MINISTÈRE
DE LA FONCTION PUBLIQUE
ET DE LA RÉFORME DE L'ÉTAT

Liberté
Égalité
Fraternité

Centre Interministériel de
Services Informatiques relatifs
aux Ressources Humaines

Cadre de cohérence technique

Normes et Contraintes

Classification

Confidentialité		Disponibilité
C2 - Confidentiel	Technique	Continuité d'activité

Information de stockage dans Oodrive

Document à stocker dans OOdrive	**OUI**	**NON**
	X	
Si oui, préciser le lien du dossier contenant le document :	Corpus documentaire du SMSIPD\7 Sécurité des infrastructures et de l'exploitation	

Suivi des modifications

Version	Date	Emetteur	Entité	Suivi des modifications
VT0.1	31/01/2023	DRO/ PFI/ PYG / MDE / FJO	ARC	Initialisation
VT.02	15/03/2023	PG / AD	SMSI	Retours Philippe Giraud / Alice Delachat
VT.03	15/04/2023	GBO	SDNSI	Retours Geoffroy Bonnet
VT.04	07/07/2023	TGO / KBE	SDNSI	Retours Thierry Goujon et Karim Ben Daali
VT.05	13/02/2025	DRO	SDNSI	Ajouts interdiction packages « -devel » Planification exercice de PRA
VT.06	01/04/2025	DRO	SDNSI	Format des adresses no-reply Bases de données mutualisées URL PORTAIL
VV1	16/06/2025	Matthieu Devallé	CISIRH	Validation du document pour le COPIL – reprise de la forme

Validation et diffusion du document

Prénom et Nom	Entité	Destinataires			
		Information	Relecture	Contribution	Validat.
Philippe CUCCURU	CISIRH/Direction				X
Geoffroy BONNET	CISIRH/SDNSI		X	X	
Emmanuel BROSSIER	CISIRH/SDPNM		X		
Philippe Giraud	CISIRH		X	X	
Mathieu DEVALLE	CISIRH/BPDSN		X	X	
Emmanuel KUNTZ	CISIRH/Lab. Innov.		X	X	
David ROELANDT	CISIRH/SDNSI/BT		X	X	
Pier-Yves GREMEAUX	CISIRH/SDSNI/BT-ARC		X	X	
Thierry Goujon	CISIRH/SDNSI/BT-APP			X	
Karim Ben Daali	CISIRH/SDNSI/BANS			X	
Philippe de Saint Aignan	CISIRH/SDNSI/BT-DBA			X	
Membres du CODIR	CISIRH	X			

Table des matières

Table des matières 4
Documents applicables 6
Documents de référence 8
Terminologie 10
1. Présentation générale 11
1.1. Objectif du document 11
1.2. Traitement des données à caractères personnelles 11
2. Exploitation 12
2.1. Répartition de la charge / Proxy 12
2.2. Sauvegardes 13
2.3. Continuité d'activité 14
2.4. Industrialisation 14
2.5. Supervision 17
2.6. Journalisation 18
2.7. Configuration 20
2.8. Virtualisation 20
2.9. Stockage 21
3. Architecture technique 22
3.1. Modèle et Services 22
3.2. API 23
3.3. Conception 24
3.4. Documentation 24
3.5. Logiciels et système 25
3.6. Découpage en zone 25
4. Développement 26
4.1. Général 26
4.2. Langages de développement 28
4.3. Tiers application 30
4.4. Tiers données 30
4.5. Tiers présentation 30

5. Réseau 31
6. Sécurité 32
6.1. Cryptographie 32
6.2. Transfert de documents contenant des données à caractères personnelles 32
6.3. Applications 33
6.4. Logiciels à la demande (SaaS) 35
6.5. Poste de travail 36
6.6. Formats d'échange 36
7. Règles supprimées 37

Documents applicables

Type du document	Origine	Nom du document	Date
Norme internationale	Organisation internationale de normalisation ISO et Commission Électrotechnique Internationale IEC	ISO/CEI 27001 - Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information	Publiée en octobre 2005 et révisée en 2017
Norme internationale	Organisation internationale de normalisation ISO et Commission Électrotechnique Internationale IEC	ISO/CEI 27701 – Techniques de sécurité – Extension d'ISO/CEI 27001 et ISO/CEI 27002 au management de la protection de la vie privée – Exigences et lignes directrices	Publiée en avril 2021
Norme nationale	Gouvernement	Circulaire du Premier ministre n° 5725/SG (NOR : PRMX1420095C) du 17 juillet 2014 sur la Politique de Sécurité des Systèmes d'Information de l'État (PSSI-E)	17 juillet 2014
Norme européenne	Union Européenne	Règlement général sur la protection des données	27 avril 2016
Norme nationale	Gouvernement	Décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics	8 avril 2022
Norme nationale	Gouvernement	Arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics	26 octobre 2022
Norme nationale	Gouvernement	Arrêté du 9 août 2021 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale	9 août 2021
Norme nationale	Gouvernement	Instruction interministérielle relative à la protection des systèmes d'informations sensibles	11/02/2015
Norme nationale	République française	Loi relative à l'informatique et aux libertés (loi « Informatique et Libertés »)	6 janvier 1978

Type du document	Origine	Nom du document	Date
Norme nationale	République française	Loi pour la confiance dans l'économie numérique	21 juin 2004
Norme nationale	République française	Loi relative à la fraude informatique	5 janvier 1988
Norme nationale	République française	Loi pour une République numérique	7 octobre 2016
Norme ministérielle	Ministre de l'Économie des Finances	Arrêté du 22 janvier 2019 portant désignation des autorités qualifiées pour la sécurité des systèmes d'information dans les services d'administration centrale, les services déconcentrés, les organismes et établissements sous tutelle du ministre de l'économie et des finances et du ministre de l'action et des comptes publics	22 janvier 2019
Norme ministérielle	Ministre de l'Économie des Finances	Arrêté du 6 décembre 2019 portant établissement des bilans annuels de la sécurité des systèmes d'information	6 décembre 2019
Norme CISIRH	CISIRH	Politique de sécurité du numérique du CISIRH	11 mars 2024
Norme CISIRH	CISIRH	Note de service portant actualisation du corpus documentaire du système de management de la sécurité de l'information et de la protection des données du CISIRH (SMSI/PD) – Documents généraux	23 octobre 2024
Norme CISIRH	CISIRH	Note de service portant actualisation du corpus documentaire du système de management de la sécurité de l'information et de la protection des données du CISIRH (SMSI/PD) – Documents spécifiques	23 octobre 2024
Norme ministérielle	Ministre de l'Économie des Finances	Arrêté PGSSI	A venir
Norme CISIRH	CISIRH	Règles de nommage des infrastructures techniques	2019

Un document applicable comprend des exigences auxquelles le CISIRH doit se conformer. Il peut s'agir de dispositions législatives ou contractuelles ainsi que des stipulations réglementaires ou des règles normatives.

Documents de référence

Type du document	Origine	Nom du document	Date
Norme nationale	Direction interministérielle du numérique	Référentiel Général d'Accessibilité pour les Administrations (RGAA)	12/2020
Norme nationale	Direction Interministérielle du Numérique et du Système d'Information et de Communication de l'État	Référentiel Général d'Interopérabilité v2.0	12/2015
Norme nationale	CIGREF	Description des 5 couches de l'urbanisation (stratégie, métier, fonctionnelle, applicative et infrastructure) avec des règles de dérivation	-
Norme nationale	Direction Interministérielle du Numérique et du Système d'Information et de Communication de l'État	Règles communes d'architecture et de gestion des référentiels de données métier	12/2013
Norme nationale	Agence nationale de la sécurité des systèmes d'information	Référentiel général de sécurité (RGS) v2.0	06/2014
Norme CISIRH	CISIRH/ARC	Cadre de mise en œuvre des API du CISIRH	
Norme CISIRH	CISIRH/BT/APP	Documentation de packaging « outil de livraison CISIRH »	
Norme internationale	Open Web Application Security Project	https://owasp.org/www-project-top-ten/	09/2021
Norme ministérielle	Ministre de l'Économie des Finances / HFDS	URI pour diagnostic et signalement de services web	04/2018
Norme nationale	CNIL	Guide Sécurité des données personnelles	
Norme nationale	CNIL	Guide RGPD de l'équipe de développement	
Norme CISIRH	CISIRH/BT/ARC	Modèle de Dossier d'architecture	07/2022
Norme CISIRH	CISIRH/BT	Modèle de Dossier d'Exploitation	
Standard	Communs	Guide de versionning SEMVER	08/2013
Standard	Communs	API modèle de maturité de Richardson	2008

Type du document	Origine	Nom du document	Date
Standard	Communs	12 factors app – applications Cloud	2011

Un document de référence apporte des renseignements ou des enseignements pouvant intégrer des recommandations sans portée obligatoire.

Terminologie

Acronyme	Signification
CCT_STE	Socle technique de référence
ANSSI	Agence nationale de sécurité des systèmes d'information
SGBD	Système de Gestion de Bases de Données
SI	Système d'information
SSI	Sécurité des systèmes d'information
DEX	Dossier d'exploitation
DAT	Dossier d'architecture Technique (remplacé par le Dossier d'Architecture)

Terme	Définition
Cadriciel	Framework applicatif
Intergiciel	Middleware

Acteurs	Rôle
Cellule architecture	Maintien de la documentation d'architecture, vérification de la conformité,
Équipes d'exploitation	Équipes en charge de l'exploitation technique et applicative du CISIRH
Équipes chargées de la réalisation	Équipes en charge de la réalisation des applications. Il peut s'agit d'une équipe interne ou d'un prestataire.

1. Présentation générale

1.1. Objectif du document

Le Cadre de cohérence Technique est composé de plusieurs documents :

- La ***Charte d'architecture*** : document regroupant les différents composants techniques et les versions associées. Ce document offre une vision de ce que doit être le système d'information du client pour ce qui est des composants techniques mis en place sur les différents projets internes. Sont traités dans ce document les aspects :
  - Infrastructure : OS, composants système, bases de données, bases NoSQL ;
  - Développement : langages, API et frameworks ;
  - Solution logicielle : Serveur Web, Intergiciels.. ;
- ***Normes et contraintes*** (présent document) : Ce document regroupe l'ensemble des règles à suivre impactant la « façon de faire » les projets, notamment sur les sujets suivants :
  - Architecture et conception
  - Développement applicatif
  - Exploitabilité
  - Réseau
  - Sécurité
  - Documentation

Le CCT s'applique à partir de sa date de validation jusqu'à ce qu'une version plus récente s'applique et remplace de fait la version précédente.

En cas de mise en place d'un produit et non d'un développement spécifique, certaines règles ou contraintes peuvent ne pas être compatibles avec le produit en question. Dans ce cas, il est demandé aux équipes en charge de la réalisation de lister ces différences et de proposer une solution alternative.

Toute règle non respectée doit être soumise à l'approbation du collège d'architecture du CISIRH et doit être notifiée dans le dossier d'architecture.

1.2. Traitement des données à caractères personnelles

La protection de la vie privée doit être intégrée dès la conception d'une solution applicative, notamment ses exigences de sécurité des données. Il conviendra de s'appuyer sur les guides édités par la CNIL notamment « **La sécurité des données personnelles** » et « '**Guide RGPD de l'équipe de développement** »

2. Exploitation

2.1. Répartition de la charge / Proxy

N°	Titre	Date de MàJ
EX1-01	Des load balancers F5 BIG IP doivent être utilisés comme points d'interconnexion entre les infrastructures du CISIRH fournissant des services sur Internet ainsi que celles fournissant des services sur le RIE.	31/01/2023
EX1-02	Les serveurs frontaux du portail des applications interministérielles RH, situés derrière les appliances F5 BIG IP, offrent une répartition de charge vers les nœuds des serveurs applicatifs en utilisant le module mod_proxy_balancer du logiciel HTTPd Apache.	31/01/2023
EX1-03	La solution privilégiée pour la répartition de charge entre les instances d'une même application, en dehors des load balancers F5 BIG IP et du portail des applications interministérielles RH, est la solution logicielle HAProxy.	31/01/2023
EX1-04	La solution retenue pour gérer les mécanismes de haute disponibilité entre les serveurs applicatifs est KeepAlived.	31/01/2023
EX1-05	Dans le cas d'un élément redondé, la charge nominale doit pouvoir être absorbée lors d'un incident sur au moins un autre élément. Par exemple s'il y a 3 instances applicatives prévues chaque instance doit pouvoir absorber 50 % de la charge nominale, afin d'absorber la charge nominale en cas de défaillance d'une instance.	31/01/2023
EX1-06	L'hébergement d'une application s'effectue sur des environnements mutualisés (infrastructure, applicatif, bases de données...) sauf accord explicite du CISIRH.	31/01/2023
EX1-07	Toutes les applications Web sont situées derrière au moins un reverse proxy (type apache httpd et portail) et potentiellement un répartiteur de charge (de type module httpd). La mise en place de ces éléments techniques doit être transparent pour l'application.	31/01/2023
EX1-08	Toute application doit prendre en compte l'utilisation de proxy sortant pour accéder à des services externes.	31/01/2023
EX1-09	Les proxies sortants sont mutualisés et fournis par les équipes d'exploitation.	31/01/2023
EX1-10	Toute application accédant ou publiant des API doit se conformer à la Doctrine API du CISIRH	31/01/2023
EX1-11	Toutes les applications doivent pouvoir être exposées sur plusieurs noms de domaines sans impacts sur l'application. Ceci sous-entend que tous les liens http internes d'une application doivent être relatifs.	26/05/2023
EX1-12	Les règles de reverse proxy (Frontaux/Portail) sont à la charge des équipes en charge de la réalisation de l'application, la réalisation peut se faire avec appui du Bureau Technique.	26/05/2023

N°	Titre	Date de MàJ
EX1-13	Les reverses proxies sont mutualisés et fournis par les équipes d'exploitation (Frontaux/Portail)	31/01/2023
EX1-14	La répartition des applications entre les serveurs du portail SSO est à la charge du Bureau Technique.	01/04/2025
EX1-15	A des fins de résilience, tous les services doivent passer par les serveurs mutualisés du portail SSO, même ceux dont l'authentification n'aie pas assurée par le portail SSO	01/04/2025
EX1-16	Tous les services en production doivent avoir une adresse d'accès (URL) au format suivant : ***(fonctionnalité.)application.cisirh.rie.gouv.fr***	01/04/2025
EX1-17	Tous les services hors production doivent avoir une adresse d'accès (URL) au format suivant : environnement.fonctionnalité.application.cisirh.rie.gouv.fr ou ***environnement(.fonctionnalité).application.sso.cisirh***	01/04/2025

2.2. Sauvegardes

N°	Titre	Date de MàJ
EX2-01	Chaque application doit prévoir un plan de sauvegarde incluant une procédure de sauvegarde et de restauration. La procédure de sauvegarde doit distinguer les données métier (fichier, base de données) des données techniques (fichiers de paramétrage).	31/01/2023
EX2-02	Le plan de sauvegarde doit inclure la durée de rétention, la fréquence des sauvegardes, et le type (incrémentale, totale, etc.), l'heure de passage des sauvegardes en fonction des contraintes projet.	31/01/2023
EX2-03	La sauvegarde des données applicatives s'appuie sur des solutions mutualisées mises en œuvre par les équipes d'exploitation du CISIRH, qui assure leur mise en œuvre.	31/01/2023
EX2-04	Le Dossier d'Exploitation (DEX) est le document qui contient la ou les procédures de sauvegarde et de restauration.	31/01/2023
EX2-05	Dans le cas d'une application éligible au PRA, elle doit disposer d'une procédure permettant de réaliser des tests de restauration sur le PRA (exemple : exercice bascule PRA).	26/05/2023
EX2-06	La ou les procédures de restauration doivent indiquer si la restauration peut se faire en place (avec remplacement des fichiers) ou non (restauration à un autre endroit que celui d'origine).	31/01/2023
EX2-07	Les procédures de restauration doivent être testées régulièrement, au minimum deux fois par an. La fréquence minimale est à déterminer en fonction de la criticité de l'application.	26/05/2023

2.3. Continuité d'activité

N°	Titre	Date de MàJ
EX3-01	Toute solution applicative gérant des données à caractère personnel doit disposer d'une procédure de reprise d'activité, même sommaire. Cf. fiche 10 du guide CNIL relatif à la sécurité des données personnelles. Cette procédure doit être testée régulièrement.	17/03/2023
EX3-02	L'inscription dans le processus de bascule PRA ou non doit être étudiée pour toute application du CISIRH (métier ou support).	14/04/2023
EX3-03	Le Bureau Technique procédera à un exercice de Bascule PRA annuellement au mois de juin pour toutes les applications éligibles.	13/02/2025

2.4. Industrialisation

N°	Titre	Date de MàJ
EX03-01	Toute application (ou sous-application) doit être identifiée par un trigramme. Ce trigramme fixé par la cellule Architecture permet d'identifier les composantes liées à une application (machine virtuelle, binaires, objets VTOM..) en accord avec la convention de nommage du Bureau Technique.	31/01/2023
EX03-02	Chaque version applicative doit être clairement identifiable et numérotée x.y.z où : • x : numéro de version majeure • y : numéro de version mineure • z : bugfix / patch Il est **interdit** de livrer en production un composant en version SNAPSHOT.	26/05/2023
EX03-03	Le nom des binaires applicatifs (issus d'un développement spécifique) doit porter les informations : • Le nom ou le trigramme de l'application • Le numéro de version Par exemple : ***<TRIGRAMME_APP>_x.y.z.war*** Afin de conserver un nom stable lors des déploiements de war l'utilisation de liens symboliques est recommandée.	31/01/2023
EX03-04	Le nom du livrable doit être normé, par défaut : **[TRIGRAMME_APPLICATION]_[SOUS_APPLICATION]**.**X.Y.Z** où : • TRIGRAMME_APPLICATION correspond au trigramme de l'application • SOUS_APPLICATION correspond éventuellement à l'identification d'un sous module de l'application • X.Y.Z correspond au numéro de version	31/01/2023

N°	Titre	Date de MàJ
EX03-05	Les livrables doivent être compressés au format **tar.gz** et contenir une arborescence compatible avec l'outil de livraison du CISIRH.	31/01/2023
EX03-06	Chaque livraison doit être complète avec les éléments ci-dessus. Dans le cas contraire, le CISIRH se réserve le droit de refuser la livraison.	31/01/2023
EX03-07	Sauf mention contraire, les scripts système doivent être au format linux et de type **bash ou ksh**	31/01/2023
EX03-08	Tout traitement automatique doit renvoyer un code retour suivant les différents cas possibles de réussite et d'échec. La documentation associée doit faire apparaître la description des codes retour.	31/01/2023
EX03-08b	Tout code retour indiquant une erreur doit avoir une valeur supérieure à 11. Les codes retours de bon fonctionnement ou avertissement doivent avoir une valeur inférieure à 11.	31/01/2023
EX03-09	Le cas échéant, une procédure de compilation doit systématiquement être prévue et doit permettre de générer les binaires livrés à partir des sources livrées.	31/01/2023
EX03-10	L'utilisation de **MAVEN** pour la gestion du cycle de développement des projets **JAVA** est obligatoire.	31/01/2023
EX03-10b	Le projet doit fournir les url de l'ensemble des repository MAVEN utilisés (hors maven central). En cas d'utilisation de librairies non disponibles sur les repository publiques, ces librairies doivent être incluses dans le livrable et ajoutées au repository du CISIRH.	31/01/2023
EX03-11	L'utilisation de **Composer** pour la gestion du cycle de développement des projets **PHP** est obligatoire.	31/01/2023
EX03-12	L'utilisation de **NPM** pour la gestion du cycle de développement des projets **NodeJS** est obligatoire.	31/01/2023
EX03-13	L'utilisation de **PIP** pour la gestion du cycle de développement des projets **Python** est obligatoire.	31/01/2023
EX03-14	Lors de la génération des binaires, l'appel aux ressources MAVEN Central, Composer, NPM et PIP doit se faire à travers le proxy NEXUS de PRODJ.	31/01/2023
EX03-15	Les langages et frameworks de développement non cités doivent obtenir l'accord de la cellule Architecture du CISIRH avant de pouvoir être utilisés.	31/01/2023
EX03-16	Les projets doivent être hébergés sur la forge Gitlab RIE du CISIRH. La visibilité doit être positionnée à « internal » par défaut.	31/01/2023
EX03-17	L'intégration continue doit reposer sur le service Gitlab-CI du CISIRH.	31/01/2023
EX03-18	Les projets doivent être évalués avec l'outil SonarQube du CISIRH.	31/01/2023

N°	Titre	Date de MàJ
EX03-19	Les applications ne doivent pas souffrir des vulnérabilités listées au Top 10 de l'OSWAP	31/01/2023
EX03-20	En cas de présence de plusieurs batchs sur un projet, le dossier d'exploitation (DEX) doit comprendre un plan de programmation présentant la séquence de passage, la plage horaire prévue et l'ordonnancement éventuel.	31/01/2023
EX03-21	Le plan de programmation doit comporter un nombre d'exécution en erreur maximum par mois.	31/01/2023
EX03-22	En cas d'erreur, le plan de programmation doit disposer de tâches de reprise.	31/01/2023
EX03-23	L'organisation des répertoires sur les serveurs doit respecter le standard suivant : • fichiers de logs dans /exploit/***app***/logs • application binaire dans /produit/***app*** • fichiers de configuration dans /exploit/***app***/conf • scripts dans /exploit/***app***/scripts	31/01/2023
EX03-24	Pour les applications ayant des environnements mutualisés sur un même serveur, le nom de l'application sera complété avec le nom de l'environnement correspondant pour les objets relatifs à l'application et l'environnement (noms des répertoires, noms des services)	26/05/2023
EX03-25	Il est demandé de fournir des scripts au format systemd permettant de réaliser les opérations de base d'exploitation pour chaque composant applicatif : • Démarrer un service/une application/un batch • Arrêter un service/une application/un batch • Vérifier le statut (démarré/arrêté et idéalement la version installée)	31/01/2023
EX03-26	Le plan de la documentation technique (DEX, DAT, DIN) est fourni par les équipes projet et doit être respecté.	26/05/2023
EX03-27	La procédure d'installation doit prévoir un mécanisme de retour-arrière, par exemple avec l'utilisation de liens symboliques vers les livrables.	31/01/2023
EX03-28	La procédure d'installation doit être entièrement automatisée.	31/01/2023
EX03-29	Pour chaque livraison une estimation de la durée d'installation nécessaire doit être fournie permettant de planifier la durée d'interruption de service.	31/01/2023
EX03-30	Il est demandé de prévoir l'automatisation du démarrage des services lors de la procédure d'installation.	31/01/2023

2.5. Supervision

N°	Titre	Date de MàJ
EX04-01	En cas d'erreur sur un traitement batch celui-ci doit notifier l'erreur sur l'outil de supervision du CISIRH.	31/01/2023
EX04-02	Chaque application – hors contrainte de produit – doit inclure une page de monitoring présentant son état avec les informations suivantes : • Numéro de version de l'application • Vérification d'accès vers l'ensemble des composants tiers qu'elle appelle (base de données, annuaire LDAP, autre application, librairie système nécessaire, etc.). Cette page doit être facilement interprétable par une sonde de supervision de type Zabbix, par exemple **check_http** avec une regex (pas de page html décorée, avec javascript etc.)	31/01/2023
EX04-03	l'URI de la page de supervision doit être **/heartbeat**. Son accès doit être contrôlé par des règles de reverse proxy (par exemple du portail SSO).	31/01/2023
EX04-04	Un batch traitant de gros volumes de données doit indiquer son état d'avancement dans les logs.	31/01/2023
EX04-05	Une durée estimative de temps d'exécution doit être précisée dans la documentation technique pour chaque traitement batch.	31/01/2023

2.6.Journalisation

N°	Titre	Date de MàJ
EX05-01	Tout composant applicatif doit générer des fichiers de logs configurables (emplacement et verbosité). Les éléments de configuration doivent figurer au DEX.	31/01/2023
EX05-02	Tout composant applicatif doit générer des fichiers de logs au format JSON.	31/01/2023
EX05-03	Toutes les traces métiers et applicatives doivent être transférables dans l'outil de centralisation des logs du CISIRH.	31/01/2023
EX05-04	Toutes les traces applicatives doivent être écrites dans un sous-répertoire de **/exploit**	31/01/2023
EX05-05	La rotation de toutes les logs (fréquence, chemins) doit être prévue et configurable dès la mise en place. Elle peut s'appuyer sur un mécanisme interne ou logrotate.	31/01/2023
EX05-06	Le cas échéant, la configuration de logrotate doit être livrée dans la livraison.	31/01/2023
EX05-07	La génération des logs applicatives doit se baser sur une solution permettant de paramétrer l'emplacement et la verbosité des logs.	31/01/2023
EX05-08	La politique de logs définissant le niveau de logs et la politique de rotation doit être externalisée des binaires applicatifs.	31/01/2023
EX05-09	Les logs applicatifs doivent à minima contenir les éléments suivants : • Horodatage • Niveau de log • Classe ou objet générant la trace • Message explicite et permettant une première analyse	31/01/2023
EX05-10	Afin d'éviter une saturation des fichiers de logs, une politique de rotation de logs doit être définie précisant si la rotation est effectuée sur n fichiers d'une taille fixe ou sur une date.	31/01/2023
EX05-11	L'application doit disposer d'un mode DEBUG, qui permet, en cas de défaillance, de comportement suspect, ou de test intensif, de suivre pas à pas son déroulement (horodatage du début et de la fin de chaque module applicatif au minimum). Le mode DEBUG correspond à minima à la bascule des logs à un niveau DEBUG. Ce mode trace doit ainsi permettre : - de suivre pas à pas le déroulement des opérations, à un niveau très fin (opération unitaire de donnée stockée, de transfert de message, de traitement) - de fournir le contenu des données liées aux opérations précédentes - d'indiquer précisément la position de l'opération dans le programme - de détailler précisément toutes les erreurs, ou problèmes, même internes La possibilité de passer en mode DEBUG à chaud serait appréciée.	31/01/2023

N°	Titre	Date de MàJ
EX05-12	Le passage en mode DEBUG des traces applicatives ne doit pas saturer le filesystem ou à défaut préciser la durée maximale d'utilisation du mode DEBUG avant saturation.	31/01/2023
EX05-13	Le passage du mode DEBUG à un mode moins verbeux doit pouvoir se faire à chaud	31/01/2023
EX05-14	Les traces applicatives en mode DEBUG doivent fournir un id de corrélation permettant de suivre toutes les opérations d'un même traitement quel que soit la machine qui la traite.	31/01/2023
EX05-15	Tout processus d'une application doit «journaliser» le moment où il est lancé et le moment où il s'arrête. En cas de fin anormale, un message d'erreur doit être journalisé. La description de ce message doit être contenue dans la documentation de mise en exploitation.	31/01/2023
EX05-16	La documentation d'architecture de l'application doit préciser la taille disque nécessaire aux logs afin d'éviter toute saturation.	31/01/2023
EX05-17	Tout composant applicatif de type application web doit fournir 2 types de logs distincts : • Logs d'accès • Logs applicatifs	31/01/2023
EX05-18	Le format des logs d'accès doit respecter le format du fichier accesslog d'apache httpd du CISIRH. Si ce n'est pas le cas, l'équipe en charge projet doit fournir le pattern grok correspondant	31/01/2023
EX05-19	Le format des logs applicatifs Java doit respecter le pattern disponible en annexe https://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html	31/01/2023

2.7. Configuration

N°	Titre	Date de MàJ
EX06-01	Les fichiers de configuration ne doivent pas contenir de secrets. Privilégier l'utilisation de variables d'environnements. En cas d'impossibilité de respecter cette exigence, une exception doit être tracée.	31/01/2023
EX06-02	Le format de fichier de configuration à privilégier est le fichier de propriétés clé/valeur	31/01/2023
EX06-04	Le(s) fichier(s) de configuration de l'application doi(ven)t être externalisé(s) des binaires applicatifs et de l'arborescence du serveur applicatif. Un nouveau déploiement du binaire ne doit pas remplacer le(s) fichier(s) de configuration.	31/01/2023
EX06-05	Le(s) fichier(s) de configuration doi(ven)t regrouper l'ensemble du paramétrage propre à l'environnement où il est exécuté.	31/01/2023
EX06-06	Il est demandé que le nombre de fichiers de configuration pour un module applicatif soit limité, idéalement, à un seul fichier.	31/01/2023
EX06-07	Dans le cas où plusieurs fichiers de configuration sont présents pour un même composant applicatif, il n'est pas admissible de devoir renseigner la même propriété dans plusieurs fichiers.	31/01/2023

2.8. Virtualisation

N°	Titre	Date de MàJ
EX07-01	Le socle de virtualisation est basé sur des produits référencés au CCT Charte d'architecture. KVM est le socle utilisé au CISIRH (hors Cloud).	31/01/2023
EX07-02	Les applications et sites Web sont – sauf mention contraire – déployées sur le socle de virtualisation du CISIRH.	31/01/2023

2.9. Stockage

N°	Titre	Date de MàJ
EX08-01	La documentation d'architecture (DAT) doit décrire la volumétrie nécessaire pour la production et éventuellement pour le projet, si ses besoins en ressources sont significatifs : • Exploitation (logs, livrables, sauvegardes, etc.) • Base de données (données, index, tablespaces etc.) • Espace disque (index type lucene) • Espace disque partagé • etc.	31/01/2023
EX08-02	L'estimation prévisionnelle des besoins en stockage doit être anticipée annuellement.	31/01/2023
EX08-03	La documentation d'architecture doit préciser la taille et le type du stockage externe (exemple : partition NFS, HCP, Swift..)	31/01/2023

3. Architecture technique

3.1. Modèle et Services

N°	Titre	Date de MàJ
AT01-01	Toutes les informations saisies ou envoyées en entrée du serveur doivent être contrôlées au niveau du serveur, y compris celles déjà validées au niveau du client.	31/01/2023
AT01-02	Une application WEB doit être du type N-Tiers.	31/01/2023
AT01-03	Le développement des applications développées et/ou hébergées par le CISIRH sont principalement basés sur les langages Java, PHP et Javascript.	31/01/2023
AT01-04	Le développement des applications développées et/ou hébergées par le CISIRH doivent être basés sur des cadriciels (frameworks)	31/01/2023
AT01-05	Toutes les couches d'une application N-Tiers doivent être indépendantes. Les interfaces entre les couches doivent s'appuyer sur des normes et standards.	31/01/2023
AT01-06	Une application ne doit comporter aucune adhérence vis-à-vis du matériel d'un constructeur particulier sur les équipements serveurs, stockage, sauvegardes et réseau.	31/01/2023
AT01-07	Chaque tiers d'une application multi-tiers doit être indépendant des autres niveaux. Il faut définir avec précision les interfaces pour permettre l'indépendance entre ces niveaux et la modification de l'un d'entre eux (déplacement, multiplication des instances, multiplication des serveurs, ...) sans impact sur les autres.	31/01/2023
AT01-08	L'usage du protocole HTTPS est obligatoire pour les accès clients. De façon générale, l'utilisation du protocole HTTPS est recommandée.	31/01/2023

3.2. API

N°	Titre	Date de MàJ
AT-API-01	Les services accessibles depuis une API doivent l'être via la solution d'API Management PISTE, même entre les applications internes du CISIRH.	31/01/2023
AT-API-02	Lors de la création de services Web, l'approche top/bottom est à privilégier en commençant par la définition des API avant leur implémentation.	31/01/2023
AT-API-03	En cas de mise en place de services REST, il est demandé de traiter les erreurs avec un code http correspondant à l'erreur et de renvoyer un contenu de type JSON avec à minima : • Un code retour • Une description Il est interdit de renvoyer une pile d'exécution ou des informations permettant de comprendre l'architecture sous-jacente mise en place.	31/01/2023
AT-API-04	Dans le cadre de la mise en œuvre d'une architecture orientée service, il est recommandé de s'appuyer sur les Web Services REST ou SOAP. Le format d'API REST/JSON est à privilégier au format SOAP/XML	13/02/2023
AT-API-05	En cas de mise en place d'API sur un projet (y compris pour des besoins internes au projet), il est demandé de façon obligatoire, de réaliser la documentation de l'API au format openAPI (v2 minimum v3 recommandée) https://www.openapis.org/. Cette définition devra être réalisée avec l'outil swagger (https://swagger.io/). Les fichiers de définition yaml et json sont des livrables attendus du projet.	31/01/2023
AT-API-06	Une API REST doit être compatible avec le modèle de maturité de Richardson au moins au niveau 2 (utilisation correcte des verbes et des codes retour du protocole http)	31/01/2023

3.3. Conception

N°	Titre	Date de MàJ
AT02-01	L'utilisation de diagrammes et de conventions de représentations graphiques ne suffit pas. Il est nécessaire d'associer aux graphiques une description textuelle en français.	31/01/2023
AT02-02	Il est demandé d'utiliser le langage de modélisation UML pour la modélisation de processus. Il est demandé les diagrammes UML suivants : • Cas d'utilisation • Classe • État-transition • Séquence (lors de traitement faisant interagir plusieurs composants techniques) Ces diagrammes doivent être ajoutés au document de conception détaillé.	31/01/2023
AT02-03	Le MCD (Modèle Conceptuel des Données) et le MPD (Modèle Physique des Données) doivent être maintenus à jour et livrés à chaque livraison.	31/01/2023

3.4. Documentation

N°	Titre	Date de MàJ
AT03-01	La documentation du projet doit respecter la politique de gestion documentaire du CISIRH.	31/01/2023
AT03-02	En phase de travail nécessitant les relectures et l'édition, les documents doivent être fournis sous une forme éditable y compris les schémas.	31/01/2023
AT03-03	La version finale d'un document peut être livrée au format PDF	31/01/2023
AT03-04	Afin d'harmoniser les livrables des plans type des documents techniques suivants sont fournis : • Dossier d'Architecture (DA) • Dossier d'Exploitation (DEX) Ces plans peuvent être enrichis en fonction des besoins du projet.	31/01/2023
AT03-05	Concernant la partie technique des projets, il est attendu les documents suivants complétés avant la mise en production : • Dossier d'Architecture (DA) • Dossier d'exploitation (DEX) • Dossier d'installation (DIN) Un document de Spécifications techniques détaillées (STD) peut être demandé. Il est préconisé de disposer d'un DA, même incomplet avant les phases de développement ou d'intégration. Ce dossier sera à compléter au fur et à mesure de l'avancée des travaux. Si la procédure d'installation est simple (via automatisation notamment), celle-ci peut figurer dans le DEX en lieu d'un DIN.	31/01/2023

3.5. Logiciels et système

N°	Titre	Date de MàJ
AT04-01	Toute application métier doit fonctionner sur un système d'exploitation conforme aux standards POSIX et/ou LSB (Linux Standard Base) et référencés dans la charte d'architecture du CISIRH.	31/01/2023
AT04-02	Pour les serveurs, l'installation d'un noyau 64 bits du système d'exploitation est obligatoire.	31/01/2023
AT04-03	Les images docker doivent reposer sur l'architecture x86-64.	31/01/2023
AT04-04	Toute application doit être compatible avec les navigateurs Edge et Firefox.	14/04/2023
AT04-05	L'utilisation de packages de développement « -devel » est proscrite.	13/02/2025

3.6. Découpage en zone

N°	Titre	Date de MàJ
AT05-01	Les applications doivent respecter une étanchéité entre les zones applicatives Internet et les zones applicatives RIE. Si une application doit déroger à cette règle, elle devra garantir un filtrage suffisant, qui sera évalué par l'ANSSI et un audit de sécurité.	31/01/2023
AT05-02	Les applications doivent respecter un découpage au sein d'une zone (Internet ou RIE) : • DMZ (reverses proxies, cache applicatif, etc.) • Application (serveur Web, serveur applicatif, batch, etc.) • Données (SGBR, base NoSQL, etc.)	31/01/2023
AT05-03	Les communications depuis la zone Internet vers la zone RIE sont interdites par défaut, en cas de besoins de ce type, les modalités de communication (port, protocole, sens des échanges, etc.) seront à discuter en atelier technique et soumis à homologation.	31/01/2023
AT05-04	Seules les communications de la zone Intranet vers la zone Internet sont autorisées. Les échanges de données inter-zones doivent toujours être initiées par la zone Intranet.	31/01/2023

4. Développement

4.1. Général

N°	Titre	Date de MàJ
DO01-01	Les applications doivent respecter les obligations déclaratives fixées par le RGAA (Référentiel général d'amélioration de l'accessibilité) : • Mention du niveau de conformité au RGAA sur la page d'accueil de l'application ; • Publications sur l'ensemble des pages de l'application d'un lien permettant d'accéder aux éléments suivants : • Déclaration d'accessibilité de l'application ; • Schéma pluriannuel de mise en accessibilité du CISIRH (incluant des plans d'action annuels dédiés à l'application).	31/01/2023
DO01-02	Le niveau d'accessibilité souhaité et les tests associés sont précisés au cas par cas par chaque projet. La cible étant un taux de conformité minimal de 75 % pour les projets du CISIRH.	31/01/2023
DO01-03	Les applications doivent se conformer au RGI (Référentiel Général d'Interopérabilité).	31/01/2023
DO01-04	Les applications doivent se conformer au RGS (Référentiel Général de Sécurité). Tout écart doit être signalé et justifié et accepté par le CISIRH. L'ensemble du corpus RGS est accessible sur le site de l'ANSSI (https://www.ssi.gouv.fr/).	31/01/2023
DO01-05	Les développements doivent respecter l'exigence de « **Security by design** » dès la conception.	31/01/2023
DO01-06	Le code source produit au profit du CISIRH doit respecter le guide RGPD pour l'équipe de développement de la CNIL	17/03/2023
DO01-07	Pour les échanges applicatifs, le CISIRH impose l'utilisation du protocole http(s) et échanges via Web Services. L'utilisation des EJB n'est pas autorisée.	31/01/2023
DO01-08	Les fonctions de recherche – sauf mention contraire – ne doivent pas être sensibles à la casse.	31/01/2023
DO01-09	Les temps de réponse moyens des pages Web ne doivent pas dépasser – sauf mention contraire – les temps suivants : • Page ou recherche simple : 2s dans 90 % des cas • Page ou recherche complexe : 5s dans 90 % des cas	31/01/2023
DO01-10	Les applications doivent se conformer au document interministériel « Cadre Commun d'Urbanisation SI Etat »	31/01/2023

N°	Titre	Date de MàJ
DO01-11	Les applications doivent se conformer au document interministériel « Cadre Commun d'Architecture des Référentiels de données »	31/01/2023
DO01-12	Les APIs publiées doivent respecter les recommandations du partage de données par API dans l'administration	31/01/2023
DO01-13	Lors de l'utilisation de composants open source, en cas d'anomalie constatée sur le composant si un correctif ou une évolution est nécessaire : • L'administration doit en être informée • Le correctif ou l'évolutif doit être soumis à la communauté gérant le composant.	31/01/2023
DO01-14	Il est demandé d'utiliser le gestionnaire de versions **GIT**.	31/01/2023
DO01-15	L'administration demande à chaque livraison un clone complet du repository git du projet (git clone –mirror) en plus des sources de l'application (sauf si le projet est accessible sur un repository public : github / gitlab). Si l'export est anonymisé (nom des développeurs : dev1 à devN) cela doit être prévu dès le départ du projet afin de conserver un historique propre du projet.	31/01/2023

DO01-16	L'export des repos git doit respecter les contraintes suivantes :
	export avec la commande --mirror
	• Tous les répertoires contenant un repo git doivent être suffixés par '.git'
	• Une archive zip doit être créée contenant le ou les repos git et doit être nommée : <NOM_PROJET>-git-repos-<VERSION>.zip où
	  ○ NOM_PROJET correspond au nom du projet
	  ○ VERSION correspond à la version au format x.y.z
		31/01/2023

DO01-17	Il est demandé la gestion des branches de développement au sens *git* comme suit : • La branche de livraison doit être ***master*** (ou main) et doit contenir les versions (tags) livrées. Cette branche doit ***toujours*** être déployable et ne doit ***jamais*** contenir de version SNAPSHOT. • Une branche, par défaut develop, doit contenir les versions « propres » internes. Cette branche correspond à la branche de recette interne des développeurs. Cette branche doit être fusionnée dans la branche principale. • Les branches sous la branche develop sont laissées à la libre utilisation des développeurs et correspondent au développement des fonctionnalités. Lors du développement des nouvelles fonctionnalités, les opérations de push doivent être réalisées sur les branches sous la branche develop. Les branches develop et master ne reçoivent que des merges ou des correctifs.	23/06/2023

N°	Titre	Date de MàJ
	Si la branche de livraison est différente de master, il convient de préciser au CISIRH le nom de cette branche et de l'indiquer dans la documentation technique (DIN ou DEX).	
DO01-18	Les IHM de l'application doivent respecter le Système de Design de l'État.	31/01/2023
DO01-19	Pendant tout le cycle de vie de l'application, les dépendances applicatives doivent être auditées et mises à jour en utilisant une solution de type DependancyCheck ou RenovateBot.	31/01/2023
DO01-20	Les développements doivent favoriser la réutilisation du code par d'autres projets notamment par l'utilisation de librairies ou de snippets lorsque cela est pertinent.	14/01/2023

4.2. Langages de développement

N°	Titre	Date de MàJ
DO02-01	Hors progiciel du marché, les langages de développement utilisables sont : Java, PHP ou Javascript.	14/04/2023
DO02-02	Il est demandé d'utiliser l'intégration continue de Gitlab pour le cycle de vie applicatif (build, packaging, tests automatisés,...).	31/01/2023
DO02-03	Les packages doivent être mis à disposition sur le service Nexus RIE du CISIRH.	31/01/2023
DO02-04	La liste des repository nécessaires à la compilation et au packaging d'une application doit être indiquée dans la documentation.	31/01/2023
DO02-05	La présence de commentaires dans le code est fortement recommandée, surtout sur les parties de codes complexes.	31/01/2023
DO02-06	La documentation doit être à présente avec à minima les informations suivantes : Description des méthodes, des paramètres d'entrée/sortie et des exceptions et erreurs	31/01/2023
DO02-07	Pour un développement externalisé, la politique de qualité du code du prestataire doit être précisée : par exemple checkstyle, PMD, cobertura, sonar, findbugs, formatter Eclipse etc. et la politique / fichiers de configuration associés doivent être livrés au CISIRH.	31/01/2023
DO02-08	L'utilisation de framework permettant de gérer la structure des projets (l'injection de dépendances, configuration) est obligatoire.	31/01/2023
DO02-09	Le développement par couche est demandé avec à minima les couches : • Présentation ou Controller • Métier ou service • DAO	31/01/2023

N°	Titre	Date de MàJ
DO02-10	Chaque nouvelle fonction (ou réécriture d'une fonction déjà existante) doit être couverte par des tests unitaires. Le rapport d'exécution de ces tests unitaires doit être remonté dans SonarQube.	31/01/2023
DO02-11	Sur les projets Java, le groupId à utiliser est « fr.gouv.cisirh.[nomProjet] », l'artifactId correspond au nom du module applicatif.	31/01/2023
DO02-12	Aucune référence aux environnements de développement ou d'intégration ne doit être présente dans les fichiers de configuration ni le code source afin de garantir la portabilité du build sur les environnements du CISIRH.	23/06/2023
DO02-13	Il est demandé de placer un fichier README.md au format Markdown à la racine de chaque module applicatif.	31/01/2023
DO02-14	Le fichier README.md doit contenir à minima : • Le nom du projet – nom du module en titre niveau 1 • Nom de l'équipe en charge du module • Un chapitre description de niveau 2 présentant le projet et le module applicatif • Un chapitre build de niveau 2 présentant la procédure de packaging à partir des sources Le reste est laissé libre.	31/01/2023
DO02-15	La procédure de compilation et de packaging de l'application doit être réalisable sur la plateforme d'intégration continue Gitlab du CISIRH. **Une erreur de compilation entraîne un rejet de livraison.**	31/01/2023

4.3. Tiers application

N°	Titre	Date de MàJ
DO03-01	Les applications JAVA doivent fonctionner avec le(s) conteneur(s) de servlet référencé(s) dans le CCT ou être exécutées en mode fatjar.	31/01/2023
DO03-02	Dans une application web, un client ne peut communiquer avec son serveur d'application qu'en https.	31/01/2023

4.4. Tiers données

N°	Titre	Date de MàJ
DO04-01	L'accès aux bases de données n'est possible que depuis le tiers application.	31/01/2023
DO04-02	L'utilisation des triggers dans une base de données est déconseillée et doit être systématiquement justifiée dans le dossier d'architecture.	31/01/2023
DO04-03	L'utilisation des procédures stockées n'est permise que dans les cas où les performances attendues ne peuvent être atteintes sans elles.	31/01/2023
DO04-04	Le tiers données et application ne sont pas sur le même serveur.	31/01/2023
DO04-05	La méthode et les contraintes pour sauvegarder les données doit être indiqué dans la documentation d'exploitation.	31/01/2023
DO04-06	Si la base de données contient des données personnelles et que le SGBD permet le chiffrement, il est fortement recommandé de procéder au chiffrement de la base de données, conformément à la réglementation.	31/01/2023
DO04-07	Les SGBDR utilisés pour les données persistantes au CISIRH sont ORACLE (privilégié), MariaDB et PostgreSQL (uniquement si le produit n'est pas compatible avec les deux SGBDR précédents).	14/04/2023
DO04-08	Les bases de données hors production doivent être mutualisées, chaque environnement applicatif disposera d'un ou plusieurs schémas dédiés.	01/04/2025

4.5. Tiers présentation

N°	Titre	Date de MàJ
DO05-01	Les applications doivent pouvoir être placées derrière un reverse proxy de type apache httpd et un répartiteur de charge de type HAProxy sans impact sur l'applicatif.	31/01/2023
DO05-02	Si une affinité de session doit être conservée entre les silos, cela doit être explicité dans le document d'architecture.	31/01/2023

5. Réseau

N°	Titre	Date de MàJ
RE01-01	Les différentes plateformes du CISIRH sont constituées d'un datacenter projet, d'un datacenter de production et d'un datacenter de secours.	31/01/2023
RE01-02	Tous les datacenters du CISIRH ont un point d'accès au RIE (Réseau interministériel de l'État) permettant des communications avec des applications inter ministérielles.	31/01/2023
RE01-03	Le point de terminaison SSL côté CISIRH doit aboutir sur un F5.	31/01/2023
RE01-04	La connexion d'un serveur vers l'extérieur passe obligatoirement par un proxy sortant.	31/01/2023
RE01-05	Le CISIRH est protégé par un équipement de sécurité type firewall.	31/01/2023
RE01-06	Tout composant raccordé au réseau doit se conformer au plan d'adressage IP du CISIRH.	31/01/2023
RE01-07	La topologie des infrastructures mutualisées (réseaux d'accès, réseaux de stockage…) ne peut évoluer dans le seul but de satisfaire les besoins d'une application spécifique.	31/01/2023
RE01-08	Les flux applicatifs doivent s'appuyer sur des protocoles de transport standardisés : - TCP pour le mode connecté, - UDP pour l'échange de messages asynchrones.	31/01/2023
RE01-09	L'application utilisera des protocoles routables au-dessus de TCP.	31/01/2023
RE01-10	Les ports applicatifs doivent être fixes, uniques et conformes au référentiel des ports du CISIRH. L'architecte du Bureau Technique est en charge de ce référentiel.	31/01/2023
RE01-11	Tout port non nécessaire au fonctionnement normal d'une application doit être fermé.	31/01/2023
RE01-12	Les ports spécifiques utilisés doivent être paramétrables pour permettre leur affectation lors des installations, évitant ainsi les doublons éventuels entre applications et facilitant les contrôles de flux réseau.	31/01/2023
RE01-13	L'utilisation des ports doit obligatoirement être conforme aux recommandations de l'IANA (ports standards compris entre 0 et 1023 et ports spécifiques à partir de 1024).	31/01/2023
RE01-14	Il est demandé de renseigner dans le document d'architecture de l'application (DA) une matrice des flux présentant pour chacun le port, le protocole, la source et la destination tant pour les services internes qu'externe à l'application et au CISIRH. Les ports non présents dans cette matrice seront considérés fermés.	31/01/2023
RE01-15	La mise à jour de la matrice des flux du projet doit être réalisée tout au long du cycle de vie du projet.	31/01/2023

6. Sécurité

6.1. Cryptographie

N°	Titre	Date de MàJ
CR-01	En fonction de l'analyse des risques et son plan d'action, l'application devra implémenter les mesures permettent d'assurer l'intégrité des donnée et leur confidentialité conformément au point 17 du guide « Sécurité des données personnelles » de la CNIL	07/07/2023

6.2. Transfert de documents contenant des données à caractères personnelles

N°	Titre	Date de MàJ
SE02-01	La confidentialité d'informations ou de documents entraîne de facto l'utilisation d'un outil de chiffrement adéquat conformément aux règles fixées par le référentiel général de sécurité (RGS). Par défaut, le logiciel utilisé sera **ZED!**.	31/01/2023

6.3. Applications

N°	Titre	Date de MàJ
SE03-01	Les applications doivent se conformer à la PSSIE (Politique de sécurité des systèmes d'information de l'Etat), voir http://www.ssi.gouv.fr/uploads/2014/11/pssie_anssi.pdf	31/01/2023
SE03-02	Les applications doivent se conformer aux référentiels de sécurité ministériels.	31/01/2023
SE03-03	Tout projet doit disposer d'une Note d'orientation SSI afin de préciser les objectifs de sécurité et de fixer la démarche d'intégration de la sécurité	07/07/2023
SE03-04	La solution technique doit s'intégrer à l'infrastructure actuelle du CISIRH et être conforme aux règles de sécurité applicables ainsi qu'au corpus documentaire du système de management de la sécurité de l'information et de la protection des données du CISIRH . D'une manière générale, elle doit être à l'état de l'art sur les aspects sécurité. Elle doit prendre en compte l'ensemble des recommandations de l'ANSSI.	31/01/2023
SE03-05	De façon générale et sauf avis contraire du CISIRH, l'authentification est réalisée sur le portail des applications interministérielles du CISIRH.	07/07/2023
SE03-06	Toute fonction d'authentification s'appuyant sur un couple « identifiant/mot de passe » mise en place dans le cadre d'un projet doit respecter les règles de base suivantes. Le système doit : • contraindre une complexité minimale obligatoire paramétrable (nombre de caractères en général, types de caractères); • forcer le changement de mot de passe au-delà d'une durée paramétrable; • empêcher la réutilisation des X (paramétrable) derniers mots de passe; • bloquer temporairement (durée paramétrable) le compte au-delà de X (paramétrable) tentatives infructueuses; • en cas d'erreur sur le mot de passe ou l'identifiant, le message renvoyé par le système ne doit pas indiquer si le compte existe ou non. • stocker une empreinte des mots de passe, générée selon un algorithme conforme au RGS. Une fonction de hachage doit être utilisée, avec une graine (« salt ») différente pour chaque utilisateur. En aucun cas le mot de passe ne doit être enregistré en clair dans la base.	31/01/2023
SE03-07	Un mot de passe ne doit **jamais** être stocké en clair dans une base de données ou un annuaire LDAP.	31/01/2023
SE03-08	Tout projet doit implémenter une durée de session maximum paramétrable	07/07/2023
SE03-09	La durée de session d'une application Web est par défaut de 30 minutes.	31/01/2023
SE03-10	Les serveurs d'application, batch, script doivent être exécutés avec un utilisateur système dédié autre que root. Il appartient aux développeurs de définir cet utilisateur dans la documentation d'exploitation en accord avec les équipes techniques du CISIRH.	31/01/2023

N°	Titre	Date de MàJ
SE03-11	Un utilisateur ne doit avoir accès qu'à son périmètre de gestion. Pour cela, l'application doit disposer d'une solution de gestion de profils applicatifs.	17/03/2023
SE03-12	Le protocole https est obligatoire pour tous les échanges. Plus généralement, un mot de passe ne doit jamais circuler en clair sur le réseau et ne jamais être écrit dans les fichiers de logs.	31/01/2023
SE03-13	L'utilisation du système d'échange est obligatoire pour les échanges externes. Le protocole de référence est PeSIT/TLS à l'état de l'art.	31/01/2023
SE03-14	Pour les échanges internes, il est préconisé de s'appuyer sur le système d'échanges. L'utilisation de rsync peut être autorisé après analyse.	31/01/2023
SE03-15	Les applications doivent être conformes aux recommandations de l'OWASP afin de se protéger contre les 10 principaux risques identifiés : http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project	31/01/2023
SE03-16	Lors de l'accès aux données, si un requête SQL utilise des paramètres, elle doit utiliser des requêtes préparées, par exemple par l'utilisation de **preparedStatement** ou **namedQuery**.	07/07/2023
SE03-17	Les interfaces d'une application ne doivent pas faire apparaître d'information sur l'architecture mise en place (serveur web, conteneur de servlet, OS, service applicatif, port, adresse IP, etc..). Ces informations ne doivent jamais être transmises, y compris en cas d'erreur.	31/01/2023
SE03-18	Les messages d'erreur doivent être anonymisés, par exemple en cas d'erreur d'authentification, le message ne doit pas distinguer les cas de mauvais login des cas de mauvais mot de passe.	31/01/2023
SE03-19	Les données dynamiques affichées en page HTML doivent être échappées et contrôlées afin d'éviter les failles XSS.	31/01/2023
SE03-20	Pendant tout le cycle de vie de l'application, les développements doivent rester compatibles avec les mises à jour de sécurité des logiciels utilisés (système d'exploitation, serveur web, moteur de servlets, bases de données...).	31/01/2023
SE03-21	Les événements pertinents en matière de sécurité, par exemple une connexion en tant qu'administrateur global de l'application, une suppression de données non réversible, doivent être inscrits dans un fichier journal, celui du système ou un journal propre à l'application, dans un format standard.	31/01/2023
SE03-22	La télémaintenance par des prestataires externes hors des locaux et des moyens du CISIRH est proscrite à tout moment de la vie du projet puis de l'application en l'absence de cadrage contractuel suffisant. Dans tous les cas, la connexion doit se faire depuis la France métropolitaine.	14/04/2023
SE03-23	L'accès aux statistiques non applicatives sera restreint aux agents en charge du suivi applicatif et aux administrateurs systèmes. L'accès aux connexions système sera restreint aux administrateurs systèmes.	31/01/2023

N°	Titre	Date de MàJ
SE03-24	Afin de garantir une bonne sécurité de l'application, il doit être possible de distinguer de manière fiable par leur URL les pages destinées au grand public (front-office), de celles destinées aux utilisateurs internes et aux administrateurs (back-office).	31/01/2023
SE03-25	Le nom des utilisateurs (et mot de passe) des bases de données n'est pas défini par le maître d'œuvre. Il doit être possible de les changer à tout moment sans impact pour l'applicatif en dehors de la modification de fichiers de configuration.	31/01/2023
SE03-26	Toutes les applications du CISIRH font l'objet d'un audit de sécurité annuel par un prestataire qualifié par l'ANSSI. Le responsable du développement s'engage à apporter les modifications suite aux éventuelles vulnérabilités détectées.	31/01/2023
SE03-27	Les données en entrées d'un système (IHM, Web Services et paramètres de batchs) doivent être contrôlées (format, taille, etc.) côté serveur.	31/01/2023
SE03-29	Les flux réseau pour lesquels la confidentialité et/ou l'intégrité doivent être garanties, qu'ils soient entre l'utilisateur et l'application ou entre deux systèmes, doivent être sécurisés par le biais de protocoles conformes au RGS (le plus souvent TLS). En aucun cas un secret ne doit circuler en clair sur le réseau.	31/01/2023
SE03-30	Les applications utilisent des ressources mutualisées. Elles ne sont pas autorisées à modifier le paramétrage d'exploitation et de sécurité des environnements dans lesquels elles s'exécutent. Les modifications de la configuration système peuvent être réalisées au sein d'un processus séparé par les administrateurs système.	31/01/2023
SE03-31	Pour les fonctions de sécurité telles que des fonctions d'identification, de signature électronique, de confidentialité ou d'horodatage, lorsque des produits validés par l'ANSSI existent, ils doivent être privilégiés.	31/01/2023
SE03-32	Les adresses de réponse « no-reply » doivent être au format « ***ne-pas-repondre.application@cisirh.finances.gouv.fr*** ». Pour les environnements hors production, le nom de l'environnement doit être précisé.	01/04/2025

6.4. Logiciels à la demande (SaaS)

N°	Titre	Date de MàJ
SE04-01	L'utilisation de logiciels à la demande (SaaS) doit être soumise à une homologation de sécurité.	31/01/2023

6.5. *Poste de travail*

N°	Titre	Date de MàJ
SE05-01	Le CISIRH fournit un poste de travail, seul autorisé à se connecter sur le système d'information du CISIRH.	31/01/2023
SE05-02	L'environnement de travail doit être protégé contre les virus, les logiciels malveillants et les intrusions.	31/01/2023
SE05-03	Ni l'utilisation d'une application ni son installation ne doivent nécessiter la désactivation ou gêner la mise à jour de l'antivirus et/ou de l'anti-logiciels malveillants et/ou du pare-feu.	31/01/2023
SE05-04	Sauf instruction contraire par les responsables sécurité, les systèmes d'exploitation et les logiciels installés sur les stations de travail doivent être à jour des correctifs validés par les structures en charge de la sécurité du SI.	31/01/2023

6.6. *Formats d'échange*

6.6.1. Général

N°	Titre	Date de MàJ
FE01-01	Tout fichier XML doit être accompagné de son schéma.	31/01/2023
FE01-02	Afin d'éviter tout problème d'encodage, l'UTF-8 est demandé sur toute la chaîne applicative.	31/01/2023
FE01-03	Les échanges de documents bureautiques internes et externes doivent respecter la politique de gestion documentaire du CISIRH.	31/01/2023
FE01-04	Pour les échanges de données, l'utilisation du format JSON ou XML est recommandée.	31/01/2023

6.6.2. Multimédia

N°	Titre	Date de MàJ
FE02-01	Les formats PNG et JPEG doivent être utilisés pour échanger les informations graphiques et les images fixes.	31/01/2023
FE02-02	Les flux audiovisuels, autorisés par le CISIRH, doivent respecter les formats MPEG-2 ou MPEG-4.	31/01/2023

7. Règles supprimées

Ce paragraphe regroupe les règles qui ont été supprimées ainsi qu'une explication associée.

N°	Titre	Raison
SE03-28	Pendant tout le cycle de vie de l'application, les développements doivent rester compatibles avec les mises à jour de sécurité des logiciels utilisés (système d'exploitation, serveur web, moteur de servlets, bases de données...).	Doublon avec SE03-20. Contenu de SE03-20 remplacé.
AT-API-07	Dans le cadre de la mise en œuvre d'une architecture orientée service, il est recommandé de s'appuyer sur les Web Services REST ou SOAP.	Doublon avec AT-API-04
AT-API-08	L'utilisation des Web Services REST est à privilégier.	Doublon avec AT-API-04

Annexes

Format de logs Log4J

(https://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html):

```
ErrorLogFormat "{ \"time\":\"%{%Y-%m-%d}tT%{%T}t.%{msec_frac}tZ\", \"function\" : \"[%-m:%l]\" , \"process\" : \"[pid %P:tid %T]\" , \"message\" : \"%M\" ,\ \"referer\"\ : \"%{Referer}i\" },"

LogFormat "{ \"time\":\"%{%Y-%m-%d}tT%{%T}t.%{msec_frac}tZ\", \"process\":\"%D\", \"filename\":\"%f\", \"remoteIP\":\"%a\", \"host\":\"%V\", \"request\":\"%U\", \"query\":\"%q\", \"method\":\"%m\", \"status\":\"%>s\", \"userAgent\":\"%{User-agent}i\", \"referer\":\"%{Referer}i\" }," combined
```

où :

%d correspond à la date du log (au format yyyy-MM-dd HH:mm:ss,SSS)

%p correspond au niveau de log (INFO, DEBUG, ERROR, etc.)

%t correspond au nom du thread courant

%C correspond au nom de la classe générant le log

%m correspond au message

remarque : En cas de problème de performance, il est possible de ne pas utiliser le **%C**

Le chiffre suivant le %C et entre {} correspond à une limitation dans le nom complet de la classe + package. Il est laissé libre.

Le message doit contenir un code permettant d'identifier l'utilisateur ayant déclenché ce message, si le message est lié à une action utilisateur.