



Ministère du Budget
et de la Réforme de l'Etat
DGME/SDAE



PREMIER MINISTRE
SGDN - DCSSI

=====

FEROS Types

Téléprocédure de référence

Simulation

=====

VERSION 1.0

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	13/04/2006	Public	1/35

FEROS Types	
Candidature	
Référence	Date
FEROS Types SimulationV1.0.doc	13/04/2006
Identification d'objet (OID)	Racine OID et gestionnaire
1.2.250.1.137.2.2.1.2.3.7.1	DGME/SDAE
Responsable	Version
DGME/SDAE – SGDN\DCSSI	V1.0
Critère de diffusion	Nombre de pages
Public	35

HISTORIQUE DES VERSIONS			
DATE	VERSION	EVOLUTION DU DOCUMENT	REDACTEUR
15/05/2005	0.1	Création du document	Fidens
13/04/2006	1.0	Version publié	DCSSI/SDAE

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	2/35

SOMMAIRE

1 INTRODUCTION 4

1.1 CONTEXTE GENERAL 4

1.2 DEFINITION DES RESPONSABILITES 5

2 DESCRIPTION DU SYSTEME ETUDIE 6

2.1 PRESENTATION DU SYSTEME-CIBLE 7

2.2 DESCRIPTION DES ELEMENTS ESSENTIELS 8

2.3 ENJEUX 11

2.4 HYPOTHESES 12

2.5 ECHELLE DE BESOINS 13

2.6 BESOINS DE SECURITE DES ELEMENTS ESSENTIELS 14

3 LES RISQUES 18

3.1 HIERARCHISATION DES RISQUES 18

3.2 DESCRIPTION DES RISQUES 19

4 OBJECTIFS DE SECURITE 28

5 LES RISQUES RESIDUELS 30

5.1 METHODES D'ATTAQUE NON RETENUES 30

5.2 TABLEAU DE COUVERTURE DES RISQUES PAR LES OBJECTIFS 35

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	3/35

1 Introduction

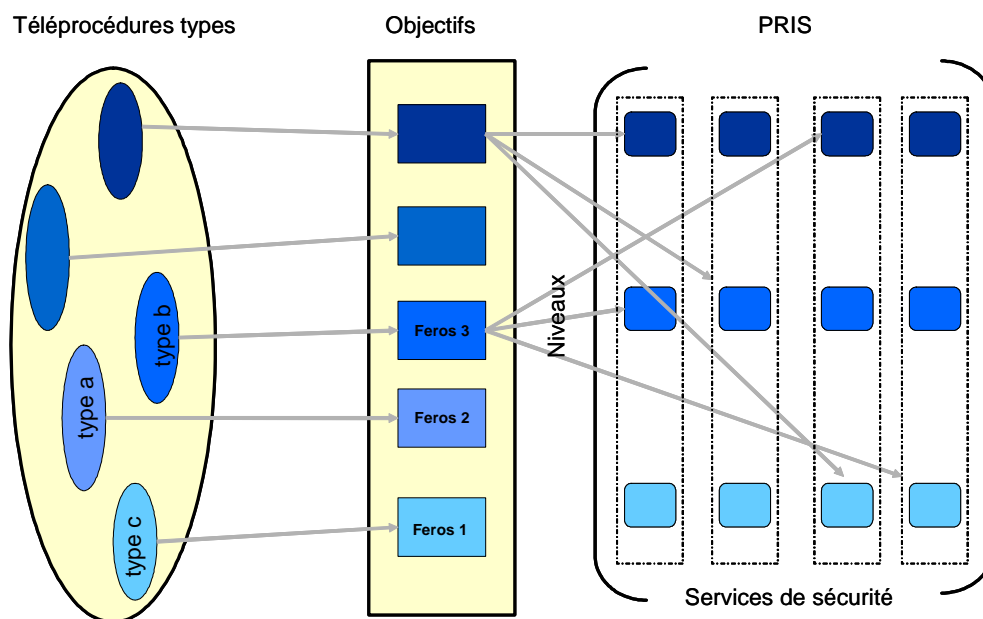
1.1 Contexte général

Poursuivant un triple objectif de modernisation des services, de simplification des démarches et de recherche d'une plus grande efficacité, l'Etat a entamé un processus de modernisation de son Administration. A ce titre, l'Etat s'est engagé dans le développement de services en ligne, gages d'amélioration de la qualité de service et de gain de productivité.

La mise en place de ces relations dématérialisées avec les usagers – citoyens, agents de l'Administration, entreprises, ... -, nécessite une confiance reconnue et partagée par les différents acteurs. Afin de favoriser l'émergence d'un climat de confiance mutuelle propre au développement de ces téléservices, la DCSSI et l'ADAE contribuent aujourd'hui à la définition d'un cadre général de sécurisation des systèmes d'information.

C'est ainsi qu'ils ont élaboré un ensemble documentaire unique baptisé PRIS, « Politique de Référencement Intersectorielle de Sécurité », déterminant pour différents services de sécurité et différents niveaux de sécurité un ensemble d'exigences juridiques et organisationnelles et de spécifications techniques ; cet ensemble deviendra la référence à laquelle les prestataires de services et les fournisseurs de produits devront se conformer.

Pour faciliter l'utilisation de cet ensemble documentaire, l'ADAE a lancé une étude, visant à établir des correspondances entre téléprocédures types et les référentiels PRIS.



FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	4/35

L'analyse générique d'objectifs de sécurité pour des téléprocédures types doit permettre de faciliter et d'homogénéiser les expressions de besoins des donneurs d'ordre en mettant à leur disposition des référentiels sur lesquels ils pourront s'appuyer pour exprimer leurs besoins spécifiques. Par exemple, le promoteur d'une téléprocédure de paiement de cotisation pourra procéder à partir de la téléprocédure type « paiement », en analysant les spécificités liées au contexte opérationnel et à la sensibilité des informations traitées, et en conservant les invariants de l'analyse (fonctions, éléments menaçants, ...)

Le choix des téléprocédures types a été réalisé sur une base statistique – étude des téléprocédures les plus largement mises en œuvre – ou en fonction des priorités de l'ADAE.

Les téléprocédures type retenues sont :

- **Consultation**
- **Simulation**
- **Démarche en ligne : déclaration**
- **Démarche en ligne : candidature**
- **Démarche en ligne : demandes**
- **Paiement en ligne**

Le présent document présente l'analyse des objectifs de sécurité pour la téléprocédure type simulation.

1.2 Définition des responsabilités

La présente analyse a été réalisée sous Maîtrise d'œuvre de l'ADAE, avec le soutien de la DCSSI qui a apporté son expertise technique.

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	5/35

2 Description du système étudié

La téléprocédure « Simulation » offre aux Internauteurs la possibilité d'analyser différentes solutions et d'en évaluer les conséquences. Dans le domaine social, ce peut être une simulation relative à des calculs de charge sociale, de manière à optimiser des dates de recrutement ou des profils de salariés. Dans le domaine fiscal, la simulation peut être effectuée pour optimiser des déclarations de revenus, des montants de donation, ... Dans le domaine médical, la simulation peut permettre d'étudier les risques inhérents à différentes situations, pour aider à la prise de décision du professionnel par exemple.

Les informations accédées peuvent être en libre accès, ou réservées à certains profils. Il est indispensable que la simulation soit accessible de manière anonyme ; cependant, il peut être également nécessaire de pouvoir conserver les données renseignées, de manière à faciliter une reprise de contexte par l'utilisateur.

Exemples de mise en œuvre

Transports exceptionnels : service d'aide à la préparation de l'itinéraire. Service d'aide de calcul de répartition des charges à l'essieu

Calcul de revalorisation des pensions alimentaires

Simulateur universel de calcul de retraite

Simulation et calcul de l'impôt sur revenu

Simulation et calcul de l'impôt de solidarité sur la fortune

Simulation d'échéancier de mensualisation de l'impôt

Défiscalisation et réduction d'impôt.

Simulation de calcul de bourses

Scénario retenu pour l'analyse

DESCRIPTION

Au titre de la téléprocédure type, on retiendra la simulation du calcul d'une pension civile de retraite.

USAGER

- Particulier

MODE OPERATOIRE

- Accès depuis les moyens informatiques propres de l'utilisateur

DOMAINE D'APPLICATION

- Social

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	6/35

2.1 Présentation du système-cible

Afin de rapprocher le modèle de la réalité, l'analyse est menée sur la base d'une téléprocédure existante – ici la simulation de calcul d'une pension civile de retraite.

Systeme-cible

Présentation

La téléprocédure « Simulation du calcul d'une pension civile de retraite » permet aux fonctionnaires d'évaluer le montant de pension alloué en fonction de leur état de carrière et leur situation familiale.

La téléprocédure est généralement utilisée pour :

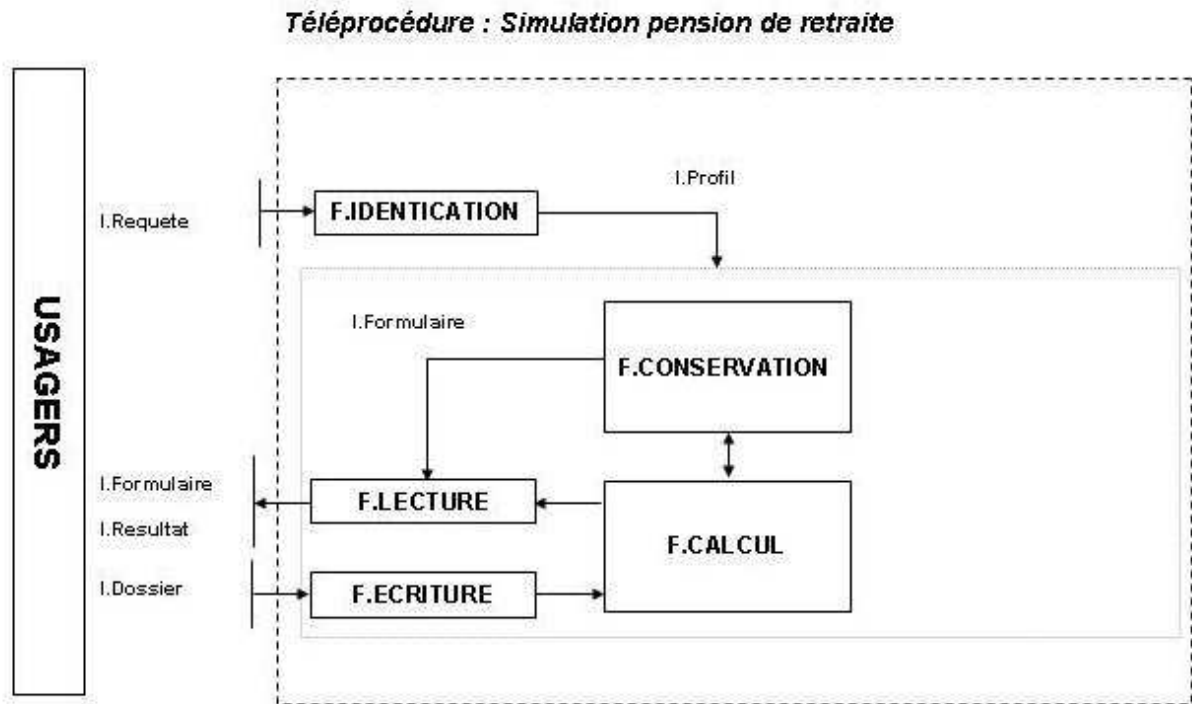
- Estimer la date de départ en retraite
- Visualiser l'impact d'un changement de situation sur la pension allouée

La simulation, totalement anonyme, est réalisée uniquement sur la base des renseignements fournis par l'utilisateur. Les résultats obtenus ne possèdent donc aucune valeur significative et ne peuvent en aucun cas être substitués à la délivrance d'un titre de pension.

L'instruction du dossier se fait en ligne mais il n'existe pas de fonctionnalités permettant de garantir la persistance des données « utilisateurs » entre les sessions. Ainsi, l'utilisateur doit ressaisir l'intégralité de son dossier s'il se déconnecte.

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	7/35

2.2 Description des éléments essentiels



Fonction : F.CALCUL

Description

Cette fonction est mise en œuvre pour calculer le montant de la pension. Pour cela, la fonction doit disposer :

- Des informations saisies par l'utilisateur
- De paramètres (indices, taux ...) conservés au niveau du référentiel

Lorsque l'utilisateur déclare sa situation, cette fonction est donc chargée de rechercher au niveau du référentiel les différentes valeurs correspondant à la situation de l'utilisateur.

Une fois identifiées, elle procède au calcul à proprement parler. Après traitement, les résultats obtenus sont présentés par l'intermédiaire de la fonction « F.LECTURE ».

Fonction : F.CONSERVATION

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	8/35

Description

Cette fonction est chargée de la problématique de conservation des informations.

Dans le cadre de cette téléprocédure, elle constitue principalement un référentiel permettant de stocker les valeurs de calcul en fonction des situations de carrière des agents de l'Etat. Ainsi, sur la base des paramètres fournis par l'utilisateur, une recherche est entreprise afin de lancer le calcul et approcher au mieux le montant de pension alloué

Contrairement à la modélisation des autres téléprocédures type, l'utilisateur n'agit pas sur la partie « conservation de données » par l'intermédiaire de la fonction « F.ECRITURE ». En effet, le référentiel est uniquement accessible en lecture.

Fonction : F.ECRITURE

Description

Cette fonction permet de soumettre de l'information à l'administration. Elle est utilisée comme support au formulaire de saisie puisqu'elle permet de spécifier les différents paramètres de la simulation.

Un contrôle de cohérence approprié est effectué de sorte que le format et la complétude de certains champs du formulaire sont rendus obligatoires. Chacune des informations saisies est ensuite passée en paramètre à la fonction de calcul.

Fonction : F.IDENTIFICATION

Description

La sous fonction "F.IDENTIFICATION" ne contrôle pas l'identité des usagers car la téléprocédure de simulation garantit leur anonymat. Elle doit uniquement être considérée comme une brique fonctionnelle support au contrôle d'accès et à la gestion des données de session.

En effet, la téléprocédure ne permet pas de sauvegarder les données renseignées. Elles sont uniquement conservées pendant la durée de la session afin de faciliter la modification d'un paramètre.

Fonction : F.LECTURE

Description

Cette fonction permet à l'administration de présenter de l'information conformément aux autorisations accordées aux usagers. Deux catégories sont répertoriées au niveau de cette téléprocédure :

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	9/35

- Les informations statiques (formulaire de saisie, aides en ligne)
- Les résultats de traitement (issus de la fonction calcul)

Contrairement à la majorité des autres téléprocédures, cette fonction n'est pas exclusivement dédiée à la mise en forme et l'affichage des informations stockées au niveau de la partie conservation de données.

Les résultats des simulations issues de la fonction de calcul sont directement affichés par cette fonction.

Information : I.Dossier

Description

Cet élément essentiel regroupe les informations fournies par l'utilisateur afin de déclarer sa situation et procéder à la simulation. Il contient plusieurs types d'information :

- Les informations d'état civil (l'anonymat est conservé)
- Le décompte des durées de service
- L'indice de rémunération
- La situation familiale (nombre d'enfants, date de naissance)

Ces informations sont utilisées pour lancer le calcul ou identifier des indices au niveau de la partie conservation de données.

Information : I.Formulaire

Description

Cet élément essentiel contient les informations contenues dans le formulaire de saisie et accessible en lecture par l'utilisateur.

Information : I.Profil

Description

Cette information fixe les autorisations d'accès qui s'appliquent au contenu et aux fonctions de la téléprocédure. Ces restrictions s'appliquent à la majorité des fonctions et permet d'identifier les droits d'accès aux données au niveau de la partie « conservation de données ».

D'autre part, elle supporte aussi la notion de gestion des données de session permettant à l'utilisateur de modifier sa saisie.

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	10/35

Information : I.Référentiel

Description Cet élément essentiel regroupe toute une série d'information permettant de faire correspondre la situation de l'utilisateur et des paramètres utilisés pour calculer le montant alloué.

Information : I.Requête

Description Requête initiale de l'utilisateur (URL).

Information : I.Résultat

Description Cet élément essentiel constitue le résultat de la simulation. Il contient plusieurs types d'information :

- Le total des services retenus
- Le détail des montants alloués
- Le total mensuel alloué

Les informations sont ensuite présentées à l'utilisateur qui peut, le cas échéant, modifier sa saisie afin d'appréhender les répercussions au niveau du résultat.

2.3 Enjeux

E.ATTENTES

Description Les récents sondages indiquent une hausse notable des attentes des utilisateurs vis à vis de l'administration électronique. L'augmentation de l'utilisation d'Internet, la confiance grandissante inspirée ou encore la simplicité d'utilisation sont autant de catalyseurs qui favorisent le développement des téléprocédures.

E.SERVICES

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	11/35

Description Cette téléprocédure s'inscrit dans le projet de modernisation des services administratifs et vise à enrichir le fonctionnement actuel.

2.4 Hypothèses

H.CONFIANCE

Description Dans le cadre de cette analyse, il est admis que les agents bénéficiant du plus haut degré de privilèges sont de confiance.

H.LOCAUX

Description Dans le cadre de l'analyse, il est admis que la téléprocédure est hébergée dans des locaux bénéficiant de mesures de sécurité adaptées. Par conséquent, les méthodes d'attaques basées sur un accès physique aux locaux seront volontairement écartées.

H.ORGANISATIONNEL

Description Dans le cadre de cette étude, les menaces organisationnelles ne seront pas traitées.

H.USAGER

Description La sécurité physique et environnementale au niveau du poste de l'utilisateur est garantie.

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	12/35

2.5 Echelle de besoins

	Confidentialité	Disponibilité	Intégrité
0	Informations publiques.	Une indisponibilité ne provoque aucune perturbation au niveau du système d'information.	La perte d'intégrité n'entraîne aucune gêne.
1	Informations personnelles mais dont la divulgation n'engendre aucune conséquence.	Une indisponibilité de quelques jours de l'application ou de la ressource est tolérable.	Une perte d'intégrité est dommageable mais les conséquences restent restreintes.
2	Informations confidentielles ne devant pas être divulguées. Une perte de confidentialité est grave mais n'entraîne aucune conséquence au niveau économique ou médiatique.	Une indisponibilité momentanée 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'utilisateurs. Les conséquences restent donc restreintes.
3	Informations confidentielles ne devant pas être divulguées. Une perte de confidentialité a des conséquences sur le plan médiatique ou financier.	Une indisponibilité à une incidence grave au niveau financier ou en terme d'image de marque.	Une perte d'intégrité des informations est très grave et impacte le fonctionnement global de la téléprocédure. Elle entraîne une perte importante au niveau financier et/ou de l'image de marque.

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	13/35

2.6 Besoins de sécurité des éléments essentiels

		Besoin de sécurité	Commentaires
F.CALCUL	Confidentialité	0	Aucun besoin au niveau de ce critère de sécurité.
	Disponibilité	1	Cette téléprocédure ne correspond pas à une démarche administrative. D'autre part, aucune contrainte d'ordre calendaire n'est présente. Dans cette situation, le besoin en disponibilité est très faible.
	Intégrité	2	Une perte d'intégrité est grave car elle peut rapidement engendrer le mécontentement de certains usagers.
F.CONSERVATION	Confidentialité	0	Aucun besoin au niveau de ce critère de sécurité.
	Disponibilité	1	Une indisponibilité de quelques jours est tolérable puisqu'il n'existe aucune contrainte d'ordre calendaire.
	Intégrité	1	Une perte d'intégrité est grave car elle peut par suite provoquer une perturbation au niveau du référentiel et conduire à des dysfonctionnements importants. Cependant, les conséquences restent limitées car la simulation est indépendante de la délivrance d'un titre de pension.
F.ECRITURE	Confidentialité	0	Aucun besoin au niveau de ce critère de sécurité.
	Disponibilité	1	Le besoin en disponibilité est moyen dans la mesure où la téléprocédure elle même ne présente qu'un besoin limité.
	Intégrité	1	Si elle peut influencer notablement le résultat obtenu, une perte d'intégrité n'est pas très grave dans la mesure où la simulation et la

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	14/35

			délivrance du titre de pension ne sont pas liées.
F.IDENTIFICATION	Confidentialité	0	Aucun besoin au niveau de ce critère de sécurité.
	Disponibilité	1	Le besoin en disponibilité au niveau de cette fonction est moyen. Les usagers peuvent facilement retarder la réalisation d'une simulation.
	Intégrité	1	Le besoin en intégrité est moyen car la simulation est réalisée à titre informatif. En aucun cas, elle ne dispense ou complète la déclaration administrative réelle.
F.LECTURE	Confidentialité	0	Aucun besoin au niveau de ce critère de sécurité.
	Disponibilité	1	Dans la mesure où la téléprocédure est une simulation qui ne répond à aucune démarche administrative, une indisponibilité de quelques jours est tolérable.
	Intégrité	1	Le besoin en intégrité est faible puisque cette fonction est chargée de la présentation des informations à l'utilisateur. Les résultats obtenus lors de la simulation n'engagent pas la responsabilité de l'administration.
I.Dossier	Confidentialité	1	Cet élément essentiel présente un besoin en confidentialité très faible dans la mesure où le dossier est totalement anonyme.
	Disponibilité	1	L'utilisateur doit posséder toute une série d'informations afin de compléter et lancer la simulation. L'utilisateur peut facilement disposer de ces données en cas de perte.
	Intégrité	1	Une perte d'intégrité au niveau des informations permettant de réaliser la simulation peut provoquer des résultats non conformes. Les conséquences restent cependant limitées car il s'agit uniquement d'une simulation.

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	15/35

I.Formulaire	Confidentialité	0	Ces informations sont publiques.
	Disponibilité	1	Afin de lancer la simulation, l'administration doit soumettre le formulaire de saisie aux usagers. Une indisponibilité de quelques jours est néanmoins acceptable.
	Intégrité	1	Le besoin en intégrité est faible car aucun traitement n'est réalisé sur la base de cette information.
I.Profil	Confidentialité	1	Le profil définit l'identité et les autorisations associées aux usagers. Cependant, le besoin en confidentialité est moyen car la simulation est réalisée à titre anonyme.
	Disponibilité	1	Le besoin en disponibilité est faible car l'utilisateur peut retarder la réalisation de la simulation.
	Intégrité	2	Le besoin en intégrité est important car il fixe les droits d'accès aux fonctions et aux données.
I.Référentiel	Confidentialité	2	En théorie, le besoin en confidentialité est faible. Cependant une perte de confidentialité pourrait exposer l'administration à des plaintes et nuire à son image de marque.
	Disponibilité	1	Le besoin en disponibilité est identique à celui que présente les autres éléments essentiels de la téléprocédure.
	Intégrité	2	Une perte d'intégrité est grave car étant donné la nature de l'élément essentiel, elle peut provoquer le mécontentement des personnes touchées.
I.Requete	Confidentialité	0	Aucun besoin en confidentialité au niveau de cet élément essentiel.
	Disponibilité	1	Le besoin en disponibilité est faible puisque l'utilisateur peut retarder sa requête.
	Intégrité	1	Le besoin en intégrité est faible car l'utilisateur

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	16/35

			peut réitérer sa requête en cas d'échec.
I.Resultat	Confidentialité	0	Le besoin en confidentialité est moyen dans la mesure où les résultats sont anonymes.
	Disponibilité	1	La simulation ne correspond pas à une démarche administrative. Elle peut être retardée.
	Intégrité	1	Cet élément essentiel présente un besoin d'intégrité moyen car les résultats obtenus ne possèdent aucune valeur significative.

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	17/35

3 Les risques

Un premier paragraphe présente une hiérarchisation des risques, qui sont décrits de manière exhaustive par la suite.

3.1 Hiérarchisation des risques

	Critères de sécurité	Opportunité
R.TRAITEMENT-ANONYMAT	3	1
R.ABUS-AUTORISATION	2	3
R.DYSFONCTIONNEMENT-ERREUR	2	3
R.GARANTIE-ORIGINE	2	3
R.DYSFONCTIONNEMENT-CONCEPTION	2	3
R.LOGICIEL-CODE	2	2
R.ABUS-IDENTITE	2	2
R.ABUS-INJECTION	2	1
R.ABUS-DEBORDEMENT	2	1
R.SATURATION-LOGICIEL	1	3
R.DIVULGATION-STOCKAGE	1	3
R.PERTE-TELECOM	1	1

Le niveau du risque « R.TRAITEMENT-ANONYMAT » a été volontairement augmenté par rapport à son niveau original car la perte de l'anonymat entraîne l'augmentation du besoin en confidentialité de l'élément essentiel « I.Dossier ».

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	18/35

3.2 Description des risques

Le tableau suivant détaille les risques identifiés lors de l'analyse.

R.ABUS-AUTORISATION	
Libellé	R.ABUS-AUTORISATION
Méthode d'attaque	39 - ABUS DE DROIT
Description	<p>L'utilisateur est accrédité de certaines autorisations qui lui donnent accès au contenu et à certaines fonctions de l'application. Le contrôle des autorisations, aussi appelé contrôle d'accès, est un dispositif généralement difficile à mettre en oeuvre de manière efficace.</p> <p>Une personne malintentionnée identifie et forge une requête vers une fonction dont le schéma de contrôle d'accès est défectueux. Elle accède par exemple à des fonctionnalités d'administration et modifie des informations au niveau du référentiel afin de provoquer le mécontentement de certaines catégories de personne.</p> <p>Etant donnée la méthode d'attaque employée par l'élément menaçant, les trois critères de sécurité sont touchés.</p> <p>Pour la confidentialité, l'élément essentiel le plus touché est l'information "I_Référentiel".</p> <p>Au niveau de la disponibilité, tous les éléments essentiels sont touchés de manière limitée puisqu'ils présentent un niveau moyen pour ce critère de sécurité.</p> <p>Concernant l'intégrité, la fonction "F.CALCUL" et l'information " I_Référentiel " sont touchées de manière importante.</p> <p>Ce risque peut engendrer :</p> <ul style="list-style-type: none"> • Des frais financiers de secours et de remise à niveau • Une perte d'image de marque • Une interruption de service • Une perturbation du fonctionnement interne

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	19/35

R.ABUS-DEBORDEMENT

Libellé R.ABUS-DEBORDEMENT

Méthode d'attaque 39 - ABUS DE DROIT

Description Cette menace consiste à provoquer un dysfonctionnement au niveau de l'application Web pour lui faire exécuter des opérations non conformes avec des privilèges avancés. Suivant le type de langage utilisé, les applications sont plus ou moins exposées à ce type de menace.

Profitant du manque de filtrage des paramètres d'entrée, une personne malintentionnée soumet une requête qui provoque un débordement de tampon au niveau de l'application Web. Elle lui permet de gagner des privilèges administratifs et de prendre le contrôle d'une des machines support à la téléprocédure.

Etant donnée la nature de ce risque, il peut toucher les trois critères de sécurité.

L'information " I_Référentiel" est la plus touchée car elle présente un besoin important en confidentialité.

Tous les éléments essentiels de la téléprocédure sont touchés avec un niveau moyen pour la disponibilité.

Enfin, ce risque porte atteinte de manière importante à l'intégrité des éléments essentiels "F.CALCUL" et "I_Référentiel".

Cela peut engendrer :

- Des frais financiers de secours et de remise à niveau
- Une infraction aux lois, aux règlements
- Une interruption de service
- Une perte d'image de marque
- Une perturbation de fonctionnement interne

R.ABUS-IDENTITE

Libellé R.ABUS-IDENTITE

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	20/35

Méthode d'attaque 39 - ABUS DE DROIT

Description

Les accréditations de compte et jetons de session présentent des failles exploitables. Une personne malintentionnée, douée de très bonnes connaissances techniques, peut compromettre des clés ou cookies de session afin de prendre connaissance d'informations sensibles.

Etant donné la méthode d'attaque dont est issue ce risque, les trois critères de sécurité sont touchés

Pour la confidentialité, l'information "I_Référentiel" est touchée avec un niveau élevé.

Concernant la disponibilité, toutes les fonctions et informations sont touchées avec un niveau moyen.

Pour l'intégrité, la fonction "F.CALCUL" et l'information "I_Référentiel" sont touchées de manière importante.

Ce risque peut engendrer :

- Des frais financiers de secours et de remise à niveau
- Une infraction aux lois, aux règlements
- Une perte d'image de marque
- Une interruption de service
- Une perturbation du fonctionnement interne

R.ABUS-INJECTION

Libellé R.ABUS-INJECTION

Méthode d'attaque 39 - ABUS DE DROIT

Description

La validation des paramètres d'entrée d'une application Web est capitale. En contournant les filtres de validation, il devient possible d'insérer une commande malveillante et d'attaquer des composants secondaires ou d'exécuter des commandes systèmes.

Une personne malintentionnée dissimule une requête SQL dans l'un des champs d'un formulaire de saisie et visualise, modifie ou efface des tables

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	21/35

du référentiel (Ex: SQL injection).

Au niveau de la confidentialité, si l'on se réfère au scénario émis, l'information "I_Référentiel" est l'élément essentiel le plus touché.

Pour la disponibilité, ce risque porte atteinte à tous les éléments essentiels car ils présentent tous un besoin de sécurité identique (niveau moyen).

Concernant l'intégrité, la fonction "F.CALCUL" et l'information "I_Référentiel" sont touchées de manière importante.

Ce risque peut engendrer :

- Des frais financiers de secours et de remise à niveau
- Une infraction aux lois, aux règlements
- Une perte d'image de marque
- Une interruption de service
- Une perturbation du fonctionnement inter

R.DIVULGATION-STOCKAGE

Libellé R.DIVULGATION-STOCKAGE

Méthode d'attaque 23 - DIVULGATION

Description Etant donnée le manque de classification au niveau de la sensibilité des informations et l'absence de moyens de chiffrement adaptés, toute une série d'informations conservées au niveau de la partie conservation de données sont divulguées. Un dysfonctionnement, une erreur d'administration ou une personne animée par un esprit de vengeance peuvent être à l'origine de cette menace.

Ce risque touche uniquement la confidentialité des éléments essentiels. Le plus touché est l'information "I.Référentiel" qui présente un besoin de sécurité important au niveau de ce critère de sécurité.

Cela peut engendrer :

- Une perte d'image de marque

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	22/35

R.DYSFONCTIONNEMENT-CONCEPTION

Libellé	R.DYSFONCTIONNEMENT-CONCEPTION
Méthode d'attaque	31 - DYSFONCTIONNEMENT LOGICIEL
Description	<p>Etant donné la relative complexité du processus de calcul de pension, une erreur d'implémentation provoque toute une série de dysfonctionnements et par suite le mécontentement des usagers.</p> <p>Conformément aux hypothèses émises lors de l'étude du système cible, il convient de considérer uniquement la perte d'intégrité induite par un dysfonctionnement d'ordre logiciel. Ainsi, ce risque touche principalement l'intégrité de l'information "I.Resultat".</p> <p>Ce risque peut engendrer :</p> <ul style="list-style-type: none"> • Une perte d'image de marque

R.DYSFONCTIONNEMENT-ERREUR

Libellé	R.DYSFONCTIONNEMENT-ERREUR
Méthode d'attaque	31 - DYSFONCTIONNEMENT LOGICIEL
Description	<p>La prise d'empreinte constitue une étape préalable à l'intrusion au sein d'une application Web. Elle consiste à glaner le maximum d'informations sur la cible afin d'entrevoir les possibilités offertes pour mener à bien les attaques. La présence de bannières explicites, le code source des pages, la nature des erreurs de traitement constituent des informations précieuses.</p> <p>Une personne externe, possédant des connaissances approfondies dans le domaine des applications Web, soumet la téléprocédure à des conditions d'utilisation extrêmes afin de générer des erreurs non traitées. Elle prend ainsi connaissance de sa structure interne ou provoque son indisponibilité. Elle obtient par exemple une série de "dumps" de base de données lui permettant de mettre en oeuvre des attaques plus complexes.</p> <p>Ce risque touche la disponibilité et l'intégrité des éléments essentiels.</p> <p>Pour la disponibilité, les éléments essentiels sont tous touchés de manière</p>

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	23/35

identique (niveau moyen).

Au niveau de l'intégrité, ce risque affecte très fortement les éléments essentiels "F.CALCUL" et "I_Référentiel".

Cela peut engendrer :

- Une interruption de services
- Une perte d'image de marque
- Une perturbation du fonctionnement interne

R.GARANTIE-ORIGINE

Libellé R.GARANTIE-ORIGINE

Méthode d'attaque 24 - INFORMATIONS SANS GARANTIE DE L'ORIGINE

Description Une personne malintentionnée, très au fait des techniques d'usurpation d'identité, détourne les communications vers son propre système. Sous couvert de la similitude avec la téléprocédure d'origine, il invite les usagers à décliner leur identité. Le principe d'anonymat n'étant plus respecté, il collecte illicitement des informations personnelles, fiscales.

Au vu du scénario de menace, ce risque touche la confidentialité et la disponibilité des éléments essentiels.

Au niveau de la confidentialité, si cette menace s'accompagne d'une perte d'anonymat, l'information "I.Dossier" est touchée avec un niveau élevé.

Pour la disponibilité, toutes les fonctions et toutes les informations sont touchées avec un niveau identique.

Cela peut engendrer :

- Une atteinte à la vie privée des usagers
- Une infraction aux lois et règlements
- Une perte d'image de marque

R.LOGICIEL-CODE

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	24/35

Libellé	R.LOGICIEL-CODE
Méthode d'attaque	26 - PIÉGEAGE DU LOGICIEL
Description	<p>L'application Web peut être utilisée comme un vecteur d'attaque. En profitant du manque de validation des entrées et sorties de l'application, l'idée consiste à insérer au sein d'un formulaire de saisie des informations qui seront ensuite affichées sans précaution préalable. Ces scripts sont ensuite exécutés de manière transparente au niveau du navigateur des personnes qui visualise la page contenant le script caché.</p> <p>Une personne malintentionnée insère un code malveillant au niveau d'une page Web lui permettant de prendre connaissance de l'identité des usagers qui se connectent et de dérober les informations saisies (fiscales, personnelles).</p> <p>En fonction de la nature du code exécuté, ce risque peut toucher les trois critères de sécurité.</p> <p>Au niveau de la confidentialité, l'information "I_Référentiel" est la plus touchée car elle présente un besoin important au niveau de ce critère. Cependant, si la perte de confidentialité s'accompagne d'une perte d'anonymat, les informations "I.Dossier" et "I.Profil" sont aussi très touchées.</p> <p>Pour la disponibilité, tous les éléments essentiels de la téléprocédure sont touchés avec un niveau moyen.</p> <p>Enfin, ce risque porte atteinte de manière importante à l'intégrité des éléments essentiels "F.CALCUL", "I_Référentiel".</p> <p>Cela peut engendrer :</p> <ul style="list-style-type: none"> • Une atteinte à la vie privée des usagers • Une infraction aux lois, aux règlements • Une perte d'image de marque

R.PERTE-TELECOM

Libellé	R.PERTE-TELECOM
Méthode d'attaque	13 - PERTE DES MOYENS DE TÉLÉCOMMUNICATION

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	25/35

Description	<p>Par vengeance ou motivation personnelle une personne malintentionnée, possédant des connaissances techniques approfondies, rend inaccessible la téléprocédure en rendant indisponible un équipement de l'infrastructure de communication qui présente une mauvaise protection.</p> <p>L'impossibilité de basculer rapidement vers une ligne de secours et l'absence de clauses contractuelles traitant du délai maximum d'indisponibilité aggrave d'autant plus la situation.</p> <p>Ce risque touche la disponibilité des informations. Elles sont toutes touchées avec le même niveau car elles présentent le même besoin.</p> <p>Cela peut engendrer :</p> <ul style="list-style-type: none"> • Une interruption de service • Une perte d'image de marque
-------------	---

R.SATURATION-LOGICIEL

Libellé	R.SATURATION-LOGICIEL
Méthode d'attaque	30 - SATURATION DU SYSTÈME INFORMATIQUE
Description	<p>Par vengeance ou motivation personnelle, une personne malintentionnée, possédant un niveau de compétence élevé, sature le pool de connexion afin d'empêcher les utilisateurs légitimes de se connecter. D'autre part, profitant de l'absence de dispositifs anti-bourrage au niveau du formulaire de saisi, elle peut aussi robotiser leur remplissage afin de générer une charge de traitement importante au niveau du serveur et rendre le système instable.</p> <p>Ce risque touche la disponibilité de tous les éléments essentiels. Ils sont touchés avec le même niveau car ils présentent un besoin identique en sécurité.</p> <p>Cela peut engendrer :</p> <ul style="list-style-type: none"> • Une interruption de service • Une perte d'image de marque

R.TRAITEMENT-ANONYMAT

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	26/35

Libellé	R.TRAITEMENT-ILLICITE
Méthode d'attaque	37 - TRAITEMENT ILLICITE DES DONNÉES
Description	<p>Une personne malintentionnée exploite les journaux de trace ou d'autre éléments lui permettant de lever l'anonymat des simulations. Il prend ainsi connaissance d'informations sensibles (fiscales, personnelles).</p> <p>Etant donné le scénario de menace émis, ce risque touche principalement la confidentialité des informations fournies par l'usager ("I.Dossier").</p> <p>Ce risque peut engendrer :</p> <ul style="list-style-type: none"> • Une atteinte à la vie privée • Une infraction aux lois, aux règlements • Une perte d'image de marque

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	27/35

4 Objectifs de sécurité

O.ANONYMAT

Contenu Des mesures doivent être prises afin de garantir l'anonymat des usagers.

O.AUTORISATION

Contenu Des mesures techniques doivent être prises pour garantir que l'utilisateur accède uniquement aux fonctions et informations autorisées uniquement les droits nécessaires.

O.CHIFFREMENT

Contenu Des mesures cryptographiques adaptées à la sensibilité des informations doivent être prises pour garantir la confidentialité des informations sur les supports.

O.CODE-MALVEILLANT

Contenu Des mesures doivent être prises afin d'empêcher la diffusion des codes malveillants par l'intermédiaire de la téléprocédure.

O.CONCEPTION

Contenu Des mesures doivent être prises afin de s'assurer de la conformité du code et du fonctionnement de la téléprocédure.

O.DEBORDEMENT

Contenu Des mesures techniques doivent être prises afin d'éviter les attaques de type "débordement de tampon".

O.GESTION-ERREUR

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	28/35

Contenu Des mesures doivent être prises afin d'optimiser la gestion des erreurs et les fuites d'informations.

O.IDENTITE

Contenu Des mesures techniques doivent être prises afin de garantir la robustesse du dispositif de gestion des sessions.

O.INJECTION

Contenu Des mesures techniques doivent être prises pour empêcher l'application de véhiculer des commandes malveillantes vers des composants secondaires.

O.ORIGINE

Contenu Des mesures doivent être prises afin de garantir l'authentification d'origine du site et empêcher le détournement des connexions.

O.TELECOM

Contenu Les dysfonctionnements des moyens de télécommunication ne doivent pas entraver la disponibilité de la téléprocédure.

O.SATURATION-RESSOURCES

Contenu Des mesures doivent être prises afin d'empêcher les personnes de consommer volontairement des ressources.

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	29/35

5 Les risques résiduels

5.1 Méthodes d'attaque non retenues

01- INCENDIE

Justification Les méthodes d'attaques d'ordre naturel ont été initialement écartées dans le cadre de cette analyse.

02- DÉGÂTS DES EAUX

Justification Les méthodes d'attaques d'ordre naturel ont été initialement écartées dans le cadre de cette analyse.

03 - POLLUTION

Justification Les méthodes d'attaques d'ordre naturel ont été initialement écartées dans le cadre de cette analyse.

04 - SINISTRE MAJEUR

Justification Les méthodes d'attaques d'ordre naturel ont été initialement écartées dans le cadre de cette analyse.

05 - DESTRUCTION DE MATÉRIELS OU DE SUPPORTS

Justification Conformément aux hypothèses émises, les méthodes d'attaques touchant la sécurité physique des locaux sont écartées.

06 - PHÉNOMÈNE CLIMATIQUE

Justification Les méthodes d'attaques d'ordre naturel ont été initialement écartées dans le cadre de cette analyse.

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	30/35

07 - PHÉNOMÈNE SISMIQUE

Justification Les méthodes d'attaques d'ordre naturel ont été initialement écartées dans le cadre de cette analyse.

08 - PHÉNOMÈNE VOLCANIQUE

Justification Les méthodes d'attaques d'ordre naturel ont été initialement écartées dans le cadre de cette analyse.

09 - PHÉNOMÈNE MÉTÉOROLOGIQUE

Justification Les méthodes d'attaques d'ordre naturel ont été initialement écartées dans le cadre de cette analyse.

10 - CRUE

Justification Les méthodes d'attaques d'ordre naturel ont été initialement écartées dans le cadre de cette analyse.

11 - DÉFAILLANCE DE LA CLIMATISATION

Justification Conformément aux hypothèses émises, les méthodes d'attaques touchant la sécurité physique des locaux sont écartées.

12 - PERTE D'ALIMENTATION ÉNERGÉTIQUE

Justification Conformément aux hypothèses émises, les méthodes d'attaques touchant la sécurité physique des locaux sont écartées.

14 - RAYONNEMENTS ÉLECTROMAGNÉTIQUES

Justification Conformément aux hypothèses émises, les méthodes d'attaques touchant la sécurité physique des locaux sont écartées.

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	31/35

15 - RAYONNEMENTS THERMIQUES

Justification Les méthodes d'attaques d'ordre naturel ont été initialement écartées dans le cadre de cette analyse.

16 - IMPULSIONS ÉLECTROMAGNÉTIQUES

Justification Conformément aux hypothèses émises, les méthodes d'attaques touchant la sécurité physique des locaux sont écartées.

17 - INTERCEPTION DE SIGNAUX PARASITES COMPROMETTANTS

Justification Méthode d'attaque jugée trop improbable.

18 - ESPIONNAGE A DISTANCE

Justification Conformément aux hypothèses émises, la sécurité physique et environnementale au niveau du poste de l'utilisateur est garantie.

19 – ECOUTE PASSIVE

Justification Peu d'intérêt dans le cas de la téléprocédure « Candidature à une offre d'emploi ».

20 - VOL DE SUPPORTS OU DE DOCUMENTS

Justification Conformément aux hypothèses émises, les méthodes d'attaques touchant la sécurité physique des locaux sont écartées.

21 - VOL DE MATÉRIELS

Justification Conformément aux hypothèses émises, les méthodes d'attaques touchant la sécurité physique des locaux sont écartées.

22 - RÉCUPÉRATION DE SUPPORTS RECYCLÉS OU MIS AU REBUS

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	32/35

Justification Conformément aux hypothèses émises, les méthodes d'attaques touchant la sécurité physique et organisationnel sont écartées.

25 - PIÉGEAGE DU MATÉRIEL

Justification Conformément aux hypothèses émises, les méthodes d'attaques touchant la sécurité physique des locaux et équipement sont écartées.

27 - GÉOLOCALISATION

Justification Méthode d'attaque inadaptée dans le cadre de cette téléprocédure.

29 - DYSFONCTIONNEMENT DU MATÉRIEL

Justification Ecartée au profit de la méthode d'attaque "Panne Matérielle".

32 - ATTEINTE À LA MAINTENABILITÉ DU SYSTÈME D'INFORMATION

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

33 - UTILISATION ILLICITE DES MATÉRIELS

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

34 - COPIE FRAUDULEUSE DE LOGICIELS

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

35 - UTILISATION DE LOGICIELS CONTREFAITS OU COPIÉS

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

35 - UTILISATION DE LOGICIELS CONTREFAITS OU COPIÉS

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	33/35

Justification La simulation est réalisée de manière anonyme et l'accès à la téléprocédure est public.

38 - ERREUR D'UTILISATION

Justification Conformément aux hypothèses émises, cette méthode d'attaque est écartée.

39 – RENIEMENT D'ACTION

Justification Sans influence dans le cadre de la téléprocédure « Candidature à une offre d'emploi ».

40 – USURPATION DE DROITS

Justification La simulation est réalisée de manière anonyme et l'accès à la téléprocédure est public.

42 - ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL

Justification Conformément aux hypothèses émises, cette méthode d'attaque est écartée dans le cadre de cette analyse.

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	34/35

5.2 Tableau de couverture des risques par les objectifs

	O.ANONYMAT	O.AUTORISATION	O.CHIFFREMENT	O.CODE-MALVEILLANT	O.CONCEPTION	O.DEBORDEMENT	O.GESTION-ERREUR	O.IDENTITE	O.INJECTION	O.ORIGINE	O.TELECOM	O.SATURATION-RESSOURCES
R.ABUS-AUTORISATION		X										
R.SATURATION-LOGICIEL												X
R.GARANTIE-ORIGINE										X		
R.DIVULGATION-STOCKAGE			X									
R.DYSFONCTIONNEMENT-CONCEPTION					X							
R.DYSFONCTIONNEMENT-ERREUR							X					
R.ABUS-IDENTITE								X				
R.LOGICIEL-CODE				X								
R.ABUS-DEBORDEMENT						X						
R.PERTE-TELECOM											X	
R.ABUS-INJECTION									X			
R.TRAITEMENT-ANONYMAT	X											

FEROS Types		Simulation		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.7.1	V1.0	04/04/2008	Public	35/35