

|  |  |
| --- | --- |
|  | Principes d’architecture |

|  |  |
| --- | --- |
|  | CNSA |
|  |  |
|  | Date : 04/03/2024  Version : 1.3 |

HISTORIQUE

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Rédacteurs | Objet |
| 30/08/2023 | 1.0 | Serge Barbosa | Version initiale |
| 31/10/2023 | 1.1 | Serge Barbosa | Prise en compte des remarques internes DSI et du Gartner |
| 25/02/2024 | 1.2 | Younès CHADLI | Revue du document |
| 04/03/2024 | 1.3 | Serge Barbosa | Finalisation du document avant validation |

DOCUMENTS DE REFERENCE

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Référence | Objet |
| 14/03/2022 |  | COG | Convention d’objectifs et de gestion État-CNSA 2022-2026 |
|  |  | SDSI | Schéma Directeur des Systèmes d’Information aligné avec la COG |

LISTE DE DIFFUSION

|  |  |
| --- | --- |
| Participants | Rôle |
|  |  |
|  |  |

AIDE A LA LECTURE

|  |  |  |  |
| --- | --- | --- | --- |
| A lire | Problème | Idée | A faire |
| Point bloquant | Note | Confidentiel |  |

TABLE DES MATIERES

[1 Introduction 4](#_Toc160456662)

[1.1 Périmètre du document 4](#_Toc160456663)

[1.2 Public visé 4](#_Toc160456664)

[1.3 Ambition stratégique de la branche autonomie à horizon 2026 4](#_Toc160456665)

[1.4 Schéma directeur du système d’information 5](#_Toc160456666)

[2 Enjeux du Système d’Information 7](#_Toc160456667)

[2.1 E1 : Simplifier les parcours 7](#_Toc160456668)

[2.2 E2 : Doter la CNSA et ses partenaires d’outils performants au service de la mission 8](#_Toc160456669)

[2.3 E3 : Préserver la sécurité des systèmes, des données et des personnes 8](#_Toc160456670)

[2.4 E4 : Respect de la doctrine technique du numérique en santé 9](#_Toc160456671)

[3 Principes d’Architecture 10](#_Toc160456672)

[3.1 P1 : Hébergement 11](#_Toc160456673)

[3.2 P2 : Architectures techniques 12](#_Toc160456674)

[3.3 P3 : Solutions applicatives 13](#_Toc160456675)

[3.4 P4 : Découplage des composants 14](#_Toc160456676)

[3.5 P5 : Briques technologiques 15](#_Toc160456677)

[3.6 P6 : Conformité de la sécurité SI 16](#_Toc160456678)

[3.7 P7 : Exploitabilité 17](#_Toc160456679)

[3.8 P8 : Résilience 18](#_Toc160456680)

[3.9 P9 : Expérience utilisateur 19](#_Toc160456681)

[3.10 P10 : Accès et habilitations 20](#_Toc160456682)

[3.11 P11 : Référentiels de données 21](#_Toc160456683)

[3.12 P12 : Durabilité 22](#_Toc160456684)

# Introduction

## Périmètre du document

Le document est construit en s’appuyant sur les enjeux du SI qui sont déclinés d’une part de l’ambition stratégique issue de la Convention d’Objectifs de Gestion [COG] et d’autre part du Schéma Directeur du Système d’Information [SDSI].

Le document présente les enjeux du système d’information et détaille les principes d’architecture associés.

Ces principes sont applicables dans cadre de la création et/ou la modification d’applications au sein de la CNSA.

## Public visé

Ce document s’adresse aux chefs de projets et responsables de pôles de la direction des systèmes d’informations et est applicable dans les choix de solutions et d’architecture auprès des prestataires en maitrise d’œuvre.

Il s’adresse également aux responsables métiers de la CNSA sur certains aspects comme la sécurité, l’ergonomie ou l’utilisation de briques technologiques mutualisées.

## Ambition stratégique de la branche autonomie à horizon 2026

La Convention d’Objectifs de Gestion [COG] de la branche Autonomie de la Sécurité sociale fixe la feuille de route pour consolider le service public de l’autonomie dans l’ensemble du territoire, dans la perspective du cap de 2030.

Les orientations et engagements associés sont résumées ci-dessous :

|  |
| --- |
| **O1 : Garantir la qualité du service public territorial de l’autonomie pour les personnes âgées, les personnes en situation de handicap et leurs proches.** |

1. Assurer l’accès de toutes les personnes à l’information, aux droits et à la citoyenneté.
2. Accompagner les professionnels des services départementaux et des MDPH pour favoriser la qualité de service et l’équité de traitement.
3. Soutenir l’autonomie des personnes âgées par la prévention et la lutte contre l’isolement social.
4. Garantir l’effectivité des droits et simplifier le parcours des personnes.

|  |
| --- |
| **O2 : Garantir un accompagnement adapté aux besoins des publics qui aspirent à vivre « chez eux », dans leur environnement de vie, en établissement et à domicile, en étant bien accompagnés.** |

1. Améliorer la connaissance des besoins et des solutions.
2. Soutenir les ARS et les conseils départementaux dans le pilotage de l’approche domiciliaire pour une offre ouverte et inclusive.
3. Aider ceux qui aident : soutenir l’attractivité des métiers de la branche et renforcer l’appui aux aidants.
4. Faciliter l’accès aux aides techniques.

|  |
| --- |
| **O3 : Structurer et outiller la nouvelle branche autonomie** |

1. Conforter le pilotage financier de la nouvelle branche Autonomie et structurer une stratégie de gestion du risque porté par la branche.
2. Renforcer l’efficience de la dépense en ESMS.
3. Favoriser le pilotage des politiques d’autonomie par les acteurs territoriaux.
4. Doter la branche Autonomie de systèmes d’information performants.
5. Adapter l’organisation des services aux missions nouvelles de la CNSA.

## Schéma directeur du système d’information

Le Schéma Directeur du Système d’Information [SDSI] fixe la feuille de route pour développer le Système d’Information en réponse à la Convention d’Objectifs de Gestion [COG], dans la perspective du cap de 2030.

Les axes et thématiques associés sont résumés ci-dessous :

|  |
| --- |
| **A1 : Développer un SI soutenant la qualité de service et d’accès aux droits.** |

Proposer une **offre de services moderne et harmonisée,** assurer l’**accès** de toutes les personnes à **l’information, aux droits et à la citoyenneté** et **accompagner les réseaux** dans le déploiement du numérique :

1. Mettre en œuvre un SI de gestion des prestations individuelles PA (**APA**)
2. Poursuivre le développement et le déploiement des SI de gestion des prestations individuelles PH (**MDPH**)
3. Faire évoluer les **portails d’information grand public** et assurer une meilleure expérience utilisateur via la proposition de téléservices notamment et l’interconnexion avec les portails d’autres organismes de la sécurité sociale
4. Simplifier les **parcours usagers** et généraliser la mesure de satisfaction des usagers des portails et outils de la CNSA
5. Mettre en œuvre des outils de gestion et portails collaboratifs pour une relation renouvelée et une meilleure **animation des réseaux** (CRM, extranet rénové…)​

|  |
| --- |
| **A2 : Renforcer la connaissance et le pilotage par la donnée de la 5e Branche.** |

Répondre aux besoins de **contrôle**, de **gestion** et d’**amélioration de la connaissance** des besoins et de l’offre et mettre en œuvre un **SI de l’offre** et **des outils et une politique d’innovation autour de la donnée**:

1. Elaborer et mettre en œuvre une démarche de gouvernance des données transverse à la caisse
2. Améliorer le recueil des données nécessaires à une gestion efficiente de l’offre et mettre en place un SI de l’offre à destination des acteurs du médico-social (ESMS et SAAD), des ARS et des CD
3. Renforcer l’outillage de la caisse en termes d’aide de la décision à travers la mise à disposition de tableaux de bord et un portail décisionnel à destination de la CNSA

|  |
| --- |
| **A3 : Transformer le cœur du SI de la branche.** |

Contribuer au **positionnement** et à l’**efficience** de la CNSA dans son **rôle de gestionnaire du risque autonomie** au travers d’une **architecture fonctionnelle et technique** modernisée et sécurisée et **d’une gouvernance** renforcée :

1. Renforcer l’outillage des fonctions support à la CNSA sur des périmètres prioritaires
2. Formaliser la stratégie de la caisse en termes d’architecture, d’urbanisation et d’externalisation et assurer le pilotage des SI
3. Renforcer la sécurité et l'interopérabilité des systèmes d’information et des données​ et moderniser l'infrastructure, mettre en place une stratégie gestion de l'obsolescence et de la dette technique et applicative
4. Assurer le maintien et l’exploitation des SI existants et nouveaux et piloter les engagements de service du système d’information (disponibilité, performance)​

# Enjeux du Système d’Information

Les enjeux du SI sont identifiés et listés dans le tableau ci-dessous :

|  |  |
| --- | --- |
| # | Enjeux |
| E1 | Simplifier les parcours |
| E2 | Doter la CNSA et ses partenaires d’outils performants au service de la mission |
| E3 | Préserver la sécurité des systèmes, des données et des personnes |
| E4 | Respect de la doctrine technique du numérique en santé |

## E1 : Simplifier les parcours

|  |
| --- |
| **Enoncé** |
| * Simplifier les parcours |
| **Implication** |
| * Fournir des IHM accessibles à tout public * Harmoniser les interfaces homme-machine * Identifier l'usager sur l'ensemble de son parcours * Référencer les données de l'usager ainsi que son parcours * Référencer les annuaires du médico-social |
| **Principes** |
| * P9 : Expérience utilisateur * [P10 : Accès et habilitations](#_P10_:_Accès) * [P11 : Référentiels de données](#_P11_:_Référentiels) |

## E2 : Doter la CNSA et ses partenaires d’outils performants au service de la mission

|  |
| --- |
| **Enoncé** |
| * Doter la CNSA et ses partenaires d’outils performants au service de la mission |
| **Implication** |
| * Harmoniser les interfaces homme-machine * Identifier de manière unique le partenaire sur tous les outils * Gérer le contrôle d’accès et les habilitations d’accès aux outils au plus près du partenaire * Mettre à disposition des outils un référentiel de données fiables |
| **Principes** |
| * [P1 : Hébergement](#_P1_:_Hébergement) * [P2 : Architectures](#_P2_:_Choix) * [P3 : Solutions applicatives](#_P3_:_Choix) * [P4 : Découplage des composants](#_P4_:_Découplage) * [P5 : Briques technologiques](#_P5_:_Briques) * [P9 : Expérience utilisateur](#_P9_:_Ergonomie) * [P10 : Accès et habilitations](#_P10_:_Accès) * [P11 : Référentiels de données](#_P11_:_Référentiels) |

## E3 : Préserver la sécurité des systèmes, des données et des personnes

|  |
| --- |
| **Enoncé** |
| * Préserver la sécurité des systèmes, des données et des personnes |
| **Implication** |
| * S’appuyer sur un hébergement adapté aux données de santé * Mettre en œuvre les mesures adaptées aux besoins de sécurité * Gérer le contrôle d’accès et les habilitations d’accès aux outils au plus près du partenaire |
| **Principes** |
| * [P1 : Hébergement](#_P1_:_Hébergement) * [P6 : Conformité de la sécurité SI](#_P6_:_Sécurité) * [P8 : Résilience](#_P8_:_Résilience) * [P10 : Accès et habilitations](#_P10_:_Accès) |

## E4 : Respect de la doctrine technique du numérique en santé

|  |
| --- |
| **Enoncé** |
| * Respect de la doctrine technique du numérique en santé |
| **Implication** |
| * Choisir des solutions respectant la doctrine technique du numérique en santé * Mettre en œuvre les mesures adaptées aux besoins de sécurité |
| **Principes** |
| * [P3 : Solutions applicatives](#_P3_:_Choix) * [P6 : Conformité de la sécurité SI](#_P6_:_Sécurité) * [P7 : Exploitabilité](#_P7_:_Exploitabilité) * [P8 : Résilience](#_P8_:_Résilience) * P12 : Durabilité |

# Principes d’Architecture

Les principes d’architecture sont reliés aux enjeux de la CNSA. Ils sont des règles et des lignes directrices fondamentales qui orientent la conception et le développement des systèmes d'information de la CNSA.

Ils servent à assurer que l'architecture IT soutient et est alignée avec les objectifs stratégiques de la CNSA, tout en promouvant l'efficacité, la sécurité, l'interopérabilité et la durabilité.

Ces principes couvrent divers aspects, tels que, la gouvernance IT, la gestion des données, l'expérience utilisateur, l'éco-responsabilité, la sécurité des informations, et l'infrastructure technologique.

Ils aident à guider les décisions concernant le choix des technologies, la conception des systèmes, la gestion des risques et la conformité réglementaire, contribuant ainsi à une architecture IT cohérente, flexible, et évolutive.

## P1 : Hébergement

|  |  |  |
| --- | --- | --- |
| **Identification du principe** | | |
| **Nom : Hébergement** | **Numéro de version : V1.0** | **Date de publication : 01/09/2023** |
| **Description** | | |
| **Le principe d'architecture "Hébergement"** se concentre sur la stratégie et les pratiques encadrant le déploiement et la gestion des environnements d'exécution des applications et des données au sein d'un système d'information (SI). Ce principe guide les choix concernant où et comment les applications, les services et les données sont hébergés pour optimiser la performance, la sécurité, la résilience et l'efficacité des coûts. | | |
| **Objectifs** | | |
| * **Sécurité et Conformité** : Garantir que l'hébergement des applications et des données respecte les exigences de sécurité et les réglementations en vigueur. * **Performance et Disponibilité** : Assurer une haute disponibilité et une performance optimale des services et des applications. * **Scalabilité et Flexibilité** : Permettre aux infrastructures d'accueillir la croissance et l'évolution des besoins de la CNSA, en adaptant les ressources de manière efficace. * **Efficience Coût** : Optimiser les coûts liés à l'hébergement, en évaluant les options telles que l'hébergement sur site, le cloud (public, privé, hybride) ou des solutions mixtes. * **Récupération après Sinistre et Continuité d'Activité** : Intégrer des stratégies de reprise après sinistre et de continuité d'activité adaptées à l'importance des systèmes hébergés. | | |
| **Directives de Mise en Œuvre** | | |
| * Le mode d’hébergement doit respecter la doctrine Cloud au centre (<https://www.numerique.gouv.fr/services/cloud/doctrine/>) * Les certifications HDS « hébergeur d’infrastructure physique » et « hébergeur infogéreur » (<https://esante.gouv.fr/labels-certifications/hds/certification-des-hebergeurs-de-donnees-de-sante>) sont exigées si l’application gère des données de santé * Les applications qui ne sont pas « cœur de métier » peuvent déroger à ce principe * Être en conformité avec les règlementations Françaises et Européennes * Mise en place d’un référentiel des capacités métier qui sont cœur de métier * Une étude de migration des applications ne respectant pas ce principe devra être menée | | |
| **Indicateurs de performance** | | |
| * Pourcentage des hébergements des applications métiers devant respecter ce principe. * Indicateurs de disponibilité et performance en mesurant la disponibilité et la performance des applications et services en fonction des objectifs définis. * Réponse aux Incidents en évaluant l'efficacité des plans de récupération après sinistre et de continuité d'activité lors des incidents. | | |

## P2 : Architectures techniques

|  |  |  |
| --- | --- | --- |
| **Identification du principe** | | |
| **Nom : Architectures techniques** | **Numéro de version : V1.0** | **Date de publication : 01/09/2023** |
| **Description** | | |
| **Le principe d'architecture « Architectures techniques »** guide la manière dont les décisions architecturales sont prises au sein de la CNSA pour le développement et la gestion de son système d'information (SI). Ce principe vise à s'assurer que les choix architecturaux soutiennent ses objectifs stratégiques, favorisent l'innovation, et garantissent l'alignement entre la technologie et les besoins métier. Il encourage une approche réfléchie et stratégique dans la sélection des architectures de SI, incluant les architectures d'applications, de données, et d'infrastructure. | | |
| **Objectifs** | | |
| * **Alignement Stratégique** : Assurer que les choix architecturaux sont en parfaite adéquation avec les stratégies et objectifs métier de l'organisation. * **Cohérence et Standardisation** : Favoriser la cohérence et la standardisation à travers le SI pour améliorer l'interopérabilité, la réutilisabilité et la maintenance. * **Agilité et Flexibilité** : Permettre au SI de s'adapter rapidement aux changements de l'environnement d'affaires grâce à des architectures flexibles et évolutives. * **Optimisation des Coûts** : Réduire les coûts totaux de propriété en faisant des choix architecturaux qui optimisent l'utilisation des ressources et minimisent les dépenses redondantes. * **Sécurité et Conformité** : Intégrer la sécurité et la conformité réglementaire dès la phase de conception pour protéger les actifs informationnels. | | |
| **Directives de Mise en Œuvre** | | |
| * Toute nouvelle application ou refonte d’application suivra les recommandations des architectures de référence, patterns du cadre de cohérence technique de la CNSA ainsi que les principes d’architectures :   + L’utilisation de solutions SaaS est à privilégier   + Dans le cas de développements d’application il faut privilégier l’utilisation de conteneurs orchestrés * Réduire les risques liés à la dette technique * Valider les dossiers d’architecture en phase de conception * Définir une trajectoire pour les applications existantes * Conformité avec le règlement général d’interopérabilité (RGI) * Conformité avec le cadre d’interopérabilité des systèmes d’information de santé (<https://esante.gouv.fr/produits-services/ci-sis>) * Faciliter l’urbanisation du système d’information dans un environnement multi-cloud * Ce principe est une exigence lors de développement de nouvelles applications | | |
| **Indicateurs de performance** | | |
| * Pourcentage d’applications respectant ce principe ou ayant une trajectoire pour atteindre ce principe. * Pourcentage de flux utilisant la plateforme d’échange de la CNSA * Pourcentage d’applications respectant le cadre de cohérence technique | | |

## P3 : Solutions applicatives

|  |  |  |
| --- | --- | --- |
| **Identification du principe** | | |
| **Nom : Solutions applicatives** | **Numéro de version : V1.0** | **Date de publication : 01/09/2023** |
| **Description** | | |
| **Le principe d'architecture « Solutions applicatives »** est fondamental pour définir et guider la sélection des technologies, des plateformes, et des frameworks qui soutiennent les objectifs stratégiques d'une organisation à travers son système d'information (SI). Ce principe vise à assurer que les décisions prises en matière d'architecture sont alignées avec les besoins métier, les contraintes techniques, la sécurité, et les objectifs de durabilité et d'évolutivité de l'organisation. | | |
| **Objectifs** | | |
| * **Alignement Stratégique** : Assurer que les choix technologiques soutiennent les objectifs stratégiques de la CNSA et facilitent l'atteinte de ses objectifs métier. * **Cohérence et Standardisation** : Promouvoir l'utilisation de normes et de pratiques cohérentes pour faciliter l'intégration, la gestion et l'évolution du SI. * **Flexibilité et Évolutivité** : Sélectionner des solutions qui permettent une adaptation et une évolution aisées face aux changements de besoins métier ou technologiques. * **Optimisation des Coûts** : Évaluer les solutions d'architecture non seulement sur la base de leur coût initial mais aussi en tenant compte du coût total de possession (TCO) et du retour sur investissement (ROI). * **Sécurité et Conformité** : Intégrer les exigences de sécurité et de conformité réglementaire dès la phase de sélection des solutions d'architecture. | | |
| **Directives de Mise en Œuvre** | | |
| * Les solutions open source doivent être privilégiées aux solutions commerciales des Editeurs. * Dans le cas de développements d’application il faut privilégier l’utilisation de conteneurs orchestrés * Le choix se fera sans remettre en cause la performance attendue (pérennité, facilité d’utilisation, coût) et en minimisant l'enfermement propriétaire et en veillant à ne pas faire appel à des compétences rares. * Rationaliser les coûts * Réduire l’enfermement propriétaire * Etablir un cadre de cohérence technique à partir d’études de choix de solutions validées en Design Authority * Les composants et solutions utilisées doivent s’appuyer sur des standards afin de simplifier le remplacement d’un composant par un autre (découplage). | | |
| **Indicateurs de performance** | | |
| * Mesure du ROI, l’amélioration de la performance et la stabilité du SI des solutions choisies. | | |

## P4 : Découplage des composants

|  |  |  |
| --- | --- | --- |
| **Identification du principe** | | |
| **Nom : Découplage des composants** | **Numéro de version : V1.0** | **Date de publication : 01/09/2023** |
| **Description** | | |
| **Le principe d'architecture « Découplage des Composants »** est une stratégie clé dans la conception de systèmes d'information (SI) robustes, flexibles et évolutifs. Ce principe vise à réduire les dépendances directes entre différents composants d'un système pour faciliter les modifications, les mises à jour et l'intégration de nouvelles fonctionnalités sans perturber le fonctionnement global du système. En appliquant ce principe, les architectes s'efforcent de créer des architectures modulaires où les composants communiquent entre eux via des interfaces bien définies. | | |
| **Objectifs** | | |
| * **Flexibilité et Adaptabilité** : Faciliter l'ajout, la modification ou le remplacement de composants sans nécessiter de changements majeurs dans le reste du système. * **Facilité de Maintenance** : Simplifier la maintenance et les mises à jour en isolant les changements à des composants spécifiques. * **Réutilisabilité** : Promouvoir la réutilisation des composants dans différents contextes ou projets, réduisant ainsi le temps et le coût de développement. * **Résilience** : Améliorer la résilience du système en limitant l'impact des défaillances d'un composant sur les autres composants. * **Scalabilité** : Permettre une scalabilité plus aisée en distribuant ou en répliquant des composants spécifiques. * **Testabilité** : Faciliter le test des composants de manière indépendante, améliorant ainsi la qualité globale du système. | | |
| **Directives de Mise en Œuvre** | | |
| * Les composants et solutions utilisées doivent s’appuyer sur des standards afin de simplifier le remplacement d’un composant par un autre (découplage). * Les API REST doivent être privilégiés pour les échanges synchrones * Le développement sous forme de micro-services doit être privilégié * Conformité avec le règlement d’interopérabilité (RGI) * Faciliter l’urbanisation du système d’information dans un environnement multi-cloud * Ce principe est une exigence lors de développement de nouvelles applications * Mettre en place une plateforme d’échange | | |
| **Indicateurs de performance** | | |
| * Pourcentage d’applications développées en micro-services. * Pourcentage de flux utilisant la plateforme d’échange. * Reduction du temps pour développer et déployer de nouvelles fonctionnalités ou évolutions. | | |

## P5 : Briques technologiques

|  |  |  |
| --- | --- | --- |
| **Identification du principe** | | |
| **Nom : Briques technologiques** | **Numéro de version : V1.0** | **Date de publication : 01/09/2023** |
| **Description** | | |
| **Le principe d'architecture "Briques Technologiques"** se réfère à l'approche structurée dans la conception et le développement de systèmes d'information (SI), où les composants technologiques sont standardisés, réutilisables, et facilement intégrables. Ce principe vise à optimiser l'efficacité, réduire la complexité, et faciliter l'évolutivité et la maintenance du SI en décomposant l'architecture en modules ou "briques" bien définis. | | |
| **Objectifs** | | |
| * **Standardisation** : Promouvoir l'utilisation de technologies et de plateformes standardisées pour faciliter l'intégration et l'interopérabilité. * **Réutilisabilité** : Encourager la conception de composants qui peuvent être réutilisés dans différents contextes ou projets, réduisant ainsi le temps de développement et les coûts. * **Flexibilité et Évolutivité** : Assurer que le SI peut évoluer facilement en ajoutant, modifiant, ou remplaçant des briques technologiques sans perturber l'ensemble du système. * **Maintenance et Support** : Simplifier la maintenance et le support en réduisant la complexité grâce à l'utilisation de composants bien connus et largement adoptés. | | |
| **Directives de Mise en Œuvre** | | |
| * Les nouvelles briques technologiques et solutions sélectionnées par les projets doivent pouvoir bénéficier aux autres projets de la CNSA. * L’exposition sous la forme de services transverses sera soumise à décision à la DA. * Le développement de services transverses est porté par le projet métier qui en a émis le premier le besoin * Identifier les services transverses. | | |
| **Indicateurs de performance** | | |
| * Nombre de services transverses. * Pourcentage d’applications utilisant ces services. * Mesurer l'impact de la réutilisation des briques technologiques sur la réduction des coûts et des délais de développement des projets. | | |

## P6 : Conformité de la sécurité SI

|  |  |  |
| --- | --- | --- |
| **Identification du principe** | | |
| **Nom : Conformité de la sécurité SI** | **Numéro de version : V1.0** | **Date de publication : 01/09/2023** |
| **Description** | | |
| **Le principe d'architecture « Conformité de la Sécurité du Système d'Information (SI) »** souligne l'importance d'aligner la conception, le développement, et l'exploitation des systèmes d'information avec les normes, les lois, et les régulations en matière de sécurité des données et de protection de la vie privée. Ce principe vise à assurer que les systèmes d'information respectent non seulement les exigences internes de sécurité mais aussi les exigences légales et réglementaires externes, minimisant ainsi les risques de non-conformité, de sanctions, et de dommages à la réputation. | | |
| **Objectifs** | | |
| * **Besoins de sécurité** : Assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des données. * **Conformité Réglementaire** : Respecter les obligations légales et réglementaires liées à la sécurité et à la protection des données, la politique d’homologation de sécurité, la doctrine technique du numérique en santé. * **Gestion des Risques** : Identifier, évaluer, et atténuer les risques liés à la sécurité des données et à la conformité. * **Confiance des Partenaires et usages** : Renforcer la confiance des usagers et partenaires dans la gestion sécurisée des données. | | |
| **Directives de Mise en Œuvre** | | |
| * Les systèmes doivent appliquer les méthodes et règles du Référentiel Général de Sécurité (RGS) et de la politique de sécurité des systèmes d’information de la CNSA. * Toute application doit obtenir une homologation de sécurité avant mise en production. * L’Etat impose que tout téléservice doit avoir une homologation de sécurité. * Intégrer la sécurité dès la conception * Respecter la politique d’homologation de sécurité de la CNSA * Respecter le processus de suivi des homologations de la CNSA | | |
| **Indicateurs de mesures de performance** | | |
| * Pourcentage d’applications ayants une homologation de sécurité valide | | |

## P7 : Exploitabilité

|  |  |  |
| --- | --- | --- |
| **Identification du principe** | | |
| **Nom : Exploitabilité** | **Numéro de version : V1.0** | **Date de publication : 01/09/2023** |
| **Description** | | |
| **Le principe d'architecture "Exploitabilité"** se concentre sur la conception et le développement de systèmes d'information avec une attention particulière à leur facilité de maintenance, leur surveillance, leur diagnostic et leur adaptation en production. L'exploitabilité, souvent vue comme une extension de la fiabilité et de la performance, vise à assurer que les systèmes sont non seulement performants et fiables lors de leur déploiement initial, mais qu'ils peuvent aussi être efficacement exploités, surveillés et améliorés tout au long de leur cycle de vie. | | |
| **Objectifs** | | |
| * **Maintenabilité :** Simplifier la mise à jour, la modification et l'amélioration des systèmes pour répondre aux évolutions des besoins métier et technologiques. * **Surveillance et Diagnostics** : Permettre une surveillance proactive et des diagnostics efficaces pour identifier et résoudre rapidement les problèmes. * **Performance et Fiabilité** : Assurer que les systèmes répondent aux exigences de performance et de fiabilité sous des charges de travail variées. * **Récupération et Robustesse** : Faciliter la récupération rapide après des incidents et renforcer la robustesse face aux pannes et aux erreurs. * **Support Utilisateur Efficace** : Fournir un support rapide et efficace aux utilisateurs, en résolvant les problèmes et en répondant aux questions pour minimiser l'impact sur les opérations commerciales. | | |
| **Directives de Mise en Œuvre** | | |
| * Les systèmes (services, processus et activités) et les échanges doivent être supervisés auditables (observabilité). * Le processus de déploiement est de type CI/CD avec une frontière claire entre le développement et l’exploitation. * Respecter la doctrine technique du numérique en santé <https://esante.gouv.fr/sites/default/files/media_entity/documents/doctrine-du-numerique-en-sante_version-2022_vf.pdf> * Améliorer la maintenabilité du SI avec des responsabilités claires entre les différents acteurs. * Améliorer la robustesse du SI en identifiant rapidement les défaillances et en maintenant les services en conditions opérationnelles. | | |
| **Indicateurs de performance** | | |
| * Pourcentage d’applications utilisant les outils et principes d’exploitation de la CNSA | | |

## P8 : Résilience

|  |  |  |
| --- | --- | --- |
| **Identification du principe** | | |
| **Nom : Résilience** | **Numéro de version : V1.0** | **Date de publication : 01/09/2023** |
| **Description** | | |
| **Le principe d'architecture "Résilience"** est un fondement critique pour la conception, le développement, et l'exploitation de systèmes d'information (SI) qui doivent rester opérationnels et performants face à des incidents, des pannes ou des catastrophes. Ce principe vise à assurer la capacité d'un SI à anticiper, absorber, s'adapter à, et se rétablir rapidement après des événements perturbateurs, qu'ils soient d'origine naturelle, technique ou humaine. | | |
| **Objectifs** | | |
| * **Continuité des Opérations** : Garantir que les services essentiels et les fonctions critiques du SI peuvent continuer à fonctionner pendant et après un incident. * **Récupération Après Sinistre** : Assurer une récupération rapide et efficace des opérations et des données après une perturbation majeure. * **Adaptabilité** : Permettre au SI de s'adapter aux changements et aux menaces émergentes sans perturbation significative des services. | | |
| **Directives de Mise en Œuvre** | | |
| * Respecter la doctrine technique du numérique en santé. <https://esante.gouv.fr/sites/default/files/media_entity/documents/doctrine-du-numerique-en-sante_version-2022_vf.pdf> * Répondre aux enjeux métier de continuité de service. * Réduire les risques liés à la dette technique. * Disposer d’un PCA/PRA. (Plan de Continuité d’Activité/Plan de Reprise d’Activité). * Proposer des solutions pérennes dans cadre de cohérence technique * Mener des audits d’architecture, des tests de performances et de robustesse. * La résilience du système doit être adaptée au niveau de sécurisation requis pour le service. * Surveillance et gestion des incidents. * Intégrer la résilience dès la phase de conception des architectures. | | |
| **Indicateurs de performance** | | |
| * Pourcentage d’applications résilientes. * Synthèse des temps de rétablissements des applications après perturbation. | | |

## P9 : Expérience utilisateur

|  |  |  |
| --- | --- | --- |
| **Identification du principe** | | |
| **Nom : Expérience Utilisateur.** | **Numéro de version : V1.0** | **Date de publication : 01/09/2023** |
| **Description** | | |
| **Le principe d'architecture "Expérience utilisateur"** est une approche de conception et de développement qui place les utilisateurs au centre du processus de développement. L'objectif est de créer des produits qui répondent aux besoins réels des utilisateurs, faciles à utiliser, et qui offrent une expérience utilisateur (UX) positive. | | |
| **Objectifs** | | |
| * **Intuitivité et Facilité d'Utilisation** : Assurer que les systèmes sont faciles à apprendre et à utiliser pour les utilisateurs finaux, quel que soit leur niveau de compétence technique. * **Engagement Utilisateur** : Créer des expériences captivantes qui encouragent l'utilisation répétée et augmentent la satisfaction des utilisateurs. * **Accessibilité** : Garantir que les systèmes sont accessibles à tous les utilisateurs, y compris ceux ayant des besoins spécifiques ou des handicaps. * **Efficacité et Productivité** : Optimiser les flux de travail pour minimiser le temps nécessaire à accomplir des tâches et améliorer la productivité globale. * **Cohérence** : Assurer une cohérence dans l'expérience utilisateur à travers différents points de contact et plateformes. | | |
| **Directives de Mise en Œuvre** | | |
| * Mettre l’accent sur l’expérience utilisateur dans la conception des applications * Simplifier les parcours en offrant une ergonomie commune pour les applications et conforme au Design Système de la CNSA. * Offrir l’accès inclusif aux téléservices. * Les interfaces utilisateurs doivent être intuitives, accessibles et adaptées aux besoins des différents types d’utilisateurs. * Les interfaces homme machine doivent être conformes au Référentiel Général d'Amélioration de l'Accessibilité (RGAA). * Pour les usagers Le système doit être accessible depuis des périphériques de bureau et mobiles (tablettes, smartphones) | | |
| **Indicateurs de performance** | | |
| * Satisfaction des Utilisateurs : Utiliser des enquêtes de satisfaction et d'autres métriques pour évaluer le degré de satisfaction des utilisateurs. * Efficacité Opérationnelle : Évaluer comment les améliorations de l'UX affectent la productivité et l'efficacité des utilisateurs dans leurs tâches quotidiennes. * Réaliser des audit RGAA | | |

## P10 : Accès et habilitations

|  |  |  |
| --- | --- | --- |
| **Identification du principe** | | |
| **Nom : Accès et habilitations** | **Numéro de version : V1.0** | **Date de publication : 01/09/2023** |
| **Description** | | |
| **Le principe d'architecture "Accès et Habilitations"** est essentiel à la gouvernance des systèmes d'information (SI), visant à assurer que l'accès aux ressources informatiques et aux données est strictement contrôlé et accordé en fonction des besoins spécifiques des utilisateurs, de leur rôle et de leur responsabilité au sein de l’écosystème de la CNSA. Ce principe repose sur des politiques, des procédures, et des technologies destinées à protéger les informations contre les accès non autorisés, tout en facilitant l'accès nécessaire à l'information pour les opérations et la prise de décision. | | |
| **Objectifs** | | |
| * **Sécurité des Données** : Protéger les informations sensibles et critiques contre les accès non autorisés, les fuites de données et les violations de sécurité. * **Conformité Réglementaire** : Assurer la conformité avec les lois et les normes en matière de protection des données et de sécurité de l'information, comme le RGPD. * **Gestion des Identités** : Gérer efficacement les identités des utilisateurs et leurs habilitations, en s'assurant que les droits d'accès sont accordés selon le principe du moindre privilège. * **Audit et Traçabilité** : Fournir une piste d'audit pour les activités d'accès aux systèmes et aux données, facilitant ainsi la détection des anomalies et la réponse aux incidents. | | |
| **Directives de Mise en Œuvre** | | |
| * Simplifier les parcours en offrant une authentification commune pour les utilisateurs (possibilité d’aller d’une application à une autre sans réauthentification). * Centralisation des mécanismes d’authentification (MFA, FranceConnect, ProSanteConnect, …). * Gérer le contrôle d’accès et les habilitations d’accès aux outils au plus près du partenaire. * Disposer d’un système d’authentification et de gestion d’habilitation unique pour les professionnels. * Disposer d’un système d’authentification et d’identification unique pour les usagers. * Les applications internes CNSA s’appuient sur l’authentification AD CNSA pour le contrôle d’accès et les habilitations des agents de la CNSA. * Les applications métier s’appuient sur le PASS (Portail d’accès sécurisé aux services) pour le contrôle d’accès et les habilitations des professionnels (interne et externe). * Les applications métier s’appuient sur un système d’authentification mutualisé à la CNSA pour les usagers (en cours de construction). | | |
| **Indicateurs de performance** | | |
| * Pourcentage d’applications internes utilisant l’AD CNSA. * Pourcentage d’applications externes utilisant le PASS pour les professionnels * Pourcentage d’applications externe utilisant le système d’authentification unique pour les usagers * Réduction du nombre d’incidents liés aux accès aux données. | | |

## P11 : Référentiels de données

|  |  |  |
| --- | --- | --- |
| **Identification du principe** | | |
| **Nom : Référentiels de données** | **Numéro de version : V1.0** | **Date de publication : 01/09/2023** |
| **Description** | | |
| **Le principe « Référentiels de Données »** est fondamental dans la conception et la mise en œuvre de systèmes d'information. Ce principe vise à promouvoir une gestion centralisée, cohérente et efficace des données à travers la CNSA, en s'assurant que les données sont accessibles, fiables et sécurisées pour tous les utilisateurs autorisés. | | |
| **Objectifs** | | |
| * **Intégrité et Qualité des Données** : Assurer l'exactitude, la cohérence et la fiabilité des données à travers l'organisation. * **Accès Centralisé aux Données** : Fournir un point d'accès unique pour simplifier la recherche et l'utilisation des données. * **Gouvernance des Données** : Établir des politiques et des procédures pour la gestion des données, incluant la sécurité, la confidentialité, et la conformité réglementaire. * **Réutilisation des Données** : Encourager la réutilisation des données pour optimiser les ressources et éviter les redondances. * **Interopérabilité** : Faciliter l'échange de données entre différents systèmes et départements. | | |
| **Directives de Mise en Œuvre** | | |
| * Utilisation de référentiels communs par les applications de la CNSA * Respect de la doctrine du numérique en santé * Les applications utilisent de préférence les référentiels annuaires des services centraux. * Les applications enrichissent les annuaires des services centraux | | |
| **Indicateurs de performance** | | |
| * Pourcentage de référentiels exposés par les services centraux * Pourcentage d’applications utilisant ces référentiels * Pourcentage d’applications qui enrichissent les données de ces référentiels * Qualité des Données : Amélioration de la qualité et de l'intégrité des données, mesurée par des indicateurs tels que le taux d'erreur dans les données et le degré de satisfaction des utilisateurs. * Accessibilité des Données : Facilité d'accès aux données pour les utilisateurs autorisés, réduisant le temps nécessaire pour trouver et utiliser les informations. * Conformité et Sécurité : Réduction des incidents de sécurité liés aux données et conformité avec les réglementations de protection des données. | | |

## P12 : Durabilité

|  |  |  |
| --- | --- | --- |
| **Identification du principe** | | |
| Nom : **Durabilité** | Numéro de version : **V1.0** | Date de publication : **01/09/2023** |
| **Description** | | |
| **Le** **Principe d’architecture « Durabilité »** dans l'architecture des systèmes d'information souligne l'importance de concevoir et de gérer les technologies de l'information (TI) d'une manière qui minimise leur impact environnemental tout en soutenant la croissance économique et le bien-être social à long terme. Ce principe encourage les organisations à adopter des pratiques responsables qui contribuent à la durabilité environnementale, économique et sociale. | | |
| **Objectifs** | | |
| * Réduction de l'Impact Environnemental : Diminuer l'empreinte écologique des activités informatiques, notamment en termes de consommation énergétique et de production de déchets. * Responsabilité Sociale : Encourager une approche éthique et socialement responsable dans l'utilisation des ressources IT. * Efficacité Économique : Optimiser les coûts opérationnels à travers une gestion plus efficace des ressources, comme l'énergie et le matériel informatique. * Conformité Réglementaire : Se conformer aux lois et régulations environnementales de plus en plus strictes. | | |
| * Directives de Mise en Œuvre | | |
| * Conception Éco-responsable : Intégrer des considérations environnementales dès les premières étapes de conception des systèmes IT, en privilégiant des solutions qui réduisent la consommation d'énergie et les déchets. * Centres de Données Écologiques : Concevoir des centres de données avec une empreinte carbone réduite. * Gestion de l'Énergie et des Ressources : Mettre en place des politiques de gestion énergétique pour les équipements informatiques, en favorisant les dispositifs à faible consommation énergétique et en optimisant la durée de vie des appareils. * Recyclage et Élimination Responsable : Collaborer avec des partenaires certifiés pour l'élimination écologique des équipements obsolètes. * Sensibilisation et Formation : Former le personnel sur les meilleures pratiques de durabilité applicables à leur travail quotidien | | |
| **Indicateurs de performance** | | |
| * Mesure de la diminution de l'empreinte carbone des activités IT. * Suivi des économies réalisées grâce à l'efficacité énergétique des systèmes et des pratiques. | | |