SICTIAM

F.E.R.O.S. STELA

Fiche d'Expression Rationnelle des Objectifs de Sécurité

CONTROLE DE LEGALITE DEMATERIALISE

Plateforme STELA

VERSION 1.0

FART STELA

CONTROLE DE LEGALITE DEMATERIALISE
Plateforme STELA

REFERENCE	DATE
FEROS STELA_Contrôle de légalité dématérialisé V 1.0	**20/09/2011**
Identification d'objet (OID)	**Racine OID et gestionnaire**
	SICTIAM/service DEMAT
RESPONSABLE	**VERSION**
SICTIAM/P.PINTARIC	**V 1.0**
Critère de diffusion	**Nombre de pages**
Public	39

HISTORIQUE DES VERSIONS

DATE	Rédacteur	Version	Evolution du document et observations
06/09/2010	Francis KUHN	0.1	Mise en place du document
06/09/2010	Pierre PINTARIC	0.2	Utilisation du style, gestion des versions, de la date du document et création du schéma fonctionnel STELA ACTES
07/09/2010	Francis KUHN	0.3	Rajout d'éléments descriptifs Fonctions, Informations, Enjeux et Hypothèses dans les chapitres 2.2, 2.3 et 2.4
07/09/2010	Pierre PINTARIC	0.4	Ajout du schéma logique et des fonctions manquantes
08/09/2010	Francis	0.5	Modifications schémas et ajouts

	KUHN/Pierre PINTARIC		
10/09/2010	Pierre PINTARIC	0.6	Mise à jour du schéma fonctionnel, description des fonctions et informations. Réalisation du tableau sur l'échelle des besoins
04/10/2010	Pierre PINTARIC / Francis KUHN / Jean-Marc RIETSCH	0.7	Utilisation de la nouvelle version EBIOS
21/10/2010	Pierre PINTARIC / Francis KUHN / Jean-Marc RIETSCH / Florence ESSELIN / Hugues DE LOISY	0.8	Complément du document avec la base du module 2
25/10/2010	Pierre PINTARIC	0.9	- Modification de la mise en page - Modification du schéma fonctionnel et complément des descriptions - Tableau es biens identifiés - Liens entre biens essentiels et biens supports - Mesures de sécurités existantes sur les biens supports
27/102010	Florence ESSELIN	0.10	- Ajout des tableaux de types de menaces/vulnérabilités - Ajout du tableau de scénarios de menaces - Déplacement du tableau des biens supports à l'étape d'étude des menaces
12/11/2010	Pierre PINTARIC	0.11	- Mise en annexe de la description des fonctions de biens essentiels - Mise en forme des derniers ajouts - Complément du type de menaces/vulnérabilités - Complément du tableau des scénarios de menaces

02/05/2011	Pierre PINTARIC / Florence ESSELIN / Hugues DE LOISY	0.12	Simplification en réduisant le périmètre de l'étude STELA comme un tout macroscopique, sans entrer dans le détail du fonctionnement et en factorisant des fonctions dans le cadre d'études autres (comme la salle serveurs, les serveurs, …) Finalisation des éléments suivants la méthode eBios
24/05/2011	Pierre PINTARIC	0.13	• Renommage de la fiche en FEROS • Complément du tableau 4.1 avec la colonne scénarios • Ajout d'exemples pour chacun des scenarios • Complément du tableau 4.2 • Ajout d'un chapitre sur les mesures à prendre et le résultat sur les évaluations de scénarios
20/09/2011	Francis KUHN / Pierre PINTARIC	1.0	• Finalisation du document

SOMMAIRE

1 INTRODUCTION

1.1 CONTEXTE GENERAL

Le SICTIAM, Syndicat Intercommunal des Collectivités Territoriales Informatisées Alpes Méditerranée, est un syndicat mixte ouvert, offrant à ses adhérents des services dans le domaine de l'informatique et des systèmes d'information en général.

A ce titre, l'établissement a souhaité s'engager dans une offre de services couvrant peu à peu tous les domaines de la dématérialisation, et ce, afin de favoriser les échanges dématérialisés avec l'Etat, mais aussi avec le citoyen et d'autres organismes. Ces procédures ont pour objectif d'améliorer la qualité des services et la productivité de l'administration.

La mise en place de relations dématérialisées avec les usagers - citoyens - administrations - autres organismes, nécessite un climat de confiance entre tous les acteurs. C'est pourquoi, le SICTIAM a souhaité prendre en compte, non seulement les normes règlementaires quand elles existent, mais aussi le cadre général de sécurisation des systèmes d'information que représente le RGS (Référentiel Général de Sécurité), créé par l'article 9 de l'ordonnance du 8 décembre 2005, et destiné à fournir aux autorités administratives les clés de compréhension et de mise en œuvre de télé-services véritablement fiables et sécurisés ; ses conditions d'élaboration, d'approbation, de modification et de publication ont été fixées par le décret n°2010-112 du 2 février 2010 et il a été approuvé par arrêté du Premier Ministre le 6 mai 2010.

1.2 LA PLATEFORME STELA

La plateforme STELA a été développée par les services du SICTIAM et placée sous licence libre CREATIVE COMMONS.

Son agrément a été obtenu après intervention du CESTI désigné par le Ministère de l'Intérieur et vérification du respect de l'ensemble des prescriptions édictées par la norme ACTES en mars 2007.

Les composantes de la norme d'échange, définie par le ministère en concertation avec ses partenaires, sont les suivantes :

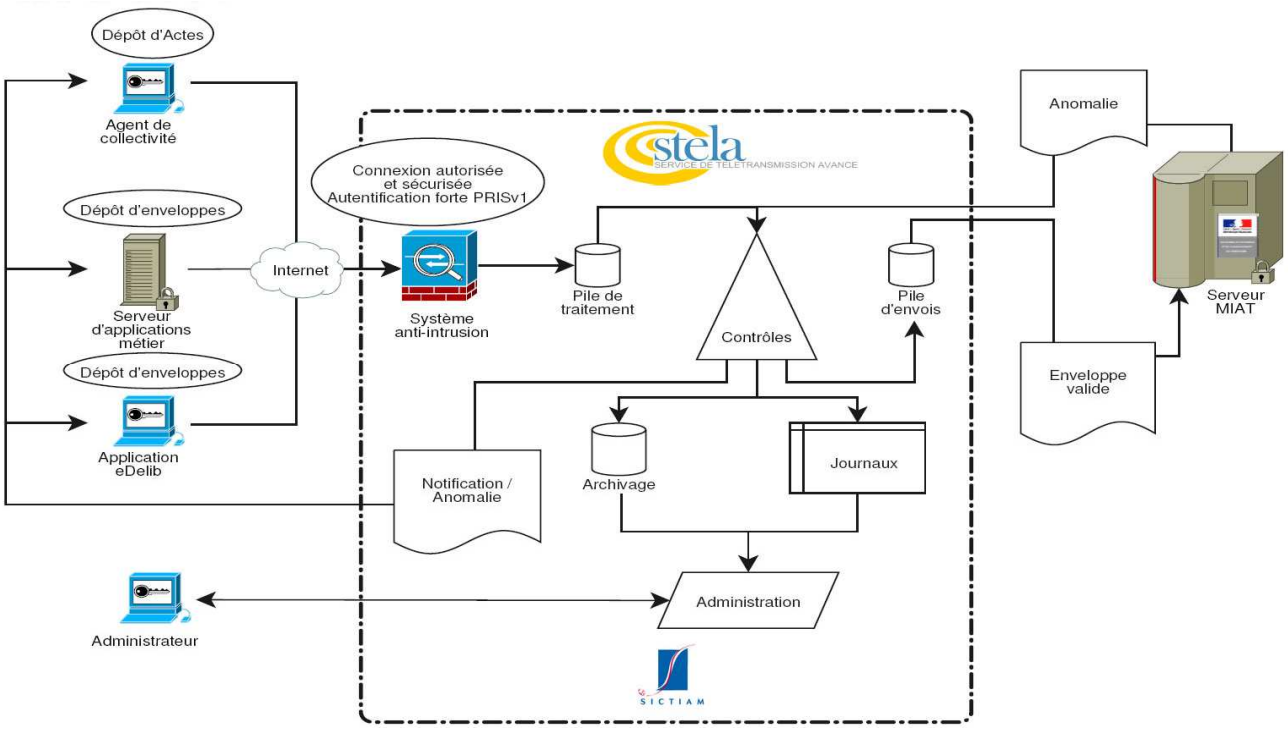
- Modélisation des données métier échangées véhiculées par les flux dématérialisés, générées et traitées par des systèmes automatisés mis à disposition des collectivités et des préfectures
- Format de fichiers échangés
- Organisation des fichiers transmis lors d'une télétransmission, et lien entre ces fichiers
- Règles de nommage des fichiers échangés
- Protocoles techniques utilisés pour la transmission des fichiers

Cette norme est complétée par les informations concernant la sécurisation de ces échanges. Ces informations font l'objet de l'annexe 1 du cahier des charges,

La sécurisation de la télétransmission vise deux objectifs :
- Authentification réciproque : s'assurer qu'une transmission vient bien de celui qui dit l'avoir envoyée, et qu'elle a bien été remise à son destinataire et non à un usurpateur,
- Intégrité : s'assurer que le fichier transmis n'a pas été altéré lors du transfert.

Le dispositif prend également en compte la sécurisation des envois d'informations d'une collectivité à son dispositif de télétransmission, quand ces informations sont ensuite transmises à la sphère Etat.

Le schéma de fonctionnement homologué par le ministère de l'Intérieur est le suivant :



1.3 DEFINITION DES RESPONSABILITES

La présente fiche a été réalisée par le SICTIAM avec le soutien de l'A.N.S.S.I. qui a apporté son expertise technique, et avec le concours de l'association FEDISA, Fédération de l'ILM (Information Lifecycle Management), du Stockage et de l'Archivage, dont le SICTIAM fait partie.

2 ETUDE DES RISQUES

Cette étude a été réalisée à l'aide de la méthode EBIOS et est maintenue à jour par le Responsable SSI (Pierre PINTARIC) ; il s'agit d'un document de travail. En effet, son contenu est nécessaire à la réalisation de l'étude et à l'élaboration des différents livrables qui pourront être communiqués par la suite.

Les éléments tels que l'étude sur les accès à la salle serveurs, les serveurs, l'infrastructure du bâtiment feront l'objet d'études complémentaires.

2.1 LE CADRE DE LA GESTION DES RISQUES

L'objectif de l'étude : déterminer les risques SSI et les mesures adaptées pour réaliser l'homologation de STELA ACTES

Le plan d'action : voir la note de cadrage de l'autorité administrative

L'organisme étudié : Syndicat Intercommunal Mixte Ouvert
Voir Contexte Général (page 6)

Définition de la gestion des risques
La gestion du risque est définie comme l'analyse des événements redoutés par l'organisme sur son activité, ainsi que leurs conséquences, les menaces correspondantes et leurs probabilités d'occurrences.

En matière de gestion des risques, les rôles et responsabilités sont définis dans la note de cadrage référence.

2.2 SOURCES DE MENACES

Le SICTIAM souhaite s'opposer aux sources de menaces suivantes :

Types de sources de menaces	Exemple	Retenu ou non
Source humaine interne, malveillante, avec de faibles capacités	Collaborateur malveillant avec des possibilités d'action limitées sur le système d'information (personnel en fin de contrat ou voulant se venger de son employeur ou de ses collègues…), stagiaire agissant de manière ludique, utilisateur désirant obtenir des avantages, personnel d'entretien.	OUI
Source humaine interne, malveillante, avec des capacités importantes	Collaborateur malveillant avec d'importantes connaissances et possibilités d'action sur le système d'information (manager ambitieux en fin de contrat ou voulant se venger de son employeur ou de ses collègues, développeur agissant par ego ou de manière ludique, fraudeur…), prestataire, personnel de maintenance ou d'assistance à distance.	OUI
Source humaine interne, malveillante, avec des capacités illimitées	Collaborateur malveillant avec des connaissances et possibilités d'action illimitées sur le système d'information (administrateur système ou réseau agissant par vengeance,	OUI

Types de sources de menaces	Exemple	Retenu ou non
	dirigeant…).	
Source humaine externe, malveillante, avec de faibles capacités	Script-kiddies, vandale.	OUI
Source humaine externe, malveillante, avec des capacités importantes	Militant agissant de manière idéologique ou politique, pirate passionné, casseur ou fraudeur, ancien employé désirant se venger d'un licenciement, concurrent, groupement professionnel, organisation de lobbying, organisation non gouvernementale.	OUI
Source humaine externe, malveillante, avec des capacités illimitées	Organisation criminelle, agence gouvernementale ou organisation sous le contrôle d'un État étranger, espions, organisation terroriste.	NON
Source humaine interne, sans intention de nuire, avec de faibles capacités	Collaborateur maladroit ou inconscient avec des possibilités d'action limitées sur le système d'information, personnel à faible conscience d'engagement, peu sensibilisé ou peu motivé dans sa relation contractuelle avec l'organisme, personnel d'entretien maladroit, stagiaire, thésard, intérimaire, utilisateur, fournisseur, prestataire, sous-traitant.	OUI
Source humaine interne, sans intention de nuire, avec des capacités importantes	Collaborateur maladroit ou inconscient avec d'importantes connaissances et possibilités d'action sur le système d'information (manager, développeur…).	OUI
Source humaine interne, sans intention de nuire, avec des capacités illimitées	Collaborateur maladroit ou inconscient avec des connaissances et possibilités d'action illimitées sur le système d'information (administrateur système ou réseau, dirigeant…).	OUI

Types de sources de menaces	Exemple	Retenu ou non
Source humaine externe, sans intention de nuire, avec de faibles capacités	Entourage du personnel, personne réalisant des travaux dans le voisinage, manifestants, visiteur maladroit, forte ambiance sonore (perte de concentration).	OUI
Source (humaine ou non) externe, sans intention de nuire, avec des capacités importantes	Matériels émettant des ondes, des vibrations, activités industrielles dégageant des substances chimiques toxiques ou susceptibles de provoquer des sinistres mineurs, trafic routier ou aérien pouvant générer des accidents.	OUI
Source (humaine ou non) externe, sans intention de nuire, avec des capacités illimitées	Matériels émettant des radiations ou des impulsions électromagnétiques, activités industrielles susceptibles de provoquer des sinistres majeurs, explosion dans le voisinage. Cf plan de prévention	NON
Virus non ciblé	Virus informatique, code malveillant non ciblé, ou ciblé, mais d'origine inconnue.	OUI
Phénomène naturel	Cf plans de prévention	NON
Catastrophe naturelle ou sanitaire	Cf plans de prévention	NON
Activité animale	Présence d'animaux susceptibles de provoquer des dégâts aux infrastructures (rongeurs…), présence d'animaux dangereux pour l'homme.	NON
Événement interne	Présence de matières corrosives, combustion de matières inflammables, incendie des locaux, explosion de matières explosives, fuite de canalisation, accident de chantier, fuite de substances chimiques, réorganisation,	NON

Types de sources de menaces	Exemple	Retenu ou non
	changement d'architecture réseau, branchement d'un composant réseau ou d'une machine incompatible, travaux de réaménagement des locaux.	

2.3 METRIQUES UTILISEES

Les critères de sécurité retenus : disponibilité, intégrité, confidentialité et preuve/traçabilité
Afin d'exprimer les besoins de sécurité, les critères de sécurité retenus sont les suivants :

Critères de sécurité	Définitions
Disponibilité	Propriété d'accessibilité, au moment voulu, des biens essentiels.
Intégrité	Propriété d'exactitude et de complétude des biens essentiels.
Confidentialité	Propriété des biens essentiels dont l'accès doit être limité aux seuls utilisateurs autorisés.
Preuve/traçabilité	Propriété destinée à compléter l'intégrité

2.3.1 Échelle de disponibilité

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de disponibilité :

Niveaux de l'échelle	Description détaillée de l'échelle
1 semaine sur 30 jours	Le bien essentiel peut être indisponible 1 semaine sur 30 jours.
2 jours sur 30	Le bien essentiel ne doit pas être indisponible plus de 2 jours sur 30.
4h sur 30 jours	Le bien essentiel ne doit pas être indisponible plus de 4 heures sur 30 jours.
1 minute sur 30 jours	Le bien essentiel ne doit pas être indisponible plus d'1 minute sur 30 jours.

2.3.2 Échelle d'intégrité

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes d'intégrité :

Niveaux de l'échelle	Description détaillée de l'échelle
Non géré	L'absence d'intégrité n'a aucun impact sur le bien essentiel
Détectable	Le bien essentiel peut ne pas être intègre si l'altération est identifiée.
Maîtrisé	Le bien essentiel peut ne pas être intègre, si l'altération est identifiée et l'intégrité du bien essentiel retrouvée.
Intègre	Le bien essentiel doit être rigoureusement intègre.

2.3.3 Échelle de confidentialité

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de confidentialité :

Niveaux de l'échelle	Description détaillée de l'échelle
Public	Le bien essentiel est public.
Limité	Le bien essentiel ne doit être accessible qu'au personnel et aux partenaires.
Réservé	Le bien essentiel ne doit être accessible qu'au personnel (interne) impliqué.
Privé	Le bien essentiel ne doit être accessible qu'à des personnes identifiées et ayant le besoin d'en connaître.

2.3.4 Échelle de traçabilité

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de traçabilité :

Niveaux de l'échelle	Description détaillée de l'échelle
Faible	Enregistrement des adresses IP des personnes qui se connectent au dispositif
Standard	Un historique des utilisateurs connectés est conservé.
Fort	Un historique des utilisateurs connectés et des informations échangées est conservé, y compris s'agissant des serveurs.

Opposable	La journalisation des échanges est conservée dans des conditions d'opposabilité vis à vis des acteurs concernés et des tiers.

2.3.5 Échelle de gravité

L'échelle suivante sera utilisée pour estimer la gravité des événements redoutés et des risques :

Niveaux de l'échelle	Description détaillée de l'échelle
Négligeable	l'organisme surmontera les impacts sans aucune difficulté.
Limitée	l'organisme surmontera les impacts malgré quelques difficultés.
Importante	l'organisme surmontera les impacts avec de sérieuses difficultés.
Critique	l'organisme ne surmontera pas les impacts (sa survie est menacée).

2.3.6 Échelle de vraisemblance

L'échelle suivante sera utilisée pour estimer la vraisemblance des scénarios de menaces et des risques :

Niveaux de l'échelle	Description détaillée de l'échelle
Minime	Cela ne devrait pas se (re)produire.
Significative	Cela pourrait se (re)produire.
Forte	Cela devrait se (re)produire un jour ou l'autre.
Maximale	Cela va certainement se (re)produire prochainement.

2.3.7 Critères de gestion des risques : la liste des règles à utiliser dans l'étude

Les critères de gestion des risques retenus sont les suivants :

Action	Critère de gestion des risques (règle choisie pour réaliser l'action)
Expression des besoins (module 2)	• Les besoins de sécurité des biens essentiels sont exprimés à l'aide des échelles correspondantes, selon le critère de sécurité étudié.

Action	Critère de gestion des risques (règle choisie pour réaliser l'action)
Estimation des événements redoutés (module 2)	• Les événements redoutés sont estimés en termes de gravité à l'aide de l'échelle définie à cet effet.
Évaluation des événements redoutés (module 2)	• Les événements redoutés sont classés par ordre décroissant de vraisemblance.
Estimation des scénarios de menaces (module 3)	• Les scénarios de menaces sont estimés en termes de vraisemblance à l'aide de l'échelle définie à cet effet.
Évaluation des scénarios de menaces (module 3)	• Les scénarios de menaces sont classés par ordre décroissant de vraisemblance.
Estimation des risques (module 4)	• La gravité d'un risque est égale à celle de l'événement redouté considéré. • La vraisemblance d'un risque est égale à la vraisemblance maximale de tous les scénarios de menaces liés à l'événement redouté considéré.
Évaluation des risques (module 4)	• Les risques dont la gravité est critique, et ceux dont la gravité est importante et la vraisemblance forte ou maximale, sont jugés comme intolérables. • Les risques dont la gravité est importante et la vraisemblance significative, et ceux dont la gravité est limitée et la vraisemblance forte ou maximale, sont jugés comme significatifs. • Les autres risques sont jugés comme négligeables.
Choix de traitement des risques (module 4)	• Les risques intolérables doivent être réduits à un niveau acceptable ou transférés, voire évités si cela est possible. • Les risques significatifs devraient être réduits, transférés ou évités. • Les risques négligeables peuvent être pris.
Homologation de sécurité (module 5)	• Le traitement des risques ne peut être validé que s'il est démontré que les risques résiduels sont acceptables et que les mesures de sécurité destinées à traiter les risques peuvent être mises en œuvre dans un délai raisonnable.

2.3.8 Biens essentiels

Les processus sont des fonctions qui traitent des informations essentielles en entrée et en sortie. Les informations sont les messages échangés entre les processus.

2 biens essentiels ont été énumérés :

- STELA ACTES : fonction permettant de transmettre les éléments entre les collectivités et les services des ministères. STELA ACTES est un tiers de télétransmission ayant comme fonction la télé-transmission des éléments
- Authentification : fonction permettant aux utilisateurs de s'authentifier

2.4 ECHELLE DE BESOINS

	Confidentialité	Disponibilité	Intégrité	Traçabilité
1	Informations publiques	Une indisponibilité d'une semaine sur 30 jours ne provoque aucune perturbation au niveau du système d'information	La perte d'intégrité n'entraine aucune gêne	La traçabilité se résume à un enregistrement des adresses IP des personnes qui se connectent au dispositif
2	Informations personnelles, mais dont la divulgation n'engendre aucune conséquence	Une indisponibilité de 2 jours sur 30 de l'application ou de la ressource est tolérable	Une perte d'intégrité est dommageable, mais les conséquences restent restreintes	Un historique des utilisateurs connectés est conservé
3	Informations confidentielles ne devant pas être divulguées. une perte de confidentialité est grave, mais n'entraine que des conséquences au niveau médiatique, mais pas au niveau économique ou juridique	Une indisponibilité de 4 heures sur 30 jours de l'application ou de la ressource est tolérable	Une perte d'intégrité des informations est grave, mais ne touche qu'un nombre limité d'usagers. Les conséquences restent donc restreintes	Un historique des utilisateurs connectés et des informations échangées est conservé, y compris s'agissant des serveurs
4	Informations confidentielles ne devant pas être divulguées. une perte de	Une indisponibilité d'1 minute sur 30 jours a une incidence grave au niveau financier	Une perte d'intégrité des informations ou des fonctions est très grave et impacte le fonctionnement global	La journalisation des échanges est conservée dans des conditions d'opposabilité vis à

	confidentialité a des conséquences sur le plan médiatique, et/ou financier et/ou juridique	et/ou en terme d'image de marque et/ou sur le plan juridique	de la téléprocédure. Elle entraine une perte importante au niveau financier et/ou de l'image de marque et peut avoir des conséquences juridiques	vis des acteurs concernés et des tiers

2.5 BESOINS DE SECURITE DES ELEMENTS ESSENTIELS

		Besoin de sécurité	Commentaires
F.AUTHENTIFICATION	Confidentialité	1	La perte de confidentialité des identifiants des utilisateurs n'entraîne aucun impact au niveau de la plate-forme, car l'authentification est assurée par un certificat SSL physique.
	Disponibilité	2	La perte de disponibilité de l'authentification empêche tout utilisateur d'accéder au service, 4h sur 30 jours d'indisponibilité est le maximum acceptable
	Intégrité	3	Si la fonction d'authentification perd son intégrité, tous les utilisateurs de la plate-forme seront impactés et de ce fait personne ne pourra s'authentifier
F.ACTES	Confidentialité	1	La divulgation des données n'entraine aucune conséquence sachant que les données sont publiques une fois que l'accusé de réception est envoyé par le Ministère.
	Disponibilité	2	La perte de disponibilité du système empêche tout élément d'être déposé, consulté ou transmis, 4h sur 30 jours d'indisponibilité est le maximum acceptable
	Intégrité	3	Les données font foi et peuvent servir de preuve juridique. L'intégrité est primordiale

2.6 BIENS IDENTIFIES

Les processus sont des fonctions qui traitent des informations essentielles en entrée et en sortie.
Les processus suivants ont été déterminés comme essentiels :

Processus métiers	Processus essentiels	Informations essentielles concernées	Service concerné
STELA ACTES	**F.AUTHENTIFICATION**	• I.PROFIL • I.ACCREDITATIONS	SICTIAM/DEMAT
	F.ACTES	• I.ENVELOPPE • I.FICHIER • I.ACCREDITATIONS • I.META DONNEES	SICTIAM/DEMAT

3 ETUDE DES EVENEMENTS REDOUTES

3.1 LES EVENEMENTS REDOUTES

Chaque ligne du tableau suivant représente un événement redouté par l'organisme ; un événement redouté est la combinaison d'un bien essentiel, d'un critère de sécurité, d'un besoin de sécurité selon les échelles de besoin, sources de menaces et impacts. La gravité de chaque évènement redouté est estimée (cf. échelle de gravité) sans tenir compte des mesures de sécurité existantes.

Evénement redouté	Processus essentiel	Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
ER1	F.AUTHENTIFICATION	La fonction Authentification est indisponible	D=2	Interne malveillant capacités illimitées ; Interne sans intention de nuire capacités illimitées ; Externe malveillant capacités importantes ; Code malveillant	Image de marque	2. Limité

Evénement redouté	Processus essentiel	Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
ER2	F.AUTHENTIFICATION	Les identifiants des utilisateurs ont été altérés ou sont corrompus.	I=3	Interne malveillant capacités illimitées ; Interne sans intention de nuire capacités illimitées ; Externe malveillant capacités importantes ; Code malveillant	Image de marque	2. Limité
ER3	F.AUTHENTIFICATION	Les identifiants des utilisateurs ont été divulgués	C=2	Interne malveillant capacités illimitées ; Interne sans intention de nuire capacités illimitées ; Externe malveillant capacités importantes ; Code malveillant	Image de marque	3. Important
ER4	F.ACTES	Le service n'est plus accessible	D=2	Interne malveillant capacités illimitées ; Interne sans intention de nuire capacités illimitées ; Externe malveillant capacités importantes ; Code malveillant	Image de marque	2. Limité

Evénement redouté	Processus essentiel	Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
ER5	F.ACTES	Les données des actes ne sont plus intègres	I=3	Interne malveillant capacités illimitées ; Interne sans intention de nuire capacités illimitées ; Externe malveillant capacités importantes ; Code malveillant	Image de marque ; Juridique	3. Important
ER6	F.ACTES	Le contenu des actes est rendu public	C=1	Interne malveillant capacités illimitées ; Interne sans intention de nuire capacités illimitées ; Externe malveillant capacités importantes ; Code malveillant	Aucun impact, les données sont publiques	1. Négligeable

3.2 LES BIENS SUPPORTS : SYSTEMES, ORGANISATIONS ET LOCAUX

Les biens supports suivants sont retenus de façon générale :

1. SYS – MAT : Systèmes informatiques et de téléphonie - Matériels
   Ce type de biens supports est constitué de l'ensemble des éléments physiques d'un système informatique (hardware et des supports de données électroniques) participant au stockage et au traitement de tout ou partie des biens essentiels.
2. SYS – LOG : Systèmes informatiques et de téléphonie - Logiciels
   Ce type de biens supports est constitué de l'ensemble des programmes participant au traitement de tout ou partie des biens essentiels (software).
3. SYS – RSX : Systèmes informatiques et de téléphonie - Canaux informatiques et de téléphonie

Ce type de biens supports est constitué de l'ensemble des vecteurs physiques de communication et de télécommunication qui transportent tout ou partie des biens essentiels.

4. ORG – PER : Organisations – Personnes
   Ce type de biens supports est constitué de l'ensemble des individus, catégories d'individus ou groupes sociaux homogènes, qui ont accès à tout ou partie des biens essentiels.
5. ORG – PAP : Organisations - Supports papier
   Ce type de biens supports est constitué de l'ensemble des Support statique non électronique contenant des données.
6. ORG – CAN : Organisations - Canaux interpersonnels
   Ce type de biens supports est constitué de l'ensemble des circuits organisationnels (canaux et processus organisationnels) et des échanges verbaux en face à face, qui transportent tout ou partie des biens essentiels.
7. LOC : Locaux
   Ce type de biens supports est constitué des infrastructures immobilières hébergeant, et nécessaires au bon fonctionnement, des systèmes informatiques (SYS) et des organisations (ORG), dans lesquels sont utilisés tout ou partie des biens essentiels.

3.2.1 Les liens entre biens essentiels et biens supports

Le tableau suivant présente les biens supports et leurs liens avec les biens essentiels :

Biens supports \ Biens essentiels	F. AUTHENTIFICATION	F. ACTES
SYS – Réseau interne		
SYS - MAT	X	X
LOG – Serveur Web	X	X
LOG – STELA	X	X
LOG – SGBD	X	X

Biens essentiels / Biens supports	F. AUTHENTIFICATION	F. ACTES
LOG – OS	X	X
LOG – intergiciel		X
RSX (Prise en compte PCA global)*1		
LOG – Utilisateur automate	X	X
ORG – Organisation		
PER – Administrateur	X	X
PER – Utilisateur commune	X	X
CAN – Enregistrement/Remise IGC	X	X
PAP – Demande d'ouverture de compte	X	X
LOC – Locaux		
LOC (Prise en compte PCA global) *2		

**1 : pris en compte dans l'étude "serveurs"*
**2 : pris en compte dans l'étude "salle serveurs"*

3.2.2 Menaces et vulnérabilités

La liste ci-dessous est issue de la base de connaissance eBios.

Menaces	Disponibilité	Intégrité	Confidentialité
SYS			
MAT	M1. Détournement de l'usage prévu d'un matériel M3. Dépassement des limites de fonctionnement d'un matériel M4. Détérioration d'un matériel M5. Modification d'un matériel M6. Perte d'un matériel	M1. Détournement de l'usage prévu d'un matériel M5. Modification d'un matériel	M1. Détournement de l'usage prévu d'un matériel M2. Espionnage d'un matériel M5. Modification d'un matériel M6. Perte d'un matériel
LOG	M7. Détournement de l'usage prévu d'un logiciel M9. Dépassement des limites de fonctionnement d'un logiciel M10. Suppression de tout ou partie d'un logiciel	M7. Détournement de l'usage prévu d'un logiciel M11. Modification d'un logiciel	M7. Détournement de l'usage prévu d'un logiciel M8. Analyse d'un logiciel M11. Modification d'un logiciel M12. Disparition d'un logiciel

	M11. Modification d'un logiciel M12. Disparition d'un logiciel		
RSX	M13. Attaque du milieu sur un canal informatique ou de téléphonie M15. Saturation d'un canal informatique ou de téléphonie M16. Dégradation d'un canal informatique ou de téléphonie M17. Modification d'un canal informatique ou de téléphonie M18. Disparition d'un canal informatique ou de téléphonie	M13. Attaque du milieu sur un canal informatique ou de téléphonie	M14. Écoute passive d'un canal informatique ou de téléphonie
ORG			
PER	M19. Dissipation de l'activité d'une personne M21. Surcharge des capacités d'une personne M22. Dégradation d'une personne M24. Départ d'une personne	M21. Surcharge des capacités d'une personne M23. Influence sur une personne	M20. Espionnage d'une personne à distance M23. Influence sur une personne M24. Départ d'une personne
PAP	M25. Détournement de l'usage prévu d'un support papier M27. Détérioration d'un support papier M28. Perte d'un support papier	M25. Détournement de l'usage prévu d'un support papier	M26. Espionnage d'un support papier M28. Perte d'un support papier
CAN	M29. Manipulation via un canal interpersonnel M31. Saturation d'un canal interpersonnel M32. Dégradation d'un canal interpersonnel M33. Modification d'un canal interpersonnel M34. Disparition d'un canal interpersonnel	M29. Manipulation via un canal interpersonnel	M30. Espionnage d'un canal interpersonnel

3.2.3 Sécurité des biens supports

Scénario de menace	Bien support	Critère	Scénarios de menaces / Vulnérabilités	Sources de menaces	Vraisemblance
SM01	LOG – Serveur Web	Disponibilité	Attaque DDOS	Interne malveillant capacités illimitées ; Interne sans intention de nuire capacités illimitées ; Externe malveillant capacités importantes ; Code malveillant	2. Significative
SM02		Intégrité	Compromission des données		2. Significative
SM03		Confidentialité	Non retenu		1. Minime
SM04	LOG – STELA	Disponibilité	Plantage de l'application / bug		2. Significative
SM05		Intégrité	Injection de code		2. Significative
SM06		Confidentialité	Non retenu		1. Minime
SM07	LOG – SGBD	Disponibilité	Plantage de l'application / bug		2. Significative
SM08		Intégrité	Injection de code		2. Significative

Scénario de menace	Bien support	Critère	Scénarios de menaces / Vulnérabilités	Sources de menaces	Vraisemblance
SM09		Confidentialité	Divulgation des comptes utilisateurs		1. Minime
SM10	LOG – OS	Disponibilité	Plantage de l'application / bug		2. Significative
SM11		Intégrité	Système de fichiers		3. Forte
SM12		Confidentialité	Cheval de Troie		1. Minime
SM13	LOG – intergiciel	Disponibilité	Plantage de l'application / bug		2. Significative
SM14		Intégrité	Plantage de l'application / bug		2. Significative
SM15		Confidentialité	Non retenu		1. Minime
SM16	LOG – Utilisateur automate	Disponibilité	Non retenu		
SM17		Intégrité	Non retenu		
SM18		Confidentialité	Non retenu		
SM19	PER – Administrateur	Disponibilité	Prise en charge par le PCA		
SM20		Intégrité	Formation insuffisante		2. Significative
SM21		Confidentialité	Non retenu		
SM22	PER – Utilisateur commune	Disponibilité	Non retenu		
SM23		Intégrité	Non retenu		
SM24		Confidentialité	Non retenu		
SM25	CAN – Enregistrement / Remise IGC	Disponibilité	Non retenu		
SM26		Intégrité	Modifications/altération d'informations sur le titulaire des futurs accès		1. Minime
SM27		Confidentialité	Interception des accès d'un titulaire		1. Minime
SM28	PAP – Demande d'ouverture de compte	Disponibilité	Non retenu		
SM29		Intégrité	Saisi d'informations incorrectes sur le titulaire des futurs accès		2. Significative
SM30		Confidentialité	Interception des informations accès pour un titulaire		1. Minime

4 ETUDES DES SCENARIOS DE MENACES

4.1 ENUMERATION DES SCENARIOS DE MENACES

4.1.1 Tableau récapitulatif

Le tableau suivant présente les menaces pesant sur les biens essentiels

Scénario	Source de menace	Menace	Bien support	Bien essentiel	Critère	Gravité	Vraisemblance	Mesure (Prévention, protection, restauration)
SR01	Interne malveillant capacités illimités Administrateur système ou réseau, dirigeant	M7. Détournement de l'usage prévu d'un logiciel *Installation d'un serveur de fichier (IRC, jeux, vidéo, etc.) sur le serveur STELA* ~~M9. Dépassement des limites de fonctionnement d'un logiciel~~ *Non retenu* M10. Suppression de tout ou partie d'un logiciel *Suppression de fichiers (prod, dev et sauvegarde) ou de données (prod, sauvegarde) de l'application* M11. Modification d'un logiciel *Modification de fichiers (prod, dev et sauvegarde) ou de données (prod, sauvegarde) de l'application.* ~~M12. Disparition d'un logiciel~~ *Non retenu car logiciels open source maintenus.* ~~M19. Dissipation de l'activité d'une personne~~ *Un administrateur est détourné de ses missions par un collègue cherchant à le mettre en difficulté et à nuire au fonctionnement du système. Non retenu.* ~~M21. Surcharge des capacités d'une personne~~ *Administrateur trop sollicité. Non retenu* ~~M22. Dégradation d'une personne~~ M24. Départ d'une personne *Conflit, un administrateur part sans effectuer le transfert de ses compétences.* ~~M25. Détournement de l'usage prévu d'un support papier~~ ~~M27. Détérioration d'un support papier~~ ~~M28. Perte d'un support papier~~ *Non retenu car tous les documents sont numérisés* ~~M29. Manipulation via un canal~~	tous (SYS/LOG, ORG/PER, ORG/PAP, ORG/CAN)	STELA	D	2. Limité objectif SSI recherché : 2. Limité	2. Significatif objectif SSI recherché : 1. Négligeable	Responsabilisation des développeurs et des administrateurs système au travers d'une charte de bonne conduite Contrôle régulier par des tiers (les autres administrateurs et développeurs) ~~Compte d'administration individuel~~ Journaliser et stocker les connections des administrateurs ~~Répartir les rôles et séparer les périmètres d'action~~

Scénario	Source de menace	Menace	Bien support	Bien essentiel	Critère	Gravité	Vraisemblance	Mesure (Prévention, protection, restauration)
		~~interpersonnel~~ ~~M31. Saturation d'un canal interpersonnel~~ ~~M32. Dégradation d'un canal interpersonnel~~ M33. Modification d'un canal interpersonnel *Mauvaises relations entre les personnes entravant les échanges d'information au quotidien.* ~~M34. Disparition d'un canal interpersonnel~~						
SR02		M7. Détournement de l'usage prévu d'un logiciel M11. Modification d'un logiciel M21. Surcharge des capacités d'une personne M23. Influence sur une personne M25. Détournement de l'usage prévu d'un support papier M29. Manipulation via un canal interpersonnel			I	3 Important objectif SSI recherché : 3. Important	2 Significatif objectif SSI recherché : 1. Négligeable	Mise en place d'un registre numérotant les demande d'ouverture de compte Gestion de projet plus efficace Contrôle régulier par des tiers (les autres administrateurs et développeurs) Dépôt des sources en externe Contrôle régulier du hash des fichiers du code source
SR03		M7. Détournement de l'usage prévu d'un logiciel M8. Analyse d'un logiciel M11. Modification d'un logiciel M12. Disparition d'un logiciel M20. Espionnage d'une personne à distance M23. Influence sur une personne M24. Départ d'une personne M26. Espionnage d'un support papier			C	1 Négligeable objectif SSI recherché : 1. Négligeable	2 Significatif objectif SSI recherché : 2. Significatif	
SR04	Interne malveillant capacités illimités	M7. Détournement de l'usage prévu d'un logiciel M9. Dépassement des limites de fonctionnement d'un logiciel M10. Suppression de tout ou partie d'un logiciel	tous	Authentifica-tion	D	2. Limité objectif SSI recherché :	2. Significatif objectif SSI recherché :	

Scénario	Source de menace	Menace	Bien support	Bien essentiel	Critère	Gravité	Vraisemblance	Mesure (Prévention, protection, restauration)
		M11. Modification d'un logiciel M12. Disparition d'un logiciel M19. Dissipation de l'activité d'une personne M21. Surcharge des capacités d'une personne M22. Dégradation d'une personne M24. Départ d'une personne M25. Détournement de l'usage prévu d'un support papier M27. Détérioration d'un support papier M28. Perte d'un support papier M29. Manipulation via un canal interpersonnel M31. Saturation d'un canal interpersonnel M32. Dégradation d'un canal interpersonnel M33. Modification d'un canal interpersonnel M34. Disparition d'un canal interpersonnel				2. Limité	2. Significatif	
SR05		M7. Détournement de l'usage prévu d'un logiciel M11. Modification d'un logiciel M21. Surcharge des capacités d'une personne M23. Influence sur une personne M25. Détournement de l'usage prévu d'un support papier M29. Manipulation via un canal interpersonnel			I	2. Limité objectif SSI recherché : 2. Limité	2 Significatif objectif SSI recherché : 2. Significatif	
SR06		M7. Détournement de l'usage prévu d'un logiciel M8. Analyse d'un logiciel M11. Modification d'un logiciel M12. Disparition d'un logiciel M20. Espionnage d'une personne à distance M23. Influence sur une personne M24. Départ d'une personne M26. Espionnage d'un support papier			C	3. Important objectif SSI recherché : 2. Limité	2. Significatif objectif SSI recherché : 2. Significatif	Gestion de projet plus efficace Responsabilisation des développeurs et des administrateurs système au travers d'une charte de bonne conduite Faire signer un acte d'engagement à toute personne quittant la structure afin de garantir la confidentialité

Scénario	Source de menace	Menace	Bien support	Bien essentiel	Critère	Gravité	Vraisemblance	Mesure (Prévention, protection, restauration)
		M28. Perte d'un support papier M30. Espionnage d'un canal interpersonnel						
SR07	Interne sans intention de nuire capacités illimitées	M7. Détournement de l'usage prévu d'un logiciel M9. Dépassement des limites de fonctionnement d'un logiciel M10. Suppression de tout ou partie d'un logiciel M11. Modification d'un logiciel M12. Disparition d'un logiciel M19. Dissipation de l'activité d'une personne M21. Surcharge des capacités d'une personne M22. Dégradation d'une personne M24. Départ d'une personne M25. Détournement de l'usage prévu d'un support papier M27. Détérioration d'un support papier M28. Perte d'un support papier M29. Manipulation via un canal interpersonnel M31. Saturation d'un canal interpersonnel M32. Dégradation d'un canal interpersonnel M33. Modification d'un canal interpersonnel M34. Disparition d'un canal interpersonnel		STELA	D	2 Limité objectif SSI recherché : 2. Limité	2 Significatif objectif SSI recherché : 2. Significatif	
SR08		M7. Détournement de l'usage prévu d'un logiciel M11. Modification d'un logiciel M21. Surcharge des capacités d'une personne M23. Influence sur une personne			I	3 Important objectif SSI recherché :	2 Significatif objectif SSI recherché :	

Scénario	Source de menace	Menace	Bien support	Bien essentiel	Critère	Gravité	Vraisemblance	Mesure (Prévention, protection, restauration)
		M25. Détournement de l'usage prévu d'un support papier M29. Manipulation via un canal interpersonnel				3. Important	2. Significatif	
SR09		M8. Analyse d'un logiciel M11. Modification d'un logiciel M12. Disparition d'un logiciel M23. Influence sur une personne M24. Départ d'une personne			C	1 Négligeable objectif SSI recherché : 1. Négligeable	2 Significatif objectif SSI recherché : 2. Significatif	
SR10	Interne sans intention de nuire capacités illimitées	M7. Détournement de l'usage prévu d'un logiciel M9. Dépassement des limites de fonctionnement d'un logiciel M10. Suppression de tout ou partie d'un logiciel M11. Modification d'un logiciel M12. Disparition d'un logiciel M19. Dissipation de l'activité d'une personne M21. Surcharge des capacités d'une personne M22. Dégradation d'une personne M24. Départ d'une personne M25. Détournement de l'usage prévu d'un support papier M27. Détérioration d'un support papier M28. Perte d'un support papier M29. Manipulation via un canal interpersonnel M31. Saturation d'un canal interpersonnel M32. Dégradation d'un canal interpersonnel M33. Modification d'un canal interpersonnel M34. Disparition d'un canal interpersonnel		Authentification	D	2 Limité objectif SSI recherché : 2. Limité	2 Significatif objectif SSI recherché : 2. Significatif	

Scénario	Source de menace	Menace	Bien support	Bien essentiel	Critère	Gravité	Vraisemblance	Mesure (Prévention, protection, restauration)
SR11		M7. Détournement de l'usage prévu d'un logiciel M11. Modification d'un logiciel M21. Surcharge des capacités d'une personne M23. Influence sur une personne M25. Détournement de l'usage prévu d'un support papier M29. Manipulation via un canal interpersonnel			I	3. Important objectif SSI recherché : 2. Limité	2. Significatif objectif SSI recherché : 2. Significatif	Gestion de projet plus efficace Responsabilisation des développeurs et des administrateurs système au travers d'une charte de bonne conduite Sensibilisation des utilisateurs aux usages d'internet afin de ne pas donner accès à son poste à tout tiers Faire signer un acte d'engagement à toute personne quittant la structure afin de garantir la confidentialité
SR12		M8. Analyse d'un logiciel M11. Modification d'un logiciel M12. Disparition d'un logiciel M20. Espionnage d'une personne à distance M23. Influence sur une personne M24. Départ d'une personne M26. Espionnage d'un support papier M28. Perte d'un support papier M30. Espionnage d'un canal interpersonnel			C	3. Important objectif SSI recherché : 2. Limité	2. Significatif objectif SSI recherché : 2. Significatif	Gestion de projet plus efficace Responsabilisation des développeurs et des administrateurs système au travers d'une charte de bonne conduite Sensibilisation des utilisateurs aux usages d'internet afin de ne pas donner accès à son poste à tout tiers Faire signer un acte d'engagement à toute personne quittant la structure afin de garantir la confidentialité
SR13	Externe malveillant capacité importante	M7. Détournement de l'usage prévu d'un logiciel *Installation d'un serveur de fichier (IRC, jeux, vidéo, etc.) sur le serveur STELA* M10. Suppression de tout ou partie d'un logiciel *Suppression de fichiers (prod, dev et sauvegarde) ou de données (prod,*	Tous	STELA	D	2. Limité objectif SSI recherché : 2. Limité	2. Significatif objectif SSI recherché : 1. Négligeable	Contrôle régulier par des administrateurs Mise en place d'un réseau sécurisé fermé entre les utilisateurs et le SI

Scénario	Source de menace	Menace	Bien support	Bien essentiel	Critère	Gravité	Vraisemblance	Mesure (Prévention, protection, restauration)
		sauvegarde) de l'application M11. Modification d'un logiciel *Modification de fichiers (prod, dev et sauvegarde) ou de données (prod, sauvegarde) de l'application.*						
SR14		M7. Détournement de l'usage prévu d'un logiciel M11. Modification d'un logiciel M21. Surcharge des capacités d'une personne M23. Influence sur une personne			I	3 Important objectif SSI recherché : 2. Limité	2 Significatif objectif SSI recherché : 1. Négligeable	Contrôle régulier par des administrateurs Mise en place d'un réseau sécurisé fermé entre les utilisateurs et le SI
SR15		M7. Détournement de l'usage prévu d'un logiciel M8. Analyse d'un logiciel M11. Modification d'un logiciel M12. Disparition d'un logiciel M20. Espionnage d'une personne à distance M23. Influence sur une personne M24. Départ d'une personne			C	1 Négligeable objectif SSI recherché : 1. Négligeable	2 Significatif objectif SSI recherché : 2. Significatif	
SR16	Externe malveillant capacité importante	M7. Détournement de l'usage prévu d'un logiciel M9. Dépassement des limites de fonctionnement d'un logiciel M10. Suppression de tout ou partie d'un logiciel M11. Modification d'un logiciel	Tous	Authentification	D	2. Limité objectif SSI recherché : 2. Limité	2. Significatif objectif SSI recherché : 2. Significatif	
SR17		M7. Détournement de l'usage prévu d'un logiciel M11. Modification d'un logiciel M23. Influence sur une personne			I	2. Limité objectif SSI recherché : 2. Limité	2 Significatif objectif SSI recherché : 2. Significatif	

Scénario	Source de menace	Menace	Bien support	Bien essentiel	Critère	Gravité	Vraisemblance	Mesure (Prévention, protection, restauration)
SR18		M7. Détournement de l'usage prévu d'un logiciel M8. Analyse d'un logiciel M11. Modification d'un logiciel M12. Disparition d'un logiciel M20. Espionnage d'une personne à distance M23. Influence sur une personne			C	3. Important objectif SSI recherché : 2. Limité	2. Significatif objectif SSI recherché : 2. Significatif	Responsabilisation des développeurs et des administrateurs système au travers d'une charte de bonne conduite Sensibilisation des utilisateurs aux usages d'internet afin de ne pas donner accès à son poste à tout tiers Faire signer un acte d'engagement à toute personne quittant la structure afin de garantir la confidentialité
SR19	Code malveillant	M7. Détournement de l'usage prévu d'un logiciel *Installation d'un serveur de fichier (IRC, jeux, vidéo, etc.) sur le serveur STELA* M10. Suppression de tout ou partie d'un logiciel *Suppression de fichiers (prod, dev et sauvegarde) ou de données (prod, sauvegarde) de l'application* M11. Modification d'un logiciel *Modification de fichiers (prod, dev et sauvegarde) ou de données (prod, sauvegarde) de l'application.*	Tous	STELA	D	2. Limité objectif SSI recherché : 2. Limité	1. Négligeable objectif SSI recherché : 1. Négligeable	
SR20		M7. Détournement de l'usage prévu d'un logiciel M11. Modification d'un logiciel M21. Surcharge des capacités d'une personne M23. Influence sur une personne			I	3 Important objectif SSI recherché : 2. Limité	2 Significatif objectif SSI recherché : 1. Négligeable	Contrôle régulier par des administrateurs Mise en place d'un réseau sécurisé fermé entre les utilisateurs et le SI
SR21		M7. Détournement de l'usage prévu d'un logiciel M11. Modification d'un logiciel M12. Disparition d'un logiciel			C	1 Négligeable objectif SSI	2 Significatif objectif SSI	

Scénario	Source de menace	Menace	Bien support	Bien essentiel	Critère	Gravité	Vraisemblance	Mesure (Prévention, protection, restauration)
		M20. Espionnage d'une personne à distance				recherché : 1. Négligeable	recherché : 2. Significatif	
SR22	Code malveillant	M7. Détournement de l'usage prévu d'un logiciel M9. Dépassement des limites de fonctionnement d'un logiciel M10. Suppression de tout ou partie d'un logiciel M11. Modification d'un logiciel	Tous	Authentification	D	2. Limité objectif SSI recherché : 2. Limité	2. Significatif objectif SSI recherché : 2. Significatif	
SR23		M7. Détournement de l'usage prévu d'un logiciel M11. Modification d'un logiciel			I	2. Limité objectif SSI recherché : 2. Limité	2 Significatif objectif SSI recherché : 2. Significatif	
SR24		M7. Détournement de l'usage prévu d'un logiciel M8. Analyse d'un logiciel M11. Modification d'un logiciel M12. Disparition d'un logiciel			C	3. Important objectif SSI recherché : 3. Important	2. Significatif objectif SSI recherché : 1. Négligeable	Sensibilisation des utilisateurs aux usages d'internet afin de ne pas donner accès à son poste à tout tiers

4.1.2 Exemples de scénarios de menaces

La liste suivante ne représente que des exemples de scénarios pour chacun des cas énoncés dans le tableau précédent, ils ne peuvent pas être considérés comme les seuls éléments de menaces. Pour chacun des scénarios présents dans le tableau précédant, d'autres exemple peuvent être trouvé, voir des exemples regroupant plusieurs scénarios.

- **SR01** : Un administrateur système du SICTIAM installe un serveur de fichiers sur l'un des serveurs STELA. Ceci va consommer des ressources (mémoire, CPU, bande passante) et rendre le service moins disponible
- **SR02** : Afin de porter préjudice à une collectivité, un développeur modifie l'application afin d'altérer les données avant leur transmission à la Préfecture. Ainsi, toutes les informations transmises par la collectivité intègrent de faux éléments
- **SR03** : Lors du départ d'un collaborateur, les accès auxquels il avait droit ne lui sont pas retirés. De ce fait, il peut continuer à accéder à la plate-forme et consulter les données auxquelles il ne devrait plus avoir accès.
- **SR04** : Afin de se venger d'une décision prise à son encontre, une des administrateurs de la plate-forme peut supprimer tous les comptes utilisateurs
- **SR05 - SR06** : Par pression sur unes des administrateurs de la plate-forme, les droits d'accès d'un utilisateur peuvent être modifiés afin de lui permettre de consulter un espace qui ne lui est pas accessible habituellement
- **SR07** : Suite à des actions de maintenance, une fausse manipulation peut supprimer toutes les données présentent sur la plate-forme. Cette dernière devient automatiquement indisponible
- **SR08** : Après une mise à jour, les données générées pour les enveloppes ACTES peuvent être erronées. Les transmissions reçues par la plate-forme seront donc incorrectes et systématiquement rejetées
- **SR09 - SR12** : Par erreur, un administrateur de la plate-forme ouvre des accès à un utilisateur sur un espace auquel il ne devrait pas avoir accès
- **SR10-SR11** : La charge de travail d'un agent du SICTIAM en charge de l'administration de la plate-forme est supérieure à la capacité dudit agent. Ceci va entrainer des oublis, des constitutions de dossiers incomplets, du retard et des erreurs amenant à la transmission d'informations erronées lors de la création des comptes utilisateurs
- **SR12** : Transmission d'un dossier d'inscription à une personne externe sans suivre les canaux de transmission habituels. Les données d'un utilisateur peuvent ainsi être divulguées
- **SR13 - SR16** : Des requêtes incessantes sur les serveurs peuvent augmenter leur charge de travail et ainsi les rendre inaccessibles par les utilisateurs tant sur l'utilisation de la plate-forme que sur l'authentification
- **SR14 - SR15** : Un hacker peut s'introduire sur la plate-forme, ensuite il peut modifier ou consulter tout ou partie des données présentes
- **SR17** : Une entité externe peut faire pression sur un des administrateurs de la plate-forme afin de modifier les informations d'un utilisateur. Ainsi lors de la transmission d'actes, les données émises vers la Préfecture ne seraient pas correctes
- **SR18** : Lors du départ d'un développeur, ce dernier peut transmettre l'intégralité du code source à un tiers afin que ce dernier l'analyse et trouve des failles de sécurité lui permettant d'accéder aux données des utilisateurs

- **SR19 - SR20 - SR21 - SR22 - SR23 - SR24** : Sur le poste d'un utilisateur (administrateur, utilisateur de collectivité, …), un logiciel espion peut être installé afin d'enregistrer toutes les actions réalisées par ce dernier. Ainsi toutes les données transmises (actes, données personnelles, code source, …) à STELA serait divulguées à un tiers

4.2 EVALUATION DES SCENARIOS DE MENACES

Le tableau suivant présente une cartographie des risques permettant de les évaluer

Vraisemblance \ Gravite	1. Négligeable	2. Significatif	3. Fort	4. Maximal	Vraisemblance / Gravite
4. Critique					4. Critique
3. Important		SR02 SR14 SR06 SR18 SR08 SR20 SR11 SR24 SR12			3. Important
2. Limité		SR01 SR13 SR04 SR16 SR05 SR17 SR07 SR22 SR10 SR23			2. Limité
1. Négligeable		SR03 SR09 SR15 SR19 SR21			1. Négligeable
Gravite / Vraisemblance	1. Négligeable	2. Significatif	3. Fort	4. Maximal	Gravite \ Vraisemblance

5 MESURES

5.1 MESURE A PRENDRE

Les mesures suivantes sont à apporter au site afin d'en améliorer la sécurité :

- **M01** : Responsabilisation des développeurs et des administrateurs système au travers d'une charte de bonne conduite
- **M02** : Contrôle régulier par les autres administrateurs et développeurs
- **M03** : Journaliser et stocker les connections des administrateurs
- **M04** : Mise en place d'un registre numérotant les demande d'ouverture de compte
- **M05** : Gestion de projet plus efficace
- **M06** : Dépôt des sources en externe
- **M07** : Contrôle régulier du hash des fichiers du code source
- **M08** : Sensibilisation des utilisateurs aux usages d'internet afin de ne pas donner accès à son poste à un tiers
- **M09** : Faire signer un acte d'engagement à toute personne à l'entrée et en quittant la structure afin de garantir la confidentialité
- **M10** : Mise en place d'un réseau sécurisé fermé entre les utilisateurs et le SI

5.2 EVALUATION DES NOUVEAUX SCENARIOS DE MENACES

Le tableau suivant présente une cartographie des risques permettant de les évaluer après application des mesures améliorant la sécurité du système

Vraisemblance \ Gravite	1. Négligeable	2. Significatif	3. Fort	4. Maximal	Vraisemblance / Gravite
4. Critique					4. Critique
3. Important	SR24	SR08			3. Important
2. Limité	SR20	SR02 SR04 SR05 SR06 SR07 SR10 SR11 SR12 SR14 SR16 SR17 SR18 SR22 SR23			2. Limité
1. Négligeable		SR01 SR03 SR09 SR13 SR15 SR19 SR21			1. Négligeable
Gravite / Vraisemblance	1. Négligeable	2. Significatif	3. Fort	4. Maximal	Gravite \ Vraisemblance

Après la mise en place des nouvelles mesures citées au chapitre 5.1, la vraisemblance ou la gravité des scénarios de menaces se réduit pour les rendre acceptables.
Néanmoins, on peut noter que le seul scénario en zone critique est le scénario SR08 portant sur les anomalies des logiciels. Malgré toutes les vérifications et tous les soins portés aux tests et aux validations, on ne peut exclure qu'un dysfonctionnement logiciel compromette la plate-forme.