



Direction des systèmes d'information

PLATEFORME APPLICATIVE TRANSVERSE RESEDA

Cahier des Clauses Techniques Particulières (CCTP)

Livret 1/2 du CCTP n°25372

Accord cadre n°25.14.031

Objet : Ce document décrit les exigences fonctionnelles, techniques, d'intégration dans le SI, de sécurité et d'organisation des prestations ainsi que les prestations attendues pour le maintien en conditions opérationnelles de la plateforme « MDM » (Master Data Management) RESEDA, des référentiels hébergés sur la plateforme (y compris l'annuaire CNRS) et si besoin, de la mise en œuvre de projets de nouveaux référentiels sur cette plateforme

SOMMAIRE

SOMMAIRE	2
TABLE DES ILLUSTRATIONS	4
1 CONTEXTE GÉNÉRAL.....	5
1.1 Objet de l'accord-cadre.....	5
1.2 Présentation synthétique du CNRS.....	6
1.3 Lieu d'exécution de l'accord-cadre.....	6
1.4 Structure du CCTP et conventions de rédaction.....	7
2 CONTEXTE DU SI AU CNRS	8
2.1 Conformités réglementaires	8
2.1.1 Politique Générale de Sécurité des systèmes d'Information	8
2.1.2 Protection des données à caractère personnel (DCP)	9
2.1.3 Interopérabilité	10
2.1.4 Accessibilité numérique.....	10
2.2 Présentation des infrastructures du SI CNRS.....	12
2.2.1 Sites et utilisateurs du système d'information	12
2.2.2 Centres serveurs	12
2.2.3 Réseau.....	12
2.2.4 Infrastructures	13
2.3 Principes d'urbanisation et d'intégration dans le SI	13
2.3.1 Principes généraux.....	13
2.3.2 Principes d'échanges	13
2.3.3 Plateformes transverses et services proposés.....	14
2.3.4 Prise en compte des changements de l'organisation structurelle du CNRS et de son environnement (Enseignement Supérieur et Recherche – ESR)	15
3 DESCRIPTION DE LA SOLUTION.....	16
3.1 Présentation Fonctionnelle.....	16
3.1.1 Fonctionnalités de Réséda Socle	20
3.1.2 Fonctionnalités du référentiel Personnel (Personnels des unités CNRS)	22
3.1.3 Fonctionnalités du référentiel Structure	25
3.1.4 Fonctionnalités du référentiel Fournisseur	28
3.1.5 Fonctionnalités du référentiel Contact.....	30
3.1.6 Fonctionnalités du référentiel des caractéristiques des unités (PPST)	32
3.1.7 Fonctionnalités du référentiel Courriel @cnrs.fr	34
3.1.8 Fonctionnalités du référentiel Partenaire	35
3.1.9 Fonctionnalités de l'annuaire CNRS basé sur les référentiels Structure et Personnel	38
3.2 Intégration dans le SI	40
3.3 Présentation technique	41
3.3.1 Caractéristiques techniques générales	41
3.3.2 Architecture Réséda.....	41
3.3.3 Architecture logicielle Réséda	42
3.3.4 Listes des couches basses implémentées.....	42
3.3.5 Architecture technique Réséda.....	43
3.4 Volumétrie du spécifique implémenté par l'intégrateur autour du progiciel EBX	44
3.5 Volumétries de données et d'utilisateurs.....	44
3.6 Données d'exploitation.....	44
3.7 Cas particulier de l'annuaire CNRS (Annuaire des laboratoires)	45
4 CADRE DE COHÉRENCE TECHNIQUE DE LA SOLUTION.....	47
4.1 Exigences d'intégration dans le SI	47
4.1.1 Répartition fonctionnelle	47

4.1.2	Echanges de données.....	47
4.1.3	Authentification, comptes utilisateurs.....	50
4.1.4	Gestion des documents.....	51
4.2	Exigences techniques.....	52
4.2.1	Eléments techniques structurants.....	52
4.2.2	Services d'infrastructure.....	52
4.2.3	Architecture applicative.....	55
4.2.4	Base de données.....	61
4.2.5	Engagements de qualité de service pour l'application.....	61
4.3	Exigences d'ergonomie-graphisme.....	63
4.3.1	Charte graphique.....	63
4.3.2	Règles d'ergonomie.....	64
4.4	Exigences de sécurité.....	64
4.4.1	Auditabilité.....	66
4.4.2	Protection des applications web.....	66
5	CADRE D'ORGANISATION DES PRESTATIONS.....	68
5.1	Système qualité.....	68
5.2	Organisation des équipes projet.....	69
5.2.1	Organisation de l'équipe projet CNRS.....	69
5.2.2	Organisation et gestion des compétences de l'équipe projet du titulaire.....	69
5.3	Dispositifs de conduite de projet.....	70
5.3.1	Structures de pilotage projet.....	70
5.3.2	Pratiques de gestion de projet.....	71
5.3.3	Indicateurs de pilotage et qualité du projet.....	72
5.4	Méthode de développement.....	73
5.4.1	Cycle de vie.....	73
5.4.2	Activités de réalisation (à la charge du titulaire).....	74
5.4.3	Activités de recette (à la charge du CNRS).....	75
5.5	Gestion des environnements.....	76
5.5.1	Postes de travail du titulaire.....	76
5.5.2	Environnement de développement.....	76
5.5.3	Environnements CNRS.....	76
5.6	Gestion des livraisons.....	77
5.7	Gestion de la documentation.....	77
5.8	Capitalisation des connaissances.....	79
5.9	Outillage de suivi et pilotage du projet.....	79
5.10	Mesures et clauses de sécurité.....	80
5.10.1	Gestion de la Sécurité par le titulaire.....	80
5.10.2	Protection des biens.....	80
5.10.3	Obligations du titulaire.....	82
5.10.4	Localisation des données.....	83
5.10.5	Audit.....	83
5.10.6	Application des plans gouvernementaux.....	84
6	ANNEXES.....	85
6.1	Documents joints.....	85
6.2	Présentation détaillée du CNRS.....	85
6.2.1	La présidence-direction générale.....	85
6.2.2	La direction générale déléguée à la science (DGD-S).....	86
6.2.3	La direction générale déléguée aux ressources (DGD-R).....	88
6.2.4	La coordination nationale de la sécurité des systèmes d'information (CNSSI).....	92
6.2.5	La direction générale déléguée à l'innovation (DGD-I).....	92
6.2.6	Les délégations régionales (DR).....	93
6.2.7	Les unités (laboratoires).....	93
6.3	Référence des exigences.....	94

6.4	Abréviations et Glossaire	94
6.4.1	Abréviations	94
6.4.2	Glossaire	97

TABLE DES ILLUSTRATIONS

Figure 1 : Réseau RENATER.....	12
Figure 2 : Présentation de la forge logicielle	59
Figure 3 : Organisation du projet au CNRS.....	69
Figure 4 : Cycle de vie en cascade itératif et incrémental	73
Figure 5 : Cycle de vie agile	74
Figure 6 : Le CNRS en région	93

1 CONTEXTE GÉNÉRAL

1.1 OBJET DE L'ACCORD-CADRE

Le présent accord-cadre a pour objet la fourniture de prestations attendues pour :

- Le maintien en conditions opérationnelles de la plateforme « MDM » (Master Data Management) RESEDA,
- Le maintien en conditions opérationnelles des référentiels hébergés sur la plateforme RESEDA (y compris l'annuaire CNRS),
- La mise en œuvre de nouvelles fonctionnalités sur les référentiels existants (y compris l'annuaire CNRS),
- Et le cas échéant, la mise en œuvre de nouveaux référentiels RESEDA.

La qualité et la gouvernance des données présentes dans chacun des référentiels est capitale pour les applications et processus qui s'appuient dessus et qui les exploitent ainsi que pour leur utilisation dans les tableaux de bord générés dans les systèmes d'informations décisionnelles de l'établissement CNRS.

Dans le cadre de la démarche continue de fiabilisation et de gouvernance métier des principaux référentiels structurants du SI du CNRS, ce dernier s'est doté d'un outil de MDM – Master Data Management ; solution EBX.Platform de la société Tibco.

La DSI du CNRS a souhaité que cette plateforme « MDM » soit intégrée de manière transverse et générique pour tout référentiel candidat dans l'architecture applicative de son SI, quel que soit le type d'implémentation de référentiel (exemple : « consolidation », « centralisation » ou « coopération »).

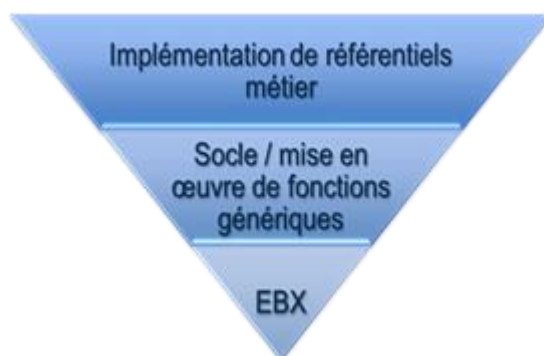
Un socle MDM générique (portail, mécanismes partagés basés sur le progiciel EBX Platform) a donc été constitué en premier lieu avant toute implémentation des premiers référentiels dessus.

L'ensemble de ce dispositif (plateforme et référentiels) a été baptisé RESEDA pour REférentiel SErviceS DAta.

Cette plateforme est opérationnelle depuis 2014. Sept référentiels sont à ce jour implémentés pour une gestion sur la plateforme Réséda :

- Référentiel Fournisseur (en production depuis fin 2014)
- Référentiel Structure (en production depuis 2016)
- Référentiel Personnel (en production depuis 2016)
- Référentiel Contact (en production depuis début 2020)
- Référentiel Courriel (en production depuis 2020)
- Référentiel Caractéristiques des unités (en production depuis 2021)
- Référentiel Partenaire (en production depuis 2023).

Il faut ajouter l'annuaire CNRS qui est sur une plateforme applicative dissociée et hors progiciel EBX Platform, et qui s'appuie sur les référentiels Réséda Structure et Réséda Personnel. Cet annuaire est en production depuis 2021.



Plateforme RESEDA = 3 niveaux ; progiciel / Socle / Référentiels

Pour ces référentiels, les utilisateurs finaux (entre 5 000 et 6 000 utilisateurs différent par mois en 2024, entre 1 000 et 1 500 par jour en 2024) font en moyenne quotidiennement entre 1 500 workflows tous référentiels confondus avec des pics à 2 500 / 3 000 sur des périodes ciblées (début d'année civile, début d'année universitaire).

Ces utilisateurs sont répartis sur l'ensemble de l'organisation du CNRS. Les acteurs présents dans les unités du CNRS représentent une part majoritaire des utilisateurs. Les utilisateurs sont donc répartis sur un millier de sites dans toute la France et à l'international pour les bureaux à l'étranger.

Par ailleurs, les utilisateurs avancés, disposant de fonctions d'administration liées à la gouvernance métier des référentiels, sont principalement localisés dans les directions fonctionnelles (DAPP, DRH, DCIF) localisées sur Paris ainsi que dans le SCTD (Service Central de Traitement de la Dépense) localisé sur Nancy.

Concernant l'annuaire CNRS, entre 10 000 et 12 000 utilisateurs différents par mois en 2024 et entre 1 000 et 1 500 par jour en 2024.

Ces utilisateurs sont répartis potentiellement dans le monde entier puisque cet annuaire, pour le volet « unité de recherche » est accessible au grand public sans aucune authentification.

Les exploitants techniques de la plateforme RESEDA et de l'annuaire CNRS sont localisés au sein de la DSI (équipes MOE, équipe Exploitation et équipe Infrastructure).

Le présent accord-cadre vise à sélectionner un titulaire sur une période maximale de 4 ans (cf CCAP) pour :

- La maintenance et les évolutions de la plateforme RESEDA (appelée Socle) et des référentiels déjà implémentés sur cette plateforme,
- L'implémentation de nouveaux référentiels au sein de la plateforme RESEDA, (le nombre de référentiels à implémenter durant l'accord-cadre n'est pas connu),
- La maintenance et les évolutions de l'annuaire CNRS.

1.2 PRÉSENTATION SYNTHÉTIQUE DU CNRS

Le Centre national de la recherche scientifique est un organisme public de recherche (Établissement public à caractère scientifique et technologique) pluridisciplinaire placé sous la tutelle du Ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation (MESRI). Sa mission est de faire progresser la connaissance et être utile à la société.

Avec près de 33 000 personnes, un budget de presque 4 milliards d'euros, plus de 1100 laboratoires répartis en France et à l'étranger, le CNRS exerce son activité dans tous les champs de la connaissance qu'il s'agisse de biologie, chimie, écologie et environnement, homme et société, ingénierie et systèmes, mathématiques, nucléaire et particules, physique, sciences de l'information ou terre et univers.

Ces domaines de recherche sont regroupés au sein de dix instituts (cf. Annexes).

Sa gouvernance est assurée par le président-directeur général du CNRS, assisté de la directrice de cabinet et de trois directeurs généraux délégués à la science, aux ressources et à l'innovation.

Des informations plus complètes sont disponibles en annexe et sur le site Web, à l'adresse suivante : <https://www.cnrs.fr/fr/le-cnrs/organisation>.

1.3 LIEU D'EXÉCUTION DE L'ACCORD-CADRE

La réalisation et maintenance de l'application s'effectue dans les locaux du titulaire.

Les comités, réunions ou ateliers de spécifications et de conception, nécessitant la présence du CNRS, se tiennent sur sites CNRS (Paris Siège, Paris Meudon ou Toulouse), ou bien en visioconférence entre ces sites.

Les modalités pratiques sont définies au démarrage de l'accord-cadre.

Les locaux du CNRS se situent :

à Paris (Siège du CNRS) :

CNRS
3 rue Michel-Ange
75794 PARIS CEDEX 16

à Meudon (DSI) :

CNRS - DSI
1 place Aristide Briand
92195 MEUDON CEDEX

à Toulouse (DSI) :

CNRS - DSI
358 rue Pierre Gilles de Gennes
31670 LABEGE

1.4 STRUCTURE DU CCTP ET CONVENTIONS DE RÉDACTION

Le livret 1 du CCTP est composé essentiellement des chapitres suivants :

- contexte du SI au CNRS : contexte dans lequel s'inscrit la réalisation et la maintenance de la solution, en terme de conformité réglementaire, d'infrastructure, d'urbanisation et d'intégration dans le système d'information existant,
- description de la solution : caractéristiques fonctionnelles, techniques et volumétrie de la solution existante à maintenir,
- cadre de cohérence technique de la solution : exigences applicables à toute évolution lors de la maintenance de la solution,
- cadre d'organisation des prestations : exigences applicables aux processus de conduite de projet, développement et maintenance de la solution, ainsi que mesures de sécurité encadrant les prestations.

Le livret 2 du CCTP contient la description des prestations et unités d'œuvre.

Les exigences vis-à-vis du titulaire sont décrites dans le présent document dans des tableaux de la forme ci-dessous. La référence est composée de 3 lettres définissant le groupe d'exigences (cf. « Référence des exigences » en annexe) et de 3 chiffres (pas nécessairement consécutifs). Les exigences sont classées selon 3 niveaux :

- Priorité 0 : exigence impérative à satisfaire obligatoirement par le titulaire
- Priorité 1 : exigence très fortement souhaitée, à justifier si non satisfaite
- Priorité 2 : exigence souhaitée, pouvant être satisfaite, partiellement ou pas par le titulaire (avec justification)

Référence	Libellé exigence	Priorité
XXX_NNN	Libellé de l'exigence	0/1/2

La solution en place actuellement n'est pas intégralement conforme à toutes les exigences présentées dans ce document. Les mises en conformité seront déclenchées le cas échéant à l'initiative du CNRS lorsqu'elles sont nécessaires, sous la forme de demandes d'évolutions. Les nouveaux développements réalisés dans le cadre de ce marché doivent être conformes aux exigences sauf dérogation expresse du CNRS.

2 CONTEXTE DU SI AU CNRS

2.1 CONFORMITÉS RÉGLEMENTAIRES

Les applications mises en œuvre par le CNRS sont soumises à des conformités réglementaires définies dans des référentiels interministériels présentés dans les paragraphes suivants.

Référence	Libellé exigence	Priorité
REGL_001-a	Les téléservices (applications destinées à la communication interadministration ou destinées à réaliser des téléprocédures ouvertes à des usagers, c'est-à-dire application grand public) sont mis en œuvre conformément aux référentiels interministériels. Les téléservices sont conformes au RGS (sécurité) : https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs	0
REGL_001-b	Les téléservices (applications destinées à la communication interadministration ou destinées à réaliser des téléprocédures ouvertes à des usagers, c'est-à-dire application grand public) sont mis en œuvre conformément aux référentiels interministériels. Les téléservices sont conformes au RGI (interopérabilité, selon le profil choisi par le CNRS) : https://www.numerique.gouv.fr/publications/interopabilite/	0
REGL_001-c	Les applications sont mises en œuvre conformément au RGAA (Référentiel général d'amélioration de l'accessibilité) : https://accessibilite.numerique.gouv.fr/	0
REGL_002-a	Pour les applications qui ne sont pas des téléservices, l'objectif de conformité au référentiel RGS est poursuivi.	2
REGL_002-b	Pour les applications qui ne sont pas des téléservices, l'objectif de conformité au référentiel RGI est poursuivi.	2
REGL_003	La page d'accueil de la solution permet d'accéder aux mentions légales : licence d'utilisation du logiciel, point de contact éditorial et technique, éventuelles mentions légales réglementaires concernant les données à caractère personnel, l'utilisation des cookies.	0
REGL_008	La gestion des cookies est conforme à la réglementation en vigueur. La solution permet d'afficher la liste des cookies nécessaires à son fonctionnement et la manière de les supprimer dans les navigateurs supportés.	0
REGL_009	La solution s'interface avec ou gère une plateforme de gestion des consentements (consent management platform) permettant de débrayer le positionnement des cookies non essentiels.	1

2.1.1 Politique Générale de Sécurité des systèmes d'Information

Concernant les aspects sécurité, les objectifs de la Politique Générale de Sécurité des systèmes d'Information (PGSI¹) du CNRS sont les suivants :

- Protéger le savoir-faire du CNRS et les données permettant de valoriser la recherche ;
- Assurer la protection du potentiel scientifique et technique et le respect des engagements internationaux ;
- Garantir la disponibilité des moyens opérationnels du CNRS ;
- Assurer le respect par le CNRS de ses obligations légales, réglementaires et contractuelles ;
- Éviter les accidents qui résulteraient de la perte de contrôle d'un processus ou tout au moins en limiter les conséquences ;
- Conserver au CNRS un statut de partenaire de confiance.

À ces fins, le CNRS applique les principes de politique générale suivants (issus de la PGSI du CNRS) :

- L'ensemble du périmètre placé sous la responsabilité du CNRS doit être couvert ;
- Toutes les exigences légales et réglementaires doivent être prises en compte ;

¹ PGSI : document diffusable sur demande à l'équipe sécurité de la DSI du CNRS

- La gestion des risques doit être réalisée de façon systématique suivant la réglementation Française et les normes internationales en vigueur ;
- L'organisation qui est mise en place pour piloter et mettre en œuvre cette politique doit disposer des moyens humains compétents en nombre suffisant ;
- Les mesures de protection devront être complétées par des mesures de défense active efficaces ;
- L'application de cette politique est contrôlée.

D'un point de vue contractuel, le titulaire doit respecter au minimum les exigences sécurité du présent CCTP.

Référence	Libellé exigence	Priorité
REGL_004	Le titulaire se conforme au cadre réglementaire applicable en terme de SSI, à savoir (de façon non exhaustive) : ■ les annexes techniques du Référentiel Général de Sécurité (RGS) ■ la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSI-E) ■ l'instruction interministérielle 901 (II901) portant sur les informations sensibles marquées « diffusion restreinte » ■ la PSSI du CNRS (PSSI-C) RGS : https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs PSSI-E : https://www.legifrance.gouv.fr/circulaire/id/38641 II 901 : https://cyber.gouv.fr/instruction-interministerielle-n901 PSSI-C : Document non public, disponible sur demande	0
REGL_005	D'un point de vue technique, le titulaire applique les différents guides de l'ANSSI : : : https://cyber.gouv.fr/publications?field_type_de_publication_target_id%5B934%5D=934	0

2.1.2 Protection des données à caractère personnel (DCP)

La politique de protection des données personnelles au CNRS se conforme à la réglementation en vigueur (Règlement européen sur la protection des données – Règlement UE 2016/679 et Loi informatique et libertés modifiée).

Pour l'ensemble des processus mobilisant son SI, le CNRS est responsable des traitements de données, qui sont inscrits dans le registre tenu par la déléguée à la protection des données (DPD) de l'établissement.

Le titulaire est informé que le transfert de données sensibles ou personnelles vers le SI du titulaire est interdit dans le cadre des prestations de cet accord-cadre.

Le titulaire est informé que s'il a lui-même recours à des sous-traitants, les dispositions qui lui sont applicables le sont automatiquement à ses sous-traitants, et qu'il fait son affaire de leur information et de la contractualisation écrite de ces obligations. Le CNRS demande communication de ces engagements lors de la phase de consultation et est à tout moment autorisé à vérifier, conformément à la clause d'audit, la réalité de cet engagement.

Le titulaire est responsable, dans les limites imposées par la loi, de la sécurité (confidentialité, intégrité et disponibilité) des DCP qu'il traite et auxquelles il a accès.

Prise en compte de la sécurité et du respect de la vie privée par défaut dans les développements

Le titulaire répond aux exigences de sécurité du présent cahier des charges, et complète sa réponse en décrivant la démarche industrielle qu'il met en œuvre pour répondre aux exigences de l'article 252 du RGPD. Il indique quels outils et quelles méthodes il met en œuvre pour atteindre l'objectif de conformité. Ces éléments peuvent faire l'objet d'un contrôle par le CNRS.

Obligation d'information du CNRS en cas de faille de sécurité impactant le SI du titulaire

En cas d'incident de sécurité touchant le SI du titulaire et pouvant mettre en péril les DCP confiées par le CNRS (notamment, compromettant les accès au SI CNRS utilisés pour la réalisation des prestations), le titulaire informe immédiatement et de manière exhaustive le CNRS de l'événement.

Le CNRS peut demander tout complément d'information pour lui permettre d'apprécier la portée de l'incident, afin d'apprécier la nécessité d'informer l'autorité de régulation et/ou les personnes concernées dans les cas prévus par la réglementation.

2.1.3 Interopérabilité

Le référentiel général d'interopérabilité (RGI) est un cadre de recommandations référençant des normes et standards qui favorisent l'interopérabilité au sein des systèmes d'information de l'administration.

Ces recommandations constituent les objectifs à atteindre pour favoriser l'interopérabilité. Elles permettent aux acteurs cherchant à interagir et donc à favoriser l'interopérabilité de leur système d'information, d'aller au-delà de simples arrangements bilatéraux.

Le RGI est défini dans l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Dans l'article 11 de cette ordonnance, le « RGI fixe les règles techniques permettant d'assurer l'interopérabilité des systèmes d'information. Il détermine notamment les répertoires de données, les normes et les standards qui doivent être utilisés par les autorités administratives. Les conditions d'élaboration, d'approbation, de modification et de publications de ce référentiel sont fixées par décret ».

Le référentiel général d'interopérabilité applicable est disponible en libre accès :

<https://www.numerique.gouv.fr/offre-accompagnement/reference-interoperabilite-rgi/>

Le titulaire respecte les dispositions du profil d'interopérabilité P08 choisi par le CNRS conformément aux objectifs de présent accord cadre.

2.1.4 Accessibilité numérique

2.1.4.1 Contexte

Comme le définit l'article 47 de la loi 2005-102 du 11 février 2005, est concerné par l'obligation légale d'accessibilité tout type d'information sous forme numérique quels que soient le moyen d'accès, les contenus et le mode de consultation.

Sont donc concernés tous les services publics de type internet, intranet, extranet, applications web (développement spécifique ou progiciels intégrés au SI), applications mobiles ainsi que les documents émanant de tous ces services (pdf...).

2.1.4.2 Niveau attendu pour l'accessibilité numérique

La solution doit prendre en compte le niveau légalement attendu pour l'accessibilité numérique qui est à ce jour le niveau double A (AA).

Le référentiel d'accessibilité applicable est disponible en libre accès :

<https://accessibilite.numerique.gouv.fr/>

Les critères à retenir du référentiel général d'accessibilité pour les administrations (RGAA) dans sa version 4.1 sont donc tous ceux permettant de répondre aux niveaux déduits [A] et [AA] du WCAG (Web Content Accessibility Guidelines).

Niveaux de conformité WCAG :

Niveau	Définition de la conformité	Critères
A (Niveau minimal)	La page web satisfait à tous les critères de succès de niveau A ou une version de remplacement est fournie.	Critères de succès essentiels pouvant raisonnablement s'appliquer à toutes les ressources web.
AA	La page web remplit tous les critères de succès de niveau A et AA ou une version de remplacement conforme au niveau AA est fournie.	Critères de succès pouvant raisonnablement s'appliquer à toutes les ressources web.

Le titulaire effectuera des pré-audits pour s'assurer du niveau de conformité avec des outils appropriés et communiquera au CNRS ses résultats.

2.1.4.3 Déclaration de conformité

Référence	Libellé exigence	Priorité
ACC_001	Sauf accord exprès du CNRS, le titulaire s'engage pour tout développement spécifique de page, à respecter un niveau de conformité supérieur à 50%.	1

Référence	Libellé exigence	Priorité
ACC_002	Pour un progiciel, le titulaire s'assure que le progiciel fourni ou distribué est accompagné d'une déclaration d'accessibilité valide. Cette déclaration est consultable via un lien conforme au RGAA.	1
ACC_003	A minima la page d'accueil de chaque application doit contenir un lien dont le nom reflète le niveau de conformité (« Accessibilité : totalement conforme » ou « Accessibilité : partiellement conforme » ou « Accessibilité : non conforme »). Ce lien pointe vers la déclaration d'accessibilité fournie par le CNRS (pdf ou page html) ou le titulaire (cas des progiciels). La mise à jour de l'intitulé du lien et de la déclaration d'accessibilité doit être possible sans nouveau déploiement de l'application. Dans la mesure du possible, il est demandé de mettre le lien dans un pied de page (footer) visible sur toutes les pages de l'application.	1
ACC_004	Le titulaire est informé que le CNRS conduit des audits de conformité, par ses propres équipes ou par celles de tiers désignés par lui, ayant pour objectifs : - de vérifier le respect par le titulaire de ses engagements initiaux mis en œuvre concernant le RGAA sur un ensemble de pages représentatives de l'application ainsi que les pages réglementaires obligatoires - de publier la déclaration de conformité (créée ou mise à jour selon l'audit) Le résultat des audits conduit à la rédaction d'un plan d'action de la part du titulaire. Les actions inscrites ne conduisent pas à facturation supplémentaire de la part du titulaire si elles découlent directement d'un constat de non-conformité par rapport : - à ses engagements initiaux ou - à la réglementation en vigueur à la date de notification de l'appel d'offre. Dans tous les autres cas (évolution de la réglementation, évolution d'une application...), le titulaire propose une cotation pour la réalisation des prestations de mise en conformité.	1

L'échantillon sur lequel est réalisé l'audit de conformité porte **au moins** sur les pages listées sur le site RGAA (<https://accessibilite.numerique.gouv.fr/obligations/evaluation-conformite/>).

2.2 PRÉSENTATION DES INFRASTRUCTURES DU SI CNRS

2.2.1 Sites et utilisateurs du système d'information

Les utilisateurs du système d'information du CNRS sont principalement répartis :

- dans les 17 délégations, en régions et en Ile de France et sur le siège parisien de l'établissement. Ils représentent environ 3000 agents, dotés principalement de poste de travail de type PC sous Windows ;
- dans l'ensemble des laboratoires, répartis sur l'ensemble du territoire. Ils représentent plus de 120 000 personnes potentiellement utilisateurs du système d'information dont plus de 30 000 agents CNRS.

2.2.2 Centres serveurs

Toutes les applications du SI et services techniques associés sont hébergés sur des centres serveurs mutualisés qui disposent des caractéristiques physiques, techniques et organisationnelles pour ce type d'activité.

Le CNRS utilise deux centres serveurs. Le centre principal d'hébergement est situé à VILLEURBANE (69) est géré par une entité interne au CNRS.

2.2.3 Réseau

Les sites CNRS sont très majoritairement connectés au réseau national de la recherche : RENATER.

RENATER offre plusieurs points de présence (Nœud de Raccordement) sur le territoire national à l'ensemble de la communauté enseignement supérieur et recherche.

Il permet de relier les sites de la recherche, directement ou au travers de réseaux métropolitains.

On trouvera sur le site du groupement d'intérêt public (GIP) en charge de ce réseau tous les éléments d'informations disponibles : <http://www.renater.fr/>

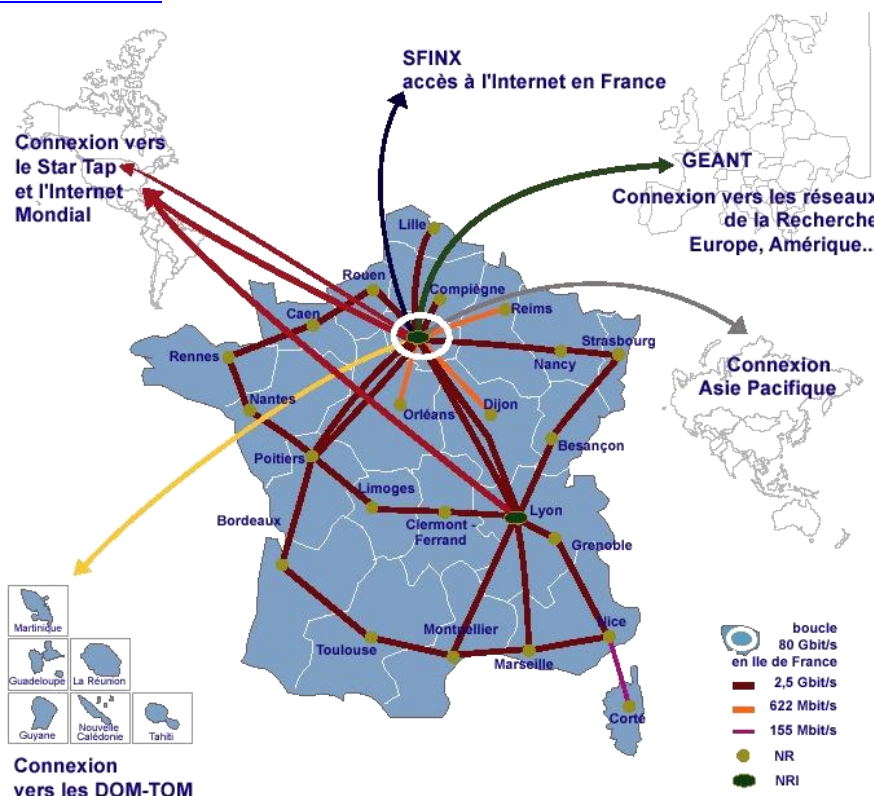


Figure 1 : Réseau RENATER

Afin d'avoir la maîtrise des flux spécifiques du système d'information du CNRS, la DSI a construit un réseau dédié, Sires, qui fédère l'ensemble des sites administratifs et des centres serveurs. Le réseau Sires s'appuie sur l'infrastructure de RENATER et il est opéré au travers d'un marché d'infogérance.

Les centres serveurs sont directement reliés sur RENATER.

Tous les flux du SI sont aujourd'hui de type IPV4. La gestion du réseau s'appuie largement sur les technologies de réseaux privés virtuels (VLAN), de translation d'adresses IP (NAT) et de chiffrement (via une technologie de type VPN ou autre).

La sécurisation des flux est basée sur du filtrage de flux et des technologies de firewall standards.

2.2.4 Infrastructures

Les infrastructures matérielles utilisées sur les centres serveurs sont normalisées. La construction de ces architectures a été basée sur deux préoccupations majeures :

- Mettre en œuvre des technologies capables de répondre aux exigences de qualité de service du SI CNRS, en termes de performances, disponibilité, intégrité et sécurité.
- Rationaliser et homogénéiser les équipements pour favoriser la maîtrise technique et minimiser les coûts de possession.

Les applications du SI CNRS sont hébergées sur une infrastructure virtualisée, sauf en cas de contraintes spécifiques.

2.3 PRINCIPES D'URBANISATION ET D'INTÉGRATION DANS LE SI

2.3.1 Principes généraux

La démarche d'urbanisation mise en œuvre à la DSI du CNRS doit accompagner, faciliter et maîtriser la transformation continue et progressive du SI en le rendant de plus en plus agile et en assurant sa pérennité pour en tirer le maximum de plus-value, en cohérence avec les orientations stratégiques, métiers et opérationnelles de l'organisme.

Cette démarche doit aider l'évolution du SI par une optimisation de l'existant, tournée vers les objectifs suivants :

- capitaliser sur les socles existants ;
- poursuivre l'intégration des différents systèmes dans l'optique d'une gestion modernisée ;
- garantir la fiabilité des données de référence dans le système d'information global.

Plus particulièrement, 4 grands principes sont mis en avant par la démarche d'urbanisation et d'intégration dans les SI :

1. Principe de cohérence forte pour aider à répartir les contours fonctionnels et informationnels entre les applications du SI dans le but d'éviter toute redondance fonctionnelle et de limiter les flux entre applications participant au même processus métier. Un modèle informationnel et un modèle des processus métier sont fortement recommandés, voire attendus, pour aider à ces choix de répartition applicative ;
2. Principe de couplage faible entre applications pour réduire les dépendances entre applications (par exemple l'appui direct sur la base de données d'une application tierce) et ainsi limiter les impacts sur le SI en cas d'évolution d'une partie de ce SI ;
3. Développer l'utilisation de briques numériques, fonctionnelles et/ou applicatives communes et mutualisées dans une logique de plateformes transverses ;
4. Prendre en compte la dimension « laboratoire » et ainsi découpler de façon modulaire (modules applicatifs disjoints) autant que faire se peut les fonctionnalités « Etablissement » des fonctionnalités « Laboratoire » dans la perspective de futures mutualisations potentielles des fonctionnalités « Laboratoire » et d'éventuelle répartition dans des SI distincts des fonctionnalités « Etablissement » et « Laboratoire » ; le tout en cohérence avec les actions parallèles éventuelles sur les mêmes sujets par les SI des établissements partenaires du CNRS.

L'architecture proposée par le titulaire est soumise à la validation de la DSI du CNRS.

2.3.2 Principes d'échanges

Pour mettre en œuvre le principe de couplage faible, des protocoles d'échanges sont établis, préconisant l'utilisation de :

- systèmes d'intermédiation (cf. § 2.3.3.1) pour éviter les échanges point à point entre deux applications en procédant par ½ flux via ces systèmes d'intermédiation ;
- formats d'échange communs sous la forme de format pivot par objet métier échangé. Le format pivot, indépendant des applications et de leur modèle de données, est une représentation partagée et intrinsèque d'un objet (métier ou

technique), tenant compte de l'ensemble de ses cas d'usages. Il précise aussi les référentiels et nomenclatures communs et partagés à utiliser éventuellement pour ses attributs ;

- fonctions d'intégration (ou services applicatifs) de ces formats pivots dans le cadre des flux entrants ;
- fonctions d'exposition (ou services applicatifs) des informations vers ces formats pivots dans le cadre des flux sortants.

Ces principes s'appliquent aussi bien aux échanges de données et informations internes au SI qu'aux échanges avec l'extérieur.

2.3.3 Plateformes transverses et services proposés

2.3.3.1 *Systèmes d'intermédiation*

Actuellement les systèmes d'intermédiation mis en œuvre dans le SI du CNRS sont :

- un gestionnaire applicatif d'échanges et de services « outil EAI/ESB CNRS » (découpage en ½ flux, format pivot des objets métiers échangés) qui a la responsabilité et la gestion des échanges en termes d'orchestration, de chronologie des flux le cas échéant, de transcodification des données vers les SI cibles ou depuis les SI sources ;
- un proxy de services web ;
- une exposition de services web de données de référence (mise à disposition des formats pivots persistés des objets métiers principalement de référence mais non limités aux données de références)

2.3.3.2 *Gestion des données de référence*

La DSI du CNRS dispose d'un outil GDR (Gestion des Données de Référence) nommé Réséda et proposant des services de gouvernance et de mise en qualité des données, de recherche approchante...des données de référence.

Cette plateforme, objet de cette consultation, est préconisée dans les cas de référentiels structurants et partagés pour lesquels une gouvernance métier est attendue entre différents acteurs métiers.

La mise à disposition, au reste du SI CNRS, des données de ces référentiels se fait par les services web de données de référence (cf §2.3.3.1).

2.3.3.3 *Fournisseur d'identité*

Les services d'authentification web centralisée du CNRS (web SSO) via le protocole SAML 2.0, sont regroupés sous la dénomination de Janus. Ils consistent en plusieurs fournisseurs d'identités (IdP) dépendant de la population à authentifier (Personnel des unités CNRS, Prestataires et usagers des unités CNRS, Externes) et du niveau d'authentification nécessaire.

Dans le cas où plusieurs fournisseurs d'identités peuvent être utilisés pour accéder à la solution, un mécanisme de sélection par l'utilisateur du fournisseur d'identité est mis en place. Ce mécanisme est nommé WAYF (Where Are You From).

Ils s'appuient sur le référentiel des comptes utilisateurs alimenté par le service IAM (cf. § 2.3.3.40).

2.3.3.4 *Service référentiel de comptes et gestion des accès et habilitations (IAM)*

Ce service recouvre des outils qui permettent la mise à jour du référentiel de comptes utilisateurs du SI CNRS à partir des données du référentiel des personnels des unités du CNRS (pour une large partie mais pas que).

Les données du référentiel des comptes utilisateurs sont exposées par des services Web à l'usage des applications. Elles sont également pour certaines transmises à l'application via le processus d'authentification.

Une gestion des accès applicatifs est également en place mais va évoluer dans le futur pour prendre en compte une plus grande automatisation et de nouvelles fonctionnalités pour l'attribution de rôles applicatifs à des comptes utilisateurs.

2.3.3.5 *Archivages courant, intermédiaire et pérenne, parapheur électronique*

L'archivage courant CNRS utilise un système de gestion électronique de document (GED) du CNRS basé sur l'outil EverSuite (<http://www.ever-team.com/>).

L'archivage intermédiaire et pérenne CNRS est basé sur la solution VITAM de l'État et exploitée, hébergée au CINES (Centre Informatique National de l'Enseignement Supérieur).

Des services sont mis en œuvre afin de permettre aux applications du SI le nécessitant de mettre en place des déversements en archivage intermédiaire ou en archivage final.

Ces déversements sont des projets à part entière, à préparer et à planifier en liaison étroite avec les équipes DSI en charge de ces plateformes d'archivage.

Une plateforme transverse de parapheur électronique, incluant des fonctionnalités de signature électronique, est également en place pour les actes nécessitant des signatures en tant que telles (ne pas confondre avec des visas électroniques). Là aussi, se rapprocher de l'équipe DSI en charge de cette plateforme si des besoins de signatures électroniques font partie du périmètre des projets.

2.3.4 Prise en compte des changements de l'organisation structurelle du CNRS et de son environnement (Enseignement Supérieur et Recherche – ESR)

Dans le cadre de la transformation progressive et continue vers un système d'information qui permet un alignement sur les stratégies de l'établissement, les outils proposés pour les SI et applications doivent prendre en considération, le plus nativement possible, les différentes restructurations du CNRS :

- Chaque année, une partie des unités de recherche est renumérotée, fusionnée, éclatée, ... (changement de référence métier) ;
- Les instances (conseils scientifiques du CNRS et des instituts, sections et commissions interdisciplinaires) du [Comité national de la recherche scientifique](#) (changement de périmètre sans changement systématique de référence métier) [renouvelées tous les 5 ans](#) ;
- Les restructurations des établissements de l'ESR (COMUE, établissements expérimentaux, fusion d'établissements, ...)
- Les restructurations organisationnelles du CNRS (exemple : en 2023, la fusion de la délégation Normandie avec la délégation Paris Michel Ange ; en 2020 le remplacement des certains types d'unités et des catégories des structures de recherche ; en 2009, le remplacement des départements scientifiques par des Instituts nationaux ; ...)

Référence	Libellé exigence	Priorité
URB_001	La solution est en capacité de fournir une continuité de service fonctionnelle dans le temps, en tenant compte des différents types de restructuration de l'organisation CNRS, impactant les SI et applications. Le choix des mécanismes à implémenter est étudié et validé entre le titulaire et le CNRS (équipes projet et transverses).	1
URB_002	La solution s'alimente du référentiel d'organisation structurelle du CNRS, à partir de ses services web dédiés.	1

Le référentiel d'organisation du CNRS est géré au sein de la plateforme Réséda, et plus particulièrement dans le référentiel Réséda Structure.

Le référentiel des établissements de l'ESR partenaires du CNRS est lui-aussi géré dans la plateforme Réséda, et plus particulièrement dans le référentiel Réséda Contact (y compris la description des restructurations ponctuelles des établissements de l'ESR) s'appuyant sur le référentiel Réséda Partenaire (cf §3.1.5 et §3.1.8).

De fait, les restructurations cycliques de l'organisation du CNRS, tout comme les éventuelles restructurations ponctuelles des établissements, sont prises en compte dans la plateforme Réséda puis diffusées à l'ensemble du SI à partir de ces référentiels, au travers de web services disponibles depuis les systèmes d'intermédiation.

L'exigence URB_002 est donc d'office respectée puisque Réséda est la source. Il s'auto alimente donc pour ses besoins propres du référentiel d'organisation du CNRS.

3 DESCRIPTION DE LA SOLUTION

3.1 PRÉSENTATION FONCTIONNELLE

La plateforme RESEDA est l'implémentation du progiciel MDM (Master Data Management) EBX Platform au sein du SI du CNRS.

Ce périmètre contient :

- Le « Socle » : fonctions complémentaires transverses nécessaires pour l'intégration du progiciel dans le SI du CNRS et elles-aussi implémentées dans le progiciel en tant que référentiel interne à la plateforme (Réséda Socle) ;
 - L'intégration de la plateforme Réséda avec le système d'intermédiation du SI du CNRS ; (flux d'information en entrée et en sortie de la plateforme Réséda) ;
 - L'intégration de la plateforme Réséda avec le système d'authentification et d'habilitations du SI du CNRS (Janus / IAM) ;
 - Le portail d'accès à la plateforme Réséda pour tout utilisateur
 - Un ensemble de fonctionnalités mutualisées au sein du Socle et réutilisables pour tout référentiel hébergé sur la plateforme Réséda, par exemple :
 - Annuaire interne de gestion des droits pour tout utilisateur sur les référentiels
 - Planificateur spécifique de tâches multifiées avec gestion de dépendances et d'exclusion (exploitation des traitements batch et complémentaire au planificateur standard EBX),
 - Notifications par mël à des utilisateurs centraux ciblés, pour des mises à jour ciblées

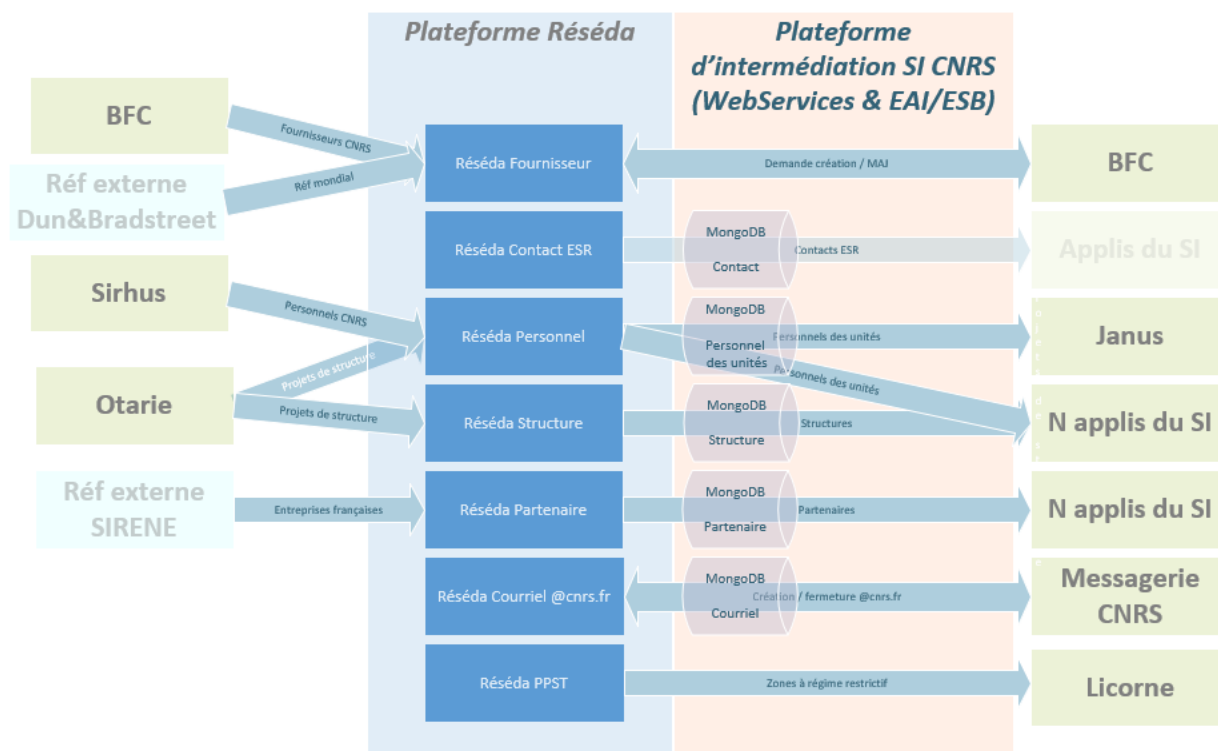
Liste non exhaustive (cf § 3.1.1 – Fonctionnalités de Réséda Socle)

- Le référentiel Personnel (CNRS et non CNRS) des unités CNRS (§ 3.1.2)
- Le référentiel Structure (unités CNRS et unités mixtes) (§ 3.1.3)
- Le référentiel Fournisseur (§ 3.1.4)
- Le référentiel Contact (§ 3.1.5)
- Le référentiel des caractéristiques des unités (PPST) (§ 3.1.6)
- Le référentiel Courriel (@cnrs.fr) (§ 3.1.7)
- Le référentiel Partenaire (§ 3.1.8)

Un annuaire CNRS (hors plateforme Réséda) (§3.1.9), basé sur les référentiels Réséda Structure et Réséda Personnel, vient compléter le périmètre de cette consultation.

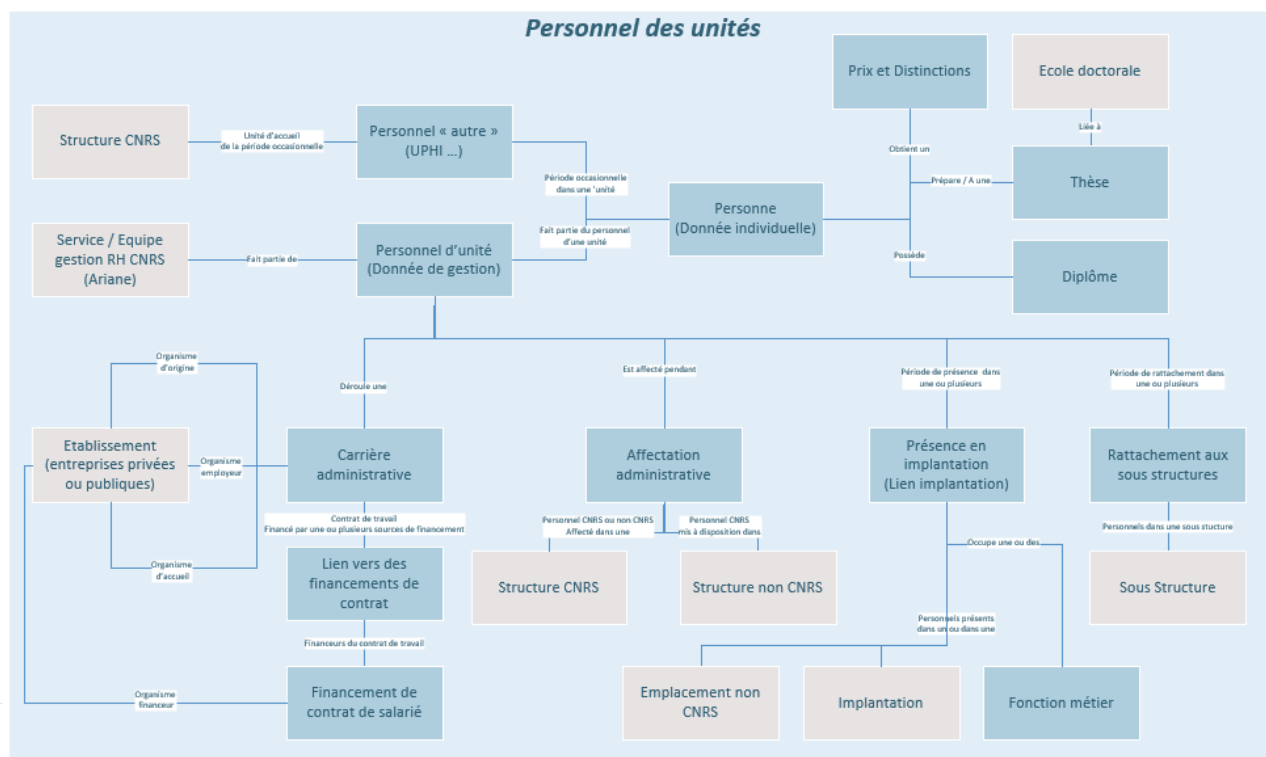
Un macro modèle informationnel présente succinctement (par couches d'abstraction) les référentiels de la plateforme, leurs interactions informationnelles entre eux et aussi avec des applications du SI du CNRS.

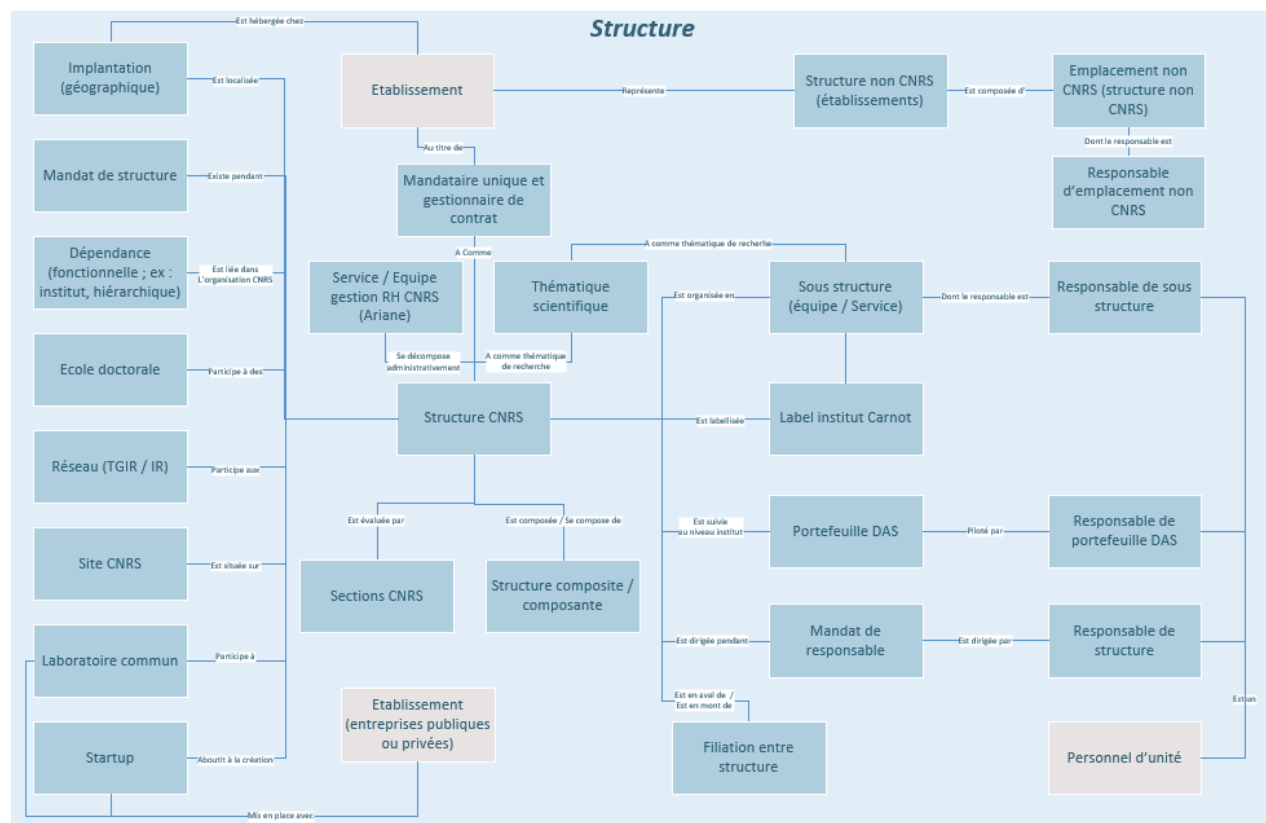
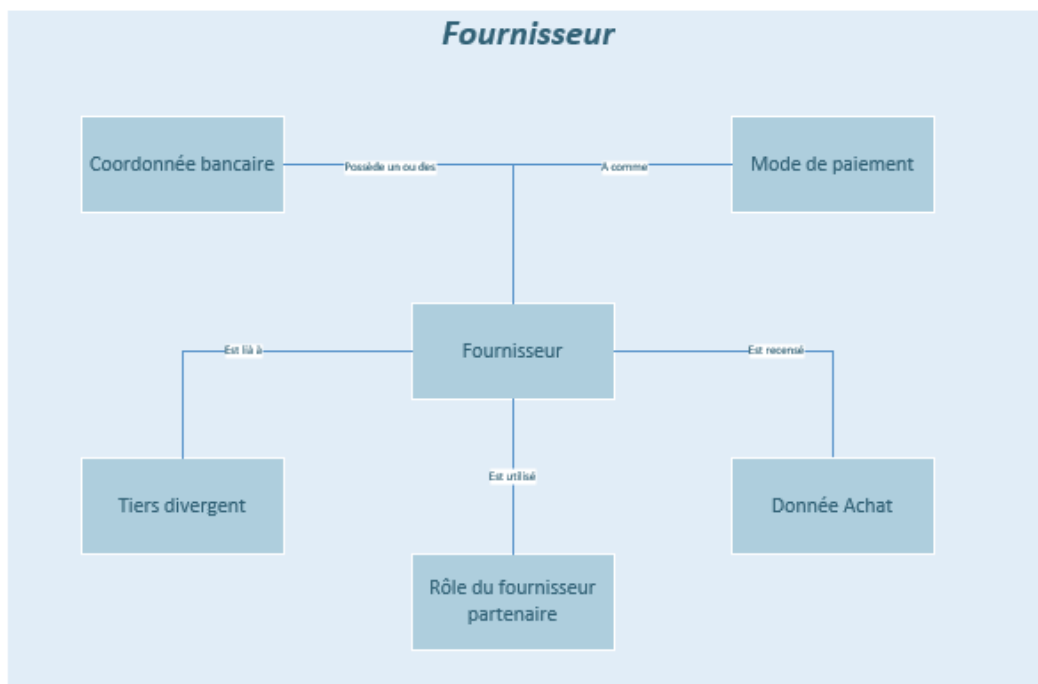
Macro modèle d'intégration au SI CNRS des référentiels hébergés sur la plateforme Réséda

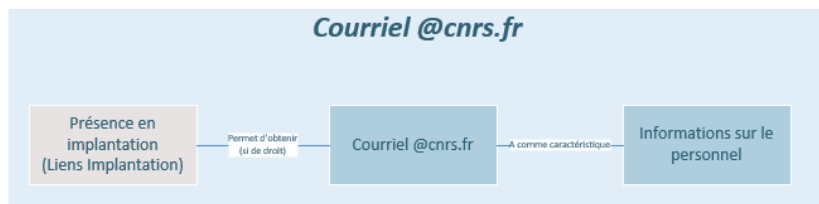
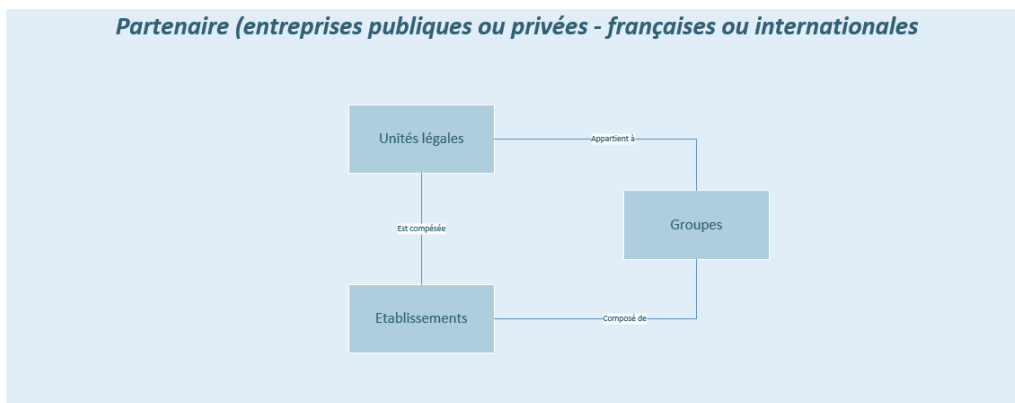
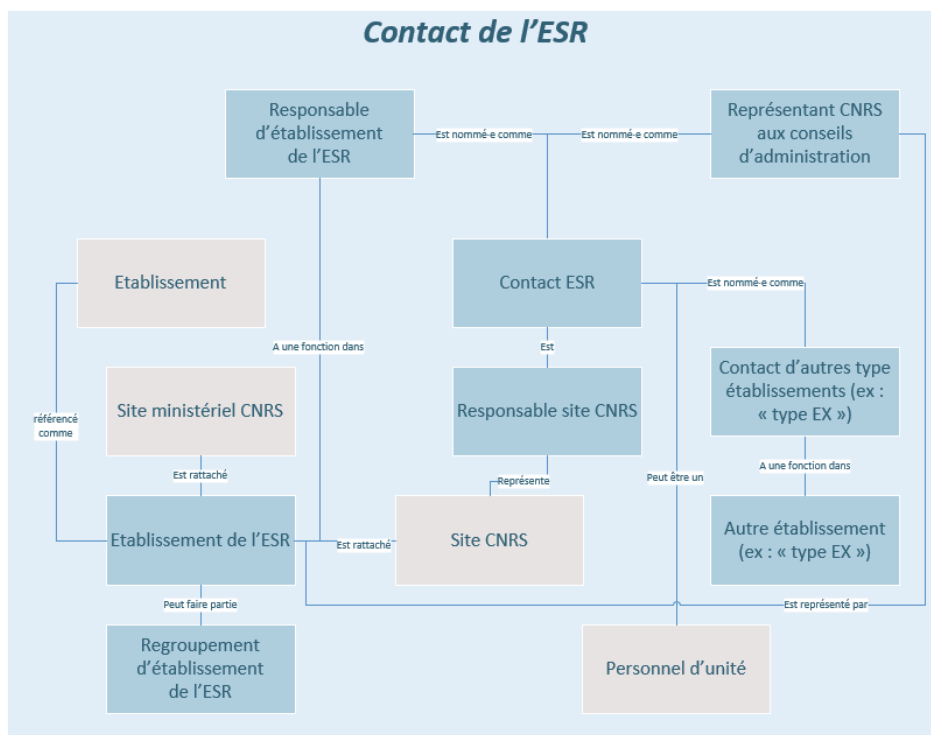


Macro modèle informationnel interne des référentiels hébergés sur la plateforme Réséda

Macro modèle informationnel du référentiel Personnel des unités



Macro modèle informationnel du référentiel Structure**Macro modèle informationnel du référentiel Fournisseur**

Macro modèle informationnel du référentiel Courriel @cnrs.fr**Macro modèle informationnel du référentiel Partenaire CNRS****Macro modèle informationnel du référentiel Contact ESR**

3.1.1 Fonctionnalités de Réséda Socle

RESEDA est composé des fonctionnalités transverses suivantes (issues du progiciel ou compléments spécifiques CNRS(*))

- Fonctions et services pour les opérations métiers élémentaires (import, export, ajout, modification, duplication, suppression de données, ...)
- Gestion unitaire ou de masse des opérations métiers élémentaires
- Génération d'identifiant unique selon un périmètre variable
- Gestion des workflows d'acquisition des références (modélisation et console de suivi)
- Gestion des workflows d'approbation (modélisation et console de suivi)
- Modélisation des référentiels et dictionnaire des données
- Planificateur de tâches multifiles (*)
- Gestion des nomenclatures et paramètres (*)
- Gestion paramétrée des états métiers des objets de référence et des transitions entre états (*)
- Gestion des contraintes d'intégrité référentielle
- Gestion de la traçabilité métier d'un référentiel
- Gestion des versions métier d'un référentiel (préparation d'un référentiel projeté par exemple, constitution d'images d'un référentiel)
- Gestion de règles métiers (*)
- Gestion des références croisées entre référentiels et avec des SI tiers (*)
- Gestion de transcodification de nomenclatures (*)
- Gestion de la qualité de données (identification et gestion de doublons potentiels)
- Gestion d'un annuaire interne des droits (profils, rôles et autorisations par utilisateur) s'appuyant pour partie sur une plateforme IAM délivrant des rôles applicatifs par utilisateur (*)
- Gestion du portail d'accès commun à tous les référentiels pour tous les utilisateurs de Réséda (*)
- Réplication de référentiels vers des schémas accessibles depuis IsQlient en consultation
- Fonctionnalités d'export / import de données sur table
- Fonctionnalités de recherche sur table (simples et avancées)
- Service de dépôt de pièces jointes via l'addon DAM (en lien avec une plateforme de GED via la plateforme EAI/ESB ou gérées uniquement dans l'application sans l'utilisation d'une GED (* pour le dépôt et la consultation dans la GED)
- Service de pages d'aide contextuelle accessible depuis les écrans Réséda (en lien avec les MUT – manuels utilisateurs présents sur l'aide en ligne Réséda gérée sous une solution CNRS basée sur SharePoint) (*)
- Service de pré-validation des espaces liés aux workflows (sera abandonné lors du portage en EBX6 prévu avant le démarrage du nouvel accord-cadre ; mais au cas où le portage EBX6 ne serait pas effectif en production)
- Service de reconstruction des caches de confidentialité et de gestion des workflows (*)
- Génération de services web simples (unitaire par table) en mode REST ou SOAP
- Services d'accès aux référentiels (entrant / sortant) via la plateforme d'intermédiation (EAI/ESB) (*)
- Génération de mèls de notification sur des écoutes de tables mises à jour (ex : notification sur une donnée modifiée ou ajoutée, une date qui arrive à échéance) (*)
- Génération de tableaux de bord de suivi des référentiels
- Génération de graphes informationnels sur les référentiels

Éléments de volumétrie permettant de mieux appréhender la complexité

Eléments	Volume
Nombres de crons	16

Nombre de flux sortants

4

Volumétrie d'écrans spécifiques

Nombre d'écrans spécifiques	Localisation / Fonction
1	Portail
1	Écran de comparaison
1	Attribution des droits
3	Gestion des images
1	Start & stop
1	Planificateur de tâches multifiles

Volumétrie et charge moyenne (jours de développement) pour les mantis Socle (correctif & évolutif) sur les 3 dernières années(Depuis T2 2022 jusqu'à 2025 inclus) :

Socle	
Sévérité	Nombre de mantis
2022	17
bloquant	1
majeur	7
mineur	9
2023	35
majeur	9
mineur	26
2024	62
majeur	11
mineur	51
2025	81
majeur	11
mineur	70
Total général	195

Socle	
Année	Charge moyenne (j/h)
2022	1.25
2023	2.55
2024	4.17
2025	4.01
Total général	3.73

Durant l'accord-cadre arrivant à échéance (T2 2022 à 2025 compris), la partie Réséda Socle a fait l'objet de petites évolutions et de 4 évolutions majeures :

- 2 pour des montées majeures de version du progiciel EBX-Platform (dont le portage d'EBX 5.9 à EBX 6.1.4)
- 2 respectivement pour des actions de chasse à l'obsolescence technique, tant sur le progiciel EBX-Platform que sur des montées de version majeure des couches basses (RedHat / Apache / Tomcat / OpenJDK) et des frameworks et librairies Java du code spécifique ajouté pour les parties spécifiques dont notamment le portail Réséda ; également une action de chasse aux services dépréciés EBX, d'adaptation suite à des API non publiques retirées

Également, en termes d'activité demandée au titulaire actuel et à titre d'exemples n'engageant pas le CNRS sur les demandes à venir auprès du futur titulaire, les référentiels ont fait l'objet de prestations pour fourniture de Manuels Utilisateurs (MUT), de mémentos et de didacticiels.

Enfin des préparations de formations (production de valises pédagogiques / préparation de jeux de données anonymisés / sessions de formations de formateurs internes) ont été commandées au titulaire actuel.

3.1.2 Fonctionnalités du référentiel Personnel (Personnels des unités CNRS)

Les fonctionnalités principales sont regroupées en plusieurs thèmes

- Intégration entrante du référentiel des personnels CNRS (SIRH CNRS Sirhus / SAP)
- Intégration entrante avec des SIRH d'établissements partenaires du CNRS pour des personnels non CNRS présents dans les unités
- Intégration entrante des projets de structure (SI Otarie) pour la mise en place des personnels non CNRS
- Intégration entrante des dossiers de personnels issus de SIRH autres que le SIRH CNRS (SIRH de partenaires de l'ESR)
- Appui interne sur les référentiels Partenaire et Structure (les données du référentiel Personnel font référence aux données des référentiels Partenaire et Structure)
- Exposition (vers d'autres SI) des références du référentiel Personnel sous 2 formats pivots (1 format complet et 1 format « light »)
- Mise à jour depuis Réséda d'un personnel CNRS présent dans une unité CNRS
- Création / mise à jour dans Réséda d'un personnel non CNRS présent dans une unité CNRS
- Création / mise à jour d'une personne présente dans une unité sans être pour autant un personnel de l'unité
- Répartition des personnels de l'unité au sein de l'organisation interne de l'unité
- Déclaration des responsables RH pour le CNRS au sein d'une unité (pour la gestion de proximité des personnels CNRS)
- Déclaration des prix et distinctions des personnels CNRS et non CNRS
- Déclaration des services / équipes pour la gestion dématérialisée RH pour le CNRS
- Déclaration, validation voire autorisations temporaires d'incompatibilités des fonctions métiers des personnels CNRS et non CNRS
- Déclaration de cosentements
- Prise en compte des restructurations des établissements
- Consultation du référentiel
- Exploitation du référentiel (au sens des traitements « batch » récurrents de nuit notamment)
- Aide à la gestion du laboratoire (exports prédéfinis)
- Contrôle a priori et a posteriori de la qualité des données du référentiel (gestion des doublons, détection des doublons potentiels)
- Administration métier du référentiel
- Gestion de l'aide en ligne, des didacticiels, des mémentos

Profils des utilisateurs

Profil	Actions à mener dans le cadre de sa fonction
Administrateur technique	■ Saisie des informations de l'ensemble du référentiel Personnel ■ Validation des informations de l'ensemble du référentiel Personnel ■ Visualisation des informations de l'ensemble du référentiel Personnel

Profil	Actions à mener dans le cadre de sa fonction
Administrateur fonctionnel	- Saisie des informations de l'ensemble du référentiel Personnel et des nomenclatures associées - Validation des informations de l'ensemble du référentiel Personnel et des nomenclatures associées - Visualisation des informations de l'ensemble du référentiel Personnel et des nomenclatures associées
Gestionnaire RH de la structure	Consultation et mise à jour (étape de saisie du processus de gestion de personnel) des personnels CNRS ou non CNRS des structures, autorisées au gestionnaire RH de la structure dans l'annuaire Réséda (par défaut, celles définies dans Janus, et potentiellement des structures attribuées par un administrateur fonctionnel, pour une période donnée)
Administrateur RH de la structure	Consultation et mise à jour (étape de validation du processus de gestion du personnel) des personnels CNRS ou non CNRS des structures autorisées au gestionnaire RH de la structure dans l'annuaire Réséda (par défaut, celles définies dans Janus, et potentiellement des structures attribuées par un administrateur fonctionnel, pour une période donnée)
Gestionnaire Institut	Consultation en mode restreint de tous les personnels présents et à venir des structures relevant de l'institut de l'utilisateur (cf casquette)
Responsable Sécurité Systèmes Informations national	- Validation des processus de mise à jour des fonctions métiers - Visualisation de l'ensemble des fonctions métiers SSI
Valideur de fonction métier	Validation des processus de mise à jour des fonctions métiers
Lecteur Institut, Direction	Accès en lecture à l'intégralité des attributs pour tous les personnels
Lecteur réduit à une liste d'attributs	Accès en lecture aux données correspondantes à celles exposées dans l'Annuaire (voir R-PER-JUR-005) pour tous les personnels « présents » souhaitant exposer leurs informations
Lecteur sur ses propres données	Accès en lecture à l'intégralité des attributs pour ses propres données
Lecteur réduit à une liste de personnels	- Accès en lecture en tous les enregistrements dont le personnel présente un lien aux implantations en vigueur ou dans le futur sur une structure qui relève d'un établissement partenaire. - Une structure relève d'un établissement partenaire quand il a un lien « Etablissement de rattachement » avec un rôle DGG à « délégué principal » et un type de partenariat à « Tutelle »
Lecteur DR	Accès en lecture à l'intégralité des attributs pour tous les personnels possédant au moins un lien en vigueur avec une implantation (ou emplacement non CNRS) relevant de sa DR
Lecteur DR réduit à une liste d'attributs	Accès en lecture à tous les personnels avec un accès restreint sur certains attributs

Éléments de volumétrie permettant de mieux appréhender la complexité

Éléments	Volume
Nombres d'objets métiers	81
Nombre de cas d'utilisation	75
Nombre de règles de gestion	658
Nombre de crons	18
Nombre de flux entrants	5
Nombre de flux sortants	4

Volumétrie d'écrans spécifiques

Nombre d'écrans spécifiques	Localisation / Fonction
1	Fiche de synthèse
1	Recherche approchante dans les workflows
1	Gestion des dédoubleonnages a posteriori
3	Workflow de changement d'implantation
1	Workflow de gestion des UHPI (Usagers/Hébergés/Prestataires/Invités)
1	Service de rattachement en masse des personnels aux sous structures
10	Saisie guidée pour déclaration des présences des personnels
3	Gestion des fonctions métiers (déclaration + validation + exception)
6	Echange entrant SIRH externes (paramétrage du partenaire + import des données SIRH + rapprochement de 1 ^{er} niveau + rapprochement du 2 nd niveau + validation des mises à jour + rapport d'intégration)

Volumétrie et charge moyenne (jours de développement) des mantis Personnel (correctif & évolutif) sur les 3 dernières années(Depuis T2 2022 jusqu'à 2025 inclus)

Personnel	
Sévérité	Nombre de mantis
2022	211
bloquant	5
majeur	100
mineur	106
2023	193
bloquant	1
majeur	101
mineur	91
2024	84
bloquant	4
majeur	44
mineur	36
2025	107
majeur	54
mineur	53
Total général	595

Personnel	
Année	Charge moyenne (j/h)
2022	2.30
2023	2.45
2024	3.52
2025	2.67
Total général	2.56

Durant l'accord-cadre arrivant à échéance (T2 2022 à 2025 compris), la partie Réséda Personnel a fait l'objet de petites évolutions et de 3 évolutions majeures :

- 1 pour les fonctions métiers généralisées
- 1 pour une gestion plus centralisée des doublons potentiels détectés lors des demandes de créations de dossiers
- 1 pour l'appui sur des dossiers issus de SIRH autres que le SIRH du CNRS

3.1.3 Fonctionnalités du référentiel Structure

Les fonctionnalités sont les suivantes

- Intégration avec le référentiel des projets de contractualisation des structures CNRS (SI Otarie) – préparation du référentiel à l'année + 1
- Appui interne sur les référentiels Partenaire et Personnel (les données du référentiel Structure font référence aux données des référentiels Partenaire et Personnel)
- Exposition (vers d'autres SI) des références du référentiel Structure sous 2 formats pivots (1 format complet et 1 format « light »)
- Consultation d'une structure (CNRS ou non CNRS)
- Mise à jour d'une structure (unité CNRS)
- Création / Mise à jour d'une structure non CNRS (unité non CNRS)
- Déclaration de l'organisation interne d'une unité
- Déclaration des mandataires et gestionnaires de contrats
- Gestion des répartitions des unités de recherche sur les sites de la recherche
- Gestion des relations fonctionnelles et organisationnelles entre les entités du CNRS (unité / institut / DR / direction)
- Gestion des implantations géographiques des unités
- Description scientifique de l'unité (thématiques / start up / réseau / composante / laboratoire commun, ...)
- Exploitation du référentiel
- Génération d'un graphe présentant la filiation éventuelle des structures CNRS
- Génération de l'organigramme interne de l'unité
- Génération d'indicateurs statistiques
- Administration métier du référentiel
- Gestion de l'aide en ligne, des didacticiels
- Mise à disposition d'images du référentiel sur des périodes passées

Profils des utilisateurs

Profils	Actions à mener dans le cadre de sa fonction
Lecteur	• Accès en lecture aux données du référentiel structure
Lecteur structure non CNRS	• Accès en lecture aux données des structures non CNRS (structures, responsables, emplacements)
Gestionnaire Unité	• Saisie des informations caractérisant l'unité dans laquelle le gestionnaire exerce sa fonction • Visualisation des informations caractérisant l'unité dans laquelle le gestionnaire exerce sa fonction et des nomenclatures externes utilisées par le référentiel Structure
Responsable Unité	• Saisie des informations caractérisant l'unité dans laquelle le responsable exerce sa fonction • Validation des informations caractérisant l'unité dans laquelle le responsable exerce sa fonction • Visualisation des informations caractérisant l'unité dans laquelle le responsable exerce sa fonction et des nomenclatures externes utilisées par le référentiel Structure
Gestionnaire DR	• Visualisation des informations caractérisant les unités rattachées à la DR pour laquelle le gestionnaire DR exerce sa fonction et des nomenclatures externes utilisées par le référentiel Structure

Profils	Actions à mener dans le cadre de sa fonction
	Saisie des informations caractérisant les implantations rattachées à la DR pour laquelle le gestionnaire DR exerce sa fonction
Gestionnaire Structure Opérationnelle	- Saisie et validation des informations caractérisant les unités opérationnelles dépendantes de l'institut principal référent dans lequel le gestionnaire exerce sa fonction - Visualisation des informations de l'ensemble du référentiel Structure et des nomenclatures externes utilisées par le référentiel Structure
Gestionnaire Structure Administrative	- Saisie et validation des informations caractérisant les unités administratives et opérationnelles non scientifiques (catégorie de structure = « administrative ») - Visualisation des informations de l'ensemble du référentiel Structure et des nomenclatures externes utilisées par le référentiel Structure
Gestionnaire Structure non CNRS	- Saisie des informations de toutes les structures non CNRS et crée des structures non CNRS - Visualisation des informations de l'ensemble du référentiel Structure et des nomenclatures externes utilisées par le référentiel Structure
Administrateur Technique	- Saisie des informations de l'ensemble du référentiel Structure et des nomenclatures externes utilisées par le référentiel Structure - Validation des informations de l'ensemble du référentiel Structure et des nomenclatures externes utilisées par le référentiel Structure - Visualisation des informations de l'ensemble du référentiel Structure et des nomenclatures externes utilisées par le référentiel Structure
Administrateur Fonctionnel	- Saisie des informations de l'ensemble du référentiel Structure et des nomenclatures externes utilisées par le référentiel Structure - Validation des informations de l'ensemble du référentiel Structure et des nomenclatures externes utilisées par le référentiel Structure - Visualisation des informations de l'ensemble du référentiel Structure et des nomenclatures externes utilisées par le référentiel Structure
Lecteur partenaire	Accès en lecture aux données du référentiel structure. Les données visibles se limite aux structures possédant un établissement de rattachement en vigueur ou dans le futur dont le lecteur est partenaire

Eléments de volumétrie permettant de mieux appréhender la complexité

Eléments	Volume
Nombres d'objets métiers	63
Nombre de cas d'utilisation	28
Nombre de règles de gestion	400
Nombre de crons	9
Nombre de flux entrants	2
Nombre de flux sortants	3

Volumétrie d'écrans spécifiques

Nombre d'écrans spécifiques	Localisation/Fonction
1	Fiche de synthèse
1	Service de tri
1	Qualité du référentiel structures
1	Filiation des structures
1	Organigrammes des sous structures

Volumétrie et charge moyenne (jours de développement) des mantis Structure (correctif & évolutif) sur les 3 dernières années(Depuis T2 2022 jusqu'à 2025 inclus)

Structure	
Sévérité	Nombre de mantis
2022	35
bloquant	2
majeur	16
mineur	17
2023	30
majeur	14
mineur	16
2024	24
bloquant	1
majeur	9
mineur	14
2025	34
majeur	10
mineur	24
Total général	123

Structure	
Année	Charge moyenne (j/h)
2022	1.33
2023	1.54
2024	2.17
2025	3.50
Total général	1.84

Durant l'accord-cadre arrivant à échéance (T2 2022 à 2025 compris), la partie Réséda Structure a fait l'objet de petites évolutions et d'1 évolution majeure :

- 1 pour la déclaration des gestionnaires et mandataires de contrats dans les unités

Également, en termes d'activité demandée au titulaire actuel et à titre d'exemples n'engageant pas le CNRS sur les demandes à venir auprès du futur titulaire, la partie Réséda Structure a fait l'objet de prestations pour fourniture de Manuels Utilisateurs (MUT), de mémentos et de didacticiels.

Enfin des préparations de formations (production de valises pédagogiques / préparation de jeux de données anonymisés / sessions de formations de formateurs internes) ont été commandées au titulaire actuel.

3.1.4 Fonctionnalités du référentiel Fournisseur

Les fonctionnalités sont les suivantes

- Intégration avec le SI Finances (SI BFC / SAP) ; c'est-à-dire réception des références de fournisseur issues du SAP Finances (BFC) et boucle « Réséda Fournisseur / BFC / Réséda Fournisseur » pour la création ou la mise à jour de référence en fin de workflow dans Réséda Fournisseur
- Alimentation depuis un référentiel externe « Dun&Bradstreet » (API Altares) du formulaire de création d'un fournisseur
- Processus d'acquisition ou de mise à jour des références Fournisseur
- Processus de suivi et pilotage des workflows d'acquisition et de mise à jour de références Fournisseur
- Processus de suivi continu de la qualité du référentiel Fournisseur (gestion des doublons, détection des doublons potentiels)
- Dépôt et consultation de pièces jointes
- Consultation du référentiel Fournisseur
- Administration métier du référentiel
- Production d'indicateurs de gouvernance du référentiel Fournisseur

Profils des utilisateurs

Rôle	Actions à mener dans le cadre de sa fonction
Lecteur	■ Accès en lecture au référentiel Fournisseur
Gestionnaire Financier Unité	■ Demande de création de fournisseur ■ Demande de modification de fournisseur (hors suppression, blocage et cession/opposition, suppression d'un RIB, modification/ suppression d'un Tiers divergent fixe ou autorisé, modification du mode de paiement, modification des conditions de paiement) ■ Accès en lecture aux informations caractérisant les fournisseurs
Gestionnaire Financier DR	■ Demande de création de fournisseur ■ Demande de modification (hors cession/opposition) de fournisseur ■ Accès en lecture aux informations caractérisant les fournisseurs
ACS Caissier	■ Demande de création de fournisseur ■ Demande de modification de fournisseur ■ Accès en lecture aux informations caractérisant les fournisseurs
Gestionnaire Tiers SCTD	■ Demande de création de fournisseur ■ Enrichissement et validation des demandes de création d'un fournisseur ■ Demande de modification de fournisseur ■ Enrichissement et validation des demandes de modification d'un fournisseur ■ Accès en lecture aux informations caractérisant les fournisseurs ■ Gestion des doublons
Administrateur Technique	■ Saisie des informations de l'ensemble du référentiel Fournisseur et des nomenclatures externes utilisées par le référentiel Fournisseur ■ Validation des informations de l'ensemble du référentiel Fournisseur et des nomenclatures externes utilisées par le référentiel Fournisseur

Rôle	Actions à mener dans le cadre de sa fonction
	Visualisation des informations de l'ensemble du référentiel Fournisseur et des nomenclatures externes utilisées par le référentiel Fournisseur
Administrateur Fonctionnel	- Saisie des informations de l'ensemble du référentiel Fournisseur et des nomenclatures externes utilisées par le référentiel Fournisseur - Validation des informations de l'ensemble du référentiel Fournisseur et des nomenclatures externes utilisées par le référentiel Fournisseur - Visualisation des informations de l'ensemble du référentiel Fournisseur et des nomenclatures externes utilisées par le référentiel Fournisseur - Supervision des workflows de données - Gestion des doublons

Éléments de volumétrie permettant de mieux appréhender la complexité

Eléments	Volume
Nombres d'objets métiers	20
Nombre de cas d'utilisation	23
Nombre de règles de gestion	200
Nombre de crons	7
Nombre de flux entrants	2
Nombre de flux sortants	1

Volumétrie d'écrans spécifiques

Nombre d'écrans spécifiques	Localisation/Fonction
1	Workflow fournisseur

Volumétrie et charge moyenne (jours de développement) des mantis Fournisseur (correctif & évolutif) sur les 3 dernières années

(Depuis T2 2022 jusqu'à 2025 inclus)

Fournisseur	
Sévérité	Nombre de mantis
2022	6
majeur	1
mineur	5
2023	5
majeur	2
mineur	3
2024	20
bloquant	4
majeur	5
mineur	11
2025	13
majeur	2
mineur	11
Total général	44

Fournisseur	
Année	Charge moyenne (j/h)
2022	7.00
2023	2.50
2024	2.05
2025	0.25
Total général	2.69

Durant l'accord-cadre arrivant à échéance (T2 2022 à 2025 compris), la partie Réséda Fournisseur a fait l'objet de petites évolutions et d'1 évolution majeure pour les n° de marchés publics dans les coordonnées bancaires

3.1.5 Fonctionnalités du référentiel Contact

Les fonctionnalités sont les suivantes

- Appui interne sur le référentiel Partenaire et plus précisément sur les partenaires référençant les établissements publics de l'ESR (Enseignement Supérieur et de la Recherche) (les données du référentiel Contact font référence aux données du référentiel Partenaire)
- Appuis internes sur les référentiels Structure et Personnel (les données du référentiel Contact font référence aux données des référentiels Structure et Personnel)
- Exposition (vers d'autres SI) des références du référentiel Contact via 3 formats pivots (1 format pivot pour les contacts, 1 format pivot pour les établissements de l'ESR, 1 format pivot pour les regroupements des établissements de l'ESR)
- Processus d'acquisition ou de mise à jour des références Contact
- Déclaration des responsables d'établissement, des représentants CNRS aux conseils d'établissement de l'ESR, des responsables CNRS des sites de recherche
- Déclaration des regroupements d'établissements de l'ESR (éventuelles restructurations de l'ESR)
- Dépôt et consultation de pièces jointes
- Génération de plusieurs publipostages (exports prédéfinis et préformatés)
- Consultation du référentiel Contact
- Administration métier du référentiel

Profils des utilisateurs

Profil	Actions à mener dans le cadre de sa fonction
Administrateur technique	■ Saisie et validation des informations de l'ensemble du référentiel Contact ■ Visualisation des informations de l'ensemble du référentiel Contact ■ Saisie et validation des mises à jour en masse ■ Accès à la fonction de publipostage ■ Accès au répertoire des pièces jointes ■ Service de reconstruction du cache ■ Service de transfert des contacts
Administrateur fonctionnel	■ Saisie et validation des informations de l'ensemble du référentiel Contact et des nomenclatures associées ■ Visualisation des informations de l'ensemble du référentiel Contact et des nomenclatures associées ■ Saisie et validation des mises à jour en masse ■ Accès au service d'attribution des droits ■ Accès à la fonction de publipostage ■ Accès au répertoire des pièces jointes ■ Service de reconstruction du cache ■ Service de transfert des contacts

Profil	Actions à mener dans le cadre de sa fonction
Gestionnaire	- Saisie et validation des informations du référentiel Contact dans le cadre de son périmètre - Consultation de la nomenclature des sites ministériels - Accès à la fonction de publipostage - Accès au répertoire des pièces jointes
Lecteur Directoire	- Visualisation des informations de l'ensemble du référentiel Contact et des nomenclatures associées - Accès à la fonction d'export CSV - Accès à la fonction de publipostage
Lecteur (360°)	- Visualisation des informations de l'ensemble du référentiel Contact et des nomenclatures associées, sauf les informations sensibles / confidentielles - Accès à la fonction d'export CSV - Accès à la fonction de publipostage
Lecteur Délégation Régionale	- Visualisation des informations de l'ensemble du référentiel Contact liées à sa DR, sauf les regroupements - Accès à la fonction d'export CSV - Accès à la fonction de publipostage
Lecteur Site	- Visualisation des informations de l'ensemble du référentiel Contact liées à son site, sauf les regroupements. - Accès à la fonction d'export CSV - Accès à la fonction de publipostage

Éléments de volumétrie permettant de mieux appréhender la complexité

Eléments	Volume
Nombres d'objets métiers	18
Nombre de cas d'utilisation	12
Nombre de règles de gestion	50
Nombre de crons	1
Nombre de flux entrants	0
Nombre de flux sortants	2

Volumétrie et charge moyenne (jours de développement) des mantis Contact (correctif & évolutif) sur les 3 dernières années
(Depuis T2 2022 jusqu'à 2025 inclus)

Contact		Contact	
Sévérité	Nombre de mantis	Année	Charge moyenne (j/h)
2022	10	2022	2.00
mineur	10	2023	2.55
2023	42	2024	1.83
bloquant	3	2025	4.50
majeur	2	Total général	2.50
mineur	37		
2024	31		
bloquant	3		
majeur	5		
mineur	23		
2025	27		
majeur	7		
mineur	20		
Total général	110		

Durant l'accord-cadre arrivant à échéance (T2 2022 à 2025 compris), la partie Réséda Contact a surtout fait l'objet de petites évolutions.

3.1.6 Fonctionnalités du référentiel des caractéristiques des unités (PPST)

Les fonctionnalités sont les suivantes :

- Appui interne sur le référentiel Structure et Personnel (les données du référentiel PPST font référence aux données des référentiels Personnels et Structure)
- Exposition des références de ce référentiel sous un format pivot restreint à une application appelante
- Processus d'acquisition ou de mise à jour des caractéristiques des unités PPST
- Génération d'exports
- Dépôt et consultation de pièces jointes
- Prise en compte des impacts des restructurations cycliques (annuelles principalement) des structures de recherche CNRS sur les structures du référentiel PPST
- Consultation du référentiel des caractéristiques des unités
- Administration métier du référentiel
- Gestion d'un annuaire des utilisateurs dédié au référentiel des caractéristiques des unités

Profils des utilisateurs

Profil	Actions à mener dans le cadre de sa fonction
Administrateur technique	■ Nomination des Administrateurs fonctionnels ■ Fonctionnalité technique Réséda / EBX (création, fusion d'espace de travail, lancement des services techniques)
Administrateur fonctionnel	■ Toutes les fonctionnalités accessibles par les gestionnaires ■ Nomination des Administrateurs techniques et des gestionnaires

Profil	Actions à mener dans le cadre de sa fonction
Gestionnaire	■ Création et modification des caractéristiques ■ Consultation de l'historique ■ Accès aux documents d'informations ■ Export de données des caractéristiques ■ Export des personnels liés ■ Nomination des Lecteurs
Lecteur	■ Visualisation des informations de ce référentiel et des nomenclatures associées (dans la limite de son périmètre)

Éléments de volumétrie permettant de mieux appréhender la complexité

Eléments	Volume
Nombres d'objets métiers	4
Nombre de cas d'utilisation	8
Nombre de règles de gestion	38
Nombre de crons	1
Nombre de flux sortants	1

Volumétrie et charge moyenne (jours de développement) des mantis du réf des caractéristiques des unités (correctif & évolutif) sur les 3 dernières années
(Depuis T2 2022 jusqu'à 2025 inclus)

Caractéristiques des unités	
Sévérité	Nombre de mantis
2022	5
mineur	5
2024	6
bloquant	2
majeur	4
2025	5
majeur	3
mineur	2
Total général	16

Caractéristiques des unités	
Année	Charge moyenne (j/h)
2024	2.00
Total général	2.00

Durant l'accord-cadre arrivant à échéance (T2 2022 à 2025 compris), la partie Réséda caractéristiques des unités a surtout fait l'objet de petites évolutions.

3.1.7 Fonctionnalités du référentiel Courriel @cnrs.fr

Les fonctionnalités sont les suivantes

- Appui interne sur le référentiel Structure et Personnel (les données du référentiel Courriel font référence aux données des référentiels Personnels et Structure)
- Exposition des références du référentiel Courriel sous un format pivot 'Courriel'
- Intégration des réponses fournies par la brique messagerie via le format pivot 'Courriel' enrichi côté Messagerie
- Processus de détermination des dénominations (adresses électroniques) des courriels (gestion des homonymies)
- Détermination automatique des éligibilités à l'attribution automatique d'une boîte mail
- Service de demande d'attribution manuelle d'une boîte mail
- Demande exceptionnelle de libération d'une dénomination
- Gestion des changements d'état civil
- Gestion du cycle de vie des courriels en lien étroit avec le référentiel Personnel (entrée / sortie de personnels)
- Dépôt des courriels activés (adresses électroniques) dans les références du référentiel Personnel
- Processus d'initialisation en masse des dénominations déjà opérationnelles (pour la gestion des migrations de boîtes mails lors de changements d'infrastructures)
- Consultation du référentiel Courriel
- Administration métier du référentiel

Profils des utilisateurs

Profil	Actions à mener dans le cadre de sa fonction
Administrateur technique	■ Saisie des informations de l'ensemble du référentiel Courriel ■ Validation des informations de l'ensemble du référentiel Courriel ■ Visualisation des informations de l'ensemble du référentiel Courriel
Administrateur fonctionnel	■ Saisie des informations de l'ensemble du référentiel Courriel et des nomenclatures associées ■ Validation des informations de l'ensemble du référentiel Courriel et des nomenclatures associées ■ Visualisation des informations de l'ensemble du référentiel Courriel et des nomenclatures associées
Consultation courriel CNRS	■ Consultation et mise à jour des courriels CNRS

Éléments de volumétrie permettant de mieux appréhender la complexité

Éléments	Volume
Nombres d'objets métiers	10
Nombre de cas d'utilisation	13
Nombre de règles de gestion	38
Nombre de crons	4
Nombre de flux entrants	1
Nombre de flux sortants	1

Volumétrie et charge moyenne (jours de développement) des mantis Courriel cnrs.fr (correctif & évolutif) sur les 3 dernières années

(Depuis T2 2022 jusqu'à 2025 inclus)

Courriels	
Sévérité	Nombre de mantis
2022	9
bloquant	1
majeur	3
mineur	5
2023	6
bloquant	1
majeur	3
mineur	2
2024	7
majeur	5
mineur	2
2025	3
mineur	3
Total général	25

Courriels	
Année	Charge moyenne (j/h)
2023	0.50
2025	4.25
Total général	3.31

Durant l'accord-cadre arrivant à échéance (T2 2022 à 2025 compris), la partie Réséda Courriel @cnrs.fr a surtout fait l'objet de petites évolutions.

3.1.8 Fonctionnalités du référentiel Partenaire

Les fonctionnalités sont les suivantes :

- Alimentation depuis un référentiel externe (Sirene - INSEE) pour les entreprises françaises (API DINUM)
Appui interne sur le référentiel Fournisseur (les données du référentiel Partenaire font référence aux données du référentiel Fournisseur)
- Exposition des références du référentiel Partenaire sous trois formats pivots : 1 format pivot « Partenaire », 1 format pivot « Etablissement » et 1 format pivot « Organisme »
- Gestion des doublons (dédoublonnage)
- Processus de déclaration ou de modification avec validation immédiate
- Processus de déclaration ou de modification avec validation différée
- Processus de gestion en masse
- Services de demande de création, de modification (API pour d'autres SI)
- Processus de Sirenage (réalignement périodique avec le référentiel français Sirene)
- Consultation du référentiel Partenaire
- Administration métier du référentiel

Profils des utilisateurs

Profil	Actions à mener dans le cadre de sa fonction
Administrateur technique	■ Saisie et validation des informations de l'ensemble du référentiel Partenaire et Paramétrage Partenaire ■ Visualisation des informations de l'ensemble du référentiel Partenaire et Paramétrage Partenaire ■ Recherche approchante ■ Saisie et validation des mises à jour en masse ■ Service de reconstruction du cache ■ Service de gestion des images (consultation) ■ Service de gestion des images (création) ■ Processus de mise à jour en masse par API ■ Processus de rapprochement fournisseur ■ Processus d'import du fichier mensuel SIRENE
Administrateur fonctionnel	■ Saisie et validation des informations de l'ensemble du référentiel Partenaire et des nomenclatures associées ■ Visualisation des informations de l'ensemble du référentiel Partenaire et des nomenclatures associées ■ Recherche approchante ■ Saisie et validation des mises à jour en masse ■ Accès au service d'attribution des droits ■ Service de gestion des images (consultation) ■ Processus de mise à jour en masse par API ■ Processus de rapprochement fournisseur
Gestionnaire	■ Saisie des informations du référentiel Partenaire dans le cadre de son périmètre ■ Visualisation des informations de l'ensemble du référentiel Partenaire et des nomenclatures associées ■ Recherche approchante
Gestionnaire Prioritaire	■ Saisie des informations du référentiel Partenaire dans le cadre de son périmètre ■ Visualisation des informations de l'ensemble du référentiel Partenaire et des nomenclatures associées ■ Recherche approchante
Lecteur sans restriction	■ Visualisation des informations de l'ensemble du référentiel Partenaire et des nomenclatures associées ■ Recherche approchante
Consultation partenaire	■ Visualisation des informations de l'ensemble du référentiel Partenaire et des nomenclatures associées, sauf les informations non diffusibles ■ Recherche approchante sur l'ensemble du réf. partenaire, sauf les partenaires dont le statut est non diffusible

Éléments de volumétrie permettant de mieux appréhender la complexité

Éléments	Volume
Nombres d'objets métiers	23
Nombre de cas d'utilisation	17
Nombre de règles de gestion	584
Nombre de crons	2
Nombre de flux entrants	3
Nombre de flux sortants	3
Nombre d'écrans spécifiques	5

Volumétrie et charge moyenne (jours de développement) des mantis Partenaire (correctif & évolutif) sur les 3 dernières années

(Depuis T2 2022 jusqu'à 2025 inclus)

Partenaires

Sévérité	Nombre de mantis
2022	131
bloquant	1
majeur	8
mineur	122
2023	125
majeur	10
mineur	115
2024	78
bloquant	3
majeur	15
mineur	60
2025	100
majeur	3
mineur	97
Total général	434

Partenaires

Année	Charge moyenne (j/h)
2022	3.30
2023	2.73
2024	4.54
2025	4.50
Total général	3.38

Durant l'accord-cadre arrivant à échéance (T2 2022 à 2025 compris), la partie Réséda Partenaire a principalement fait l'objet de développements pour des compléments de conception, de sa recette complète et de son déploiement en production. Des petites évolutions sont venues post ouverture afin de stabiliser le référentiel.

3.1.9 Fonctionnalités de l'annuaire CNRS basé sur les référentiels Structure et Personnel

Cet annuaire comprend deux volets : un volet « grand public » (internet) et un volet « CNRS » (intranet).

Le volet « CNRS » s'adresse à tous les personnels présents dans les unités du CNRS (personnels déclarés dans Réséda Personnel, que le personnel soit CNRS ou non CNRS).

Ce volet « CNRS » est présenté dès lors que l'utilisateur s'est authentifié au préalable. Une fois authentifié, aucune restriction sur les données ou les recherches (restriction sur les données, sur les recherches, etc) n'est appliquée.

Le volet « grand public » est destiné à tout internaute et est accessible sans authentification.

Techniquement, l'annuaire CNRS est en dehors de la plateforme Réséda.

Il s'agit d'un site web développé en Java, s'exécutant dans un serveur d'application Tomcat installé sur un système d'exploitation Linux.

L'annuaire CNRS n'embarque pas de persistance de données dédiée pour son utilisation.

Il s'appuie :

- Sur des données métiers (formats pivots Réséda Structure et formats pivots Réséda Personnel) et des nomenclatures métiers ; toutes ces informations sont hébergées dans des collections MongoDB elles-mêmes alimentées depuis les services sortants Réséda Structure et Réséda Personnel appelés par la couche EAI/ESB du SI du CNRS
- Sur des données techniques pour du paramétrage de l'application, hébergées dans la plateforme Réséda, dans un référentiel dédié à l'hébergement de paramétrage applicatif pour des applications autres que Réséda.

L'annuaire CNRS est composé de 3 parties applicatives :

1. Un site web développé en Java (OpenJDK 17) et s'appuyant sur des frameworks (*Spring version 5.3.36, Bootstrap version 5.3.3, ...*) ; site accessible sur Internet
2. Un service de présentation en charge du rendu graphique, accessible par service Rest (uniquement par des applications autorisées, à travers l'EAI/ESB CNRS)
3. Un service de données, accessible par service Rest (uniquement par des applications autorisées, à travers l'EAI/ESB)

Les trois parties applicatives listées ci-dessus peuvent s'exécuter chacune sur leur propre serveur d'application ou sur un serveur d'application commun. Dans le contexte actuel, l'utilisation d'un serveur d'application commun est la configuration mise en œuvre sur tous les environnements (intégration / recette / production).

A noter que ces développements se font directement par l'équipe du titulaire sur la forge logicielle de la DSI du CNRS.

Éléments de volumétrie permettant de mieux appréhender la complexité

Éléments	Volume
Nombre de cas d'utilisation	27
Nombre de règles de gestion	234
Nombre d'écrans	36

Volumétrie et charge moyenne (jours de développement) des mantis Annuaire CNRS (correctif & évolutif) sur les 3 dernières années

(Depuis T2 2022 jusqu'à 2025 inclus)

Annuaire des labos	
Sévérité	Nombre de mantis
2022	12
bloquant	2
majeur	7
mineur	3
2023	20
majeur	2
mineur	18
2024	10
bloquant	2
majeur	2
mineur	6
2025	13
bloquant	1
majeur	1
mineur	11
Total général	55

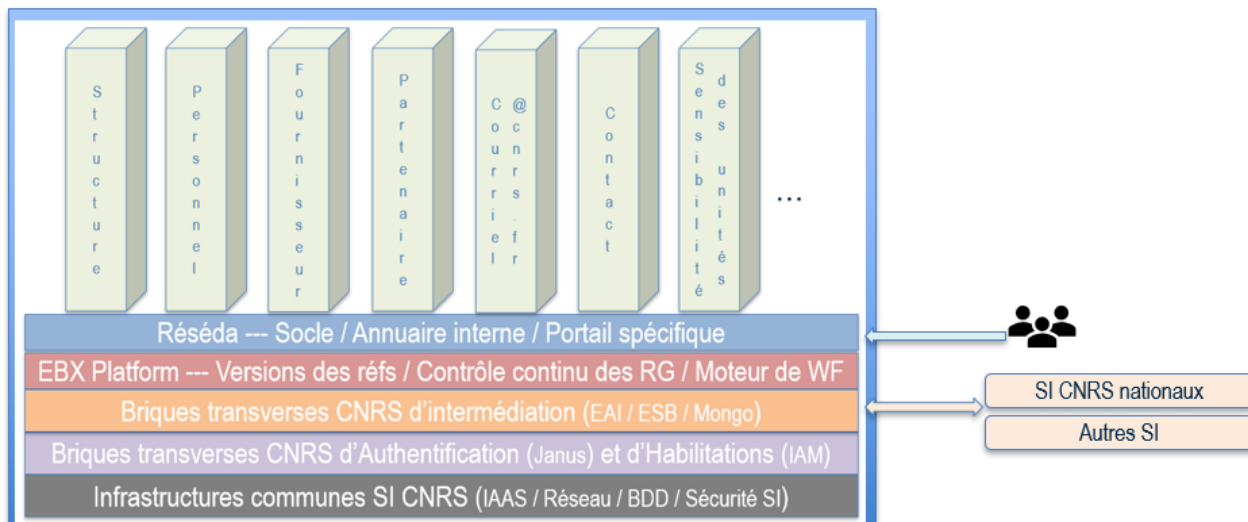
Annuaire des labos	
Année	Charge moyenne (j/h)
2022	3.30
2023	2.73
2024	4.54
2025	4.50
Total général	3.38

Durant l'accord-cadre arrivant à échéance (T2 2022 à 2025 compris), la partie Annuaire CNRS a fait l'objet d'1 opération complète de chasse à la dette technique (couches basses + Framework + Librairies) ainsi que des petites évolutions.

3.2 INTÉGRATION DANS LE SI

La plateforme Réséda est intégrée au SI du CNRS en s'appuyant sur :

- Les briques d'authentification et d'habilitations du SI du CNRS (Janus / IAM)
- La brique d'intermédiation du SI du CNRS composée d'une plateforme transverse de gestion des échanges d'information (EAI/ESB Fuse) et d'une persistance (stockage) des formats pivots au sein d'une base MongoDB.



3.3 PRÉSENTATION TECHNIQUE

3.3.1 Caractéristiques techniques générales

La plateforme Réséda fonctionne sur le serveur d'application Java / Tomcat installé sur une plateforme Linux. Les données sont stockées dans une base de données ODA Oracle (Oracle 19c début 2025).

Un important projet de migration de la version du progiciel EBX est en cours début 2025.

Elle vise le passage de la version EBX 5.9 vers la nouvelle architecture progicielle liée aux versions EBX 6.x

Début 2025, la version cible pour cette montée de version n'est pas déterminée. A minima, ce sera la version EBX 6.2 sortie fin 2024 (si suffisante pour atteindre les mêmes niveaux de performance que la version en production début 2025 EBX 5.9.26).

Autrement dit, début 2025 l'éditeur Tibco est toujours en phase d'ajustement de son architecture « made in EBX6 » via des versions régulières mises à disposition pour améliorer, faciliter les portage EBX5 vers EBX6.

D'ici le début du futur marché lié à cet appel d'offres, la version cible du portage peut avoir évoluée.

Tous les environnements Réséda sont hébergés sur le centre serveur IN2P3. Réséda utilise les infrastructures du domaine « transverse » de ce centre et bénéficie à ce titre de l'architecture de sécurité et du pool d'outils d'administration.

L'architecture de Réséda est supervisée via l'outil CNRS Panoptes (basé sur la solution de supervision Centreon).

3.3.2 Architecture Réséda

Réséda production se compose de cinq serveurs :

- Deux serveurs pour le portail Réséda : identiques, point d'entrée de la plateforme Réséda pour les utilisateurs finaux et fonctionnant en mode load balancing
- Un premier serveur EBX dit « master 1 / M1 » disposant des référentiels du Socle (dont l'annuaire interne), Courriel (@cnrs.fr), Contact, Partenaire, Personnel, Structure, Sirene (copie du référentiel INSEE)
- Un second serveur EBX dit « master 2 / M2 » disposant du référentiel Fournisseur.
- Un troisième serveur EBX dit « master 3 / M3 » disposant du référentiel Caractéristiques des unités.

Le serveur EBX master 1 constitue un nœud important dans la mesure où ce dernier est maître sur le Socle et sert donc d'une part à assurer la connexion des utilisateurs, et d'autre part à construire les pages du portail Réséda.

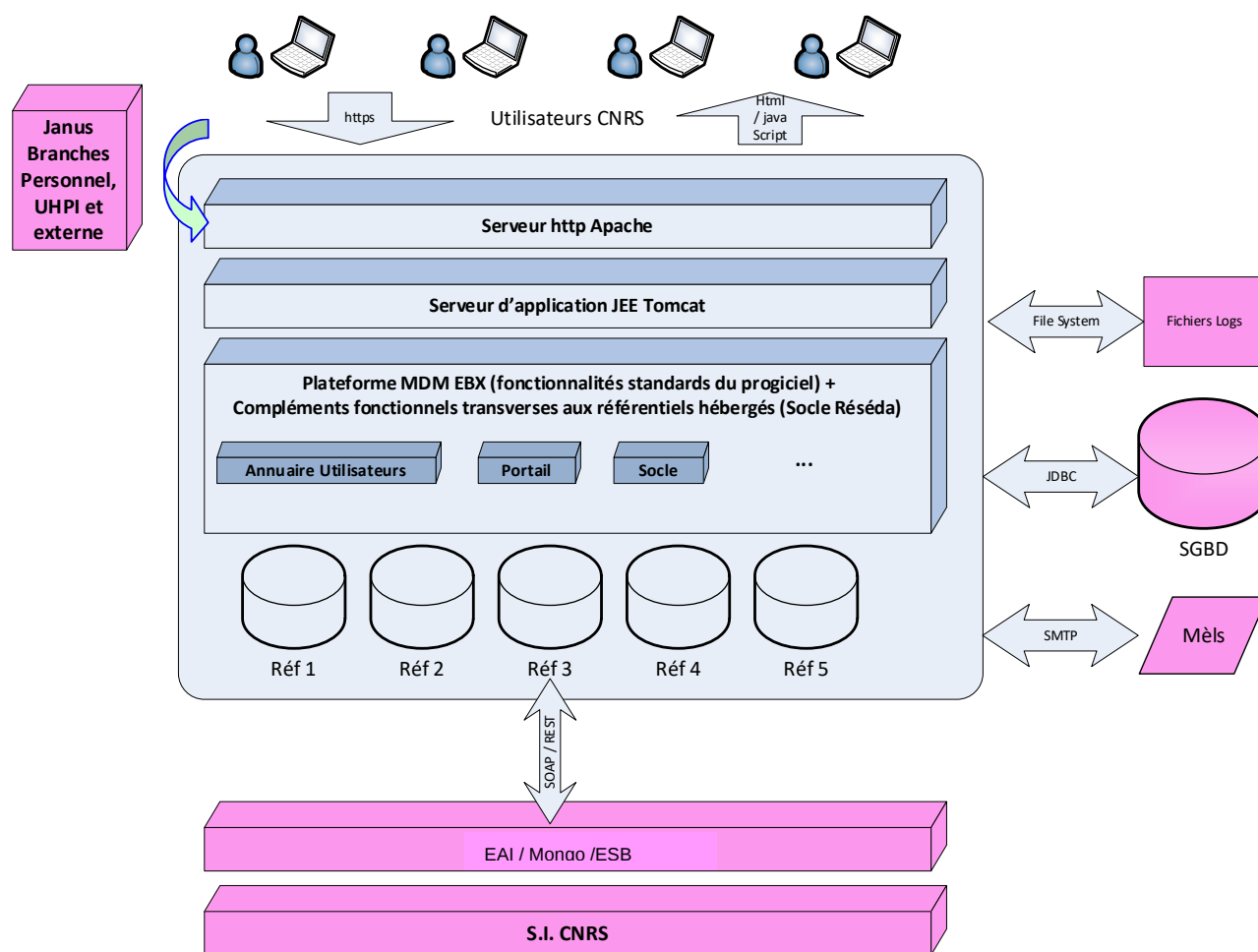
Les pages web du portail se composent d'un bandeau et d'un menu construit dynamiquement par le portail et d'iframes pointant vers les instances masters EBX 1, 2 & 3 suivant le référentiel concerné.

Des répliques régulières de référentiels existent entre les instances EBX via le mécanisme standard du progiciel « mode Hub D3 ».

Le module standard EBX SQLConnect est activé sur certains référentiels afin de répliquer quotidiennement les données de ces points de vérité vers des tables accessibles en lecture seule via un requêteur externe (début 2025 via l'outil ISQLIENT d'Oracle).

Ces tables de réplica sont stockées dans le schéma Oracle de l'instance EBX maître des référentiels concernés par ladite réplique.

3.3.3 Architecture logicielle Réséda



L'architecture applicative de la plateforme RÉSEDA est composée de :

- Une base de données Oracle
- Une application web dite Portail Réséda (Apache, OpenJDK et Tomcat)
- De trois instances progiciel EBX (éditeur Tibco) qui sont autant d'applications web (Apache, OpenJDK et Tomcat)

3.3.4 Listes des couches basses implémentées

3.3.4.1 Serveur MASTER EBX

Nature	Logiciel	Commentaire
OS	Linux Red Hat 8.5	
Serveur HTTP	Apache 2.4	
Serveur applicatif	Tomcat 10	
Java	OpenJDK 17	
MDM	EBX 6	Addons EBX activés : Match and Merge (MAME), Digital Asset Management (DAM), Information Search (Tese), Insight
Machine	VMWare ou serveur physique	

3.3.4.2 *Serveur de Base de données*

L'ensemble de la plateforme Réséda est persisté sur une base de données Oracle qui est hébergée sur des serveurs dédiés exploités par d'autres équipes de la DSI du CNRS et dont la responsabilité ne fait pas partie du périmètre de cet appel d'offres.

La création des différents éléments constituant la base Oracle du référentiel est entièrement packagée dans les programmes standard EBX. Le progiciel est de type « model driven » et les ajustements de modélisation sont automatiquement transcrits dans la base de données sans intervention des équipes DBA ou autres.

Chaque instance EBX maître doit disposer de son propre schéma de base de données

Nature	Logiciel
OS	Linux
BD	Oracle

3.3.5 Architecture technique Réséda

3.3.5.1 *Caractéristiques, spécificités*

L'architecture s'appuie sur les infrastructures mutualisées du domaine transverse du centre serveur IN2P3 du CNRS :

- Accès et raccordement réseau
- Logique de sécurisation
- Sauvegardes des serveurs et des bases de données

3.3.5.2 *Schémas de l'architecture haute disponibilité*

La plateforme Réséda est considérée comme une application critique ; en conséquence elle est installée en production dans un environnement suffisamment disponible.

Cela se traduit en termes d'infrastructure pour l'environnement de production par un appui sur une architecture haute disponibilité basée sur :

- Des serveurs d'applications (VM) hébergeant les instances portail d'une part et des serveurs d'applications hébergeant les instances EBX d'autre part ; un Load Balancer qui répartit la charge entre les deux instances du portail Réséda.
- La mise en œuvre d'une architecture orientée « silo application » basée sur des unités logiques de stockage dédiées à chaque instance EBX. Chaque serveur peut voir une ou plusieurs unités logiques de stockage.
- La persistance des données en haute disponibilité s'appuie sur une solution Oracle ; la combinaison avec le point précédent permet d'avoir un PRA (Plan de Reprise d'Activité) sur la partie Applicative Réséda.

3.3.5.3 *Environnements Réséda*

Il existe 4 environnements :

- un environnement d'intégration pour le titulaire en amont de la livraison pour recette CNRS
- un environnement de recette CNRS
- un environnement de production
- un environnement de formation

Tous ces environnements sont supportés par les infrastructures CNRS. Le CNRS a en charge le maintien de ces infrastructures et prend en charge les montées de version des couches basses (en accord et de manière concertée avec le titulaire).

En ce qui concerne les installations applicatives sur l'environnement d'intégration, le titulaire a en charge le déroulement des installations (en coordination avec l'équipe projet DSI Réséda), notamment pour valider les MINS (Manuels d'INStallation) qui seront livrés au CNRS pour les installations par les équipes CNRS sur les environnements de recette, de production et de formation.

Comme cité précédemment les installations applicatives sur les environnements de recette et de production sont déroulées par l'équipe CNRS d'exploitation (en coordination avec l'équipe projet DSI Réséda). Le titulaire peut être amené à être en soutien pour certaines installations sensibles ou importantes.

3.4 VOLUMÉTRIE DU SPÉCIFIQUE IMPLÉMENTÉ PAR L'INTÉGRATEUR AUTOUR DU PROGICIEL EBX

Le tableau ci-dessous concerne les développements complémentaires de contextualisation pour le CNRS réalisés depuis la mise en œuvre de la plateforme Réséda, dont le titulaire actuel à la charge MOE-d.

Module	Lignes de code	Classes	Méthodes
Réséda	595096	4363	28958
Total	595096	4363	28958

3.5 VOLUMÉTRIES DE DONNÉES ET D'UTILISATEURS

Références	Référentiel Structure	Environ 6 000 références de structures CNRS Environ 1 200 références de structures non CNRS
	Référentiel Personnel	Environ 450 000 références
	Référentiel Fournisseurs	Environ 295 000 références
	Référentiel Contact	Environ 1 400 références
	Référentiel Partenaire	Environ 45 000 références
	Référentiel Courriel @cnrs.fr	Environ 95 000 références
Utilisateurs	Nombre d'utilisateurs déclarés	Environ 5 000 utilisateurs par mois
	Nombre de visites	En moyenne 15 000 visites par mois
	Nombre d'utilisateurs sur une journée ouvrée	En moyenne, entre 500 et 1 500

3.6 DONNÉES D'EXPLOITATION

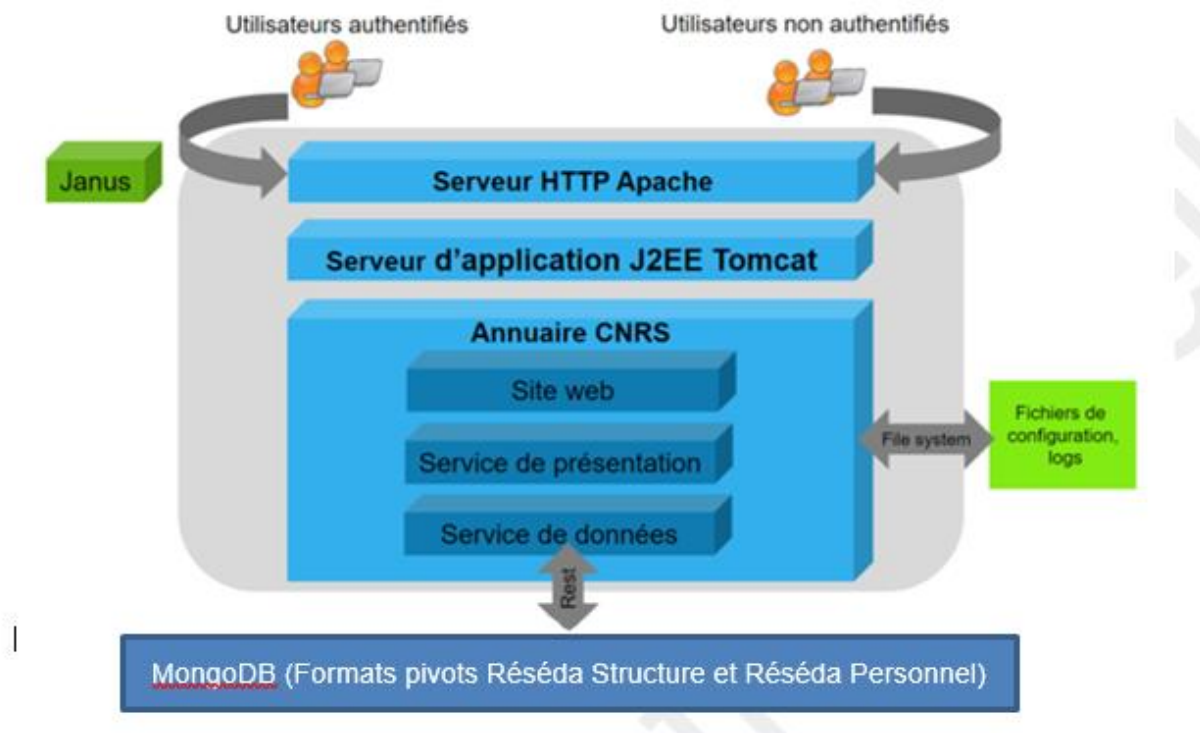
Volumétrie entre 2022 et 2025 inclus

- plus de 998 000 workflows
- plus de 1 800 000 versions de travail des référentiels (workflows / flux entrants / administration)
- plus de 2 750 000 transactions EBX sur les points de vérité (N actions C/U/D par transactions EBX)
- plus de 190 000 pièces jointes liées
- plus de 3 400 vues personnalisées créées et enregistrées par les utilisateurs finaux
- plus de 640 filtres personnalisés enregistrés par les utilisateurs finaux
- plus de 34 000 exports de données réalisés
- BDD de production = 360 Go de données utiles

3.7 CAS PARTICULIER DE L'ANNUAIRE CNRS (ANNUAIRE DES LABORATOIRES)

L'annuaire CNRS est un site web développé en Apache, OpenJDK et Tomcat, répondant à la charte graphique CNRS (notamment pour sa cible « grand public »),

L'annuaire CNRS est composé des 3 applications suivantes : site web, service de présentation et service de données.



Les applications décrites ci-dessus peuvent s'exécuter chacune sur leur propre serveur d'application ou sur un serveur d'application commun. L'utilisation d'un serveur d'application unique et donc commun aux 3 applications est le choix retenu en production depuis son ouverture en octobre 2021.

Environnements Annuaire CNRS

Il existe 3 environnements :

- Un environnement d'intégration pour le titulaire en amont de la livraison pour recette CNRS
- Un environnement de recette CNRS
- Un environnement de production

Tous ces environnements sont supportés par les infrastructures CNRS. Le CNRS a en charge le maintien de ces infrastructures et prend en charge les montées de version des couches basses (en accord et de manière concertée avec le titulaire).

En ce qui concerne les installations applicatives sur l'environnement d'intégration, le titulaire a en charge le déroulement de ces installations (en coordination avec l'équipe projet DSI Réséda), notamment pour valider le bon déroulement du MINS (Manuel d'INStallation) qui sera fourni aux équipes CNRS pour les installations en environnement de recette et de production.

En ce qui concerne les installations applicatives sur les environnements de recette et de production, celles-ci sont déroulées par l'équipe CNRS d'exploitation (en coordination avec l'équipe projet DSI Réséda). Le titulaire peut être amené à être en soutien pour certaines installations sensibles ou importantes.

Serveurs

Nature	Logiciel
OS	Linux Red Hat 9
Serveur HTTP	Apache 2.4
Serveur applicatif	Tomcat 9
Java	openJDK 17
Machine	VMWare

Indications en termes de développement

A noter que ces développements se font directement sur la forge logicielle du CNRS.

Module	Lignes de code	Classes	Méthodes
Annuaire Des Laboratoires CNRS	35213	409	3643
Total	35213	409	3643

Indications en termes de nombre de connexions sur une année

Mois	Visiteurs différents	Visites	Pages
Jan 2024	9 637	25 802	1 124 331
Fév 2024	9 059	23 709	992 422
Mar 2024	9 589	25 443	1 083 145
Avr 2024	10 641	26 424	1 135 020
Mai 2024	9 513	21 570	917 078
Juin 2024	9 367	23 114	1 054 319
Juil 2024	8 781	23 029	1 104 651
Aoû 2024	6 528	14 238	581 901
Sep 2024	11 382	27 553	1 160 523
Oct 2024	12 561	30 280	1 329 569
Nov 2024	11 295	25 598	1 181 215
Déc 2024	10 250	23 315	955 170
Total	118 603	290 075	12 619 344

4 CADRE DE COHÉRENCE TECHNIQUE DE LA SOLUTION

Ce chapitre donne les exigences applicables à tout nouveau développement, que ce soit lors de la mise en œuvre d'une nouvelle application ou dans le cadre d'évolutions d'une application existante. Il n'impose pas dans la réponse une quelconque prise en compte d'office de l'existant pour le rendre compatible avec les exigences de priorité « 0 ».

Si besoin, ces actions seront priorisées et planifiées dans le courant de l'accord-cadre à venir par des évolutions à l'initiative du CNRS.

4.1 EXIGENCES D'INTÉGRATION DANS LE SI

L'architecture de la solution est compatible avec l'architecture générale du SI du CNRS.

4.1.1 Répartition fonctionnelle

Référence	Libellé exigence	Priorité
URB_003	Pour assurer que l'architecture des solutions nationales va dans le sens d'une répartition urbanisée des fonctionnalités entre les applications selon le principe de cohérence fonctionnelle et informationnelle forte, l'équipe projet doit faire valider son périmètre fonctionnel et informationnel par l'équipe urbanisation de la DSI.	0
URB_004	Lors de la conception et de la réalisation de la solution, les architectures transverses sont privilégiées, entre autres par l'utilisation des plateformes mutualisées et la réutilisation des briques applicatives (notion de service, voire micro-service). Ceci afin de ne pas implémenter ou développer une fonction ou un contrôle métier déjà outillé dans une autre application ou service.	1
URB_005	Lors de la conception et de la réalisation de la solution, les fonctions restant à développer pour la solution sont prévues autant que possible pour être mutualisées, voire transformées en (micro-)services utilisables par d'autres applications.	1
URB_006	L'architecture de la solution découple les fonctionnalités « Etablissement » des fonctionnalités « Laboratoire » dans des modules applicatifs distincts qui proposent des interfaces de communication (interface - programmation orientée objet, webservices, API REST, etc.). Le choix des mécanismes pour ces interfaces de communication à implémenter est étudié et validé entre le titulaire et le CNRS (équipes projet et transverses).	1

4.1.2 Échanges de données

4.1.2.1 Modalités générales

Les interfaces entrantes ou sortantes entre la solution et les autres applications du SI peuvent s'effectuer de plusieurs façons dont voici les principales : échanges de fichiers (XML, CSV, ...), échanges de messages (Broker), et services Web de type REST, tout en passant systématiquement par un des systèmes d'intermédiation du CNRS (cf. § 2.3.3.1).

L'objectif du CNRS est la mise en œuvre du principe de couplage faible entre les systèmes d'intermédiation et l'application.

Les échanges de données entre le gestionnaire d'échanges et de services CNRS et la plateforme Réséda (flux entrants et flux sortants), se font au travers d'une couche d'abstraction (matérialisée par des services) pour permettre au gestionnaire d'échanges et de services CNRS d'assurer la gestion chronologique des échanges (quotidien, à la demande, ...) tout en disposant de services, portés par la plateforme Réséda, appelables par le gestionnaire d'échanges et de services CNRS à tout moment (en journée, en traitement batch).

Dans le cas des flux par appel de services web, le passage par le gestionnaire d'échanges et de services du CNRS n'est pas obligatoire, toutefois, afin de garder un découplage des échanges, ces appels de services web passent à travers un proxy de service web (de manière transparente pour l'application appelante). Dans certains cas justifiés, la mise en œuvre des services web peut être réalisée via le gestionnaire d'échanges et de services du CNRS.

Au final, la solution d'échange pour chacun des flux est définie conjointement avec le CNRS dans le cadre d'ateliers de travail dans la limite des règles prévalant au CNRS sur l'intégration des SI.

Pour les flux entrants, le CNRS détermine et met à disposition, en fonction des besoins, les données échangées nécessaires à la plateforme Réséda.

Cependant dans le cas où certains flux entrants sont à développer par le CNRS pour les besoins spécifiques de la plateforme Réséda, l'équipe projet Réséda au sens large (équipe DSI + titulaire) doit déterminer son besoin au plus tôt, ajuster son planning le cas échéant, pour permettre au CNRS la mise à disposition du nouveau flux avant la livraison de la solution.

Référence	Libellé exigence	Priorité
URB_007	Le titulaire prévoit le bon fonctionnement et la continuité de service fonctionnel de la solution qu'il développe, y compris des éventuels outils d'intégration proposés, au regard de l'architecture générale du SI, et en particulier vis-à-vis des systèmes d'intermédiations retenus au CNRS. En particulier, la solution : ▣ tient compte des arrêts de services de la solution, avec éventuellement l'émission d'un message de non disponibilité, afin de ne pas provoquer d'erreur (technique) pour les services appelants ; ▣ prend en compte et pallie la non réponse d'un service appelé en passant, par exemple, dans un mode dégradé non bloquant.	1
URB_008	Si la solution fait appel à des services fonctionnels portés par un autre SI ou application, ou met à disposition des services fonctionnels, la gestion de ces communications passe par les systèmes d'intermédiation du CNRS.	1
URB_009	La solution a la responsabilité de réaliser les services d'intégration des données et les services d'exposition des informations dont elle est propriétaire. La conception de ces services est validée par le CNRS (équipes projet et transverses).	1
URB_010	Les échanges entre la solution et le reste du SI se font via des formats pivots.	1
URB_011	Les formats pivots non fournis par le CNRS sont de préférence basés sur des formats pivots existants et reconnus par la communauté. Le choix des formats pivots est validé par le CNRS (équipes projet et transverses).	1
URB_012	Les formats pivots sont facilement évolutifs en limitant les impacts sur leurs usages déjà en cours.	1
URB_013	La description des formats pivots spécifiquement développés pour le CNRS respecte un formalisme prescrit par la DSI du CNRS.	1
URB_014	Si la mise en œuvre d'échange nécessite la transcodification de certaines données (nomenclatures par exemple), celle-ci est effectuée par les systèmes d'intermédiation au cours du flux, à partir de tables de transcodification administrées par le gestionnaire de données de référence du CNRS. Les systèmes d'intermédiations prennent seulement en compte une transcodification simple, de type valeur ou groupe de valeur vers une autre valeur, sans application de règles métier. Celles-ci sont éventuellement mises en place dans le gestionnaire de données de référence du CNRS qui héberge les tables de transcodification. A noter que si les échanges se font via les services web, ces derniers ne réalisent aucune transcodification.	2
URB_015	La solution va chercher les objets métiers, dont elle a besoin et en récupère, au moment où elle en a besoin, uniquement la population qui l'intéresse et uniquement le sous-ensemble des caractéristiques (partie du format pivot) qui lui est nécessaire. Autrement dit, seules les données / objets métiers nécessaires sont présents dans les flux entrants de la solution.	1
URB_016	En fonction des éléments d'analyse, le titulaire détermine l'ensemble des données strictement nécessaires dans le cadre de données personnelles (contrainte du règlement européen sur la protection des données – RGPD), au bon fonctionnement de la solution.	1
URB_017	L'utilisation de données extérieures à la solution n'implique pas un stockage de ces données dans la solution, et est mis en balance avec le nombre, la fréquence et le volume des flux nécessaires pour consommer ces données, afin d'optimiser les ressources. Aussi, la nécessité de stocker les données externes dans la solution doit être étudiée et validée entre le titulaire et le CNRS (équipes projet et transverses).	2
URB_019	La solution expose toute la population des objets métiers dont elle est maître, avec le contenu complet du format pivot (FP), y compris les règles de diffusion, et/ou niveau de sensibilité.	1

Référence	Libellé exigence	Priorité
	Autrement dit, la solution ne fait aucune restriction sur l'exposition des objets métiers qu'elle gère.	
URB_018	Pour chaque objet métier dont la solution est propriétaire, un service d'exposition permet au choix : ■ une diffusion au fil de l'eau des objets métier modifiés par la solution ; ■ une diffusion sous forme de flux à la demande ; ■ un flux complet ou différentiel sur des critères à définir en conception détaillée (<i>par exemple, uniquement sur les objets modifiés depuis l'envoi précédent ou depuis une date définie, uniquement un sous ensemble des objets métier, uniquement un objet métier donné</i>). ■ une sélection des objets métier et/ou une partie de leurs caractéristiques, en fonction de critères à définir en conception détaillée. Le choix des mécanismes d'exposition à implémenter est étudié et validé entre le titulaire et le CNRS (équipes projet et transverses)."	1
URB_021	Pour les objets métier dont la solution est propriétaire, et pour lesquels il y a une utilité, un service de recherche permet une recherche approchante, sur des caractéristiques à définir en conception détaillée.	2

4.1.2.2 Modalités d'implémentation

Les flux d'échange de données doivent techniquement adopter les règles d'implémentation suivantes :

Référence	Libellé exigence	Priorité
ECH_001	Les échanges inter-applicatifs passent par les systèmes d'intermédiation du CNRS. La solution ne communique qu'avec ces systèmes d'intermédiation, quel que soit le flux entrant ou sortant et propose des services permettant d'interagir avec eux.	1
ECH_002	La solution produit et reçoit des informations préformatées au format pivot défini par le CNRS. Les systèmes d'intermédiation ne portent pas les règles de gestion métier.	0
ECH_003	L'interfaçage avec les systèmes d'intermédiation est effectué via des services web du type REST. Pour la diffusion de ses données au reste du SI, la solution privilégie un appel à un service web CNRS de diffusion des données.	1
ECH_004	La fréquence des échanges de données se fait selon un mode ""fil de l'eau"" différentiel (plage modulable) ou complet sur validation du CNRS.	1
ECH_005	Les formats utilisés pour les échanges de données sont XML, JSON et CSV, mais ces formats ne sont pas limitatifs. Le référentiel général d'interopérabilité (http://references.modernisation.gouv.fr/interopabilite) gouverne le choix des formats.	1
ECH_006	Seuls des protocoles de transport de données chiffrés sont utilisés comme par exemple les protocoles « SSH » (scp, sftp, etc). Se référer au RGS 2.0 annexes B1, B2 et B3 pour les versions des protocoles et algorithmes de chiffrement autorisés (https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents).	0
ECH_007-a	Pour tous les types de flux, la confidentialité des données transmises est garantie. Les moyens techniques utilisés sont décrits dans la documentation.	0
ECH_007-b	Pour tous les types de flux, l'intégrité des données transmises est garantie. Les moyens techniques utilisés sont décrits dans la documentation.	0
ECH_007-c	Pour tous les types de flux, l'unicité des requêtes est garantie pour éviter les attaques par rejeux. Les moyens techniques utilisés sont décrits dans la documentation.	0
ECH_007-d	Pour tous les types de flux, l'identité du client et du serveur de communication est garantie. Les moyens techniques utilisés sont décrits dans la documentation.	0
ECH_008	Pour assurer la confidentialité et l'intégrité des données lors des échanges, le chiffrement des données en supplément du chiffrement des protocoles de transport (cf. ECH_006) est une mesure de protection dont l'opportunité est jugée au regard de la sensibilité. Ce chiffrement est réalisé à la source et le déchiffrement à la destination, sans possibilité d'interception par les systèmes d'intermédiation et de transport selon les normes de chiffrement en vigueur (cf. annexe B du RGS : https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-	0

Référence	Libellé exigence	Priorité
	documents). Il est cependant toléré que le système d'intermédiation du CNRS assure le chiffrement en cas d'impossibilité de le réaliser à la source.	
ECH_009	L'authentification des appels à un service web, de type REST, est réalisée soit par certificat, soit par identifiant/mot de passe stocké de manière confidentielle.	0
ECH_010	Lorsque l'usage d'un broker est nécessaire, c'est celui du gestionnaire d'échange et de services du CNRS, via son API (JMS de préférence) qui est utilisé.	1

4.1.3 Authentification, comptes utilisateurs

Les services d'authentification CNRS (cf. § 2.3.3.3) sont disponibles sur plusieurs environnements :

- production : réservé à la production de la solution,
- recette : réservé à la recette de la solution,
- formation : réservé à la formation de la solution,
- test : seul environnement accessible au titulaire, ne contenant pas de données réelles et dont l'objectif est de permettre au titulaire de valider les aspects techniques liés aux briques d'authentification.

Le titulaire assure les développements applicatifs nécessaires pour s'interfacer avec le(s) fournisseur(s) d'identité du CNRS (cf. § 2.3.3.3). Si plusieurs fournisseurs peuvent être choisis, un WAYF doit être mis en place.

Les droits et profils applicatifs associés sont stockés dans l'annuaire de l'application.

Le titulaire reste responsable de la solution mise en œuvre qui doit respecter les principes de fonctionnement suivants :

- L'application délègue l'authentification des utilisateurs au fournisseur d'identité du CNRS (cf. § 2.3.3.3).
- Une fois le client SAML intégré à l'application, c'est le fournisseur d'identité qui se charge d'authentifier l'utilisateur.
- L'authentification des utilisateurs par les services d'authentification CNRS est possible soit par certificats (AC CNRS / TCS), soit par email/mot de passe (en se basant sur les informations contenues dans le référentiel des comptes utilisateurs du CNRS), soit avec une solution d'authentification multi-facteurs.
- Le navigateur est toujours redirigé vers un des fournisseurs d'identité CNRS et c'est ensuite, lors de l'authentification sur ce fournisseur d'identité, que l'utilisateur peut fournir ses identifiant et authentifiant.
- Une fois l'utilisateur authentifié auprès d'un fournisseur d'identité CNRS, le navigateur de l'utilisateur envoie à l'application l'identifiant opaque dans un jeton de réponse SAML. Ce jeton contient aussi des attributs de l'utilisateur authentifié. La liste des attributs diffusés est spécifique à chaque application et limitée à ses besoins.
- Le contrôle d'accès à l'application effectué par le fournisseur d'identité CNRS se limite à dire si les informations d'authentification de l'utilisateur sont correctes. Il atteste juste que l'utilisateur est référencé dans le SI du CNRS. L'application doit assurer elle-même son contrôle d'accès à partir des rôles et droits applicatifs gérés dans l'application. Si nécessaire, les droits et profils applicatifs associés sont stockés dans la base de l'application.
- Le service provider (SP) fourni par la DSI du CNRS peut restreindre l'accès à l'application sur la base d'attributs retournés par le fournisseur d'identité.
- Le critère d'accès est donc l'appartenance ou non de l'utilisateur au référentiel des comptes utilisateurs du CNRS.
- Dans le cas d'une gestion des droits déléguée à la brique de gestion des accès et habilitations du CNRS (cf. § 0), les rôles applicatifs peuvent être gérés et calculés de manière centralisée. Ces rôles applicatifs sont disponibles dans les services web des données des utilisateurs. Dans certains cas ils peuvent aussi être transmis à l'application lors de l'authentification. Les droits fins sont stockés et gérés dans la solution.

Référence	Libellé exigence	Priorité
AUTH_001-a	L'authentification à la solution se fait à partir du fournisseur d'identité CNRS pour les utilisateurs des unités CNRS et sinon au moyen de la fédération RENATER.	1
AUTH_001-b	Pour les utilisateurs qui ne sont présents ni dans le fournisseur d'identité CNRS, ni dans la fédération RENATER, le CNRS étudie les modalités de gestion des comptes. L'utilisation de comptes locaux n'est possible que sur autorisation expresse du CNRS.	0
AUTH_002-a	Dans le cas de comptes locaux, la solution comprend des fonctionnalités de gestion de ces comptes.	0

Référence	Libellé exigence	Priorité
AUTH_002-b	Dans le cas de comptes locaux, les mots de passe ne sont jamais stockés en clair mais dans une forme transformée par une fonction cryptographique non réversible conforme au Référentiel Général de Sécurité (https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs) et la transformation des mots de passe fait intervenir un sel aléatoire.	0
AUTH_003	Un service de découverte (WAYF) est mis en place lorsque le fournisseur d'identités CNRS n'est pas le seul fournisseur d'identité utilisé.	0
AUTH_004	La création d'un compte utilisateur pour accéder à la solution est effectuée par un mécanisme de provisioning et non par saisie manuelle. Le provisioning peut être effectué via l'utilisation du service web qui expose le référentiel des comptes utilisateurs (annuaire référentiel du CNRS), à la demande ou au fil de l'eau ou encore via les informations issues de l'authentification. La création automatique de compte sur demande de l'utilisateur directement dans l'application est interdite.	1
AUTH_005	Pour les personnels présents dans les unités du CNRS, l'origine des données pour la création et la modification des comptes utilisateurs est l'annuaire référentiel du CNRS.	0
AUTH_006	Un mécanisme de gestion du cycle de vie des comptes utilisateurs de la solution est mis en place.	1
AUTH_007	La modification d'un compte utilisateur dans la solution est effectuée via des services web ou via les systèmes d'intermédiation du CNRS.	1
AUTH_008	Les phases d'identification et d'authentification sont séparées de l'ensemble des actions applicatives de l'utilisateur dès la conception de la solution afin de permettre la plus grande modularité possible, et donc une facilité, quant au choix du mécanisme d'identification et d'authentification.	1
AUTH_009	Le contrôle d'accès à l'application est renforcé directement sur le reverse proxy hébergeant le Service Provider par la vérification d'un attribut spécifique exposé par le référentiel des comptes pour refuser l'accès aux utilisateurs authentifiés qui n'auraient pas de droits sur l'application. Dans ce cas, une page d'erreur spécifique est à prévoir pour indiquer de manière claire à l'utilisateur qu'il n'a pas les droits nécessaires pour accéder au service/à l'application. Ce contrôle s'ajoute mais ne se substitue pas aux contrôles de droits des utilisateurs réalisés par l'application.	1

Référence	Libellé exigence	Priorité
HAB_001	La solution permet de définir différents rôles applicatifs selon les fonctions métier et les responsabilités des utilisateurs.	0
HAB_002	La solution permet de définir des rôles applicatifs en fonction des fonctions métier et du domaine d'appartenance, ainsi que des accès associés (lecture, écriture, etc.). Ces rôles sont associés à des périmètres correspondant au besoin et/ou au droit d'en connaître pour les populations considérées.	1
HAB_003	La solution permet de définir ou provisionner des comptes d'accès permanents et temporaires (définition d'une date de début et une date de fin de la validité du compte).	1
HAB_004	La solution permet la désactivation des comptes utilisateurs.	0
HAB_005	Lorsque des comptes par défaut existent, il doit être possible de les désactiver, les renommer, modifier le mot de passe ou les supprimer sans impact sur l'application.	1

4.1.4 Gestion des documents

Référence	Libellé exigence	Priorité
DOC_001	Les documents gérés par la solution sont stockés sur la plateforme de GED du CNRS. Dès lors, les fonctionnalités d'ajout/modification/lecture/suppression de documents invoquées depuis la solution sont réalisées à travers des services web proposés par la GED du CNRS par l'intermédiaire des systèmes d'intermédiation.	1

4.2 EXIGENCES TECHNIQUES

4.2.1 Éléments techniques structurants

La plateforme Réséda et l'annuaire CNRS sont tous les deux accessibles depuis internet. Les terminaux utilisés pour accéder à Réséda sont principalement des ordinateurs. L'annuaire CNRS peut également être accédé depuis des smartphones et des tablettes en plus des ordinateurs, ce qui implique une gestion du *responsive design*.

4.2.2 Services d'infrastructure

4.2.2.1 Architecture générale

La solution est construite sur une architecture logicielle intégrée, c'est-à-dire :

- s'appuyant sur une gestion des données unique,
- s'appuyant sur des mécanismes d'accès, d'authentification et de gestion de la confidentialité proposant une ergonomie homogène pour l'ensemble des fonctionnalités,
- disposant d'un outillage d'administration dédié.

Référence	Libellé exigence	Priorité
INF_001	Partout où cela est possible, les privilèges accordés aux comptes de service utilisés par la solution sont minimisés au strict nécessaire. <i>Exemple: accès BDD, accès au système de fichiers, ...</i>	0
INF_002	L'exploitation et l'administration « fonctionnelle » de la solution est réalisée par une IHM spécifique, si possible dédiée, avec des comptes nominatifs dédiés. Elle ne nécessite pas de connexions en SSH ou d'actions nécessitant une console (<i>ex : récupération de logs récurrente, édition de fichiers de paramétrage pour lancer une campagne, etc.</i>).	0
INF_003	La solution ne peut pas être proposée en mode SaaS.	0

4.2.2.2 Caractéristiques système

Les exigences système suivantes doivent être respectées :

Référence	Libellé exigence	Priorité
INF_004	Le serveur HTTP de référence est Apache sur Linux. L'autre plateforme acceptée est la solution IIS sous Windows.	0
INF_005	Dans le cas où la solution nécessite un serveur d'application Java préinstallé, la référence est Tomcat. Une autre solution peut être acceptée sur dérogation.	1
INF_006	Le système d'exploitation serveur de référence est Red Hat Enterprise Linux, le système d'exploitation Windows serveur est toléré.	0
INF_007	La configuration d'un serveur PHP exécute uniquement les modules nécessaires à la solution, qui sont les seuls actifs. Cette liste est définie et communiquée par le titulaire. Certains modules sont explicitement interdits (notamment ceux permettant un appel direct au système d'exploitation). Certaines fonctions sont interdites : <code>disable_functions = system, exec, shell_exec, passthru, phpinfo, show_source, highlight_file, popen, proc_open, fopen_with_path, dbmopen, dbase_open, putenv, move_uploaded_file, chdir, mkdir, rmdir, chmod, rename, filepro, filepro_rowcount, filepro_retrieve, posix_mkfifo</code> .	0
INF_008	Toutes les montées de versions mineures pour les OS serveurs (de type Linux), les modules serveurs applicatifs et bases de données, sont effectuées avec un déclenchement automatique, pour tout ce qui a été installé par le gestionnaire de paquets.	0

De plus, le titulaire a pris en compte dans son offre les exigences sur la sécurité des applications définies au chapitre 4.4.

4.2.2.3 Caractéristiques réseau

La solution mise en œuvre s'appuie impérativement sur l'infrastructure réseau existante et intègre les aspects suivants :

- tous les échanges sont compatibles avec les protocoles IPv4 et IPv6 ;
- tous les flux du système d'information sont recensés et maîtrisables, en terme de capacité à appréhender le mode de fonctionnement protocolaire associé, et à assurer le filtrage par des équipements de type « pare-feu » ; le titulaire fournit une matrice des flux de l'application, indiquant clairement les protocoles, ports et sens de communication utilisés par ces flux ;
- le serveur applicatif n'est pas directement visible des navigateurs clients, des éléments de type « reverse-proxy » étant intercalés dans le flux (Navigateur ⇄ [HTTPS] ⇄ Reverse Proxy ⇄ [HTTP] ⇄ Serveur applicatif) ;
- le fonctionnement de l'application intègre la mise en œuvre de composantes techniques souvent déployées dont notamment les réseaux privés virtuels (VLAN), la translation d'adresses IP (NAT), l'utilisation de serveurs de type Reverse Proxy, les « pare-feux », le chiffrement (via une technologie de type VPN ou autre) ;
- la solution est parfaitement inter opérante avec les principaux services Internet (DNS, SMTP, FTP, NTP, SNMP, etc.), dans leurs versions chiffrées quand elles existent. Elle respecte en particulier les principaux RFC associés à chacun des protocoles, et les règles en usage dans la communauté Internet.

Référence	Libellé exigence	Priorité
INF_009	Les flux entre les postes clients et le(s) serveur(s) applicatif(s) passent par une DMZ avec rupture de flux effectuée par des reverse proxy.	0
INF_010	Les seuls flux « réseau » (hors flux techniques comme "DNS", "EAI", ...) légitimes sont les suivants : ■ reverse proxy → serveur d'application ■ serveur d'application → serveur de base de données	0
INF_011	Les flux entrants de systèmes externes sont soumis à autorisation de la sécurité. Dans le cas où ils sont autorisés, ils passent par des services en DMZ.	0
INF_012	Les flux sortants sont chiffrés conformément aux dispositions réglementaires (cf. RGS Annexe B1, B2, B3 https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents), passent un proxy HTTP et sont initiés par le CNRS.	0
INF_013	La compatibilité IPv6 est assurée de façon native. En production, les communications se font en IPv4 sauf décision expresse du CNRS.	2
INF_014	Les connexions VPN sont obligatoirement effectuées en site à site IPSEC IKEv2, le roaming user SSL avec chiffrement au niveau réglementaire requis est toléré avec identification du terminal et de l'utilisateur	0
INF_015	Un filtrage protocolaire L4 au minimum est mis en service sur les systèmes d'exploitation, s'appuyant sur une matrice de flux documentée, permettant de limiter au strict nécessaire : ■ les ports d'écoute ■ les sources pouvant joindre chaque port (<i>exemple : un port d'écoute destiné à un échange interapplicatif n'est joignable que par l'autre pair de communication</i>) ■ les destinations légitimes lorsqu'il s'agit de flux sortants. Par défaut, un serveur n'initie pas de trafic réseau, en dehors du trafic nécessaire à sa mise à jour. Le titulaire fournit la matrice des flux en tant que livrable.	0
INF_016	L'administration de la solution est compatible avec des solutions d'administration de type bastion.	0
INF_017	La prise de main depuis l'extérieur passe par un VPN puis un bastion.	0

4.2.2.4 Exploitabilité de la solution

L'application doit être techniquement paramétrable à souhait, et elle doit être facilement exploitable par les équipes qui la maintiennent en condition opérationnelle. En particulier, les exigences suivantes sont à respecter par l'application :

Référence	Libellé exigence	Priorité
INF_018	Les solutions applicatives permettant d'assurer la continuité d'activité (<i>ex. serveurs d'application redondants</i>) sont nécessaires lorsque le besoin est confirmé par les besoins de continuité de la solution. Dans ce cas, la scalabilité du service doit pouvoir se faire par l'ajout de nœud(s) sur les différentes couches (tiers) de la solution (hors base de données).	0

Référence	Libellé exigence	Priorité
INF_019	L'hébergement en production bénéficie d'une politique de sauvegarde définie en fonction des besoins de reprise d'activité de la solution. Les sauvegardes sont déportées pour être suffisamment isolées du site de production.	0
INF_020	Les technologies à base de containers (de type Docker) ne sont pas préconisées tant que le CNRS ne s'est pas doté de l'outillage adapté.	1
INF_021	L'application doit être compatible avec un environnement d'exécution durci selon les règles définies par le CNRS, ces règles sont issues des profils SCAP 1.3 publiés par le NIST pour les systèmes d'exploitation.	1

4.2.2.5 *Caractéristiques d'observabilité*

Le CNRS effectue la supervision de ses applications en collectant les informations suivantes :

- métriques techniques du système d'exploitation et composants,
- logs des composants de bas niveau (système d'exploitation, base de données, serveur web, ...),
- logs applicatifs issus de fichiers de logs fournis par l'application avec un format facilitant leur analyse.

4.2.3 Architecture applicative

4.2.3.1 Normes d'architecture

Les exigences et recommandations techniques concernant l'architecture applicative sont les suivantes :

Référence	Libellé exigence	Priorité
DEV_001	L'architecture sépare bien les aspects essentiels de la solution (présentation, aspects métiers, accès aux données) afin de faciliter la testabilité et l'extensibilité de la solution. Une attention particulière est portée à l'abstraction de la base de données, afin de permettre la mise en place de l'intégration continue du code et faciliter les éventuels changements de base de données.	0
DEV_002	La haute disponibilité est mise en place pour les solutions identifiées comme ayant le besoin de disponibilité attendu le plus élevé.	0
DEV_003	L'architecture est de type client léger, les clients lourds ou riches basés sur des technologies de plugins dans les navigateurs (tels que les applets, Flash, ActiveX, ...) sont interdits. Tous les traitements et vérifications sont réalisés au moins du côté serveur : aucune entrée cliente n'est considérée comme fiable par défaut.	0
DEV_004	L'usage de Java WebStart est temporairement toléré lorsqu'il n'existe aucune alternative (par exemple si besoin de signature numérique)	1
DEV_005	Il est interdit de déployer sur les postes de travail des logiciels créant des adhérences autres que le navigateur, en dehors de certaines exceptions à justifier.	1
DEV_006	La solution est utilisable à partir d'un navigateur Web sur un protocole de transport TLS aussi bien pour les solutions à visibilité internet que les solutions internes. Le CNRS impose les technologies Web natives (HTML5, CSS3...) limitant les interactions avec le système d'exploitation et le respect des standards du W3C.	1
DEV_007	L'architecture n'est pas monoposte.	0
DEV_008	En plus du français, la gestion d'au moins une langue étrangère (l'anglais) est fournie.	1
DEV_009	Les libellés (messages d'erreur, champs, texte, ...) sont externalisés, soit en base soit via un fichier de propriétés. <i>Par exemple, les nomenclatures ne sont pas stockées dans le code applicatif mais sont externalisées.</i>	1
DEV_010	Toute émission de mails doit respecter les règles suivantes : 1. L'expéditeur (« from » de l'entête ET de l'enveloppe) utilise un sous-domaine de cnrs.fr dédié à l'application (ex : @monappli.cnrs.fr). 2. L'application utilise le relai SMTP local du serveur pour l'envoi des mails, soit de manière implicite, soit en spécifiant l'usage du relai localhost « 127.0.0.1:25 » si nécessaire. Ce relai local acheminera alors les mails vers les relais centralisés qui assureront l'émission externe, en cohérence avec le SPF du domaine d'émission. 3. Le domaine de sortie est choisi parmi ceux autorisés par les relais de la DSI 4. La solution n'utilise pas l'adresse mail des utilisateurs pour les domaines non gérés par la DSI comme clause FROM, sous peine d'usurpation d'identité et blacklistage (par exemple, il est interdit d'envoyer des mails de type john.doe@google.com) 5. La solution respecte un formalisme de message imposé par le CNRS 6. La solution supporte l'envoi de messages numériquement signés par le standard S/MIME 7. Il est recommandé de ne pas envoyer de pièces jointes, dans le cas où ce serait nécessaire, la solution permet le paramétrage de la limite la taille des pièces jointes 8. La solution prévoit des envois par lots en cas de besoin, et limite le nombre de destinataires par lot et la fréquence d'envoi. En cas de besoin d'envoi de messages aux utilisateurs de la solution, un serveur SMTP dédié (fourni par la DSI si la solution est hébergée par la DSI) est utilisé	0

4.2.3.2 Langages

Les exigences et recommandations techniques concernant les langages utilisés sont les suivantes :

Référence	Libellé exigence	Priorité
DEV_011	L'ensemble des langages et des composants nécessaires à la solution sont utilisés dans les versions mentionnées dans le document CCT_Versions-cibles (ce document est mis à jour régulièrement). Le document, dans sa version courante est applicable à tout moment, ce qui implique des mises à jour régulières des applicatifs en conséquence.	0

Référence	Libellé exigence	Priorité
DEV_012	Sauf contrainte contractuelle, le choix du langage et des frameworks est le résultat d'un consensus entre la DSI et le titulaire en charge de la réalisation de la solution.	0
DEV_013	Les frameworks de développement doivent être ouverts, éprouvés, avec une large communauté active, maîtrisés par le titulaire en charge de la réalisation solution, et permettre d'automatiser les tests unitaires. Leur choix est justifié en regard des gains attendus en termes de développement et d'évolutivité. Les versions utilisées sont systématiquement celles qui sont les plus récentes et qui présentent la durée de support la plus longue.	1
DEV_014	Pour une solution Java, le framework utilisé est Spring Boot avec le serveur web embarqué (la solution ne requiert donc pas d'être installée dans un conteneur de servlets).	1
DEV_015	Pour une solution PHP, le framework utilisé est Symfony.	1
DEV_016	Le nombre de composants externes complémentaires est limité au strict minimum. L'utilisation de composants externes, progiciels, logiciels tiers respecte les règles suivantes : 1. Son fournisseur est engagé sur le maintien dans la durée d'une réelle API de communication 2. Les évolutions de la solution peuvent être menées sans avoir systématiquement recours à des consultants experts de ces composants tiers. 3. Les développements spécifiques n'ont pas d'impact sur les montées de version, ou bien ces impacts sont intégrés comme un coût additionnel en début de projet 4. Le code tiers utilisé dispose d'une licence d'utilisation bien identifiée, n'induisant pas pour le CNRS de contraintes d'acquisition ou d'aliénation de ses droits. Les licences libres sont recommandées.	0

4.2.3.3 Normes de développement

En fonction de la technologie retenue, des préconisations concernant les méthodologies et règles de développement sont applicables et s'appliquent notamment pour le code spécifique développé pour le CNRS.

Les recommandations ci-après s'appliquent de manière plus générale à l'ensemble des technologies.

Le CNRS est attentif à la qualité logicielle de l'application et à ses capacités d'évolution.

D'une manière générale, le titulaire doit utiliser autant que possible des standards pérennes normalisés ou reconnus du marché.

Les exigences et recommandations techniques concernant les normes de développement sont les suivantes :

Référence	Libellé exigence	Priorité
DEV_017	Les développements sont modulaires afin de faciliter la maintenance et l'évolutivité du code.	0
DEV_018	Les erreurs sont traitées de manière à assurer la sécurité dans les développements (toutes les erreurs levées lors de l'exécution doivent être traitées en conséquence).	0
DEV_019	Les bibliothèques de logs utilisées sont ouvertes, éprouvées, avec une large communauté active, et maîtrisées par le titulaire. Les logs sont paramétrables et gèrent a minima les niveaux suivants : ■ ERROR : une erreur technique non récupérable est survenue dans la solution ; en général, la solution n'est plus opérationnelle ensuite ■ WARN : un point d'attention a été soulevé, ou une erreur récupérable est survenue ■ INFO : permet de suivre le fonctionnement métier de l'application, plus les étapes importantes de la vie de l'application ■ DEBUG : permet de voir le fonctionnement technique de la solution.	0
DEV_020-a	La solution journalise des événements permettant l'audit des connexions effectuées à la solution, et le suivi des opérations importantes. Les opérations à tracer ainsi que le format du contenu de ces journaux sont définis conjointement entre le titulaire et le CNRS. Les logs issus de l'application sont dans des fichiers textes dans un format permettant leur analyse.	0
DEV_020-b	L'application utilise une bibliothèque de logs qui permet de paramétrer la destination des événements de logs (par exemple syslog).	0
DEV_022	La solution ne récupère pas de code externe (en dehors sa phase de construction), sauf si la dépendance a été définie explicitement, intégralement et statiquement dans son code.	0

Référence	Libellé exigence	Priorité
DEV_023	Le paramétrage technique de la solution est réalisé au travers de fichiers de configurations qui doivent être stockés de manière indépendante du code applicatif.	0
DEV_024	Afin de lutter contre les risques d'injection de code, les requêtes SQL adressées à la base de données sont faites au moyen de requêtes préparées fortement typées ou par l'intermédiaire d'une couche d'abstraction assurant le contrôle des paramètres.	0
DEV_025	Les tests unitaires sont automatisés, avec un taux de couverture minimum défini d'un commun accord entre tous les acteurs du projet. Ces tests doivent s'exécuter sans erreur dans la forge du CNRS (les cas d'erreurs résiduels devront être justifiés par le titulaire).	0
DEV_026	Des frameworks sont utilisés pour développer les tests unitaires, dans les versions mentionnées dans le document CCT_Versions-cibles (ce document est mis à jour régulièrement). Les tests unitaires livrés en même temps que les fonctionnalités couvertes servent aux tests de non régression et peuvent fournir à travers des outils de couverture de tests un indicateur de qualité.	1
DEV_027	Les codes doivent être documentés et lisibles. Les composants (modules, classes, méthodes) doivent reposer sur une nomenclature de nommage normalisée et cohérente.	0
DEV_028	Les packages sont préfixés en utilisant fr.cnrs	0
DEV_029	Au niveau OS, le jeu de caractères pour la solution est UTF-8.	1
DEV_030	Les solutions sont compatibles avec la liste des navigateurs/OS et versions associées dans le document CCT-Versions-cibles (ce document est mis à jour régulièrement). La notion de support d'une plate-forme cliente impose que l'ensemble des fonctionnalités attendues soit disponible dans des conditions de complétude, d'ergonomie et de performance tout à fait normales. Les niveaux de prises en charge possibles sont les suivants : - Maximal : Les navigateurs dans cette catégorie doivent offrir aux visiteurs toutes les performances techniques, visuelles et fonctionnelles définies par le cahier des charges et la maquette graphique, - Dégradé : Les navigateurs doivent permettre une expérience utilisateur équivalente au niveau précédent mais qui peut toutefois présenter des différences considérées comme négligeables (décalages minimes, arrondis, ombrages...), - Minimal : L'intégration HTML/CSS est accessible et agencée convenablement, mais aucun effort n'est porté sur la compatibilité visuelle avec les niveaux précédents.	0
DEV_031	L'utilisation de Javascript est autorisée notamment pour fluidifier les échanges avec la solution, <i>par exemple en effectuant des contrôles côté client</i> . Cependant, ces contrôles côté client ne se substituent pas aux contrôles côté serveur qu'il faut impérativement réaliser.	0
DEV_032	Il est interdit de construire un framework Javascript.	0
DEV_033	L'architecture de services web recommandée est l'architecture de type REST.	1
DEV_034	Le CNRS n'impose pas d'outil de génération de PDF particulier dans la mesure où l'outil choisi est ouvert, éprouvé, avec une large communauté active, et maîtrisé par le titulaire.	0
DEV_035	Les outils de requêtage mis à disposition sont paramétrés de manière à limiter les risques de dégradation des performances de la plate-forme en cas d'utilisation malavisée par certains utilisateurs. Les outils de requêtage garantissent le respect des droits d'accès de l'utilisateur.	0
DEV_036	Les éléments d'architecture critiques, complexes ou difficiles à appréhender font l'objet de paragraphes spécifiques dans la documentation permettant leur bonne compréhension.	0
DEV_037	Les dossiers d'architecture technique (DARC), spécifications techniques détaillées (STD) ainsi que les manuels d'exploitation (MEX) et d'installation (MINS) sont actualisés par le titulaire autant que de besoin. Ils sont réputés être à jour à tout moment.	0
DEV_038	La gestion des types d'environnements (développement, recette, production, ...) est prise en charge dans la solution pour adapter automatiquement le niveau de fonctionnalité de la solution (<i>exemple : activation du debug, paramétrages d'envoi de mails, etc.</i>). Les propriétés de l'environnement sont renseignées sur l'instance déployée et facilement modifiables (<i>exemple : fichier unique à modifier au moment du déploiement</i>)	2

Référence	Libellé exigence	Priorité
DEV_039	L'ensemble des éléments du bandeau, l'ensemble des couleurs, des polices de caractères, des espaces, filets, comportements au passage de la souris, aplats couleurs, paramétrages de tableaux, gestion des menus et onglets, sont gérés par une feuille de style CSS (pas de code couleur ni de mise en page en dur dans le code de la page).	1
DEV_040	Eviter au maximum l'utilisation de tables pour gérer la mise en forme dans le code HTML.	2
DEV_041	Les configurations des systèmes et des logiciels utilisés par la solution (notamment Java, PHP) sont obligatoirement durcies à l'état de l'art (cf. https://cyber.gouv.fr/publications/securiser-un-site-web), afin de limiter la surface d'attaque et la fuite d'informations par trop grande verbosité. On citera en particulier et sans exhaustivité : ■ la suppression des balises « meta » dans l'entête HTML lorsque celles-ci indiquent le logiciel ayant généré la page ; ■ la suppression des éléments visibles sur la page indiquant les outils (CMS, éditeur, etc.) utilisés ; ■ la limitation en production des informations de débogage dans les messages d'erreur (en évitant par exemple de fournir la requête SQL qui a généré une erreur) ; ■ l'utilisation de pages d'erreurs personnalisées pour ne pas reposer sur les pages par défaut facilement reconnaissables ; ■ dans certains cas, l'utilisation de l'erreur 404 générique plutôt que d'une erreur 401, 403, 405, etc. pour éviter de révéler trop d'informations sur le fonctionnement ou le contenu en accès limité du site ; ■ la banalisation des entêtes HTTP qui peuvent fournir des informations de version trop précises sur le serveur ou le système d'exploitation employés ; ■ le rejet, en production, des requêtes HTTP TRACE qui n'ont d'intérêt qu'en phase de débogage.	0

4.2.3.4 *Outillage de développement*

Le CNRS opère une forge logicielle afin de favoriser la qualité logicielle, la réduction de la dette technique et l'intégration continue.

Cette forge est composée des éléments suivants :

- un service de gestion de configuration et de dépôt interne : Gitlab
- un service d'intégration continue : Gitlab CI et Gitlab runners
- un analyseur de code : Sonar
- un gestionnaire d'artéfacts : Artifactory

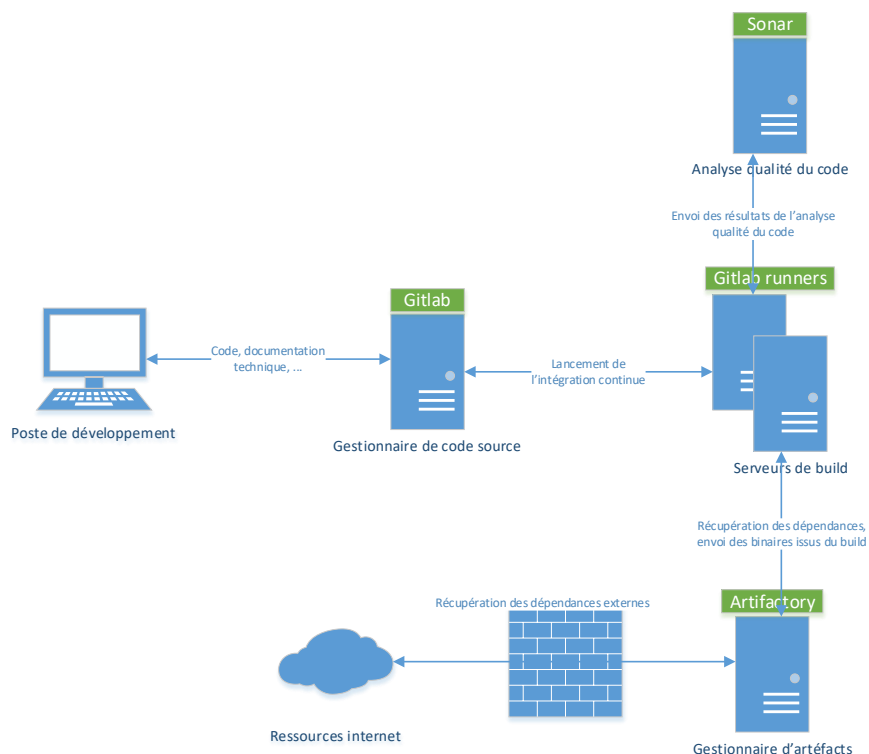


Figure 2 : Présentation de la forge logicielle

Le titulaire doit utiliser la forge de développement de la DSI du CNRS dans l'objectif d'améliorer la qualité selon les cas suivants :

- Dépôt du code source spécifique de Réséda à chaque mise en production d'une version Réséda
- Développement complet de l'Annuaire CNRS (construction comprise des livrables pour installation vers les différents environnements).

Le CNRS étudie la possibilité d'automatiser autant que possible le déploiement de ses applications, et il appréciera toute mesure prise en ce sens.

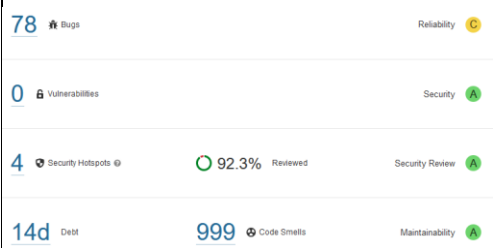
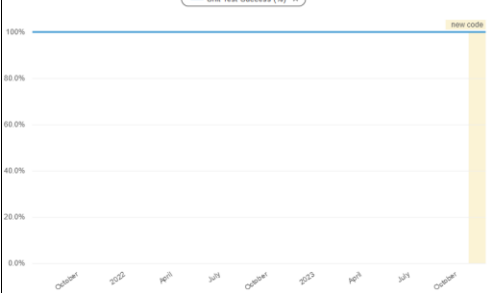
Le CNRS utilise les outils Ansible et Tower pour automatiser autant que possible le déploiement de ses applications.

L'outil de vérification de la qualité du code utilisé à la DSI est SonarQube (<https://www.sonarsource.com/products/sonarqube/>).

Au démarrage de l'accord-cadre, les équipes CNRS et titulaire se mettent d'accord sur le profil SonarQube à utiliser afin d'évaluer la qualité du code source.

Les métriques particulièrement suivies par le CNRS sont les suivantes :

Métrique SonarQube	Description métrique	Cible CNRS
	Taux de commentaires	$\geq 15 \%$
	Duplication de code	$\leq 8 \%$

Métrique SonarQube	Description métrique	Cible CNRS
	Respect des règles de codage et sévérité	Pas d'anomalies de niveau « blocker » et « critical ». Analyser les majeures
	La couverture de tests unitaires (pourcentage de lignes de code du projet qui est appelé pendant la phase de test)	supérieur à 50%
	Le taux de succès des tests unitaires	égal à 100%

Le niveau de conformité à atteindre fait l'objet d'une concertation entre le titulaire et le CNRS.

Plus que l'atteinte de seuils définis, le CNRS est attentif à l'évolution des métriques au cours du temps (lors de chaque livraison majeure de l'application).

Les exigences concernant les outils de développement du titulaire sont les suivantes :

Référence	Libellé exigence	Priorité
DEV_042	Le CNRS n'impose pas de contrainte sur l'outil de développement intégré (IDE) dans la mesure où l'outil choisi est maîtrisé par le titulaire.	2
DEV_043	Pour les cas qui nécessitent des interactions avec des éléments externes (tests, environnement d'intégration ou de recette, ...), des mocks/bouchons sont utilisés. L'usage de bibliothèques de mocks est possible. Le CNRS n'impose pas d'outil particulier dans la mesure où celui choisi est ouvert, éprouvé, avec une large communauté active, et maîtrisé par le titulaire.	0
DEV_044	JMeter est l'outil préconisé pour les tests de charge, si un autre outil est proposé il doit être ouvert, éprouvé, avec une large communauté active, et maîtrisé par l'équipe en charge de son utilisation.	1
DEV_045	Un moteur de production est utilisé afin de gérer les dépendances de la solution, le lancement des tests automatisés, sa construction, la publication des artefacts sur un gestionnaire d'artefacts, ... Pour les projets Java, Maven ou Gradle est utilisé. Pour les projets PHP sous Symfony, Composer est utilisé.	1
DEV_046	Le nommage des artefacts générés par la phase de construction de la solution suit les normes de nommage standard (<i>par exemple Maven pour les projets Java, Composer pour les projets PHP</i>).	1
DEV_047	Le gestionnaire de source Git est utilisé pour la gestion des codes sources. Le CNRS dispose d'un outil de gestion de code source Gitlab dans lequel se trouve le code source de la solution (soit en posant les commits directement dans le Gitlab du CNRS, soit avec un mécanisme de synchronisation - à la charge du titulaire - dans le cas où le titulaire souhaite utiliser des dépôts Git qui ne sont pas ceux du CNRS).	0
DEV_048	La notion de tag (au sens Git) est utilisée pour faire le lien entre les modifications de code source et la version de la livraison.	0

Référence	Libellé exigence	Priorité
DEV_049	Un modèle de gestion des branches Git est utilisé (<i>par exemple Gitflow</i>) en accord avec le CNRS.	1
DEV_050	Le CNRS dispose d'un outil d'analyse statique de code source, SonarQube, utilisé pour analyser le code de la solution. Le titulaire a la possibilité d'utiliser également un outil d'analyse de qualité du code, qui peut ne pas être SonarQube. Des indicateurs et des métriques de qualité logicielle reposant sur ces outils sont proposés par le titulaire. Les éléments de qualité remontés par l'outil SonarQube du CNRS et analysés ensuite, sont définis au démarrage du projet.	1
DEV_051	Le CNRS dispose d'un outil d'intégration continue, Gitlab CI, utilisé a minima pour lancer l'analyse Sonar. De manière générale, la solution est construite par cet outil. Le code source contient un fichier ".gitlab-ci.yml" indiquant la marche à suivre pour construire le projet (ce qui inclut au minimum la récupération des dépendances, le lancement des tests automatisés, la construction de la solution et la publication des artéfacts). Tout autre mode de construction est à discuter au démarrage du projet.	1
DEV_052	Le titulaire exécute une tâche de construction automatique avant toute livraison au CNRS afin de valider la bonne réalisation des opérations de compilation, de réussite des tests unitaires ainsi que de vérifications des éventuelles licences.	1
DEV_053	La livraison et l'installation de la solution est réalisée de façon outillée et automatisée en évitant toute opération manuelle (sauvegarde système, rollback, ...). Il n'y a pas de recommandation particulière pour le choix de l'outil d'installation, mais l'outillage écrit pour réaliser cette tâche est également géré dans l'outil de gestion de code Gitlab du CNRS.	1
DEV_054	Le titulaire se synchronise avec le gestionnaire de version (Git) du CNRS à chaque livraison pour le code spécifique développé pour le CNRS afin que le CNRS ait une visibilité sur le code, les tests unitaires et les tests d'intégration associés.	0
DEV_055	La réussite de l'ensemble des tests unitaires est une condition nécessaire à l'acceptation d'une livraison majeure. Le niveau de réussite des tests unitaires à atteindre peut cependant faire l'objet d'une concertation en cas de forte contrainte au cas par cas.	1
DEV_056	Les modifications de schémas de base de données sont automatisées par l'application soit par le lancement de commandes de migration fournies par le framework, soit lors du démarrage de l'application.	1

4.2.4 Base de données

Les exigences et recommandations techniques concernant les bases de données sont les suivantes :

Référence	Libellé exigence	Priorité
BDD_001	Une base de données (relationnelle ou non relationnelle si c'est pertinent) est utilisée pour gérer la persistance des données.	0
BDD_002	Les solutions de SGBD de référence sont PostGreSQL et MongoDB.	1
BDD_003	La non adhérence au SGBD est assurée, les requêtes ne doivent pas être implémentées directement dans le code. Dans le cas des langages orientés objet, un ORM (mapping entre le modèle relationnel et le modèle objet) est utilisé. Dans les autres cas, une couche d'abstraction de la base de données est utilisée. Lorsque des requêtes SQL sont implémentées, elles le sont en respectant le standard SQL ANSI.	1
BDD_004	Au niveau SGBD, le jeu de caractères utilisé est UTF-8	1
BDD_005	Tous les objets de la base de données sont documentés.	1

4.2.5 Engagements de qualité de service pour l'application

4.2.5.1 Disponibilité

Les périodes de maintenance programmée se font à des périodes décidées en commun accord entre le CNRS et le titulaire.

La plateforme Réséda est ouverte à l'ensemble des unités (unités mixtes du CNRS et unités propres du CNRS) et aux services administratifs (structures administratives) du CNRS par une exposition publique ouverte sur Internet.

L'Annuaire CNRS est ouvert non seulement à l'ensemble des personnels des unités du CNRS mais aussi au grand public par une exposition publique ouverte sur Internet.

La disponibilité de la plateforme Réséda, la sécurité et la confidentialité des données de la plateforme Réséda sont des caractéristiques majeures car :

- La plateforme Réséda consomme depuis la plateforme d'intermédiation des données depuis le SI du CNRS.
- La plateforme Réséda administre et met à disposition des applications tierces au travers de la plateforme d'intermédiation des données référentielles.
- Les utilisateurs du CNRS habilités à utiliser la plateforme Réséda peuvent via des écrans consulter les données des référentiels et pour certains profils ils peuvent mettre à jour tout ou partie des données.

Le tableau ci-dessous récapitule les besoins en termes de disponibilités de la plateforme Réséda et de l'Annuaire CNRS.

Pour le calcul des différents indicateurs ci-dessous, il convient de soustraire les durées dont la responsabilité n'est pas du titulaire ; à savoir :

- Les serveurs SGBD (Oracle / MongoDB) et toute procédure d'administration des SGBD – cf. remarque dans la dernière ligne du tableau ci-dessous
- Les incidents sur le matériel, sur les couches basses des serveurs applicatifs (OS, réseau) et sur les serveurs environnants (DMZ / Reverse Proxy / EAI-ESB / ...).

Besoins de disponibilité	
Plage horaire nécessitant un niveau de disponibilité garantie en termes d'accès utilisateur	jours ouvrés de 8h-19h
Plage horaire d'intervention souhaitée par le titulaire sur la prestation PROJ – 6 (en cas de réalisation d'une mise en production sous traitée auprès du titulaire)	jours ouvrés 19h-8h
Plage horaire nécessitant un niveau de disponibilité garantie en termes de flux de données	jours ouvrés avec interruption maximum de 4h pour intervention programmée
Niveau de disponibilité requis sur la plage horaire garantie, hors interventions planifiées	6 heures d'arrêt cumulées maximum par trimestre (heures d'arrêt sous responsabilité du titulaire)
Garantie de temps maximum de rétablissement requis suite à un incident de service interrompu (GTR)	4 heures

En cas de dépassement de ces seuils de disponibilité, à charge du titulaire, des pénalités seront appliquées (cf. CCAP)

4.2.5.2 Intégrité

La solution doit permettre un contrôle de l'intégrité des données (intégrité structurelle et intégrité du contenu).

En cas de corruption de données, la perte de données acceptable est de 24h. Si nécessaire, l'application doit avoir la possibilité de reprendre les flux ou les batch qui auront été générés lors de la période de perte de données.

Le CNRS doit parfaitement maîtriser la nature des données utilisées par l'application et les mécanismes permettant de restaurer un jeu de données cohérent et exhaustif en cas de nécessité.

Le titulaire est tenu de fournir un descriptif exhaustif des données utilisées et des contraintes techniques associées à une restauration. L'usage des contraintes référentielles est fortement conseillé.

4.2.5.3 Performances

Le CNRS définit comme suit les caractéristiques de performances attendues de l'application :

- Connexion au serveur (contrôle des accès compris) et affichage de la page d'accueil en moins de 5 secondes.
- Temps d'affichage d'une IHM de saisie / consultation inférieur à 3s dans 80% des cas.
- Temps d'exécution d'une requête de recherche inférieur à 10 secondes,

- Temps de génération d'un état inférieur à 20 secondes.

Ces chiffres correspondent à des transactions simples et largement utilisées dont le temps de réponse est mesuré sur le poste client hébergé sur le même réseau.

Certaines fonctionnalités peuvent déroger à ces règles. Toutefois elles doivent :

- faire l'objet d'un accord explicite du chef de projet DSI,
- afficher à l'utilisateur des éléments permettant de juger de leur avancement.

Le titulaire fournit au CNRS :

- des éléments de dimensionnement de la plateforme de production pour garantir un niveau de performance conforme au besoin en regard des éléments de volumétrie disponibles ;
- des éléments de tuning de la plateforme permettant d'optimiser les performances (système, base de données, ...).

Le titulaire fournit au CNRS en même temps que chaque version stable de l'application le rapport des tests de performances qui auront été menés.

Ce rapport met particulièrement en avant les éléments chiffrés concrets qui permettent de valider les temps de réponses exigés par le CNRS en condition de forte charge applicative. Il met aussi en évidence les composantes techniques de l'application nécessitant le plus de ressources techniques et induisant des temps de réponses significatifs.

4.3 EXIGENCES D'ERGONOMIE-GRAPHISME

Les applications Web du CNRS doivent répondre à des impératifs d'identité et d'ergonomie. Elles doivent également suivre des recommandations techniques pour leur intégration (cf. § 4.2.3.3) afin de satisfaire au mieux les exigences d'accessibilité auxquelles tous les services Web d'un établissement public doivent se conformer.

Elles doivent appliquer les règles décrites ci-dessous afin de respecter une cohésion intra et inter-applicative au sein du CNRS.

Les éléments concernant l'ergonomie et le graphisme pourront être ajustés en cours de réalisation, de manière concertée entre le titulaire et l'équipe projet CNRS.

Référence	Libellé exigence	Priorité
ERG_001	Les règles d'ergonomie et de graphisme mises en œuvre dans la solution sont formalisées dans les spécifications fonctionnelles détaillées. Elles sont réputées être à jour à tout moment.	1

4.3.1 Charte graphique

Référence	Libellé exigence	Priorité
ERG_002	Un bandeau est positionné en haut de la page sur l'ensemble de la solution. Le bandeau est composé du logo du CNRS situé à gauche de la page. A droite du logo, il y a le nom de la solution. Si le nom de la solution n'est pas explicite pour les utilisateurs, le titre est accompagné d'un sous-titre qui décrit ce que fait la solution. Le bandeau intègre, en haut à droite au-dessus du titre, une zone de liens utiles (connexion/déconnexion, accès au profil, aide, documentation, choix de langue, paramètres divers...) sauf solution responsive smartphone. Les tailles et espacements seront précisés avec le graphiste de la DSI.	1
ERG_003	L'ensemble de la solution utilise les mêmes éléments de la feuille de style de manière logique et uniforme : police de caractère, liens de navigation, intitulés de champ, titres de différents niveaux, messages informatifs et d'aides à la saisie, messages d'alerte, etc. Il en est de même pour la sémiologie des pictogrammes.	0
ERG_004	La solution utilise une gamme de codes couleurs et de polices préconisées par le CNRS. Si besoin est, cette gamme peut être enrichie avec la contribution du CNRS.	1
ERG_005	Dans le cas d'une solution responsive, l'organisation des écrans peut s'appuyer sur des grilles (grid). Toutes les fonctionnalités essentielles de la solution sont accessibles quel que soit le média. L'apparence du bandeau et la disposition des liens utiles sont optimisées pour apparaître sur une interface de smartphone.	1

4.3.2 Règles d'ergonomie

L'application doit être ergonomique c'est-à-dire qu'elle doit être facilement utilisable, fonctionnelle et compréhensible par l'ensemble des utilisateurs, ce de manière aisée, déductible et conviviale.

L'application doit accompagner l'utilisateur qui doit savoir ce qu'il doit faire sur la page active. Il doit également pouvoir naviguer et se repérer dans l'ensemble de l'application. Pour cela, l'application doit utiliser les systèmes de navigation les plus adaptés ; *par exemple : menus, onglets, enchaînements d'étapes, etc.*

Les éléments fonctionnels du cœur de page doivent être disposés de manière à permettre une lecture facile, avec des éléments regroupés et structurés et des titres explicites.

La conception de l'IHM peut faire appel à des composants d'IHM innovants ; *par exemple : effets de transition, de transparence, mouvements, auto complétion, etc.*

L'application doit être conçue de manière globale et homogène.

Référence	Libellé exigence	Priorité
ERG_006	La taille des fenêtres est adaptable à différentes tailles et résolutions d'écrans. Aucune fenêtre de la solution ne comporte d'ascenseur horizontal.	1
ERG_007	Les tableaux sont conçus de manière optimisée (utilisation de formules synthétiques, de pictogrammes, interlignages valorisés par des couleurs de fond, mise en valeur des entêtes, des liens, ordre des colonnes pertinent, système de navigation pour les tableaux longs).	1
ERG_008	Les titraillies et entêtes sont explicites et clairement structurées et hiérarchisées (utilisation de la feuille de style CSS et des balises h1, h2, etc.).	0
ERG_009	Les éléments de navigation sont clairs et explicites. Dans le cas d'arborescences complexes, un chemin de navigation apparaît.	1
ERG_010	Dans le cas de solution responsive, l'interface est adaptée au pilotage de l'ihm via un doigt (zone cliquable agrandie, survol impossible, navigation par balayage de l'écran, etc.). Les textes sont agrandis.	1

4.4 EXIGENCES DE SÉCURITÉ

Le référentiel des exigences sécurité est présenté dans le tableau ci-dessous. Lorsque nécessaire, il est complété par des éléments détaillés dans les paragraphes suivants.

Référence	Libellé exigence	Priorité
SSI_001	Un dossier de sécurité pour la solution détaillant les mesures de sécurité opérationnelle mises en application, ainsi que tous les éléments de preuve de la réelle application de ces mesures (captures d'écran, fichiers de configuration, compte rendus...) est créé et maintenu. Il indique également comment ces mesures sont régulièrement vérifiées et le dossier comprend le CR des vérifications, le compte-rendu des audits. Ce même dossier constitue une preuve de mise en œuvre des mesures de sécurité conformément au RGPD.	0
SSI_002	Le framework utilisé dispose d'un historique clair et vérifiable de ses vulnérabilités. A date d'implémentation, il ne présente pas de faille non corrigée. L'historique permet d'évaluer la réactivité de correction et la fréquence des failles, et est un argument du choix.	0
SSI_004	Lorsque l'analyse de risque en détermine la nécessité, le chiffrement des données est à mettre en place. Les outils et/ou protocoles de chiffrement utilisés doivent être qualifiés et certifiés par l'ANSSI.	0
SSI_005	Validation des entrées utilisateur : toute saisie utilisateur est vérifiée côté serveur en conformité avec le format, la taille, la sémantique et le type de données attendu.	0
SSI_006	Audit statique de code : le cycle de développement inclut des phases régulières d'audit statique de code, par l'utilisation d'outils d'aide à l'analyse et/ou par revue de code par un pair. Le titulaire fournit au CNRS les états réguliers de cette analyse.	1
SSI_007	Déconnexion à temps contraint paramétrable : l'utilisateur de la solution est déconnecté de sa session après un temps paramétrable dans la solution. Cette durée est implémentée de manière cohérente dans l'ensemble des modules techniques nécessaires à la solution.	0
SSI_008-a	Les identifiants de session utilisateur sont aléatoires avec entropie d'au moins 128 bits.	0

Référence	Libellé exigence	Priorité
SSI_008-b	L'attribut Secure est associé au cookie de l'identifiant de session utilisateur.	0
SSI_008-c	L'attribut HttpOnly est associé au cookie de l'identifiant de session utilisateur.	0
SSI_009	Les informations liées aux habilitations des utilisateurs ne sont jamais passées en paramètres de URL.	0
SSI_010	Gestion des erreurs applicatives : les messages d'erreur applicatifs sont présentés à l'utilisateur en masquant toute information technique divulguant les composants de la solution et leurs versions.	0
SSI_011-a	Lors de la mise en œuvre d'un téléchargement montant (upload) de fichiers, le téléversement est effectué dans une zone disque tampon, puis le fichier est déplacé hors de l'arborescence d'hébergement web.	1
SSI_011-b	Lors de la mise en œuvre d'un téléchargement montant (upload) de fichiers, la vérification du fichier repose sur le type MIME (sans faire confiance ni à l'extension du fichier ni aux entêtes HTTP reçues) et la taille du fichier. En cas de discordance le fichier est refusé.	1
SSI_011-c	Lors de la mise en œuvre d'un téléchargement montant (upload) de fichiers, la vérification de la présence de logiciels malveillants est réalisée par l'antivirus installé sur le système d'exploitation.	1
SSI_011-d	Lors de la mise en œuvre d'un téléchargement montant (upload) de fichiers, le nom du fichier téléchargé est anonymisé.	1
SSI_012	Gestion des vulnérabilités : une surveillance des vulnérabilités applicatives est mise en place pendant la durée de la vie de la solution, et à la correction <i>pro bono</i> de celles-ci. Ces vulnérabilités peuvent toucher toutes les briques applicatives nécessaires à la solution.	0
SSI_013	Dans le cadre d'un développement spécifique, une licence logicielle est choisie par le CNRS conformément à ses besoins. Une référence à cette licence apparaît dans chaque fichier source produit.	0
SSI_014	Lorsque des fonctions de visa ou de signature électronique sont mises en œuvre, elles respectent les dispositions du règlement eIDAS (https://cyber.gouv.fr/le-reglement-eidas-n9102014) et du RGS (https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs). La mise en œuvre est obligatoirement discutée avec le département Sécurité.	0
SSI_015	En fonction des résultats de l'analyse de risques et/ou de l'analyse d'impact sur la protection des données (AIPD) menées, les données stockées sont chiffrées au repos (at rest) selon les dispositions du RGS Annexe B2 (https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents). Les clés de chiffrement sont stockées de manière à n'être disponibles que pour les personnels ayant besoin d'en connaître. Dans certains cas, les administrateurs techniques et fonctionnels peuvent ne pas avoir accès aux données.	0
SSI_016	La solution prend en compte les besoins d'archivage numérique pérenne de ses données, conformément aux directives CNRS en cours. Quand cela est possible, elle implémente un connecteur vers le SAE intermédiaire transverse du CNRS.	1
SSI_019	Conformément au RGPD, quand le traitement réalisé par la solution relève d'un consentement de l'utilisateur, la solution se charge de vérifier l'existence de ce consentement.	0
SSI_020	Pour protéger les données, les environnements hors production n'utilisent pas les informations des données de production sauf dérogation expresse du CNRS.	0
SSI_021	Les journaux générés par la solution, les logiciels intermédiaires, les serveurs web et d'application, le système d'exploitation, les équipements réseaux et de sécurité couvrent au niveau de détail requis par la réglementation les activités de connexions et les opérations importantes menées sur ces systèmes quelle que soit la source (utilisateur, administrateur, scripts ou processus particulier) afin d'identifier l'auteur et la substance d'une action illicite, délictueuse, ou criminelle.	0
SSI_022	Les journaux générés par la solution, les logiciels intermédiaires, les serveurs web et d'application, le système d'exploitation, les équipements réseaux et de sécurité sont établis dans un format structuré dont les champs couvrent a minima pour chaque événement, requête ou action : ■ l'horodatage ■ le compte utilisateur ou processus associé ■ l'adresse IP ou la source à l'origine [en cas d'interaction distante] ■ le libellé intelligible de l'événement ou l'action	0

Référence	Libellé exigence	Priorité
	☐ le code retour de l'action [option] ☐ un identifiant unique de corrélation [option] ☐ la taille de la requête [option]	
SSI_023	Les journaux générés par la solution, les logiciels intermédiaires, les serveurs web et d'application, le système d'exploitation, les équipements réseaux et de sécurité sont tous horodatés de manière fiable et synchronisés sur une même source temps en indiquant notamment le fuseau horaire si les journaux ne sont pas établis en heure UTC.	0
SSI_024	Les journaux générés par la solution, les logiciels intermédiaires, les serveurs web et d'application, le système d'exploitation, les équipements réseaux et de sécurité sont exportés en temps réel hors du système générateur, de manière fiable et intégrée vers un système central de collecte spécifié par le CNRS.	0

4.4.1 Auditabilité

Niveau de traçabilité

La solution met en œuvre obligatoirement la politique de traçabilité de l'ensemble des accès (autorisés et refusés) et des opérations réalisées. Ces traces doivent contenir à minima les informations suivantes :

- Date et heure de l'accès (avec une information d'horodatage fiable) : connexion et déconnexion ;
- Compte d'accès ;
- Etat de l'accès : autorisé ou refusé (et la raison en cas d'échec) ;
- Opérations réalisées ;
- Adresse IP source et protocole d'accès.

De plus, la solution doit implémenter ces fonctions autour de la gestion des traces :

- Durée de rétention des traces (mécanisme de rotation des traces, capacité de rétention maximale) ;
- Centralisation des traces ;
- Sauvegarde des traces ;
- Archivage des traces ;
- Protection des traces (pour assurer leur disponibilité, intégrité et confidentialité) ;
- Supervision des traces.

Gestion des traces

La solution doit permettre un reporting sur les :

- Opérations en général ;
- Accès et les opérations qualifiées comme sensibles réalisées ;
- Sortie d'information (ou exports de données) ;
- Données non intégrées.

L'accès à ces rapports doit être réservé aux personnes clairement identifiées et habilitées.

4.4.2 Protection des applications web

L'application se doit de réduire au maximum les risques d'intrusion et de prévenir les stratégies d'attaques potentielles venant du web.

L'application ne doit pas être sensible à ce type de risques connus (liste non-exhaustive) :

- les injections de codes (de tous types : SQL, XML, Null Byte, LDAP, Mail Command, OS Command, XQuery...) ;
- les attaques par XSS (Cross Site Scripting) ;
- les attaques par des faiblesses dans la gestion des droits et des sessions ;
- les attaques par références directes aux objets ;

- les attaques par « Cross-Site Request Forgery » ;
- les attaques basées sur des erreurs de configuration ;
- les attaques sur des failles de restriction d'URL ;
- les attaques sur des URL d'accès aux objets prévisibles ;
- les attaques sur des redirections abusives.

Pour cela, l'application intègre, au moins, les dispositifs suivants :

- en cas d'utilisation d'espace privé (identifiant de session, etc.) dans les cookies, privilégier les cookies SSL (attribut secure), associer obligatoirement l'attribut HTTPOnly et associer systématiquement les attributs « Path, Domain et Expire » ;
- prévoir une déconnexion au bout de 20 minutes sans saisie ;
- prévoir une possibilité de déconnexion explicite pour l'utilisateur ;
- l'identifiant de session est à initier par le serveur ;
- l'identifiant de session doit être de type aléatoire et non-prédictible et d'une entropie d'au moins 128 bits ;
- l'identifiant de session doit être forgé après l'authentification ;
- lier l'identifiant de session à l'ID utilisateur, mais aussi à son adresse physique (adresse IP) ;
- interdire le passage d'informations sur les habilitations en paramètre ;
- interdire le passage de commandes (SQL, interpréteur..) directement dans les paramètres ;
- contrôler systématiquement les paramètres (formulaires et requêtes), au niveau du serveur ;
- préférer les POST au GET ;
- interdire les références directes aux objets dans les paramètres ;
- systématiser les contrôles d'accès aux objets et aux ressources ;
- gérer les accès multiples aux ressources ;
- durcir les paramètres et possibilités de redirections et de forward ;
- restreindre les accès aux URL d'administration ;
- gérer les erreurs applicatives pour les masquer à l'utilisateur ;
- un système de token par action serait un plus.

5 CADRE D'ORGANISATION DES PRESTATIONS

5.1 SYSTÈME QUALITÉ

En ce qui concerne la qualité, le CNRS préconise de s'appuyer sur la norme ISO 9001 (Systèmes de management de la qualité) et sur des référentiels de bonnes pratiques tels que :

- ITIL® : Bibliothèque pour l'infrastructure des technologies de l'information (Information Technology Infrastructure Library)
- Agile : Manifeste pour le développement agile de logiciels.

Le CNRS est particulièrement attentif à la forte orientation utilisateur, l'approche processus et l'amélioration continue.

Le plan assurance qualité (PAQ) explicite les dispositions qualité (organisation, méthodes, outillage...) nécessaires à la bonne exécution du projet pour toutes les prestations définies dans l'accord-cadre. Il définit les procédures applicables à l'ensemble du périmètre de l'accord-cadre.

Le CNRS peut effectuer des audits de l'application du PAQ. Dans ce cas, le CNRS prévient le titulaire dans les formes mentionnées au CCAP en précisant la nature, le déroulement et le calendrier souhaité.

Côté CNRS, le chef de projet informatique est garant de l'application des dispositions qualité pour le périmètre de son projet. Il est accompagné dans cette activité par la cellule qualité de la DSI, en particulier lors du démarrage de l'accord-cadre. La cellule qualité DSI s'assure du partage des dispositions qualité entre les différents projets et veille à l'homogénéisation des pratiques.

Référence	Libellé exigence	Priorité
QUA_001	Le titulaire fournit au CNRS un plan assurance qualité. Le PAQ est ajusté d'un commun accord avec le CNRS lors du démarrage de l'accord-cadre. Il est mis à jour tant que de besoin tout au long de l'accord-cadre avec l'accord des deux parties.	0
QUA_002	Le titulaire respecte les normes, méthodes et standards qualité du plan assurance qualité. Chaque non-respect d'une exigence du plan qualité est justifié par le titulaire et approuvé par le CNRS avant d'être mis en œuvre.	0
QUA_003	Le titulaire identifie dans son équipe projet les rôles de rédaction et mise à jour du plan assurance qualité, de mise en œuvre opérationnelle des dispositions d'assurance et contrôle qualité.	1
QUA_062	Le titulaire définit dans le PAQ et met en œuvre les contrôles, revues ou audits qualité qu'il juge nécessaires et suffisants dans le contexte du projet, afin de garantir au CNRS la qualité de la prestation et du produit fourni.	1
QUA_004	Le titulaire définit une démarche d'amélioration continue décrivant les dispositions générales mises en œuvre pour faire progresser la qualité de la prestation et du produit fourni (chapitre du PAQ ou document à part). Il met en œuvre cette démarche tout au long de l'accord cadre. Il livre et présente au CNRS un bilan et un plan de progrès à la fin de chaque version majeure mise en production. En phase de maintenance, il livre et présente annuellement au CNRS un bilan de l'année passée et un plan de progrès pour l'année à venir.	1

5.2 ORGANISATION DES ÉQUIPES PROJET

5.2.1 Organisation de l'équipe projet CNRS

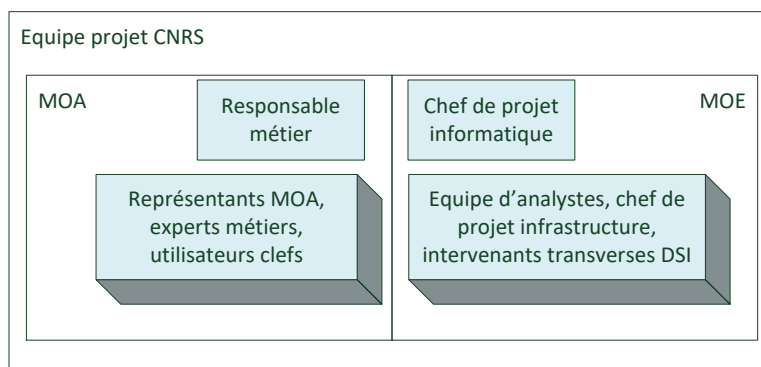


Figure 3 : Organisation du projet au CNRS

Chaque référentiel Réséda comprend une organisation telle que décrite ci-dessus.

La composition de l'équipe projet CNRS est la suivante :

- un **directeur de projet informatique** appartenant à la DSI ;
- un **responsable de l'équipe Réséda MOE** appartenant à la DSI, dont un **chef de projet infrastructure** ;
- des **chefs de projet métier MOA** par référentiel appartenant aux directions référentes DRH, DAPP, DCIF et FSD ;
- des **équipes projet maîtrise d'ouvrage (MOA)** par directions référentes ;
- des **chefs de projet MOE** par référentiel.
- une **équipe Réséda MOE (DSI)** ;

Le/la directeur(trice) de projet pilote les volets financiers, contractuels, opérationnels et coordonne / suit globalement l'avancement de l'ensemble des référentiels en projet, en évolutions et en maintenance corrective.

Le/la responsable de l'équipe Réséda suit opérationnellement les différentes actions en cours sur les référentiels et sur la plateforme.

Côté maîtrises d'ouvrage, les chefs de projet métiers s'appuient sur des représentants des différentes MOA, des experts métier et des utilisateurs, pour définir les besoins métier, les prioriser, participer à la définition de la solution fonctionnellement et enfin mettre en œuvre la conduite du changement.

Côté maîtrise d'œuvre, les chefs de projet informatique sont garants de la mise en œuvre (conception fonctionnelle, suivi de la réalisation, sécurité de la solution, qualification en environnement de recette CNRS) et de l'intégration dans le SI CNRS. Ils s'appuient sur l'équipe Réséda et sur des équipes transverses à la DSI (urbanisation, EAI, sécurité, qualité-méthodes, graphisme...).

Ils sont accompagnés par un chef de projet infrastructure en charge de coordonner et suivre les actions des équipes techniques de la DSI : infrastructure (gestion de parc, système, réseau), web, bases de données, exploitation.

L'interlocuteur CNRS privilégié du titulaire pour les relations contractuelles est le directeur de projet informatique.

5.2.2 Organisation et gestion des compétences de l'équipe projet du titulaire

Le titulaire met en œuvre une organisation et une gouvernance pour piloter l'accord-cadre. Il identifie les compétences nécessaires et s'assure du maintien de ces compétences tout au long de l'accord-cadre.

Référence	Libellé exigence	Priorité
QUA_005	Le titulaire définit dans le PAQ et met en œuvre une organisation et une gouvernance pour piloter l'accord-cadre, en regard de celle du CNRS. Il identifie les profils types (a minima : chef de projet - interlocuteur privilégié du CNRS, responsable technique - architecte, responsable	1

Référence	Libellé exigence	Priorité
	sécurité, responsable qualité et développeur). Il précise pour chaque profil les compétences associées et le taux de disponibilité minimal.	
QUA_006	Le titulaire propose dans le PAQ et met en œuvre une organisation des équipes adaptée aux différentes prestations de l'accord-cadre et aux phases de la méthode de développement du projet.	1
QUA_008	Le titulaire communique au CNRS une matrice de couverture des profils types et compétences par l'équipe projet ainsi que l'identité et le CV de chaque membre de l'équipe dès la notification de l'accord-cadre et à chaque changement d'un membre de l'équipe projet.	1
QUA_009	Le titulaire s'engage sur une équipe ferme pour le démarrage de l'accord-cadre, a minima pour les profils types de chef de projet et responsable technique.	1
QUA_010	Le titulaire assure tout au long de la durée de l'accord-cadre : ■ le maintien de la qualité : respect des profils types déposés dans l'offre du titulaire pour chacun des intervenants ; ■ le maintien de la continuité : pas plus d'un changement au cours d'une période de six (6) mois glissants parmi les profils clés du titulaire, sauf en cas de force majeure.	1
QUA_011	En cas de nécessité de remplacement d'un membre de l'équipe, la période de recouvrement est comprise a minima entre deux (2) semaines et un (1) mois en fonction du profil. Ce délai de transfert de compétences et de connaissances du contexte du CNRS et du projet est défini en accord avec le CNRS et strictement respecté.	1
QUA_012	Le titulaire informe le CNRS par écrit de tout changement concernant l'équipe projet avec un préavis de trois (3) mois pour les profils clefs ou un (1) mois sinon.	1
QUA_013	Le titulaire met en œuvre des dispositions pour gérer la variation de charges de son équipe afin de garantir sa flexibilité et sa réactivité en fonction de l'activité du projet.	1

5.3 DISPOSITIFS DE CONDUITE DE PROJET

5.3.1 Structures de pilotage projet

Les principales structures à mettre en place entre le CNRS et le titulaire pour assurer le bon déroulement du projet sont décrites ci-dessous :

- **Comité mensuel de suivi (MOA/MOE/titulaire) dénommé COSUI :**
 - il a pour objet le pilotage global des activités du titulaire (y compris qualité et sécurité), ainsi que le suivi de l'avancement des activités sur les différentes applications du périmètre (risques, indicateurs, planning global, ressources). Il décide du lancement de nouvelles évolutions voire référentiel et dans ce cadre, valide la planification globale des actions demandées au titulaire ;
 - il est composé pour le CNRS du directeur de projet informatique de l'accord-cadre, du responsable de l'équipe Réséda et des chefs de projet métiers et informatiques des différents référentiels de la plateforme, des membres des équipes projets métiers et DSI en fonction de l'ordre du jour, d'un éventuel représentant des départements qualité et sécurité, et de la direction de la DSI, et pour le titulaire, a minima, du directeur de projet et du chef de projet ;
 - pour chaque réunion de comité, un ordre du jour systématique et un document support sont préparés par le titulaire et diffusés au préalable, aux participants et un compte-rendu est rédigé et envoyé à son issue. Le CNRS valide le compte-rendu dans les cinq jours. A défaut de réponse, le compte-rendu est réputé approuvé par le CNRS.
- **Comité hebdomadaire de projet (MOE/titulaire) dénommé COPRO :**
 - il a pour objet le pilotage régulier des activités du titulaire, ainsi que le suivi opérationnel des projets de référentiels (suivi des actions, des versions et livraisons...) ;
 - il est composé pour le CNRS du responsable de l'équipe Réséda et des chefs de projet informatique ainsi que des membres de l'équipe Réséda et pour le titulaire, a minima, du chef de projet ;
 - pour chaque réunion de comité, un document dénommé « CRA – Compte Rendu d'Avancement » est mis à jour et trace opérationnellement les actions en cours. Ce CRA est maintenu par le titulaire. Le CNRS valide la dernière version du CRA dans les cinq jours. A défaut de réponse, le CRA est réputé approuvé par le CNRS.
- **Comité hebdomadaire de suivi technique (MOE/titulaire) dénommé COTEC :**

- il a pour objet le pilotage régulier des activités en lien avec les équipes techniques de la DSI ;
 - il est composé a minima pour le CNRS des membres de l'équipe Réséda en charge du socle Réséda et du chef de projet infrastructure en charge de coordonner et suivre les actions des équipes techniques de la DSI : infrastructure (gestion de parc, système, réseau), web, bases de données, exploitation ; et pour le titulaire, a minima, du chef de projet et l'architecte technique
 - pour chaque réunion de comité, un tableau de suivi des actions est pris en charge par l'équipe Réséda et géré par cette même équipe en commun avec le chef de projet infrastructure CNRS.
- **Comité trimestriel de suivi contractuel (MOE/titulaire) dénommé COCON :**
- il a pour objet le pilotage régulier des aspects contractuels et financiers (commandes / factures) en lien avec l'équipe Marchés de la DSI ;
 - il est composé a minima pour le CNRS du directeur de projet informatique, de la responsable de l'équipe Marchés DSI ; pour le titulaire le directeur de projet
 - pour chaque réunion de comité, un ordre du jour systématique et un document support sont préparés par le titulaire et diffusés au préalable, aux participants et un compte-rendu est rédigé et envoyé à son issue. Le CNRS valide le compte-rendu dans les cinq jours. A défaut de réponse, le compte-rendu est réputé approuvé par le CNRS.
- **Comité Semestriel de suivi cybersécurité (MOE/titulaire) dénommé COSEC :**
- il a pour objet le pilotage régulier des aspects cybersécurité et le plan d'assurance sécurité en lien avec les équipes techniques de la DSI et le département cybersécurité de la DSI
 - il est composé a minima pour le CNRS d'un membre de l'équipe Réséda en charge du socle Réséda et d'un représentant du département cybersécurité ; et, à minima, du porteur des aspects cybersécurité du marché et des prestations.
 - pour chaque réunion de comité, un ordre du jour systématique et un document support sont préparés par le titulaire et diffusés au préalable, aux participants et un compte-rendu est rédigé et envoyé à son issue. Le CNRS valide le compte-rendu dans les cinq jours. A défaut de réponse, le compte-rendu est réputé approuvé par le CNRS.

Référence	Libellé exigence	Priorité
QUA_014	Le titulaire met en œuvre et participe aux comités de suivi selon une fréquence mensuelle ou définie en accord avec le CNRS.	1
QUA_015	Le titulaire met en œuvre et participe aux comités de projet selon une fréquence hebdomadaire définie en accord avec le CNRS.	1
QUA_016	Le titulaire fournit aux participants des comités un document support dans les deux jours ouvrés précédant la réunion.	1
QUA_017	Le titulaire rédige et adresse le compte-rendu des comités aux participants dans les deux jours ouvrés consécutifs au comité.	1
QUA_018	Le titulaire propose dans le PAQ et met en œuvre toute autre structure de pilotage adaptée aux différentes prestations de l'accord-cadre.	1

5.3.2 Pratiques de gestion de projet

Le CNRS souhaite qu'à minima le titulaire mette en œuvre les pratiques de gestion de projet suivantes :

Référence	Libellé exigence	Priorité
QUA_020	Chaque réunion ou point téléphonique entre le titulaire et le CNRS fait l'objet d'une trace écrite (courriel, compte-rendu de réunion) rédigée par le titulaire et à valider par l'ensemble des participants dans un délai fixé par les 2 parties.	1
QUA_021	Chaque courriel envoyé suit les préconisations suivantes : ■ préfixer l'objet du message avec le nom du projet : « [Nom projet] sujet » ; ■ si nécessaire, indiquer l'urgence attendue pour la réponse en précisant URGENT dans l'objet du message « [nom-projet] URGENT sujet » ;	1

Référence	Libellé exigence	Priorité
	- dans le corps du message, préciser ce qui est attendu du destinataire : simple information, avis, décision, action... Si nécessaire, indiquer la date d'échéance attendue pour la réponse ; - éviter les pièces jointes, les remplacer par des liens vers l'outil collaboratif du CNRS.	
QUA_022	Le titulaire suit et informe le CNRS des actions identifiées lors des comités ou réunions diverses avec le CNRS.	1
QUA_023	Le titulaire tient à jour et diffuse au CNRS un planning du projet, global pour l'ensemble du projet et détaillé pour la phase à venir.	1
QUA_024	Le titulaire gère les risques du projet qui ont été formalisés dans son offre et ajustés lors du démarrage et tout au long de l'accord-cadre.	1
QUA_025	Le titulaire définit les procédures d'alertes et d'arbitrage.	1
QUA_026	Le titulaire met en œuvre une procédure de gestion de crise en cas d'alerte avérée. Il précise le processus d'escalade suivi pour le traitement et la résolution de ces problèmes.	0

La gestion de crise s'impose dans le cas d'incident persistant (délai de résolution indéterminable, correction impossible ou inefficace), d'incident de sécurité de grande envergure (attaque virale), d'incidents multiples, de risque d'altération de données (perte de sauvegarde, ...), de risque avéré sur le fonctionnement et les missions du CNRS (atteinte à l'image de marque), et de l'occurrence de tout événement à caractère improbable ou de criticité catastrophique (atteinte à la sauvegarde des personnes ou des biens).

5.3.3 Indicateurs de pilotage et qualité du projet

Des indicateurs pertinents sont définis pour permettre de suivre l'avancement du projet et d'anticiper la survenance des difficultés. Ces indicateurs sont mesurés régulièrement et présentés par le titulaire lors des comités.

Les indicateurs que le CNRS souhaite suivre sont notamment les suivants :

- indicateurs de pilotage :
 - état d'avancement des prestations en cours (livrées, qualifiées CNRS, facturées)
 - coûts et ressources prévues, affectées, consommées
 - turnover de l'équipe projet
 - respect des délais de diffusion des documents pour les comités
 - taux de satisfaction client
- indicateurs de qualité du code :
 - taux de couverture des tests unitaires automatisés
 - taux de commentaires
 - convention de nommage
 - complexité du code, couplage
 - mesures de performance
- indicateurs de qualité des livraisons :
 - respect des délais de livraison
 - nombre d'anomalies² (bloquantes, majeures, mineures) en recette et en production, ratio nombre anomalies/charge commandée, nombre d'anomalies imputables à des régressions
 - nombre de livraisons nécessaires au prononcé de la validation (documents et logiciels)

Le titulaire peut proposer de nouveaux indicateurs, dans la mesure où ils permettent de piloter efficacement le projet.

Le plan de mesure explicite les indicateurs, leurs modalités de calculs (formule, période retenue, outillage), leurs objectifs à atteindre et leurs modalités de suivi.

Référence	Libellé exigence	Priorité
QUA_027	Le titulaire fournit au CNRS un plan de mesure (chapitre du plan assurance qualité ou document à part) adapté à la méthode de développement du projet. Le plan de mesure est ajusté d'un commun accord avec le CNRS lors du démarrage de l'accord-cadre. Il est mis à jour tant que de besoin tout au long de l'accord-cadre avec l'accord des deux parties.	1

² La définition et la typologie des anomalies sont décrites dans le glossaire du Livret 2 du CCTP.

Référence	Libellé exigence	Priorité
QUA_028	Le titulaire élabore, maintient et livre lors des différents comités les tableaux de bord conformes au plan de mesure comprenant les indicateurs adaptés au niveau du comité concerné.	0

5.4 MÉTHODE DE DÉVELOPPEMENT

5.4.1 Cycle de vie

Les activités à mener tout au long du projet se répartissent de la manière suivante :

- expression des besoins (à la charge du CNRS) ;
- réalisation (à la charge du titulaire) : spécifications fonctionnelles et techniques détaillées, conception, paramétrage ou développements spécifiques, tests unitaires, d'intégration, de validation, de non-régression, de performance et de sécurité ;
- recette (à la charge du CNRS, avec assistance éventuelle du titulaire) : validation des développements en environnement de recette ;
- mise en production (à la charge du CNRS, avec assistance éventuelle du titulaire) : initialisation du système, mise en production ;
- en parallèle, conduite du changement (à la charge du CNRS, avec assistance éventuelle du titulaire) : communication, formation des utilisateurs, documentations utilisateurs, organisation de l'assistance.

Pour l'enchaînement de ces activités, le CNRS préconise un cycle de vie itératif et incrémental³, découpé en plusieurs versions mises en production sur décision du CNRS. Chaque version suit globalement un cycle en cascade.

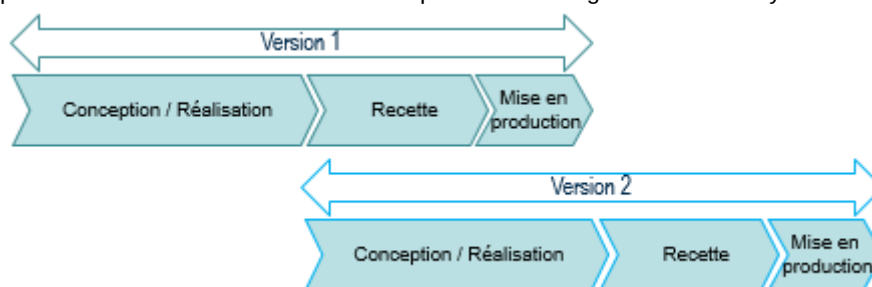


Figure 4 : Cycle de vie en cascade itératif et incrémental

Toutes les dispositions mises en œuvre par le titulaire pour donner visibilité au CNRS sur la réalisation d'une version en cours sont appréciées par le CNRS.

Afin de vérifier l'avancement régulier des travaux et de détecter en amont les problèmes, le titulaire peut planifier, en accord avec le CNRS, une ou plusieurs mises à disposition intermédiaires des produits de la commande. Elles donnent lieu, le cas échéant et selon le livrable, à des remarques pour les documents ou des déclarations d'anomalies (pour l'application). Elles ne donnent pas lieu à des opérations de réception au sens du CCAP.

Si le contexte s'y prête (complexité/criticité de l'évolution ou d'un nouveau référentiel), le CNRS peut demander au titulaire de mettre en place une méthode de développement orientée agile. La mise en œuvre de cette méthode de développement orientée agile doit prendre en compte la synchronisation nécessaire avec les autres projets en cours et la capacité du CNRS d'y faire face, en plus des éléments propres au projet.

Les activités à réaliser, les livrables attendus et l'outillage de suivi et pilotage du projet demeurent globalement les mêmes qu'en mode non orienté agile, tels que définis dans l'accord-cadre.

La décision de suivre une méthode de développement orientée agile ainsi que la validation des modalités de sa mise en œuvre opérationnelle reviennent in fine au CNRS. Sa mise en œuvre opérationnelle et son suivi sont à la charge du titulaire.

³ La notion d'incrémental sous-entend ici qu'une première itération de la mise en œuvre d'une fonctionnalité peut être suivie d'une deuxième itération visant à la compléter ou la modifier au vu de ce qu'a matérialisé la première itération mais également au vu de ce que l'ajout d'autres fonctionnalités a pu mettre en évidence pour l'utilisateur.



Figure 5 : Cycle de vie agile

Référence	Libellé exigence	Priorité
QUA_029	Le titulaire définit dans le PAQ et met en œuvre une méthode de développement itérative-incrémentale, adaptée au contexte du projet ou de l'évolution. Il identifie les phases, entrées attendues, activités, rôles et livrables fournis.	1
QUA_031	Le titulaire, en accord avec le CNRS, définit le périmètre des versions et des itérations en fonction des exigences fonctionnelles (priorités des utilisateurs), ergonomiques, techniques et dans un objectif de réduction des risques.	1
QUA_030	Dans le cas où le CNRS demande une méthode de développement orientée agile, Scrum est préconisé (cf. https://www.scrum.org). Le titulaire définit dans le PAQ les modalités de sa mise en œuvre opérationnelle. Le cycle de développement de l'application est découpé en versions mises en production, elles-mêmes composées d'itérations (sprints de durée fixe) permettant de disposer rapidement de nouvelles fonctionnalités. Les activités à réaliser, les livrables attendus et l'outillage de suivi et pilotage du projet demeurent les mêmes qu'en mode non orienté agile. L'ensemble de la documentation est créée, mise à jour et livrée de façon itérative et incrémentale.	1
QUA_007	Dans le cas où le CNRS demande une méthode de développement orientée agile, le titulaire définit dans le PAQ les rôles spécifiques liés au mode agile (<i>par exemple</i> : product owner, proxy product owner, scrum master, équipe de développement). L'attribution des rôles aux membres des équipes CNRS et titulaire se fait en concertation avec le CNRS.	1
QUA_019	Dans le cas où le CNRS demande une méthode de développement orientée agile, le titulaire définit dans le PAQ les objectifs, la fréquence ainsi que les participants du titulaire et du CNRS pour chaque rituel mis en place (<i>par exemple</i> : <i>sprint planning</i> , <i>daily scrum</i> , <i>sprint review</i> , <i>sprint retrospective</i>).	1

5.4.2 Activités de réalisation (à la charge du titulaire)

Le titulaire conduit les travaux de réalisation en respectant les exigences applicables.

Afin de minimiser les phases de recette du CNRS (nombre d'anomalies⁴ minimal et période réduite de tests de recette), le titulaire maximise la qualité des documents de conception et du code produit et propose une organisation pertinente quant à ses propres tests (organisation, outillage...).

Lors de la phase de réalisation (développement de la version initiale d'un référentiel ou d'évolutions importantes sur un référentiel existant), le CNRS préconise fortement au titulaire de mettre en œuvre un cycle de vie itératif et incrémental sur cette phase de réalisation (à valider avec l'équipe CNRS avant mise en œuvre) afin de constituer des livraisons applicatives intermédiaires, et de respecter les pratiques suivantes :

- identifier les itérations du cycle et les versions incrémentales de l'application, en fonction des exigences fonctionnelles (priorités des utilisateurs), ergonomiques ou techniques et des risques. Une des premières itérations doit permettre de matérialiser les règles de présentation des écrans et de navigation dans l'application ;
- planifier chaque livraison et validation de version incrémentale ;
- si les délais sont trop courts pour effectuer des livraisons intermédiaires de l'application, s'appuyer sur une maquette puis sur des livraisons et des validations intermédiaires de la documentation de conception.

Toutes les dispositions mises en œuvre par le titulaire pour donner visibilité au CNRS sur les développements en cours seront appréciées par le CNRS.

Nota Bene : la notion d'incrémental sous-entend ici qu'une première itération de la mise en œuvre d'une fonctionnalité pourra être suivie d'une deuxième itération visant à la compléter ou la modifier au vu de ce qu'aura matérialisé la première itération mais également au vu de ce que l'ajout d'autres fonctionnalités aura pu mettre en évidence pour l'utilisateur.

⁴ La définition d'une anomalie est décrite dans le glossaire du Livret 2 du CCTP.

Référence	Libellé exigence	Priorité
QUA_032	Le titulaire décrit dans le PAQ le déroulement des ateliers de travail avec le CNRS : leur déclenchement en lien avec le cycle de vie du projet, leurs modalités de déroulement, les supports produits (avant, après et dans quels délais).	1
QUA_033	Le titulaire intègre dans sa démarche de conception de la solution une méthode d'analyse de l'expérience utilisateur (UX) afin de prendre en compte les critères de satisfaction de l'utilisateur.	2
QUA_034	Le titulaire s'appuie sur une maquette pour faire valider au CNRS, avant codage, les règles d'ergonomie, de présentation des écrans et de navigation dans l'application.	1
QUA_035	Les spécifications fonctionnelles détaillées sont formalisées sous forme de cas d'utilisation et de diagrammes UML.	1
QUA_036	Le titulaire définit dans le PAQ la stratégie de tests qu'il met en place pour le projet, en couverture des exigences fonctionnelles, techniques et d'interface. Il en précise également les différents niveaux (unitaire automatisé ou manuel, d'intégration, de validation, de non-régression, de performance unitaire et/ou plus global, de sécurité) et l'outillage associé.	1
QUA_037	Le titulaire adapte l'activité de test à la méthode de développement du projet.	1
QUA_038	Dans le cas où le CNRS demande une méthode de développement orientée agile, le titulaire définit dans le PAQ et met en œuvre : - l'utilisation de user stories permettant de spécifier le contenu du backlog de chaque itération (tout en assurant la rédaction finale des spécifications fonctionnelles détaillées sous forme de cas d'utilisation), - des techniques de tests adaptées (tels que Test Driven Development, Acceptance Test-Driven Development...).	1

5.4.3 Activités de recette (à la charge du CNRS)

Le CNRS rédige son cahier de recette pour ses propres tests. En aucun cas, ce cahier ne peut être utilisé par le titulaire pour passer ses tests d'intégration ou de validation.

La recette CNRS est composée de différents types de tests :

- fonctionnels, techniques, intégration dans le SI, sécurité (par la maîtrise d'œuvre DSI) ,
- métier (par les maîtrises d'ouvrage).

Une analyse de la qualité du code et de l'architecture logicielle peut également être réalisée par la DSI (en plus des comptes rendus et indicateurs fournis par le titulaire).

Dans le cas où le CNRS demande une méthode de développement orientée agile, le CNRS définit des tests d'acceptance au début de chaque itération (sprint) qui sont déroulés par le titulaire lors de la démonstration de fin d'itération. Ces tests d'acceptance ne suffisent généralement pas à valider l'itération livrée. C'est pourquoi ils se prolongent pendant les itérations suivantes et à l'issue de la dernière itération d'une version, l'équipe CNRS effectue une recette finale de l'ensemble de l'application.

Le CNRS passe des scénarios de tests en environnement de recette à chaque livraison logicielle ou évolution du paramétrage.

Les résultats des tests du CNRS sont consignés dans des dossiers de tests ou dans l'outil de gestion des tests de recette du CNRS.

Les anomalies détectées par le CNRS sont formalisées et classifiées selon 3 niveaux de gravité (cf. glossaire du Livret 2 du CCTP) dans l'outil de gestion des anomalies et évolutions du CNRS.

Dans le cas où le CNRS demande une méthode de développement orientée agile, la correction de ces anomalies est intégrée soit dans l'itération en cours (pour les bloquantes), soit dans les itérations à venir. La priorité et la planification données à la correction de ces anomalies sont fixées conjointement par l'équipe de développement et par le CNRS.

Référence	Libellé exigence	Priorité
QUA_039	Le titulaire s'engage à corriger la totalité des anomalies issues de la recette avant mise en production, sauf dérogation explicite du CNRS.	0

5.5 GESTION DES ENVIRONNEMENTS

5.5.1 Postes de travail du titulaire

Le titulaire respecte les contraintes suivantes pour les postes de travail de tous les membres de son équipe :

Référence	Libellé exigence	Priorité
ENV_001	Le titulaire fournit pour ses équipes, les postes de travail, imprimantes, scanner... et les logiciels, ainsi que les fournitures bureautiques, y compris lorsque la réalisation s'effectue dans les locaux du CNRS.	0
ENV_002	Le titulaire respecte les contraintes du cadre de cohérence technique (CCT) au niveau de la connectivité SSL, et regroupe dans un réseau dédié tous les postes de travail non hébergés dans les locaux du CNRS et devant accéder aux ressources serveurs et bureautiques du CNRS.	0

5.5.2 Environnement de développement

La plate-forme de développement et de tests unitaires mise en œuvre par le titulaire doit respecter les contraintes suivantes :

Référence	Libellé exigence	Priorité
ENV_003	Le titulaire met en œuvre une plate-forme de développement et tests pour son besoin propre, compatible avec l'environnement cible de production qui fait référence.	0
ENV_004	Dans certains cas, le titulaire peut être amené à implémenter sur la plate-forme de développement des « bouchons » afin de simuler des connexions aux services d'infrastructures qui seront utilisés sur les autres environnements (en particulier l'EAI/ESB et le service d'authentification). Ces actions sont à décider en commun avec l'équipe projet CNRS	1

5.5.3 Environnements CNRS

Le CNRS fournit et administre l'ensemble des plates-formes serveurs du projet à l'exception de la plate-forme de développement et de tests du titulaire :

- Un environnement d'Intégration : cet environnement permet au titulaire de tester l'intégration de l'application dans le SI (authentification et EAI/ESB compris).
- Un environnement de Recette : cet environnement permet au CNRS de réaliser les tests de recette (Vérification d'Aptitude) de l'application avant mise en production.
- Un environnement de Production : cet environnement héberge l'application accessible aux utilisateurs et permet au CNRS de réaliser la Vérification de Service Régulier.
- Un environnement de Formation : cet environnement est dédié aux formations des utilisateurs à l'application.

Le CNRS est responsable des briques mutualisées comme les frontaux web, le SSO (Single Sign-On) et les serveurs de base de données.

Le CNRS est responsable (installation et exploitation) des composants d'infrastructures, OS, stockage, réseau, sur tous les environnements (intégration, recette, formation et production). Le dimensionnement des environnements est selon les besoins et l'utilisation de chacun d'eux.

Le CNRS assure l'exploitation applicative des environnements de recette, formation et production.

Le CNRS utilise l'outil Ansible Tower pour automatiser les déploiements des applications lorsque cela est possible.

Les environnements de recette, de formation et de production ne sont pas accessibles au titulaire. Cependant, en cas de besoin, le CNRS peut demander au titulaire de l'accompagner dans la recherche de résolutions de problèmes existants.

Les exigences suivantes s'appliquent au paysage applicatif précité :

Référence	Libellé exigence	Priorité
ENV_005	Un environnement d'Intégration est préparé par le CNRS. Il est ensuite à la charge du titulaire de procéder aux installations applicatives sur ces environnements. Le titulaire est autonome sur ces environnements.	0
ENV_006	Les environnements de recette, de formation et de production ne sont pas accessibles au titulaire. Cependant, en cas de besoin, le CNRS demande au titulaire d'y accéder, sur site CNRS uniquement.	0

5.6 GESTION DES LIVRAISONS

La réalisation d'une commande par le titulaire donne lieu par celui-ci à la mise à disposition des livrables mentionnés dans chaque prestation (cf. Livret 2). La procédure de livraison s'effectue selon les modalités suivantes :

Référence	Libellé exigence	Priorité
QUA_040	Chaque livraison d'un produit fini effectuée par le titulaire est accompagnée d'un bon de livraison, précisant la version des composants livrés (application ou document), la liste des exigences et des modifications implémentées, en particulier la liste des fiches de relecture prises en comptes ou la liste des anomalies corrigées dans la version. Ce bon de livraison est déposé par le titulaire dans l'outil collaboratif du CNRS.	1
QUA_041	Un courriel est adressé à l'équipe projet CNRS l'informant de la mise à disposition de la livraison et contenant un lien vers le bon de livraison.	1
QUA_042	Pour les livraisons documentaires, le titulaire utilise l'outil collaboratif du CNRS.	1
QUA_043	Pour les livraisons applicatives, le titulaire utilise la forge DSI, pour y déposer l'ensemble des composants de l'application et les manuels d'installation et d'exploitation (cf. « Description des livrables documentaires » en annexe du Livret 2) qui permettent au CNRS de mettre en œuvre et d'exploiter l'application livrée.	1
QUA_044	Tous les éléments fournis lors d'une livraison applicative (y compris le code source) permettent d'identifier l'application concernée et sa version livrée. Toute version de l'application est identifiée par un numéro de version unique : version.sous-version.état technique[-rcN] : - le numéro de version est incrémenté à chaque évolution fonctionnelle importante, - le numéro de sous-version : lors d'une évolution fonctionnelle minime, - l'état technique : lors d'une correction logicielle (par rapport à la version en production), [-rcN] : (optionnel) numéro de Release Candidate pour les livraisons en recette ; ce numéro de Release Candidate n'est pas présent dans la version finale (pour la production)	1
QUA_045	En cas de livraison d'un delta, le titulaire procède à une re-livraison totale une fois la version stabilisée.	1
QUA_046	En accord avec le CNRS, les livraisons applicatives peuvent être accompagnées d'une démonstration de l'application par le titulaire, en présence du titulaire et de l'équipe CNRS.	2

5.7 GESTION DE LA DOCUMENTATION

La documentation produite par le titulaire doit être de qualité et permettre une bonne compréhension des mécanismes développés à des fins d'exploitation et de maintenabilité.

Référence	Libellé exigence	Priorité
QUA_047	Tous les documents produits dans le cadre du présent accord-cadre sont livrés sous format électronique modifiable (donc pas uniquement en pdf).	1
QUA_048	Les documents du projet sont déposés et partagés par le CNRS et le titulaire dans l'outil collaboratif du CNRS.	1
QUA_049	Le titulaire remet à l'issue de l'accord-cadre l'ensemble de la documentation fonctionnelle et technique de l'application à jour (créée et modifiée tout au long de l'accord-cadre).	0

L'objectif du CNRS est de tendre vers l'application de dispositions communes pour la documentation des différentes applications. Dans le cas de l'application Réséda, où il existe des principes de gestion de la documentation spécifiques, ils sont appliqués tels quels ou évoluent sur demande du CNRS.

Les principes de gestion de la documentation préconisés au CNRS sont les suivants :

Référence	Libellé exigence	Priorité
QUA_050	Tout document produit contient : le nom du document, une référence, la date de dernière mise à jour, la version, l'historique des versions (si besoin), le sommaire, les pages numérotées, les marques de révision apparentes d'une version à l'autre (si besoin).	1
QUA_051	Chaque document reçoit une référence unique au sein du projet (nom du fichier) : Nom-du-projet_Identification-du-document_[Confidentialité_]Vx.y ou Nom-du-projet_Identification-du-document_[Confidentialité_]Date-evenement avec : ■ Identification-du-document = nom représentatif du contenu, de la forme : Type-document_[Code-domaine]_Libelle-libre ■ Confidentialité : code indiquant le niveau de confidentialité du document, DL, DC ou DR ■ Vx.y : version du document pour les documents de référence ■ Date-evenement au format AAAAMMJJ pour les documents événementiels (CR de réunion...). La référence du document ne contient aucun caractère accentué ni espace (à remplacer par « - »).	1
QUA_052	Chaque document mentionne dans sa référence le code de confidentialité. Seuls les documents de niveau classification PUBLIC (cible de diffusion non contrôlée : la publication de l'information présente un impact nul pour l'organisme) n'ont pas de code de classification. Les différents codes et niveaux de classification sont les suivants : ■ DL : DIFFUSION LIMITEE + Mention pour une information dont la cible n'est pas nominative mais dont la mention précise les structures ou entités destinataires de l'information ou des personnes es-qualité. La mention spécifique associée au niveau de classification peut être suffisante pour définir la liste de diffusion. Une divulgation non autorisée de l'information aurait un impact modéré ; ■ DC : DIFFUSION CONFIDENTIELLE pour une information dont la cible n'est pas nominative mais précise les structures ou entités destinataires de l'information, des personnes es-qualité et qui doit être diffusée via un canal dont l'accès est strictement contrôlé. Une divulgation non autorisée de l'information aurait un impact important ; ■ DR : DIFFUSION RESTREINTE conformément à l'I1901 pour une information dont la cible est nominative ou précise les structures ou entités destinataires de l'information, des personnes es-qualité ayant besoin d'en connaître et qui doit être diffusée via un canal dont l'accès est strictement contrôlé. Une divulgation non autorisée de l'information aurait un impact catastrophique.	0
QUA_053	Pour chaque document, un marquage est apposé afin de signifier le niveau de protection et les mesures réglementaires à appliquer en ce qui concerne la communication, la diffusion, la reproduction, la conservation et la destruction de ceux-ci : le niveau de classification (DIFFUSION LIMITEE, DIFFUSION CONFIDENTIELLE ou DIFFUSION RESTREINTE) est apposé en haut de chaque page en caractères gras, rouge et en capitales.	0
QUA_054	Le numéro de version du document est incrémenté à chaque modification du contenu du document devant faire l'objet d'une diffusion (il n'est pas incrémenté pour des corrections portant sur la forme du document - fautes de frappe, d'orthographe, ...). Le numéro de version est de la forme : x.y, avec : ■ x : incrémenté à chaque évolution majeure du document (<i>par exemple</i>, ajout de chapitres, changement de version de l'application, refonte du document...) ■ y : incrémenté à chaque évolution mineure (<i>par exemple</i>, prise en compte de remarques de relecture, ajout de précisions...).	1
QUA_055	Les documents du projet sont initiés à partir de modèles. Ces modèles sont définis au démarrage de l'accord-cadre et référencés dans le plan assurance qualité. Ils peuvent être issus soit du fonds documentaire du CNRS soit de celui du titulaire.	1

Le CNRS formalise ses remarques au travers d'une fiche de relecture pour les documents qui ont fait l'objet d'une livraison, par marques de révision dans le document pour les comptes rendus et les mises à dispositions intermédiaires.

Une partie de la documentation peut éventuellement être gérée dans le Wiki du CNRS.

Les règles et pratiques à mettre en œuvre autour de la gestion documentaire sont ajustées d'un commun accord au démarrage de l'accord-cadre.

5.8 CAPITALISATION DES CONNAISSANCES

La capitalisation des connaissances acquises lors de l'exécution des prestations est un facteur clés de succès, tant pendant la durée d'exécution de l'accord-cadre que lors de la phase de réversibilité éventuelle en fin d'accord-cadre. A ce titre, le titulaire met en œuvre les pratiques suivantes :

Référence	Libellé exigence	Priorité
QUA_056	Le titulaire identifie les informations ne relevant pas de la documentation, nécessaires à ses équipes pour exécuter correctement les prestations objet de l'accord-cadre. Il peut s'agir, sans que la liste ne soit exhaustive, de procédures, de guides opératoires, d'une base de connaissance, ... Il s'assure également de leur suivi, de leur mise à jour et de la gestion de leur obsolescence.	1
QUA_057	Le titulaire rend compte de l'avancement de la mise en œuvre du système de capitalisation pendant le comité de suivi du projet.	1
QUA_058	Le titulaire livre annuellement ou à la demande les informations relevant de la capitalisation des connaissances dans les formats compatibles avec les outils du CNRS.	1

5.9 OUTILLAGE DE SUIVI ET PILOTAGE DU PROJET

Le CNRS utilise les outils suivants :

- gestion des anomalies et des évolutions : Mantis (<https://www.mantisbt.org/>)
- assistance : e-dem, basé sur JIRA Service Desk (désormais Jira Service Management <https://www.atlassian.com/fr/software/jira/service-management>)
- base de connaissance, wiki : Confluence (<https://fr.atlassian.com/software/confluence>)
- gestion documentaire, collaboratif : CoRe, basé sur Microsoft SharePoint (<https://www.microsoft.com/fr-fr/>)
- modélisation : PowerAMC (<https://www.sap.com/france/products/powerdesigner-data-modeling-tools.html>)
- gestion des tests de recette : [Dossier](#) de tests et de recette - Excel

Référence	Libellé exigence	Priorité
QUA_059	Le titulaire utilise les outils ci-dessous, fournis par le CNRS : ■ l'outil libre Mantis, pour le suivi des anomalies et du portefeuille de demandes d'évolution, ■ l'outil CoRe, basé sur la plate-forme collaborative MS SharePoint, pour le partage des documents, livraisons documentaires, calendriers, annuaires, suivi d'actions...	1
QUA_060	Le CNRS se réserve la possibilité de changer l'un ou l'autre des outils présentés ci-dessus, au cours de la durée de vie de l'accord-cadre. Dans ce cas, le titulaire en est informé suffisamment à l'avance et procède également au changement d'outillage dans ses relations avec le CNRS. Ce changement est réputé n'avoir aucun impact financier quant à l'exécution du présent accord-cadre.	1

Ces outils sont mis en œuvre et paramétrés par le CNRS. Ils sont accessibles par les équipes maîtrise d'œuvre et maîtrise d'ouvrage CNRS, et le sont également par le titulaire (avec des profils différents). Les pratiques mises en place autour de ces outils sont préconisées par la cellule qualité de la DSI du CNRS, elles sont communiquées au titulaire et ajustées d'un commun accord au démarrage de l'accord-cadre.

Référence	Libellé exigence	Priorité
QUA_061	Le titulaire met en œuvre des outils bureautiques et de gestion de projet qui supportent des formats compatibles avec les outils utilisés ou préconisés par le CNRS, mais non fournis au titulaire :	1

Référence	Libellé exigence	Priorité
	- suite bureautique : MS Office, - gestion de projet : MS Project, - modélisation des données : PowerAMC, - dossiers et suivi des tests : Excel, - wiki : Confluence.	

Le titulaire peut le cas échéant proposer d'autres outils pour compléter ceux proposés par le CNRS. Toutefois, ceux-ci seront soumis à acceptation par celui-ci.

5.10 MESURES ET CLAUSES DE SÉCURITÉ

5.10.1 Gestion de la Sécurité par le titulaire

Responsabilité

Référence	Libellé exigence	Priorité
SECU_001	L'organisation de la sécurité des systèmes d'information du titulaire pour le projet est décrite dans le PAS. L'équipe comporte a minima : - Une personne de niveau hiérarchique supérieur formé et compétent en SSI capable de prendre des décisions dans la conduite du projet, responsable du respect des dispositions du PAS - Une personne intégrée ou proche des équipes de MOE du titulaire en charge du projet responsable de la mise en œuvre du PAS - La rédaction, la mise à jour et le suivi du PAS sont à la charge du titulaire	0

Dans l'exercice de leurs activités, les intervenants sont liés par un devoir de réserve et astreints au secret professionnel.

Sensibilisation, qualification et formation

Référence	Libellé exigence	Priorité
SECU_002	Le titulaire indique au CNRS la fréquence et le contenu des actions de formation et de sensibilisation de ses personnels aux enjeux et aux méthodes de Sécurité.	0

5.10.2 Protection des biens

Protection des sites

Référence	Libellé exigence	Priorité
SECU_003	Si le titulaire exécute les prestations à partir de ses propres locaux ou en télétravail, il opère en « <i>site sûr</i> » dont les caractéristiques sont à évaluer avec le département Sécurité de la DSI. Cette disposition est également valable pour le support ou la maintenance à distance. Le titulaire ne détient à aucun moment de données de production significatives sur ses infrastructures. Le cas échéant, le titulaire réalise un dossier de type « <i>site sûr</i> » incluant les modalités d'accès aux ressources de la DSI et les mesures de sécurité nécessaires à l'accomplissement des prestations. Si un Plan d'Assurance Sécurité existe, le dossier « <i>site sûr</i> » lui sera annexé. En cas de télétravail, aucun accès aux environnements ou aux données de production n'est autorisé.	0
SECU_004	Le titulaire fournit un dossier de site sûr décrivant les mesures de sécurité physique en place dans les locaux qu'il utilise pour l'accomplissement des prestations. Ce dossier traite des thématiques suivantes sous les angles technique et organisationnel : - Infrastructures informatiques (réseaux et systèmes) - Contrôle d'accès physique aux locaux - Contrôle d'accès logique aux systèmes - Postes de travail - Liaisons réseaux externes (WAN, réseaux privés avec le CNRS) - Plan de reprise/de continuité d'activité	0

Référence	Libellé exigence	Priorité
	■ Télétravail ordinaire et télétravail exceptionnel ■ Gestion de crise	

Protection du système d'information

Référence	Libellé exigence	Priorité
SECU_005	Le titulaire dispose de dispositifs, de procédures et de moyens qu'il met en œuvre afin protéger les actifs du CNRS. Ces moyens permettent en particulier de : ■ contrer les virus et codes malveillants ■ protéger son réseau contre les intrusions. Il décrit les mesures mises en œuvre.	0

Politique de contrôle d'accès

Référence	Libellé exigence	Priorité
SECU_006	Le titulaire dispose d'une politique, de mesures et de dispositifs pour gérer le contrôle d'accès à ses locaux et à ses systèmes d'information. Cette politique concerne notamment : ■ la politique d'attributions des droits ■ les méthodes d'accès (authentification et autorisation) ■ la gestion des identifiants uniques ■ la politique de mots de passe et de gestion de l'authentification forte ■ les processus d'autorisation pour l'accès et les privilèges des utilisateurs ■ les processus de gestion des listes de personnes autorisées à participer aux activités de TMA ■ les processus de révocation des droits ■ la politique et les processus de révision des droits d'accès ■ le contenu de la charte interne utilisateur et/ou de la charte interne administrateur Le titulaire décrit les mesures en place. Il fournit en particulier sa PSSI d'entreprise.	0

Gestion des vulnérabilités

Référence	Libellé exigence	Priorité
SECU_007	Le titulaire dispose de procédures de gestion interne des vulnérabilités sur le système d'information qu'il met en œuvre pour assurer les activités de développement, de maintenance et de support. Il décrit les méthodes et outils en place pour la découverte et le suivi de la correction de ces vulnérabilités.	0

Gestion des incidents

Référence	Libellé exigence	Priorité
SECU_008	Le titulaire dispose de procédures de gestion des incidents internes de sécurité sur le système d'information qu'il met en œuvre pour assurer les activités de développement, de maintenance et de support.	0

Exigences de Sécurité concernant les personnels extérieurs

Référence	Libellé exigence	Priorité
SECU_009	Le titulaire met en œuvre des moyens de contrôle pour s'assurer du respect des exigences de sécurité du CNRS par ses sous-traitants éventuels, ainsi que des consultants ou techniciens amenés à intervenir dans le cadre des prestations. Il fournit les éléments contractuels le liant avec ses partenaires prouvant les obligations qui leur incombent dans ce domaine.	0

Travail dans les zones sécurisées

Référence	Libellé exigence	Priorité
SECU_010	Le titulaire ne doit jamais intervenir physiquement sur un site du CNRS ou géré par le CNRS sans être mandaté et surveillé par du personnel du CNRS ou mandaté par le CNRS. Il doit refuser d'assurer sa prestation, si le personnel encadrant du CNRS ou mandaté par le CNRS ne respecte pas son obligation de surveillance. Il notifie l'incident à sa direction et au RSSI de la DSI. Le délai d'exécution de la prestation est suspendu jusqu'à ce que le personnel encadrant du CNRS ait pris les mesures nécessaires à cette surveillance. Le titulaire n'est pas autorisé, sauf autorisation expresse du CNRS, à photographier, faire des enregistrements audio ou vidéo des locaux ou des équipements du CNRS. De même, il est interdit au titulaire d'introduire du matériel photographique, vidéo, audio ou d'autres matériels d'enregistrement dans les locaux du CNRS ou géré par le CNRS, sauf autorisation expresse du CNRS.	0

Stockage et échange d'informations

Référence	Libellé exigence	Priorité
SECU_011	Le titulaire met en œuvre des moyens techniques conformes aux recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) afin de protéger de toutes divulgations indésirables volontaires ou accidentelles, toutes les informations relatives au CNRS : ■ lors du stockage de celles-ci en dehors des sites physiques du CNRS, pendant et après les prestations. ■ lors des échanges avec le CNRS, quel qu'en soit le moyen (e-mail, partage de fichier, etc.). De plus le titulaire effacera les informations qu'il aura en sa possession, immédiatement et en fournissant au CNRS un quitus formel : ■ sur simple demande du CNRS ■ en fin de prestation	0

Gestion des sauvegardes

Référence	Libellé exigence	Priorité
SECU_012	Le titulaire donne au CNRS l'ensemble des éléments techniques concourant à une sauvegarde intégrale et régulière des données du CNRS qui lui sont confiées et des données nécessaires à l'exécution des prestations (plan de sauvegarde, procédures, script d'arrêt/démarrage, objets à sauvegarder, intégrité temporelle des données, etc.). La solution du titulaire doit permettre au CNRS de mettre en place des tests réguliers de restauration des sauvegardes.	0

Rétrocession des informations du CNRS

Référence	Libellé exigence	Priorité
SECU_013	Le titulaire précise les mesures et dispositifs qui garantissent le retour au CNRS et la destruction des informations du CNRS qu'il a en sa possession à l'expiration ou à la résiliation du marché. Le titulaire fournit au CNRS l'ensemble de la documentation nécessaire et une description précise des éléments techniques permettant au CNRS d'extraire les données de la solution dans un format compréhensible (<i>par exemple fichier csv et schéma relationnel des données</i>). Ces éléments doivent permettre au CNRS de reprendre ces données dans une autre solution le cas échéant.	0

5.10.3 Obligations du titulaire

Référence	Libellé exigence	Priorité
SECU_014	Le titulaire reconnaît être tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art. En particulier, il s'engage	0

	à informer le CNRS des risques d'une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d'actions correctives ou de prévention. Le titulaire est responsable du maintien en condition de sécurité des systèmes nécessaires à la réalisation des prestations jusqu'à leur échéance. Le titulaire ne peut se dégager de cette responsabilité que si, après qu'il ait informé le CNRS de failles dans la sécurité du système, de manière circonstanciée, précise et détaillée, et qu'il ait proposé une ou des solutions de nature à pallier la faille, le CNRS a choisi de ne pas mettre en œuvre ces préconisations.	
--	---	--

5.10.4 Localisation des données

Référence	Libellé exigence	Priorité
SECU_015	Les lieux d'hébergement des données du CNRS, dont les journaux, les jeux d'essai pour les environnements de développement (liste non-exhaustive), satisfont aux exigences de sécurité du donneur d'ordres (CNRS) et aux dispositions de la loi informatique et libertés en vigueur. Tout transfert de données en dehors des Etats de l'UE est soumis à avis, et autorisation préalable du CNRS, après avis de son Délégué à la Protection des Données. Le titulaire communique la liste de tous les lieux de stockage de données (site d'hébergement principal, site(s) de secours, etc.). Si la faisabilité technique de cette exigence s'avère délicate dans le cadre d'architectures distribuées, il est demandé au titulaire d'être en mesure de localiser, a posteriori, et non en permanence, le lieu de stockage des données, en particulier suite à un incident. Enfin, le titulaire doit fournir au CNRS tous les éléments attestant qu'il satisfait bien aux exigences réglementaires ci-dessus, quel que soit la localisation.	0

5.10.5 Audit

Référence	Libellé exigence	Priorité
SECU_016	Le titulaire est informé de la volonté du CNRS de conduire ou organiser des audits réguliers des systèmes d'information. Ces audits techniques et organisationnels ont pour objectifs de vérifier le respect par le titulaire de ses engagements initiaux en termes d'organisation et de moyens mis en œuvre concernant la SSI. Le CNRS peut, à tout moment, à son initiative, par ses propres équipes ou par celles de tiers désignés par lui (sélectionnés sur la liste des prestataires qualifiés en audit SSI publiée sur le site de l'ANSSI à la date de commande de l'audit https://cyber.gouv.fr/produits-services-qualifies?field_type_service_value[passi]=passi), procéder à des audits des prestations confiées au titulaire, afin de : ■ vérifier les engagements de niveaux de service, de qualité, de sécurité des prestations réalisées ; ■ vérifier la mise en application des règles d'organisation, des méthodes, des pratiques mises en œuvre pour réaliser les prestations. A cet effet, le CNRS ou son mandataire désigné met en œuvre tous les moyens qu'il juge nécessaire pour s'assurer du parfait achèvement des prestations. Ceci inclut, sans volonté d'exhaustivité : ■ la communication de documents tenus à jour par le titulaire (plans, documentations, contrats, certifications, rapports...) ; ■ l'audition orale d'équipes de maîtrise d'œuvre (techniciens, ingénieurs, responsables techniques, opérationnels, responsables de la sécurité, équipes de direction...) ; ■ la conduite de tout audit organisationnel ou technique, en boîte blanche, noire ou grise. Le CNRS s'engage à respecter un préavis raisonnable conforme aux dispositions du CCAP avant tout déclenchement d'audit. Le résultat des audits est présenté au titulaire, et conduit à la rédaction d'un plan d'action. Les actions inscrites ne conduisent pas à facturation supplémentaire de la part du titulaire si elles découlent directement d'un constat de non-conformité par rapport : ■ à ses engagements initiaux ou ■ à la réglementation en vigueur à la date de notification de l'appel d'offres.	0

	Dans tous les autres cas (évolution de la réglementation, évolution de la PSSI du CNRS, évolution d'une application modifiant son profil de risque...), le titulaire peut proposer une cotation pour la réalisation des prestations de mise en conformité. Le résultat des audits de conformité aboutit à un avis formel du CNRS ■ conforme : l'audit n'a pas révélé de dysfonctionnements majeurs, et les engagements qui ont été audités sont tenus ; ■ conforme avec réserves : des dysfonctionnements mineurs ont été relevés ou des objectifs ne sont pas remplis au niveau de l'engagement de service attendu. Dans ce cas, le titulaire propose un plan de remédiation aux dysfonctionnements à court terme : le plan est soumis au CNRS dans les huit jours après communication de l'avis formel, et l'engagement de remédiation ne peut dépasser six mois. Le titulaire démontre à ses frais que les engagements sont tenus à l'issue du plan d'action ; ■ non conforme : tout ou partie des engagements ne sont pas tenus, ou des dysfonctionnements majeurs ont été constatés. Dans ce cas, le titulaire engage des actions selon les modalités décrites supra, sous astreinte journalière de remise en conformité.	
--	--	--

5.10.6 Application des plans gouvernementaux

Référence	Libellé exigence	Priorité
SECU_017	Dans le cadre de l'application de plans gouvernementaux, les autorités françaises peuvent décider la mise en œuvre d'un ensemble de mesures spécifiques destinées à lutter contre des attaques notamment terroristes visant les systèmes d'information de l'État ou les systèmes d'information et réseaux de télécommunications. Il peut également s'agir de mesures d'entraînement à la réaction en cas d'incident. Dans le cadre du marché, le titulaire peut être concerné par ces alertes décidées au niveau gouvernemental, et s'engage à appliquer les consignes de sécurité données par le CNRS. Ces mesures sont susceptibles d'évoluer. Les modifications sont régulièrement transmises durant l'exécution du marché. Le titulaire est tenu de mettre immédiatement en œuvre les dites dispositions, quand bien même elles auraient un impact significatif sur le coût de la prestation. Dans ce dernier cas, les conséquences financières de ces dispositions sont tirées soit par voie d'avenant, soit, en cas de désaccord persistant entre le CNRS et le titulaire, par les tribunaux compétents. Sans impact significatif sur les coûts, le respect de cette exigence est réputé réalisé pro bono.	0

6 ANNEXES

6.1 DOCUMENTS JOINTS

Les documents suivants sont joints au présent CCTP. Ils sont applicables tout le long de l'accord cadre.

Le CNRS pourra faire évoluer ces documents au cours de l'accord cadre en fonction des évolutions technologiques rendues nécessaires par l'état de l'art. Ces évolutions pourront faire l'objet de commandes au titulaire le cas échéant.

Nom	Description	Type ⁵
Annexe 1 : Tableau des exigences	Ce document présente : - les exigences applicables dans le cadre des développements et de la maintenance de la solution (onglet « cadre de cohérence technique ») - les exigences applicables à l'organisation des prestations (onglet « organisation des prestations »)	[A]
Annexe 2 : CCT_Versions-cibles	Ce document présente à un instant t (ce document évolue régulièrement dans le temps et n'est donc pas figé en termes d'engagement) les versions cibles des composants applicatifs et les éléments de compatibilité navigateurs requis dans le cadre des développements et de la maintenance d'applications	[A]
Réséda ; Spécifications-Fonctionnelles-Détaillées	Ces documents décrivent les spécifications fonctionnelles détaillées du socle et des référentiels Réséda	[A]

6.2 PRÉSENTATION DÉTAILLÉE DU CNRS

6.2.1 La présidence-direction générale

Les entités suivantes sont rattachées à la présidence-direction générale :

- la direction de la communication (DIRCOM)
- le fonctionnaire de sécurité de défense (FSD)
- la délégation à la protection des données (DPD)
- la direction de l'audit interne (DAI)
- la mission pour la place des femmes (MPDF)

6.2.1.1 *Direction de la communication (DIRCOM)*

La **DIRCOM** élabore et met en œuvre la stratégie de communication du CNRS. Elle développe la communication scientifique et institutionnelle vers le grand public, mettant en valeur les résultats scientifiques et les talents présents au sein de l'organisme avec l'objectif d'accroître son attractivité et de valoriser son image.

6.2.1.2 *Mission pour la place des femmes (MPDF)*

La **MPDF** au CNRS agit comme un observatoire chargé d'impulser, de conseiller et d'évaluer la prise en compte du genre dans la politique globale de l'établissement. La mission travaille en étroite collaboration avec les structures du CNRS. Son action vise à développer l'égalité professionnelle entre femmes et hommes au sein du CNRS, à promouvoir la transversalité de l'approche « genre » en recherche, et à valoriser les carrières scientifiques et techniques auprès des jeunes, notamment les jeunes filles. Elle compte des partenaires variés, en France comme à l'étranger.

Des informations plus complètes sont disponibles à l'adresse suivante : <https://mpdf.cnrs.fr/>.

⁵ [A] = document applicable
[R] = document de référence (cf. dans le glossaire au § 6.4.2)

6.2.1.3 *Délégation à la protection des données (DPD)*

Conformément au règlement européen sur la protection des données personnelles, la **DPD** est chargée de la conformité en matière de protection des données au sein du CNRS. Ses missions sont principalement les suivantes :

- Informer et conseiller l'organisme et les responsables de traitement sur les obligations en matière de protection des données ;
- Contrôler le respect de la réglementation sur la protection des données et la bonne application des procédures, méthodes et consignes relatives à ce domaine ;
- Dispenser des conseils pour ce qui concerne l'analyse d'impact relative à la protection des données et vérifier son exécution ;
- Coopérer avec la Commission nationale de l'informatique et des libertés (CNIL), autorité de contrôle, et être le point de contact pour toute question relative aux traitements et à la protection de données ;
- S'assurer de la tenue de la documentation relative aux traitements.

6.2.2 La direction générale déléguée à la science (DGD-S)

La **DGD-S** conduit, aux côtés du président-directeur général, la politique scientifique de l'établissement. Elle coordonne l'action des dix instituts du CNRS, veille à promouvoir l'interdisciplinarité et organise les partenariats avec les divers acteurs de la recherche, à l'échelle régionale, nationale, européenne ou internationale.

Pour remplir ses missions, la DGD-S s'appuie sur :

- les dix instituts et les unités de recherche qui leur sont rattachées,
- trois directions fonctionnelles :
 - la direction Europe et international (DEI),
 - la direction des données ouvertes de la recherche (DDOR),
 - la direction d'appui aux partenariats publics (DAPP),
- la mission pour les initiatives transverses et interdisciplinaires (MITI),
- la mission pour l'expertise scientifique (MPES),
- la mission programmes nationaux (MiPN)
- le Comité Très grandes infrastructures de recherche (TGIR),
- le secrétariat général du Comité national (SGCN).

Des informations plus complètes sont disponibles à l'adresse suivante : <https://www.cnrs.fr/fr/le-cnrs/organisation>.

6.2.2.1 *Les instituts*

Les **instituts** sont les structures de mise en œuvre de la politique scientifique de l'établissement. Les directeurs des instituts participent à l'élaboration de la politique scientifique du CNRS et définissent les modalités de son application.

Chaque institut anime et coordonne l'action d'un ensemble cohérent d'activités de recherche relevant de plusieurs disciplines. Des programmes interdisciplinaires de recherche intéressant plusieurs instituts peuvent être décidés par le président après avis du conseil scientifique et approbation du conseil d'administration.

- [CNRS Biologie](#) : il a pour mission de développer et coordonner des recherches en biologie qui visent à décrypter la complexité du vivant, des atomes aux biomolécules, de la cellule à l'organisme entier et aux populations.
- [CNRS Chimie](#) : il a pour mission de développer et de coordonner les recherches concernant l'élaboration de nouveaux composés, la compréhension de la réactivité chimique, l'élucidation toujours plus fine et la prédiction des relations entre la structure des composés au niveau atomique et leurs propriétés..
- [CNRS Ecologie & Environnement](#) : il a pour mission de développer et de coordonner les recherches poursuivies dans les domaines de l'écologie et de l'environnement, incluant la biodiversité et les relations hommes-milieus.
- [CNRS Ingénierie](#) : il a pour mission d'assurer le continuum entre recherche fondamentale, ingénierie et technologie en privilégiant l'approche "système" à partir du développement des disciplines au cœur de l'institut.
- [CNRS Mathématiques](#) : il a pour mission de développer et de coordonner les recherches dans les différentes branches des mathématiques, allant des aspects fondamentaux aux applications. Il contribue aussi à la structuration de la communauté mathématique française et à son insertion dans la communauté internationale.

- [CNRS Nucléaire & Particules](#) : il a pour mission de promouvoir et fédérer les activités de recherche poursuivies dans les domaines de la physique nucléaire, physique des particules et astroparticules.
- [CNRS Physique](#) : il a pour mission de développer et de coordonner les recherches dans le domaine de la physique avec deux motivations principales : le désir de comprendre le monde et la volonté de répondre aux enjeux actuels de notre société.
- [CNRS Sciences humaines & sociales](#) : il a pour mission de développer les recherches sur l'homme, aussi bien comme producteur de langages ou de savoirs que comme acteur économique, social ou politique.
- [CNRS Sciences informatiques](#) : il a pour mission de développer des recherches dans les domaines des sciences informatiques et du numérique. L'un de ses principaux objectifs est de les positionner, avec les sciences de l'information, au cœur des enjeux pluri et interdisciplinaires en s'appuyant sur un partenariat avec les autres instituts du CNRS et plus particulièrement CNRS Ingénierie.
- [CNRS Terre & Univers](#) : il a pour mission d'élaborer, développer et coordonner les recherches d'ampleur nationale et internationale en astronomie, sciences de la Terre, de l'océan et de l'espace.

6.2.2.2 *La direction Europe et internationale (DEI)*

La **DEI** coordonne l'ensemble des opérations conduites par le CNRS pour contribuer à structurer et consolider l'espace de la recherche dans l'Union Européenne.

Elle met en place les outils nécessaires au soutien de partenariats bilatéraux, européens ou internationaux, s'inscrivant dans le cadre de la politique du CNRS en matière de coopération internationale.

Elle apporte son appui aux unités de recherche qui s'engagent dans des actions structurantes avec des partenaires étrangers, y compris des organismes et universités étrangers.

Des informations plus complètes sont disponibles sur le site Web de la DEI à l'adresse suivante : <https://international.cnrs.fr/>

6.2.2.3 *La direction d'appui aux partenariats publics (DAPP)*

La **DAPP** porte et exprime la politique partenariale du CNRS avec les institutions publiques et les collectivités territoriale. A ce titre, elle contribue au déploiement des stratégies scientifiques du CNRS sur les différents sites, en lien avec les établissements d'enseignement supérieur et par ailleurs coordonne les opérations par lesquelles le CNRS, organisme national, contribue avec les acteurs locaux au développement et au rayonnement de grands pôles scientifiques de site..

Elle pilote l'élaboration et le suivi des conventions et accords entre le CNRS d'une part, les universités et les écoles, les collectivités territoriales, les organismes et autres acteurs nationaux de la recherche d'autre part.

Elle conçoit des éléments de l'infrastructure de données – administration de base de données, production d'indicateurs, assistance à maîtrise d'ouvrage d'applications du système d'information – utiles à l'élaboration de la politique scientifique de l'organisme.

Pour réaliser ses missions, la DAPP déploie son action en s'appuyant sur 5 services :

- Le service « Partenariats publics territoriaux » contribue à la définition et à la mise en œuvre de politiques différenciées en lien avec les directeurs et directrices scientifiques référents (DSR), les délégués et déléguées régionaux (DR) et leurs adjoints respectifs. Il coordonne les actions du CNRS qui concourent au développement et au rayonnement des sites. Il pilote l'élaboration et le suivi des conventions conclues entre le CNRS d'une part, et les universités, écoles ou collectivités territoriales d'autre part. ;
- Le service « Institutions nationales » assure le suivi des relations entre le CNRS et les organismes nationaux de recherche et les ministères. En particulier, il pilote l'élaboration et le suivi des conventions conclues entre le CNRS et ces institutions ;
- Le service « Structures et outils d'animation » coordonne l'ensemble du processus administratif de création et d'évolution des structures entre le CNRS et les établissements de l'ESR, ainsi que la création des outils d'animation. Il pilote la campagne annuelle d'accueils en délégation ;
- Le service « Données et Indicateurs » centralise les données décrivant les structures de recherche et d'appui à la recherche, administre des bases de données, réalise des études et produit des indicateurs institutionnels. Il concourt également à la conception de la plateforme d'aide à la décision ;
- Le service « Maîtrise d'ouvrage de systèmes d'information » est en charge de la maîtrise d'ouvrage et de l'administration fonctionnelle de plusieurs référentiels transverses à l'organisme et d'applications du système d'information relevant des activités de la DGDS ou dédiées à des processus métier. Il a la charge de la définition de modules de plateformes d'aide à la décision et leur intégration dans le système d'information de l'organisme.

6.2.2.4 *Le Secrétariat général du Comité national (SGCN)*

Le **SGCN** assiste l'ensemble des instances et assure l'évolution des processus relevant de la mise en œuvre de leurs missions.

Par son soutien aux travaux du comité national (conseils, prospective, évaluation des chercheurs), le SGCN garantit le fonctionnement des instances et en accompagne les évolutions en lien avec la direction du CNRS, les instituts et les autres acteurs de la recherche scientifique.

Il a pour fonctions de :

- organiser les processus relatifs au conseil, à la prospective et à l'évaluation individuelle des chercheurs dans le respect de la réglementation,
- assurer le suivi des instances,
- assurer une veille juridique, réglementaire,
- diffuser les travaux du comité national,
- assurer la maîtrise d'ouvrage des systèmes d'information afférent aux processus.

Des informations plus complètes sont disponibles sur le site Web du SGCN à l'adresse suivante : <http://www.cnrs.fr/comitenational/sgcn/accueil.htm>

6.2.3 *La direction générale déléguée aux ressources (DGD-R)*

La **DGD-R** conduit, aux côtés du président, la politique administrative et financière de l'établissement. Elle a en charge le développement des ressources humaines et des activités de soutien à la recherche. Dans ce cadre, et en relation étroite avec la DGD-S, elle s'appuie sur les compétences des instituts du CNRS.

Pour remplir ses missions, la DGD-R s'appuie sur :

- dix-sept délégations régionales,
- six directions fonctionnelles :
 - la direction des ressources humaines (DRH)
 - la direction de la stratégie financière, de l'immobilier et de la modernisation (DSFIM)
 - la direction des comptes et de l'information financière (DCIF)
 - la direction des affaires juridiques (DAJ)
 - la direction des systèmes d'information (DSI)
 - la direction de la sûreté (DIRSU)
- une structure transversale : la mission transverse d'appui au pilotage (MTAP)
- un pôle santé et sécurité au travail composé de :
 - la coordination nationale de médecine de prévention (CNMP)
 - le coordination nationale de prévention et de sécurité (CNPS).

Des informations plus complètes sont disponibles à l'adresse suivante : <https://www.cnrs.fr/fr/le-cnrs/organisation>.

6.2.3.1 *La direction des ressources humaines (DRH)*

La **DRH** est en charge de la préparation et de la mise en œuvre des orientations stratégiques dans son domaine ainsi que du dialogue social.

Elle assure, en relation étroite avec la DSFIM, la programmation, la préparation budgétaire et le suivi de la masse salariale et des emplois. Elle est garante de l'accompagnement et de la valorisation des ressources humaines, ainsi que de la gestion statutaire des agents. Dans son domaine, elle assure un rôle de conseil et d'expertise juridique, et elle est en charge de la maîtrise d'ouvrage des systèmes d'information, ainsi que de l'administration des données.

La politique des ressources humaines du CNRS s'articule autour de plusieurs axes :

- Recruter des compétences variées ;
- Garantir l'évolution professionnelle tout au long du parcours ;
- Accompagner les agents dans leur vie professionnelle.
-

La Direction est divisée en 3 pôles d'action, dans lesquels se répartissent 14 services :

- L'équipe de Direction
- La Direction déléguée aux cadres supérieurs (DDCS)
- Carrières et développement professionnel :
 - le Service du développement professionnel Chercheurs (SDPC)
 - le Service du développement professionnel Ingénieurs et Techniciens (SDPIT)
 - le Service central des concours (SCC)
 - le Service formation et itinéraires professionnels (SFIP)
- Pilotage et expertise :
 - le Service des effectifs et du contrôle de gestion (SECG)
 - le Service Observatoire des métiers et de l'Emploi Scientifique (OMES)
 - le Service conseil et expertise juridique (SCEJ)
 - le Service systèmes et traitement de l'information (SSTI)
 - le Service communication et marketing (SCOM)
- le Service administratif et financier (SAF) Politique et relations sociales :
 - le Service responsabilité sociale de l'entreprise (SRSE)
 - le Service Pensions et Accidents du Travail (SPAT)
 - la **Erreur ! Source du renvoi introuvable.**
 - La Mission Relations Sociales (MRS)

Les responsabilités directes de gestion s'exercent au sein des services des ressources humaines (SRH) des délégations régionales. Ces services assurent la gestion administrative des personnels, la formation, le conseil en RH et garantissent un service social aux agents.

6.2.3.2 *La direction de la stratégie financière, de l'immobilier et de la modernisation (DSFIM)*

La **DSFIM** est en charge de la prospective et de la mise en œuvre des orientations stratégiques dans son domaine. Elle assure la programmation, la préparation et l'exécution du budget, et fait le lien entre l'allocation des ressources et la réalisation des objectifs. Elle est chargée de l'optimisation des ressources, de la modernisation de la gestion, et de la mise en œuvre de la stratégie patrimoniale.

6.2.3.2.1 *La direction déléguée aux achats et à l'innovation (DDAI)*

La **DDAI** a un rôle de pilotage de la politique achat du CNRS, et de passation et de suivi des marchés nationaux.

6.2.3.2.2 *Le service de la Politique Immobilière (SPI)*

Le **SPI** définit et met en œuvre, en liaison avec les instituts et les délégations régionales, la politique immobilière de l'établissement. Il coordonne l'action des responsables de l'immobilier dans les délégations régionales du CNRS.

Il a en charge la préparation des décisions du Président sur les opérations d'investissement et en assure le suivi de l'exécution, notamment budgétaire. Il arrête également la stratégie de l'établissement en matière de maintenance et d'entretien des bâtiments.

Il assure la maîtrise d'ouvrage d'opérations d'envergure nationale.

6.2.3.3 *La direction des comptes et de l'information financière (DCIF)*

La **DCIF** est garante de la régularité des opérations comptables et de la cohérence de l'ensemble des informations financières et comptables.

Elle assure le suivi et l'enregistrement des actes de gestion liés à la mise en œuvre des crédits et à l'exécution du budget. Elle garantit l'exhaustivité et la qualité des données. Elle restitue l'information financière selon les besoins et les calendriers des services utilisateurs, de la direction de l'établissement ou des tutelles.

Dans son domaine, elle est en charge de la maîtrise d'ouvrage des systèmes d'information ainsi que de l'administration des données.

Des informations plus complètes sont disponibles sur le site Web de la DCIF à l'adresse suivante : <https://www.cnrs.fr/fr/dcif>

6.2.3.4 *La direction des affaires juridiques (DAJ)*

La **DAJ** assure une mission de conseil, d'expertise, de veille juridique et de défense de l'établissement.

Elle assure le secrétariat du conseil d'administration (CA) du CNRS et est chargée de l'organisation des processus électoraux concernant l'établissement.

Ses activités s'articulent autour de **6 pôles** et **1 secrétariat général** :

- Pôle Accords Propriété Intellectuelle Valorisation (APIV)
- Pôle Ingénierie des Structures (IdS)
- Pôle Droit Public Economique et Règlementation (DPER)
- Pôle Responsabilité pénale et Maîtrise des Risques (RMR)
- Pôle Pilotage et Ressources Juridiques (PRJ)
- Pôle National de Conservation des Données et Documents (PNC2D)
- Secrétariat général pour les Elections et le Conseil d'Administration (SECA)

La direction anime également le **réseau des juristes du CNRS** (réseau e-loi).

6.2.3.5 *La direction des systèmes d'information (DSI)*

La **DSI** définit et met en œuvre les systèmes d'information de gestion et de pilotage des activités de l'établissement, en adéquation avec les orientations stratégiques et métiers de l'établissement (RH, finance, décisionnel, formation, référentiels, valorisation, missions...).

Elle gère également les outils mis en commun avec les partenaires du CNRS tels que l'Amue et les universités, ainsi que la sécurité des systèmes d'information (outils et services, animation du réseau des correspondants sécurité...).

Enfin, la DSI met à disposition des laboratoires une offre de services numériques (ODS) destinée à simplifier, soutenir et sécuriser leur quotidien (travail collaboratif, mobilité, services cloud, sauvegarde des données, exploitation sécurisée de sites internet...).

La DSI comprend :

- **La Direction** : le directeur de la DSI est assisté d'une directrice adjointe et d'une directrice adjointe administrative.
- **Le Secrétariat Général** est chargé des aspects administratifs de la DSI. Il gère les ressources humaines, le budget, le contrôle de gestion, la logistique et les achats.
- **Le département SI Finance** assure le maintien en conditions opérationnelles et la mise en œuvre des évolutions fonctionnelles et techniques de BFC (budget, finance, comptabilité) et de l'Infocentre métier Finance, SI financiers du CNRS.
- **Le département SI Laboratoires et soutien à la recherche** assure le maintien en conditions opérationnelles et la mise en œuvre des évolutions fonctionnelles et techniques des applications à destination des laboratoires et des services centraux notamment pour la gestion des achats, la gestion des missions, le dialogue de gestion, la gestion du patrimoine immobilier, la gestion de la valorisation et les appels à projets. Il assure également la conduite de projets de développement d'applications dans son périmètre d'activité.
- **Le département SI Ressources humaines et paie** assure le maintien en conditions opérationnelles et la mise en œuvre des évolutions fonctionnelles et techniques de Sirhus (Système d'Information Ressources Humaines des Unités et Services du CNRS), de l'infocentre métier RH et des convertisseurs équivalent temps plein travaillé (ETPT).
- **Le département Solutions applicatives métiers et décisionnel** assure le maintien en conditions opérationnelles et la mise en œuvre des évolutions fonctionnelles et techniques des applications ressources humaines, santé, prévention, sécurité et décisionnel. Il réalise également la conduite de projets de développement d'applications dans son périmètre d'activité.
- **Le département Cybersécurité** met en œuvre la politique de sécurité des SI du CNRS pour l'ensemble des SI qui sont sous la responsabilité de la DSI. Il pilote et met en œuvre les démarches d'homologation de son périmètre. Il détermine les risques, objectifs et mesures de sécurité à intégrer dans les applications, services, outils, architectures et infrastructures. Il contrôle les mises en œuvre techniques et organisationnelles. Il définit, met en place et maintient les services de confiance numériques du CNRS. Il gère les incidents de sécurité de son périmètre. Il participe et collabore aux travaux de la CNSSI et de son centre de cyberdéfense.
- **Le département Plateforme des référentiels et de dématérialisation** met en œuvre les principaux référentiels structurants du SI. Il est chargé de les maintenir en conditions opérationnelles (plateforme GDR – Gestion des Données de Référence). Il est aussi chargé de la mise en œuvre des plateformes de dématérialisation des

documents, de préservation et de conservation de ces derniers (services de GED – Gestion Electronique de Documents et de SAE – Système d'Archivage Electronique).

- **Le département Architecture et assistance applicatives** met en place et maintient les annuaires et outils de gestion d'habilitations, fournit de l'assistance en termes d'expertise développement et architecture applicative. Il met en place et maintient les outils d'intégration des données et assure l'assistance utilisateurs.
- **Le département Infrastructures SI** est chargé de spécifier, mettre en œuvre, opérer et maintenir les infrastructures (notamment réseaux, systèmes, bases de données) du SI du CNRS. Il accompagne toutes les activités portées par la DSI dans le domaine des infrastructures et de l'exploitation technique.
- **Le département Sites web, communication, accompagnement projet** conçoit et met en œuvre les outils pour la communication et le travail collaboratif au sein du CNRS (intranet, portails, espaces collaboratifs, sites web). Il accompagne le déroulement des projets SI au niveau urbanisation (études pour l'intégration de nouveaux besoins), qualité-méthodes et ergonomie des technologies interface homme machine (IHM). Enfin, il a en charge la communication interne et externe de la DSI.

La DSI est implantée sur deux sites Toulouse-Labège (31) et Meudon (92).

Des informations plus complètes sont disponibles à l'adresse suivante : <https://www.cnrs.fr/fr/dsi>

6.2.3.6 *Direction de la sûreté (DIRSU)*

La **DIRSU** participe à la définition et à la mise en œuvre de la politique de sûreté et de sécurité afin de protéger les agents et le patrimoine de l'établissement.

Elle met en œuvre les processus de préservation et de maîtrise des risques d'atteintes volontaires aux personnes et au patrimoine matériel et immatériel au sein du CNRS.

La direction de la sûreté participe à la définition et à la mise en œuvre de la protection du potentiel scientifique et technique de la Nation au sein du CNRS.

Ses missions s'articulent étroitement avec les fonctions exercées par le Fonctionnaire de sécurité de défense (FSD). Le directeur de la sûreté est également Fonctionnaire de sécurité de défense du CNRS.

La direction comprend :

- Le responsable de la sécurité des systèmes d'information du CNRS (RSSIC) en tant que chargé de mission auprès du directeur de la sûreté pour le domaine de la sécurité de l'information et de la sécurité des réseaux et systèmes d'information.
- Le conseiller national à la sécurité des transports de marchandises dangereuses (TMD) du CNRS chargé de recommander à toutes les entités du CNRS et, le cas échéant, à ses partenaires les actions et les procédures applicables aux transports de matières dangereuses. Il assure à ce titre une veille des réglementations internationales et nationales.
- Le conseiller pour l'intelligence économique qui est en charge de la mise en œuvre de la politique d'intelligence économique au CNRS dans le cadre de la politique nationale d'intelligence économique en lien avec les services compétents de l'Etat.

6.2.3.7 *La mission transverse d'appui au pilotage (MTAP)*

La **MTAP** mène des projets et actions dépassant les périmètres des directions métiers et services relevant des directions générales déléguées pour apporter un appui au pilotage du CNRS, faciliter le quotidien des unités et des fonctions supports et fluidifier les interactions des réseaux de la Direction générale déléguée aux ressources, en délégations régionales et en instituts.

Elle coordonne l'ensemble des relations avec les délégations régionales. Elle garantit le lien entre les entités de la DGD-R, et celles de la DGD-S, dont notamment la coordination avec les instituts.

Des informations plus complètes sont disponibles à l'adresse suivante : <https://www.cnrs.fr/fr/mtap>

6.2.3.8 *Le Pôle Santé et Sécurité au Travail (PSST)*

Le **PSST** du CNRS est composé de la coordination nationale de prévention et de sécurité (CNPS) et de la coordination nationale de médecine de prévention (CNMP).

Il participe à la politique de prévention des risques professionnels en vue de préserver la santé, la sécurité des personnes et des biens ainsi que de veiller à la protection de l'environnement.

Il conseille la direction et les délégués régionaux, anime et coordonne les personnels des services concernés et représente le CNRS au sein des instances internes et externes.

6.2.3.8.1 La Coordination nationale de médecine de prévention (CNMP)

La **CNMP** :

- conseille la direction sur l'organisation de la médecine de prévention au CNRS ;
- intervient auprès de la direction pour la mise en œuvre de la politique de santé au travail de l'établissement ;
- anime, en liaison avec les délégués régionaux, le réseau des personnels de santé ;
- définit et veille à la mise en œuvre des actions de formations en appui de la politique de santé au travail.

Des informations plus complètes sont disponibles sur le site Web du CNMP à l'adresse suivante : <https://www.dgdr.cnrs.fr/SST/CNMP/>

6.2.3.8.2 La Coordination nationale de prévention et de sécurité (CNPS)

L'activité de conseil et de coordination au niveau national pour toutes les questions concernant l'hygiène, la sécurité des personnes et des biens et la protection de l'environnement est confiée à la **CNPS** placée au sein de la DGD-R.

Des informations plus complètes sont disponibles sur le site Web du CNPS à l'adresse suivante : <https://www.dgdr.cnrs.fr/SST/CNPS/>

6.2.4 La coordination nationale de la sécurité des systèmes d'information (CNSSI)

La **CNSSI** a pour mission le pilotage de la mise en œuvre de la politique de sécurité des systèmes d'information du CNRS (PSSI-C). Elle anime la chaîne fonctionnelle de la sécurité des systèmes d'information de l'établissement. Elle coordonne les relations internes et externes, dans son domaine, avec les partenaires de l'établissement. Elle comprend le centre de cybersécurité du CNRS, dédié à la détection et la gestion des incidents de cybersécurité dans son périmètre de gestion.

6.2.5 La direction générale déléguée à l'innovation (DGD-I)

La **DGD-I** conduit, aux côtés du président-directeur général, la politique de transfert des résultats de la recherche, de leur valorisation et des interactions avec le monde socio-économique.

Elle définit les lignes directrices contractuelles et d'organisation afin d'accélérer les processus de transfert et de valorisation. Elle veille pour cela à construire des relations de confiance efficaces avec les partenaires académiques des unités de recherche et à amplifier les relations avec les acteurs socio-économiques. Elle coordonne la politique de l'établissement en ce qui concerne les relations avec les industriels et la création d'entreprises.

Elle pilote le suivi et le contrôle de l'accomplissement des missions confiées par le CNRS à CNRS-Innovation et aux sociétés d'accélération du transfert de technologies (SATT).

Elle a en charge le suivi et la maîtrise des coûts budgétaires associés à l'exercice des missions de transfert et de valorisation.

Pour remplir ses missions, la DGD-I s'appuie sur :

- la Direction des relations avec les entreprises (DRE),
- CNRS Innovation,
- l'ensemble des entités de la DGD-S et de la DGD-R impliquées dans les actions de valorisation de l'établissement et de la filiale CNRS Innovation.

Des informations plus complètes sont disponibles à l'adresse suivante : <https://www.cnrs.fr/fr/le-cnrs/organisation>.

6.2.5.1 La direction des relations avec les entreprises (DRE)

La **DRE** met en œuvre la stratégie du CNRS en matière de valorisation de la recherche et du transfert de technologie et organise, avec les instituts et les délégations régionales, l'interface entre les unités de recherche et les entreprises.

Elle assure le pilotage des actions de type prématuration en lien avec les Instituts.

Elle soutient les partenariats avec les grands groupes industriels sur la base de projets scientifiques communs et négocie les accords-cadres.

Elle assure le lien opérationnel avec les SATT, les instituts de recherche technologiques (IRT) et les instituts pour la transition énergétique (ITE), et les pôles de compétitivité.

6.2.5.2 CNRS Innovation

CNRS Innovation a pour mission de protéger des résultats de laboratoires du CNRS par des titres de propriété intellectuelle, de gérer le portefeuille de brevets et logiciels ainsi constitué, et d'en assurer le transfert vers le monde socio-économique. Elle porte le programme de prématuration du CNRS ainsi que son programme d'accompagnement à la création de start-up (RISE).

Des informations plus complètes sont disponibles à l'adresse suivante : <https://www.cnrsinnovation.com/>

6.2.6 Les délégations régionales (DR)

Les dix-sept **DR** du CNRS sont les interlocutrices de premier plan des partenaires de l'organisme sur le terrain. Elles ont un rôle de gestion et d'accompagnement de proximité des laboratoires répartis sur le territoire. Elles apportent notamment leur aide pour le montage de projets industriels et de programmes européens.

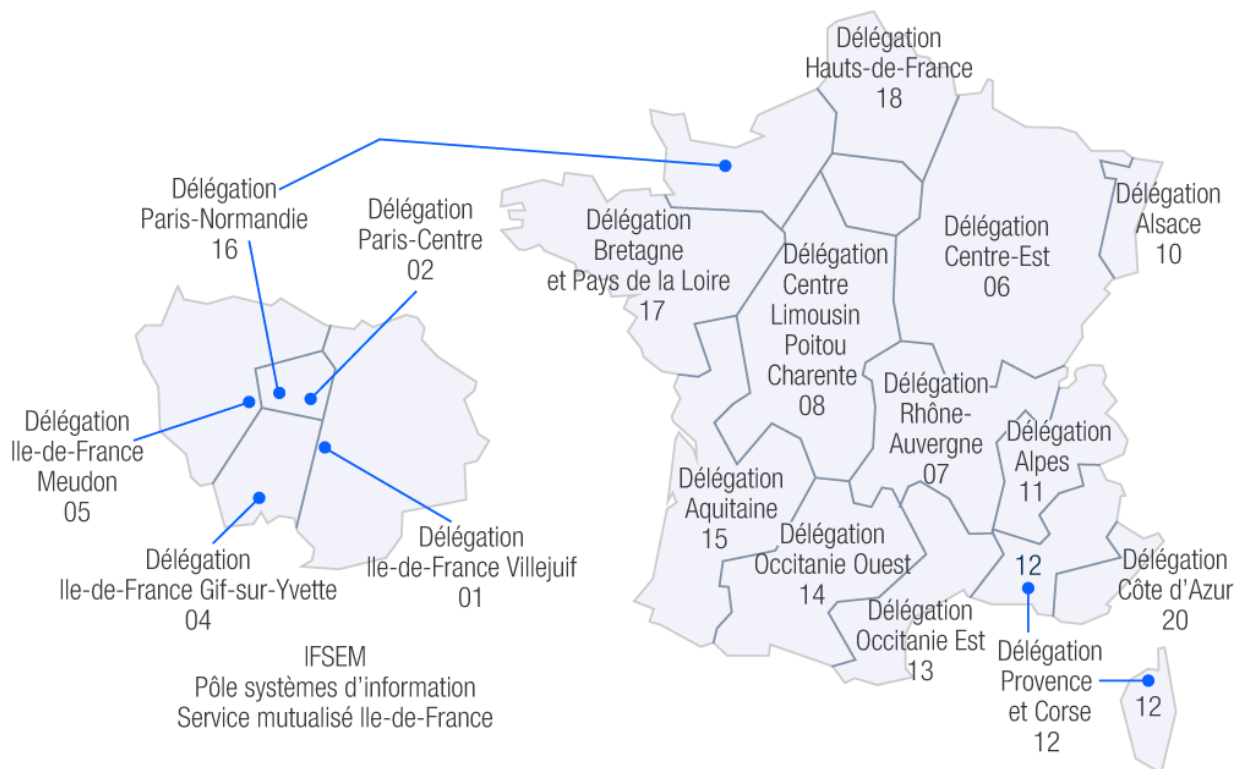


Figure 6 : Le CNRS en région

Des informations plus complètes sont disponibles à l'adresse suivante : <https://www.cnrs.fr/fr/delegations-regionales-du-cnrs>

6.2.7 Les unités (laboratoires)

Le CNRS compte environ 1100 laboratoires répartis sur l'ensemble du territoire français. Ce sont en très grande majorité des unités mixtes de recherche (UMR) associées à une université, une école supérieure ou un autre organisme de recherche. À ces laboratoires s'ajoutent 80 laboratoires de recherche internationaux, un nombre en progression constante.

Les **laboratoires** du CNRS sont les « briques de base » de l'établissement. Leurs équipes, formées de chercheurs, d'ingénieurs et de techniciens, sont à l'origine de la production et de la transmission des connaissances. Les laboratoires sont pour la plupart des unités mixtes de recherche, associant des partenaires du monde académique (universités, écoles et autres organismes de recherche) et industriel.

6.3 RÉFÉRENCE DES EXIGENCES

Référence	Groupe d'exigence
ACC	Accessibilité
AUTH	Authentification
BDD	Base de données
DEV	Développement
DOC	Stockage des documents
ECH	Echange de données
ENV	Environnements
ERG	Ergonomie
HAB	Habilitations
INF	Infrastructure
QUA	Qualité
REGL	Conformité réglementaire
SECU	Mesure et clauses de sécurité
SSI	Sécurité des systèmes d'information
URB	Urbanisation

6.4 ABRÉVIATIONS ET GLOSSAIRE

6.4.1 Abréviations

Le tableau suivant présente la liste des abréviations utilisées dans ce document.

Sigle	Description
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	Application Programming Interface (interface de programmation applicative)
BAPI	Business Application Programming Interface
BDD	Base De Données
CAS	Central Authentication Service
CCAP	Cahier des Clauses Administratives
CCT	Cadre de Cohérence Technique
CCTP	Cahier des Clauses Techniques Particulières
CF	Comptabilité Finance
CNIL	Commission nationale de l'informatique et des libertés
CNMP	Coordination Nationale de Médecine de Prévention
CNPS	Coordination Nationale de Prévention et de Sécurité
CNRS	Centre National de la Recherche Scientifique
CSS	Cascading Style Sheets
CSV	Comma-separated values
DAJ	Direction des Affaires Juridiques
DAO	Data Access Object (objet d'accès aux données)
DAPP	Direction d'Appui aux Partenariats Publics
DCIF	Direction des Comptes et de l'Information Financière

Sigle	Description
DCP	Donnée à caractère personnel
DDAI	Direction Déléguée aux Achats et à l'Innovation
DERCI	Direction Europe de la Recherche et Coopération Internationale
DEV	plateforme de DEveloppement
DRE	Direction des Relations avec les Entreprises
DGD-I	Direction Générale Déléguée à l'Innovation
DGD-R	Direction Générale Déléguée aux Ressources
DGD-S	Direction Générale Déléguée à la Science
DINUM	Direction Interministérielle du Numérique
DNS	Domain Name System (système de noms de domaine)
DR	Délégation Régionale
DRH	Direction des Ressources Humaines
DSFIM	Direction de la Stratégie Financière, de l'Immobilier et de la Modernisation
DSI	Direction des Systèmes d'Information
DU	Directeur d'Unité
EAI/ESB	Enterprise Application Integration (intégration d'applications d'entreprise) / Enterprise Service Bus
EPST	Etablissement Public à caractère Scientifique et Technique
ETPT	Equivalent Temps Plein Travaillé
FOR	plate-forme de FORmation
FSD	Fonctionnaire de Sécurité de Défense
FTP	File Transfer Protocol (protocole de transfert de fichiers)
GED	Gestion Electronique de Documents
GIP	Groupement d'Intérêt Public
HTML	HyperText Markup Language (langage de balisage d'hypertexte)
HTTP	HyperText Transfer Protocol (protocole de transfert hypertexte)
HTTPS	HyperText Transfer Protocol Secure (protocole de transfert hypertexte sécurisé)
IdP	Identity Provider (fournisseur d'identité)
IHM	Interface Homme Machine
IN2P3	Institut national de physique nucléaire et physique des particules
INC	Institut de chimie
INEE	Institut écologie et environnement
INP	Institut de physique
INS2I	Institut des sciences de l'information et de leurs interactions
INSB	Institut des sciences biologiques
INSHS	Institut des sciences humaines et sociales
INSIS	Institut des sciences de l'ingénierie et des systèmes
INSMI	Institut des sciences mathématiques et de leurs interactions
INSU	Institut national des sciences de l'univers
IPsec	Internet Protocol Security (protocole de sécurité internet)
IPv4	Internet Protocol version 4 (protocole internet version 4)
J2EE	Java 2 Enterprise Edition

Sigle	Description
JMS	Java Message Service
JSON	JavaScript Object Notation (format de données textuelles dérivé de la notation des objets du langage JavaScript)
JSR	Java Specification Request
LAN	Local Architecture Network (réseau local)
LDAP	Lightweight Directory Access Protocol (protocole d'accès aux annuaires)
MESRI	Ministère de l'Enseignement Supérieur et de la Recherche et de l'Innovation
MCO	Maintien en Condition Opérationnelle
MDM	Master Data Management (gestion des données de référence)
MOA	Maîtrise d'ouvrage
MOE	Maîtrise d'œuvre
MPR	Mission Pilotage et Relations avec les délégations régionales et les instituts
NAT	Network Address Translation (mécanisme de translation d'adresses)
NTP	Network Time Protocol (protocole d'heure réseau)
OS	Operating System
PGI	Progiciel de Gestion Intégré
PGSI	Politique Générale de Sécurité de l'Information
PAQ	Plan Assurance Qualité
PAS	Plan Assurance Sécurité
PSSI	Politique de Sécurité des Systèmes d'Information
PSST	Pôle Santé et Sécurité au Travail
REC	plate-forme de RECette
RENATER	REseau NAional de télécommunications pour la Technologie, l'Enseignement et la Recherche
REST	REpresentational State Transfer
RFC	Requests For Comments (demande de commentaires)
RGAA	Référentiel général d'Accessibilité pour les Administrations
RGI	Référentiel Général d'Interopérabilité
RGPD	Règlement Général sur la Protection des Données
RGS	Référentiel Général de Sécurité
RH	Ressources Humaines
RSSIC	Responsable de la Sécurité des Systèmes d'Information du CNRS
SAE	Service d'archivage électronique
SAML	Security Assertion Markup Language (langage de balisage d'informations d'authentification)
SAN	Storage Area Network (réseau de stockage)
SGBD	Système de Gestion de Base de Données
SGCN	Secrétariat Général du Comité national
SHA	Secure Hash Algorithm
SI	Système d'Information
SIRH	Système d'Information des Ressources Humaines
SMTP	Simple Mail Transfer Protocol (protocole simple de transfert de courrier)
SNMP	Simple Network Management Protocol (protocole simple de gestion de réseau)

Sigle	Description
SP	Service Provider (fournisseur de services)
SQL	Structured Query Language (langage de requête structurée)
SSH	Secure SHell
SSI	Sécurité des Systèmes d'Information
SSI	Service des Systèmes d'Information
SSL	Secure Socket Layer
SSO	Single Sign-On (authentification unique)
SPV	Service du Partenariat et de la Valorisation
TLS	Transport Layer Security
VLAN	Virtual Local Area Network (réseau local virtuel)
VPN	Virtual Private Network (réseau privé virtuel)
W3C	World Wide Web Consortium
WCAG	Web Content Accessibility Guidelines (règles pour l'accessibilité des contenus Web)
XML	eXtensible Markup Language (langage de balisage extensible)
XSS	Cross Site Scripting

6.4.2 Glossaire

Le tableau suivant présente le glossaire des termes utilisés dans ce document.

Terme	Description
Authentification multifacteur	Méthode d'authentification dans laquelle l'utilisateur doit fournir au minimum deux facteurs de vérification pour accéder à une ressource de type application, compte en ligne ou VPN.
Document applicable	Document devant être obligatoirement appliqué par le titulaire
Document de référence	Document pouvant être utilement consulté par le titulaire
EAI/ESB	Plateforme d'intermédiation des flux de données
Flux	Tout échange de données ou d'information entre deux briques applicatives (y compris services d'intermédiation), quelle que soit la modalité et forme de cet échange. Un flux peut être entièrement manuel, ou peut faire appel à des services web, ou peut passer par l'EAI/ESB, ou
LDAP	Protocole permettant l'interrogation et la modification des services d'annuaire.
REST	Style d'architecture d'échange de données autour de services web basés sur le protocole HTTP
Shibboleth	Mécanisme de propagation d'identités, développé par le consortium Internet2, qui regroupe 207 universités et centres de recherche. Pour toute information complémentaire se référer au site suivant : http://shibboleth.net/
Téléservice	Application destinée à la communication interadministration ou destinée à réaliser des téléprocédures ouvertes à des usagers, c'est-à-dire application grand public.