



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



PREMIER MINISTRE
SGDN - DCSSI

=====

FEROS Types

Téléprocédure de référence

Candidature

=====

VERSION V1.0

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	1/45

FEROS Type	
Candidature	
Référence	Date
FEROS Type_CandidatureV1.0.doc	26/04/2006
Identification d'objet (OID)	Racine OID et gestionnaire
1.2.250.1.137.2.2.1.2.3.1.1	DGME/SDAE
Responsable	Version
DGME/SDAE – SGDN\DCSSI	V1.0
Critère de diffusion	Nombre de pages
Public	45

HISTORIQUE DES VERSIONS			
DATE	VERSION	EVOLUTION DU DOCUMENT	REDACTEUR
15/05/2005	0.1	Création du document	Fidens
26/04/2006	1.0	Publication	DCSSI/SDAE

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	2/45

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	6
2.2	DESCRIPTION DES ELEMENTS ESSENTIELS	7
2.3	ENJEUX	12
2.4	HYPOTHESES	13
2.5	ECHELLE DE BESOINS	13
2.6	BESOINS DE SECURITE DES ELEMENTS ESSENTIELS	14
3	LES RISQUES	21
3.1	HIERARCHISATION DES RISQUES	21
3.2	DESCRIPTION DES RISQUES	22
4	OBJECTIFS DE SECURITE	37
5	LES RISQUES RESIDUELS	40
5.1	METHODES D'ATTAQUE NON RETENUES	40
5.2	TABLEAU DE COUVERTURE DES RISQUES PAR LES OBJECTIFS.....	44

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	3/45

1 Introduction

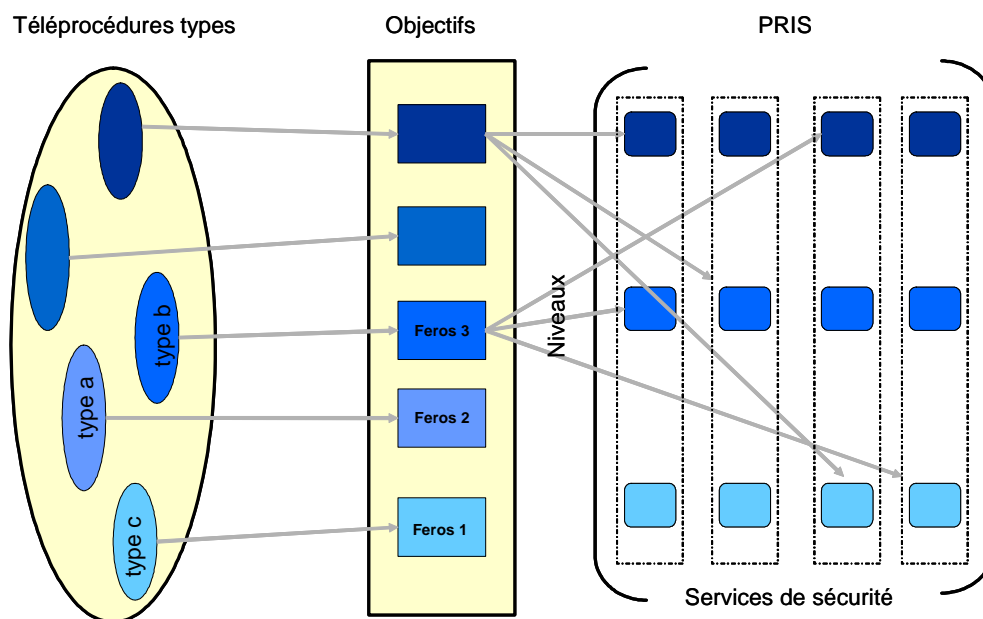
1.1 Contexte général

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 Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	4/45

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 « démarche en ligne : candidature ».

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 Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	5/45

2 Description du système étudié

Cette téléprocédure offre aux Internautes la possibilité d'effectuer une candidature par Internet. La candidature nécessite la plupart du temps une phase d'adhésion. Elle comporte en général des informations de nature confidentielle (médicales, sociales, financières ou fiscales) renseignées dans le dossier accompagnant la candidature.

Exemples de mise en œuvre

Candidature dans l'enseignement supérieur

Candidature au permis de conduire

Candidature à une offre d'emploi (annonce de l'ANPE)

Candidature au conseil des prud'hommes

Candidature à des concours de la fonction publique

Scénario retenu pour l'analyse

DESCRIPTION

Au titre de la téléprocédure type, on retiendra la candidature à une offre d'emploi, réalisée par un particulier.

USAGER

- Particulier

MODE OPERATOIRE

- Accès depuis les moyens informatiques propres de l'utilisateur

DOMAINE D'APPLICATION

- Social

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 le service de candidature à une offre d'emploi.

Systeme-cible

Présentation

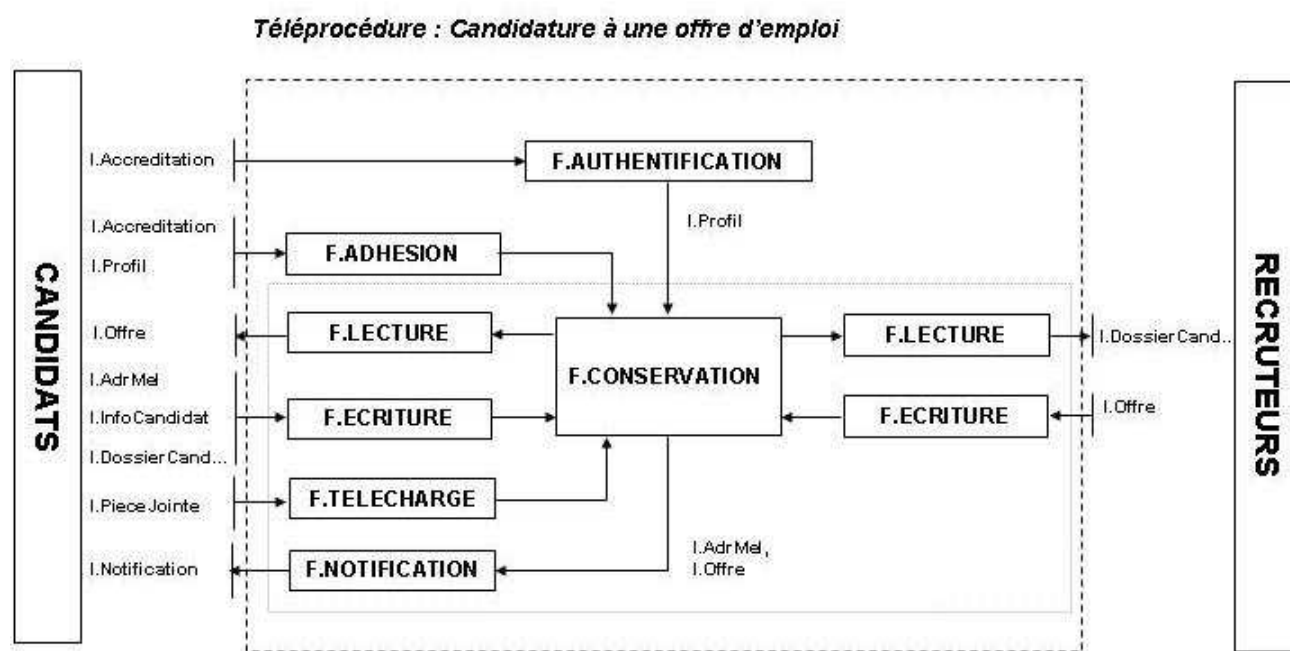
La téléprocédure « Candidature à une offre d'emploi » est destinée à faciliter la relation entre recruteurs et candidats. Elle permet d'améliorer la diffusion des offres et de simplifier la phase d'instruction des candidatures.

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	6/45

Le portail met à disposition des usagers, une liste d'offres alimentées et mises à jour par les recruteurs. Elles peuvent être consultées en ligne ou, si le candidat est inscrit et a renseigné ses préférences, envoyées directement par mèl.

Les candidatures sont réalisées via un formulaire unique de saisie qui facilite la gestion des éléments du dossier et, le cas échéant, permet de joindre des pièces dématérialisées. Les demandes valides sont alors traitées et directement présentées au recruteur. La suite donnée est notifiée au candidat par l'intermédiaire de son adresse mèl, par courrier...

2.2 Description des éléments essentiels



Fonction : F.AUTHENTIFICATION

Description

La sous fonction « F-AUTHENTIFICATION » n'est pas un préalable systématique à l'accès à la téléprocédure. Elle permet l'utilisation de fonctionnalités avancées disponibles aux seuls utilisateurs inscrits.

Ainsi, elle assure le contrôle des accréditations des usagers et, en cas de succès, leur permet d'accéder à un espace personnalisé.

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	7/45

Fonction : F.CONSERVATION

Description

Cette fonction est chargée de l'ensemble de la problématique de conservation des informations. Dans le cadre de la téléprocédure "Candidature à une offre d'emploi", les données spécifiques stockées sont :

- Les informations des candidats inscrits (voir « I.InfoCandidat »)
- Les offres d'emplois disponibles (voir « I.Offre »)
- Les dossiers de candidature (voir « I.DossierCandidature »)
- Les pièces jointes aux dossiers de candidature (voir « I.PieceJointe »)

Les différents acteurs n'agissent pas directement sur la partie conservation de donnée. Ils accèdent aux informations par l'intermédiaire des fonctions « F.LECTURE » et « F.ECRITURE » conformément aux autorisations fixées.

Fonction : F.ECRITURE

Description

Cette fonction permet de soumettre de l'information en agissant directement sur la partie conservation de données. Le chargement du contexte applicatif fixe les autorisations qui s'appliquent sur la base des notions de groupe et d'identité.

Elle est utilisée par les recruteurs qui rédigent de nouvelles offres et alimentent le back office. Pour les candidats, elle supporte la notion de formulaire de saisie qui permettent de:

- Renseigner ses données personnelles
- Déposer une candidature

Un contrôle de cohérence approprié est effectué lors de la saisie d'informations liées à la validité du dossier ou des traitements.

Fonction : F.ADHESSION

Description

Dans le cadre de la téléprocédure « Candidature à une offre d'emploi », la phase d'inscription est optionnelle. L'accès aux offres peut aussi se faire de manière anonyme puisque le candidat est amené à décliner son identité au sein du formulaire de candidature.

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	8/45

Cette fonction est donc mise en œuvre comme support au suivi des dossiers de candidature et offre des fonctionnalités de personnalisation de l'environnement en garantissant la persistance des préférences de l'utilisateur.

Ainsi, le candidat est par exemple en mesure de :

- Déposer des pièces jointes de manière permanente sur le serveur.
- S'abonner à la liste de diffusion.
- Créer des agents de recherche afin de simplifier ses démarches.
- Suivre l'état de ses candidatures.

L'ensemble de ces fonctionnalités apporte un gain d'efficacité dans la mesure où le candidat est susceptible de multiplier les demandes.

Fonction : F.LECTURE

Description

Cette fonction de présentation permet à l'administration de soumettre de l'information aux usagers. Elle est mise en œuvre pour présenter :

- Les informations issues d'un traitement (erreurs, validations)
- Les informations statiques (formulaire, Aide en ligne)
- Les informations usagers (Offres, Dossiers)

Le chargement du contexte applicatif (voir « I.Profil ») permet de restreindre les informations accessibles au niveau de la partie conservation de données en fonction du rôle et des préférences des usagers.

Ainsi, en suivant le principe de la téléprocédure, les candidats sont en mesure de visualiser l'ensemble des offres d'emploi. De leur côté, les recruteurs prennent connaissance des candidatures portant sur leurs offres.

Fonction : F.NOTIFICATION

Description

Cette fonction permet d'automatiser l'envoi des offres d'emploi par messagerie électronique. Elle peut être considérée comme un gestionnaire de liste de diffusion et permet de notifier les usagers inscrits en fonction de leurs critères de recherche.

Ce processus est réalisé automatiquement dès l'édition de l'offre par le recruteur.

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	9/45

Fonction : F.TELECHARGEMENT

Description Cette fonction permet au candidat de joindre des documents dématérialisés (CV, lettre de motivation) à sa demande. Il les rend disponible au recruteur par « Upload » sur le serveur de l'administration. D'un point de vue technique, le procédé est comparable à celui utilisé habituellement au niveau de la messagerie électronique.

Information : I.Accreditations

Description Couple d'informations de type « identifiant/mot de passe » préalablement définis par l'utilisateur lors de la phase d'inscription. Il permet à ce dernier d'accéder à son espace personnel.

Information : I.AdrMel

Description Adresse mèl du candidat. Cette information permet d'alimenter la liste de diffusion ou d'établir la relation entre le recruteur et le candidat en cas de réponse positive.

Information : I.DossierCandidature

Description Cet élément essentiel constitue la réponse d'un candidat à une offre mise en ligne sur le portail. Il contient plusieurs types d'informations :

- Des informations personnelles portant sur le candidat (Identité, Adresse,...)
- La réponse à l'annonce (Cursus, Motivation,...)
- Des pièces jointes

Les informations sont ensuite présentées au recruteur qui décide de la suite à donner au dossier. Le cas échéant, il peut prendre contact (mèl ou courrier) avec le candidat en utilisant les informations contenues dans le dossier.

Si la suite à donner est défavorable, les informations de suivi de dossier du candidat sont mises à jour par le recruteur puis le dossier est classé et archivé.

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	10/45

Information : I.InfoCandidat

Description

Cet élément essentiel regroupe toute une série d'informations permettant au candidat de postuler plus facilement et d'améliorer la recherche des offres correspondant à ses critères.

Ces informations sont définies lors de la phase d'inscription et sont à tout moment modifiables par l'utilisateur. Elles regroupent :

- L'identité du candidat
- La liste de ses pièces jointes
- Le suivi de ses candidatures
- Ses préférences de navigation et de recherches

Le but est de diminuer le temps nécessaire à l'instruction des dossiers en évitant la ressaisie d'informations ou le téléchargement de nouveaux fichiers entre chaque candidature.

Information : I.NotificationOffre

Description

Mèl de notification envoyé au candidat lorsqu'un recruteur rédige une offre qui correspond à ses critères de recherche. Les informations contenues dans le mèl de notification sont identiques à celles de l'élément essentiel « I.Offre ».

Information : I.Offre

Description

Ensemble des informations contenues dans l'offre. Elle est rédigée par le recruteur et contient plusieurs types d'informations :

- Un descriptif de l'emploi
- La date limite de dépôt des candidatures
- Le profil du candidat (mots clés)
- Une référence unique

Chaque nouvelle offre vient enrichir la liste des offres existantes. Dès que la date limite de dépôt est dépassée, l'offre est rendue inaccessible de sorte qu'aucune candidature ne peut plus être déposée.

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	11/45

Information : I.PieceJointe

Description Pièce dématérialisée jointe au dossier de candidature par l'intermédiaire de la fonction "F.TELECHARGEMENT". Il s'agit généralement d'un Curriculum Vitae ou d'une lettre de motivation.

Information : I.Profil

Description Cette information fixe les autorisations d'accès qui s'appliquent au contenu et aux fonctions de la téléprocédure. Ces restrictions touchent la majorité des fonctions et permettent d'identifier les données accessibles en lecture et en écriture au niveau de la partie « conservation de données ».

En cas d'inscription et sous condition de la validité des accréditations, le profil offre la possibilité à l'utilisateur de charger ses préférences et d'accéder à ses données personnelles.

Information : I.Requete

Description Requête initiale indiquant la ressource à laquelle l'utilisateur souhaite accéder.

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 Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	12/45

Description Cette téléprocédure s'inscrit dans le projet de modernisation des services administratifs et vise à simplifier les nombreuses démarches actuelles.

2.4 Hypothèses

H.CONFIANCE

Description Dans le cadre de cette analyse, il sera 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.

2.5 Echelle de besoins



FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	13/45

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.

2.6 Besoins de sécurité des éléments essentiels

Dans le contexte de la « démarche en ligne candidature à une offre d'emploi », les besoins en disponibilité sont limités, du fait qu'il n'est pas fait habituellement état d'une date d'échéance impérative. Par contre, dans la plupart des candidatures, cette notion de date de fin de dépôt est présente et doit impérativement être prise en compte. En conséquence, nous avons globalisé le besoin de sécurité en disponibilité et considéré celui-ci comme plus élevé que dans le seul contexte de la candidature à une offre d'emploi.

		Besoin de sécurité	Commentaires
--	--	--------------------	--------------

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	14/45

F.AUTHENTIFICATION	Confidentialité	0	Aucun besoin de confidentialité au niveau de cet élément essentiel.
	Disponibilité	1	Le besoin en disponibilité est faible puisque cette fonction permet uniquement l'accès à des fonctionnalités avancées et n'interdit pas le fonctionnement standard de la procédure. Une indisponibilité ne provoque pas de dysfonctionnement majeur.
	Intégrité	1	Le besoin en intégrité est faible puisque cette fonction permet uniquement de charger un profil personnalisé afin de faciliter la navigation.
F.CONSERVATION	Confidentialité	0	Aucun besoin de confidentialité au niveau de cet élément essentiel.
	Disponibilité	2	Le besoin en disponibilité est élevé car la fonction conserve les informations nécessaires au traitement des candidatures.
	Intégrité	2	Une perte d'intégrité serait très préjudiciable car la majorité des informations sont stockées par cette fonction.
F.ECRITURE	Confidentialité	0	Aucun besoin de confidentialité au niveau de cet élément essentiel.
	Disponibilité	2	Le besoin en disponibilité est élevé puisque les demandes sont soumises à une date limite de dépôt. Une indisponibilité de quelques heures est cependant acceptable.
	Intégrité	2	Une perte d'intégrité est grave car elle peut influencer la validité des dossiers de candidature.
F.ADHESION	Confidentialité	0	Aucun besoin de confidentialité au niveau de cet élément essentiel.

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	15/45

	Disponibilité	1	Le besoin en disponibilité est faible puisque cette fonction permet uniquement au candidat de s'inscrire afin d'accéder à des fonctionnalités avancées.
	Intégrité	1	Le besoin est faible car une perte d'intégrité n'influence pas la consultation des offres et le dépôt des dossiers.
F.LECTURE	Confidentialité	0	Aucun besoin de confidentialité au niveau de cet élément essentiel.
	Disponibilité	2	Le besoin en disponibilité est élevé puisque les demandes sont soumises à une date limite de dépôt. Une indisponibilité de quelques heures est cependant acceptable dans la mesure où le candidat dispose généralement d'un laps de temps assez important.
	Intégrité	2	Une perte d'intégrité est grave dans la mesure où cette fonction de présentation permet au candidat de prendre connaissance des offres disponibles. Une indisponibilité de quelques heures est cependant acceptable.
F.NOTIFICATION	Confidentialité	0	Aucun besoin de confidentialité au niveau de cet élément essentiel.
	Disponibilité	1	Le besoin est moyen car l'indisponibilité ne provoque aucun dysfonctionnement majeur. Les offres sont toujours accessibles en se connectant directement sur le portail.
	Intégrité	2	Une perte d'intégrité au niveau de la fonction de notification est grave car elle peut engendrer des dysfonctionnements importants au niveau de la téléprocédure.
F.TELECHARGEMENT	Confidentialité	0	Aucun besoin de confidentialité au niveau de cet élément essentiel.
	Disponibilité	2	Le besoin en disponibilité est important

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	16/45

			car il est quelquefois obligatoire de mettre à disposition du recruteur certaines pièces dématérialisées.
	Intégrité	2	Une perte d'intégrité au niveau de cet élément essentiel est grave car elle peut remettre en question la validité de certaines candidatures.
I.Accreditations	Confidentialité	2	En théorie, le besoin en confidentialité au niveau des accréditations peut être considéré comme moyen puisque ces informations permettent uniquement d'accéder à des fonctionnalités avancées (Suivi des candidatures, Gestion des pièces jointes ...). Dans la pratique, en fonction de la nature de l'inscription, une perte de confidentialité peut induire une atteinte importante à la vie privée.
	Disponibilité	1	La perte des accréditations est tolérable puisque le candidat peut généralement les récupérer via une procédure spécifique. De plus, l'utilisateur peut toujours accéder au portail anonymement.
	Intégrité	1	Une perte d'intégrité est tolérable puisque le candidat peut généralement les récupérer via une procédure spécifique.
I.AdrMel	Confidentialité	1	L'adresse mèl du candidat est une information personnelle qui présente des besoins limités en confidentialité.
	Disponibilité	1	Le besoin en disponibilité est moyen puisque l'adresse mèl permet uniquement l'envoi des mèls de notification.
	Intégrité	1	Le besoin en intégrité est moyen puisque l'adresse mèl permet uniquement l'envoi des mèls de notification.
I.DossierCandidature	Confidentialité	1	Les dossiers peuvent contenir des informations personnelles qui ne doivent

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	17/45

			<p>pas être divulguées à des tiers sans le consentement du candidat.</p> <p>Cependant, dans la majorité des cas les données du dossier de candidature ne présentent pas un niveau de confidentialité très important.</p>
	Disponibilité	2	Les candidatures doivent être déposées avant la date de fin de dépôt. Etant donné le laps de temps dont dispose le candidat, une indisponibilité de quelques heures est cependant tolérable.
	Intégrité	3	Afin d'être valide, le dossier de candidature doit demeurer parfaitement intègre.
I.InfoCandidat	Confidentialité	1	Le besoin en confidentialité est identique à celui émis pour "I.DossierCandidature" puisque cet élément essentiel contient les informations personnelles des usagers inscrits sur le portail.
	Disponibilité	1	Une indisponibilité de cet élément essentiel est tolérable car le candidat peut éventuellement ressaisir ses informations manuellement pour constituer son dossier de candidature.
	Intégrité	3	Une perte d'intégrité au niveau des informations des candidats est grave puisqu'elle peut par suite toucher la validité des dossiers déposés.
I.NotificationOffre	Confidentialité	0	Le besoin en confidentialité au niveau de cet élément essentiel est nul puisque les mails de notification contiennent uniquement un récapitulatif des offres.
	Disponibilité	1	Le besoin en disponibilité est directement lié à celui que présente la fonction "F.NOTIFICATION".
	Intégrité	1	Le besoin en intégrité est moyen car en cas de problème le candidat peut consulter l'offre en se connectant

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	18/45

			directement sur le portail.
I.Offre	Confidentialité	0	Le besoin en confidentialité au niveau de cet élément essentiel est nul car l'accès aux différentes offres est public.
	Disponibilité	2	Une indisponibilité est grave puisqu'elle empêche les candidats de postuler. Elle est cependant tolérable si elle est inférieure à quelques heures.
	Intégrité	2	Une perte d'intégrité est grave car elle peut rendre impossible la consultation de l'offre.
I.PieceJointe	Confidentialité	1	Les pièces jointes peuvent contenir des informations personnelles qui ne doivent pas être divulguées à des tiers sans le consentement du candidat.
	Disponibilité	2	Cet élément essentiel présente le même besoin en disponibilité que le dossier de candidature.
	Intégrité	2	Le besoin en intégrité est élevé puisque la pièce jointe peut être un élément important du dossier de candidature.
I.Profil	Confidentialité	2	Le besoin en confidentialité au niveau du profil est important car il définit l'identité et les autorisations associées aux candidats.
	Disponibilité	2	Le dépôt des candidatures est soumis à des contraintes d'ordre calendaire strictes. L'indisponibilité de cet élément essentiel empêche les usagers d'accéder à la téléprocédure. Elle ne doit donc pas être supérieure à quelques heures.
	Intégrité	2	Le besoin en intégrité est important car cet élément essentiel fixe les droits d'accès aux fonctions et aux données.
I.Requete	Confidentialité	0	Le besoin en confidentialité est nul.
	Disponibilité	0	Aucun besoin en disponibilité.

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	19/45

	Intégrité	0	Aucun besoin en intégrité
--	-----------	---	---------------------------

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	20/45

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

	Critère de sécurité	Opportunité
R.USURPATION-IDENTITE	3	4
R.ORIGINE-NOTIFICATION	3	4
R.DIVULGATION-STOCKAGE	3	3
R.ABUS-AUTORISATION	3	3
R.ORIGINE-GARANTIE	3	3
R.LOGICIEL-PIECE_JOINTE	3	3
R.ABUS-INJECTION	3	2
R.ABUS-IDENTIFICATION	3	2
R.DYSFONCTIONNEMENT-ERREUR	3	2
R.LOGICIEL-CODE	3	2
R.LOGICIEL-FONCTION_CACHEE	3	1
R.ALTERATION-CANAL	3	1
R.ABUS-DEBORDEMENT	3	1
R.PANNE-INTEGRITE	2	3
R.SATURATION-SPAM	2	3
R.SATURATION-RESSOURCES	2	3

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	21/45

R.SATURATION-PIECE_JOINTE	2	2
R.TELECOM-PERTE	2	1
R.DIVULGATION-MAILING	2	1

Suivant la nature des téléprocédures de candidature, les informations stockées peuvent présenter un besoin en confidentialité supérieur. Afin de globaliser la hiérarchisation, le niveau du risque « R.DIVULGATION-STOCKAGE » a été volontairement augmenté par rapport à son niveau original dans la procédure « candidature à une offre d'emploi », qui sert de référence à l'analyse.

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 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.

Une personne malintentionnée identifie et forge une requête vers une fonction dont le schéma de contrôle d'accès est défectueux. Il accède alors à des fonctionnalités réservées aux recruteurs, à des informations sur les dossiers des autres candidats.

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

Pour la confidentialité, l'élément essentiel le plus touché est l'information "I.Accréditation". Les informations "I.InfoCandidat", "I.DossierCandidature", "I.PieceJointe", "I.Profil" sont impactées de manière moins importante (niveau moyen).

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	22/45

Au niveau de la disponibilité, il s'agit des fonctions "F.CONSERVATION", "F.LECTURE", "F.ECRITURE", "F.TELECHARGEMENT" ainsi que les informations "I.PieceJointe", "I.DossierCandidature", "I.Offre", "I.Profil".

Concernant l'intégrité, les éléments essentiels très fortement touchés sont les informations "I.DossierCandidature", "I.InfoCandidat". Les informations "I.Offre", "I.PieceJointe", "I.Profil" et les fonctions "F.CONSERVATION", "F.LECTURE", "F.ECRITURE", "F.NOTIFICATION", "F.TELECHARGEMENT" sont aussi touchées de manière importante.

Ce risque peut engendrer :

- Une atteinte à la vie privée
- Des frais financiers de secours et de remise à niveau
- Une interruption de service
- Une perturbation du fonctionnement interne

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 de la machine support à la téléprocédure.

Les trois critères de sécurité sont touchés par ce risque.

L'élément essentiel le plus fortement touché au niveau de la confidentialité est l'information "I.Accréditation". Les informations "I.InfoCandidat", "I.DossierCandidature", "I.PieceJointe", "I.Profil" sont impactées de

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	23/45

manière moins importante (niveau moyen).

Au niveau de la disponibilité, il s'agit des éléments essentiels "F.CONSERVATION", "F.LECTURE", "F.ECRITURE", "F.TELECHARGEMENT", "I.PieceJointe", "I.DossierCandidature", "I.Offre", "I.Profil".

Concernant l'intégrité, les éléments essentiels très fortement touchés sont les informations "I.DossierCandidature", "I.InfoCandidat". Les informations "AdrMèl", "I.Offre", "I.PieceJointe", "I.Profil" et les fonctions "F.CONSERVATION", "F.LECTURE", "F.ECRITURE", "F.NOTIFICATION", "F.TELECHARGEMENT" sont aussi touchées de manière importante.

Ce risque peut engendrer :

- Une atteinte à la vie privée
- Frais financiers de secours et de remise à niveau
- Une interruption de service
- Une perturbation du fonctionnement interne

R.ABUS-IDENTIFICATION

Libellé R.ABUS-IDENTIFICATION

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 les mots de passe (Force Brute), des clés ou cookies de session afin de prendre connaissance des candidatures des autres usagers ou accéder à leurs espaces personnels.

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

Pour la confidentialité, l'élément essentiel le plus touché est l'information "I.Accréditation". Les informations "I.InfoCandidat", "I.DossierCandidature", "I.PieceJointe", "I.Profil" sont impactées de manière moins importante (niveau moyen).

Les fonctions "F.CONSERVATION", "F.LECTURE", "F.ECRITURE",

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	24/45

"F.TELECHARGEMENT" ainsi que les informations "I.PieceJointe", "I.DossierCandidature", "I.Offre", "I.Profil" sont fortement touchées au niveau de la disponibilité.

Pour l'intégrité, les éléments essentiels très fortement touchés sont les informations "I.DossierCandidature", "I.InfoCandidat". Les informations "I.Offre", "I.PieceJointe", "I.Profil" et les fonctions "F.CONSERVATION", "F.LECTURE", "F.ECRITURE", "F.NOTIFICATION", "F.TELECHARGEMENT" sont aussi touchées de manière importante car elles présentent aussi des besoins de sécurité importants.

Ce risque peut engendrer :

- Une atteinte à la vie privée
- Des frais financiers de secours et de remise à niveau
- Une interruption de service
- Une perturbation du fonctionnement interne

Opportunité

Moyennement probable ou nécessite un certain niveau d'expertise et/ou du matériel spécifique

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 la table contenant les candidatures des usagers (Ex: SQL injection).

Ce risque touche les trois critères de sécurité.

Pour la confidentialité, l'élément essentiel principalement touché est l'information "I.Accréditation". Les informations "I.InfoCandidat", "I.DossierCandidature", "I.PieceJointe", "I.Profil" sont impactées de

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	25/45

manière moins importante (niveau moyen).

Au niveau de la disponibilité, il s'agit des fonctions "F.CONSERVATION", "F.LECTURE", "F.ECRITURE", "F.TELECHARGEMENT" ainsi que les informations "I.PieceJointe", "I.DossierCandidature", "I.Offre", "I.Profil".

Concernant l'intégrité, les éléments essentiels très fortement touchés sont les informations "I.DossierCandidature", "I.InfoCandidat". Les informations "I.Offre", "I.PieceJointe", "I.Profil" et les fonctions "F.CONSERVATION", "F.LECTURE", "F.ECRITURE", "F.NOTIFICATION", "F.TELECHARGEMENT" sont aussi touchées de manière importante.

Ce risque peut engendrer :

- Une atteinte à la vie privée
- Des frais financiers de secours et de remise à niveau
- Une interruption de service
- Une perturbation du fonctionnement interne

R.ALTERATION-CANAL

Libellé R.ALTERATION-CANAL

Méthode d'attaque 36 - ALTÉRATION DES DONNÉES

Description Cette menace consiste à modifier illicitement les données en transit sur le medium de communication. Une personne malintentionnée, disposant d'un point d'accès illicite au niveau de la liaison entre l'utilisateur et l'administration, modifie les dossiers de candidature. Il peut ainsi espérer favoriser sa candidature en perturbant la transmission des autres dossiers.

Ce risque porte uniquement atteinte à la confidentialité et l'intégrité des informations qui transite entre l'utilisateur et l'administration.

Au niveau de la confidentialité, les éléments essentiels les plus durement touchés sont ceux qui présentent le plus fort besoin. Dans le cadre de la téléprocédure "Candidature à une offre d'emploi", Il s'agit principalement de l'information "I.Accréditation". Les informations "I.InfoCandidat", "I.DossierCandidature", "I.PieceJointe", "I.Profil" sont impactées de manière moins importante.

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	26/45

Pour l'intégrité, les éléments essentiels très fortement touchés sont les informations "I.DossierCandidature", "I.InfoCandidat". Les informations "AdrMèl", "I.Offre", "I.PieceJointe", "I.Profil" sont aussi touchées de manière importante mais présentent un besoin qui est légèrement moins important.

Cela peut engendrer :

- Une atteinte à la vie privée des usagers
- Une infraction aux lois et règlements

R.DIVULGATION-MAILING

Libellé R.DIVULGATION-MAILING

Méthode d'attaque 23 - DIVULGATION

Description Profitant d'un défaut d'implémentation ou d'une erreur de configuration du logiciel de mailing, une personne malintentionnée obtient la liste des adresses mèl des personnes inscrites au niveau du portail. Cette liste peut par exemple être utilisée afin de faire pression sur les différents candidats ou diffuser illicitement du contenu.

Etant donné le scénario de menace émis, seule la confidentialité des informations "I.AdrMèl" et "InfoCandidat" est touchée.

Cela peut engendrer :

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

R.DIVULGATION-STOCKAGE

Libellé R.DIVULGATION-STOCKAGE

Méthode d'attaque 23 - DIVULGATION

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	27/45

Description	<p>Etant donné le manque de classification au niveau de la sensibilité des informations et l'absence de moyens de chiffrement adaptés, toute une série d'informations personnelles relatives aux dossiers de candidatures des usagers 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.</p> <p>Ce risque porte uniquement atteinte à la confidentialité des éléments essentiels. L'information "I.Accreditation" est très touchée tandis que "I.InfoCandidat", "I.DossierCandidature", "I.PieceJointe", "I.Profil" sont impactés de manière moins importante.</p> <p>Ce risque peut engendrer :</p> <ul style="list-style-type: none"> • Une atteinte à la vie privée des usagers • Une infraction aux lois et règlements • 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 les plus touchés sont "F.CONSERVATION", "F.LECTURE", "F.ECRITURE", "F.TELECHARGEMENT", "I.PieceJointe", "I.DossierCandidature", "I.Offre" et "I.Profil".</p>

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	28/45

Pour l'intégrité, les éléments essentiels "I.DossierCandidature", "I.InfoCandidat" sont très fortement touchés. D'autre part, il touche également les fonctions "F.CONSERVATION", "F.LECTURE", "F.ECRITURE", "F.TELECHARGEMENT", "F.NOTIFICATION" et les informations "I.Offre", "I.PieceJointe", "I.Profil" ayant un besoin en intégrité élevé.

Cela peut engendrer :

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

R.LOGICIEL-CODE

Libellé R.LOGICIEL-CODE

Méthode d'attaque 26 - PIÉGEAGE DU LOGICIEL

Description 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.

Une personne malintentionnée insère un code malveillant au niveau de son dossier lui permettant de dérober des informations sensibles, de provoquer un dysfonctionnement ou encore d'installer un cheval de troie au niveau du poste du recruteur.

Par vengeance ou motivation personnelle, une personne malintentionnée peut aussi profiter d'une vulnérabilité logicielle en insérant du code malveillant au niveau des offres d'un recruteur. Il peut ainsi espérer perturber la campagne de recrutement.

Suivant la nature des codes, ce risque touche les trois critères de sécurité.

L'information "I.Accreditation" est très fortement touchée au niveau de la confidentialité. D'autre part, les informations "I.InfoCandidat", "I.DossierCandidature", "I.PieceJointe", "I.Profil" sont affectées avec une intensité légèrement moins importante.

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	29/45

Pour la disponibilité, les éléments essentiels "F.CONSERVATION", "F.LECTURE", "F.ECRITURE", "F.TELECHARGEMENT", "I.PieceJointe", "I.DossierCandidature", "I.Offre", "I.Profil" possèdent des besoins importants susceptibles d'être impactés.

Enfin, ce risque porte atteinte de manière très importante à l'intégrité des éléments essentiels "I.DossierCandidature", "I.InfoCandidat". D'autre part, il touche les fonctions "F.CONSERVATION", "F.LECTURE", "F.ECRITURE", "F.TELECHARGEMENT", "F.NOTIFICATION" et les informations "I.Offre", "I.PieceJointe", "I.Profil" ayant un besoin en intégrité élevé.

Cela peut engendrer :

- Une atteinte à la vie privée des usagers
- Une perte d'image de marque
- Une perturbation de fonctionnement de tiers
- Une perturbation du fonctionnement interne

R.LOGICIEL-FONCTION_CACHEE

Libellé R.LOGICIEL-FONCTION_CACHEE

Méthode d'attaque 26 - PIÉGEAGE DU LOGICIEL

Description Une personne malintentionnée utilise des fonctionnalités cachées introduites durant la phase de conception de l'application afin de favoriser sa candidature. Elle peut par exemple être en mesure de visualiser, modifier ou encore supprimer illicitement des demandes effectuées par d'autres candidats.

Au niveau de la confidentialité, l'information "I.Accreditation" est très fortement touchée. D'autre part, les informations "I.InfoCandidat", "I.DossierCandidature", "I.PieceJointe", "I.Profil" sont affectées avec une intensité légèrement moins importante.

Pour la disponibilité, les éléments essentiels "F.CONSERVATION", "F.LECTURE", "F.ECRITURE", "F.TELECHARGEMENT", "I.PieceJointe", "I.DossierCandidature", "I.Offre", "I.Profil" sont fortement affectés.

Enfin, ce risque porte atteinte de manière très importante à l'intégrité des

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	30/45

éléments essentiels "I.DossierCandidature", "I.InfoCandidat". Les fonctions "F.CONSERVATION", "F.LECTURE", "F.ECRITURE", "F.TELECHARGEMENT", "F.NOTIFICATION" et les informations "I.Offre", "I.PieceJointe", "I.Profil" présente aussi un besoin en intégrité élevé.

Ce risque peut engendrer :

- Une atteinte à la vie privée des usagers
- Une infraction aux lois et règlements
- Des poursuites judiciaires et pénalité

R.LOGICIEL-PIECE_JOINTE

Libellé R.LOGICIEL-PIECE_JOINTE

Méthode d'attaque 26 - PIÉGEAGE DU LOGICIEL

Description Profitant de la faiblesse du dispositif de filtrage des pièces jointes, une personne malintentionnée insère un fichier piégé dans son dossier afin de provoquer un dysfonctionnement au niveau du poste du recruteur.

Suivant la nature du fichier, les trois critères de sécurité peuvent être touchés.

L'élément essentiel le plus fortement touché au niveau de la confidentialité est l'information "I.Accréditation". Les informations "I.InfoCandidat", "I.DossierCandidature", "I.PieceJointe", "I.Profil" sont impactés de manière moins importante (niveau moyen).

Au niveau de la disponibilité, il s'agit des éléments essentiels "F.CONSERVATION", "F.LECTURE", "F.ECRITURE", "F.TELECHARGEMENT", "I.PiceJointe", "I.DossierCandidature", "I.Offre", "I.Profil".

Concernant l'intégrité, les éléments essentiels "I.DossierCandidature", "I.InfoCandidat" sont très fortement touchés. Les informations "I.Offre", "I.PieceJointe", "I.Profil" et les fonctions "F.CONSERVATION", "F.LECTURE", "F.ECRITURE", "F.NOTIFICATION", "F.TELECHARGEMENT" sont aussi touchées de manière importante.

Il peut engendrer :

- Une atteinte à la vie privée des usagers

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	31/45

- Frais financiers de secours et de remise à niveau
- Infraction aux lois, aux règlements

R.ORIGINE-GARANTIE

Libellé R.ORIGINE-GARANTIE

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 utilisateurs à remplir un dossier de candidature factice ou prend connaissance de leurs accréditations. De cette manière, il peut par exemple espère favoriser sa candidature en limitant le nombre de dossier reçu par l'administration.

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

Au niveau de la confidentialité, c'est l'information "I.Accrediation" qui est touchée avec le niveau le plus élevé. En effet, elle présente un besoin élevé sur ce critère de sécurité.

Pour la disponibilité, les informations "I.DossierCandidature", "I.Offre" sont très touchées car elles sont soumises à des contraintes strictes d'ordre calendaire.

Cela peut engendrer :

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

R.ORIGINE-NOTIFICATION

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	32/45

Libellé	R.ORIGINE-NOTIFICATION
Méthode d'attaque	24 - INFORMATIONS SANS GARANTIE DE L'ORIGINE
Description	<p>Le protocole d'échange de courrier électronique n'impose pas de principe formel d'identification de l'expéditeur. Profitant de cette lacune, une personne malintentionnée diffuse de fausses notifications sous couvert de l'identité du site de l'administration. Il peut par exemple procéder à la désinformation des candidats afin de favoriser sa candidature.</p> <p>Etant donné le scénario émis, ce risque touche uniquement l'intégrité. Il affecte l'information "I.Notification" avec un niveau moyen.</p> <p>Cela peut engendrer :</p> <ul style="list-style-type: none"> • Une infraction aux lois, aux règlements

R.PANNE-INTEGRITE

Libellé	R.PANNE-INTEGRITE
Méthode d'attaque	28 - PANNE MATÉRIELLE
Description	<p>Suite à la panne de l'un des équipements matériels ou à un dysfonctionnement logiciel, il s'établit une perte de cohérence au niveau des dossiers en cours de saisie. Les candidats se trouvent alors dans l'impossibilité d'y réaccéder afin de réaliser des modifications.</p> <p>Il convient de considérer uniquement la perte d'intégrité induite par une panne matérielle. Ainsi, ce risque touche très fortement l'intégrité des informations stockées "I.DossierCandidature", "I.InfoCandidature".</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 perturbation du fonctionnement interne

R.SATURATION-PIECE_JOINTE

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	33/45

Libellé	R.SATURATION-PIECE_JOINTE
Méthode d'attaque	30 - SATURATION DU SYSTÈME INFORMATIQUE
Description	<p>Une personne malintentionnée rend indisponible la téléprocédure en uploadant sur le serveur des fichiers de taille importante.</p> <p>Ce risque touche uniquement la disponibilité des éléments essentiels. Les plus affectés sont les fonctions "F.CONSERVATION", "F.LECTURE", "F.ECRITURE", "F.TELECHARGEMENT" ainsi que les informations "I.PieceJointel", "I.DossierCandidature", "I.Offre", "I.Profil".</p> <p>Il peut provoquer :</p> <ul style="list-style-type: none"> • Une interruption de service • Une perte d'image de marque

R.SATURATION-RESSOURCES

Libellé	R.SATURATION-RESSOURCES
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, elle peut aussi robotiser le remplissage des formulaires afin de rendre indisponible le système.</p> <p>Ce risque touche uniquement la disponibilité des éléments essentiels. Les plus touchés sont "F.CONSERVATION", "F.LECTURE", "F.ECRITURE", "F.TELECHARGEMENT", "I.PieceJointe", "I.DossierCandidature", "I.Offre", "I.Profil" car ils possèdent des besoins importants susceptibles d'être impactés.</p> <p>Cela peut engendrer :</p> <ul style="list-style-type: none"> • Une interruption de service • Une perte d'image de marque

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	34/45

R.SATURATION-SPAM

Libellé R.SATURATION-SPAM

Méthode d'attaque 30 - SATURATION DU SYSTÈME INFORMATIQUE

Description La mauvaise gestion de la politique de mailing provoque de graves dysfonctionnements au niveau du FAI, de l'administration et des usagers. La non conformité du serveur de messagerie par rapport à la politique de filtrage du FAI, le format des mès de notification ou encore la configuration des clients de messagerie des clients peuvent être source de désagréments.

Ce risque touche uniquement la disponibilité des éléments essentiels.

Ceux qui possèdent le plus fort besoin au niveau de ce critère de sécurité sont les plus touchés. Il s'agit de "F.CONSERVATION", "F.LECTURE", "F.ECRITURE", "F.TELECHARGEMENT", "I.PieceJointe", "I.DossierCandidature", "I.Offre", "I.Profil".

Cela peut engendrer :

- Une interruption de service
- Une perte d'image de marque

R.TELECOM-PERTE

Libellé R.PERTE-TELECOM

Méthode d'attaque 13 - PERTE DES MOYENS DE TÉLÉCOMMUNICATION

Description 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.

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.

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	35/45

Ce risque touche la disponibilité des informations. Les plus touchées sont "I.PieceJointe", "I.DossierCandidature", "I.Offre", "I.Profil".

Cela peut engendrer :

- Une interruption de service
- Une perte d'image de marque

R.USURPATION-IDENTITE

Libellé R.USURPATION-IDENTITE

Méthode d'attaque 40 - USURPATION DE DROIT

Description Une personne malintentionnée utilise le système pour communiquer de faux dossiers, dans le but de porter préjudice à l'administration ou à des candidats potentiels. La possibilité de réaliser une candidature sans fournir d'informations d'identification spécifiques rend ce type de menace envisageable.

Etant donné le scénario de menace, ce risque porte uniquement atteinte à l'intégrité des informations du dossier de candidature "I.DossierCandidature".

Ce risque peut engendrer :

- Une atteinte à la vie privée des usagers
- Une infraction aux lois, aux règlements

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	36/45

4 Objectifs de sécurité

O.AUTORISATION

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

O.CANAL

Contenu Des mesures techniques doivent être prises afin de garantir l'intégrité des données transmises par le canal de communication.

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.GARANTIE

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	37/45

Contenu Des mesures doivent être prises afin de garantir l'authentification d'origine du site.

O.DYSFONCTIONNEMENT

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

O.IDENTIFICATION

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

O.IDENTITE

Contenu Des mesures doivent être prises afin de contrôler l'identité des usagers.

O.INJECTION

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

O.INTEGRITE

Contenu Des mesures techniques doivent être prises afin de garantir l'intégrité des données conservées.

O.MAILING

Contenu Des mesures doivent être prise afin de garantir la confidentialité des abonnements à la mailing list.

O.NOTIFICATION

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	38/45

Contenu Des mesures doivent être prises afin de garantir l'origine et l'intégrité des notifications envoyées aux candidats.

O.PIECE-JOINTE

Contenu Des mesures techniques doivent être prises afin de filtrer les pièces jointes au dossier candidature.

O.SATURATION-CONNEXION

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

O.SATURATION-PIECE_JOINTE

Contenu Des mesures doivent être prises afin d'empêcher les personnes de consommer volontairement des ressources en uploadant des fichiers de taille importante.

O.SATURATION-SPAM

Contenu Des mesures techniques doivent être prise afin de garantir la conformité de la politique de mailing

O.TELECOM

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

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	39/45

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 Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	40/45

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 Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	41/45

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 Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	42/45

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.

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	43/45

37 - TRAITEMENT ILLICITE DES DONNÉES

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

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 ».

42 - ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL

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

5.2 Tableau de couverture des risques par les objectifs

	O.TELECOM	
	O.SATURATION-SPAM	
	O.SATURATION-PIECE JOINTE	
	O.SATURATION-CONNEXION	
	O.PIECE-JOINTE	
	O.NOTIFICATION	
	O.MAILING	
	O.INTEGRITE	
	O.INJECTION	
	O.IDENTITE	X
	O.IDENTIFICATION	
	O.DYSFONCTIONNEMENT	
	O.GARANTIE	
	O.DEBORDEMENT	
	O.CONCEPTION	
	O.CODE-MALVEILLANT	
	O.CHIFFREMENT	
	O.CANAL	
	O.AUTHORISATION	
R.USURPATION-IDENTITE		

FEROS Type		Candidature		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.1.1	V1.0	13/04/2006	Public	44/45

