

*Sécurité du système d'information de la branche Famille de la
sécurité sociale*

D o c u m e n t a t i o n d e r é f é r e n c e

Politique de Sécurité du Système d'Information



☐	Public
☒	Interne
☐	Diffusion restreinte
☐	Confidentiel

Objet du document	La Politique de Sécurité du système d'Information (PSSI) est le document de référence de la branche Famille de la sécurité sociale qui définit les objectifs, principes et règles permettant d'assurer la protection du système d'information.
--------------------------	--

Historique du document

Version	Date	Objet	Auteur(s)
V1	Mars 2017	Version initiale	
V2	Mai 2025	Mise à jour de la politique	Fabien MALBRANQUE Olivier HUCHULSKI Wassima HAJJI

Valideurs

Prénom / NOM	Entité / Fonction	Date de validation
Fabien MALBRANQUE	Directeur Contrôle Interne et Sécurité Numérique – DCISN - DSI	27/06/2025
Laurent TRELUYER	Directeur général délégué chargé des systèmes d'information - DSI	29/07/2025

Sommaire

1. Objet du document	4
2. Champ d'application	4
2.1 Périmètre d'application	4
2.2 Gestion des évolutions	4
3. Enjeux et objectifs de la sécurité des systèmes d'information	5
3.1 Enjeux en matière de SSI	5
3.2 Objectifs opérationnels en matière de SSI	6
4. Gouvernance de la sécurité des SI au sein de la CNAF	7
4.1 Gouvernance et comitologie	7
4.2 Démarche de mise en œuvre de la sécurité	8
5. Objectifs et règles de sécurité (PSSI MCAS)	9
5.1 Politique, organisation et gouvernance	9
5.2 Ressources humaines	10
5.3 Gestion des biens	12
5.4 Intégration de la sécurité dans le cycle de vie des systèmes d'information	13
5.5 Sécurité Physique	17
5.6 Sécurité des réseaux	19
5.7 Exploitation des systèmes d'information	22
5.8 Sécurité du poste de travail	32
5.9 Sécurité du développement des systèmes	35
5.10 Traitement des incidents	36
5.11 Continuité d'activité	38
5.12 Conformité, audit, inspection, contrôle	39
6. Objectifs et règles complémentaires	40
6.1 Sécurité des annuaires	40
6.2 Usages de l'intelligence artificielle	40
7. Corpus documentaire sécurité	42

1. OBJET DU DOCUMENT

Le présent document définit la **Politique de Sécurité des Systèmes d'Information (PSSI)** de la CNAF.

La présente PSSI formalise les principes directeurs et les exigences de sécurité que la branche Famille de la sécurité sociale s'engage à appliquer pour garantir la protection des systèmes d'information. Elle constitue un **référentiel stratégique**, définissant le **cadre général** de la sécurité applicable à l'ensemble des **agents, prestataires et partenaires** ayant accès aux ressources numériques de la CNAF et des organismes de son réseau.

Cette politique s'appuie sur la **PSSI des Ministères chargés des affaires sociales (PSSI MCAS)**, approuvée par arrêté le 1^{er} octobre 2015. La PSSI MCAS décline elle-même les orientations de la PSSIE (Politique de sécurité des Systèmes d'Information de l'Etat), en ciblant les spécificités des ministères sociaux et de leurs infrastructures critiques.

La PSSI de la CNAF est alignée sur ces politiques nationales, tout en étant **déclinée et adaptée au contexte propre à la branche Famille de la sécurité sociale**, à ses enjeux métiers et à la sensibilité de ses systèmes d'information. Elle précise les objectifs de sécurité, les rôles et responsabilités, ainsi que les principes de gouvernance et de pilotage mis en œuvre au sein de la CNAF et des organismes de son réseau.

Enfin, cette politique est **complémentaire à la PGSSI** (Politique Générale de Sécurité des Systèmes d'Information) de la CNAF, qui décrit la stratégie, la réglementation applicable et l'organisation de la sécurité de la Branche. Ensemble, ces documents visent à assurer la **confidentialité, l'intégrité, la disponibilité, la traçabilité** et la résilience des informations traitées, conformément aux exigences légales, réglementaires et aux bonnes pratiques de la cybersécurité.

[NIS2] Cette démarche s'inscrit en adéquation avec l'objectif de sécurité n°2 « Mise en œuvre d'un cadre de gouvernance de la sécurité numérique » et des moyens de mise en œuvre relatifs à la 'Politique de sécurité des systèmes d'information' attendus pour une entité essentielle (attendus (a), (b) et (c)).

2. CHAMP D'APPLICATION

2.1 Périmètre d'application

Tel que précisé dans la **Politique Générale de Sécurité des Systèmes d'Information (PGSSI)** de la branche Famille de la sécurité sociale, la sécurité des systèmes d'information couvre **l'ensemble des informations traitées**, quels que soient leur **format** (électronique, imprimé, manuscrit, vocal, image etc.) ou leur **mode de traitement** (création, modification, conservation, échange, suppression).

La présente politique s'applique à **l'ensemble des activités** des Organismes de la branche Famille de la sécurité sociale, ainsi qu'à celles de leurs partenaires, prestataires, fournisseurs et sous-traitants ayant accès aux systèmes d'information de la Branche, quels que soient leurs lieux d'implantation géographiques ou leurs modalités d'intervention.

Cette PSSI s'étend donc à **l'ensemble des ressources du système d'information** dans le but de garantir leur sécurité tout au long de leur cycle de vie.

2.2 Gestion des évolutions

La présente PSSI est un document vivant qui est **revu périodiquement** pour assurer sa **pertinence**, sa **conformité réglementaire** et son **adéquation avec les enjeux de sécurité** de la branche Famille de la sécurité sociale. Cette révision prend en compte :

- Les évolutions des référentiels nationaux, notamment les directives et politiques de sécurité ministérielles (PSSI MCAS) et interministérielles (PSSIE) ;

- Les nouvelles obligations légales ou réglementaires applicables (ex : transposition de la directive NIS, RGPD etc.) ;
- Les recommandations, guides et bonnes pratiques publiés par l'ANSSI, en tant qu'autorité nationale en matière de cybersécurité ;
- Les résultats d'analyses de risques, de contrôles internes ou d'audits réalisés au sein de la branche Famille de la sécurité sociale ;
- Le retour d'expérience des incidents de sécurité ou des tests de continuité ;
- Les évolutions du contexte organisationnel, technologique ou du périmètre fonctionnel de la Branche.

En complément, la présente PSSI est **progressivement enrichie par tout document interne** (charte, directive, politique appliquée, instruction technique) permettant de **détailler, d'explicitier ou de compléter** les règles de sécurité applicables au sein de la branche Famille de la sécurité sociale. Cette approche vise à constituer, de manière itérative, un **corpus documentaire de sécurité cohérent et complet**, tenant compte des priorités et de la maturité des différents sujets au sein de la Branche.

[NIS2] Cette démarche s'inscrit en adéquation avec l'objectif de sécurité n°2 de NIS 2 « Mise en œuvre d'un cadre de gouvernance de la sécurité numérique » et des moyens de mise en œuvre relatifs à la ' Politique de sécurité des systèmes d'information' attendus pour une entité essentielle (attendu (e)).

3. ENJEUX ET OBJECTIFS DE LA SECURITE DES SYSTEMES D'INFORMATION

3.1 Enjeux en matière de SSI

En tant qu'**Entité Essentielle (EE)**, la CNAF a la responsabilité de garantir un haut niveau de sécurité pour ses systèmes d'informations. Cette exigence s'inscrit dans le cadre de la **directive européenne NIS** (Network and Information Security), transposée en droit français, qui impose aux EE des obligations renforcées en matière de cybersécurité.

La sécurité des systèmes d'information (SSI) est un **enjeu stratégique** pour la CNAF et l'ensemble du réseau des organismes de la branche Famille de la sécurité sociale. Cette sécurité ne concerne pas uniquement les infrastructures informatiques, mais s'étend à l'ensemble des ressources humaines, matérielles, logicielles et organisationnelles mobilisées pour traiter l'information, en interne comme dans les échanges avec les partenaires externes.

Dans ce contexte, toute indisponibilité, altération ou divulgation non autorisée d'informations ou de services numériques peut entraîner des **conséquences majeures**, tant sur la continuité des services publics que sur la réputation ou la conformité réglementaire de l'Organisme.

La sécurité des systèmes d'information porte ainsi plusieurs types d'enjeux pour la branche Famille de la sécurité sociale :

❖ Enjeux de continuité de service des activités de l'État

La continuité des services assurés par la branche Famille de la sécurité sociale, notamment ceux liés aux prestations sociales essentielles, dépend directement de la disponibilité et de la résilience des systèmes d'information. Une défaillance pourrait provoquer une interruption de service, une non-conformité aux Directives Nationales de Sécurité (DNS), ou encore des retards dans la fourniture de prestations, avec des répercussions sociales et économiques importantes.

❖ Enjeux de confiance et d'image

Les usagers, partenaires et parties prenantes attendent un haut niveau de confiance dans les services numériques proposés par la CNAF. Une atteinte à la sécurité des systèmes d'information peut :

- Porter atteinte à la confiance des citoyens en cas d'interruption de service ou d'erreur dans le traitement de leurs droits ;
- Entraîner des violations de données personnelles, soumises au RGPD et au contrôle de la CNIL ;

- Nuire à la crédibilité institutionnelle, en cas de compromission de données financières, sociales ou décisionnelles ;
- Affecter la relation de confiance avec les partenaires et fournisseurs, notamment dans le cadre des marchés publics.

❖ **Enjeux d'organisation interne**

Les systèmes d'information de la CNAF sont au cœur de l'organisation des activités métier. Leur défaillance entraînerait inévitablement une désorganisation opérationnelle, un ralentissement des processus et une perte d'efficacité. Compte tenu de l'intégration forte des processus métiers dans les outils numériques, toute interruption ou indisponibilité peut compromettre la qualité du service rendu et la prise de décision.

3.2 Objectifs opérationnels en matière de SSI



Afin de répondre aux enjeux stratégiques, organisationnels et réglementaire présentés précédemment, la sécurité des systèmes d'information de la branche Famille de la sécurité sociale s'articule autour de quatre objectifs fondamentaux, constituant le socle de la protection de l'information : le socle DICT (disponibilité, intégrité, confidentialité et traçabilité).

Le respect de ces objectifs vise à garantir un niveau de sécurité adapté aux missions de service public de la Branche, et repose sur plusieurs axes d'action complémentaires :

1. Réaliser les analyses de risques

La démarche de sécurisation commence par une évaluation rigoureuse des risques. L'analyse de risques permet d'identifier les menaces, les vulnérabilités et impacts potentiels pesant sur les actifs du système d'information. Elle constitue un levier essentiel pour définir des mesures de sécurité proportionnées aux enjeux, et pour contribuer à la gestion globale des risques de la branche Famille de la sécurité sociale. Cette analyse (au format EBIOS RM) est conduite de manière itérative et intégrée aux cycles de vie des projets.

2. Garantir la conformité réglementaire

Les systèmes d'information sont mis en conformité avec les exigences légales, réglementaires et normatives applicables, notamment celles émanant de :

- La CNIL et du RGPD (protection des données personnelles)
- La directive NIS (sécurité des réseaux et systèmes d'information des EE)
- Le Référentiel général de sécurité (RGS)

Cette conformité implique un suivi des actifs au sein de la branche Famille de la sécurité sociale et des évolutions juridiques pour une intégration en continue dans les processus métiers et techniques.

3. Sensibiliser et former l'ensemble des acteurs

La sécurité des systèmes d'information dépend fortement des comportements et pratiques des utilisateurs et des administrateurs. Des actions de sensibilisation et de formation sont mises en place au profit des différents acteurs de la Branche. Ces actions visent à favoriser la prise de conscience des risques numériques, le respect des règles de sécurité et l'adoption des réflexes appropriés en cas d'incidents.

4. Sécuriser et maintenir les SI en condition de sécurité (MCS)

La sécurité technique s'applique à l'ensemble des composants du système d'information de la branche Famille de la sécurité sociale (postes de travail, équipements réseaux, applications métiers, serveurs etc.). Les systèmes font l'objet d'un maintien en condition opérationnelle (MCO) et surtout d'un maintien en condition de sécurité (MCS), incluant notamment :

- L'application régulière des correctifs de sécurité

- La gestion rigoureuse des comptes, des droits et des accès
- Le suivi des vulnérabilités et la mise en œuvre des mesures correctives
- La sécurité physique des locaux et équipements sensibles

5. Gérer les incidents, les crises et la continuité d'activité

Un dispositif de gestion des incidents de sécurité est mis en œuvre pour détecter, signaler, analyser et traiter tout événement susceptible de compromettre la sécurité du SI de la branche Famille de la sécurité sociale. De tels événements sont portés à la connaissance des acteurs pertinents, à savoir du RSSI, de l'AQSSI voire de l'ANSSI et du FSSI le cas échéant.

Par ailleurs, des dispositifs de gestion de crise et de continuité d'activité sont définis et testés au sein de la CNAF pour permettre une reprise rapide des activités critiques.

4. GOUVERNANCE DE LA SECURITE DES SI AU SEIN DE LA CNAF

4.1 Gouvernance et comitologie

La gouvernance de la sécurité des systèmes d'informations de la branche Famille de la sécurité sociale est définie dans la **Politique Générale de Sécurité des Systèmes d'Information** (PGSSI). Ce document de référence présente l'organisation, les rôles, responsabilités et principes de pilotage permettant d'assurer une gestion efficace, coordonnée et conforme aux exigences réglementaires de la SSI.

Pour l'ensemble des informations relatives à la structure de gouvernance, aux acteurs de la sécurité, aux circuits de décision et aux mécanismes de pilotage, il convient de se référer à la PGSSI, qui constitue le cadre général applicable. Toutefois, les éléments structurants suivants sont rappelés dans la présente politique afin de garantir une bonne compréhension des dispositifs de sécurité mis en œuvre au sein de la Branche.

La sécurité des SI de la branche Famille de la sécurité sociale repose sur **trois chaînes en coordination depuis les services du Premier ministre jusqu'aux intervenants sécurité au sein des administrations** :

1. Une **chaîne décisionnelle**, entre le Secrétariat général à la sûreté et à la défense nationale (SGDSN), le ministre, le service du haut fonctionnaire de défense du ministère des affaires sociales (SHFDS) et l'AQSSI (Directeur Général de la CNAF) ;
2. Une **chaîne fonctionnelle**, entre ANSSI (Agence nationale de la sécurité des systèmes d'information), le FSSI (Fonctionnaire de la sécurité des systèmes d'information), la fonction de RSSI (Responsabilité de la sécurité du système d'information assurée par le Directeur de la Direction Contrôle Interne et Sécurité Numérique, sous l'autorité du Directeur général délégué des systèmes d'information) ;
3. Une **chaîne opérationnelle**, entre le centre opérationnel de l'ANSSI, la fonction de responsabilité de la sécurité du système d'information (assurée par le Directeur du Contrôle Interne et de la Sécurité Numérique), les équipes chargées de la sécurité des systèmes d'information de la Branche et l'ensemble des maîtrises d'œuvre en tant que besoin. Étant donné ses obligations en termes de protection des données, le DPD est obligatoirement et immédiatement informé des incidents quels qu'ils soient afin d'étudier l'éventualité d'une notification de violation de données.

La sécurité du SI de la branche Famille de la sécurité sociale implique des acteurs externes, parmi lesquels :

- **L'ANSSI** et notamment le **CERT FR**¹ qui assure un point de contact pour la gestion des incidents

¹ Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (ANSSI)

- **Le service du Haut Fonctionnaire de Défense et de Sécurité (HFDS) du Ministère et son FSSI**
- **La CNIL** sur les sujets relatifs à la sécurité des données à caractère personnel

Au sein de la CNAF, les principaux acteurs jouant un rôle dans la sécurité du SI sont :

- **La DCFN** (Direction Comptable et Financière Nationale) à travers son pôle « sécurité du risque informatique », qui assure la sécurisation du risque informatique de la Branche, en lien avec DSI et la MACSSI.
- **La MACSSI** (Mission de l'Analyse de la Conformité et de la Sécurité des Systèmes d'Information) qui assume, pour l'ensemble de la branche Famille de la sécurité sociale, l'ensemble des missions relatives à la protection des données à caractère personnel.
- **La DCISN** (Direction Contrôle Interne et sécurité Numérique) qui comprend en son sein le RSSI, définit et met en œuvre les normes et standards de sécurité, construit et contrôle les mécanismes de PRA/PCA, veille à l'application des réglementations, forme et sensibilise les agents aux enjeux de sécurité, etc. Le RSSI a notamment la charge du suivi de la conformité du SI aux mesures énoncées dans la présente PSSI. Il est le point de contact privilégié de l'ANSSI.
- Les acteurs opérants sur le plan local, parmi lesquels : **les MSSI** (managers de la Sécurité des Systèmes d'Informations), les **RIL** (Relais informatiques et Libertés) et les **RPCA** (Responsables de plan de continuité d'activité).

Pour piloter, suivre et arbitrer les actions liées à la cybersécurité au sein de la branche Famille de la sécurité sociale, ces acteurs s'organisent autour d'une comitologie établie et identifiée. Ces instances assurent la cohérence des orientations stratégique, la coordination et le suivi opérationnel des dispositifs. Elles incluent notamment :

- Le COSIM (Comité de suivi des incidents majeurs)
- L'INFOSEC (Réunion de sensibilisation aux enjeux de sécurité)
- Le CMES (Comité de management des événements de sécurité)
- Les instances relatives au traitement des incidents de sécurité ou la gestion de crise (CEC : cellule d'expertise cyber ; CRS : cellule de réponse sécurité)

[NIS2] Cette démarche s'inscrit en adéquation avec l'objectif de sécurité n°2 de NIS 2 « Mise en œuvre d'un cadre de gouvernance de la sécurité numérique » et des moyens de mise en œuvre relatifs aux 'Rôles et responsabilités' (attendus (a), (b) et (c)).

4.2 Démarche de mise en œuvre de la sécurité

La mise en œuvre de la gouvernance de la sécurité des systèmes d'information de la branche Famille de la sécurité sociale repose sur un **Système de Management de la Sécurité de l'Information (SMSI)** formalisé dans la PGSSI. Ce système constitue le cadre de référence pour structurer, piloter et faire évoluer la cybersécurité dans une logique d'amélioration continue.



Le SMSI s'appuie sur les principes de la roue de Deming (**PDCA**) et vise à garantir un niveau de sécurité proportionné aux enjeux, aligné sur les objectifs métiers, et conforme aux exigences réglementaires. Ce pilotage repose notamment sur :

- Une **approche par les risques**
- La définition des **rôles et responsabilités**
- La **connaissance du périmètre** à protéger (identification des actifs essentiels et de processus critiques)
- La mise en œuvre des **mesures de sécurité** adaptées (organisationnelles, techniques, physiques et humaines)
- La **préparation à l'incident** (gestion des incidents, PRA/PCA, gestion de crise)
- La promotion d'une **culture de sécurité** (sensibilisation et formation)

[NIS2] Cette démarche s'inscrit en adéquation avec l'objectif de sécurité n°2 de NIS 2 « Mise en œuvre d'un cadre de gouvernance de la sécurité numérique » dans la mise en place d'un SMSI conforme aux exigences prévues dans la norme ISO/CEI 27001:2022.

5. OBJECTIFS ET REGLES DE SECURITE (PSSI MCAS)

Ce chapitre présente **les 34 objectifs de sécurité tels qu'issus de la PSSI MCAS**, répartis en **13 domaines** clés. Ces objectifs se traduisent en un **ensemble de règles** visant à garantir un niveau de sécurité cohérent avec les enjeux opérationnels. Les règles listées dans ce document sont celles sélectionnées pour leur applicabilité à la branche Famille de la sécurité sociale. Ces règles associées servent notamment de **base au référentiel de contrôle interne de la Branche**.

Une attention particulière a également été portée au **rapprochement avec les exigences de la directive NIS2**, afin d'assurer une cohérence avec les standards européens et nationaux en matière de cybersécurité et de gestion des risques.

5.1 Politique, organisation et gouvernance

Objectif 1 : Organisation de la sécurité des systèmes d'information

Mettre en place une organisation adéquate, garantissant la prise en compte préventive et réactive de la sécurité.

Organisation SSI

ORG-SSI : Organisation SSI

La branche Famille de la sécurité sociale déploie une organisation dédiée à la sécurité des systèmes d'informations (SSI) à l'échelle de l'ensemble de l'organisation. Cette organisation est explicitement décrite dans le document « Politique Générale de Sécurité des Systèmes d'Information » (PGSSI) qui détaille la gouvernance et la comitologie mise en œuvre.

Cette politique est diffusée et portée à la connaissance de tous les agents. La PGSSI décline également le système de management de la sécurité de l'information (SMSI) mis en œuvre au sein de la Branche.

[NIS 2] Objectif de sécurité n°2, « Rôles et responsabilités », attendu (c).

Acteurs SSI

ORG-ACT-SSI : Identification des acteurs SSI

L'organisation SSI de la branche Famille de la sécurité sociale s'appuie sur des acteurs de la sécurité des systèmes d'information clairement identifiés, à tous ses niveaux d'organisation (au niveau national et au niveau local). Les rôles et responsabilités de ces acteurs sont décrits dans la PGSSI de la CNAF. La CNAF tient également à jour un annuaire national de ces acteurs SSI.

Responsabilités internes

ORG-RSSI : Désignation du responsable SSI

Le directeur général de la CNAF est désigné autorité qualifiée de la sécurité des systèmes d'information (AQSSI) et est amené à exercer en tant qu'autorité d'homologation des SI de la Branche.

L'AQSSI s'appuie sur son RSSI, Directeur de la DCISN (Direction du contrôle Interne et de la Sécurité Numérique) pour piloter et gérer la sécurité du système d'information de la Branche, et veiller à l'application de la présente politique. Le RSSI est notamment le point de contact privilégié des partenaires externes (ANSSI) sur les sujets relatifs aux incidents de sécurité.

Les MSSI (Managers de la Sécurité du Système d'information) constituent les relais locaux du RSSI ; ils disposent d'une lettre de mission formalisant leurs rôles et précisant leurs domaines de responsabilités en matière de sécurité des systèmes d'informations.

[NIS 2] Objectif de sécurité n°2, « Rôles et responsabilités », attendus (a) et (b).

ORG-RESP : Formalisation des responsabilités

La PGSSI, validée par l'AQSSI, le DSI, le RSSI, la MACSSI et le Directeur Comptable et Financier de la CNAF, fixe la répartition au sein de la Branche des rôles et des responsabilités en matière de SSI de chaque entité (au niveau national et au niveau local). La PGSSI est portée à la connaissance de l'ensemble des acteurs de la Branche.

[NIS 2] Objectif de sécurité n°2, « Rôles et responsabilités », attendus (a), (b) et (c).

Responsabilités vis-à-vis des tiers

ORG-TIERS : Question contractuelle des tiers

Le RSSI coordonne les actions permettant l'intégration des clauses liées à la SSI dans tout contrat ou convention impliquant un accès par des tiers à des informations ou à des ressources informatiques. Ces exigences de sécurité sont inscrites dans les CCTP de la Branche.

Le Plan d'Assurance de Sécurité de l'information (PAS) rassemble tous les contrôles de sécurité et services acceptés et contractés afin de garantir les conditions de sécurité exigées dans le cadre des prestations commanditées par la CNAF. A travers ce PAS, le prestataire accepte, le cas échéant, d'être audité afin de vérifier les engagements définis et la conformité aux exigences établies.

[NIS 2] Objectif de sécurité n° 3, « Sécurité numérique dans les contrats avec les prestataires et fournisseurs informatiques », attendus (a) et (b).

Application des mesures de sécurité au sein de l'entité

ORG-APP-INSTR : Application de l'instruction

Le RSSI planifie les actions de mise en application de la PSSI conformément aux orientations définies dans le schéma directeur du système d'information (SDSI) de la CNAF. La feuille de route annuelle SSI offre une visibilité sur ces actions et permet d'en rendre compte à l'autorité qualifiée (AQSSI), ainsi qu'au besoin, au FSSI.

ORG-APP-DOCS : Formalisation des documents d'application

Le RSSI formalise et tient à jour les documents d'application, approuvés par l'autorité qualifiée (AQSSI), permettant la mise en œuvre des mesures de la PSSI au sein de la branche Famille de la sécurité sociale.

5.2 Ressources humaines

Objectif 2 : Ressources humaines

Faire des personnes les maillons forts des systèmes d'information sur le périmètre de la branche Famille de la sécurité sociale.

Utilisateurs

RH-SSI : Charte d'application SSI

La CNAF met en œuvre la « Charte nationale de sécurité de l'utilisateur du système d'information » (LR-2017-069) qui définit les règles d'usage et de sécurité que l'organisme et les utilisateurs s'engagent à respecter, permettant ainsi de garantir un juste équilibre entre, d'une part, les objectifs de sécurité de l'organisme et, d'autre part le respect de la vie privée et des libertés individuelles des utilisateurs. La mise en œuvre de cette charte au sein de la branche Famille de la sécurité sociale est notamment soutenue par la CNIL. La charte est portée à la connaissance de l'ensemble des agents de la branche Famille de la sécurité sociale, en annexe du règlement intérieur.

En complément, la « Charte nationale de sécurité de l'administrateur du système d'information » s'applique spécifiquement aux administrateurs du système d'information de la branche Famille de la sécurité sociale. Elle précise les moyens d'action, les droits et les devoirs des administrateurs dans l'exercice de leurs activités.

[NIS2] Objectif de sécurité n°4, attendu (a).

Personnel permanent

RH-MOTIV : Choix et sensibilisation des personnes tenant les postes clés de la SSI

Une attention particulière est portée au recrutement des personnes-clés de la SSI. Le RSSI et les MSSI de la Branche sont spécifiquement formés à travers un programme dédié à la sécurité numérique adapté à leurs responsabilités. En effet, les responsables informatiques et MSSI sont sensibilisés dès leur arrivée, puis de manière continue aux enjeux et devoirs liés à leur fonction, notamment à travers les réunions d'information organisées par la DCISN :

- Les réunions d'information Sécurité du SI (INFOSEC)
- Les réunions de présentation du référentiel de Contrôle Interne du SI (CISI)

[NIS2] Objectif de sécurité n°4, attendu (e).

RH-CONF : Personnel de confiance

Toute personne amenée à manipuler des informations sensibles fait l'objet d'une vigilance particulière en matière de probité, dans le respect des dispositions légales en vigueur. Les sanctions applicables en cas de négligence ou d'acte malveillant sont précisées dans le règlement intérieur, diffusé à l'ensemble des agents de la Branche. Ces exigences sont également stipulées dans les conventions, contrats commerciaux et PAS (plan d'assurance sécurité) conclus avec les tiers.

RH-UTL : Sensibilisation des utilisateurs des systèmes d'information

Tous les utilisateurs du système d'information de la CNAF sont régulièrement informés des exigences de sécurité. Ils sont formés et sensibilisés, dès leur arrivée puis à minima à une fréquence annuelle, à l'utilisation des outils de travail conformément aux règles de sécurité des systèmes d'information.

Cette sensibilisation est complétée par des instructions spécifiques, partagées à l'ensemble des acteurs, pour promouvoir des exigences de sécurité spécifiques (exemple : *Instruction relative aux outils non maîtrisés* « Utilisation des outils numériques gratuits – Quelques règles de prudence » (IT 2018-031)).

De surcroît, un « espace métier informatique » dédié à la sécurité informatique est également mis à la disposition de l'ensemble des agents de la CNAF pour les éclairer sur les informations actuelles et essentielles liées à la Sécurité du système d'information et les guider vers les documents de référence mis à disposition (supports de sensibilisation, vidéos explicatives, panorama de la cybermenace, etc.).

[NIS2] Objectif de sécurité n°4, attendu (b).

En raison de la nature des données traitées par la CNAF, les agents sont particulièrement sensibilisés au respect du secret professionnel dans le cadre de leurs missions. Ce secret s'applique à l'ensemble des informations détenues par la CNAF concernant les allocataires, quelle que soit leur forme ou leur support. Ces clauses de confidentialités sont précisées dans la lettre « Le secret professionnel et les règles de communication de données lors de contacts avec les allocataires » (LR 2024-257).

Mouvement de personnel

RH-MOUV : Gestion des arrivées, mutations et des départs

La Branche met en œuvre un processus structuré et strictement appliqué pour encadrer les arrivées, mutations et départs des collaborateurs, y compris des prestataires et partenaires. Ce processus couvre l'ensemble du cycle de vie des accès afin d'assurer une maîtrise continue des droits, du matériel et des moyens d'accès physiques. Ce processus comprend :

- La gestion des accès informatiques :
 - Attribution, modification ou suppression des droits selon le principe du moindre privilège
 - Mise à jour des droits lors des changements de fonction et désactivation des comptes au départ
- La gestion des habilitations :
 - Les habilitations sont définies au regard des fonctions et revues régulièrement dans le cadre du plan de contrôle interne (bonnes pratiques du référentiel PS143)
- La gestion des accès physiques :
 - Registre actualisé des agents et tiers autorisés à accéder aux bâtiments et zones sensibles
 - Mise en œuvre de dispositifs d'accès sécurisés
- Matériel et équipements mobiles :
 - Suivi de l'attribution du matériel (ordinateurs, téléphones, matériels périphériques)
 - Restitution encadrée lors des circuits de sortie et révocation des accès distants au départ
- Sensibilisation à l'entrée :
 - Diffusion de la réglementation en vigueur (règlement intérieur, charte informatique)
 - Présentation et sensibilisation aux règles de sécurité

[NIS2] Objectif de sécurité n°4, attendu (d).

Personnel non permanent

RH-NPERM : Gestion du personnel non permanent (stagiaire, intérimaires, prestataires ...)

Les règles de la PSSI s'appliquent pleinement à l'ensemble des personnels non permanents (stagiaires, intérimaires, prestataires) utilisant les systèmes d'information de la branche Famille de la sécurité sociale. Des dispositions spécifiques sont mises en œuvre pour assurer cela.

Un parcours d'intégration incluant un volet SSI est proposé par les ressources humaines aux stagiaires et intérimaires.

Les prestataires sont quant à eux engagés contractuellement à travers le plan d'assurance sécurité (PAS) et les clauses décrites dans les contrats commerciaux le cas échéant.

5.3 Gestion des biens

Objectif 3 : Cartographie des systèmes d'information

Tenir à jour une cartographie détaillée et complète des systèmes d'information.

[NIS2] Cette démarche s'inscrit en adéquation avec l'objectif de sécurité n°5 de NIS2 « Maîtrise des systèmes d'information », 'Cartographie des systèmes d'information'.

GDB-INVENT : Inventaire des ressources informatiques.

La CNAF établit et maintient à jour un inventaire des ressources informatiques sous sa responsabilité, au travers des rapports de l'outil d'inventaire, tant au niveau national que local. Cet inventaire inclut : stations et serveurs, appareils (ordinateurs, téléphones, appareils périphériques), matériels de connexion, ensemble des équipements connectés au réseau local. Ces derniers sont répertoriés avec pour chaque équipement les informations nécessaires à leur identification (nature, identifié du propriétaire, système d'exploitation, utilisation). L'inventaire est tenu à disposition du RSSI, le cas échéant.

GDB-CARTO : Cartographie

La CNAF maintient une cartographie actualisée de son système d'information, couvrant les centres informatiques, les architectures réseau, ainsi que les architectures techniques globales et simplifiées. Cette cartographie identifie les points sensibles et les zones critiques en lien avec la nature des informations traitées. La cartographie est enrichie par des vues spécifiques issues des outils de gestion d'inventaire, de supervision des infrastructures et de pilotage des référentiels techniques.

Une cartographie dédiée au « SIE » (système d'information essentiel) est également tenue à jour. Tous ces éléments sont accessibles au RSSI et à l'AQSSI et permettent à la CNAF d'assurer un maintien en condition opérationnel et de sécurité de ses systèmes et de pouvoir réagir sans retard à un incident de sécurité les affectant.

[NIS2] Objectif de sécurité n°5, 'Cartographie des systèmes d'information' attendu (a).

MC-GDB-REC : Mesure complémentaire à la PSSI MCAS – Recensement

La CNAF établit et tient à jour une liste complète de ses activités et services (y compris ceux qui ne correspondent pas aux critères faisant de la CNAF une entité essentielle), avec l'identification des systèmes d'informations associés. Cette liste permet de tracer les dépendances critiques et de désigner les responsables fonctionnels de chaque système.

Les systèmes d'information pour lesquels il est décidé de ne pas appliquer les objectifs de sécurité doivent être explicitement justifiés.

Ces éléments sont révisés au minimum à chaque évolution significative du périmètre d'activité de la Branche.

[NIS2] Objectif de sécurité n°1, attendus (a) à (c).

Objectif 4 : Qualification et protection de l'information.

Qualifier l'information de façon à adapter les mesures de protection.

La qualification de l'information en fonction du besoin de confidentialité au sein de la branche Famille de la sécurité sociale est la suivante :

- *Publique* : informations réputées publiques et notamment celles publiées en ligne ;
- *Interne* : documents communicables au titre des dispositions relatives à l'accès aux documents administratifs, la diffusion n'est pas possible vers des membres externes à l'organisme
- *Diffusion restreinte* : documents transmis uniquement à une liste spécifiée et restreinte de destinataires et non communicable sans autorisation préalable
- *Confidentiel* : informations sensibles relevant de la sécurité de l'organisme ou des personnes, soumises à des règles strictes de protection.

GDB-QUALIF-SENSI : Qualification des informations

La CNAF met en place une politique de classification des informations, précisant quatre niveaux de sensibilité prédéfinis (publique, interne, diffusion restreinte et confidentiel). Un marquage adapté est apposé sur les documents, courriels et supports afin de rappeler la sensibilité des informations partagées et d'en cadrer la diffusion.

GDB-PROT-IS : Protection des informations

L'utilisateur doit protéger les informations qu'il est amené à manipuler dans le cadre de ses fonctions, selon leur sensibilité et tout au long de leur cycle de vie, depuis la création du brouillon jusqu'à son éventuelle destruction. L'instruction technique « Protection des informations sensibles grâce au chiffrement » (2017-099) encadre notamment le recours au chiffrement pour les données personnelles ou informations classées confidentielles.

5.4 Intégration de la sécurité dans le cycle de vie des systèmes d'information

Objectif 5 : Gestion des risques et homologation de sécurité

Apprécier, traiter, et communiquer sur les risques relatifs à la sécurité des systèmes d'information.

INT-HOMOLOG-SSI : Homologation de sécurité des systèmes d'information.

La branche Famille de la sécurité sociale met en œuvre une gouvernance des risques SSI intégrée à la stratégie globale. Cette gouvernance vise à garantir une prise en compte effective du risque numérique dans les décisions et à mobiliser les moyens adaptés pour y répondre.

Dans cette optique, tout système d'information fait l'objet d'une décision d'homologation de sa sécurité avant sa mise en exploitation dans les conditions d'emploi définies. L'homologation est l'acte selon lequel l'autorité d'homologation atteste formellement auprès des utilisateurs que le système d'information est protégé conformément aux objectifs de sécurité fixés et que les risques résiduels sont acceptés.

Le « Guide d'homologation de sécurité des systèmes d'information » de la CNAF (IT 2025-132) est partagé à l'ensemble des acteurs concernés.

La décision d'homologation s'appuie sur un corpus documentaire identifié incluant notamment : le référentiel réglementaire applicable (incluant la présente PSSI), toute analyse de conformité avec un référentiel spécifiquement applicable, une analyse de risques (sur le modèle EBIOS RM), le plan de traitement des risques identifiés (incluant échéance et responsable des actions), les résultats des contrôles de sécurité (audits, tests de pénétration) etc.

Le dossier est revu au plus tard à une échéance de 3 ans et au minimum à chaque évolution majeure du contexte métier, technique ou organisationnel ou en cas d'incident de sécurité.

[NIS2] Objectif de sécurité n°2, 'Gestion de la conformité', attendus (a), (b) et (c).

Objectif de sécurité n° 16, attendus (a) à (d).

MC-INT – AUDIT : Mesure complémentaire à la PSSI MCAS – Audits de la sécurité du SI

La CNAF met en œuvre un programme d'audit de ses systèmes d'information, intégré le cas échéant à l'homologation ou la réhomologation des systèmes. Les audits peuvent être réalisés par le recours à un prestataire d'audit en sécurité des systèmes d'information (PASSI), qualifié par l'ANSSI.

Les audits couvrent notamment les aspects organisationnels, techniques, physiques et peuvent inclure des tests d'intrusion, audits de code ou de configuration. Un plan d'action (incluant échéances et responsables) est systématiquement établi à l'issue des audits afin de traiter les non-conformités ou vulnérabilités identifiés.

[NIS2] Objectif de sécurité n° 17, attendus (a) à (d).

Objectif 6 : Maintien en condition de sécurité des systèmes d'information

Gérer dynamiquement les mesures de protection, tout au long de la vie du système d'information.

[NIS2] Cette démarche s'inscrit en adéquation avec l'objectif de sécurité n°5 de NIS2 « Maîtrise des systèmes d'informations », 'Maintien en condition opérationnelle et de sécurité, attendus (a) à (k).

INT-SSI : Intégration de la sécurité dans les projets.

La sécurité des systèmes d'information est prise en compte dans toutes les phases des projets informatiques, sous le contrôle de l'autorité d'homologation, de la conception et de la spécification du système jusqu'à son retrait du service. Les développements nationaux mais aussi locaux sont soumis à une procédure d'homologation dès les premières phases du projet. Le « Guide d'homologation de sécurité des systèmes d'information » (IT 2025-132) cadre cette démarche.

INT-QUOT-SSI : Mise en œuvre au quotidien de la SSI.

La sécurité des systèmes d'information se traite au quotidien par des pratiques d'hygiène informatique. Des procédures écrites définissent les actes élémentaires du maintien en condition de sécurité lors des phases de conception, évolution ou retrait d'un système. Tout système d'information doit faire l'objet, outre le maintien en condition opérationnelle, d'un maintien en condition de sécurité.

La CNAF met en œuvre une procédure de MCO/MCS de ses ressources informatiques, incluant les matériels, logiciels et systèmes embarqués. Cette procédure repose notamment sur une veille active des vulnérabilités et des correctifs de sécurité (en provenance des éditeurs, de l'ANSSI, du CERT) prise en charge par une équipe dédiée (le CSIRT²) au sein de la DCISN. L'application des correctifs est réalisée sans délais.

La CNAF veille à la mise à jour en continue de ses ressources (depuis les ressources officielles mises à disposition par les éditeurs et fournisseurs). Lorsque les mises à jour ne sont pas possibles, des mesures d'atténuation sont mises en place pour réduire le niveau de risque. L'ensemble des logiciels est maintenu dans une version supportée par les éditeurs. En cas d'utilisation d'une version obsolète, des mesures de réduction de risque spécifiques sont appliquées.

[NIS2] Objectif de sécurité n°5, 'Maintien en condition opérationnelle et de sécurité' attendus (a), et (c) à (k).

INT-TDB : Créer un tableau de bord SSI.

L'état de la sécurité des systèmes d'information fait l'objet d'un suivi régulier à travers des synthèses partagées avec les parties prenantes concernées. Ces éléments rendent compte notamment de l'avancement des actions engagées dans le cadre de la sécurité des systèmes d'information, de la couverture du contrôle interne, de la gestion des incidents etc. Ils permettent d'éclairer le pilotage stratégique et opérationnel de la sécurité.

Objectif 7 : Produits et services labellisés

Utiliser des produits et services dont la sécurité est évaluée et attestée selon des procédures reconnues par l'ANSSI, afin de renforcer la protection des sécurités informatiques.

INT-AQ-PSL : Acquisition de produits et services de confiance.

² Computer Security Incident Response Team (CSIRT) est une unité spécialisée dans la gestion et la réponse aux incidents de cybersécurité

La Branche recommande le recours à des produits ou services de sécurité certifiés ou qualifiés, en particulier pour les composants critiques. Lorsque cela est pertinent, cette exigence est intégrée aux marchés sous forme de critère de sélection ou de clause spécifique.

Objectif 8 : Gestion des prestataires

Veiller aux exigences de sécurité lorsqu'il est fait appel à de la prestation par des tiers.

INT-PRES-CS : Clauses de sécurité.

Toute prestation SI de la Branche intègre systématiquement des clauses de sécurité précisant les obligations des prestataires en matière de SSI et leur conformité avec les exigences réglementaires (incluant NIS2). Ces exigences sont formalisées dans le « Plan d'assurance sécurité (PAS) » et via les clauses spécifiques dans les CCTP.

La prise en compte des exigences réglementaires et de sécurité dans les cas de sous-traitance incluant un traitement de données personnelles, est quant à elle cadrée dans la politique « Marchés et RGPD : sécurisation juridique des situations de sous-traitance qui concernent des données personnelles » (IT 2020-027).

Par ailleurs, un avis de sécurité émis par la DCISN peut être fourni lors de tout appel d'offre afin d'éclairer les choix et garantir la prise en compte des enjeux de sécurité dès la phase de contractualisation.

[NIS2] Objectif de sécurité n°3, 'Sécurité numérique dans les contrats avec les prestataires et fournisseurs informatiques' attendu (a).

INT-PRES-CNTRL : Suivi et contrôle des prestations fournies.

Le maintien du niveau de sécurité des prestations dans le temps repose sur la mise en œuvre de contrôles réguliers à différents niveaux :

- En amont des projets, les PAS et CCTP sont systématiquement revus et validés par les services achats et juridiques afin de garantir la cohérence et la conformité des exigences de sécurité attendues tout au long du cycle de vie du marché.
- Le « Plan d'Assurance Sécurité (PAS) » prévoit la possibilité pour la CNAF ou un tiers mandaté d'auditer le prestataire, celui-ci s'engageant à fournir toutes les informations utiles permettant de vérifier ses engagements.

[NIS2] Objectif de sécurité n°3, 'Sécurité numérique dans les contrats avec les prestataires et fournisseurs informatiques' attendu (b).

MC-INT-PRES-CARTO : Mesure complémentaire à la PSSI MCAS – Cartographie de l'écosystème

La CNAF maintient une cartographie à jour de son écosystème numérique, recensant les prestataires et fournisseurs informatiques avec lesquels il existe une relation contractuelle, ainsi que les interconnexions avec des systèmes d'information tiers. Pour chaque acteur externe, un point de contact est identifié.

[NIS2] Objectif de sécurité n°3, 'Cartographie de l'écosystème' attendus (a) et (b).

INT-REX-AR : Analyse de risques.

Toute opération d'externalisation s'appuie sur une analyse de risques préalable, de façon à formaliser des objectifs de sécurité et définir des mesures adaptées. Le cas échéant, cette analyse inclue une analyse d'impact relative à la protection des données. L'ensemble des objectifs de sécurité ainsi formalisés permet de définir une cible de sécurité servant de cadre au contrat établi avec le prestataire.

INT-REX-HB : Hébergement.

L'hébergement des systèmes d'information traitants des données sensibles est nécessairement conforme aux exigences réglementaires, et privilégié sur le territoire national ou celui de l'Union Européenne. Lorsque cela est pertinent, le recours à des hébergeurs qualifiés est encouragé.

- Le « Plan d'Assurance Sécurité (PAS) » de la Branche impose aux prestataires que les données personnelles soient strictement hébergées au sein de l'Union Européenne.
- La « Politique appliquée à la sécurité des systèmes d'information hébergés dans le Cloud » (2025-026) précise que si la localisation des données hébergées n'est pas réalisée en France ou dans l'Union Européenne, des clauses contractuelles doivent être établies avec les fournisseurs pour respecter l'ensemble des réglementations européennes et françaises. En cas de refus de respecter ces clauses, la CNAF se réserve le droit d'exclure le dit fournisseur.

Ces exigences visent notamment à garantir le respect des obligations légalement et réglementaires applicables en matière de protection de la donnée (RGPD notamment).

INT-REX-HS : Hébergement et clauses de sécurité.

Les contrats d'hébergement souscrits par la CNAF sont également soumis à des clauses relatives à la sécurité du système d'information. Ces clauses sont décrites dans le « **Plan d'Assurance Sécurité (PAS)** ». Elles prévoient notamment des engagements du prestataire sur :

- La conservation des traces, sauvegarde des informations, des logiciels et des images systèmes
- La journalisation des événements et la protection de l'information journalisée
- La mise en place de mesures contre les logiciels malveillants
- La gestion des vulnérabilités techniques
- La gestion et le traitement des incidents liés à la sécurité de l'information
- La mise en œuvre de la continuité de la sécurité de l'information etc.

Les clauses spécifiques à l'hébergement dans le Cloud sont quant à elles décrites dans la « Politique appliquée à la sécurité des SI hébergés dans le Cloud » (IT 2025-026) et incluent :

- Les engagements de disponibilité des services,
- L'intégrité des sources confiées à l'hébergeur, la confidentialité de l'ensemble des éléments transmis, le chiffrement des données
- La réversibilité des données ainsi que leur destruction irréversible à la fin des contrats
- La garantie du maintien en condition de sécurité et du signalement de tout incident de sécurité
- L'auditabilité du service, la traçabilité des actions
- La conformité réglementaire en matière de traitement des données, de localisation des hébergements et des équipes œuvrant sur le système.

5.5 Sécurité Physique

Objectif 9 : Sécurité physique des locaux abritant les systèmes d'information

Inscrire la sécurisation physique des SI dans la sécurisation physique des locaux et dans les processus associés.

PHY-ZONES : Découpage des sites en zones de sécurité.

Un découpage des sites en zones physiques de sécurité est effectué selon des règles établies et en liaison avec les managers de la sécurité des systèmes d'information locaux (MSSI) et les services en charge de l'immobilier, de la sécurité et des moyens généraux. Pour chaque zone, des critères d'autorisation d'accès stricts sont définis et appliqués. Un zonage spécifique a par ailleurs été réalisé sur les data centers, incluant des mesures renforcées de contrôle d'accès physique, afin d'assurer un niveau de protection adapté à la sensibilité des équipements et des données hébergées.

Règles de sécurité s'appliquant aux zones d'accueil du public

PHY-PUBL : Accès réseau en zone d'accueil du public.

Tout accès réseau installé dans une zone d'accueil du public est filtré ou isolé du reste du réseau informatique de la Branche.

PHY-SENS : Protection des informations sensibles au sein des zones d'accueil.

Le traitement d'informations sensibles au sein des zones d'accueil est à éviter. Si un tel traitement est strictement nécessaire, il doit rester ponctuel et exceptionnel. Des mesures particulières sont alors adoptées, notamment en matière de protection audiovisuelle, ainsi qu'en matière de protection des informations stockées sur les supports.

Règles de sécurité complémentaires s'appliquant aux locaux techniques

PHY-TECH : Sécurité physique des locaux techniques.

L'accès aux locaux techniques abritant des équipements d'alimentation et de distribution d'énergie, ou des équipements de réseau et de téléphonie, est physiquement protégé. Ces locaux font l'objet d'un classement spécifique dans le cadre du zonage de sécurité.

[NIS2] Objectif de sécurité n°6, attendu (b).

PHY-TELECOM : Protection des câbles électriques et de télécommunications.

Le câblage réseau est protégé contre les dommages et les interceptions des communications qu'ils transmettent. En complément, les panneaux de raccordements et les salles des câbles sont placés en dehors des zones d'accueil du public et leur accès est contrôlé.

PHY-CTRL : Contrôles anti-piégeages.

Des contrôles anti-piégeages peuvent être réalisés sur les systèmes d'information identifiés comme sensibles. Ces opérations sont effectuées par du personnel habilité et formé à cet effet, avec si nécessaire le recours à des prestataires spécialisés pour des interventions ponctuelles de type « dépoussiérage ».

Objectif 10 : Sécurité physique des centres informatiques

Dimensionner les protections physiques des centres informatiques en fonction des enjeux liés à la concentration des moyens et données abrités.

Règles générales

PHY-CI-LOC : Découpage des locaux en zones de sécurité.

Un découpage des centres informatiques en zones physiques de sécurité est effectué selon des règles établies et en liaison avec les managers de la sécurité des systèmes d'information locaux (MSSI) et les services en charge de l'immobilier, de la sécurité et des moyens généraux. Pour chaque zone, des critères d'autorisation d'accès stricts sont définis et appliqués. Un zonage spécifique a par ailleurs été réalisé sur les data centers, incluant des mesures renforcées de contrôle d'accès physique, afin d'assurer un niveau de protection adapté à la sensibilité des équipements et des données hébergées.

[NIS2] Objectif de sécurité n°6, attendu (a).

PHY-CI-HEBERG : Convention de service en cas d'hébergement tiers.

Dans le cas où un tiers gère tout ou partie des locaux du centre informatique, une convention de service, définissant les responsabilités mutuelles en matière de sécurité, est établie entre ce tiers et la CNAF.

Règles de sécurité complémentaires s'appliquant aux zones internes et restreintes

PHY-CI-CTRLACC : Contrôle d'accès physique.

L'accès aux zones internes (autorisées uniquement au personnel du centre informatique ou aux visiteurs accompagnés) et restreintes (autorisées aux seules personnes habilitées ou aux visiteurs accompagnés) repose sur un dispositif de contrôle d'accès physique. Ce dispositif s'appuie sur des produits qualifiés et bénéficie d'un maintien en condition de sécurité rigoureux.

Par ailleurs, une protection physique renforcée est mise en place pour des zones identifiées, notamment par le biais de la vidéosurveillance, du gardiennage et de systèmes d'alertes. Ces dispositifs visent à prévenir, détecter et permettre une réaction rapide en cas d'accès non autorisé.

[NIS2] Objectif de sécurité n°6, attendus (b) et (c).

PHY-CI-MOYENS : Délivrance des moyens d'accès physique.

La délivrance des moyens d'accès physique repose sur un processus formel lié au circuit d'arrivée et de départ du personnel, incluant la vérification d'identité. L'accès aux zones sensibles est strictement limité aux personnes autorisées et habilitées. Toute autre personne amenée à y intervenir (prestataire, technicien, personnel de nettoyage ou visiteurs) le fait uniquement sous surveillance permanente. Les droits d'accès sont accordés au regard du besoin strictement nécessaire à l'exécution des missions des personnes.

[NIS2] Objectif de sécurité n°6, attendus (d) et (e).

PHY-CI-TRACE : Traçabilité des accès.

Une traçabilité des accès, par les visiteurs externes, aux zones restreintes est mise en place. Ces traces sont alors conservées, dans le respect des textes protégeant les données personnelles.

Règles de sécurité complémentaires s'appliquant aux salles informatiques et aux locaux techniques

PHY-CI-ENERGIE : Local énergie.

L'alimentation secteur des équipements est conforme aux règles de l'art, de façon à se prémunir des atteintes à la sécurité des personnes et équipements liées à un défaut électrique.

PHY-CI- CLIM : Climatisation.

Un dispositif de climatisation dimensionné en fonction des besoins énergétiques du système informatique est installé. Des procédures de réaction en cas de panne, connues du personnel, sont élaborées et vérifiées régulièrement. Ces dispositions visent à prévenir toute surchauffe des équipements, pouvant engendrer une perte du service voire une détérioration du matériel.

PHY-CI-INC : Lutte contre l'incendie.

Des dispositifs de protection incendie sont installés dans les locaux techniques, conformément aux exigences de sécurité. Les procédures de réaction à un incendie sont définies et régulièrement testées. Les salles techniques doivent être propres. Aucun carton, papier, ou autre source potentielle de départ de feu n'est entreposé dans ces locaux.

PHY-CI-EAU : Lutte contre les voies d'eau.

Une étude sur les risques dus aux voies d'eau doit être réalisée. Cette étude doit notamment prendre en compte le risque de fuite sur un collecteur d'eau douce.

Objectif 11 : Système d'information de sûreté (contrôle d'accès)

Traiter de manière globale la sécurité des systèmes d'information et de communication qui assurent la sûreté d'un site.

Les sites indispensables à la réalisation des missions de la branche s'appuient sur des services support des activités de sûreté physique. Dans ce cadre, l'appellation « services de systèmes d'information et de communication de sûreté » regroupe :

- ▶ Les services support des activités de contrôle d'accès et détection d'intrusion (CTA), permettant au personnel de sûreté :
 - ▶ D'authentifier, d'autoriser et de tracer l'accès à une ressource physique (contrôle d'accès) ;
 - ▶ De détecter, d'alerter et de tracer en cas de tentative d'accès non autorisé (détection d'intrusion).
- ▶ Les services support des activités de vidéo-surveillance (VS), fournissant au personnel de sûreté un système de caméras disposées sur l'ensemble du site, de transport des flux vidéo, d'enregistrement, d'archivage et de visionnage de ces vidéos ;
- ▶ Les services support de la gestion technique des bâtiments (GTB), permettant de superviser et de gérer l'ensemble des équipements des bâtiments du site, et d'avoir une vue globale de l'état de ces bâtiments ;
- ▶ Les services support de la sécurité incendie (INC), regroupant l'ensemble des moyens informatiques mis en œuvre pour détecter, informer, intervenir et/ou évacuer tout ou partie du site en cas d'incendie.

PHY-SI-SUR : Sécurisation du système d'information de sûreté.

Pour les sites physiques considérés comme importants, des mesures de protection doivent être définies et appliquées en se basant sur les conclusions d'une analyse de risques. L'analyse de risques conduit à la désignation des briques essentielles dont il faut assurer la protection contre des actes malveillants. Un système de gestion de la sécurité du système d'information de sûreté (s'inspirant de la norme ISO 27001) assure le maintien en condition de sécurité. L'emploi de produits labellisés, quand ils existent, est fortement recommandé.

5.6 Sécurité des réseaux

Objectif 12 : Usage sécurisé des réseaux nationaux

Utiliser pour les organismes éligibles les infrastructures nationales, en respectant les règles de sécurité qui leur sont attachées.

RES-MAITRISE : Systèmes autorisés sur le réseau.

Seuls les équipements gérés et configurés par les équipes habilitées peuvent être connectés au réseau local de la branche Famille de la sécurité sociale.

Cette exigence est notamment rappelée au sein de la « Charte nationale de sécurité de l'utilisateur du SI » (LR-2017-069) qui stipule que « l'utilisateur s'engage à ne pas connecter du matériel personnel au système ».

d'information [...] et en aucun cas directement au système informatique ». Il en est de même pour les matériels dont l'origine n'est pas connue et non contrôlée.

Cette restriction est techniquement assurée par un dispositif de contrôle d'accès au réseau (NAC) configuré en mode bloquant, qui empêche toute connexion d'équipements non enregistrés ou non conformes.

[NIS2] Objectif de sécurité n°9, attendus (a) à (e).

RES-INTERCO : Interconnexion avec des réseaux externes.

Toutes les interconnexions vers l'extérieur sont réalisées via des équipements de sécurité maîtrisés par la Direction du système d'information de la Branche. Les interconnexions réalisées en dehors de l'infrastructure du réseau national (avec les prestataires ou partenaires) sont quant à elle dûment répertoriées afin d'assurer leur maîtrise (connaissance des fournisseurs d'accès, réversibilité, MCO).

RES-ENTSOR : Mettre en place un filtrage réseau pour les flux sortants et entrants.

Tous les flux réseau, qu'ils soient entrants ou sortants, transitent exclusivement via des équipements de sécurité dédiés, tels que des pare-feux et des serveurs proxy. Les configurations en place empêchent les machines du réseau interne de la Branche de contourner ces dispositifs, garantissant un filtrage systématique et un contrôle des communications.

[NIS2] Objectif de sécurité n°7, 'Cloisonnement', attendus (e) et (f) et 'Filtrage des communications', attendu (d).

RES-PROT : Protection des informations.

Les accès à Internet sont obligatoirement réalisés via les pare-feux et/ou proxys, garantissant un filtrage centralisé et conforme aux exigences de sécurité de la Branche. Lorsqu'une information sensible doit transiter sur un réseau non maîtrisé, elle doit être protégée par un chiffrement adapté.

L'instruction technique de « Protection des informations sensibles grâce au chiffrement » (IT-2017-099) précise les modalités de mise en œuvre du chiffrement pour assurer la protection de ces informations lors de leur transmission.

Objectif 13 : Usage sécurisé des réseaux locaux

Maîtriser les interconnexions de réseaux locaux. Configurer de manière adéquate les équipements de réseau actifs.

RES-CLOIS : Cloisonner le système d'information en sous-réseaux de niveaux de sécurité homogènes.

Le réseau est segmenté, des zones sont définies en fonction du niveau de sécurité des actifs qu'elles irriguent ; un filtrage strict des flux autorisés est mis en place, seuls les flux nécessaires au fonctionnement et au maintien en conditions opérationnelles de sécurité des systèmes sont autorisés. Par défaut les flux qui ne sont pas explicitement autorisés sont interdits.

La segmentation du système d'information de la branche Famille de la sécurité sociale est un objectif de sécurité poursuivi de manière continue.

[NIS2] Objectif de sécurité n°7, 'Cloisonnement', attendus (a), (b), (c), (d), (g) et (h).

RES-INTERCOGEO : Interconnexion des sites géographiques locaux d'un organisme.

L'interconnexion au niveau local de réseaux locaux d'un organisme de la Branche n'est possible que si la proximité géographique le justifie et sous réserve de la mise en place de connexions dédiées à cet effet, et de passerelles sécurisées et homologuées par le RSSI et l'AQSSI.

RES-RESS : Cloisonnement des ressources en cas de partage de locaux.

Dans le cas où un organisme de la Branche partage des locaux (bureaux ou locaux techniques) avec des partenaires, des mesures de cloisonnement des ressources informatiques sont mises en place. Si le cloisonnement n'est pas physique, les mesures prises doivent être validées par le RSSI et l'AQSSI.

Objectif 14 : Accès spécifiques

Ne pas porter atteinte à la sécurité du système d'information par le déploiement d'accès non supervisés.

RES-INTERNET-SPECIFIQUE : Cas particulier des accès spécifiques dans un organisme

Afin de maîtriser les risques liés à l'exposition directe à Internet, les accès spécifiques nécessaires à certains usages métiers sont strictement encadrés. Toute demande doit faire l'objet d'une dérogation auprès du RSSI de la CNAF (ou de l'autorité d'homologation), formalisée et argumentée, soumise à validation préalable. Les

accès accordés sont ensuite mis en œuvre exclusivement sur des postes isolés physiquement et logiquement du réseau interne de la Branche. Ce dispositif permet de limiter l'impact potentiel d'une compromission, en assurant une séparation claire avec les ressources critiques du système d'information.

Objectif 15 : Usage sécurisé des réseaux sans fil

Maîtriser le déploiement, la configuration et l'usage des réseaux sans fil.

RES-SSFIL : Mise en place de réseaux sans fil.

Les réseaux Wi-Fi de la CNAF sont entièrement maîtrisés par la DSI et leur déploiement respecte des mesures spécifiques de sécurité fondées sur une analyse de risques, conformément au principe de défense en profondeur. Le choix de l'opérateur Wi-Fi repose également sur des critères de sélection intégrant des exigences précises en matière de sécurité. Le schéma d'architecture Wi-Fi assure la traçabilité de ce déploiement au niveau de la Branche.

Les réseaux Wi-Fi sont cloisonnés dans des VLAN dédiés et les flux sont chiffrés. Seuls les terminaux de la Branche, authentifiés par certification, peuvent accéder au réseau interne.

Le service Wi-Fi destiné aux allocataires dans les espaces d'accueil des CAF est lui totalement isolé du système d'information interne. L'instruction technique 2019-204 encadre le dispositif de déploiement de ce Wi-Fi visiteurs.

Objectif 16 : Sécurisation des mécanismes de commutation et de routage

Configurer les mécanismes de commutation et de routage pour se protéger des attaques.

RES-COUCBAS : Implanter des mécanismes de protection contre les attaques sur les couches basses.

Une attention particulière est portée à la sécurisation des couches bases du réseau de la Branche de façon à se prémunir des attaques usuelles. Ainsi, le réseau LAN est protégé contre les attaques usuelles telles que les tempêtes de broadcast, et intègre des mécanismes de sécurité comme le *DHCP snooping*.

RES-SECRET : Modifier systématiquement les éléments d'authentification par défaut des équipements et services.

Afin de garantir un niveau de sécurité conforme aux exigences définies, les éléments d'authentification par défaut des équipements sont systématiquement modifiés lors de leur mise en service. En particulier, les mots de passe par défaut des équipements actifs (pares-feux, commutateurs, routeurs) sont remplacés. Par ailleurs, l'authentification des administrateurs sur ces équipements repose sur une infrastructure centralisée via LDAP, assurant une meilleure traçabilité et un contrôle renforcé des accès.

[NIS2] Objectif de sécurité n°10, 'Authentification', attendu (b).

RES-DURCI : Durcir les configurations des équipements de réseaux.

Les équipements réseaux font l'objet d'un durcissement systématique lors de leur mise en service. Ce durcissement inclut la désactivation des interfaces et services non utilisés, la mise en œuvre de mécanismes de protection du plan de contrôle, ainsi que le remplacement des mots de passe et certificats par défaut. Ces mesures visent à limiter la surface d'attaque et à garantir la résilience des équipements face aux menaces connues.

Objectif 17 : Cartographie réseau

Tenir à jour une cartographie détaillée et complète des réseaux et des interconnexions.

RES-CARTO : Élaborer les documents d'architecture technique et fonctionnelle.

L'architecture réseau du système d'information de la Branche est formalisée à travers des documents d'architecture technique et fonctionnelle. Ces documents sont régulièrement mis à jour pour refléter l'évolution du SI et sont stockés sur des espaces de travail sécurisés, dont l'accès est strictement limité aux administrateurs.

Objectif 18 : Architecture des centres informatiques

Appliquer les principes de défense en profondeur à l'architecture matérielle et logicielle des centres informatiques.

ARCHI-HEBERG : Principes d'architecture de la zone d'hébergement.

L'architecture des infrastructures d'hébergement de la Branche est conçue selon les principes de défense en profondeur afin de garantir la disponibilité, la confidentialité, l'intégrité et la traçabilité (DICT) des traitements. Elle repose sur une segmentation rigoureuse en zones de sécurité (DMZ), des environnements cloisonnés selon les usages, et des VLAN dédiés. Le filtrage des flux applicatifs et d'administration est appliqué selon le principe du moindre privilège. Les ressources critiques sont isolées sur des machines dédiées selon les besoins de sécurité et de performance.

ARCHI-STOCKCI : Architecture de stockage et de sauvegarde.

Le réseau de stockage repose sur une architecture SAN dédiée, spécifiquement conçue pour répondre aux besoins des centres informatiques en termes de performance et de disponibilité. En complément, certains besoins de stockage sont couverts via des solutions de stockage sur le LAN, intégrées à l'architecture globale et encadrées par des règles de sécurité appropriées.

ARCHI-PASS : Passerelle Internet.

L'ensemble des accès internet est centralisé et géré par la DSI de la CNAF, au travers de passerelles homologuées répondant aux exigences de sécurité définies. Ces interconnexions sont formellement encadrées et un schéma d'infrastructure Internet est tenu à jour.

5.7 Exploitation des systèmes d'information

Objectif 19 : Protection des informations sensibles

Définir et mettre en œuvre des mesures de protection renforcées pour les informations sensibles.

EXP-PROT-INF : Protection des informations sensibles en confidentialité et en intégrité.

Des mesures sont en place pour garantir la confidentialité et l'intégrité des informations sensibles de la Branche. Une instruction spécifique encadre le recours au chiffrement pour la protection des données sensibles (IT 2017-099), notamment lorsqu'elles transitent sur des réseaux non homologués. Par ailleurs, une politique d'identification et d'authentification des accès internes au SI de la branche Famille de la sécurité sociale (IT 2018-046) est appliquée pour encadrer les règles d'identification et d'authentification des comptes d'accès au SI de la branche Famille de la sécurité sociale. Enfin, une liste formalisée des personnes habilitées à accéder aux bases de données est tenue à jour.

Objectif 20 : Surveillance et configuration des ressources informatiques

Durcir les configurations des ressources informatiques, et surveiller les interventions opérées sur celles-ci.

EXP-TRAC : Traçabilité des interventions sur le système.

Les interventions de maintenance sur les ressources informatiques de la Branche sont systématiquement tracées. Les traces systèmes et traces de sécurité sont collectées de manière centralisée au sein de solutions dédiées à la supervision et à la journalisation des événements. Par ailleurs, la CNAF dispose d'un SOC (Security Operations Center)³ susceptible d'exploiter ces traces dans le cadre d'analyses de sécurité ou d'investigations post-incidents.

EXP-CONFIG : Configuration des ressources informatiques.

Les systèmes d'exploitation et les logiciels installés sur les ressources informatiques de la branche Famille de la sécurité sociale font l'objet d'un durcissement systématique. Une « checklist » de configuration sécurisée est complétée et soumise à la DCISN lors de chaque nouvelle installation de composant, en particulier sur un système d'information indispensable à la réalisation des missions de la branche, afin d'assurer la mise en œuvre des mesures de sécurité attendues. En complément, un tableau de bord de suivi des mises à jour permet de superviser en continu l'état de mise à jour des systèmes d'exploitation déployés, garantissant ainsi la conformité continue aux exigences de sécurité applicables.

³ Security Operation Center (SOC) est une structure dédiée à la surveillance, l'analyse et à la réponse aux cybermenaces

Les ressources sont configurées de manière sécurisée, en s'appuyant sur les recommandations des éditeurs, des fabricants ou de l'ANSSI.

[NIS2] Objectif de sécurité n°18, attendus (c) et (d).

EXP-DOC-CONFIG : Documentation des configurations.

La configuration standard des ressources informatiques est documentée et mise à jour à chaque changement notable.

Objectif 21 : Gestion des autorisations et contrôle d'accès logique aux ressources

Authentifier les usagers et contrôler leurs accès aux ressources des systèmes d'information de la CNAF, en fonction d'une politique explicite d'autorisations.

Contrôle des accès logiques

EXP-ID-AUTH : Identification, authentification et contrôle d'accès logique.

La politique d'identification, d'authentification et de gestion des accès (IT 2018-046) est formellement appliquée à l'ensemble des utilisateurs internes du SI de la Branche (comptes standards et comptes à privilèges).

L'authentification individuelle est systématiquement requise pour l'accès aux ressources, conformément aux exigences rappelées dans la « Charte nationale de sécurité de l'utilisateur du système d'information » (LR 2017-069) de la Branche. L'emploi d'un compte individuel du SI est réservé à l'utilisateur ou au processus auquel ce compte a été attribué.

[NIS2] Objectif de sécurité n°10, 'Identification', attendus (a) et (b) et 'Droit d'accès, attendu (a).

Objectif de sécurité n°11, 'Comptes d'administration', attendu (c).

Des mécanismes d'authentification forte sont déployés pour gérer l'accès aux ressources.

Le contrôle des accès logiques est géré à travers un processus formalisé, aligné sur le cycle de vie des ressources humaines, assurant l'attribution, la modification et la révocation des droits selon le principe du moindre privilège.

Les mécanismes d'accès aux postes de travail sont décrits dans l'instruction de « Sécurisation des accès au poste de travail » (IT 2024-217).

[NIS2] Objectif de sécurité n°10, 'Authentification', attendu (a).

MC-EXP- ID-PARTAGE : Mesure complémentaire à la PSSI MCAS – Gestion des comptes partagés

L'usage de comptes partagés est strictement limité aux situations ou contraintes technique ou opérationnelles empêchant la création de comptes individuels. Dans ces cas, des mesures de sécurité complémentaires sont mises en place pour garantir la traçabilité et réduire les risques associés.

Chaque compte partagé est attribué uniquement à des utilisateurs explicitement autorisés. Les éléments d'authentification sont modifiés à chaque changement de périmètre d'accès et ne sont accessibles qu'aux personnes habilitées.

[NIS2] Objectif de sécurité n°10, 'Identification', attendu (c) et 'Authentification', attendus (c) et (d).

EXP-DROITS : Droits d'accès aux ressources.

La gestion des droits d'accès au sein de la branche Famille de la sécurité sociale repose sur les principes de moindre privilège et de besoin d'en connaître, appliqués systématiquement à l'ensemble des ressources du système d'information. Les droits d'accès ne sont attribués qu'aux seules ressources nécessaires à la réalisation des activités et qu'aux seuls utilisateurs et processus justifiant d'un besoin au regard des missions.

[NIS2] Objectif de sécurité n°10, 'Droits d'accès', attendus (b) et (c).

Un référentiel des habilitations est maintenu pour tracer et contrôler les droits accordés aux utilisateurs en fonction de leur rôle, de leur périmètre fonctionnel et du niveau de sensibilité des données concernées. Le cycle de vie des droits (attribution, modification, suppression) est encadré par une procédure interne, et fait l'objet d'un suivi, en lien avec les évolutions des missions ou des mouvements de personnels.

La revue du référentiel des habilitations est intégrée au plan de contrôle interne de la Branche et est effectué au moins annuellement pour vérifier les exigences de sécurité établies et le cas échéant corriger les anomalies.

[NIS2] Objectif de sécurité n°10, 'Droits d'accès', attendu (d).

Objectif de sécurité n°11, 'Comptes d'administration', attendu (g).

EXP-PROFILS : Gestion des profils d'accès aux applications.

Les applications manipulant des données sensibles sont conçues ou configurées de manière à permettre une gestion fine par profils d'accès. Ces profils sont une fois de plus définis selon le principe du besoin d'en connaître et mettent en œuvre le moindre privilège en ne donnant à chaque utilisateur que les droits strictement nécessaires à l'exercice de ses missions.

Processus d'autorisation

EXP-PROC-AUTH : Autorisations d'accès des utilisateurs.

L'autorisation d'accès aux ressources du système d'information repose sur un processus formalisé de gestion des habilitations, intégré aux procédures d'arrivée, de mobilité et de départ du personnel de la branche Famille de la sécurité sociale. Ce processus permet de garantir que les accès sont accordés de manière justifiée, tracée et conforme au principe du besoin d'en connaître.

EXP-REVUE-AUTH : Revue des autorisations d'accès.

Une revue des autorisations d'accès est réalisée annuellement sous le contrôle du RSSI et avec l'appui des Manager de la sécurité du système d'information (MSSI) locaux. Cette revue prend forme dans le cadre du plan de contrôle interne annuel de la CNAF. Le plan de contrôle interne annuel de la branche Famille de la sécurité sociale est diffusé par la Direction Comptable et Financière de la CNAF, au travers d'une instruction technique.

Gestion des authentifiants

EXP-CONF-AUTH : Confidentialité des informations d'authentification.

Les informations d'authentification (mots de passe d'accès aux SI, clés privées liées aux certificats électroniques, etc.) sont considérées comme des données sensibles. Les règles s'imposant à la gestion de ces informations par les utilisateurs sont précisées dans la Charte nationale de l'utilisateur de la branche Famille de la sécurité sociale (LR 2017-069), en vue de protéger les droits d'accès au système d'information. Les agents de la CNAF sont sensibilisés à ces enjeux de confidentialité dès leur arrivée.

Lorsque pour des raisons techniques ou opérationnelles la modification d'éléments secrets n'est pas possible, la CNAF met en œuvre un contrôle d'accès approprié à la ressource concernée ainsi que des mesures de réduction du risque lié à l'utilisation d'un élément secret d'authentification fixe, assurant également la traçabilité des accès.

[NIS2] Objectif de sécurité n°10, 'Authentification', attendus (f) et (g).

EXP-GEST-PASS : Gestion des mots de passe.

La Charte nationale de l'utilisateur (LR 2017-069) rappelle les exigences relatives à la gestion des mots de passe par les utilisateurs et précise qu'il convient de « ne pas en conserver d'enregistrement non sécurisé » et de « ne le communiquer à personne ». La branche Famille de la sécurité sociale met à disposition de ses agents un gestionnaire de mots de passe permettant une sauvegarde dans une base de données chiffrée.

EXP-INIT – PASS : Initialisation des mots de passe.

Chaque compte utilisateur est créé avec un mot de passe initial aléatoire unique.

EXP-POL-PASS : Politiques de mots de passe.

Les règles de gestion et de protection des mots de passe donnant accès aux applications et infrastructures nationales, sont respectées dans chaque organisme de la branche Famille de la sécurité sociale. Les recommandations de la Charte nationale des utilisateurs du SI (LR 2017-069) et de la « Politique appliquée d'identification et d'authentification des accès internes » (IT 2018-046) s'appliquent « à toutes les personnes intervenant ou accédant au SI de la branche Famille de la sécurité sociale quel que soit le lieu depuis lequel cet accès s'opère ».

La politique de mot de passe définie par la CNAF respecte les recommandations de l'ANSSI en matière de complexité, en tenant compte du niveau de complexité maximal permis par la ressource concernée, et en matière de fréquence de renouvellement.

[NIS2] Objectif de sécurité n°10, 'Authentification', attendu (e).

EXP-CERTIFS : Utilisation de certificats électroniques.

L'utilisation de certificats électroniques respecte les règles édictées par le Référentiel général de sécurité (RGS).

EXP-QUAL-PASS : Contrôle systématique de la qualité des mots de passe.

La politique de mots de passe de la branche Famille de la sécurité sociale est techniquement imposée, déployée dans l'environnement. Ces règles permettent de contrôler les paramètres établis afin de garantir la conformité avec les exigences de sécurité définies. Un contrôle périodique des paramètres techniques relatifs aux mots de passe est réalisé.

Gestion des authentifiants d'administration

EXP-SEQ-ADMIN : Séquestre des authentifiants « administrateur ».

La « Politique appliquée d'identification et d'authentification des accès internes au système d'information de la branche Famille de la sécurité sociale » (IT 2018-046) décrit les spécificités liées à l'usage des comptes administrateurs, notamment les exigences renforcées en matière de gestion des identifiants. Les authentifiants administrateurs sont gérés au sein d'un coffre-fort numérique dédié.

Les actions d'administration sont systématiquement tracées et les journaux sont conservés, permettant d'identifier les utilisateurs ayant exercé des droits spécifiques.

EXP-POL-ADMIN : Politique de mots de passe « administrateurs ».

Chaque administrateur dispose d'un identifiant et d'un mot de passe propre destinés à l'administration, comme explicité dans la « Politique appliquée d'identification et d'authentification des accès internes au système d'information de la branche Famille de la sécurité sociale » (IT 2018-046).

EXP-DEP-ADMIN : Gestion du départ d'un administrateur des SI.

En cas de départ d'un administrateur disposant de privilèges sur des composants des SI, les comptes individuels dont il disposait sont immédiatement désactivés. Les éventuels mots de passe d'administration dont il avait connaissance sont changés (exemples : mots de passe des comptes fonctionnels, comptes génériques ou comptes de service utilisés dans le cadre des fonctions de l'administrateur).

Objectif 22 : Sécurisation de l'exploitation

Fournir aux administrateurs les outils nécessaires à l'exercice des tâches de sécurité des systèmes d'information et configurer ces outils de manière sécurisée.

Administration des systèmes

EXP-RESTR-DROITS : Restriction des droits.

Sauf exception dûment motivée et validée par le RSSI, les utilisateurs, quel que soit leur statut, n'ont pas de droits d'administration (domaine, local). Dans le cas d'une exception, celle-ci est tracée et renouvelée annuellement. A défaut de renouvellement, les privilèges d'administration sont supprimés.

EXP-PROT-ADMIN : Protection des accès aux outils d'administration.

L'accès aux outils et interfaces d'administration est strictement limité aux personnes habilitées, selon une procédure formelle d'autorisation d'accès.

EXP-HABILIT-ADMIN : Habilitation des administrateurs.

L'habilitation des administrateurs s'effectue selon une procédure validée par l'autorité d'homologation. Le nombre de personnes habilitées pour des opérations d'administration est connu et validé par l'autorité d'homologation.

La « Politique appliquée d'identification et d'authentification des accès internes au SI de la branche Famille de la sécurité sociale » (2018-046) encadre l'attribution des comptes relevant d'actions d'administration.

Le recensement des comptes d'administration est tenu à jour et le contrôle des habilitations forme partie intégrante du contrôle interne réalisé par la Branche.

[NIS2] Objectif de sécurité n°11, 'Comptes d'administration', attendus (b) et (f).

EXP-GEST-ADMIN : Gestion des actions d'administration.

Les ressources des réseaux d'administration sont gérées et configurées. Les opérations d'administration sont réalisées exclusivement à partir de comptes d'administration, via un bastion, permettant de tracer individuellement l'ensemble des actions effectuées par les administrateurs. Ces actions sont tracées dans le cadre de la collecte des logs systèmes et l'ensemble des journaux est centralisé dans un outil de supervision dédié. L'imputabilité des actions d'administration peut donc être gérée au niveau individuel, le cas échéant.

[NIS2] Objectif de sécurité n°11, 'Comptes d'administration', attendus (a) et (d).

Objectif de sécurité n°19, attendu (b).

Lorsque des raisons techniques ou opérationnelles ne permettent pas d'effectuer des actions d'administration à partir d'un compte d'administration, l'entité met en œuvre des mesures permettant d'assurer le contrôle de ces actions d'administration et des mesures de réduction du risque lié à l'utilisation d'un compte non dédié à l'administration.

[NIS2] Objectif de sécurité n°11, 'Comptes d'administration', attendu (e).

EXP-SEC-FLUXADMIN : Sécurisation des flux d'administration.

Les opérations d'administration sont effectuées au moyen d'un réseau d'administration dédié et s'appuient sur des protocoles sécurisés. Les ressources matérielles des réseaux d'administration sont utilisées exclusivement pour réaliser les actions d'administration.

Lorsque des raisons techniques ou opérationnelles ne permettent pas de dédier le poste de travail physique de l'administrateur pour les actions d'administration, des mesures de durcissement et de cloisonnement du système d'exploitation du poste de travail sont mises en œuvre pour permettre d'isoler le système d'exploitation utilisé pour les actions d'administration du système d'exploitation utilisé pour les autres actions.

Les communications associées à des actions d'administration sont protégées par des mécanismes de chiffrement et d'authentification conformes à l'état de l'art et aux recommandations de l'ANSSI. A défaut, des mesures de protection de la confidentialité et de l'intégrité de ces flux sont mises en place pour renforcer le contrôle et la traçabilité des actions d'administration.

[NIS2] Objectif de sécurité n°19, attendus (a) à (l).

EXP-CENTRAL : Centraliser la gestion du système d'information.

Afin de gérer efficacement un grand nombre de postes d'utilisateurs, de serveurs ou d'équipements réseau, les administrateurs utilisent des outils centralisés, permettant l'automatisation de traitements quotidiens et offrant une vue globale et pertinente sur le système d'information.

EXP-SECXDIST : Sécurisation des outils de prise de main à distance.

La prise de main à distance d'une ressource informatique connectée au SI de la CNAF n'est réalisable que par les agents dûment autorisés par la DSI, sur les ressources informatiques de leur périmètre.

Les mesures de sécurité relatives à la prise de main à distance sont définies dans la « Politique appliquée de prise de main à distance » de la Branche (IT 2024-200). Cette politique se base sur les préconisations de l'ANSSI en matière de « Recommandation de sécurité relatives à la télé assistance » pour préciser les règles de sécurité qui s'imposent au sein de la branche Famille de la sécurité sociale.

Administration des domaines

EXP-DOM-POL : Définir une politique de gestion des comptes du domaine.

La « Politique appliquée d'identification et d'authentification des accès internes au système d'information de la branche Famille de la sécurité sociale » (IT 2018-046) documente la gestion des comptes du domaine de la CNAF.

EXP-DOM-PASS : Configurer la stratégie des mots de passe des domaines.

La « Politique appliquée d'identification et d'authentification des accès internes au système d'information de la branche Famille de la sécurité sociale » (IT 2018-046) explicite les règles de gestion des mots de passe, notamment celles relatives à leur complexité, durée de validité et renouvellement.

Cette politique est mise en œuvre via des stratégies de groupe (GPO) appliquées sur les contrôleurs de domaines, garantissant l'application uniforme des exigences sur l'ensemble des comptes.

Les paramètres en vigueur imposent notamment un nombre minimal de caractères, l'utilisation de types de caractères variés ainsi qu'un verrouillage temporaire des comptes après plusieurs tentatives infructueuses. Ces mesures sont conformes aux « Recommandations de sécurité relatives à l'Active Directory » publiées par l'ANSSI.

EXP-DOM-NOMENCLAT : Définir et appliquer une nomenclature des comptes du domaine.

La « Politique appliquée d'identification et d'authentification des accès internes au système d'information de la branche Famille de la sécurité sociale » (IT 2018-046) définit une nomenclature standardisée des comptes, permettant de distinguer clairement les comptes utilisateurs standards, les comptes à privilèges (comptes administrateurs) et les comptes génériques (comptes de services et comptes techniques).

Cette nomenclature facilite la gestion, le suivi et la traçabilité des accès et constitue un prérequis essentiel à l'application des principes de moindre privilège et de séparation des responsabilités dans l'administration du système d'information de la Branche.

EXP-DOM-RESTADMIN : Restreindre au maximum l'appartenance aux groupes d'administration du domaine.

L'appartenance aux groupes d'administration du domaine est strictement limitée aux cas d'usage identifiés et revus régulièrement dans le cadre du processus de gestion des habilitations.

La majorité des opérations d'administration sont réalisées à l'aide de comptes disposants de droits locaux délégués ou rattachés à des groupes d'administration restreinte définis, conformément au principe du moindre privilège. Ce fonctionnement, conforme aux recommandations de l'ANSSI, permet de réduire la surface d'attaque et de limiter les privilèges aux seuls usages indispensables.

EXP-DOM-SERV : Maîtriser l'utilisation des comptes de service et comptes techniques.

Les comptes à privilèges génériques (comptes de service et comptes techniques) sont stockés dans un coffre-fort électronique intégré au référentiel des logiciels de sécurité validés par la CNAF. Les règles d'identification et d'authentification des ces comptes sont décrits dans la « Politique appliquée d'identification et d'authentification des accès internes au système d'information de la branche Famille de la sécurité sociale » (IT 2018-046).

EXP-DOM-LIMITSERV : Limiter les droits des comptes de service.

L'utilisation des comptes génériques à privilèges (comptes de service et comptes techniques) est réduite à son strict minimum et approuvée par la DCISN de la DSI qui en assure le référentiel national. L'utilisation de ces comptes est strictement limitée et leur création fait l'objet d'une demande justifiée auprès de la DCISN.

EXP-DOM-OBSOLET : Désactiver les comptes du domaine obsolètes.

La gestion des comptes est notamment encadrée par le processus de gestion des habilitations, intégrant systématiquement la désactivation ou suppression des comptes obsolètes, notamment en cas de départ, de changement de poste ou de fin d'usage d'un service. Ce processus repose sur une synchronisation avec la gestion des ressources humaines de la branche Famille de la sécurité sociale et une revue régulière des comptes.

[NIS2] Objectif de sécurité n°10, 'Identification' attendu (e).

EXP-DOM-ADMINLOC : Améliorer la gestion des comptes d'administrateur locaux.

Afin de prévenir la réutilisation des comptes administrateurs locaux, un mécanisme de gestion individualisée des mots de passe a été mise en œuvre (mot de passe administrateur unique, complexe, régulièrement renouvelé et stocké de manière sécurisée dans un référentiel central). Cette mesure permet de réduire les risques de compromission latérale et contribue à l'application du principe du moindre privilège.

Envoi en maintenance et mise au rebut

EXP-MAINT-EXT : Maintenance externe.

Tous les postes de travail de la branche Famille de la sécurité sociale sont chiffrés de manière systématique, à l'aide d'une solution conforme aux exigences de sécurité en vigueur. En cas d'envoi en maintenance externe, cette mesure garantit la protection des données en cas de compromission physique. Pour les équipements manipulant des données particulièrement sensibles, des mesures complémentaires peuvent être prises, notamment la rétention des supports internes. Par ailleurs, les opérations de maintenance externe sont encadrées contractuellement, incluant des engagements de confidentialité et de sécurité adaptés.

EXP-MIS-REB : Mise au rebut.

La CNAF applique une procédure stricte de mise au rebut des ressources informatiques (Directives de mise au rebut et de recyclage des matériels informatiques). Conformément à la « Politique nationale de sauvegarde des données » en vigueur (LR 2018-003), toutes les unités de disques et les serveurs nationaux font systématiquement l'objet d'un effacement sécurisé des données avant leur réutilisation ou leur destruction. Cet effacement est formalisé par un document de traçabilité conservé pendant cinq ans. Les équipements obsolètes, endommagés ou en fin de vie sont quant à eux physiquement détruits, afin de garantir l'irréversibilité de l'effacement des données, notamment celles à caractère sensible.

Lutte contre les codes malveillants

EXP-PROT-MALV : Protection contre les codes malveillants.

L'ensemble des postes de travail et des serveurs de la branche Famille de la sécurité sociale est équipé d'une solution de protection contre les codes malveillants de type XDR, assurant une détection multi-canal et une réponse centralisée aux menaces.

Une solution de protection distincte est également utilisée pour les ressources exposées à des accès externes, afin de garantir un niveau de sécurité renforcé dans les zones à risque accru.

Les journaux générés par l'ensemble de ces solutions sont centralisés dans un système de supervision de la sécurité (SIEM) et exploités par le centre opérationnel de sécurité (SOC⁴) de la DCISN, permettant une corrélation des événements et une détection rapide des comportements suspects.

La CNAF veille à maintenir à jour les bases de connaissances des outils de protection contre les codes malveillants.

[NIS2] Objectif de sécurité n°5, 'Maintien en condition opérationnelle et de sécurité', attendu (b).

Objectif de sécurité n°9, attendus (f) et (g).

EXP-GEST-ANTIVIR : Gestion des événements de sécurité.

Les événements de sécurité générés par les outils de protection contre les codes malveillants sont automatiquement centralisés dans une console d'administration dédiée. Cette centralisation permet une visibilité unifiée sur l'ensemble du parc de la CNAF et facilite l'analyse des incidents de sécurité.

Les journaux sont collectés et corrélés dans le système de supervision de la sécurité (SIEM) afin de permettre une gestion a posteriori des incidents (exemples : serveur constamment infecté, virus détecté et non éradiqué par l'antivirus, etc.).

Cette architecture permet une détection précoce, un suivi statistique et une réponse rapide aux événements de sécurité liés aux menaces virales.

EXP-MAJ-ANTIVIR : Mise à jour des composants du système de protection contre les codes malveillants.

La mise à jour des composants du système de protection contre les codes malveillants est assurée de manière automatisée sur les postes de travail et les serveurs, conformément aux directives nationales définies par la DSI et validées par le RSSI. Un dispositif centralisé permet de superviser l'état de ces mises à jour et des rapports mensuels de suivi sont produits afin d'en garantir l'efficacité.

EXP-NAVIG : Configuration du navigateur Internet.

Les navigateurs déployés par la DSI de la CNAF sont configurés de manière centralisée selon des paramètres définis au niveau national, afin d'assurer un usage maîtrisé et sécurisé sur l'ensemble des serveurs et postes de travail.

Mise à jour des systèmes et des logiciels

EXP-POL-COR : Définir et mettre en œuvre une politique de suivi et d'application des correctifs de sécurité.

Une politique de gestion des correctifs de sécurité est définie et mise en œuvre au sein de la branche Famille de la sécurité sociale afin de garantir le maintien du niveau de sécurité des systèmes dans le temps. Elle s'appuie sur l'infrastructure de gestion centralisée des postes et serveurs permettant d'organiser le déploiement des mises à jour (en fonction de la criticité des systèmes, de leur niveau d'exposition et des contraintes opérationnelles). Ce dispositif repose sur une documentation formalisée et des rapports de suivi permettant de vérifier l'application effective des correctifs de sécurité.

EXP-COR-SEC : Déploiement des correctifs de sécurité.

Le déploiement des correctifs de sécurité est assuré de manière centralisée par la DSI de la CNAF, conformément aux préconisations proposées par la DCISN.

⁴ Security Operation Center (SOC) est une structure dédiée à la surveillance, l'analyse et à la réponse aux cybermenaces

EXP-OBSOLET : Assurer la migration des systèmes obsolètes.

L'ensemble des logiciels utilisés dans le système d'information de la CNAF doit être maintenu à jour et disposer d'un support éditeur actif. Un suivi régulier est assuré sur l'état de support des systèmes afin d'identifier les versions obsolètes ou en fin de vie. En cas de fin de support, une analyse de risque peut être conduite par la DCISN pour évaluer les impacts de la situation, identifier les mesures de traitement nécessaires (migration, isolement, compensations de sécurité etc.) et engager les actions correctrices nécessaires en lien avec les équipes techniques.

EXP-ISOL : Isoler les systèmes obsolètes restants.

Il est nécessaire d'isoler les systèmes obsolètes, gardés volontairement pour assurer un maintien en condition opérationnelle des projets, et pour lesquels une migration n'est pas envisageable. Chaque fois que cela est possible, cette isolation doit être effectuée au niveau du réseau (filtrage strict), des éléments d'authentification (qui ne doivent pas être communs avec le reste du SI) et des applications (pas de ressources partagées avec le reste du SI).

Journalisation

EXP-JOUR-SUR : Journalisation des alertes.

Les systèmes disposent de mécanismes de journalisation des événements de sécurité, avec conservation des traces dans des conditions garantissant leur intégrité et leur confidentialité. A la CNAF, ces événements sont centralisés via une solution de supervision (de type SIEM). L'intégrité des traces collectées est assurée par les mécanismes techniques du système de collecte et formalisée contractuellement dans les engagements de service de l'hébergement.

Les équipes en charge de l'activité de supervision de sécurité (le SOC⁵ au sein de la DCISN) assurent la prise en compte des événements de sécurité issus de l'EDR au maximum sous 24 heures ouvrés. Dans une optique d'amélioration continue, les journaux et événements de sécurité sont collectés lorsqu'ils sont utiles à la détection de scénarios de menace. Le SOC œuvre à la mise en place de corrélations et la prise en compte de ces scénarios de menaces supplémentaires.

[NIS2] Objectif de sécurité n°12, attendus (f) et (g).

Objectif de sécurité n°20, attendus (a) à (d).

EXP-POL-JOUR : Définir et mettre en œuvre une politique de gestion et d'analyse des journaux de traces.

La politique de journalisation des événements de sécurité est définie par le RSSI de la Branche, validée par l'autorité qualifiée et appliquée aux systèmes concernés. Les exigences de journalisation sont intégrées aux appels d'offres et aux plans d'assurance sécurité contractés avec les prestataires. Ces documents rappellent l'obligation de journaliser les événements de sécurité significatifs, ainsi que les mesures de protection contre l'altération ou l'accès non autorisé aux données journalisées.

L'analyse des journaux est réalisée par le centre opérationnel de sécurité (SOC) au sein de la DCISN, à l'aide notamment d'un outil de corrélation, permettant la détection des événements anormaux ou malveillants.

EXP-CONS-JOUR : Conservation des journaux.

Les journaux des événements de sécurité sont conservés sur six mois glissants, hors contraintes légales et réglementaires particulières imposant des durées de conservation spécifiques (RGPD notamment).

[NIS2] Objectif de sécurité n°20, attendu (e).

Objectif 23 : Défense des systèmes d'information

Défendre les systèmes d'information nécessite une vigilance de tous, et des actions permanentes.

EXP-GEST-DYN : Gestion dynamique de la sécurité.

⁵ Security Operation Center (SOC) est une structure dédiée à la surveillance, l'analyse et à la réponse aux cybermenaces

La détection d'activités anormales et la surveillance des flux sont assurées par le centre opérationnel de sécurité (SOC⁶) de la DCISN, y compris en dehors des heures ouvrées grâce à un dispositif de débordement. Ce dernier s'appuie sur une solution de supervision configurée pour notamment identifier les scénarios de compromission définis.

Gestion des matériels informatiques fournis à l'utilisateur

EXP-MAIT-MAT : Maîtrise des matériels.

Les postes de travail de la branche Famille de la sécurité sociale sont fournis aux utilisateurs par l'organisme et sont gérés et configurés par la Branche. La connexion d'équipements non maîtrisés, non administrés ou non mis à jour par l'organisme sur des équipements et des réseaux professionnels est interdite, comme le précise la « Charte nationale de sécurité de l'utilisateur du système d'information » (LR 2017-069) de la Branche.

EXP-PROT-VOL : Rappel des mesures de protection contre le vol.

Les postes fixes bénéficient des mesures de protection physique offertes par la Branche (câbles de sécurité, meubles fermant à clé). Chaque utilisateur doit veiller à la sécurité des supports amovibles (clés USB et disques amovibles), notamment en les conservant dans un endroit sûr. Il est recommandé de chiffrer les données contenues sur ces supports. Les supports contenant des données sensibles doivent être stockés dans des meubles fermant à clef.

EXP-DECLAR-VOL : Déclarer les pertes et vols.

Toute perte ou vol d'une ressource de la Branche doit être déclarée. Le processus de déclaration d'une perte ou d'un vol est décrit dans l'instruction technique « Mise à disposition d'une procédure décrivant le processus de gestion du vol ou de la perte de matériel nomade » (IT 2024-157). Ce processus vise à assurer la mise en œuvre rapide d'actions techniques permettant de réduire le risque de sécurité pour le SI et, le cas échéant, d'estimer les risques encourus en matière de protection des données.

EXP-REAAFFECT : Réaffectation de matériels informatiques.

La gestion des postes et supports lors de départs ou affectations s'inscrit dans un cadre organisationnel défini. Des pratiques d'effacement des données peuvent être mises en œuvre le cas échéant.

Nomadisme

EXP-NOMAD-SENS : Déclaration des équipements nomades aptes à traiter des informations sensibles.

L'usage nomade des équipements est encadré par une politique dédiée, qui précise les conditions d'accès aux ressources depuis l'extérieur. Seuls les équipements dûment autorisés peuvent être utilisés à cette fin.

De plus, les mémoires de masse des postes de travail et équipements mobiles permettant d'accéder à distance au système d'information de la CNAF sont protégés par des mécanismes de chiffrement et d'authentification.

[NIS2] Objectif de sécurité n°8, attendu (e).

EXP-ACC-DIST : Accès à distance au système d'information de l'organisme.

L'accès distant au système d'information de la branche Famille de la sécurité sociale repose sur une authentification forte, mise en œuvre via différents mécanismes (VPN avec authentification renforcée, tunnels sécurisés établis par le MDM, ou portail d'accès distant en SSL sécurisé).

Tout accès à distance ne faisant pas l'objet d'une telle authentification forte fait office d'exception et doit faire l'objet d'une dérogation spécifique ou d'un plan de traitement temporaire pour les cas techniques bloquants.

[NIS2] Objectif de sécurité n°8, attendus (a) à (d).

Sécurisation des imprimantes et copieurs multifonctions manipulant des informations sensibles

EXP-IMP-SENS : Impression des informations sensibles.

⁶ Security Operation Center (SOC) est une structure dédiée à la surveillance, l'analyse et à la réponse aux cybermenaces

Les impressions d'informations sensibles doivent être réalisées de manière à garantir la confidentialité des documents. La « Charte nationale de sécurité de l'utilisateur du système d'information » (LR 2017-069) de la Branche rappelle notamment aux utilisateurs la nécessité de ne pas laisser de documents confidentiels sans surveillance sur les périphériques d'impression.

EXP-IMP-2 : Sécurité des imprimantes et copieurs multifonctions.

Les imprimantes et copieurs multifonctions sont considérés comme des ressources informatiques à part entière. Leur usage est encadré par les bonnes pratiques de sécurité et leur exposition au réseau est limitée conformément aux principes de cloisonnement.

Objectif 24 : Exploitation sécurisée des centres informatiques

Exploiter de manière sécurisée les centres informatiques en s'appuyant sur des procédures adaptées et sur la maîtrise des outils de supervision.

Sécurité des ressources informatiques

EXP-CI-OS : Systèmes d'exploitation.

Les systèmes d'exploitation utilisés au sein de la Branche sont maintenus à jour et font l'objet d'un suivi afin de garantir leur support par l'éditeur. Un processus de gestion du parc de la CNAF permet de contrôler les versions déployées. Les postes sont configurés à partir d'un master standardisé limitant les services et applications installés, conformément au principe de réduction de la surface d'attaque. L'attribution des droits d'administration est elle encadrée par un processus défini, limitant ces droits aux seuls cas justifiés.

Seules les ressources logicielles nécessaires à la réalisation des activités et services de la Branche ou au maintien en conditions opérationnelle ou de sécurité sont installées et conservées sur le système d'information. Lorsque des raisons techniques ou opérationnelles ne permettent pas de désactiver ou désinstaller une ressource logicielle, la CNAF met en œuvre des mesures permettant de réduire le risque associé.

[NIS2] Objectif de sécurité n°18, attendus (a) et (b).

EXP-CI-LTP : Logiciels en Tiers Présentation.

Les logiciels déployés en tiers présentation font l'objet d'une configuration renforcée afin de limiter leur exposition aux attaques. Un dispositif de filtrage applicatif est en place, permettant de contrôler les requêtes entrantes et renforcer la protection des services accessibles depuis l'extérieur.

EXP-CI-LTA : Logiciels en Tiers Application.

Les règles de développement sécurisé, et les configurations des logiciels en Tiers Application doivent être appliquées. La « Politique appliquée de sécurité dans les développements » (IT 2024-101) encadre l'ensemble des bonnes pratiques de sécurité à appliquer pour sécuriser les applications de la branche Famille de la sécurité sociale.

EXP-CI-LTD : Logiciels en Tiers Données.

Les logiciels en tiers données font l'objet de mesures de sécurité renforcées (restrictions d'accès, interdictions de connexions, gestion des privilèges). Ces exigences sont documentées dans les dossiers d'architecture technique (DAT) produits dans le cadre des projets, permettant d'assurer la traçabilité et la justification des choix de sécurité.

EXP-CIPROTFIC : Passerelle d'échange de fichiers.

Les échanges de fichiers entre application s'effectuent via des protocoles sécurisés (SSL/TLS, VPN chiffré, interconnexions contrôlées), dans le respect des exigences de confidentialité et d'intégrité.

La plateforme nationale d'échanges partenaires sécurisés (PEPS) déployée au niveau national offre un cadre sécurisé pour la transmission de fichiers (IT 2024-065).

EXP-CI-FILT : Filtrage des flux applicatifs.

Une politique de segmentation du réseau est appliquée afin de limiter les surfaces d'attaque et de filtrer les flux entre zones de sécurité distinctes. Les règles de filtrage mises en place n'autorisent que les communications identifiées et documentées, et permettent par défaut de bloquer les autres.

Les configurations de filtrage et matrices de flux sont documentées dans les dossiers d'architecture technique (DAT) et peuvent être vérifiées via des extractions des équipements de filtrage réseau.

[NIS2] Objectif de sécurité n°7, 'Filtrage des communications' attendus (a), (b) et (c).

EXP-CI-ADMIN : Flux d'administration.

Les actions d'administration sont effectuées au moyen d'un réseau d'administration dédié.

Les flux d'administration sont différenciés selon leur périmètre : d'un côté les flux liés à l'infrastructure, de l'autre ceux liés à l'administration des applications.

La séparation appliquée des profils attribués est décrite dans la « Politique appliquée d'identification et d'authentification des accès internes au SI de la branche Famille de la sécurité sociale » (IT 2018-046) ainsi que dans la « Charte nationale de sécurité de l'utilisateur du SI » (LR 2017-069). Les droits sont ainsi attribués en fonction du rôle (administrateur système, gestionnaire d'application etc.), conformément aux schémas d'administration définis.

[NIS2] Objectif de sécurité n°19, attendus (a) et (h).

EXP-CI-EFFAC : Effacement de support.

Le reconditionnement et la réutilisation des disques durs pour un autre usage (ex : réattribution d'une machine/serveur) ne sont autorisés qu'après une opération d'effacement sécurisé des données.

EXP-CI-DESTR : Destruction de support.

La fin de vie d'un support ou d'un matériel embarquant un support de stockage s'accompagne d'une opération de destruction avant remise au rebut, conformément au processus de mise au rebut de la Branche.

De surcroît, le « Plan d'Assurance Sécurité » (IT XXXX) contractualisé avec les prestataires rappelle les exigences relatives à la fourniture, par les prestataires, des rapports de destruction sécurisée de toutes les données de la CNAF présentes sur des supports.

EXP-CI-TRAC : Traçabilité / imputabilité.

Afin d'assurer une cohérence dans les échanges entre applications ainsi qu'une traçabilité pertinente des événements techniques et de sécurité, les centres d'exploitation de la Branche emploient une référence de temps commune : NTP (Network Time Protocol).

EXP-CI-SUPERVIS : Supervision.

Un cloisonnement entre les flux de supervision (remontée d'informations) et les flux d'administration (commandes, mises à jour) doit être mis en place.

EXP-CI-AMOV : Accès aux périphériques amovibles.

L'accès aux supports informatiques amovibles fait l'objet d'un traitement adapté, plus particulièrement lorsqu'ils ont été utilisés pour mémoriser de l'information sensible ou lorsqu'ils sont utilisés pour des opérations d'exploitation.

EXP-CI-ACCRES : Accès aux réseaux.

Dans les centres informatiques (Datacenter), les accès aux réseaux sont encadrés par des procédures de sécurité. Les accès physiques aux équipements sont restreints aux personnels habilités et font l'objet d'un contrôle rigoureux. L'attribution des adresses IP est formalisée et tracée afin d'assurer la maîtrise des connexions et prévenir toute connexion non autorisée, ainsi que la vérification de la conformité des équipements avant toute connexion.

EXP-CI-AUDIT : Audit/contrôle.

Le RSSI de la Branche pilote des audits réguliers du système d'information relevant de sa responsabilité.

5.8 Sécurité du poste de travail

Objectif 25 : Sécurisation des postes de travail

Durcir les configurations des postes de travail en protégeant les utilisateurs.

Mise à disposition du poste

PDT-GEST : Fourniture et gestion des postes de travail.

Les postes de travail utilisés à des fins professionnelles sont fournis et administrés par l'équipe locale en charge des systèmes d'information. Tout équipement non géré ne peut être connecté au réseau qu'après demande d'autorisation expresse du RSSI. Conformément à la « Charte nationale de sécurité de l'utilisateur du SI » (LR 2017-069), seuls les « équipements conformes à l'architecture technique nationale sont autorisés à se connecter au SI de la branche Famille de la sécurité sociale, tout dérogation nécessite une autorisation écrite préalable ».

PDT-CONFIG : Formalisation de la configuration des postes de travail.

La configuration des postes de travail repose sur des règles techniques définies au niveau national. Ces règles assurent un niveau homogène de sécurité et de conformité au sein de la Branche, et leur application garantit le durcissement des postes et la maîtrise des environnements.

Sécurité physique des postes de travail**PDT-VEROUIL : Verrouillage des postes.**

Un câble physique de sécurité est fourni avec chaque poste portable. Les utilisateurs sont sensibilisés à son utilisation dès leur arrivée au sein de la Branche.

Lorsque l'unité centrale d'un poste fixe est peu volumineuse, donc susceptible d'être facilement emportée, elle doit être protégée contre le vol par un système d'attache (par exemple un câble antivol).

Gestion des privilèges sur les postes de travail**PDT-PRIVIL : Privilèges des utilisateurs sur les postes de travail.**

La gestion des privilèges des utilisateurs sur leurs postes de travail suit le principe du « moindre privilège » : chaque utilisateur ne dispose que des privilèges nécessaires à la conduite des actions relevant de sa mission. Ce principe fait l'objet de rappels réguliers adressés aux responsables SSI par voie de communication interne, afin d'en assurer la bonne application.

PDT-PRIV : Utilisation des privilèges d'accès « administrateur ».

Les privilèges d'accès « administrateur » sont utilisés uniquement pour les actions d'administration le nécessitant. Les règles d'utilisation des profils sont rappelées dans la « Politique appliquée d'identification et d'authentification des accès internes au SI de la branche Famille de la sécurité sociale » (IT 2018-046).

PDT-ADM-LOCAL : Privilèges des utilisateurs sur les postes de travail.

L'accès au compte « administrateur local » sur les postes de travail est strictement limité aux équipes en charge de l'exploitation et du support sur ces postes de travail.

L'attribution de droits d'administration locaux est encadrée et limitée par un dispositif de gestion spécifique.

Protection des informations**PDT-STOCK : Stockage des informations.**

Dans la mesure du possible, les données traitées par les utilisateurs sont stockées sur des espaces réseau, eux-mêmes sauvegardés selon les systèmes de sauvegarde de la Branche.

PDT-SAUV-LOC : Sauvegarde / synchronisation des données locales.

Dans le cas où des données doivent être stockées en local sur le poste de travail, des moyens de synchronisation ou de sauvegarde sont fournis aux utilisateurs.

PDT-PART-FIC : Partage de fichiers.

Le partage de répertoires ou de données hébergées localement sur les postes de travail est à proscrire.

PDT-CHIFF-SENS : Chiffrement des données sensibles.

La politique relative à la « Protection des informations sensibles grâce au chiffrement » (IT 2017-099) explicite le cadre et les principes de mise en œuvre du chiffrement des données sensibles.

Tout besoin de déploiement d'un outil de chiffrement spécifique peut être identifié en s'appuyant sur l'expertise de la MACSSI ou des Relais informatiques et Libertés (RIL). Il convient ensuite de s'adresser à la DCISN ou aux MSSI chargés d'évaluer et de déterminer la solution de chiffrement la plus adaptée au besoin.

PDT-AMOV : Fourniture de supports de stockage amovibles.

Lorsque nécessaire, les supports de stockage amovibles (clés USB et disque durs externes, notamment) sont fournis aux utilisateurs par l'équipe locale chargée des systèmes d'information. La « Charte nationale de sécurité de l'utilisateur du SI » (LR 2017-069) rappelle néanmoins les exigences de sécurité relatives à cet usage. En effet, l'utilisateur doit veiller à ce qu'aucune information présentant un caractère confidentiel ou contenant des données à caractère personnel ne puisse transiter sans protection sur ce support.

Nomadisme

PDT-NOMAD-ACCES : Accès à distance aux Systèmes d'Information de l'entité.

L'accès distant au système d'information de la branche Famille de la sécurité sociale repose sur une authentification multi facteurs, mise en œuvre via différents mécanismes (Windows Hello, VPN avec authentification renforcée, tunnels sécurisés établis par le MDM, ou portail d'accès distant en SSL sécurisé).

[NIS2] Objectif de sécurité n°8, attendus (a) à (d).

PDT-NOMAD-PAREFEU : Pare-feu local.

Les accès à distance sont protégés par un dispositif de pare-feu assurant un filtrage strict des connexions entrantes et sortantes.

PDT-NOMAD-STOCK : Stockage local d'information sur les postes nomades.

Le stockage local d'information sur les postes de travail nomades doit être limité au strict nécessaire. Les mémoires de masse des postes de travail et équipements mobiles permettant d'accéder à distance au système d'information de la CNAF sont protégés par des mécanismes de chiffrement et d'authentification.

[NIS2] Objectif de sécurité n°8, attendu (e).

PDT-NOMAD-FILT : Filtre de confidentialité.

Pour les postes de travail nomades manipulant des données sensibles, un filtre de confidentialité est fourni par la CNAF et doit être positionné sur l'écran dès lors que le poste est utilisé en dehors des sites de la Branche.

Objectif 26 : Sécurisation des imprimantes et copieurs multifonctions

Paramétrer les imprimantes et copieurs multifonctions afin de diminuer leur surface d'attaque.

PDT-MUL-DURCISS : Durcissement des imprimantes et copieurs multifonctions.

Les imprimantes et copieurs multifonctions hébergés localement dans un organisme font l'objet d'un durcissement en termes de sécurité : changement des mots de passe initialement fixés par le « constructeur », désactivation des interfaces réseau inutiles, suppression des services inutiles, chiffrement des données sur le disque dur lorsque cette fonctionnalité est disponible, configuration réseau statique.

Objectif 27 : Sécurisation de la téléphonie

Sécuriser la téléphonie pour protéger les utilisateurs contre des attaques malveillantes.

Les recommandations de l'objectif 27 de la PSSI MCAS ne s'appliquent pas à la Branche dans la mesure où les téléphones fixes sont en cours de suppression. Néanmoins, les utilisateurs sont invités à adopter des pratiques de sécurité conformes aux recommandations en vigueur, notamment en veillant à la confidentialité de leurs communications, à la protection de leurs terminaux et au changement régulier des codes d'accès ou mots de passe associés aux services vocaux ou applicatifs.

Objectif 28 : Contrôles de conformité

Contrôler régulièrement la conformité des paramétrages de sécurité appliqués aux postes de travail.

PDT-CONF-VERIF : Utiliser des outils de vérification automatique de la conformité.

La conformité des configurations des postes de travail est vérifiée de manière régulière. Ces mécanismes de contrôle permettent de détecter les écarts par rapport aux règles de sécurité définies, de prévenir les dérives dans le temps et de garantir un niveau homogène de protection du parc informatique.

5.9 Sécurité du développement des systèmes

Objectif 29 : Développement des systèmes

Reconnaître la sécurité comme une fonction essentielle, et la prendre en compte dès la conception des projets.

PDT-INTEGR-SECLOC : Intégrer la sécurité dans les développements locaux.

Toute initiative de développement informatique, qu'elle soit nationale ou locale, doit respecter les exigences de sécurité concernant la prise en compte des mesures de sécurité dans les projets et les développements. Cette prérogative est appliquée au sein de la Branche au travers de la « Politique appliquée de sécurité dans les développements » (IT 2024-101) qui renseigne sur les mesures et outils utilisables (ex : outils d'analyse statique de code) pour parvenir à identifier et couvrir les risques liés aux développements.

De surcroît, le service à l'origine du projet se porte garant de réaliser une démarche d'homologation du système menant à une commission d'homologation permettant à l'Autorité d'Homologation de se prononcer. Cette procédure, intégrant l'ensemble des tests de sécurité pertinents, est décrite et encadrée au sein de la Branche à travers le « Guide d'homologation de sécurité des systèmes d'information » (IT 2025-132).

DEV-SOUS-TRAIT : Intégrer des clauses SSI dans les contrats de sous-traitance de développement informatique.

Lors de l'écriture d'un contrat de sous-traitance de développement, des clauses spécifiques relatives à la sécurité des systèmes d'information sont systématiquement intégrées via le « **Plan d'assurance sécurité (PAS)** ». Ces clauses couvrent notamment les exigences suivantes :

- Séparation des environnements : les environnements de développement sont strictement isolés des environnements de tests et de production, afin de limiter les risques d'accès non autorisé
- Protection des données personnelles : l'usage de données à caractère personnel dans les environnements de développement est interdit
- Développement sécurisé : les équipes de développement sont régulièrement sensibilisés aux bonnes pratiques à respecter (référentiel OWASP notamment) tout au long du cycle de développement.
- Contrôle des changements : toute modification apportée au système dans le cadre du développement est soumise à des procédure de gestion des changements, assurant la traçabilité et la validation des évolutions
- Tests de sécurité : des tests spécifiques des mécanismes de sécurité sont réalisés au cours du développement, afin de vérifier l'efficacité des mesures mises en œuvre et d'identifier d'éventuelles vulnérabilités.

Objectif 30 : Développements logiciels et sécurité

Mener les développements logiciels selon une méthodologie de sécurisation du code produit.

DEV-FUITES : Limiter les fuites d'information.

Les fuites d'informations techniques sur les logiciels utilisés permettent aux attaquants de déceler plus facilement d'éventuelles vulnérabilités. Il est donc impératif de limiter fortement la diffusion d'informations au sujet des produits utilisés au sein de la Branche, même si cette précaution ne constitue pas une protection en tant que telle.

DEV-LOG-ADHER : Réduire l'adhérence des applications à des produits ou technologies spécifiques.

Lors des phases de conception et de spécification technique, une attention particulière est portée à limiter l'adhérence des applications à des environnements logiciels ou matériels spécifiques. Cette approche vise à garantir la pérennité et la sécurité des applications, en réduisant leur dépendance à des composants susceptibles de devenir obsolètes, vulnérables ou non maintenus.

Dans cette perspective, la Branche développe activement l'usage de la conteneurisation, qui permet d'isoler les applications de leur environnement d'exécution, de faciliter leur portabilité et de renforcer le maintien en condition de sécurité (MCS).

DEV-LOG-CRIT : Instaurer des critères de développement sécurisé.

Comme décrit par la « Politique appliquée de sécurité dans les développements » (IT 2024-101), les critères de sécurité sont intégrés dès les phases de développement applicatif. Ces critères s'appuient notamment sur les bonnes pratiques issues de référentiels tels que l'OWASP pour garantir un niveau de sécurité homogène dans les développements réalisés, même une fois passées les phases de définition et de conception. Afin de renforcer la détection précoce des vulnérabilités, les développements font notamment l'objet d'analyses à l'aide d'outils de contrôle de code source. Les rapports sont ensuite exploités pour corriger les écarts identifiés et améliorer la qualité de code sur le plan sécuritaire.

DEV-LOG-CYCLE : Intégrer la sécurité dans le cycle de vie logiciel.

La sécurité est intégrée à toutes les étapes du cycle de vie d'un projet au sein de la branche Famille de la sécurité sociale, depuis l'expression des besoins jusqu'à la maintenance applicative, en passant par la rédaction du cahier des charges et les phases de recette.

DEV-LOG-WEB : Améliorer la prise en compte de la sécurité dans les développements Web.

Les développements Web sont encadrés par les règles de sécurité décrites dans la « Politique appliquée de sécurité dans les développements » (IT 2024-101). Ces règles sont issues de référentiels reconnus, tels que les guides de l'OWASP.

De surcroît, les exigences réglementaires relatives au RGPD et à la loi informatique et Libertés sont rappelées dans l'instruction technique « Conformité des sites Web portant les couleurs de la Branche au regard du RGPD et de la loi Informatique et Libertés » (IT 2022-056). Cette instruction encadre la création de tout site Web dont la branche Famille de la sécurité sociale porte la responsabilité juridique (développement interne ou externe, hébergement interne ou externe).

DEV-LOG-AUTH : Authentification des utilisateurs.

Il est strictement interdit de développer des annuaires locaux aux applications, l'authentification des utilisateurs est portée par les mécanismes d'annuaires mis en œuvre par la DSI, les projets doivent utiliser ces mécanismes.

Objectif 31 : Applications à risques

Accompagner le développement sécurisé d'applications à risques par des contre-mesures minimisant l'impact d'attaques nouvelles.

DEV-FILT-APPL : Mettre en œuvre des fonctionnalités de filtrage applicatif pour les applications à risque.

Les applications exposées à des risques élevés font l'objet de mesures de protection renforcées. Un dispositif de filtrage applicatif dédié est déployé au niveau de l'infrastructure de la Branche pour intercepter et analyser les flux. L'objectif étant de pouvoir détecter et bloquer les tentatives d'exploitation de vulnérabilités ou des comportements anormaux.

5.10 Traitement des incidents

Objectif 32 : Chaînes opérationnelles

Partager l'information (alertes, incidents) dans le respect des règles de prudence et mutualiser les opérations de remise en état, de façon à lutter efficacement contre les attaques.

TI-OPSS-SSI : Chaînes opérationnelles SSI.

Les alertes et incidents de sécurité sont traités selon des procédures établies, documentées et partagées entre les différentes parties prenantes.

- Les alertes diffusées par les instances nationales, telles que le CERT FR⁷, sont réceptionnées et qualifiées par le CSIRT⁸ de la CNAF (au sein de la DCISN), avant d'être transmises aux équipes techniques concernées pour mise en œuvre des mesures correctives.
- Les événements de sécurité détectés sont analysés en première instance par le SOC⁹, qui évalue leur impact et les risques associés. Lorsqu'un événement est qualifié d'incident, une cellule de réponse à incident est activée. Celle-ci mobilise notamment la MACSSI, en particulier lorsque l'incident est susceptible d'impliquer une violation de données à caractère personnel.
- Si un incident présente un impact majeur ou une gravité particulière, il peut être requalifié en crise. Comme définit et encadré par le plan de gestion de crise, une cellule de crise est alors constituée pour inclure l'ensemble de la chaîne fonctionnelle SSI.

Des exercices sont organisés pour tester les procédures en place. Une gouvernance dédiée assure le pilotage des échanges entre parties prenantes et veille à la capitalisation des retours d'expérience et des enseignements associés, ainsi que leur intégration le cas échéant au plan de continuité et de reprise d'activité de la Branche.
[NIS2] Objectif de sécurité n°12, attendus (a) à (d).

MC-TI-GES-CRISE : Mesure complémentaire à la PSSI MCAS – Gestion de crise

La Branche Famille de la sécurité sociale dispose d'un dispositif formalisé de gestion de crise, mis à jour régulièrement et activable dès lors qu'un incident de sécurité significatif est identifié. Ce dispositif repose sur une gouvernance identifiée, avec des procédures de réponse claires et un annuaire de contacts internes et externes mobilisables. Les critères d'activation et de désactivation du dispositif de gestion de crise sont définis, ainsi que les procédures d'isolement et de restauration des services, en lien avec les plans de continuité et de reprise d'activité.

Une stratégie de communication en situation de crise est également prévue.

Dans une logique d'amélioration continue, des retours d'expérience (RETEX) sont réalisés à la suite d'un exercice ou d'une crise réelle, afin d'identifier les mesures correctives à mettre en œuvre.

La plateforme de pilotage stratégique (PiPAC) assure la disponibilité des moyens de communication de secours en temps de crise.

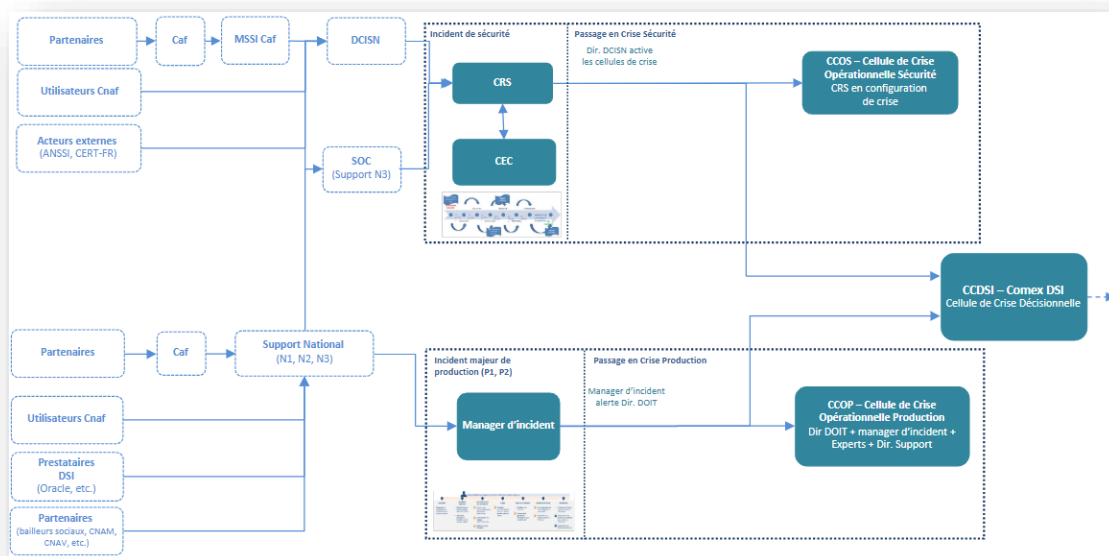
Par ailleurs, une stratégie d'entraînement est définie afin de tester régulièrement les dispositifs mis en place.

Schéma d'alerte et escalade en crise

⁷ Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (ANSSI)

⁸ Computer Security Incident Response Team (CSIRT) est une unité spécialisée dans la gestion et la réponse aux incidents de cybersécurité

⁹ Security Operation Center (SOC) est une structure dédiée à la surveillance, l'analyse et à la réponse aux cybermenaces



[NIS2] Objectif de sécurité n°14, attendus (a) à (i). Objectif de sécurité n°15, attendus (a) à (d).

Traitement des alertes de sécurité émises par les instances nationales (FSSI / ANSSI)

TI-MOB : Mobilisation en cas d'alerte.

En cas d'alerte de sécurité au niveau national, la chaîne SSI de la Branche se mobilise sous le pilotage du RSSI afin de veiller à la bonne application des exigences formulées par les instances nationales, dans les meilleurs délais.

Remontée des incidents de sécurité rencontrés

TI-QUAL-TRAIT : Qualification et traitement des incidents.

La chaîne fonctionnelle SSI de la Branche est informée par la chaîne opérationnelle de tout incident de sécurité, et contribue si nécessaire à la qualification de l'incident et au pilotage de son traitement.

Après chaque incident majeur, une analyse des causes de l'incident est réalisée afin d'identifier les mesures de sécurité permettant de limiter la vraisemblance d'un nouvel incident ou d'en réduire l'impact.

[NIS2] Objectif de sécurité n°12, attendu (e).

TI-INC-REM : Remontée des incidents.

Les incidents identifiés comme ayant un impact potentiel dépassant le périmètre de la CNAF font l'objet d'une remontée au CERT FR¹⁰, au CERT SOCIAL¹¹ et au FSSI, le cas échéant. Les incidents sont recensés et documentés.

5.11 Continuité d'activité

Objectif 33 : Gestion de la continuité d'activité des SI

Se doter de plans de continuité d'activité, et les tester.

¹⁰ Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (ANSSI)

¹¹ Organisation interbranche qui coordonne les caisses nationales de la Sécurité Sociale avec pour mission d'éviter ou de limiter les conséquences des cyberattaques pour les organismes publics du secteur santé et social

Définition du plan de continuité d'activité des systèmes d'information de la CNAF

PCA-LOCAL : Définition du plan national de continuité d'activité des systèmes d'information.

Le RSSI de la CNAF définit et met en œuvre un plan de continuité d'activité (PCA) (incluant un plan de reprise d'activité (PRA)) des systèmes d'informations.

Pour chaque activité et service, la Branche définit et documente la durée maximale d'interruption admissible (DMIA) et la perte de données maximale admissible (PDMA). A partir du bilan d'impact sur l'activité (BIA), le PCA est ensuite décliné pour prendre en compte les scénarios de crise d'origine cyber en cohérence avec la durée maximale d'interruption admissible et la perte de données maximale admissible.

L'identification de ces mesures de continuité s'appuie notamment :

- Sur la cartographie de l'écosystème ;
- Sur la procédure de gestion des incidents pour détecter et réagir au plus tôt aux incidents ;
- Sur la procédure de gestion des crises d'origine cyber pour permettre la reprise au plus tôt des services.

[NIS2] Objectif de sécurité n°13, attendus (e) à (g).

Mise en œuvre du plan de continuité d'activité des systèmes d'information

PCA-SUIVILOCAL : Suivi de la mise en œuvre du plan de continuité d'activité des Système d'Information (PCA des SI).

Le RSSI de la CNAF s'assure de la bonne mise en œuvre des dispositions prévues dans le plan de continuité d'activité des systèmes d'information.

PCA-PROC : Mise en œuvre des dispositifs techniques et des procédures opérationnelles.

Les équipes informatiques mettent en œuvre les dispositifs techniques et les procédures opérationnelles contribuant à la continuité des SI, en assurent la supervision au quotidien et la maintenance dans le temps.

PCA-SAUVE : Protection de la disponibilité des sauvegardes.

Au travers du plan de sauvegarde de l'activité (PSA), la CNAF définit et met en œuvre les procédures de sauvegarde et de restauration de ses systèmes d'informations et de ses données. Les mécanismes de sauvegarde sont dimensionnés pour répondre aux besoins de disponibilité associés aux différents services et aux différentes activités fournis par l'entité. Les processus de sauvegarde sont testés régulièrement.

Les sauvegardes de données ne sont pas soumises aux mêmes risques de sinistres que les données sauvegardées, elles sont protégées d'un incident les rendant inexploitable.

[NIS2] Objectif de sécurité n°13, attendus (a) à (d).

PCA-PROT : Protection de la confidentialité des sauvegardes.

Les sauvegardes sont traitées de manière à garantir leur confidentialité et leur intégrité.

Les sauvegardes sont redondées sur différents médias et différents sites. La confidentialité des sauvegardes est assurée par une gestion maîtrisée des habilitations et un chiffrement. Leur intégrité est assurée par les fonctions d'immuabilité utilisées.

Maintien en conditions opérationnelles du plan de continuité d'activité des Systèmes d'Information

PCA-EXERC : Exercice régulier du plan local de continuité d'activité des systèmes d'information.

Le RSSI organise des exercices réguliers, afin de tester le plan de continuité d'activité des systèmes d'information.

PCA-MISAJOUR : Mise à jour du plan local de continuité d'activité des systèmes d'information.

Le RSSI assure le maintien à jour du plan de continuité d'activité des Systèmes d'Information.

5.12 Conformité, audit, inspection, contrôle

Objectif 34 : Contrôles réguliers

Effectuer des contrôles (audits, inspections) et des exercices réguliers de façon à mesurer les progrès accomplis et corriger les manquements.

CONTR-SSI : Contrôles locaux.

La conformité à la PSSI ministérielle (PSSI MCAS) et à la PSSI de la Branche est vérifiée par des contrôles réguliers, dans le cadre du contrôle interne. Le RSSI conduit des actions locales d'évaluation de la conformité à la PSSI et contribue à la consolidation, dans un bilan annuel, de l'état d'avancement de sa mise en œuvre.

CONTR-BILAN-SSI : Bilan annuel.

La CNAF établit un bilan annuel mesurant sa maturité SSI globale.

6. OBJECTIFS ET REGLES COMPLEMENTAIRES

Afin de garantir l'actualisation continue du dispositif de sécurité au regard de l'évolution des technologies et des usages numériques, la présente PSSI intègre des recommandations complémentaires aux objectifs de sécurité de la PSSI MCAS. Ces recommandations sont amenées à être enrichies au regard de l'évolution des technologies et du niveau de menace.

6.1 Sécurité des annuaires

Les annuaires constituent une brique critique de l'infrastructure du système d'information de la CNAF : ils assurent l'identification, l'authentification et la gestion des droits d'accès pour l'ensemble des utilisateurs et des ressources. A ce titre, leur sécurité conditionne directement celle du système d'information dans son ensemble. Afin de garantir l'intégrité, la confidentialité et la disponibilité des annuaires, la Branche met en œuvre des mesures de sécurité renforcées, en particulier sur les composants répertoriés comme « cœur de confiance ». La CNAF s'appuie notamment sur les recommandations publiées par l'ANSSI relatives à l'administration sécurisée (Tier0 pour Active Directory).

MC-ANN-SSI : Application des correctifs de sécurité

Les correctifs de sécurité fournis par les éditeurs des annuaires ou des composants associés sont appliqués sans délai. Une veille est réalisée sur les vulnérabilités touchant les services d'annuaire afin d'en assurer un traitement rapide.

MC-ANN-ADM : Administration dédiée et cloisonnée

L'administration des ressources du cœur de confiance est réalisée exclusivement par des comptes d'administration dédiés (distincts des comptes bureautiques), depuis des ressources dédiées. Les connexions vers le cœur de confiance font l'objet d'un filtrage strict.

MC-ANN-REV : Revue régulière de la configuration

Une revue régulière de la configuration des annuaires est effectuée pour identifier les comptes ou éléments non conformes, obsolètes ou inutiles. Cette revue s'appuie autant que possible sur des outils automatisés pour fiabiliser l'analyse.

[NIS2] Objectif de sécurité n°11, 'Sécurité des annuaires', attendus (a) à (g).

6.2 Usages de l'intelligence artificielle

L'usage d'outils ou de services reposant sur des techniques d'intelligence artificielle, qu'ils soient développés en interne de la Branche ou utilisés via des fournisseurs externes, est encadré afin d'en maîtriser les risques de sécurité, d'éthique et de conformité. Les objectifs de sécurité listés ci-dessous sont complétés par des politiques appliquées spécifiques ; à l'instar de l'instruction technique « Cadre d'utilisation de l'IA à destination

des développeurs » (IT 2024-208) et « Présentation de la politique de Branche en matière d'intelligence artificielle générative » (IT 2025-148).

MC-IA-1 : Intégration de la sécurité dès la conception

Comme pour tout projet de la Branche, la sécurité est intégrée dans toutes les phases du cycle de vie des systèmes d'IA, depuis la conception jusqu'à l'exploitation. Une analyse de risques est menée avant toute phase, en tenant compte des risques spécifiques liés à l'IA (données, modèles, flux, usages).

MC-IA-2 : Maîtrise de la chaîne logicielle et des dépendances

Les bibliothèques, modules externes et frameworks utilisés dans les systèmes d'IA sont soumis à une évaluation rigoureuse de leur niveau de confiance. Le recours aux principes de type DevSecOps est requis pour garantir la sécurité des environnements.

Les phases du système (entraînement, test, production) sont cloisonnées dans environnements distincts.

Le déploiement des systèmes d'IA en production fait l'objet d'une sécurisation de la chaîne de livraison, de tests métiers et de d'audits de sécurité.

MC-IA-3 : Sécurité des données et confidentialité

Les données utilisées pour l'entraînement sont protégées en intégrité et ne proviennent que de sources légitimes et maîtrisées. Les systèmes d'IA intègrent, à l'instar des autres projets de la Branche, les principes de minimisation de données, de confidentialité dès la conception et de limitation des accès selon le besoin d'en connaître.

Les enjeux de confidentialité des données sont pris en compte dès la conception du système d'IA, au travers notamment d'une cartographie détaillée de l'ensemble des jeux de données utilisés à chaque phase du système.

MC-IA-4 : Hébergement de confiance

A l'instar de l'ensemble des projets de la branche Famille de la sécurité sociale, les systèmes d'IA sont hébergés dans des environnements sécurisés et adaptés au niveau de sensibilité des traitements. Dans le cas d'un déploiement dans un Cloud, les solutions d'hébergement de données en France ou dans l'Union Européenne sont privilégiées. La « Politique appliquée à la sécurité des SI hébergés dans le Cloud » (IT 2025-026) s'applique dans ce cadre.

MC-IA-5 : Suivi, journalisation et traçabilité

Les systèmes d'IA disposent nécessairement de mécanismes de journalisation détaillés couvrant l'ensemble des traitements réalisés, les requêtes et les interactions avec d'autres applicatifs métiers.

MC-IA-6 : Sensibilisation et gouvernance

Les agents de la Branche concernés, sont sensibilisés aux risques spécifiques liés aux IA. La DCISN et le RSSI accompagnent les projets d'IA pour s'assurer de la prise en compte des exigences de sécurité nécessaires.

7. CORPUS DOCUMENTAIRE SECURITE

Thème	Titre du document	Référence	Description
Gouvernance	Politique Générale de Sécurité des Systèmes d'Information (PGSSI) de la branche Famille de la sécurité sociale	A référencer	La Politique Générale de Sécurité des Systèmes d'information (PGSSI) de la branche Famille de la sécurité sociale définit le cadre stratégique, organisationnel et réglementaire du processus support qu'est la sécurité de l'information au sein de l'organisme.
	Charte nationale de sécurité de l'utilisateur du système d'information et de la charte nationale de sécurité de l'administrateur du système d'information	LR 2017-069	Cette lettre réseau diffuse à l'ensemble de la Branche les deux chartes informatiques en vigueur. Ces chartes fixent les règles nationales de sécurité du SI dans le respect des réglementations en vigueur et s'appliquent à tous les organismes du réseau de la branche Famille de la sécurité sociale.
	Plan de sauvegarde de l'activité (PSA)	-	Le plan de sauvegarde de l'activité précise les conditions organisationnelles et techniques mises en place dans le respect de l'application de la politique nationale de sauvegarde. Il vise, en cas de problème, à garantir à la branche Famille de la sécurité sociale, que l'information est présente et récupérable dans une structure de stockage pour pouvoir reprendre l'activité sur le lieu de travail ou sur un autre site.
	Politique nationale de sauvegarde (PNS) des données	LR 2018-003	Cette lettre réseau formalise la politique de sauvegarde de l'information gérée par la Branche. Elle pose les principes relatifs à la sauvegarde des données, au rôle de chacun des acteurs dont les missions du Service National de Sauvegarde (SNS). Elle fixe également les délais de rétention des données par domaine d'application.
	Politique nationale d'archivage (PNA)	LR 2018-002	Cette lettre réseau vise à formaliser la politique d'archivage de l'information gérée par la Branche. Elle pose les principes relatifs à l'archivage des données et au rôle de chacun des acteurs.
	Le secret professionnel et les règles de communication de données lors des contacts avec les allocataires	LR 2024-257	Cette lettre réseau rappelle les exigences relatives au respect du secret professionnel par les agents de la CNAF et les règles de communication de données lors des contacts avec des parties externes.
	Doctrine d'application de la directive NIS	IT 2022-110	Cette doctrine d'application de la Directive Network Information and Security (NIS) définit le cadre réglementaire, stratégique, organisationnel et technique permettant de mettre en conformité la branche Famille de la sécurité sociale vis à vis de la directive NIS, à la suite de la désignation de la CNAF en tant qu'Opérateur de Services Essentiels (OSE).
	Guide d'homologation de sécurité des systèmes d'information	IT 2025-132	Le Guide d'homologation de sécurité formalise la démarche d'évaluation, de décision et de suivi permettant d'autoriser la mise en service d'un système d'information en maîtrisant ses risques.
	Plan d'Assurance de Sécurité (PAS) de l'information	A référencer	Le Plan d'Assurance de Sécurité (PAS) de l'information est un document rassemblant tous les contrôles de sécurité et des services de sécurité acceptés et

			contractés afin de garantir les conditions de sécurité exigées dans les prestations commanditées par la CNAF.
	Présentation de la politique de Branche en matière d'intelligence artificielle générative	IT 2025-148	Cette IT présente le cadre général de la branche Famille en matière d'IA : doctrine de Branche, charte éthique, cadrage des bonnes pratiques et orientations technologiques prises pour la Branche.
Accès au système d'information	Politique appliquée d'identification et d'authentification des accès internes au SI de la branche Famille de la sécurité sociale	IT 2018-046	Cette instruction fixe les règles d'identification et d'authentification pour les comptes individuels, nominatifs et non partagés des utilisateurs internes et des Administrateurs du SI CNAF.
Exploitation et architecture	Installation d'un Wi-Fi visiteurs dans les espaces d'accueil des CAF	IT 2019-204	Cette instruction vise à cadrer le déploiement du Wi-Fi gratuit dans les espaces d'accueil destinés aux visiteurs.
	Procédure décrivant le processus de gestion du vol ou de la perte de matériel nomade	IT 2024-157	Cette instruction définit une procédure normalisée de signalement des pertes et vols de matériels à l'ensemble du réseau. Ce processus simplifie la prise en charge des incidents depuis la déclaration de perte ou de vol jusqu'à la remise du nouveau matériel à l'agent.
	Politique appliquée de prise de main à distance	IT 2024-200	Cette instruction identifie les bonnes pratiques de sécurité à appliquer pour intervenir, à distance, sur les ordinateurs connectés au SI CNAF (stations et serveurs).
	Sécurisation des accès au poste de travail	IT 2024-217	Cette instruction technique définit la stratégie d'accès au poste de travail et la mise en œuvre notamment de l'authentification multi-facteurs (MFA).
	Politique Appliquée à la Sécurité des Systèmes d'information hébergés dans le Cloud	IT 2025-026	Ce document a pour objectif de sécuriser les services numériques de la branche Famille de la sécurité sociale externalisés dans le cloud, en respectant le cadre réglementaire, normatif et légal et d'identifier les exigences de sécurité applicables.
Sécurité des développements	Conformité des sites Web au regard du RGPD et de la loi informatique et Libertés	IT 2022-056	Cette instruction a pour objectif d'aider les organismes de la Branche à mettre en conformité leurs sites web et à intégrer le plus en amont possible les exigences réglementaires dans le cadre de projets (y compris au sein des expressions de besoins et les appels d'offres).
	Politique appliquée de sécurité dans les développements	IT 2024-101	Cette instruction permet de définir les bonnes pratiques de sécurité à appliquer dans les développements. Elle a pour objectif de sécuriser les applications de la Branche en luttant contre les attaquants qui utilisent différents chemins à travers une application, pour porter atteinte au SI de la CNAF.
	Cadre d'utilisation de l'IA à destination des développeurs	IT 2024-208	Ce document décrit le cadre d'utilisation des solutions d'Intelligence Artificielle générative à appliquer dans les développements de la branche Famille de la sécurité sociale.
Protection des données	Utilisation des outils numériques gratuits – Quelques règles de prudence	IT 2018-031	Cette instruction a pour objectif de caractériser les risques de non-conformité à la loi Informatique et Libertés du 6 janvier 1978 modifiée qu'encourt la Branche en utilisant certains d'entre eux et d'évoquer, chaque fois que possible, l'existence de solutions alternatives plus respectueuses de la protection des données personnelles, ceci dans l'attente de la mise en œuvre de solutions internes nationales répondant aux différents besoins.
	Marchés et RGPD : sécurisation juridique des situations de sous-	IT 2020-027	Cette instruction a pour objectifs de mieux définir les cas de sous-traitance et d'en donner des exemples concrets au sein de la Branche, de permettre aux organismes

	traitance qui concernent des données personnelles		concernés de « sécuriser » juridiquement la sous-traitance si elle porte sur des données personnelles et de mettre à disposition un modèle de clauses de sous-traitance RGPD, à adapter au regard de la nature de la prestation et des données personnelles traitées.
	RGPD appliqué au travail collaboratif avec Microsoft 365 au sein de la branche Famille de la sécurité sociale	LR 2024-097	Cette lettre réseau a pour objet de présenter les principes applicables au sein de la branche Famille de la sécurité sociale pour garantir le respect du RGPD dans les usages des outils collaboratifs de l'environnement de travail Microsoft 365.
	Protection des informations sensibles grâce au chiffrement	IT 2017-099	Cette information technique vise à vulgariser le chiffrement et fournir les instructions nécessaires pour les cas d'usage les plus fréquents dans lesquels le chiffrement doit être mis en œuvre.
	Déploiement de la plateforme PEPS	IT 2024-065	Cette instruction porte sur le déploiement de la plateforme d'échanges partenaires sécurisée (PEPS) à destination de l'ensemble du réseau.