

# Cahier des Clauses Techniques Particulières

RELANCE

PRESTATIONS D'HEBERGEMENT ET D'INFOGERANCE POUR  
LES SITES INTERNET DES CCI DE LA REGION HAUTS DE  
FRANCE

*Réf.marché : CCIR-DSI-2024-94*

*Date et heure limites de réception des offres :*

**MARDI 11 FEVRIER 2025 A 12H00**

**2025**



# SOMMAIRE

## TABLE DES MATIERES

ARTICLE 1. OBJET DE LA CONSULTATION, DEFINITION DU BESOIN ET PRESENTATION DE L'EXISTANT .....	3
ARTICLE 2. DEROULEMENT DU PROJET .....	4
2.1 Devoir de conseil .....	4
2.2 Equipe projet et méthodologie .....	4
2.3 Recette.....	4
ARTICLE 3. PRESTATIONS ATTENDUES.....	5
3.1 Infogérance.....	5
3.2 Service de Haute disponibilité .....	6
3.3 Gestion des sauvegardes .....	6
3.4 Supervision .....	6
3.5 Interface Unique.....	7
3.6 Services spécifiques .....	7
3.7 Reprise de l'existant .....	7
ARTICLE 4. EXIGENCES DE SECURITE.....	8
4.1 Mise à jour et correctifs de sécurité.....	8
4.2 Sauvegarde et restauration .....	9
4.3 Continuité d'activité .....	9
4.4 Authentification.....	9
4.5 Confidentialité et Intégralité des flux.....	10
4.6 Imputabilité, traçabilité .....	10
4.7 Personnel en charge des prestations .....	11
4.8 Qualification et expérience, formation et sensibilisation .....	11
4.9 Exigences de sécurité concernant les personnels extérieurs .....	11
4.10 Intervention des sociétés de maintenance ou de support de solutions informatiques .....	11
4.11 Hébergement.....	11
4.12 Audit de sécurité.....	12
4.13 RGPD .....	12

## ARTICLE 1. OBJET DE LA CONSULTATION, DEFINITION DU BESOIN ET PRESENTATION DE L'EXISTANT

---

La direction des systèmes d'information de la CCI Hauts-de-France, en charge des solutions d'hébergement pour l'ensemble des sites internet souhaite obtenir une solution d'hébergement répondant à l'ensemble de ses besoins. Nous recherchons une solution simple et robuste pour l'ensemble de nos sites actuels et à venir.

La CCIR Hauts-de-France souhaite une mise en œuvre opérationnelle de l'outil au plus tard le 31/04/2025.

Les sites sont gérés principalement par la DSI de la CCI HDF, mais certains sites sont contractuellement gérés par un prestataire.

La CCI HDF souhaite avoir un responsable de compte identifié nommé « Interlocuteur Unique ».

La solution devra être hébergée au sein de l'Union Européenne

Le candidat doit procéder à l'ensemble des opérations requises pour installer les composants de la solution technique retenue dans l'environnement de production.

Afin de répondre aux objectifs cités plus hauts, le Titulaire apportera son expertise en termes de conseil et de propositions tant d'un point de vue technique que professionnel.

Le candidat intégrera à son offre (dans le document « cadre de réponse ») la réversibilité, à savoir la description des dispositifs et procédures qu'il propose, permettant à la CCI Hauts-de-France ou à un autre hébergeur de reprendre cette prestation d'exploitation et d'hébergement en fin de marché.

La CCIR Hauts-de-France veut promouvoir la protection de l'environnement, vous détaillerez dans votre réponse vos actions dans ce domaine, tant au niveau de l'hébergement que de votre entreprise.

Le prestataire actuellement en charge des prestations d'hébergement et d'infogérance pour les sites internet de la CCI Région HAUTS-DE-FRANCE est la SAS ECRITEL

Nous avons 7 machines virtuelles :

Nom	CPU	RAM (GiB)	OS	DD (GiB)	OPTION
SMTP-01	1	1.95	Debian 10.11	100	

BDD-01	4	7.79	Debian 10.11	100	
FRONT-01	4	7.79	Debian 10.13	100	
FRONT-02	4	7.79	Debian 10.13	200	
HD-01	8	15.62	Debian 11.9	200	Haute Dispo
APP-01	8	15.62	Debian 12.5	100	
PPAPP-01	4	7.79	Debian 12.5	100	

## ARTICLE 2. DEROULEMENT DU PROJET

---

### 2.1 Devoir de conseil

La CCI Hauts-de-France souhaite que le candidat retenu soit force de propositions et de conseils d'un point de vue aussi bien fonctionnel que technique.

Dans sa réponse le candidat précisera donc les moyens qu'il compte mettre en oeuvre pour assurer cette prestation de conseils.

### 2.2 Equipe projet et méthodologie

Une équipe projet dédiée sera mise en place et un référent de la maîtrise d'ouvrage sera nommé comme interlocuteur permanent du candidat. Il sera appuyé par un Chef de Projet Technique de la DSI. Cette équipe se réunira au lancement du projet et se réunira ensuite selon le planning prévisionnel qui sera défini à la réunion de lancement.

Les mécanismes de pilotage et le suivi opérationnel du projet doivent être mis en place en conformité avec les pratiques agiles. Ces mécanismes doivent permettre le pilotage régulier des activités du titulaire.

### 2.3 Recette

Le recettage provisoire a pour objet de contrôler la conformité fonctionnelle et technique de la prestation issue de la réalisation de chaque phase.

Aucun recettage ne pourra être prononcé tacitement. La recette sera prononcée conjointement par le pouvoir adjudicateur et le Titulaire.

Le signalement des anomalies sera communiqué au candidat au fur et à mesure de la détection des anomalies (tous les jours ou toutes les semaines).

Après analyse des nouvelles anomalies, le candidat proposera ensuite un plan d'action et un calendrier pour leurs résolutions.

## **ARTICLE 3. PRESTATIONS ATTENDUES**

---

### **3.1 Infogérance**

- Le candidat fournira un service d'infogérance complet :
- Dimensionnement et mise en œuvre des infrastructures nécessaires à l'exploitation et l'hébergement de la solution, incluant notamment les serveurs, les systèmes de stockage, les systèmes de sauvegarde, les moyens d'interconnexion ;
- Hébergement de ces infrastructures et prestations associées (installation/désinstallation des équipements...)
- Exploitation de la solution (suivi des traitements planifiés, mise en œuvre des procédures de sauvegarde/restauration du système) et administration des bases de données
- Fourniture des logiciels nécessaires à l'exploitation des infrastructures et des applications
- Mise en œuvre de matériels et logiciels permettant de mesurer et piloter les niveaux de service effectifs.
- Gestion des certificats : le cryptage SSL sera activé par défaut pour tous les sites hébergés à partir de certificats Let's Encrypt. Leur gestion (renouvellement) sera intégrée dans le cadre des prestations de base de l'infogérance. La CCI Hauts-de-France pourra commander au besoin des certificats SSL avec garantie

Nous attendons au minimum un Support 5/7 8H – 18H par courriel et/ou web et/ou téléphone avec GTI H+2 et GTR H+4.

Vous explicitez dans votre offre, les réponses apportées pour :

- Garantir un taux de disponibilité et les temps de réponse
- Surveiller, sécuriser et superviser la plateforme
- Assurer la maintenance
- Sauvegarder les données (à chaud et sans interruption de services)
- Proposer un plan de reprise d'activité en cas d'incident (exemple: défaillance du NAS)

La localisation des centres de données (datacenters) devra être précisée par les candidats.

Le candidat indiquera si la plateforme ou les plateformes sont connectés en double induction et, le cas échéant, précisera les opérateurs concernés.

Vous définirez précisément les prestations fournies dans le cadre de l'infogérance et préciserez si elles sont limitées en temps.

Nous souhaitons une interface d'administration pour l'ensemble des sites avec la possibilité de gérer les sites et d'ajouter des utilisateurs externes (qui auront de fait accès au support en plus des utilisateurs

de la CCIR HDF), de visualiser l'état du serveur et d'accéder aux services minimums détaillés dans l'article 3.6.

Si votre solution permet la mise en place de cette interface, vous présenterez ses caractéristiques.

### 3.2 Service de Haute disponibilité

Pour le ou les sites web que nous désignerons, nous attendons comme service de haute disponibilité la bascule automatique sur l'hébergement distant en cas d'indisponibilité ou de dégradation des services du site Internet.

Le candidat présentera dans son mémoire technique une option de haute disponibilité dans un datacenter distant.

### 3.3 Gestion des sauvegardes

Il est attendu au minimum :

- une sauvegarde différentielle tous les soirs
- une sauvegarde complète hebdomadaire
- une sauvegarde complète mensuelle
- une sauvegarde complète annuelle.

Se référer à l'article 4.2 pour plus de précisions.

Vous présenterez la solution de restauration de la sauvegarde ainsi que son mode d'accès.

### 3.4 Supervision

La transmission des rapports de supervision fera état d'un rapport mensuel par mail englobant la supervision applicative et système, en plus des alertes immédiates en cas de dysfonctionnement.

#### Indicateurs

La qualité des prestations d'hébergement fait l'objet d'une surveillance constante suivant des indicateurs objectifs portant notamment sur :

- la capacité ;
- la disponibilité du service ;
- la sécurité ;
- les performances ;
- le nombre d'incidents ;
- le temps de correction des incidents.

Le candidat de l'hébergement fournira la liste des indicateurs de fonctionnement concernant la sécurité, les réseaux et les plateformes qu'il met à disposition.

Il explicitera les modalités d'accès à ces indicateurs ainsi que les dispositifs d'alertes qui leurs attachés pour remonter les informations (mail, sms, ...)

### Supervision système :

Supervision quotidienne des espaces disque, charge CPU, utilisation mémoire, cache

### Supervision applicative :

Analyse mensuelle des versions logicielles utilisés (PHP / MySQL/ MariaDB / PostgreSQL / WordPress / Drupal...) avec préconisation de montée de version

### Supervision des sites web :

Disponibilité, état des services, interventions, certificats (date d'expiration)

#### 3.5 Interface Unique

Nous souhaitons une interface unique (portail client) pour l'infogérance et la supervision.

Vous présenterez cette interface en détaillant les données d'infogérance et de supervision disponibles et non disponibles.

Vous complétez cette présentation avec des copies d'écrans de la solution.

#### 3.6 Services spécifiques

Chaque site internet pourra exploiter les services suivants (dans leurs dernières versions stables au moment de la commande) : PHP / base de données (MySQL/MariaDB ou PostgreSQL) / Accès à un gestionnaire de la base de données choisie / FTP / SSH / tâches planifiées / SMTP/Messagerie.

Pour PHP, les versions proposées pour chaque site incluront 7.4, 8.0, 8.1, 8.2 et les suivantes à venir.

Les accès d'administration (comme ftp/ssh/gestion BDD) seront limités aux IP désignées par la CCI Région Hauts-de-France.

Pour chaque site hébergé, nous souhaitons pour gérer les accès FTP, la version de Php, la redirection http vers https, la mise en œuvre de HSTS, la gestion du certificat SSL.

Les certificats Let's encrypt disposeront d'un renouvellement automatique.

Vous présenterez les modalités de mise en place de ces services et le cas échéant les services supplémentaires intégrés à votre offre qui ne génèrent pas de coûts additionnels.

#### 3.7 Reprise de l'existant

Vous détaillerez les besoins pour réaliser cette prestation ainsi que les prérequis et les tâches ne pouvant relever de votre prestation.

Le délai maximum pour la reprise de données est de six (6) semaines.

## ARTICLE 4. EXIGENCES DE SECURITE

---

Le candidat précisera les moyens mis en œuvre dans le cadre du processus d'amélioration continu de la sécurité, à savoir :

- La fréquence ainsi que le périmètre technique et organisationnel des audits réalisés en interne par les équipes du prestataire ou par une société tierce
- Les mesures correctives à la suite aux insuffisances constatées lors de la vérification

Le candidat fournira son Plan d'Assurance Sécurité en relation avec les prestations attendues avec a minima les éléments suivants :

- **Politique de sécurité** : Description des objectifs de sécurité à respecter.
- **Organisation de la sécurité** : Qui est responsable de la sécurité (rôles et responsabilités).
- **Mesures de protection** : Procédures techniques et organisationnelles pour sécuriser les systèmes.
- **Gestion des incidents** : Plan en cas de violation de la sécurité ou d'incidents.
- **Conformité réglementaire** : Respect des normes légales et spécifiques au marché.

### 4.1 Mise à jour et correctifs de sécurité

Le titulaire applique les correctifs recommandés par les fournisseurs de solutions matérielles ou logicielles (logiciels système ou applicatifs, logiciels embarqués) sur l'ensemble des sites dont il a la charge.

En cas d'alerte grave (attaque virale, faille critique) annoncée par le CERTA (Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques), le correctif doit être appliqué dans un délai de 24 heures sur les sites du donneur d'ordres (serveurs web, base de données...)

Lorsqu'aucun correctif n'est pas disponible, le titulaire doit suivre les recommandations de l'éditeur ou du CERTA dans le cadre d'un contournement provisoire. Si le contournement nécessite la désactivation d'une fonctionnalité indispensable au système, le titulaire s'engage à proposer des mesures permettant d'éviter l'exploitation de la vulnérabilité.

Le traitement des alertes mineures pourra intervenir durant les périodes de maintenance hebdomadaires ou mensuelles.

Les passages de correctifs doivent être précédés d'une sauvegarde spécifique des applications et des données contenues, ainsi que de tests sur un environnement de pré production.

Le titulaire devra mettre à jour le dossier de définition avec la liste des correctifs de sécurité appliqués sur les serveurs et communiquer au pouvoir adjudicateur la version actualisée du document.

La validation du bon fonctionnement du système se fera conjointement avec les équipes techniques du titulaire et le chef de projet responsable de l'application hébergée.

En cas d'alerte donnée par les équipes d'experts du titulaire, par l'administration ou le CERTA, le maître d'ouvrage sera notifié par téléphone et courrier électronique avant toute opération. La décision de l'action ne pourra être prise que par des personnels de la maîtrise d'ouvrage désignés par écrit. En



particulier, le responsable sécurité de la maîtrise d'ouvrage sera le correspondant privilégié pour le suivi des opérations.

Le titulaire s'engage à fournir une adresse mail, un numéro de téléphone et les périodes correspondantes d'opération (heures ouvrables) permettant au maître d'ouvrage de suivre le traitement d'une alerte.

#### 4.2 Sauvegarde et restauration

Le titulaire doit prendre toutes les mesures qui s'imposent en termes de sauvegarde et de restauration pour se conformer au niveau de service exigé. Les opérations de sauvegardes donnent lieu à un compte-rendu par messagerie avec indicateur de réussite ou d'échec. La fiabilité des sauvegardes sera mise à l'épreuve par des tests de restauration mensuels, dont les rapports seront communiqués dans le mois suivant les tests.

Un double exemplaire des sauvegardes doit être conservé dans des locaux physiquement séparés du centre informatique du prestataire hébergeant l'application du donneur d'ordres. Le titulaire doit prendre des mesures permettant de garantir la confidentialité des données relatives aux sauvegardes : confidentialité des flux lors des opérations de sauvegardes ; stockage sécurisé des sauvegardes.

En cas de sauvegarde externalisée, les sauvegardes doivent être chiffrées avant leur transfert.

#### 4.3 Continuité d'activité

Le titulaire doit prendre toutes les mesures nécessaires pour assurer la disponibilité de l'application, conformément aux exigences définies dans la clause relative au niveau de service exigé.

Le candidat indiquera les mesures techniques, organisationnelles et procédurales qu'il s'engage à prendre pour assurer la continuité d'activité de l'application, ou en cas de sinistre la reprise d'activité.

Les procédures de sauvegarde et de secours seront auditées.

#### 4.4 Authentification

Pour chaque interface d'accès au système (Interface Homme-Machine, interface entre applications), le titulaire doit fournir une documentation précisant :

- Les mécanismes d'authentification mis en œuvre (protocoles, algorithmes de hachage et de chiffrement utilisés)
- La liste exhaustive des comptes d'accès existants ainsi que des rôles et privilèges qui y sont associés

Les interfaces d'accès aux fonctionnalités doivent impérativement authentifier un utilisateur.

Les identifiants des comptes d'accès sont nominatifs. L'utilisation d'un même compte par plusieurs personnes n'est pas autorisée sauf si une contrainte le justifiant est acceptée par le donneur d'ordres. Dans ce cas, le candidat présentera les mesures techniques et/ou organisationnelles pour garantir l'imputabilité.

- L'utilisation de mots de passe constructeur ou par défaut est interdite.
- L'utilisation de protocoles dont l'authentification est en clair est interdite
- Les mots de passe doivent satisfaire les contraintes de complexité suivantes :
  - Avoir une longueur minimale de 8 caractères (sauf limitation technique)
  - Comporter au minimum une majuscule, un chiffre et un caractère spécial
  - Ne pas être vulnérable aux attaques par dictionnaire.

L'utilisation de certificats clients et serveurs pour l'authentification est une alternative préférable aux mots de passe à condition que la clef privée soit protégée dans un matériel adéquat.

#### 4.5 Confidentialité et Intégralité des flux

Tous les flux d'administration doivent être chiffrés par des procédés fiables (SSH, TLS, Ipsec,etc.), garantissant la confidentialité et l'intégrité des données.

De manière générale, tous les flux contenant des informations sensibles et circulant sur un réseau public doivent être chiffrés par des procédés apportant ces mêmes garanties.

Le candidat indiquera l'ensemble des mécanismes et mesures mis en œuvre pour garantir la confidentialité et l'intégrité des flux d'administration.

Le candidat décrira dans sa réponse les différents mécanismes de protection prévus pour contrer les attaques classiques sur IP et les protocoles associés.

Seuls les services utiles au bon fonctionnement de l'application doivent être activés. Les autres services doivent être désactivés et si possible désinstallés.

#### 4.6 Imputabilité, traçabilité

Les informations suivantes devront être enregistrées :

- Entrée en session d'un utilisateur : date, heure, identifiant de l'utilisateur et du terminal ; réussite ou échec de la tentative
- Actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits : date, heure, identité de l'utilisateur, nom de l'objet, type de la tentative d'accès, réussite ou échec de la tentative
- Création / suppression d'un objet soumis à l'administration des droits : date, heure, identifiant de l'utilisateur, nom de l'objet, type de l'action
- Actions d'utilisateurs autorisés affectant la sécurité de la cible : date, heure, identité de l'utilisateur, type de l'action, nom de l'objet sur lequel porte l'action.

#### 4.7 Personnel en charge des prestations

Le titulaire s'engage à fournir une liste, régulièrement mise à jour, des personnels autorisés à intervenir sur les applications mises en place pour la CCI de Région Hauts de France, ainsi que leur niveau d'habilitation (types d'accès et ressources concernée).

#### 4.8 Qualification et expérience, formation et sensibilisation

Le candidat indiquera dans sa réponse :

- Les qualifications, diplômes ainsi que le niveau d'expérience des personnels retenus pour la réalisation des prestations
- La fréquence et le contenu des actions de formation et de sensibilisation des personnels de l'hébergeur aux enjeux de sécurité.

#### 4.9 Exigences de sécurité concernant les personnels extérieurs

Le candidat précisera les moyens de contrôle mis en œuvre pour s'assurer du respect des exigences de sécurité par ses sous-traitants éventuels, ainsi que des consultants ou techniciens amenés à intervenir dans le cadre du support et de la maintenance sur les applications mises en place pour la CCI de Région Hauts de France.

#### 4.10 Intervention des sociétés de maintenance ou de support de solutions informatiques

Les intervenants des sociétés assurant la maintenance ou le support technique de solutions doivent être accompagnés par une personne habilitée à intervenir sur le système pendant toute la durée de leur intervention. Si un intervenant a besoin de se connecter au système, il doit utiliser un compte spécifique permettant de garantir l'imputabilité de ses actions.

Le candidat présentera les mesures techniques et organisationnelles pour empêcher les extractions massives d'information (par exemple : extraction d'une copie de la base de données à partir d'un poste dédié à l'administration).

Les applications hébergées restent la propriété de la CCI de Région Hauts de France.

#### 4.11 Hébergement

##### **Continuité des services essentiels (énergie, climatisation et télécommunications)**

Une solution de secours doit être mise en œuvre en cas de dysfonctionnement de l'alimentation électrique, de la climatisation ou des moyens de communication.

Le candidat décrira les moyens mis en œuvre afin d'assurer la continuité des services essentiels (énergie, climatisation, télécommunications) sur le site d'exploitation du système : situation et caractéristiques générales du site d'exploitation ; protection et redondance électriques (groupes électrogènes, onduleurs, protection contre les surtensions, etc.) ; contrats de service avec les fournisseurs d'accès, caractéristiques des liaisons de secours ; systèmes de climatisation ; moyens de supervision et remontées d'alarme ; les équipements utilisés par le système du donneur d'ordres, en particulier les composants redondants seront décrits (alimentations, disques, cartes contrôleurs,

serveurs, équipements réseau, liens réseau) ; Le candidat précisera les éventuels agréments gouvernementaux ou certificats de conformités qu'il détient.

#### Protection contre les incendies, la foudre et les dégâts des eaux

Le candidat décrira les moyens mis en œuvre en ce qui concerne : la prévention, la détection et le traitement des incendies ; la protection contre les dégâts des eaux ; la protection contre la foudre et les surtensions. Il sera notamment indiqué dans la réponse si les bâtiments du site d'exploitation se situent ou non en zone inondable.

#### **Surveillance et contrôle des accès aux locaux de l'hébergeur, en particulier au local d'hébergement du système d'information**

Le site d'hébergement doit être surveillé 24h/24 et 7j/7.

Le titulaire doit mettre en œuvre un dispositif permettant de réserver l'accès aux locaux hébergeant l'ensemble des machines et postes de travail utilisés aux seules personnes autorisées par le client : filtrage des accès au bâtiment ou aux étages, et filtrage des accès aux salles machines. Il définira les conditions d'accès du client au service (horaires d'ouverture, cas d'indisponibilité ponctuelle, etc.).

Le candidat doit détailler tous les moyens mis en œuvre afin d'assurer la sécurité des locaux d'hébergement, notamment : moyens de surveillance, dispositifs anti-intrusion ; contrôle et enregistrement des accès (gardiennage, sas, moyen d'identification, etc.) ; protection physique des équipements (verrouillage des baies, etc.)

#### 4.12 Audit de sécurité

La CCI HDF pourra, à tout moment, contrôler que les exigences de sécurité sont satisfaites par les dispositions prises par le titulaire.

Les audits pourront être réalisés par la CCI HDF, ou faire appel à l'expertise d'un organisme ou d'une société tierce présentant des compétences en matière de sécurité.

Des analyses de vulnérabilité, des tests d'intrusion réseau ou applicatifs pourront être menés.

La recette de la solution d'hébergement comprend une revue des systèmes permettant de s'assurer d'une implémentation conforme aux exigences de sécurité. La correction d'éventuelles anomalies détectées sont à la charge du candidat

#### 4.13 RGPD

Le candidat s'engage à respecter les obligations en vigueur liées au RGPD et se porte garant du respect de sa mise en application.