaux du système
03 – POLLUTION Propagation, dans ou proximité du site d'une plate-forme, d'une pollution chimique, nucléaire ou biologique, de fumées ou de poussières conduisant à endommager ou à rendre inaccessible une plate-forme du système
04 - SINISTRE MAJEUR Dommages physiques occasionnés à une plate-forme du système ou à son environnement, par un phénomène majeur naturel, un accident industriel ou un acte volontaire survenu à proximité du site de la plate-forme
05 - DESTRUCTION DE MATÉRIELS OU DE SUPPORTS Destruction ou altération d'un équipement ou d'un support de stockage d'une plate-forme du système, due à un accident ou une négligence ou encore à un acte délibéré, par une personne ayant accès à cet élément
06 - PHÉNOMÈNE CLIMATIQUE Perturbation du fonctionnement d'une plate-forme ou altération des éléments stockés en raison de conditions climatiques dépassant la limite des caractéristiques de fonctionnement ou de stockage des ressources Techniques. Le site est placé dans une zone géographiquement sensible à des conditions climatiques extrêmes
07 - PHÉNOMÈNE SISMIQUE Dommages physiques occasionnés à une plate-forme du système ou à son environnement, par un phénomène sismique
08 - PHÉNOMÈNE VOLCANIQUE Dommages physiques occasionnés à une plate-forme du système ou à son environnement, par un phénomène volcanique
09 - PHÉNOMÈNE MÉTÉOROLOGIQUE Dommages physiques d'une plate-forme du système ou de son environnement ou perturbations de fonctionnement, occasionnées par un phénomène météorologique d'ampleur inhabituelle (foudre, pluie, neige, vent)
10 – CRUE Inondation des locaux d'une plate-forme, de ceux de stockage de supports, de documents ou de d'équipements, de ceux d'exploitation, de ceux d'alimentation électrique ou de télécommunication, ou inondation à proximité empêchant l'accès physique du personnel d'exploitation
11 - DÉFAILLANCE DE LA CLIMATISATION Arrêt ou dysfonctionnement de la climatisation dans les locaux d'une plate-forme, de ceux de stockage de supports, de documents ou de d'équipements, suite à une panne ou un acte volontaire
12 - PERTE D'ALIMENTATION ÉNERGÉTIQUE Surtensions, perturbations ou arrêt de l'alimentation électrique d'une plate-forme du système
13 - PERTE DES MOYENS DE TÉLÉCOMMUNICATION Incident rendant indisponibles les moyens de télécommunication nécessaires au fonctionnement du système ou à son utilisation
14 - RAYONNEMENTS ÉLECTROMAGNÉTIQUES Perturbation du fonctionnement d'équipements d'une plate-forme du système ou des communications, en raison d'incompatibilités électromagnétiques entre équipements ou à cause d'une source de rayonnement à proximité

Type de menace référentiel EBIOS
15 - RAYONNEMENTS THERMIQUES Effet thermique provoqué par un sinistre ou des conditions météorologiques exceptionnelles (incendie de forêt), Engin provoquant un effet thermique entrainant un dysfonctionnement ou une destruction des matériels (déchets nucléaires, explosion thermo nucléaire)
16 - IMPULSIONS ÉLECTROMAGNÉTIQUES Destruction ou altération des équipements d'une plateforme du système ou de ses servitudes (alimentation électrique, climatisation, télécommunications), à la suite d'une impulsion électromagnétique d'origine nucléaire ou industrielle à proximité du site
17 - INTERCEPTION DE SIGNAUX PARASITES COMPROMETTANTS Capture et exploitation de signaux conduits ou émis par les équipements, signaux pouvant être porteurs d'informations confidentielles
18 - ESPIONNAGE A DISTANCE Observation des activités d'exploitation ou d'administration du système par des personnes non autorisées (visiteurs, caméras cachées, observateurs par des fenêtres)
19 - ÉCOUTE PASSIVE Au niveau des réseaux ou des supports de communication utilisés, interception des échanges entre un utilisateur et le système, entre deux plates-formes du système, entre deux équipements d'une même plate-forme
20 - VOL DE SUPPORTS OU DE DOCUMENTS Vol de documents du système, vol ou substitution d'un support de stockage d'informations dans un site du système, dans un site de stockage (sauvegarde par exemple) lors d'un transport de support; ou lors de la restitution partielle ou totale du dossier sur support papier ou support informatique
21 - VOL DE MATÉRIELS Vol ou substitution d'équipements dans les locaux d'une plate-forme, ou dans ceux de stockage, ou à la faveur de la maintenance ou de transport de ces équipements, avec capture éventuelle de données résiduelles
22 – RECUPERATION DE SUPPORTS RECYCLES OU MIS AU REBUT Exploitation de données résiduelles sur les supports de stockage ou les équipements retirés du système avant réemploi par ailleurs ou mise au rebut
23 – DIVULGATION Personne interne à l'organisme qui, par négligence diffuse de l'information à d'autres personnes de l'organisme n'ayant pas le besoin d'en connaître, ou à l'extérieur. Personne diffusant consciemment de l'information à d'autres personnes de l'organisme n'ayant pas le besoin d'en connaître, ou à l'extérieur.
24 - INFORMATIONS SANS GARANTIE DE L'ORIGINE Réception et exploitation dans le système d'information de l'organisme de données externes ou de matériels non adaptés provenant de sources extérieures. Personne transmettant des informations fausses, destinées à être intégrées au système d'information, pour désinformer le destinataire et porter atteinte à la fiabilité du système ou la validité des informations.
25 - PIÉGEAGE DU MATÉRIEL Implantation de fonctionnalités illicites dans un équipement ou une plate-forme du système, en vue de provoquer des dysfonctionnements ou des détournements d'information
26 - PIÉGEAGE DU LOGICIEL Implantation et activation de fonctions illicites (cheval de Troie, bombe logique, virus, keylogger...) dans les logiciels du système ou propagation de telles fonctions à partir des dispositifs d'accès des utilisateurs ou des postes de travail des autres accédants
27 - GÉOLOCALISATION Localisation géographique d'une personne à son insu, à partir des informations contenues dans le système
28 - PANNE MATÉRIELLE Panne d'un matériel du système, entraînant la dégradation de service ou l'indisponibilité du système
29 - DYSFONCTIONNEMENT DU MATÉRIEL Dysfonctionnement d'un matériel du système, entraînant la dégradation de service ou l'indisponibilité du système

Type de menace référentiel EBIOS
30 - SATURATION DU SYSTÈME INFORMATIQUE Saturation des équipements du système liée à un défaut de capacité ou de conception ou à une sollicitation anormale du système (attaque de type déni de service par exemple)
31 - DYSFONCTIONNEMENT LOGICIEL Fonctionnement non conforme du logiciel du système, résultant d'un défaut de réalisation, d'installation, de maintenance ou d'exploitation
32 - ATTEINTE À LA MAINTENABILITÉ DU SYSTÈME D'INFORMATION Impossibilité ou difficulté à assurer le maintien en condition opérationnelle du système, du fait de défauts de conception du système, d'insuffisances du dispositif de soutien, de défaillances de fournisseurs, d'obsolescence de ressources techniques
33 - UTILISATION ILLICITE DES MATÉRIELS Accès à un équipement du système par une personne non autorisée et utilisation de cet équipement pour accéder aux fonctions ou aux données du système
34 - COPIE FRAUDULEUSE DE LOGICIELS Copie de logiciels du système en vue de leur utilisation par ailleurs
35 - UTILISATION DE LOGICIELS CONTREFAITS OU COPIÉS Mise en oeuvre dans le système de logiciels dont les droits d'utilisation ou d'exploitation sont insuffisants
36 - ALTÉRATION DES DONNÉES Modification/altération des données échangées entre les équipements ou les plates-formes du système ou entre le système et les dispositifs d'accès des utilisateurs (menace de type Man in the middle), ou modification/altération des données sur les supports de stockage (voire substitution de support) ou dans les équipements du système
37 - TRAITEMENT ILLICITE DES DONNÉES Utilisation des données de santé ou des données personnelles à d'autres fins que celles autorisées par la législation ou un règlement
38 - ERREUR D'UTILISATION Erreur d'exploitation ou d'intervention, erreur d'utilisation.
39 - ABUS DE DROIT Utilisation ou exploitation du système par une personne autorisée, dans but malintentionné (exemples : pour un administrateur ou un exploitant : accord de droits d'administration ou d'exploitation à des personnes non habilitées, rapprochement de données ; pour un PS : accès selon un mode techniquement utilisable mais en dehors du contexte légitime d'emploi)
40 - USURPATION DE DROIT Usurpation de l'identité ou des droits d'accès d'une personne autorisée, par une personne malintentionnée
41 – RENIEMENT D'ACTIONS Contestation, par une personne autorisée, des actions effectuées sur le système ou ses informations
42 - ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL Indisponibilité du personnel d'exploitation ou d'administration ou impossibilité pour celui-ci d'accéder au système effectuer les actions nécessaires (exemples : pandémie, évacuation d'un site, mouvement social)