MISE EN ŒUVRE ET MAINTENANCE DE SITES D'INTRANETS ET DE PORTAILS MÉTIER CNRS

Cahier des Clauses Techniques Particulières (CCTP)

Livret 1/2 du CCTP n°26463

Accord cadre n°26.14.027

Objet : Ce document décrit le contexte du projet, la description de la solution cible ainsi que la trajectoire de construction pour la mise en œuvre et la maintenance de sites web internes CNRS dont Intranet CNRS, Portail DU, Portail RH et Bourse aux matériels.

SOMMAIRE

1 CONTEXTE GÉNÉRAL 5
1.1 Objet de l'accord-cadre 5
1.2 Présentation synthétique du CNRS 6
1.3 Echéancier prévisionnel du projet 6
1.4 Lieu d'exécution de l'accord-cadre 6
1.5 Structure du CCTP et conventions de rédaction 7
2 CONTEXTE DU SI AU CNRS 8
2.1 Conformités règlementaires 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 9
2.1.4 Accessibilité numérique 10
2.1.5 Principes de réalisation numérique responsable 12
2.2 Présentation des infrastructures du SI CNRS 13
2.2.1 Sites et utilisateurs du système d'information 13
2.2.2 Centres serveurs 13
2.2.3 Réseau 13
2.2.4 Infrastructures 14
2.3 Principes d'urbanisation et d'intégration dans le SI 14
2.3.1 Principes généraux 14
2.3.2 Principes d'échanges 15
2.3.3 Plateformes transverses et services proposés 15
2.3.4 Prise en compte des changements de l'organisation structurelle du CNRS et de son environnement (Enseignement Supérieur et Recherche – ESR) 17
3 DESCRIPTION DU PÉRIMÈTRE FONCTIONNEL 19
3.1 Solutions applicatives 19
3.1.1 Intranet du CNRS 19
3.1.2 Portail DU 21
3.1.3 Portail RH 22
3.1.4 Bourse aux matériels 23
3.2 Autres exigences fonctionnelles 24
3.2.1 Recherche 24
3.2.2 Traduction 24
3.2.3 Mutualisation et homogénéité 25
3.3 Intégration dans le SI 25
3.4 Conduite du changement 26
4 CADRE DE COHÉRENCE TECHNIQUE DE LA SOLUTION 27
4.1 Exigences d'intégration dans le SI 27
4.1.1 Répartition fonctionnelle 27
4.1.2 Echanges de données 27
4.1.3 Authentification, comptes utilisateurs 30
4.2 Exigences techniques 32
4.2.1 Choix du CMS et de la base de données 32
4.2.2 Eléments techniques structurants 33
4.2.3 Services d'infrastructure 33
4.2.4 Architecture applicative 36
4.2.5 Base de données 43
4.2.6 Engagements de qualité de service pour l'application 43
4.3 Exigences d'ergonomie-graphisme 44
4.3.1 Charte graphique 44

4.3.2 UX/UI et règles d'ergonomie 45
4.3.1 Référentiel OPQUAST 45
4.4 Exigences de sécurité 45
4.4.1 Auditabilité 46
4.4.2 Protection des applications web 46
4.5 Exigence d'intégration des outils d'Intelligence Artificielle 47
4.6 Protection des données personnelles 48
4.6.1 Organisation de la protection des données 48
4.6.2 Obligation des parties 49
4.6.3 Information des personnes et traitement des demandes d'accès aux données 50
4.6.4 Recours à des sous- traitants 50
4.6.5 Durée de conservation des données et archivage 51
4.6.6 Destruction, réversibilité 51
4.6.7 Analyse d'impact sur la vie privée 51
4.6.8 Exigences de sécurité 52
4.6.9 Traitement des incidents impactant les données à caractère personnel 52
4.6.10 Audit 52
4.6.11 Coopération avec les autorités de contrôle 53
5 CADRE D'ORGANISATION DES PRESTATIONS 54
5.1 Système qualité 54
5.2 Organisation des équipes projet 54
5.2.1 Organisation de l'équipe projet CNRS 54
5.2.2 Organisation et gestion des compétences de l'équipe projet du titulaire 56
5.2.3 Organisation des instances de la gouvernance 56
5.2.4 Pratiques de gestion de projet 58
5.2.5 Indicateurs de pilotage et qualité du projet 59
5.3 Méthode de développement 59
5.3.1 Cycle de vie 59
5.3.2 Activités de réalisation (à la charge du Titulaire) 61
5.3.3 Activités de recette (à la charge du CNRS) 62
5.4 Gestion des environnements 62
5.4.1 Postes de travail du titulaire 62
5.4.2 Environnement de développement 63
5.4.3 Environnements CNRS 63
5.5 Gestion des livraisons 63
5.6 Gestion de la documentation 64
5.7 Capitalisation des connaissances 65
5.8 Outillage de suivi et pilotage du projet 66
5.9 Mesures et clauses de sécurité 67
5.9.1 Gestion de la Sécurité par le titulaire 67
5.9.2 Protection des biens 67
5.9.3 Obligations du titulaire 70
5.9.4 Localisation des données 70
5.9.5 Audit 70
5.9.6 Application des plans gouvernementaux 71
6 RESPONSABILITÉ SOCIÉTALE DES ENTREPRISES (RSE) 72
6.1 Responsabilité environnementale 72
6.1.1 Écoconception 72
6.1.2 Principes de réalisation numérique responsable 72
6.2 Responsabilité sociétale 72
6.2.1 Accessibilité numérique 72
6.2.2 Formation des personnels affectés à l'exécution 72
6.2.3 Prévention du sexisme et du harcèlement 72

7 ANNEXES 73
7.1 Documents joints 73
7.2 Référence des exigences 73
7.3 Abréviations et glossaire 74
7.3.1 Abréviations 74
7.3.2 Glossaire 74
7.4 Présentation détaillée du CNRS 75
7.4.1 La présidence-direction générale 75
7.4.2 La Direction générale déléguée aux ressources (DGD-R) 76
7.4.3 Les délégations régionales (DR) 78
7.4.4 Les unités (laboratoires) 79

1 CONTEXTE GÉNÉRAL

1.1 OBJET DE L'ACCORD-CADRE

Le présent accord-cadre a pour objet la fourniture de prestations de réalisation/maintenance et d'évolutions de sites web intranets et portails internes au CNRS, en technologie Drupal, y compris des prestations annexes (formations, conduite du changement, expertises, …).

Le marché comprend notamment la refonte en technologie Drupal / PostgreSQL de quatre de ses applications nationales actuellement en technologie Microsoft SharePoint : Intranet du CNRS, Portail DU, Portail RH, Bourse aux matériels.

Les applications Intranet du CNRS, Portail DU et Portail font partie de la tranche ferme du marché.

L'application Bourse aux matériels relève d'une tranche optionnelle.

La technologie Microsoft SharePoint ne va plus permettre la mise en œuvre de plateforme on premise. Les solutions de cloud ne sont pas acceptables, notamment à cause du Cloud Act américain. Certaines fonctionnalités de SharePoint vont être dépréciées.

L'objectif principal est ainsi de mettre en service ces refontes d'applications d'ici 2029.

Nota : dans l'ensemble des documents il est utilisé indifféremment les termes « **application** » ou « **site** » pour désigner les diverses briques à réaliser : Intranet du CNRS, Portail DU, Portail RH, Bourse aux matériels.

Par le terme « **plateforme** », le CNRS entend l'ensemble des briques hébergées au CNRS nécessaires pour le fonctionnement de ces applications. Certaines briques peuvent être mutualisées, si pertinent, pour leur utilisation par plusieurs applications.

Le présent accord-cadre a pour objet la fourniture de prestations de mise en œuvre initiale et de maintenance de ces applications :

- Réalisation avec le CMS Drupal de l'Intranet du CNRS, de Portail DU, de Portail RH et de Bourse aux matériels, et intégration avec les autres systèmes du CNRS (DAM, web analytics, référentiels…) :
    - Définition de l'infrastructure (dimensionnement VM, RAM, CPU, stockage, etc.) et de l'architecture (Drupal, système de mise en cache, accélérateur de site, etc.) répondant aux exigences techniques et de sécurité du CNRS, conjointement avec le CNRS
    - Développement et configuration des applications
    - Rédaction des procédures d'installation et de paramétrage des composants logiciels (Drupal, système de mise en cache, accélérateur de site, etc.),
- Reprises des données provenant des applications de la plateforme SharePoint,
- Tierce maintenance applicative (TMA) des applications, c'est-à-dire assurer le correctif et l'évolution des applications mises en œuvre,
- Maintien en condition opérationnelle et de sécurité (MCO/MCS) des applications, c'est-à-dire identifier les mesures permettant de garantir la disponibilité, la performance et la sécurité des applications mises en œuvre,
- Support aux équipes CNRS en charge de la mise en œuvre sur la plateforme CNRS : installation des composants logiciels, des applications, MCO/MCS…
- Prestations annexes (formations, conduite du changement, expertises…).

Le CNRS se réserve la possibilité d'introduire dans le périmètre du MCO/MCS, des applications basées sur la technologie Drupal :

- **Qu'il a développé lui-même**
- **Que des unités (laboratoires, Délégations régionales, Directions) ont fait développer par un tiers.**

Prestations expressément exclues du périmètre du présent accord-cadre :

- L'hébergement des sites sera réalisé sur un cloud privé (IaaS) fourni par le CNRS.

- L'installation de la plateforme est de la responsabilité du CNRS.
- L'exploitation et l'administration de la plateforme sont de la responsabilité du CNRS.
- L'administration fonctionnelle des applications est de la responsabilité du CNRS.
- La production du contenu éditorial des sites est de la responsabilité du CNRS.
- Le CMS dispose de sa propre gestion des ressources multimédias. Il est cependant prévu, additionnellement, de pouvoir se connecter à un DAM pour y puiser des médias. Ce DAM (Digital Asset Management) est opéré exclusivement par le CNRS.
- La génération des newsletters est réalisée via une plateforme marketing en mode SaaS (BREVO) gérée par la Direction de la communication.

Le document Livret1_Annexe_RACI décrit de manière détaillée la matrice RACI des responsabilités partagées entre le CNRS et le titulaire pour gérer la plateforme CNRS.

1.2 PRÉSENTATION SYNTHÉTIQUE DU CNRS

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

Avec plus de 34 000 personnes, un budget de 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. § 7.4.1.3).

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 (cf. § 7.4) et sur le site Web, à l'adresse suivante : https://www.cnrs.fr/fr/le-cnrs/organisation.

1.3 ECHÉANCIER PRÉVISIONNEL DU PROJET

Le projet démarre dès la notification de l'accord-cadre envisagée au 1er semestre 2027 avec la prestation de lancement.

Les prestations de développement et reprise des données des applications du périmètre initial seront commandées en parallèle ou en léger décalé selon un planning à établir avec le titulaire.

Les mises en service de chacune des applications pourront se faire indépendamment les unes des autres.

Les hypothèses calendaires suivantes sont retenues à l'heure de la publication :

- Le CNRS souhaite disposer d'une première livraison en recette de chacune des applications fin 2027 / début 2028.
- Les premières mises en production sont souhaitées en 2028.
- La mise en production finale, avec reprise des données finalisée, des applications du périmètre initial est souhaitée au plus tard début 2029.

Le titulaire propose dans son offre un planning visualisant les différentes phases du projet, et de chacun des quatre sous-projets de refonte, prenant en compte les éléments précités ainsi que les découpages en itérations/lots de chaque développement.

Ces éléments seront consolidés conjointement lors du démarrage de l'accord-cadre.

1.4 LIEU D'EXÉCUTION DE L'ACCORD-CADRE

La réalisation et maintenance de la solution s'effectue dans les locaux du titulaire.

Les comités, réunions ou ateliers de spécifications et de conception, nécessitant la présence du CNRS, se tiennent en visioconférence entre les sites CNRS et le site du titulaire ou sur sites CNRS.

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

Les locaux du CNRS se situent :

CNRS – DSI (MOE)
358 rue Pierre Gilles de Gennes - 31670 LABEGE

Services et directions du siège du CNRS (MOA)
3 rue Michel-Ange - 75794 PARIS CEDEX 16

1.5 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 : exigences métier et fonctionnelles pour la réalisation de la solution initiale,
    - avec une synthèse des besoins métiers et fonctionnels dans ce document
    - des expressions des besoins métiers et fonctionnels détaillées en annexe pour chaque application à refondre
        - Intranet du CNRS
        - Portail DU
        - Portail RH
        - Bourse aux matériels
- cadre de cohérence technique de la solution : exigences applicables à la solution initiale et 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, objets de la commande.

Les exigences vis-à-vis du titulaire sont décrites dans le présent document dans des tableaux de la forme ci-dessous.

Référence	Libellé exigence
XXXX_[XXXX_]NNN	Libellé de l'exigence

La référence est composée de lettres XXXX définissant le groupe et le sous-groupe d'exigences (cf. « Référence des exigences » en annexe) et de chiffres NNN (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)

Ces informations sont indiquées dans l'Annexe 1 : Tableau des exigences (§ 7.1 Documents joints).

2 CONTEXTE DU SI AU CNRS

2.1 CONFORMITÉS RÈGLEMENTAIRES

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

Référence	Libellé exigence
REGL_103	Les applications sont mises en œuvre conformément au RGAA (Référentiel général d'amélioration de l'accessibilité) : https://accessibilite.numerique.gouv.fr/
REGL_104	Pour les applications qui ne sont pas des téléservices, l'objectif de conformité au référentiel RGS est poursuivi.
REGL_105	Pour les applications qui ne sont pas des téléservices, l'objectif de conformité au référentiel RGI est poursuivi.
REGL_106	Les solutions applicatives sont mises en œuvre conformément au RGESN (Référentiel général d'écoconception de services numériques) : https://ecoresponsable.numerique.gouv.fr/publications/referentiel-general-ecoconception/.
REGL_107	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.
REGL_108	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.
REGL_109	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.
REGL_110	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.
REGL_111	La mise en place de cookies non essentiels est validée par le CNRS.

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 (PGSI[1]) 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, règlementaires et contractuelles ;
- Eviter 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.

A 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 règlementaires doivent être prises en compte ;
- La gestion des risques doit être réalisée de façon systématique suivant la règlementation Française et les normes internationales en vigueur ;

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

- 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
REGL_112	Le titulaire se conforme au cadre réglementaire applicable en termes 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 (II 901) 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

2.1.2 Protection des données à caractère personnel (DCP)

Référence	Libellé exigence
REGL_113	Le titulaire se conforme aux réglementations applicables en termes de protection des données à caractère personnel : - Règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD), - Loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et textes pris pour son application. - Les traitements sont également réalisés en conformité avec toute délibération et recommandation de la Commission nationale de l'informatique et des libertés (CNIL).

La politique de protection des données personnelles au CNRS et ses exigences sont décrites au § 4.6 Protection des données personnelles.

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 P1 choisi par le CNRS conformément aux objectifs du présent accord cadre.

L'application des autres profils d'interopérabilité, P2 (si SOAP, XML), P3 (si génération de zip, pdf, …), P4 (si archivage), fera l'objet d'un accord préalable du CNRS.

2.1.4 Accessibilité numérique

Dans le cadre du développement des applications/sites, le titulaire est tenu de respecter les obligations légales françaises en matière d'accessibilité numérique, conformément à l'article 47 de la loi n° 2005-102 du 11 février 2005, au décret n° 2019-768 du 24 juillet 2019, et au Référentiel Général d'Amélioration de l'Accessibilité (RGAA) version 4.1.2, basé sur les WCAG 2. Le respect du RGAA est requis pour les applications/sites, et une déclaration d'accessibilité spécifique est produite pour chaque application/site.

1. Conformité au RGAA 4.1.2

- **Taux de conformité RGAA** : Le titulaire garantit que l'ensemble des pages des sites atteignent un taux conforme aux critères du RGAA 4.1.2, sauf dérogations exceptionnelles dûment justifiées (voir section 4).
- **Périmètre d'application** : Cette exigence s'applique à toutes les pages, fonctionnalités, et contenus (interfaces, formulaires, contenus multimédias, contenus dynamiques) de chaque site.
- **Standards techniques** : Le code HTML, CSS, et JavaScript est conforme aux standards W3C (HTML5, CSS3) et compatible avec les technologies d'assistance (lecteurs d'écran comme NVDA, JAWS, VoiceOver, et afficheurs braille).

2. Déclaration d'accessibilité par application/site

- **Rédaction et publication** : Le titulaire fournit une déclaration d'accessibilité distincte pour chaque site, conforme au modèle du RGAA 4.1.2. Chaque déclaration est publiée sur le site concerné, dans une section facilement accessible (par exemple, en pied de page ou dans une rubrique dédiée). Chaque déclaration inclut :
  - Une affirmation explicite du taux de conformité sur les pages échantillonnées du site concerné, ou une justification claire des écarts en cas de non-conformité partielle.
  - Une liste des éventuelles non-conformités spécifiques au site, avec explications et justifications.
  - Un lien vers un formulaire de contact dédié permettant aux utilisateurs de signaler des problèmes d'accessibilité pour le site concerné. L'adresse courriel de contact sera fournie par le CNRS.
  - Une mention de la possibilité de saisir le Défenseur des droits en cas de non-réponse à une réclamation dans un délai d'un mois.
- **Accessibilité des déclarations** : Chaque déclaration est rédigée dans un format accessible, compatible avec les technologies d'assistance, et disponible en lecture facile si pertinent.
- **Centralisation** : Une page centralisée liste les liens vers le Schéma Pluriannuel Accessibilité Numérique du CNRS, les annexes et le plan d'action de l'année en cours. Ces documents sont fournis par le CNRS.

3. Audit et validation

- **Audit par site** : Le titulaire réalise un audit d'accessibilité distinct pour chaque site, conformément à la méthodologie RGAA 4.1.2. Chaque audit couvre un échantillon représentatif de pages et de fonctionnalités spécifiques au site, démontrant le taux de conformité RGAA sur les pages échantillonnées.
- **Rapport d'audit par site** : Pour chaque site, le titulaire fournit un rapport détaillé incluant :
  - Le taux de conformité.
  - La liste des pages auditées et des critères RGAA vérifiés.
  - Les résultats des tests avec les principales technologies d'assistance (NVDA, JAWS, VoiceOver, etc.).
  - Une confirmation que toutes les non-conformités éventuelles ont été corrigées avant livraison.
- **Tests utilisateurs** : Des tests avec des utilisateurs en situation de handicap (visuel, auditif, moteur, cognitif) sont organisés pour chaque site afin de valider l'accessibilité pratique et l'ergonomie des interfaces.
- **Outils d'évaluation** : Les audits combinent des outils automatiques (par exemple, WAVE, Axe) et une vérification manuelle pour garantir l'exactitude des résultats.

4. Dérogations exceptionnelles

- **Charge disproportionnée** : Toute dérogation pour cause de charge disproportionnée est spécifique à un site donné, justifiée par une analyse détaillée (coût, impact, alternatives possibles), et soumise à l'approbation préalable du maître d'ouvrage. Cette justification est incluse dans la déclaration d'accessibilité du site concerné.
- **Incompatibilité technique** : Toute dérogation pour incompatibilité technique est documentée avec des preuves techniques et un plan de contournement ou de correction future, spécifique au site.
- **Validation des dérogations** : Les dérogations sont validées par le maître d'ouvrage et conformes aux exigences du RGAA 4.1.2.

5. Plan d'action en cas de non-conformité

- **Correction immédiate par site** : Si des non-conformités sont identifiées lors des audits, le titulaire les corrige dans un délai défini par le maître d'ouvrage, afin d'atteindre le taux de conformité RGAA sur les pages échantillonnées de chaque site.
- **Plan d'action par site** : Un plan d'action spécifique à chaque site est fourni, incluant :
  - La liste des non-conformités identifiées pour le site.
  - Les mesures correctives prévues.
  - Un calendrier précis pour les corrections.
- **Vérification post-correction** : Un audit complémentaire par site est réalisé pour confirmer la conformité RGAA après correction.

6. Maintenance et suivi

- **Conformité continue** : Le titulaire garantit que toute mise à jour ou évolution d'un site maintient un taux de conformité de RGAA sur les pages échantillonnées auditées.
- **Mise à jour des déclarations** : Chaque déclaration d'accessibilité est actualisée selon la périodicité requise dans le RGAA ou à chaque modification majeure du site concerné, confirmant le maintien du taux de conformité RGAA.

7. Responsabilité légale

- **Conformité légale** : Le titulaire est pleinement responsable du respect des obligations légales fixées par l'article 47 de la loi n° 2005-102, le décret n° 2019-768, et le RGAA 4.1.2 pour chaque site. Tout manquement peut entraîner des sanctions administratives ou judiciaires, notamment via le Défenseur des droits.
- **Pénalités contractuelles** : En cas de non-atteinte du taux de conformité de RGAA sur les pages échantillonnées d'un site, sauf dérogations validées, le titulaire doit prendre en charge les coûts de mise en conformité.
- **Documentation** : Le titulaire fournit une documentation complète pour chaque site, prouvant la conformité RGAA, incluant les rapports d'audit, les justificatifs de dérogations, et les plans d'action correctifs.

8. Références réglementaires

- **Le titulaire se conforme aux textes suivants :**
  - Article 47 de la loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées.
  - Décret n° 2019-768 du 24 juillet 2019 relatif à l'accessibilité aux personnes handicapées des services de communication au public en ligne.
  - Référentiel Général d'Amélioration de l'Accessibilité (RGAA) version 4.1.2, disponible sur le site de la DINUM (Direction interministérielle du numérique).
- Les WCAG 2 (Web Content Accessibility Guidelines) sont utilisées comme base technique pour la mise en œuvre.

9. Livrables attendus

- Une déclaration d'accessibilité distincte pour chaque site, publiée et indiquant le taux de conformité sur les pages échantillonnées ou justifiant toute dérogation.
- Un rapport d'audit initial par site, démontrant la conformité RGAA des pages échantillonnées.
- Des rapports d'audit complémentaires pour chaque phase de mise à jour ou évolution d'un site.
- Un plan d'action spécifique par site pour la correction des non-conformités, si applicable.
- Une documentation technique détaillant les mesures prises pour assurer l'accessibilité de chaque site (code, tests, outils utilisés).

Le référentiel d'accessibilité applicable est disponible en libre accès :
https://accessibilite.numerique.gouv.fr/

2.1.5 Principes de réalisation numérique responsable

Le CNRS a pour ambition de mettre à disposition de ses utilisateurs des applications conçues dans une démarche écoresponsable afin de réduire au maximum ses émissions de gaz à effet de serre (GES) et ses besoins en ressources énergétiques. Les principaux leviers sont listés ci-dessous :

1. CMS et composants :

- Favoriser la mutualisation et l'utilisation de briques transverses ;
- Choisir des composants libres et pérennes, reconnus et maintenus par la communauté ;

2. Optimisation du code et des ressources :

- Le code HTML, CSS et JavaScript devra être conforme aux standards W3C.
- Limiter les solutions proposées dans les applications aux besoins réels des utilisateurs (frugalité des besoins) ;
- Privilégier des solutions techniques simples et peu coûteuses vis-à-vis des données échangées (ex : poids des pages, formats utilisés …) ;
- Dans le cadre de la gestion des fichiers stockés sur la plateforme, intégrer la possibilité pour l'utilisateur de visualiser les informations dans le navigateur en évitant les téléchargements, d'obtenir un lien de visualisation plutôt que de téléchargement, puis un lien de téléchargement pour intégration ou vignette quand c'est possible.

3. Design & Performance des pages :

- Faire du Responsive Design avec l'idée de limiter la bande passante
- Proposer une mise en cache efficace
- Optimiser le poids des pages (poids du code, poids des images -optimisation compression, format vectoriel le cas échéant..-, adaptation à la résolution, utiliser la pagination plutôt que le défilement infini, Compresser les images en WebP, AVIF et JPEG optimisées, selon compatibilité des navigateurs. Éviter les GIFS et plutôt utiliser des animations en CSS.)
- Une compression automatique (sans perte) sera mise en œuvre sur les images. Qu'il s'agisse d'un média uploadé par un contributeur, ou d'un média récupéré de l'extérieur (flux RSS, API, etc.).
- Le nombre de requêtes HTTP sera minimisé par le regroupement et la minification des ressources.

4. Données :

- Dimensionner de façon juste les infrastructures ;
- Accroître la durée de vie des applications en améliorant leur urbanisation et leur maintenance ;
- Proposer des stratégies de gestion du cycle de vie des données pour limiter le stockage inutile ;
- Prévoir une purge automatique des logs, sauvegardes et bases d'audit (périodicité à définir)

5. Suivi et mesure de l'impact :

- Un audit initial de performance environnementale (EcoIndex, Lighthouse ou équivalent) sera fourni à la livraison
- Proposer des outils permettant de suivre la performance environnementale sur la durée, à l'aide de rapports. Green-it CLI est une piste. Il est possible de générer des rapports, sur des parcours précis, et d'automatiser en partie. Attention, les solutions tiers propriétaires, peuvent ne pas convenir au regard du coût budgétaire et environnemental que cela peut engendrer.
- Améliorer la sécurisation des applications pour limiter l'occurrence des incidents et leur coût de gestion.
- Proposer une série d'indicateurs de mesure pour le pilotage
- Faire des recommandations pour maintenir une démarche éco-responsable lors des évolutions futures

Le titulaire respecte au mieux ces grands principes qui doivent guider ses choix de conception.

Ces exigences peuvent être complétées par les préconisations du chapitre « Services numériques » du guide « Bonnes pratiques numérique responsable pour les organisations » de la Direction Interministérielle du Numérique (DINUM) :
https://ecoresponsable.numerique.gouv.fr/docs/2023/guide-de-bonnes-pratiques-numerique-responsable-version-1.pdf.

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 centre principal d'hébergement, 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 connecter 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 : https://www.renater.fr/

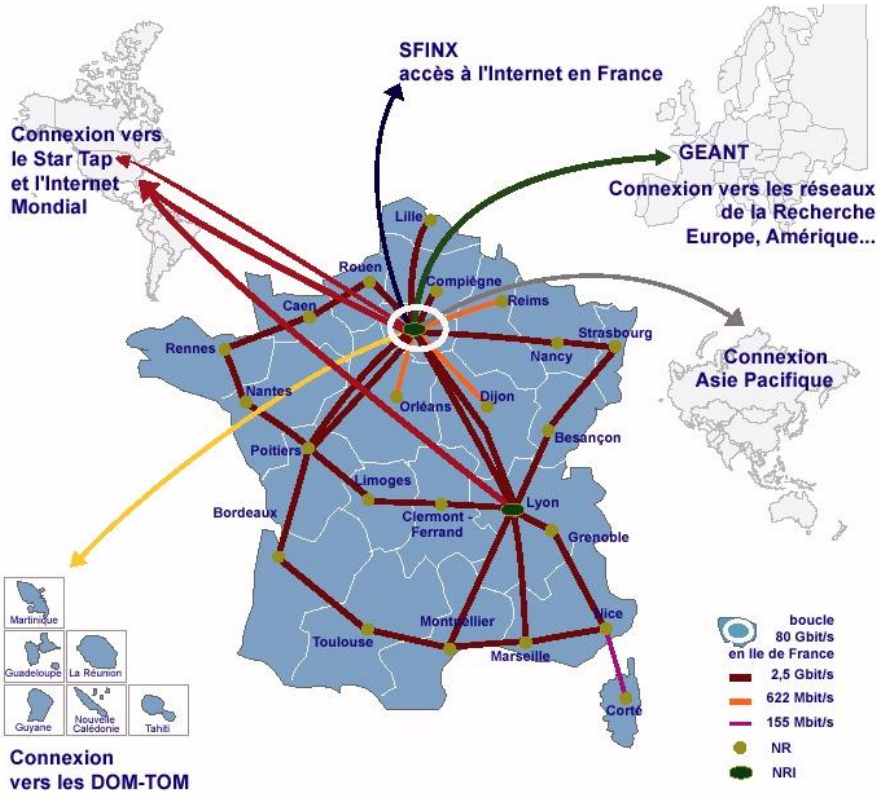


Figure 1 : Réseau RENATER

Afin d'avoir la maîtrise des flux spécifiques du système d'information du CNRS, la DSI a construit un réseau dédié et privé, Sires, qui fédère l'ensemble des sites administratifs et des centres serveurs. 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 ;
- favoriser la conception d'un SI écoresponsable.

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 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 échanges sont conçus en respectant le principe de frugalité des données échangées (échanges limités aux données strictement nécessaires) dans un souci de conception écoresponsable et de limitation des ressources utilisées.

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 ESB CNRS » (découpage en ½ flux, format pivot des objets métiers échangés, exposition de services web) qui a la responsabilité et la gestion des échanges. Le cas échéant, il assure l'orchestration, la chronologie des flux, ainsi que la 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 de référence). L'accès aux données des référentiels se fait au travers d'une API REST qui interroge une base de données qui retourne des données au format JSON ou XML.

2.3.3.2 Gestion des données de référence

La DSI du CNRS dispose d'un outil MDM – Master Data Management (GRD-Gestion des Données de Référence) nommé Réséda et proposant des services de gouvernance afin d'assurer la qualité, l'intégrité et l'exactitude des données de référence tout au long de leur cycle de vie.

L'usage de cette plateforme est fortement préconisé pour les référentiels structurants et partagés pour lesquels une gouvernance métier est attendue entre différents acteurs métiers.

Actuellement Réséda gère les référentiels suivants (liste non exhaustive) :

- Structures organisationnelles du CNRS ;
- Personnels (CNRS et non CNRS) des structures du CNRS ;
- Fournisseurs ;
- Partenaires ;
- Contacts.

Ainsi qu'un certain nombre de nomenclatures.

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. plus haut).

2.3.3.3 Gestion des accès et habilitations

2.3.3.3.1 Fournisseurs d'identité et authentification

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) dépendants de la population à authentifier (Personnel des structures du CNRS, Prestataires et usagers des unités CNRS, Externes) et du niveau d'authentification nécessaire.

Plusieurs fournisseurs d'identité sont proposés par le CNRS :

- Pour les personnels des structures du CNRS : **Janus** pour une authentification simple et **Janus+** pour une authentification multifacteur (MFA) (service dédié aux applications sensibles du CNRS).
- Pour les usagers, les hébergés, les prestataires et les invités (UHPI) des structures du CNRS : **Janus UHPI** pour une authentification simple et **Janus+ UHPI** pour une authentification multifacteur (MFA) (service dédié aux applications sensibles du CNRS).
- Pour les externes non UHPI connus du CNRS : **Janus-ext**. Ce fournisseur est historique, et son usage est remplacé progressivement par les fournisseurs Janus UHPI et Janus+ UHPI.

Il est également possible d'authentifier les personnels académiques des établissements d'enseignement supérieur et de recherche grâce à leur fournisseur d'identité en s'appuyant sur la **fédération d'identité Education-Recherche de Renater**.

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 peut être un service de découverte SAML.

Ces services s'appuient sur le référentiel des personnels des structures du CNRS (cf. § 2.3.3.2) et sur Sésame (cf. § 2.3.3.3.2).

2.3.3.3.2 Habilitation des utilisateurs

Les services d'habilitation des utilisateurs sont regroupés sous la dénomination de **Sésame** (parfois appelé également IAM – Identity and Access Management). Ces services permettent l'attribution des profils d'habilitation et des rôles applicatifs à des comptes utilisateurs afin de centraliser de manière cohérente les politiques d'accès au SI.

Cette centralisation peut être totale ou partielle : les droits d'accès fins (ex : lecture / écriture sur des données, accès à des modules ou IHM) restent généralement gérés au niveau des applications métiers, afin de couvrir des cas d'usage spécifiques à chaque application.

Ces services s'appuient sur le référentiel des personnels et des structures du CNRS (cf. § 2.3.3.2).

Les utilisateurs ayant une habilitation de contribution, d'approbation ou les administrateurs de l'application devront s'authentifier avec un deuxième facteur.

Actuellement, les utilisateurs CNRS avec des habilitations élevées utilisent déjà Janus+ pour d'autres application du SI.

Le CNRS est en cours de mise en place un deuxième facteur dans Janus pour des habilitations intermédiaires.

La solution à mettre en place sera définie d'un commun accord avec le CNRS lors du lancement des développements. Le deuxième facteur via Janus ou Janus+ est préféré à un nouveau mode (via un module 2FA de Drupal par exemple).

Dans tous les cas cette authentification 2FA ne doit pas impliquer une mire de service de découverte (anciennement WAYF) pour l'accès à l'application de tous les utilisateurs. Il est préférable que l'authentification 2FA soit demandée lorsque l'utilisateur veut atteindre le backoffice.

2.3.3.3.3 Provisionnement des comptes utilisateurs

Les services permettant d'obtenir les informations sur les comptes utilisateurs du SI CNRS sont regroupés sous la dénomination de **Référentiel des utilisateurs**.

Les données du référentiel des utilisateurs sont exposées par des services Web à l'usage des applications pour assurer le provisionnement et le dé-provisionnement des comptes utilisateurs dans le SI. Certaines de ces données sont transmises à l'application via le processus d'authentification SAML.

Ces services s'appuient sur le référentiel des personnels et des structures du CNRS (cf. § 2.3.3.2), sur Janus (cf. § 2.3.3.3.1) et sur Sésame (cf. § 2.3.3.3.2).

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
URB_101	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).

Le référentiel d'organisation du CNRS est géré via l'outil GDR, et plus particulièrement dans le référentiel Réséda Structure.

Le référentiel des établissements de l'ESR partenaires du CNRS est lui-aussi géré dans cet outil, 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. 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 sont diffusées à l'ensemble du SI à partir de ces référentiels, au travers de web services disponibles depuis les systèmes d'intermédiation.

Référence	Libellé exigence
URB_102	La solution s'alimente du référentiel d'organisation structurelle du CNRS, à partir de ses services web dédiés.

3 DESCRIPTION DU PÉRIMÈTRE FONCTIONNEL

Toutes les actions nécessaires à la bonne exécution de l'accord-cadre et de ses marchés subséquents par le Titulaire qui ne sont pas expressément mises à la charge du Bénéficiaire par le Cahier des Clauses Administratives Particulières ou par le Cahier des Clauses techniques Particulières, sont à la charge du Titulaire, quand bien même elles n'auraient pas été spécifiquement listées dans les pièces de l'accord-cadre et des marchés subséquents, qu'elles émanent du Bénéficiaire ou du Titulaire.

Le périmètre du présent accord-cadre inclut des projets de refonte d'applications existantes. Il s'agit des quatre solutions applicatives décrites ci-après. Ces applications sont décrites par ailleurs de façon détaillée dans les expressions de besoin fonctionnelles métiers suivantes :

- Livret 1 Annexe Fonctionnelle Intranet CNRS
- Livret 1 Annexe Fonctionnelle Portail RH
- Livret 1 Annexe Fonctionnelle Portail DU
- Livret 1 Annexe Fonctionnelle Bourse aux matériels (dans le cadre d'une tranche optionnelle)

Pourront également être introduites dans le périmètre de l'accord-cadre :

- De nouveaux projets de refonte d'applications déjà existantes développées sur d'autres technologies.
- De nouveaux projets d'intranets/extranets ou de portail métier.
- L'intégration d'intranets ou de portail métier développés sur les mêmes technologies (CMS DRUPAL) hors du présent accord-cadre, que le CNRS souhaite introduire dans son périmètre, selon les modalités prévues au Cahier des clauses techniques particulière.

Les nouvelles réalisations confiées au titulaire dans le cadre du présent accord-cadre sont conditionnées par le choix initial de la technologie par le CNRS. Ce choix initial est de la responsabilité exclusive du CNRS.

Nota :

Dans les expressions de besoin des quatre applications, des balises sont mentionnées :

- Balise « **Évolution par rapport à l'existant** » : fonctionnalités modifiant ou étendant les fonctionnalités existantes, incluses dans le périmètre initial de la refonte de l'application.
- Balise « **Évolution ultérieure** » : fonctionnalités prévues pour une implémentation future, non incluses dans le périmètre initial de la refonte de l'application.

Les fonctionnalités mentionnées avec la balise « Evolution ultérieure » ne sont pas à prendre en compte dans les estimations des charges et des coûts des versions initiales forfaitaires.

3.1 SOLUTIONS APPLICATIVES

3.1.1 Intranet du CNRS

Outil permettant aux directions, services administratifs, instituts et délégations du CNRS de mettre à disposition de l'ensemble des personnels présents dans les unités du CNRS (personnels CNRS ou non) l'information validée et utile à chacun et délivrée dans le respect de la ligne éditoriale. Cette information est répartie au sein de rubriques et n'est publiée qu'après approbation.

L'intranet du CNRS permet également la production de la Lettre interne du CNRS, mensuelle, qui informe les personnels des unités CNRS des actualités institutionnelles et pratiques de l'organisme : carrière, missions, congés, supports de communication, comité d'entreprise, nominations, prix, bulletins officiels, appels d'offres ou à projets, événements, newsletters…

L'accès à l'intranet du CNRS est soumis actuellement à authentification sur le Fournisseur d'identités du CNRS uniquement. La contribution dans les rubriques est soumise à autorisation en fonction de l'appartenance aux groupes de sécurité définis dans la plateforme.

Périmètre : le service est destiné

- A tout le personnel des unités du CNRS

Acteurs :

- En consultation, tout le personnel des unités du CNRS, via le fournisseur d'identité Janus :
  - Le personnel CNRS (34 000 personnes) ;
  - Le personnel non CNRS travaillant dans les laboratoires mixtes CNRS (90 000 personnes qui se rajoutent aux 34 000 précédents ;
- Les contributeurs et approbateurs (environ 400).

L'intranet CNRS met en œuvre des fonctions de publication, de gestion de version des pages (pas des documents et médias), de workflow de publication, de recherche.

Le design applique la charte graphique du CNRS.

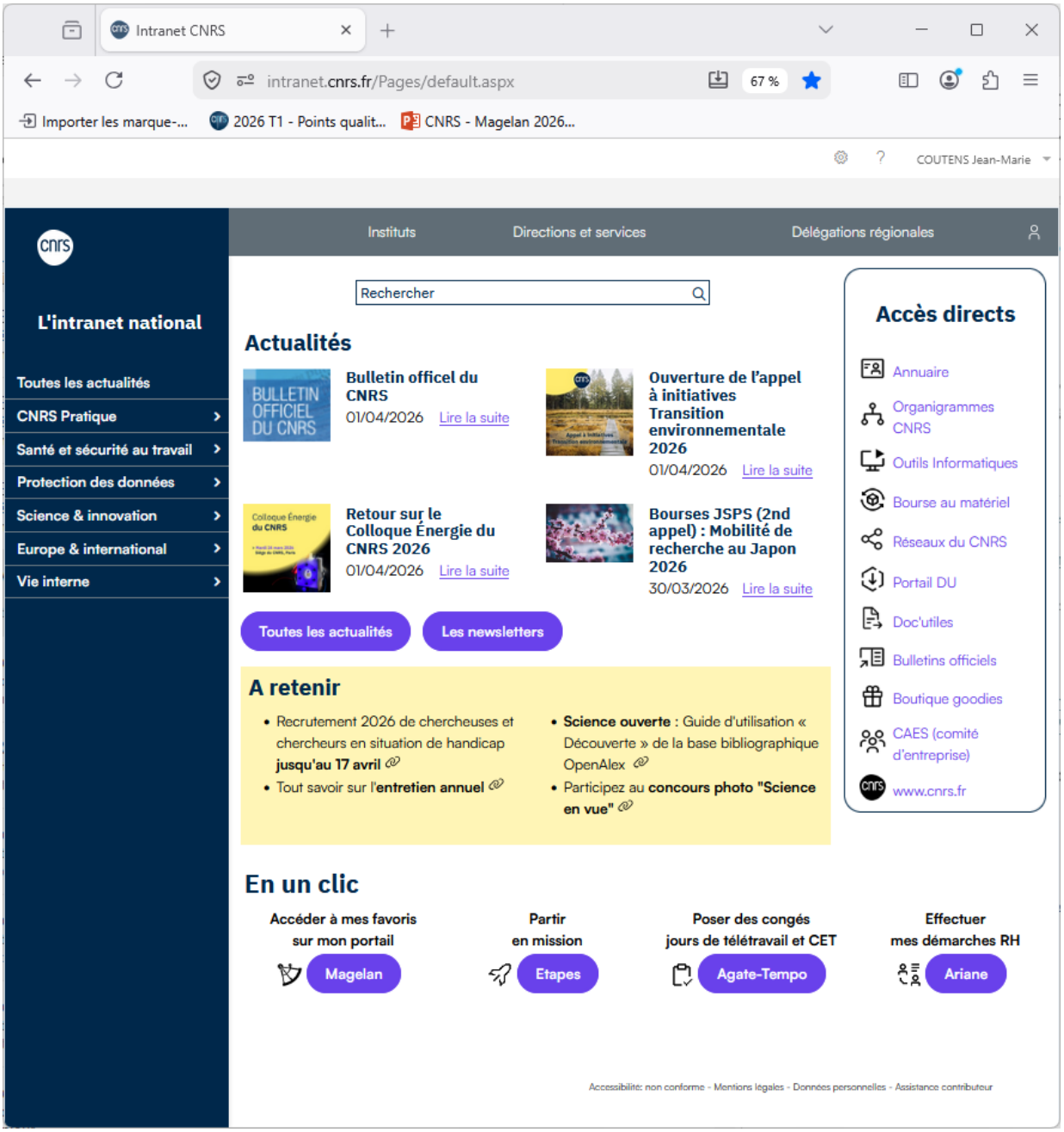


Figure 2 : Intranet CNRS

3.1.2 Portail DU

Aide au pilotage pour les directeurs d'unité (DU) et les équipes de direction des unités. Parmi les outils à disposition, une base de connaissance structurée autour des principaux sujets liés au pilotage d'une unité, un calendrier listant les actions clés des DU mois par mois dans les campagnes CNRS ou encore des points de contact facilités entre les DU, leur institut et leur délégation.

Périmètre : le service est destiné

- Aux équipes de direction des unités (DU, DU adjoints, responsables administratifs) qui peuvent être personnel CNRS ou non, ils s'authentifient via le fournisseur d'identité CNRS Janus, soit environ 3800 utilisateurs.

Acteurs :

- En consultation, la population identifiée ci-dessus.
- Contributeurs : la maitrise d'ouvrage centralise la plupart des contributions. 2 directions fonctionnelles sont également contributrices sur les rubriques concernant leur domaine métier.

Le Portail DU met en œuvre des fonctions de publication et de recherche.

Le Calendrier DU est un affichage spécifique d'actions, également affichées par ailleurs par campagne.

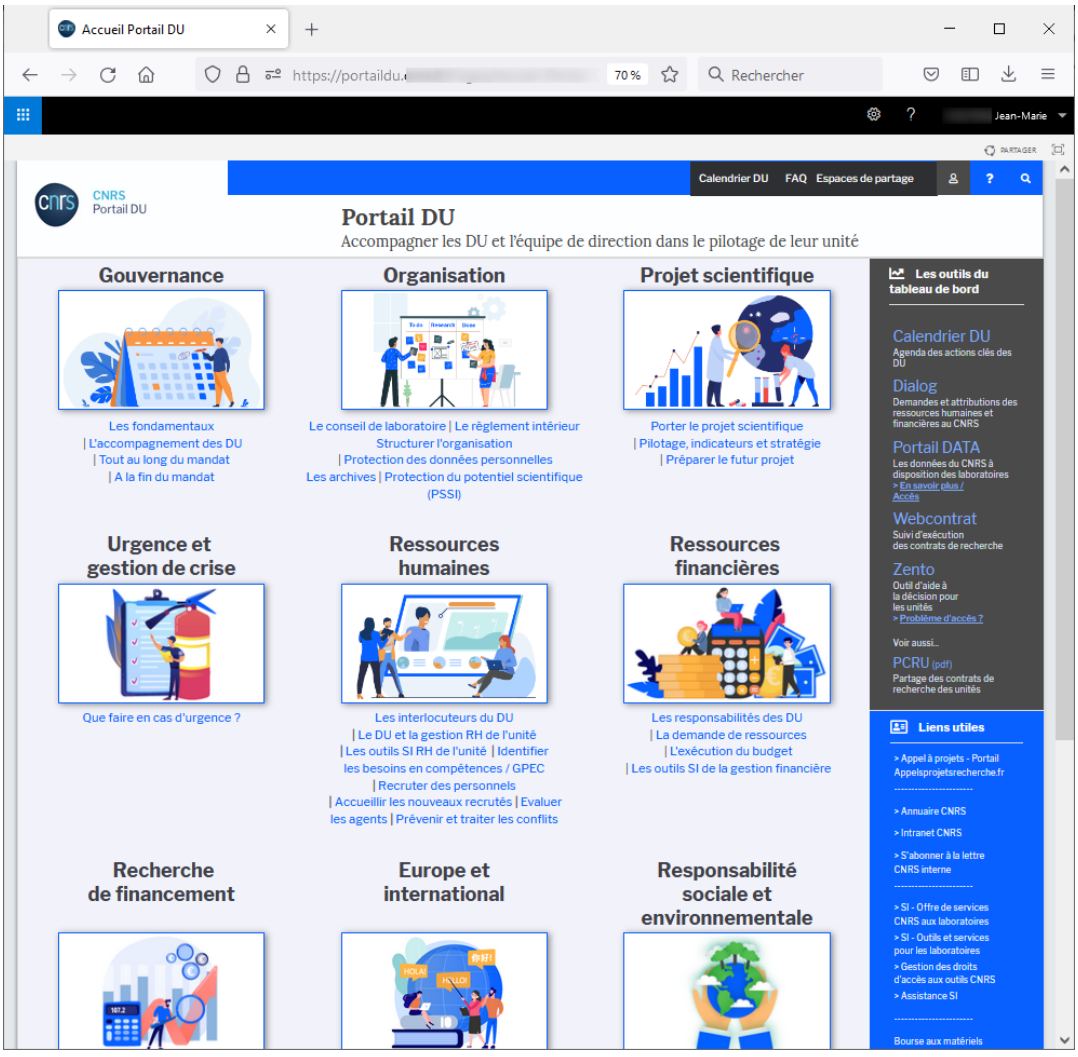


Figure 3 : Portail DU

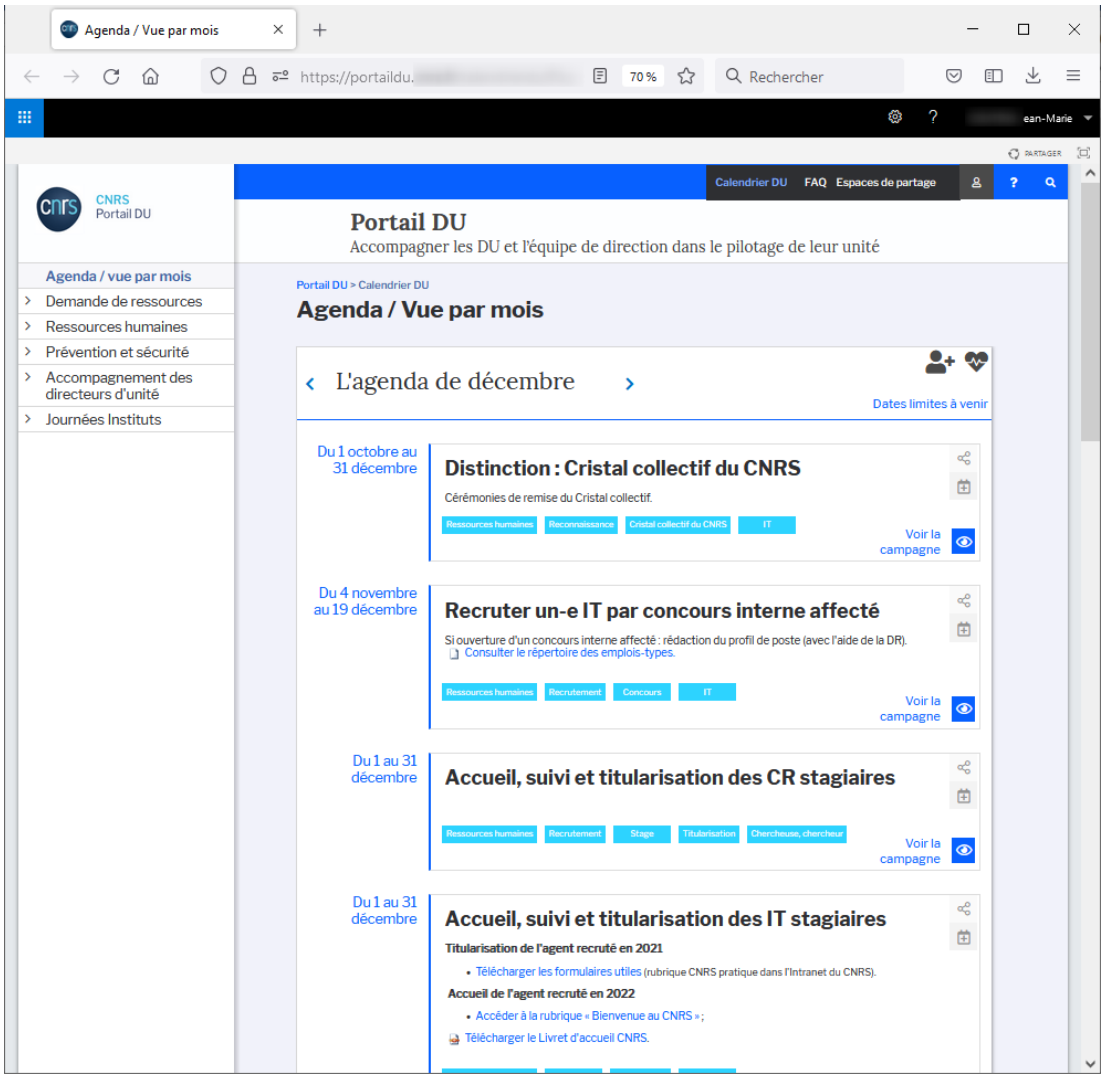


Figure 4 : Calendrier DU

3.1.3 Portail RH

Portail centralisateur de la réglementation, de la documentation et de la communication pour les personnes clé de la filière RH. Il permet de structurer et de capitaliser l'information et la communication entre la DRH, les services RH des délégations et les unités, il propose des liens vers les textes de référence et les différentes applications RH.

Le Portail RH est notamment composé d'une page par thématique RH accessible via un menu (environ 50 thématiques), de FAQ, d'actualités, d'un calendrier et de listes de liens.

Périmètre : le service est destiné

- A la filière RH du CNRS
  - Collaborateurs RH de la DRH (Direction des Ressources Humaines)
  - Collaborateurs RH au sein des SRH (Services de Ressources Humaines) des Délégations régionales
  - Correspondants de la filière RH en laboratoire

Acteurs :

- En consultation, la population identifiée ci-dessus (600 personnes), via le Fournisseur d'identité du CNRS Janus.
- Les contributeurs (environ 60 personnes de la DRH).

Le Portail RH met en œuvre des fonctions de publication, de gestion de version, de recherche.

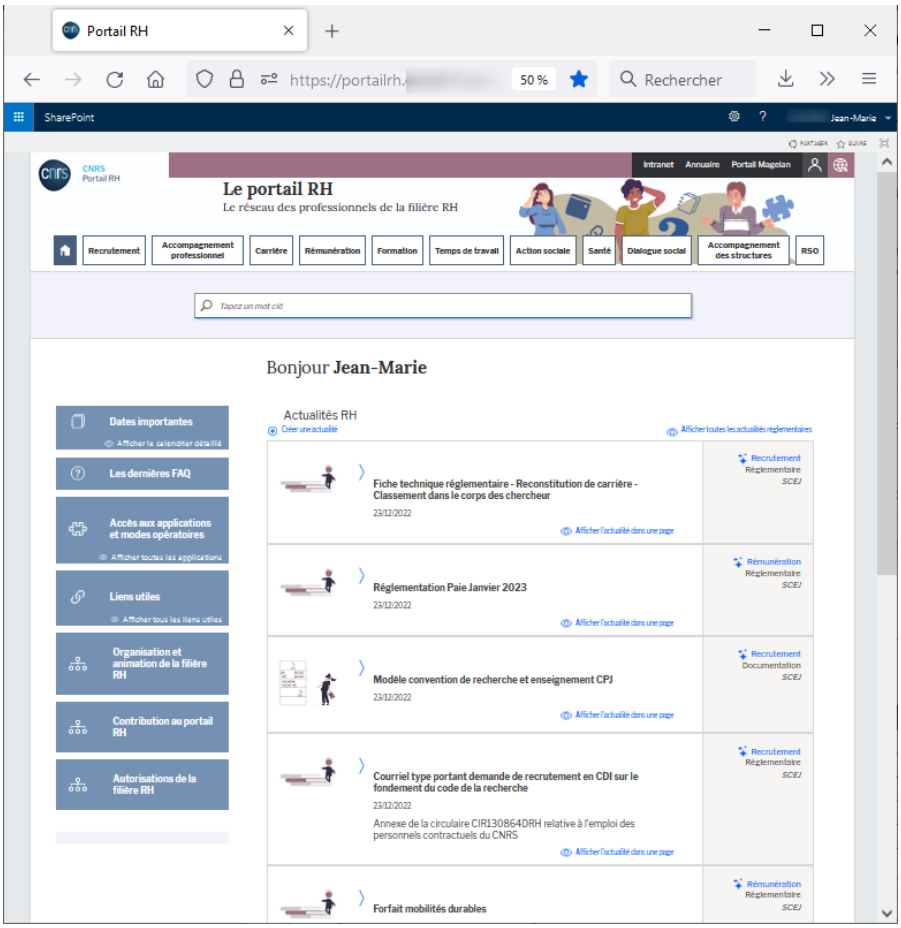


Figure 5 : Portail RH

3.1.4 Bourse aux matériels

La Bourse aux matériels facilite l'acquisition et la cession de matériels d'occasion entre unités et services du CNRS.

Il s'agit d'un service d'annonces qui permet de consulter et de déposer des annonces de cession, de don, de prêt et de recherche de matériel d'occasion. Les annonces sont publiées par les unités et services du CNRS.

Périmètre : le service est destiné au personnel des unités du CNRS (qu'il soit agent CNRS ou non)

Acteurs :

- En consultation, tout le personnel des unités du CNRS, qui s'authentifie via le fournisseur d'identité CNRS Janus
- Les créateurs d'une annonce : tout le personnel des unités du CNRS
- Les modérateurs : maîtrise d'ouvrage

Il est envisagé que la Bourse aux matériels soit ouverte à tous les organismes de la fédération d'identités Education Recherche de Renater, ou à seulement certains partenaires de cette fédération d'identités. La solution proposée devra permettre cette évolution.

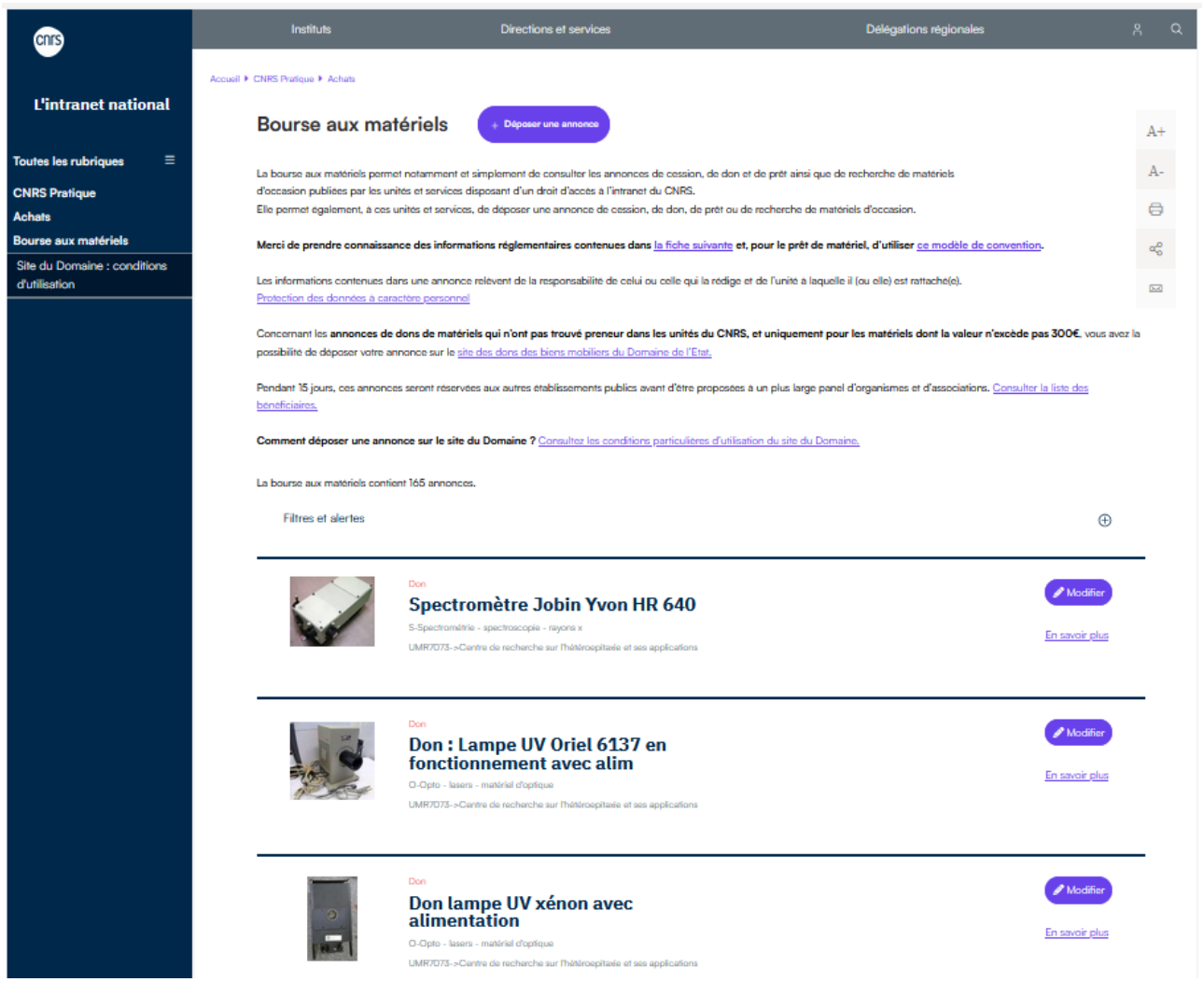


Figure 6 : Bourse aux matériels

3.2 AUTRES EXIGENCES FONCTIONNELLES

3.2.1 Recherche

Chaque application doit disposer d'un moteur de recherche efficace portant sur tous les types de contenu de l'application (exemples : pages HTML, actualités, documents (pdf compris), tags…).

Si le titulaire propose un composant pour l'indexation et la recherche, comme Elastic ou Solr, il s'assurera que :

- Les performances de la recherche sont satisfaisantes pour l'utilisateur
- L'application est robuste à la perte de ce composant de recherche
- La mise en œuvre du composant de recherche pour une application ne peut pas dégrader la fonctionnalité de recherche des autres applications.

3.2.2 Traduction

Les applications actuelles ne sont pas traduites en anglais.
Les refontes ne doivent pas comprendre la traduction pour leur mise en service, mais l'apport de la traduction doit être prévu dans un second temps.

Si certains éléments peuvent être traduits via un service d'IA qui respecte les exigences IA du CCTP, certains, selon leur niveau de sensibilité, ne pourront pas être traduits par un service d'IA en SaaS.

3.2.3 Mutualisation et homogénéité

Lorsque cela s'y prête, il faut privilégier au maximum la mutualisation/réutilisation de modules ou de code spécifique. Par exemple, l'intranet du CNRS comporte des intranets des délégations régionales, des intranets d'instituts et des intranets de directions fonctionnelles. Ces intranets doivent respecter la même charte et la même arborescence, avec des contenus spécifiques.

Dans le cadre de certaines applications complexes, comme l'intranet du CNRS, il faut également prévoir du partage de contenu entre les différents « sous-sites » ou « intranets ». Mais a priori il n'y aura pas de partage de contenu entre les différentes applications.

Les relations avec d'autres composants du SI, comme par exemple l'authentification SAML pourront certainement donner lieu à des mutualisations (a minima au niveau du code source).

Le titulaire proposera des solutions homogènes pour toutes les applications (par exemple les composants du backoffice doivent être homogènes quel que soit le périmètre des contributeurs : pour l'intranet CNRS, quelle que soit la rubrique nationale, l'institut ou la délégation régionale).

3.3 INTÉGRATION DANS LE SI

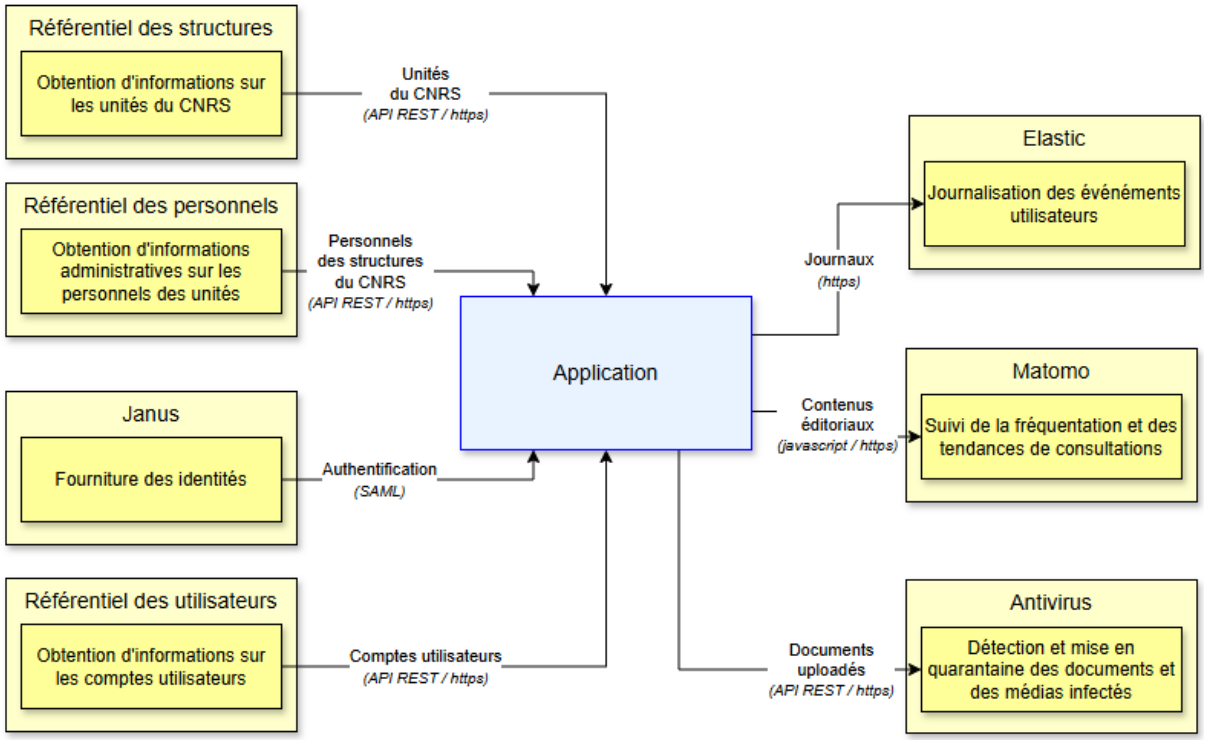


Figure 7 : Intégration dans le SI

Les applications à développer par le titulaire doivent s'intégrer avec d'autres applications du SI du CNRS :

- **Référentiel des structures** pour obtenir des informations sur les unités du CNRS (données issues de *Réséda Structure*) au travers d'une API REST.
- **Référentiel des personnels** pour obtenir des informations administratives sur les personnels des structures du CNRS (données issues de *Réséda Personnel*) au travers d'une API REST.
- **Janus** pour assurer l'authentification centralisée à la solution au travers du protocole SAML.
- **Référentiel des utilisateurs** pour assurer le provisionnement et le dé-provisionnement des comptes utilisateurs et de leurs accès (données issues de *IAM* et de *Sésame*) au travers d'une API REST.
- **Elastic** pour journaliser les traces et les événements liées à l'utilisation de la solution.

    - **Nota bene :** cette plateforme Elastic du CNRS est réservée à la journalisation des traces et ne pourra pas être utilisée comme composant Elastic pour l'indexation et la recherche. Si ce choix est pris dans la solution du titulaire, il faudra une brique dédiée supplémentaire.

- **Matomo** pour suivre la fréquentation de la solution par ses utilisateurs au travers d'une intégration de code Javascript dans l'application cible.
- **Protection au téléchargement contre les menaces de cyber sécurité (appelé Web Service Antivirus)** pour détecter et mettre en quarantaine tout document ou ressource multimédia touché par une infection virale au travers d'une API REST. Il s'agit d'une analyse comprenant une émulation de menace pouvant durer plusieurs secondes voire quelques minutes. La solution doit gérer les réponses intermédiaires de l'antivirus en relançant automatiquement des appels à l'API **en tâche de fond**, jusqu'à finalisation de l'analyse, afin de ne pas bloquer l'utilisateur durant le délai d'analyse.
    - Si la solution permet l'utilisation du protocole ICAP, il est possible d'utiliser directement ICAP plutôt que l'API REST du Web Service Antivirus.
    - Le titulaire doit proposer une stratégie pour gérer cette attente, en contraignant au minimum l'utilisateur et avec pour cible de ne téléverser le fichier sur le serveur qu'une fois l'analyse terminée et concluante. Sinon une justification de la solution est fournie.

L'hébergement de ces autres applications est réalisé sur un cloud privé (IaaS) fourni par le CNRS. Cet hébergement, l'exploitation, l'administration et le MCO de ces applications sont exclus du présent accord-cadre.

L'intranet doit par ailleurs s'interfacer avec 2 autres applications :

- **DAM** (Digital Asset Management basé sur *Keepeek*) pour obtenir des ressources multimédias à intégrer dans les contenus éditoriaux au travers d'une API REST (appelée directement ou via le module Drupal de Keepeek). Le DAM doit faire office de référentiel en lecture seule.
    - Drupal ne pourra pas alimenter le DAM.
    - Le titulaire prévoit plusieurs bibliothèques de media dans sa solution DRUPAL pour stocker séparément les données provenant du DAM de celles gérées localement, comme les vignettes générées par Drupal.
- **Plateforme marketing** (basé sur *Brevo*) pour élaborer des newsletters à partir des contenus éditoriaux publiés sur la solution au travers d'une API REST ou d'un Data Feed Brevo.

Ces deux applications en mode SaaS font l'objet de marchés spécifiques, en dehors du présent accord-cadre.

3.4 CONDUITE DU CHANGEMENT

Suite au développement des refontes des applications et à la reprise des données, et avant la mise en service des applications, il sera potentiellement demandé des prestations de conduite du changement.

Cela consistera par exemple :
- A produire des manuels d'utilisateurs pour les contributeurs, pour les approbateurs
- A élaborer des formations pour les contributeurs d'une application
- A animer des sessions de formations.

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.

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
URB_103	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 et le titulaire font valider le périmètre fonctionnel et informationnel de la solution par l'équipe urbanisation de la DSI.
URB_104	Lors de la conception et de la réalisation de la solution, les architectures transverses nationales et pilotées par la DSI 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.
URB_105	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 services utilisables par d'autres applications.
URB_106	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).'

4.1.2 Echanges 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, JSON, 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 l'application (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 l'application, 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 l'application.

Cependant dans le cas où certains flux entrants sont à développer par le CNRS pour les besoins spécifiques de la solution, le 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
URB_107	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.
URB_108	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.
URB_109	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).
URB_110	Les échanges entre la solution et le reste du SI se font via des formats pivots.
URB_111	Les formats pivots non fournis par le CNRS sont 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).
URB_112	Les formats pivots sont facilement évolutifs en limitant les impacts sur leurs usages déjà en cours.
URB_113	La description des formats pivots spécifiquement développés pour le CNRS respecte un formalisme prescrit par la DSI du CNRS.
URB_114	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.
URB_115	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.
URB_116	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.
URB_117	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 est étudiée et validée entre le titulaire et le CNRS (équipes projet et transverses).
URB_118	La solution expose toute la population des objets métier dont elle est maîtresse, avec le contenu complet du format pivot, y compris les règles de diffusion, et le niveau de sensibilité. Autrement dit, la solution ne fait aucune restriction sur l'exposition des objets métier qu'elle gère.

Référence	Libellé exigence
URB_119	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 (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). - une sélection d'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).
URB_120	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.

4.1.2.2 Modalités d'implémentation

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

Référence	Libellé exigence
ECH_101	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.
ECH_102	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.
ECH_103	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.
ECH_104	La fréquence des échanges de données se fait selon un mode "fil de l'eau" différentiel (plage modulable) ou complet sur validation du CNRS.
ECH_105	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/interoperabilite) gouverne le choix des formats.
ECH_106	L'encodage des données échangées est UTF-8. En cas d'impossibilité, le choix de l'encodage est étudié et validé entre le titulaire et le CNRS.
ECH_107	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. SSI_CRYPT_101) 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-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_108	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.
SSI_COM_102	Les seuls flux entrants de production (hors flux techniques, ex. : DNS, ESB, etc.) légitimes sont les suivants : - Reverse proxy --> Serveur d'application - Serveur d'application --> Serveur de base de données
SSI_COM_103	Il existe une matrice de flux bilatéraux documentée et tenue à jour pour l'ensemble des serveurs et des postes clients impliqués dans la solution. Cette matrice de flux est techniquement implémentée sur des dispositifs de filtrage (pare-feux). Les flux non explicitement déclarés dans la matrice de flux sont techniquement interdits.
SSI_COM_104	Pour tous les types de flux, la confidentialité des données transmises est garantie par des moyens techniques décrits dans la documentation.

Référence	Libellé exigence
SSI_COM_105	Pour tous les types de flux, l'intégrité des données transmises est garantie par des moyens techniques décrits dans la documentation.
SSI_COM_106	Pour tous les types de flux, l'unicité des requêtes est garantie pour éviter les attaques par rejeu par des moyens techniques décrits dans la documentation.
SSI_COM_107	Pour les flux d'échange entre applications, l'identité du client et du serveur de communication est garantie par des moyens décrits dans la documentation.
SSI_COM_108	L'authentification des appels à un service web est réalisée par des mécanismes permettant de garantir la confidentialité des identifiants. Les moyens techniques utilisés sont décrits dans la documentation.
SSI_COM_109	Les flux sortants initiés depuis les serveurs de la solution sont limités au strict nécessaire. Lorsque ces flux sont établis vers une zone de sensibilité moindre (ex : SI usuel vers Internet, SI sensible vers SI usuel), ils passent obligatoirement par des serveurs mandataires spécifiques (ex : relais SMTP, DNS, NTP ou serveur mandataire HTTP). Ces serveurs assurent la rupture protocolaire et contrôlent la conformité et la destination des flux. Ils sont situés dans des zones réseaux cloisonnées et dédiées à cet usage (type DMZ). Les moyens techniques utilisés sont décrits dans la documentation. Précision : cette règle est valable quelles que soient les modalités d'hébergement et les maîtres d'œuvre.
SSI_COM_110	Les connexions VPN site à site sont effectuées en VPN IPSEC. Précision : se référer au RGS 2.0 annexes B1, B2 et B3 pour les versions des protocoles et algorithmes de chiffrement autorisés
SSI_COM_111	Les connexions VPN client à site sont effectuées en VPN IPSEC ou VPN SSL avec authentification du terminal et de l'utilisateur.
SSI_COM_112	L'émission de messages de type email par la solution doit être contrôlée afin d'éviter le détournement de la fonction (spam ou diffusion de contenu malveillant) : - L'émetteur doit être fixé de façon fiable sur une adresse et un nom d'expédition n'autorisant pas de réponse (« no-reply ») et identifiant clairement l'application émettrice. - La liste des destinataires doit également être maîtrisée (ex : listes pré-établies ou listes de diffusion, domaines cibles en liste blanche, nombre de destinataires limités etc.). - Le contenu des messages doit reposer sur des modèles préétablis et n'incluant pas de code pouvant être interprétés de façon détournée par les clients. A ce titre, l'envoi de messages au format « texte brut » et sans pièce jointe est à privilégier.

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,
- 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. § 2.3.3.3.1). Si plusieurs fournisseurs peuvent être choisis, un mécanisme de sélection du fournisseur d'identité est mis en place. Ce mécanisme peut être un service de découverte SAML.

Le choix du client SAML est proposé par le titulaire. Il peut être intégré à la solution, sous forme de plugin, ou externe. Le client SAML est un composant de sécurité qui doit être fiable et maintenu.

Pour les applications hébergées sur les infrastructures propres de la DSI du CNRS comme c'est le cas dans le présent accord-cadre, le CNRS peut mettre en place un service intégré de service provider (SP) SAML 2.0 et si besoin un service de découverte SAML, de technologie Shibboleth[2].

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

[2] Cf. définition dans le glossaire (cf. § **Erreur ! Source du renvoi introuvable.**)

- L'application délègue l'authentification des utilisateurs aux services d'authentification du CNRS (cf. § 2.3.3.3.1).
- Une fois le client SAML intégré à l'application, ce sont les fournisseurs d'identité qui se chargent d'authentifier l'utilisateur CNRS.
- L'authentification des utilisateurs par les services d'authentification CNRS est possible soit par identifiant/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 contenu du jeton est chiffré avec un certificat fournis par le titulaire.
- 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.
- Dans le cas où le service provider (SP) est fourni par la DSI du CNRS, ce dernier peut restreindre l'accès à l'application sur la base d'attributs retournés par le fournisseur d'identité. Si c'est la solution qui intègre le traitement de la réponse SAML, c'est à cette dernière de s'assurer des contrôles d'accès.
- Le critère d'accès effectué par les fournisseurs d'identité du CNRS est donc l'appartenance ou non de l'utilisateur au référentiel des utilisateurs du CNRS (cf. § 2.3.3.3.3).
- Dans le cas d'une gestion des droits déléguée à la brique d'habilitation des utilisateurs (cf. § 2.3.3.3.2), les rôles applicatifs peuvent être gérés et calculés de manière centralisée. Ces rôles applicatifs sont disponibles dans le référentiel des utilisateurs (cf. § 2.3.3.3.3). 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
AUTH_101	Dans le cas de comptes locaux, la solution comprend des fonctionnalités de gestion de ces comptes.
AUTH_102	Un service de découverte SAMLest mis en place lorsque le fournisseur d'identités CNRS n'est pas le seul fournisseur d'identité utilisé.
AUTH_103	Pour les personnels présents dans les unités du CNRS, l'origine des données pour la création et la modification des comptes utilisateurs est le référentiel des utilisateurs du CNRS.
AUTH_104	La modification d'un compte utilisateur dans la solution est effectuée via des services web ou via les systèmes d'intermédiation du CNRS.
AUTH_105	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.
AUTH_106	Le contrôle d'accès à la solution est renforcé sur la brique implémentant les échanges SAML avec les fournisseurs d'identité en utilisant des attributs spécifiques exposés dans la réponse SAML. 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 la solution. Ce contrôle s'ajoute mais ne se substitue pas aux contrôles de droits des utilisateurs réalisés par la solution.
SSI_AUTH_101	Lorsque la population utilisatrice est fédérée au sein du fournisseur d'identité CNRS (cas des utilisateurs des unités) ou de la fédération RENATER, la solution s'appuie sur ces services d'authentification pour l'authentification des utilisateurs.
SSI_AUTH_102	Lorsque la population utilisatrice n'est ni fédérée au sein du fournisseur d'identité CNRS (cas des utilisateurs des unités), ni de la fédération RENATER, les modalités de gestion des comptes permettent de garantir à tout moment : - la confidentialité des moyens d'authentification, - que seules les personnes légitimes disposent des accès. La gestion des comptes locaux lorsqu'elle est incontournable, est explicitement autorisée et documentée.

Référence	Libellé exigence
SSI_AUTH_103	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 et la transformation des mots de passe fait intervenir un sel aléatoire. Précisions : se référer au RGS 2.0 annexes B1, B2 et B3 pour les fonctions cryptographiques conformes.
SSI_AUTH_104	La création d'un compte utilisateur, hormis pour les fonctionnalités de type téléservice, pour accéder à la solution est effectuée par un mécanisme de provisioning (et non par saisie manuelle ou par création automatique sur demande de l'utilisateur directement dans la solution). Dans le cas de téléservice, la création automatique de compte à l'initiative de l'utilisateur est étudiée et validée entre le titulaire et le CNRS Précisions : 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 via les informations issues de l'authentification.
SSI_AUTH_105	Un mécanisme de gestion du cycle de vie des comptes utilisateurs de la solution est mis en place (y compris pour les comptes locaux le cas échéant). Précision : la gestion du cycle de vie inclut, entre autres, des mécanismes outillés d'ajout, de suppression, et de suspension de comptes et la possibilité de gestion d'une durée de vie pour les comptes
SSI_AUTH_106	La solution permet de définir différents rôles applicatifs selon les fonctions métier et les responsabilités des utilisateurs. Ces rôles applicatifs sont limités au strict nécessaire en application du principe du moindre privilège.
SSI_AUTH_107	Lorsque des comptes par défaut existent, la solution permet de les désactiver, les renommer, modifier le mot de passe ou les supprimer sans impact sur le service fourni.
SSI_AUTH_108	Les privilèges accordés aux comptes de service utilisés par la solution sont limités au strict nécessaire en application du principe du moindre privilège. Précision : il s'agit des comptes d'accès aux bases de données, au système de fichiers, etc.
SSI_AUTH_109	Des comptes d'administration dédiés (différents des comptes utilisateurs affectés aux personnels administrateurs techniques) sont les seuls utilisés pour réaliser les actions d'administration technique ou pour effectuer des diagnostics techniques.
SSI_AUTH_110	L'administration technique de la solution passe par un bastion d'administration assurant la traçabilité des actions.
HAB_101	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.
HAB_102	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).
HAB_103	La solution permet la désactivation des comptes utilisateurs.

4.2 EXIGENCES TECHNIQUES

4.2.1 Choix du CMS et de la base de données

Le titulaire sera force de proposition concernant l'architecture technique la plus adéquate pour répondre aux exigences du CNRS. Cette architecture sera validée en début de projet en concertation avec le CNRS.

La brique applicative centrale des solutions applicatives sera la solution open source Drupal. La version précise à intégrer sera déterminée au début de la phase de mise en œuvre du projet en concertation avec le CNRS.

Le choix des « thèmes » sera soumis à la validation du CNRS.

Le titulaire utilisera en priorité les modules contribués, supportés par la communauté Drupal, maintenus régulièrement, en veillant à en limiter le nombre. Les modules seront de préférence reconnus par la Security Team de Drupal.

Sur Drupal, une majorité de modules à jour techniquement, demeurent en version alpha ou bêta durant de longues périodes. Le CNRS accepte leur utilisation, même si l'objectif à terme n'est d'avoir que des modules « stables ».

Le choix des modules à intégrer est idéalement gouverné par :

- La réactivité de la communauté à l'origine du module (et sa taille)
- L'ancienneté du module et son historique en termes de sécurité
- Le rapport service rendu sur risque induit
- La facilité de mise à jour et l'impact sur la mise à jour des autres modules et du cœur Drupal. Certains modules étant plus structurant que d'autre, ou pouvant engendrer à terme des régressions et une dette technique.

Ces éléments sont présentés par le titulaire à l'appréciation du CNRS, afin d'éclairer son choix pour la liste des modules initialement proposés et pour chaque nouveau module proposé à l'intégration. En cas de refus par le CNRS, le titulaire propose un module alternatif pour le même service rendu. Le CNRS peut aussi décider d'abandonner la fonctionnalité.

Le titulaire veillera également à suivre les bonnes pratiques Drupal, notamment dans les développements spécifiques.

L'architecture Drupal proposée ne nécessitera pas l'usage de containers.

Pour la base de données, le choix du CNRS est PostgreSQL.

Les fichiers des pièces jointes sont stockés sur les disques de préférence à en base de données.

Le titulaire produira les configurations de tous les composants spécifiques aux applications Drupal comme les caches applicatifs Redis, ou les briques Varnish si jugés nécessaires pour la solution. Les documentations d'installations fournies par le titulaire permettront à l'équipe d'exploitation du CNRS de suivre la procédure malgré leur absence de connaissance sur ces briques.

4.2.2 Eléments techniques structurants

L'application est une application ouverte sur Internet, à des utilisateurs authentifiés, et accessible également via des dispositifs mobiles

4.2.3 Services d'infrastructure

4.2.3.1 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.

4.2.3.2 Caractéristiques système

Les exigences système suivantes doivent être respectées :

Référence	Libellé exigence
INF_101	Le serveur HTTP de référence est Apache sur Linux.
INF_103	Le système d'exploitation serveur de référence est Red Hat Enterprise Linux.

Référence	Libellé exigence
INF_104	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 : 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. Pour les progiciels PHP, l'utilisation des fonctions ci-dessus est limitée aux seules les fonctions strictement nécessaires au progiciel sont autorisées.

4.2.3.3 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
INF_105	Les flux entre les postes clients et le(s) serveur(s) applicatif(s) passent par une DMZ avec rupture de flux effectuée par exemple par des reverse proxy.
INF_106	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.
INF_107	La compatibilité IPv6 est assurée de façon native. En production, les communications se font en IPv4 sauf décision expresse du CNRS.

4.2.3.4 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
INF_108	La solution répond au besoin de disponibilité exprimé, de la manière la plus sobre possible.
INF_109	Une politique de sauvegarde est définie en fonction des besoins, et est restreinte au strict nécessaire.
INF_110	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.
INF_111	L'application est compatible avec un environnement d'exécution durci selon les règles définies par le CNRS, ces règles sont issues des profils SCAP d'une version 1.3 ou supérieure publiées par le NIST pour les systèmes d'exploitation.
SSI_EXP_101	La prise de main à distance d'un actif quelconque de la solution (serveur, actif réseau, poste de travail…) depuis l'extérieur passe par un VPN puis un bastion.

Référence	Libellé exigence
SSI_EXP_102	Les composants matériels et logiciels de la solution, incluant (liste non exhaustive) les appliances, équipements réseaux, systèmes d'exploitation, firmwares, hyperviseurs, middlewares et applications, produisent des traces exhaustives relatives aux activités de connexion, aux requêtes, aux actions et événements importants relatifs à la solution, quelle que soit la source (utilisateur, administrateur, scripts ou processus particulier), au niveau de détail requis par la réglementation.
SSI_EXP_103	Les traces générées par la solution sont dans un format structuré dont les champs couvrent a minima : - l'adresse IP ou la source à l'origine [en cas d'interaction distante] - le compte utilisateur ou processus associé - le libellé intelligible de l'évènement ou l'action - le code retour de l'action [option] - un identifiant unique de corrélation [option] - la taille de la requête [option]
SSI_EXP_104	Les traces générées par la solution sont horodatées de manière fiable et synchronisées sur une même source de temps en indiquant notamment le fuseau horaire si les traces ne sont pas établies en heure UTC.
SSI_EXP_110	Les traces générées par la solution sont stockées sur 12 mois glissants. Précision : l'effacement des traces plus anciennes est obligatoire.
SSI_EXP_105	Les traces produites par la solution sont exportées dès leur génération hors du système générateur, de manière fiable et intègre vers un système central de collecte en utilisant le serveur syslog local au serveur qui aura en charge ce transfert vers un séquestre. Un client Elasticsearch sera également installé sur le serveur pour permettre la consultation de ces traces.
SSI_EXP_106	Toutes les montées de versions mineures pour les OS serveurs, 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.
SSI_EXP_107	Les ressources matérielles et logicielles composant la solution sont intégrées dans un processus de veille en vulnérabilités et correctifs pendant la durée de vie de la solution. Précision : cette exigence porte sur l'existence d'un processus de veille en vulnérabilités. Pour être conforme à l'exigence, le processus de gestion de vulnérabilité est connu, documenté et appliqué.
SSI_EXP_108	Des moyens d'administration dédiés sont utilisés pour réaliser les actions d'administration technique ou pour effectuer des diagnostics techniques. Précision : les moyens d'administration incluent les postes d'administration et leur environnement (VLAN, etc.)
SSI_EXP_109	Les configurations des matériels (inclus les solutions appliances les équipements réseau) et des systèmes (inclus les OS, les firmwares et les hyperviseurs) embarqués dans la solution sont durcies.
SSI_INF_101	Les sauvegardes sont déportées pour être suffisamment isolées du site de production.
SSI_INF_102	Les sauvegardes font l'objet de dispositions de protection physiques et logiques permettant d'assurer le même niveau de disponibilité, de confidentialité et d'intégrité que l'environnement de production.

4.2.3.5 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.

4.2.4 Architecture applicative

4.2.4.1 Normes d'architecture

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

Référence	Libellé exigence
DEV_101	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.
DEV_102	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.
DEV_103	L'usage de Java WebStart est interdit.
DEV_104	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.
DEV_105	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.
DEV_106	Le CNRS impose les technologies Web natives (HTML5, CSS3…) limitant les interactions avec le système d'exploitation et le respect des standards du W3C.
DEV_107	En plus du français, la gestion d'au moins une langue étrangère (l'anglais) est fournie.
DEV_108	Les libellés (messages d'erreur, champs, texte, ...) sont externalisés, soit en base soit via un fichier de propriétés. Par exemple, les nomenclatures ne sont pas stockées dans le code applicatif mais sont externalisées.
DEV_109	Toute émission de mails respecte 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. Le nombre maximum de mails envoyés par unité de temps est paramétrable au niveau de l'application
SSI_PCA_103	Les mécanismes de redondance et de haute disponibilité sont mis en œuvre sur les ressources de la solution le nécessitant pour répondre au besoin de disponibilité et de continuité de service de la solution.

4.2.4.2 Langages

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

Référence	Libellé exigence
DEV_110	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.
DEV_111	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.

Référence	Libellé exigence
DEV_112	Les frameworks de développement sont ouverts, éprouvés, avec une large communauté active, maîtrisés par le titulaire en charge de la réalisation de la solution, et permettent 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.
DEV_114	Pour une solution PHP, le framework utilisé est Symfony.
DEV_115	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.

4.2.4.3 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
DEV_116	Les développements sont modulaires afin de faciliter la maintenance et l'évolutivité du code.
DEV_117	Les erreurs sont traitées de manière à assurer la sécurité dans les développements (toutes les erreurs levées lors de l'exécution sont traitées en conséquence).
DEV_118	Les librairies 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.
DEV_119	La solution journalise des événements permettant l'audit des connexions effectuées à la solution, et le suivi des opérations importantes.
DEV_120	L'application utilise une librairie de logs qui permet de paramétrer la destination des événements de logs (par exemple syslog).
DEV_121	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.
DEV_122	Le paramétrage technique de la solution est réalisé au travers de fichiers de configurations qui sont stockés de manière indépendante du code applicatif.
DEV_123	Les tests unitaires sont automatisés, avec un taux de couverture minimum défini d'un commun accord entre tous les acteurs du projet. Ces tests s'exécutent sans erreur dans la forge du CNRS (les cas d'erreurs résiduels seront justifiés par le titulaire).

Référence	Libellé exigence
DEV_124	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.
DEV_125	Les codes sont documentés et lisibles. Les composants (modules, classes, méthodes) reposent sur une nomenclature de nommage normalisée et cohérente.
DEV_126	Pour les langages supportant les packages ou modules, les éléments de code source doivent être organisés avec le préfixe « fr.cnrs »
DEV_127	Au niveau OS, le jeu de caractères pour la solution est UTF-8.
DEV_128	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 offrent aux visiteurs toutes les performances techniques, visuelles et fonctionnelles définies par le cahier des charges et la maquette graphique, Dégradé : Les navigateurs permettent 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.
DEV_129	L'utilisation de Javascript est autorisée notamment pour fluidifier les échanges avec la solution, par exemple en effectuant des contrôles côté client. Cependant, ces contrôles côté client ne se substituent pas aux contrôles côté serveur qu'il faut impérativement réaliser.
DEV_130	Il est interdit de construire un framework Javascript.
DEV_131	L'architecture de services web recommandée est l'architecture de type REST.
DEV_132	L'outil de génération de PDF est open source, éprouvé, avec une large communauté active, et maîtrisé par le titulaire.
DEV_133	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.
DEV_134	Les éléments d'architecture critiques, complexes ou difficiles à appréhender font l'objet de paragraphes spécifiques dans la documentation permettant leur bonne compréhension.
DEV_135	Les dossiers d'architecture technique, les 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.
DEV_136	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 (exemple : activation du debug, paramétrages d'envoi de mails, etc.). Les propriétés de l'environnement sont renseignées sur l'instance déployée et facilement modifiables (exemple : fichier unique à modifier au moment du déploiement)
DEV_137	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).
DEV_138	Le développement (code et organisation de page) est conçu en accord avec les règles d'accessibilité du RGAA.
DEV_139	Éviter au maximum l'utilisation de tables pour gérer la mise en forme dans le code HTML.

4.2.4.4 Gestion du cache applicatif

La mise en place d'un cache applicatif côté backend de la solution DRUPAL est souhaitée (comme avec l'utilisation de Redis par exemple), afin d'optimiser les performances des requêtes vers la base de données.

Il est également préférable d'avoir une ségrégation des briques de gestion du cache en backend par application afin de conserver de la robustesse d'une application vis-à-vis des autres.

4.2.4.5 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

Le CNRS encourage toute initiative du titulaire pour utiliser un outil d'analyse et de mesure d'écoresponsabilité du code produit, et fournir des indicateurs associés.

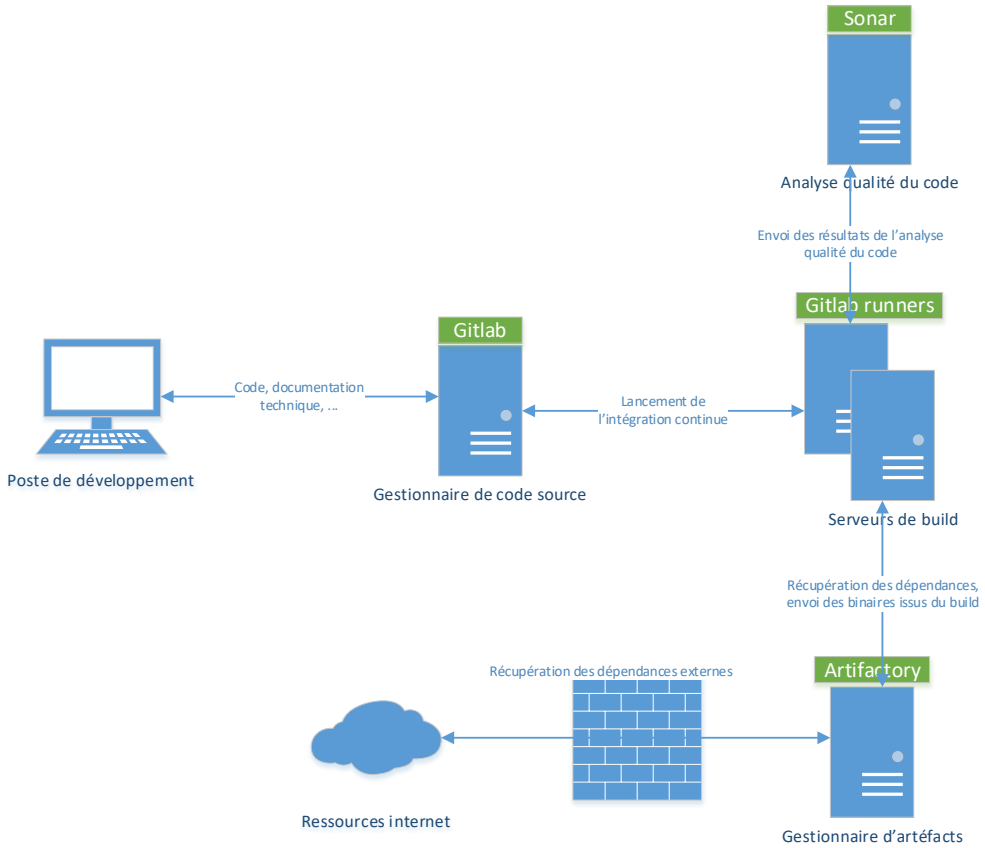


Figure 8 : Présentation de la forge logicielle

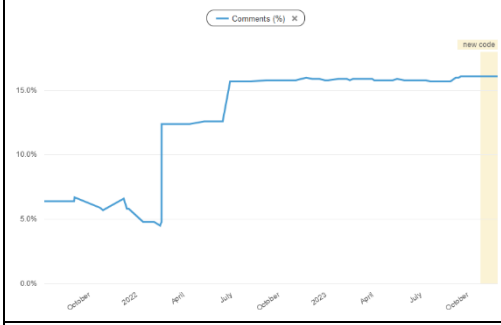
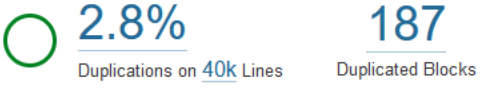
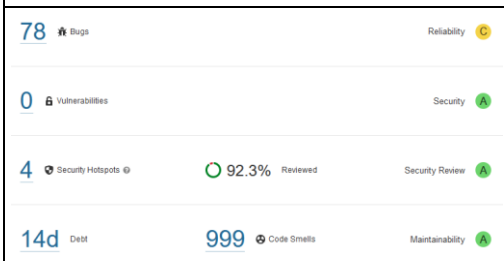
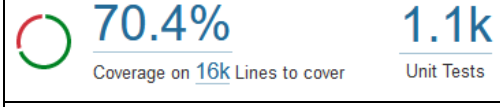
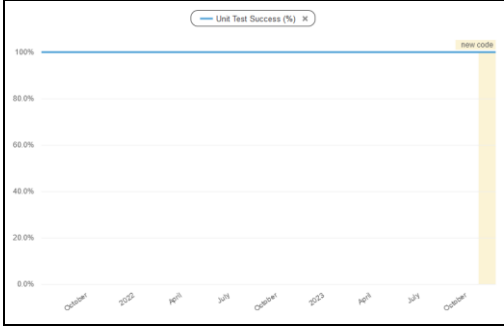
Le titulaire doit utiliser la forge de développement de la DSI du CNRS pour :
- Avoir la totalité du code source développé par le titulaire dans la forge DSI (Gitlab)
- S'il y a un besoin d'intégration continue, elle est réalisée dans la forge DSI avec Gitlab CI.

Le CNRS utilise l'outil Ansible 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	*Le seuil sera défini au lancement du projet*
	Duplication de code	*Le seuil sera défini au lancement du projet*
	Respect des règles de codage, problèmes potentiels de sécurité	Pas d'anomalies de niveau « blocker et « critical ». Analyser les majeures. Pas de vulnérabilités.
	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).

En amont de la première livraison de la première version de la première application/portail à déployer, le titulaire aidera le CNRS pour adapter la forge pour les besoins spécifiques liées à la technologie DRUPAL. Il s'agira par exemple de prévoir les runners Gitlab et Artifactory avec Composer, adapter les pipelines, configurer Sonar…

Le titulaire prévoit une solution permettant un déploiement sur chacun des environnements (développement, intégration, recette et production) et gérant les spécificités des configurations de chacun.

La forge du CNRS sera ensuite utilisée par le titulaire et le CNRS pour les livraisons et déploiement de chaque version.

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

Référence	Libellé exigence
DEV_140	Le titulaire choisit l'outil de développement intégré (IDE) dont il a la maitrise. Celui-ci est maintenu.

Référence	Libellé exigence
DEV_141	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 librairies 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.
DEV_142	JMeter est l'outil préconisé pour les tests de charge, si un autre outil est proposé il est ouvert, éprouvé, avec une large communauté active, et maîtrisé par l'équipe en charge de son utilisation.
DEV_143	Un moteur de production est utilisé afin de gérer les dépendances de la solution, le lancement des tests automatisés, sa construction, la publication des artéfacts sur un gestionnaire d'artéfacts, … Pour les projets Java, Maven est utilisé. Pour les projets PHP sous Symfony, Composer est utilisé.
DEV_144	Le nommage des artéfacts générés par la phase de construction de la solution suit les normes de nommage standard (par exemple Maven pour les projets Java, Composer pour les projets PHP).
DEV_145	Le gestionnaire de source Git est utilisé pour la gestion des codes sources. Le CNRS dispose d'un outil de gestion de code source dans lequel se trouve le code source de la solution (soit en posant les commits directement dans le dépôt Git 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).
DEV_146	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.
DEV_147	Un modèle de gestion des branches Git est utilisé (par exemple Gitflow) en accord avec le CNRS.
DEV_148	Le CNRS dispose d'un outil d'analyse statique de code source, 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 celui du CNRS. 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 d'analyse statique du code du CNRS et analysés ensuite, sont définis au démarrage du projet.
DEV_149	Le CNRS dispose d'un outil d'intégration continue, utilisé a minima pour lancer l'analyse via l'outil d'analyse statique du code. De manière générale, la solution est construite par cet outil d'intégration continue. Le code source contient un fichier 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.
DEV_150	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.
DEV_151	La livraison et l'installation de la solution est réalisée de façon outillée et automatisée en évitant toute opération manuelle (sauvegarde système, actions en base de données, mise à jour de fichiers, …). L'application est conçue de telle manière que sa livraison et son installation sont réalisables avec l'outil d'orchestration du CNRS. Le cas échéant, l'outillage écrit pour réaliser cette tâche est également géré dans l'outil de gestion de code du CNRS.
DEV_152	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.
DEV_153	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.

Référence	Libellé exigence
DEV_154	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.
DEV_155	Dans le cadre d'un développement spécifique, une licence logicielle est choisie par le CNRS conformément à ses besoins. Une référence à cette licence apparait dans chaque fichier source produit.
SSI_DEV_101	L'administration fonctionnelle de la solution est réalisée par une IHM spécifique, si possible dédiée. Elle ne nécessite pas de connexions en SSH ou d'actions nécessitant une console (ex : récupération de logs récurrente, édition de fichiers de paramétrage pour lancer une campagne, etc.).
SSI_DEV_102	Les configurations des middlewares et des logiciels embarqués dans la solution sont durcies. Précision : les guides de durcissement des éditeurs et constructeurs et les guides de durcissement de l'ANSSI sont à appliquer.
SSI_DEV_103	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.
SSI_DEV_104	Lorsque la solution propose une fonction de téléversement de fichier (upload), le contrôle du type MIME du fichier téléversé est effectué (sans faire confiance ni à l'extension du fichier ni aux entêtes HTTP reçues). Le fichier est refusé s'il n'est pas conforme à des attendus de type MIME prédéfinis. Les moyens techniques utilisés sont décrits dans la documentation.
SSI_DEV_105	Lorsque la solution propose une fonction de téléversement de fichier (upload), le contrôle de la taille du fichier téléversé est effectuée. Le fichier est refusé s'il n'est pas conforme à des attendus de taille prédéfinis. Les moyens techniques utilisés sont décrits dans la documentation.
SSI_DEV_106	Lorsque la solution propose une fonction de téléversement de fichier (upload), la vérification de la présence de logiciels malveillants est réalisée. La présence d'un code malveillant implique la suppression du fichier concerné. Les moyens techniques utilisés sont décrits dans la documentation.
SSI_DEV_107	Lorsque la solution propose une fonction de téléversement de fichier (upload), le nom du fichier téléversé ne comporte pas de données à caractère personnel et n'est pas prédictible.
SSI_DEV_108	La solution intègre des mécanismes de sensibilisation (encarts, popups ou bandeaux sur les interfaces utilisateur) dès lors que les services fournis par la solution ou les données traitées par la solution font état d'une sensibilité particulière.
SSI_DEV_109	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. Les constats issus de ces audits sont tous traités de manière proportionnée au risque induit et font l'objet d'un plan d'action formalisé.
SSI_DEV_110	Le cycle de développement inclut des phases régulières de revues des vulnérabilités liées aux dépendances logicielles. Les constats issus de ces revues sont tous traités de manière proportionnée au risque induit et font l'objet d'un plan d'action formalisé.
SSI_DEV_111	Le processus de développement inclut des dispositions bloquant les mises en production d'un code présentant des vulnérabilités ayant un impact significatif sur la sécurité des données.
SSI_DEV_112	Le processus de développement inclut des dispositions permettant de prendre en compte les vulnérabilités résiduelles du code mis en production (dette sécurité).
SSI_DEV_113	Toute saisie utilisateur est vérifiée côté serveur en conformité avec le format, la taille, la sémantique et le type de données attendu.

Référence	Libellé exigence
SSI_DEV_114	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.
SSI_DEV_115	Les identifiants de session utilisateur sont aléatoires.
SSI_DEV_116	Les informations liées à l'authentification, l'autorisation, l'habilitation des utilisateurs ne sont jamais passées en paramètres des URL.
SSI_DEV_117	Les bannières de connexion et les messages d'erreur applicatifs sont présentés à l'utilisateur en masquant toute information technique divulguant les composants de la solution et leurs versions.
SSI_DEV_118	La solution ne récupère pas de code externe (en dehors de sa phase de construction), sauf si la dépendance a été définie explicitement, intégralement et statiquement dans son code.
SSI_DEV_119	La solution met en œuvre des mécanismes de protection contre les différents types d'injection de données ou formats non attendus dans la solution (ex: injections SQL, modification de requêtes LDAP, modification d'arguments ou paramètres d'exécution d'un exécutable etc.)
SSI_DEV_120	Les composants logiciels utilisés pour le développement (inclus les bibliothèques de développement, l'environnement de développement, les outils de compilation et d'interprétation, etc.) disposent d'un historique clair et vérifiable de leurs vulnérabilités et ne présentent pas de faille non corrigée à la date de l'implémentation.

4.2.5 Base de données

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

Référence	Libellé exigence
BDD_101	Une base de données (relationnelle ou non relationnelle si c'est pertinent) est utilisée pour gérer la persistance des données.
BDD_102	Les solutions de SGBD de référence sont PostGreSQL et MongoDB (dans ce cas uniquement pour des données non structurées).
BDD_103	La non adhérence au SGBD est assurée, les requêtes ne sont pas implémentées directement dans le code applicatif (batchs compris), ni au travers de procédures stockées. 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.
BDD_104	Au niveau SGBD, le jeu de caractères utilisé est UTF-8
BDD_105	Tous les objets de la base de données sont documentés.

4.2.6 Engagements de qualité de service pour l'application

4.2.6.1 Disponibilité

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

Pour le déploiement d'une nouvelle version applicative ou toute opération de maintenance d'un composant logiciel, l'interruption de service acceptable est de 4h en continu une fois par mois (en production).

4.2.6.2 Intégrité

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

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.

4.2.6.3 Performances (temps de réponse)

Le temps d'affichage d'une ressource (page, requête de recherche, etc.) doit être inférieur ou égal à 5 secondes dans 98% des cas et inférieur à 3 secondes dans 50% des cas.

Ce temps de réponse est mesuré sur un échantillonnage défini conjointement avec le CNRS au démarrage du projet, à partir d'un poste de supervision hébergé sur le même réseau en amont du reverse proxy.

Si des cas particuliers dérogent à cette règle, ils doivent faire l'objet d'un accord explicite du chef de projet DSI.

Le titulaire fournit au CNRS :

- des éléments de dimensionnement de la plate-forme de production pour garantir un niveau de performance conforme au besoin en regard des éléments de volumétrie disponibles, tout en respectant les principes d'écoresponsabilité (pas de surdimensionnement) ;
- des éléments de tuning de la plate-forme 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 performance 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.

4.2.6.4 Charge

Le titulaire doit mettre en place des tests de charges afin d'ajuster les ressources frontales de la plateforme avant la mise en service d'une application.

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 afin de satisfaire au mieux les exigences d'accessibilité auxquelles tous les services Web d'un établissement public doivent se conformer (cf 2.1.4 Accessibilité numérique).

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.

Le développement des sites se fera de manière « responsive ». Seront pris en compte au moins : une version smartphone, tablette et écran HD.

4.3.1 Charte graphique

Le CNRS mettra à disposition du titulaire, la charte graphique du CNRS composée :

- d'un guide digital sous Figma, orienté sites web de communication externe, à titre d'exemple,
- d'un kit Bootstrap dédié au développement d'applications, accompagné d'un guide numérique le décrivant.

Le titulaire devra respecter précisément les fondamentaux, tout en étant force de proposition, créatif, pour aboutir à des interfaces conformes, innovantes et modernes.

Référence	Libellé exigence
ERG_101	L'interface de la solution respecte la charte du CNRS. Les éléments de base sont décrits dans le guide numérique du CNRS (couleurs, comportements, titrailles, boutons, navigation...).

Référence	Libellé exigence
ERG_102	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.
ERG_103	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.

4.3.2 UX/UI et règles d'ergonomie

L'arborescence des sites sera communiquée par le CNRS. Elle sera basée globalement sur la navigation des applications actuelles et pourra être adaptée en concertation avec le titulaire.

L'application est ergonomique, c'est-à-dire qu'elle est facilement utilisable, fonctionnelle et compréhensible par l'ensemble des utilisateurs, ce de manière aisée, déductible et conviviale. Le temps d'apprentissage pour les usagers, externes ou contributeurs, doit être réduit au minimum.

L'application accompagne l'utilisateur qui sait ce qu'il doit faire sur la page active. Il peut également pouvoir naviguer et se repérer dans l'ensemble de l'application. Pour cela, l'application utilise les systèmes de navigation les plus adaptés.

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 et clairement hiérarchisés.

La conception de l'IHM peut faire appel à des composants d'IHM innovants, *par exemple : effets de transition, de transparence, auto complétion, etc*. en restant vigilant toutefois à ne pas alourdir exagérément le poids des pages. Entre plusieurs composants rendant le même service, le choix sera guidé par des critères d'écoresponsabilité (poids du composant, consommation en ressources, pérennité et maintenabilité).

L'application est conçue de manière globale et homogène.

La solution doit comprendre des gabarits de pages qui contraignent les contributeurs de chacune des applications à respecter le RGAA au maximum.

Référence	Libellé exigence
ERG_104	La taille des fenêtres est adaptable à différentes tailles et résolutions d'écrans. Aucune fenêtre de la solution ne comporte d'ascenseur horizontal.
ERG_105	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).
ERG_106	Les titrailles et entêtes sont explicites et clairement structurées et hiérarchisées (utilisation de la feuille de style CSS et des balises h1, h2, etc.).
ERG_107	Les éléments de navigation sont clairs et explicites. Dans le cas d'arborescences complexes, un chemin de navigation apparaît.
ERG_108	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.).

4.3.1 Référentiel OPQUAST

Le titulaire poursuivra l'objectif de conformité au référentiel OPQUAST.

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
SSI_101	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, comptes 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.
SSI_103	Les environnements hors production (développement, intégration, essai, recette, école, pré-production, formation, etc.) n'utilisent pas les données et accès de production.
SSI_CRYPT_101	Seuls des protocoles de transport de données chiffrés sont utilisés. Précisions : 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
SSI_PDI_101	Un inventaire des ressources matérielles et logicielles composant la solution et de leurs versions est maintenu à jour.

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 autours 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 la génération de rapports sur les :

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

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 (CSRF) » ;
- les attaques pas « Server-Side Request Forgery (SSRF) » ;
- 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 ;
- les attaques liées à l'utilisations de composants applicatifs vulnérables ou obsolètes ;
- les risques de sécurité de l'OWASP Top 10 (https://owasp.org/www-project-top-ten/).

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 ;
- permettre l'intégration dès le développement de « Content Security Policy (CSP) » stricts ;
- un système de token par action serait un plus.

4.5 EXIGENCE D'INTÉGRATION DES OUTILS D'INTELLIGENCE ARTIFICIELLE

Aucune solution d'IA ne peut être implémentée sans l'autorisation expresse du CNRS.

Dans le cas où le candidat propose de l'IA, les exigences ci-dessous s'appliquent. De plus, le candidat décrit dans son offre son utilisation de l'IA dans chaque phase du projet (modèle IA utilisé – souverain ou non, type d'hébergement – on premise, cloud, localisation, sécurité souscrite pour l'IA…).

A noter que les applications actuelles n'utilisent pas d'IA.

Référence	Libellé exigence
SSI_IA_101	Les systèmes d'Intelligence Artificielle mis en œuvre dans la solution sont conformes aux réglementations en vigueur, notamment en ce qui concerne la traçabilité de leurs résultats et la documentation associée au modèle.
SSI_IA_102	Les jeux de données d'entraînement des systèmes d'Intelligence Artificielle mis en œuvre dans la solution sont protégés, par des moyens techniques ou de gouvernance, contre les attaques visant à manipuler le jeu de données (attaques dites par « empoisonnement des données »).
SSI_IA_103	La solution utilise des modèles open-source ou développés par des entreprises européennes.
SSI_IA_105	Le service IA est cloisonné afin d'empêcher les échanges d'informations avec les autres clients de la plateforme.
SSI_IA_106	Aucun appel n'est initié par l'IA de manière autonome sans le contrôle et l'autorisation explicite de l'utilisateur final.
SSI_IA_107	La solution propose : - pour une utilisation API, une politique de "Zero Data Retention" qui peut être désactivée sous dérogation après évaluation de la sensibilité des données et des réglementations en vigueur, - pour une utilisation conversationnelle (chatbot), toutes les données transmises par l'utilisateur sont supprimées quand l'utilisateur supprime la conversation.
SSI_IA_108	Sauf accord spécifique, toutes les données sont purgées régulièrement.
SSI_IA_110	L'indisponibilité du système d'IA n'a aucune incidence sur la disponibilité du service rendu.
SSI_IA_111	Par défaut, aucune interaction du SIA n'est autorisée avec le SI que ce soit en lecture ou écriture. Tout besoin d'interaction est validé par le CNRS.
SSI_IA_112	Le système d'IA est protégé en filtrant les entrées et les sorties des utilisateurs, et le cas échéant les actions de l'IA. Il est recommandé de mettre en place des fonctions permettant de se prémunir d'une fuite de données ou d'une fuite de modèle dans les réponses : - Une fonction de filtre de requêtes malveillantes des utilisateurs avant envoi au modèle ; - Une fonction de filtre de requêtes jugées non légitimes d'un point de vue métier ; - Une fonction de filtre d'informations internes du modèle (paramètres, entraînement) dans les réponses ; - Une fonction de filtre d'informations définies comme sensibles dans les réponses (ex. : coordonnées personnelles, références de projets, etc.); - Une limite sur la taille des réponses (nombre de caractères maximum).

4.6 PROTECTION DES DONNÉES PERSONNELLES

Le CNRS a mis en place des mesures et l'organisation pour respecter l'ensemble des exigences liées à la protection des données personnelles conformément aux dispositions de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et du règlement européen n°2016/679 sur la protection des données personnelles.

La politique de protection des données est pilotée par la Déléguée à la protection des données du CNRS, qui s'appuie pour sa mise en œuvre dans le présent accord-cadre notamment sur la Direction des systèmes d'information, la Direction de la communication, la Direction des ressources humaines et la Mission transverse d'appui au pilotage.

4.6.1 Organisation de la protection des données

Dans le cadre du présent accord-cadre, le CNRS est responsable des traitements de données personnelles. Ces derniers ont pour finalités :

- La gestion des sites intranet administrés par le CNRS : fourniture et publication de contenus, gestion du fonctionnement et de la sécurité du site, exploitation et maintenance (tierce maintenance applicative, gestion des profils et des accès) ;
- La gestion des identités ;
- La gestion des traces ;
- La gestion des référentiels Réséda.

Le titulaire intervient en qualité de sous-traitant pour le traitement des données nécessaires dans le cadre des prestations du présent accord-cadre définies au §1.1 Objet de l'accord-cadre.

Les données à caractère personnel correspondent :

- à des données d'identification
- à des données liées à la vie professionnelle
- à des données de connexion.

Les personnes concernées sont les personnes liées au CNRS (agents CNRS ou non), au titulaire, toute personne utilisant les sites intégrés dans le présent accord.

4.6.2 Obligation des parties

Chaque Partie s'engage à respecter l'ensemble des exigences liées à la protection des données personnelles conformément aux dispositions de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et du règlement européen n°2016/679 sur la protection des données personnelles.

Les Parties assurent et préservent la sécurité, la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes de traitement et des données personnelles et documents contenus dans le périmètre relevant de leurs attributions.

Le CNRS en tant que responsable de traitement inscrit le traitement de données personnelles dans le registre des traitements de données tenu par la Déléguée à la Protection des Données du CNRS.

Conformément aux dispositions de l'article 28 du RGPD et de l'article 60 de la loi Informatique et libertés, le sous-traitant s'engage à :

- traiter les données uniquement dans le cadre de la prestation ;
- traiter les données conformément aux dispositions de la prestation et à toute autre instruction du responsable du traitement. Dans l'hypothèse où le sous-traitant estimerait qu'une instruction documentée du responsable du traitement dans le cadre de la prestation pourrait être considérée comme illicite au regard du RGPD ou de la loi Informatique et libertés, il s'engage à en informer immédiatement le responsable du traitement, étant précisé que celui-ci sera seul juge de la validité des instructions données et que cette information ne saurait en aucun cas suspendre la bonne exécution de la prestation par le sous-traitant.

Le titulaire tient un registre des traitements des données qu'il opère pour le compte du CNRS. Ce registre peut être consulté à tout moment par le CNRS, ou par l'autorité de régulation compétente (Commission nationale de l'informatique et des libertés – CNIL).

Les Parties se communiquent le nom et les coordonnées de leur délégué à la protection des données respectivement désigné.

Les Parties s'engagent à coopérer avec les autorités de protection des données compétentes, notamment en cas de demande d'information ou de contrôle.

Chaque Partie demeure responsable des dommages qui lui seraient imputables concernant la protection des Données à caractère personnel faisant l'objet d'un traitement dans le cadre de l'exécution des Prestations (ex : fuite ou perte de données, intrusion informatique, etc.).

Le titulaire s'engage à mettre en œuvre une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement et atténuer les éventuelles conséquences négatives d'une faille de sécurité.

Il met à la disposition du CNRS toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits par le CNRS ou tout auditeur dûment mandaté par lui.

Référence	Libellé exigence
DCP_001	Le titulaire a mis en place une politique de protection des données personnelles conformément à la réglementation en vigueur
DCP_002	Le titulaire a désigné un délégué à la protection des données, chargé de piloter la politique de protection des données.

Référence	Libellé exigence
DCP_003	Le titulaire tient un registre des traitements de données à caractère personnel qu'il opère pour le compte du CNRS. Ce registre peut être consulté à tout moment par le CNRS, ou par tout prestataire d'audit désigné par le CNRS, ou par l'autorité de régulation compétente (Commission nationale de l'informatique et des libertés – CNIL).

4.6.2.1 Formation des personnels

Référence	Libellé exigence
DCP_004	Le titulaire doit assurer la formation de ses personnels à la protection des données personnelles. Il communique chaque année au CNRS la liste des formations dispensées (nature, dates).

4.6.2.2 Confidentialité

Les données exploitées et hébergées sont, pour partie des données à caractère personnel dont la sensibilité est forte au sens de la règlementation sur la protection des données personnelles.

Référence	Libellé exigence
DCP_005	Le titulaire veille à ce que les personnels autorisés à traiter les données à caractère personnel s'engagent à en respecter la confidentialité ou soient soumis à une obligation légale appropriée de confidentialité et reçoivent la formation nécessaire en matière de protection des données à caractère personnel. Le titulaire s'engage à n'utiliser et ne conserver les données transmises que pour les seules finalités définies dans l'accord-cadre.

4.6.3 Information des personnes et traitement des demandes d'accès aux données

Il est convenu que le CNRS est seul tenu de l'obligation de fournir aux personnes dont les données sont traitées l'ensemble des informations requises par les articles 13 et 14 du RGPD.

Par ailleurs, il est tenu du traitement des demandes des personnes concernées par ces traitements dans le cadre de l'exercice de leurs droits conformément aux articles 15 et suivants du RGPD.

Le titulaire s'engage à apporter son aide et communique toute information dont le CNRS aurait besoin pour s'acquitter de ces obligations.

Référence	Libellé exigence
DCP_006	Le titulaire ne peut, de sa propre autorité, rectifier, supprimer ou restreindre le traitement des Données à caractère personnel traitées pour le compte du CNRS, sauf sur instructions écrites du CNRS.
DCP_007	Le titulaire informe le CNRS dans les plus brefs délais (et en tout état de cause dans les cinq jours ouvrables suivant sa réception) de toute communication reçue d'une Personne concernée concernant les droits de cette Personne concernée d'accéder, de modifier ou de corriger les Données à caractère personnel et de se conformer à toutes les instructions du CNRS en réponse à ces communications.

4.6.4 Recours à des sous- traitants

Référence	Libellé exigence
DCP_008	Lorsque le titulaire fait appel à des sous-traitants au sens des articles 4 et 28 du RGPD, les dispositions qui lui sont applicables le sont automatiquement à ces sous-traitants. Une contractualisation adaptée est établie entre le titulaire et ses sous-traitants conformément à l'article 28 du RGPD.
DCP_009	Le titulaire s'assure que ses sous-traitants présentent les garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences des dispositions en vigueur en matière de protection des données personnelles pour le présent accord-cadre.

DCP_010	Le titulaire communique au CNRS la liste exhaustive des sous-traitants auxquels il fait appel pour la réalisation des prestations du présent accord-cadre. Il indique les noms et coordonnées des sociétés, l'objet de la prestation, les finalités de traitement, les catégories de données concernées, les lieux d'hébergement des données.
DCP_011	En cas de changement de sous-traitant ayant un impact sur les données à caractère personnel au titre du présent accord-cadre, le titulaire le notifie au CNRS avant le début des prestations. Le CNRS peut s'opposer à ce que le titulaire utilise ledit nouveau sous-traitant en notifiant le titulaire par écrit dans les dix (10) jours ouvrables suivant la réception de la notification du titulaire conformément au mécanisme décrit ci-dessus. Si le CNRS estime que le sous-traitant proposé ne satisfait pas au critère du présent accord-cadre, le titulaire propose sans surcoût au CNRS un nouveau sous-traitant qui respecte les contraintes du présent accord-cadre. Si le titulaire n'est pas en mesure de mettre à disposition une telle modification dans un délai raisonnable, qui ne doit pas dépasser trente (30) jours, le CNRS pourra résilier le présent accord-cadre uniquement pour les Services qui ne peuvent pas être fournis par le titulaire sans l'utilisation dudit nouveau sous-traitant en fournissant une notification écrite au titulaire.
DCP_012	Le recours à des sous-traitants ne dégage aucunement le titulaire de ses responsabilités au titre de l'exécution des prestations.

4.6.5 Durée de conservation des données et archivage

Référence	Libellé exigence
DCP_013	Aucune donnée personnelle n'est conservée au-delà de la fin de l'accord-cadre (hors cas particulier des données de logs et archivages).
DCP_014	Le long de la durée de l'accord-cadre, les données de logs et d'archivages conservées respectent les dispositions définies par le CNRS.
DCP_015	Le long de la durée de l'accord-cadre, le titulaire supprime les comptes administrateurs sur demande du CNRS. Les données associées aux comptes administrateurs sont supprimées. Le titulaire fournit, sur demande du CNRS, la preuve confirmant les suppressions de ces comptes administrateurs et des données associées.

4.6.6 Destruction, réversibilité

Référence	Libellé exigence
DCP_016	Lors de la résiliation ou à l'expiration de l'accord-cadre, ou sur demande écrite du CNRS à n'importe quel moment que ce soit, le titulaire devra, à ses propres frais, détruire tous les documents, et tout autre support pouvant contenir des Données personnelles, sans conserver aucune partie ou copie de ceux-ci. Un bordereau d'élimination devra être établi.
DCP_017	Le titulaire fournit au CNRS un Certificat de destruction des Données à caractère personnel sous une forme acceptable pour le CNRS, signé par un employé du titulaire qui a supervisé cette destruction.
DCP_018	Aucune copie ni doublon des Données à caractère personnel ne seront créées à l'insu du CNRS.

4.6.7 Analyse d'impact sur la vie privée

Référence	Libellé exigence
DCP_019	Le titulaire collabore avec le CNRS pour la réalisation des analyses d'impact sur la vie privée.

4.6.8 Exigences de sécurité

Référence	Libellé exigence
DCP_020	Le titulaire s'oblige à prendre toutes précautions utiles afin de protéger les données contre toute destruction accidentelle ou illicite, perte, altération, diffusion et de garantir que les données ne soient déformées, endommagées ou communiquées à des personnes non autorisées. Le titulaire s'engage à mettre en œuvre une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement et atténuer les éventuelles conséquences négatives d'une faille de sécurité. Il met à la disposition du pouvoir adjudicateur toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits par le pouvoir adjudicateur ou tout auditeur dûment mandaté par lui. Le titulaire fournit un Plan Assurance Sécurité (PAS) qui intègre les dispositions pour la protection des données personnelles. Le titulaire prend les mesures de sécurité adaptées conformément aux exigences de sécurité du CNRS.

4.6.9 Traitement des incidents impactant les données à caractère personnel

Référence	Libellé exigence
DCP_021	Dès lors que dans le cadre d'un incident de sécurité, il est constaté une violation avérée ou potentielle des données ou des traitements des données à caractère personnel, le titulaire communique au CNRS dans les meilleurs délais, et sous 24 heures au plus tard après en avoir pris connaissance, la survenance de cette faille ou violation de sécurité ayant (ou pouvant potentiellement avoir).
DCP_022	Une fois cette communication effectuée, le titulaire fournit au CNRS notamment toute information relative à la nature de la violation, au nombre de personnes concernées, aux catégories et au nombre d'enregistrements de données à caractère personnel concernés, ainsi qu'aux conséquences probables de la violation, aux mesures prises pour y remédier et atténuer les éventuelles conséquences négatives.
DCP_023	Les incidents, failles et violations liés aux données ou au traitement des données à caractère personnel constituent des incidents de sécurité dont la gestion doit en être conforme.
DCP_024	Dans le cas d'un incident de sécurité très sévère (tel que défini par la CNIL), et à la demande du CNRS, le titulaire doit missionner un tiers indépendant pour une évaluation et un audit d'urgence de la faille de sécurité, et fournir au CNRS une copie complète de ce rapport.
DCP_025	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.
DCP_026	Le niveau de priorité accordé aux incidents de sécurité impactant les données à caractère personnel est automatiquement le niveau le plus élevé.
DCP_027	Le CNRS notifie à la CNIL, dans les meilleurs délais et si possible dans les 72 heures, toute violation de données à caractère personnel, sauf si, en fonction notamment des éléments transmis par le titulaire sur ladite violation, elle n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes concernées.
DCP_028	Lorsque la violation des données est susceptible d'engendrer un risque élevé pour les droits et libertés, le CNRS notifie aux personnes concernées ladite violation dans les meilleurs délais conformément à la règlementation.

4.6.10 Audit

Référence	Libellé exigence
DCP_029	En complément des audits sécurité, le responsable du traitement dispose du droit de faire procéder à ses frais, par ses services ou tout tiers de son choix, à un audit du sous-traitant en vue de vérifier le respect par ce dernier de ses obligations au titre du présent document.

4.6.11 Coopération avec les autorités de contrôle

Référence	Libellé exigence
DCP_030	Le CNRS et le titulaire s'engagent à coopérer avec les autorités de protection des données compétentes, notamment en cas de demande d'information ou de contrôle.
DCP_031	Le titulaire informera le CNRS par écrit et dès que possible (mais au plus tard un (1) jour ouvrable à compter de la date d'une telle demande) de toute demande faite par un gouvernement, par un organisme chargé de l'application des lois et/ou des réglementations : – D'informations concernant le CNRS – D'accès aux Données Personnelles à moins que la notification au CNRS ne soit interdite par la réglementation Française. Le titulaire coopérera avec le CNRS pour répondre à ces demandes.
DCP_032	Le CNRS doit être immédiatement informé des inspections et mesures effectuées par l'autorité de contrôle, dans la mesure où elles concernent le traitement des données à caractère personnel. Ceci s'applique également dans la mesure où le titulaire fait l'objet d'une enquête ou est partie à une enquête d'une autorité compétente en relation avec des infractions à toute loi civile ou pénale, ou règle ou réglementation administrative concernant le traitement des Données à caractère personnel en relation avec l'accord-cadre.

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 règlementation.

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 DSI 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
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.
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.
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.
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.
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.

5.2 ORGANISATION DES ÉQUIPES PROJET

5.2.1 Organisation de l'équipe projet CNRS

Les applications sont organisées par projet métier côté MOA : Intranet, Portail DU, Portail RH et Bourse aux matériels, avec une équipe MOE DSI commune pour le socle et les activités transverses.

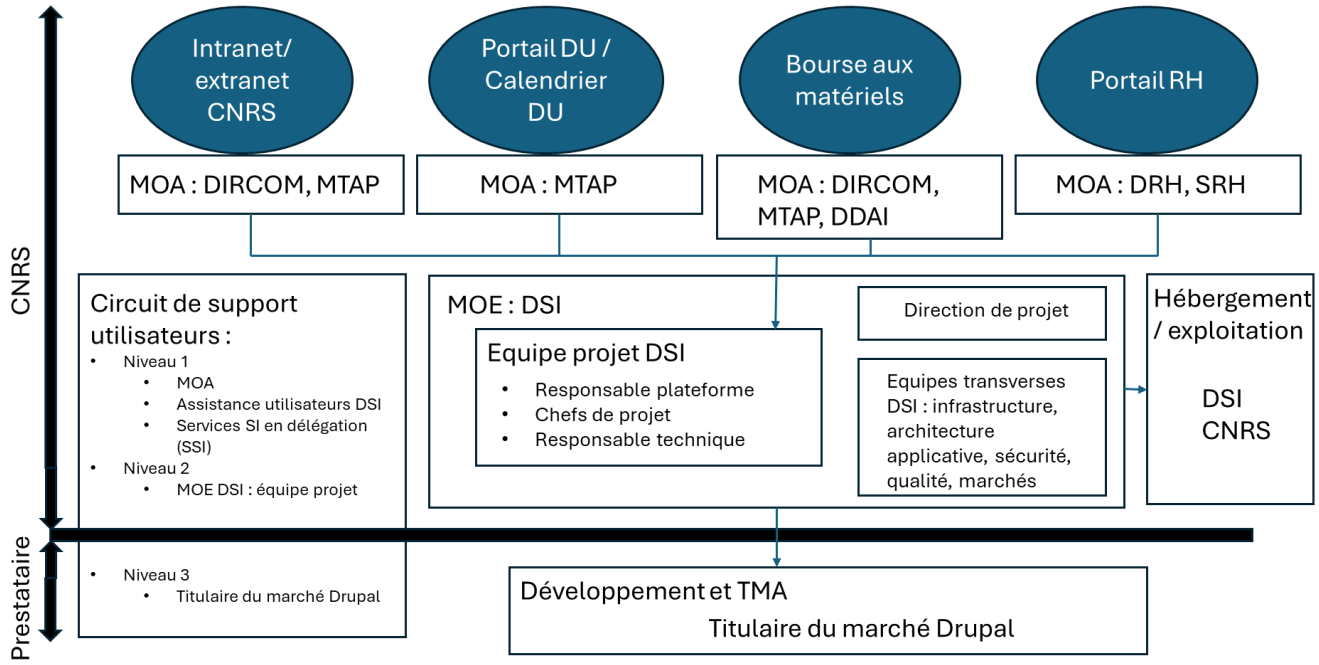


Figure 9 : Organisation du projet

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

- des **équipes projet maîtrise d'ouvrage (MOA)** avec :
    - un **responsable métier** par projet appartenant aux équipes métier MTAP (Mission Transverse d'Appui au Pilotage), DIRCOM (Direction de la communication), DRH (Direction des Ressources Humaines) ou DDAI (Direction déléguée aux achats et à l'innovation)
- une **équipe maîtrise d'œuvre (MOE)** appartenant à la DSI, département « Sites web, communication, accompagnement projet » :
    - un **responsable de la plateforme**; il est en charge de la cohérence des actions, des évolutions et de la disponibilité de l'ensemble de la plateforme ;
    - un **chef de projet** par projet métier ;
    - une **responsable technique ;**
    - **une directrice de projet**.

Côté maîtrise d'ouvrage, le responsable métier s'appuie sur des représentants des différentes MOA, des experts métier et des utilisateurs, pour définir les besoins métier, les prioriser, valider la solution fonctionnellement et mettre en œuvre la conduite du changement.

Côté maîtrise d'œuvre, chaque chef de projet est garant de l'intégration de l'application dans le SI CNRS. Il/elle s'appuie sur des équipes transverses à la DSI (infrastructure, urbanisation, EAI, sécurité, qualité-méthodes, graphisme, marchés…). Un des chefs de projet est par ailleurs chargé de la cohérence du socle technologique mis en œuvre pour les différentes applications. Il est accompagné par une responsable technique en charge de coordonner et suivre les actions des équipes techniques de la DSI : infrastructure (gestion de parc, système, réseau), bases de données, exploitation.

Chaque chef de projet est administrateur technique de l'application correspondante.

La directrice de projet (responsable du département « Sites web, communication, accompagnement projet » à la DSI) pilote et coordonne l'ensemble des composantes du projet ; elle s'assure de l'exécution par le titulaire de ses obligations au titre du contrat, notamment les conditions dans lesquelles le titulaire fournit le service fiable et sécurisé attendu par le CNRS.

L'équipe exploitation de la DSI, est en charge de l'installation, exploitation et administration technique des environnements de recette et production. Une matrice RACI (cf document Livret1_Annexe_RACI) définit le partage des responsabilités entre le titulaire et le CNRS. L'équipe exploitation de la DSI est en contact avec le service CNRS (hors DSI) en charge de l'hébergement.

L'organisation de l'équipe CNRS et les responsables en charge du contrat sont identifiés dans le « Plan Qualité » (PAQ).

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

Le titulaire définit dans le PAQ et met en œuvre une organisation et une gouvernance pour piloter l'accord-cadre. Il adapte l'organisation des équipes aux différentes prestations de l'accord-cadre.

Il identifie les compétences nécessaires et s'assure du maintien de ces compétences tout au long de l'accord-cadre.

Le titulaire désigne a minima les profils suivants :

- directeur de projet : chargé de la gestion, de la coordination et de la fourniture des prestations. Il tient informé et rencontre régulièrement les responsables CNRS
- chef de projet par application métier, responsable opérationnel du développement et de la TMA
- responsable technique
- architecte applicatif
- webdesigner / UX-UI designer
- lead développeur back et front
- développeur back et front
- ingénieur DevOps / Sysadmin en charge des configurations et de la documentation pour les installations des composants spécifiques (Redis, Varnish, Drupal…) qui sera ensuite effectuée par les équipes d'exploitation du CNRS qui n'a pas ces compétences
- responsable sécurité chargé de piloter l'ensemble de la sécurité du projet. Il prend en charge l'organisation des comités de suivi sécurité : convocation, proposition d'ordre du jour, rédaction des comptes-rendus
- responsable qualité chargé de l'assurance et contrôle qualité sur le projet.

Il précise pour chaque profil les compétences associées et le taux de disponibilité minimal. Il précisera également les éventuelles certifications (et la date). Il est attendu des profils "lead front", des certifications sur l'accessibilité numérique (RGAA), éventuellement des certifications Opquast, ainsi que des certifications Drupal pour les profils "lead développeur" et "développeur".

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.

Le titulaire s'engage sur une équipe ferme pour le démarrage de l'accord-cadre, a minima pour les profils types de directeur de projet et chefs de projet.

Le titulaire identifie les profils clefs de son équipe.

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.

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. 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.

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.

5.2.3 Organisation des instances de la gouvernance

Le titulaire assure le pilotage, la préparation, l'organisation et l'animation des différentes instances de gouvernance définies en accord avec le CNRS.

Les principales instances de gouvernance à mettre en place entre le CNRS et le titulaire pour assurer le bon déroulement du projet sont décrites ci-dessous. Le titulaire propose dans le PAQ et met en œuvre toute autre structure de pilotage adaptée aux différentes prestations de l'accord-cadre.

Comité de direction
Objectif : bilan de l'avancement et de l'exécution du contrat, bilan du respect des engagements (niveaux de service), bilan de l'amélioration continue, bilan financier, choix stratégiques à arbitrer, perspectives à moyen et long terme
Périodicité :

- annuel ;

Composition type :

- Directeur des systèmes d'information CNRS ou son représentant
- Le Délégué régional Occitanie Ouest ou son représentant
- Responsable du contrat pour le CNRS
- Responsable du contrat pour le titulaire
- Chaque partie peut convier les personnes intéressées à la tenue des débats

Livrables associés à la charge du titulaire :

- Ordres du jour, convocations, documents d'organisation
- Supports de présentation
- Comptes-rendus, soumis à validation du CNRS
- Tout document demandé par le CNRS sous préavis de 8 jours avant la tenue des débats

Comité de pilotage (COPIL)
Objectif : pilotage global des activités du titulaire, ainsi que suivi de l'avancement des activités sur les différentes applications du périmètre (bilan de la période, faits marquants, prochaines échéances clés et perspectives, risques, indicateurs, planning global, ressources, suivi financier). Il décide du lancement d'une nouvelle prestation et dans ce cadre, valide la commande
Périodicité : mensuel pendant la réalisation des quatre applications, trimestriel ensuite
Composition type :

- Le Délégué régional Occitanie Ouest ou son représentant
- Directrice de projet CNRS
- Responsable de la plateforme et chefs de projet applicatifs CNRS
- Directeur de projet du titulaire
- Chefs de projet du titulaire
- Chaque partie peut convier les personnes intéressées à la tenue des débats

Livrables associés à la charge du titulaire :

- Ordres du jour, convocations, documents d'organisation
- Supports de présentation
    - Dont une présentation portant sur les mises à jour de sécurité (correctifs et vulnérabilités majeures, feuille de route macro proposée)
- Comptes-rendus, soumis à validation du CNRS
- Présentation des indicateurs clés de performance et de qualité
- Plan d'assurance qualité (PAQ) mis à jour
- Plan de réversibilité mis à jour (une fois par an)
- Bilan et plan de progrès (une fois par an)
- Tout document demandé par le CNRS sous préavis de 8 jours avant la tenue des débats.

Comité de suivi opérationnel (COSUI)
Objectif : pilotage régulier des activités du titulaire, ainsi que suivi opérationnel d'un projet (suivi des actions, des versions et livraisons, des vulnérabilités…)
Périodicité : hebdomadaire, avec une partie commune et une partie par application pendant la réalisation ; à ajuster ensuite en fonction de l'activité et en accord avec le titulaire
Composition type :

- Responsable de la plateforme et chefs de projet applicatifs CNRS
- Chef de projet du titulaire
- Chaque partie peut convier les personnes intéressées à la tenue des débats

Livrables associés à la charge du titulaire :

- Ordres du jour, convocations, documents d'organisation
- Supports de présentation
    - Dont une présentation portant sur les mises à jour de sécurité (correctifs, vulnérabilités, feuille de route détaillée proposée)
- Comptes-rendus, soumis à validation du CNRS
- Revue des outillages opérés par le titulaire et de la mise à jour de leurs contenus
- Tout document demandé par le Bénéficiaire sous préavis de 8 jours avant la tenue des débats

Comité sécurité (COSEC)
Objectif : bilan des faits marquants sécurité de la période, revue des accès privilégiés, arbitrage des recommandations sécurité, revue de la PSSI et de sa mise en œuvre, suivi des urgences sécurité et incidents après cellule de crise et crise

gérée…
Périodicité : mensuel pendant la réalisation des quatre applications, trimestriel ensuite. Le COSEC peut être adossé au COPIL.
Composition type :

- RSSI de la DSI du CNRS ou son représentant
- Responsable plateforme CNRS
- Responsable technique CNRS
- Chef de projet du titulaire
- Responsable de la sécurité du titulaire
- Chaque partie peut convier les personnes intéressées à la tenue des débats

Livrables associés à la charge du titulaire :

- Ordres du jour, convocations, documents d'organisation
- Supports de présentation
- Comptes-rendus, soumis à validation du CNRS
- Présentation des tableaux de bord et indicateurs sécurité (sur les thématiques : habilitations, accès, incidents de sécurité, correctifs, vulnérabilité, sauvegardes)
- Plan d'assurance sécurité (PAS) mis à jour
- Tout document demandé par le CNRS sous préavis de 8 jours avant la tenue des débats

Les comités se tiennent par défaut en visioconférence, ou en présentiel dans les locaux du CNRS avec accord des deux parties.

Pour chaque réunion de comité, un ordre du jour systématique et un document support sont diffusés au préalable aux participants et un compte-rendu est rédigé et diffusé à son issue.
Le titulaire fournit aux participants des comités un document support au plus tard deux jours ouvrés avant la réunion.
Le titulaire rédige et adresse le compte-rendu des comités aux participants dans les deux jours ouvrés consécutifs au comité.
Le compte rendu devient définitif après validation par le CNRS.

5.2.4 Pratiques de gestion de projet

Le CNRS souhaite qu'a minima le titulaire mette en œuvre les pratiques de gestion de projet suivantes pour les projets et les applications :

Référence	Libellé exigence
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.
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 » ; - 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.
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.
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.
QUA_025	Le titulaire définit les procédures d'alertes et d'arbitrage.
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.

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 , 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).

5.2.5 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 différents comités.

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

- indicateurs de pilotage :
  - état d'avancement des prestations en cours (livrées, recettées, 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
  - mesures d'éco-responsabilité si disponibles
- indicateurs de qualité des livraisons :
  - respect des délais de livraison
  - nombre d'anomalies[3] (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
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.
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.

5.3 MÉTHODE DE DÉVELOPPEMENT

5.3.1 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) ;
- conception fonctionnelle : (à la charge du CNRS ou du titulaire, en fonction du contexte) : spécifications fonctionnelles globales, maquettes,
- réalisation (à la charge du titulaire) : spécifications fonctionnelles et techniques détaillées, conception technique détaillée, paramétrage ou développements spécifiques, tests unitaires, d'intégration, de validation, de non-

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

régression, de performance et de sécurité, analyse et traitement des anomalies remontées par l'outil d'analyse de code SonarQube et les outils DRUPAL le cas échéant, proposition d'adaptation sous forme de merge-request des playbooks Ansible de déploiement automatisés le cas échéant ;

- intégration (à la charge du titulaire) : validation de la procédure d'installation et des développements en environnement d'intégration (comprenant la compatibilité des modules DRUPAL, la performance des requêtes SQL, la vérification des permissions…);
- 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, comprenant les étapes spécifiques à DRUPAL, 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.

Ce cycle de vie doit intégrer les spécificités liées aux développements de sites DRUPAL, à chaque étape.

Pour l'enchaînement de ces activités, le CNRS préconise un cycle de vie itératif et incrémental[4], découpé en plusieurs versions mises en production sur décision du CNRS. Chaque version suit globalement un cycle en cascade.

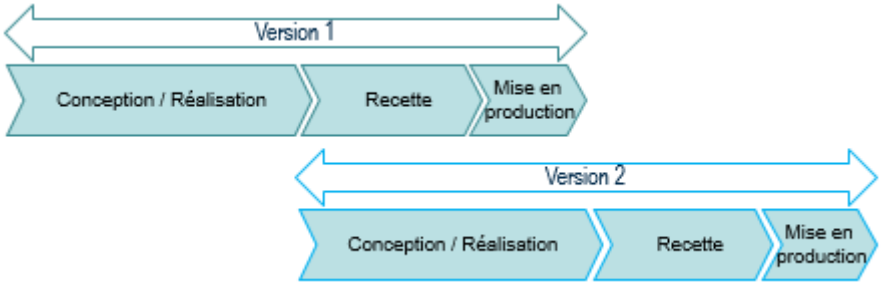


Figure 10 : Cycle de vie en cascade itératif et incrémental

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 du projet, taille et compétence de l'équipe, pilotage par les délais…), 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.

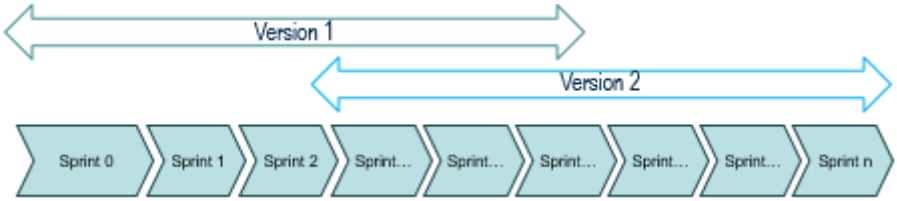


Figure 11 : Cycle de vie agile

[4] 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.

Référence	Libellé exigence
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.
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.
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.
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 (*par exemple :* 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.
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 (*par exemple : sprint planning, daily scrum, sprint review, sprint retrospective*).

5.3.2 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'anomalies[5] 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…).

Référence	Libellé exigence
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).
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.
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.
QUA_035	Les spécifications fonctionnelles détaillées sont formalisées sous forme de cas d'utilisation et de diagrammes UML.
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.
QUA_037	Le titulaire adapte l'activité de test à la méthode de développement du projet.

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

Référence	Libellé exigence
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…).

5.3.3 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
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.

5.4 GESTION DES ENVIRONNEMENTS

5.4.1 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
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.
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.

5.4.2 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
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.
ENV_004	Le titulaire implémente 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).

5.4.3 Environnements CNRS

Pour chaque projet du périmètre, 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 le déploiement et l'intégration de l'application dans le SI du point de vue technique uniquement (authentification, services web de données de référentiels et ESB compris). Les données utilisées dans cet environnement ne sont pas issues de données métier de production. Les tests de bout en bout de cas d'usage métier sont effectués avec des données de tests et l'adaptation de bouchons.
- 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 pourra être ajouté si besoin, dans le cas où les environnements de recette ou production ne pourraient pas être utilisés pour réaliser les formations.

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 et production). La configuration logicielle des environnements de recette est la même que celle de production, alors que la configuration de l'infrastructure sous-jacente (CPU, RAM, …) est équivalente ou proportionnelle (selon les projets) à celle de l'environnement de production.

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

Le CNRS utilise l'outil Redhat AAP (Ansible Automation Platform), pour automatiser les déploiements des applications.

Les exigences suivantes s'appliquent au paysage applicatif précité :

Référence	Libellé exigence
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 cet environnement. Le titulaire est autonome sur cet environnement.
ENV_006	Les environnements de recette 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.

Le document Livret1_Annexe_RACI décrit de manière détaillée la matrice RACI des responsabilités partagées entre le CNRS et le titulaire pour les environnements à mettre en œuvre.

5.5 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
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.
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.
QUA_042	Pour les livraisons documentaires, le titulaire utilise l'outil collaboratif du CNRS.
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.
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)
QUA_045	En cas de livraison d'un delta, le titulaire procède à une re-livraison totale une fois la version stabilisée.
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.

5.6 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, de maintenabilité et de réversibilité.

Référence	Libellé exigence
QUA_047	Tous les documents produits dans le cadre du présent accord-cadre sont livrés sous format électronique modifiable (donc pas uniquement en pdf).
QUA_048	Les documents du projet sont déposés et partagés par le CNRS et le titulaire dans l'outil collaboratif du CNRS.
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).

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

Référence	Libellé exigence
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).

Référence	Libellé exigence
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 « - »).
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'II901 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.
QUA_053	Pour chaque document, un marquage est apposé afin de signifier le niveau de protection et les mesures règlementaires 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.
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 (par exemple, ajout de chapitres, changement de version de l'application, refonte du document…) - **y** : incrémenté à chaque évolution mineure (*par exemple, prise en compte de remarques de relecture, ajout de précisions…*).
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.

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.

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.

5.7 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
QUA_056	Le titulaire identifie les informations (hors livrables documentaires), 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.
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.
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.

5.8 OUTILLAGE DE SUIVI ET PILOTAGE DU PROJET

Le CNRS utilise les outils suivants avec une utilisation partagée possible avec le titulaire :

- gestion des anomalies et des évolutions : Mantis (https://www.mantisbt.org/)
- gestion documentaire, collaboratif : CoRe, basé sur Microsoft SharePoint (https://www.microsoft.com/fr-fr/microsoft-365/sharepoint/collaboration)

Référence	Libellé exigence
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...
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.

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
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 : - création graphique : Figma, Sketch, - suite bureautique : MS Office, - gestion de projet : MS Project, - modélisation des données : Draw.io, - dossiers et suivi des tests : SquashTM, - 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.

L'utilisation par le titulaire d'offres « cloud public » pour ses outils collaboratifs est prohibée.

5.9 MESURES ET CLAUSES DE SÉCURITÉ

5.9.1 Gestion de la Sécurité par le titulaire

Responsabilité

Référence	Libellé exigence
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

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
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.

5.9.2 Protection des biens

Protection des sites

Référence	Libellé exigence
SECU_003	Si le titulaire exécute les prestations à partir de ses propres locaux ou en télétravail, il opère en « site sûr » 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 signifiantes sur ses infrastructures. Le cas échéant, le titulaire réalise un dossier de type « site sûr » 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 « site sûr » lui sera annexé. En cas de télétravail, les accès aux environnements ou aux données de production ne sont autorisés que sur autorisation expresse du CNRS suite à la validation des dispositifs de télétravail décrit par le titulaire..
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 - Télétravail ordinaire et télétravail exceptionnel - Gestion de crise

Protection du système d'information

Référence	Libellé exigence
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.

Politique de contrôle d'accès

Référence	Libellé exigence
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.

Gestion des vulnérabilités

Référence	Libellé exigence
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.

Gestion des incidents

Référence	Libellé exigence
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.

Exigences de Sécurité concernant les personnels extérieurs

Référence	Libellé exigence
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.

Travail dans les zones sécurisées

Référence	Libellé exigence
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.

Stockage et échange d'informations

Référence	Libellé exigence
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

Gestion des sauvegardes

Référence	Libellé exigence
SECU_012	Le titulaire donne au CNRS l'ensemble des éléments techniques concourant à une sauvegarde intègre 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.

Rétrocession des informations du CNRS

Référence	Libellé exigence
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 (*par exemple fichier csv et schéma relationnel des données*). Ces éléments doivent permettre au CNRS de reprendre ces données dans une autre solution le cas échéant.

5.9.3 Obligations du titulaire

Référence	Libellé exigence
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 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.

5.9.4 Localisation des données

Référence	Libellé exigence
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 règlementaires ci-dessus, quel que soit la localisation.

5.9.5 Audit

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), 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.

Référence	Libellé exigence
SECU_016	Le résultat des audits techniques et organisationnels de SSI 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 règlementation en vigueur à la date de notification de l'appel d'offres. Dans tous les autres cas (évolution de la règlementation, 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.

5.9.6 Application des plans gouvernementaux

Référence	Libellé exigence
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 lesdites 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.

6 RESPONSABILITÉ SOCIÉTALE DES ENTREPRISES (RSE)

Le présent article récapitule des obligations listées dans les différentes pièces du marché.

6.1 RESPONSABILITÉ ENVIRONNEMENTALE

6.1.1 Écoconception

Les solutions applicatives sont mises en œuvre conformément au RGESN (Référentiel général d'écoconception de services numériques) : https://ecoresponsable.numerique.gouv.fr/publications/referentiel-general-ecoconception/

6.1.2 Principes de réalisation numérique responsable

Le CNRS a pour ambition de mettre à disposition de ses utilisateurs des applications conçues dans une démarche écoresponsable afin de réduire au maximum ses émissions de gaz à effet de serre (GES) et ses besoins en ressources énergétiques. Les principaux leviers sont listés au paragraphe 2.1.5 ci-dessus

6.2 RESPONSABILITÉ SOCIÉTALE

6.2.1 Accessibilité numérique

Les principes concernés sont traité au paragraphe 2.1.4 au-dessus.

6.2.2 Formation des personnels affectés à l'exécution

Le titulaire veille à ce que les personnels affectés à l'exécution du marché bénéficient, pendant la durée d'exécution des prestations, des actions de formation nécessaires au maintien et au développement des compétences directement requises pour leur réalisation.

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.

6.2.3 Prévention du sexisme et du harcèlement

Le titulaire met en œuvre, pour les personnels affectés à l'exécution du marché, des actions de sensibilisation et de prévention des comportements sexistes, du harcèlement et des violences sexistes et sexuelles. Il informe les personnels concernés des modalités de signalement et de traitement des situations susceptibles de survenir dans le cadre de l'exécution des prestations et désigne, le cas échéant, un interlocuteur identifié à cet effet.

7 ANNEXES

7.1 DOCUMENTS JOINTS

Nom	Fichier correspondant
Livret 1	Intranets_CCTP-Livret1
Livret 1 Annexe Fonctionnelle Intranet CNRS	Intranets_CCTP-Livret1_Annexe_Fonctionnelle_Intranet CNRS
Livret 1 Annexe Fonctionnelle Portail RH	Intranets_CCTP-Livret1_Annexe_Fonctionnelle_Portail RH
Livret 1 Annexe Fonctionnelle Portail DU	Intranets_CCTP-Livret1_Annexe_Fonctionnelle_Portail DU
Livret 1 Annexe Fonctionnelle Bourse aux matériels	Intranets_CCTP-Livret1_Annexe_Fonctionnelle_Bourse aux matériels
Livret 1 Annexe RACI	Intranets_CCTP-Livret1_Annexe_RACI
Livret 1 Annexe CCT Versions cibles	Intranets_CCTP-Livret1_Annexe_CCT_Versions_Cibles
Livret 1 Annexe Charte Graphique	Intranets_CCTP-Livret1_Annexe_Charte_Graphique
Livret 2	Intranets_CCTP-Livret2

7.2 RÉFÉRENCE DES EXIGENCES

Référence	Groupe ou sous-groupe d'exigence
ACC	Accessibilité
AUTH	Authentification
BDD	Base de données
DEV	Développement
DOC	Stockage des documents
ECH	Echange de données
ERG	Ergonomie
ENV	Environnements
ERG	Ergonomie, graphisme
HAB	Habilitations
INF	Infrastructure
QUA	Qualité
REGL	Conformité règlementaire
SECU	Mesure et clauses de sécurité
SSI	Sécurité des systèmes d'information
SSI_COM	Sécurité des communications
SSI_CRYPT	Cryptographie
SSI_EXP	Exploitabilité
SSI_PCA	Plan de Continuité d'Activité SSI
SSI_PDI	Politique de l'information SSI
URB	Urbanisation

7.3 ABRÉVIATIONS ET GLOSSAIRE

7.3.1 Abréviations

Sigle	Description
CMS	Content Management System ou système de gestion de contenus
DAM	Data asset management
DNS	Domain Name System ou système de nom de domaine
IaaS	Infrastructure as a service ou infrastructure en tant que service
MCO	Maintien en Condition Opérationnelle
MCS	Maintien en Condition de Sécurité
RGAA	Référentiel général d'amélioration de l'accessibilité
RGESN	Référentiel général d'écoconception de services numériques
RGPD	Règlement général sur la protection des données
SaaS	Software as a service ou logiciel en tant que service
SI	Système d'information
SLA	Service Level Agreement ou niveaux de service
SSO	Single Sign-On ou authentification unique
TMA	Tierce Maintenance Applicative

7.3.2 Glossaire

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
CCTP	Cahier des Clauses Techniques Particulières
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, etc.
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 : https://www.shibboleth.net/
Téléservice	Application destinée à la communication inter-administration ou destinée à réaliser des téléprocédures ouvertes à des usagers, c'est-à-dire application grand public.

7.4 PRÉSENTATION DÉTAILLÉE DU CNRS

7.4.1 La présidence-direction générale

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

- la direction de la communication (DIRCOM)
- la délégation à la protection des données (DPD)

7.4.1.1 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.

7.4.1.2 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 règlementation 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.

7.4.1.3 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-milieux.
- 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.

7.4.2 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 et des dix-sept délégations 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 (PSST) composé de :
  - le coordination nationale de prévention et de sécurité (CNPS)
  - la coordination nationale de médecine de prévention (CNMP)
- la coordination nationale de la sécurité des systèmes d'information (CNSSI).

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

7.4.2.1 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 Mission pour la place des femmes (MPDF)
  - 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.

7.4.2.2 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.

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** : la directrice de la DSI est assistée d'un directeur adjoint 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 MDM – Master Data Management). 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

7.4.2.3 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

7.4.3 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.

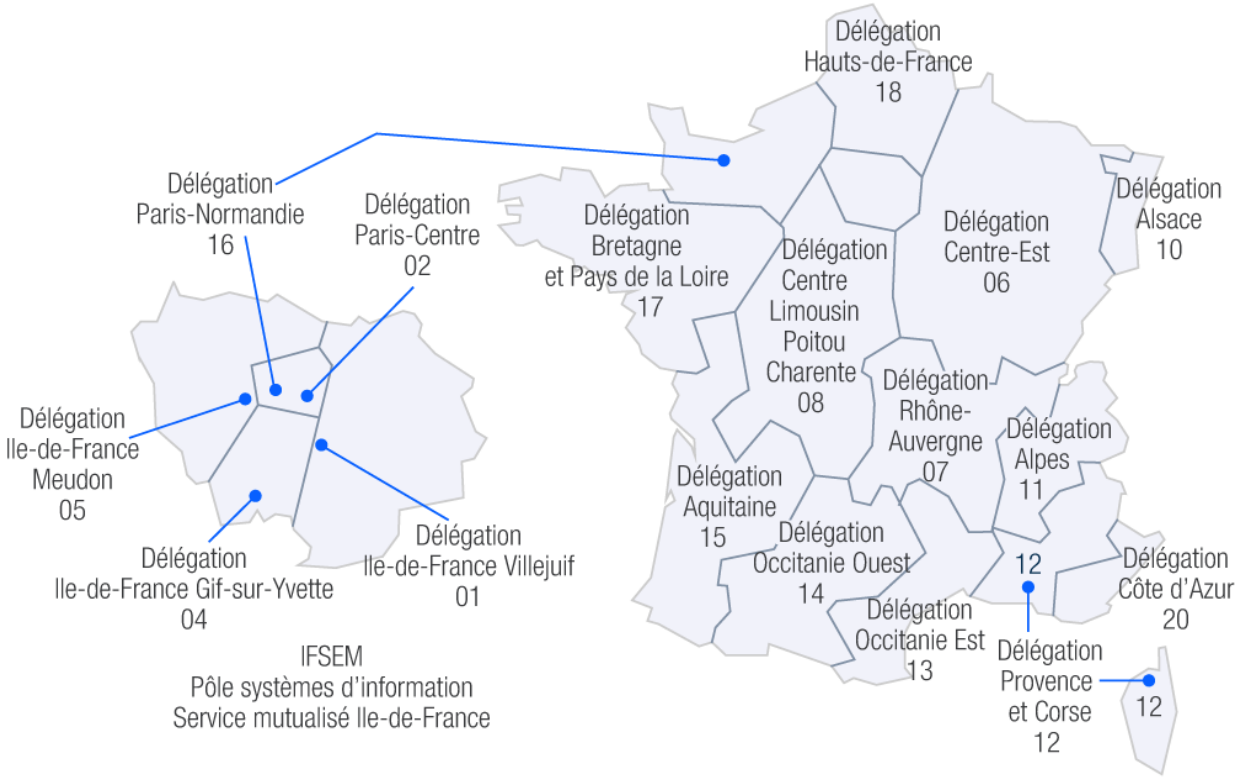


Figure 12 : Le CNRS en région

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

7.4.4 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.