

Politique de Sécurité des Systèmes d'Information



- ☒ public
- ☐ interne
- ☐ diffusion restreinte
- ☐ confidentiel

REVISIONS DU DOCUMENT

Date	Objet
Juin 2017	Version initiale

Table des matières

1. OBJET DU DOCUMENT	4
2. CHAMP D'APPLICATION	4
2.1 PERIMETRE D'APPLICATION	4
2.2 GESTION DES EVOLUTIONS	4
3. ENJEUX ET OBJECTIFS DE LA SECURITE DES SYSTEMES D'INFORMATION	4
3.1 ENJEUX	4
3.2 DES ENJEUX DE CONTINUITE DE SERVICE DES ACTIVITES DE L'ÉTAT	5
3.3 DES ENJEUX D'IMAGE LIES A UNE DEFAILLANCE DANS LE SERVICE AUX CITOYENS	5
3.4 DES ENJEUX D'ORGANISATION INTERNE	5
3.5 OBJECTIFS OPERATIONNELS EN MATIERE DE SSI	5
3.6 MESURES PARTICULIERES POUR LE MINISTERE CHARGE DES AFFAIRES SOCIALES (MCAS)	6
4. MISE EN ŒUVRE DE LA GOUVERNANCE DE LA SECURITE NUMERIQUE.	6
5. OBJECTIFS ET REGLES DE SECURITE	9
POLITIQUE, ORGANISATION, GOUVERNANCE	9
RESSOURCES HUMAINES	10
GESTION DES BIENS	10
INTEGRATION DE LA SECURITE DANS LE CYCLE DE VIE DES SYSTEMES D'INFORMATION	11
SECURITE PHYSIQUE	11
SECURITE DES RESEAUX	12
ARCHITECTURE DES SI	14
EXPLOITATION DES SYSTEMES D'INFORMATION	14
SECURITE DU POSTE DE TRAVAIL	18
SECURITE DU DEVELOPPEMENT DES SYSTEMES	19
TRAITEMENT DES INCIDENTS	20
CONTINUITE D'ACTIVITE	20
CONFORMITE, AUDIT, INSPECTION, CONTROLE	21
6. GLOSSAIRE	22
ANNEXE 1 – OBJECTIFS ET REGLES GENERALES DE SECURITE	23
ANNEXE 2- GESTION DES INCIDENTS LIES A LA SECURITE DE L'INFORMATION	23
ANNEXE 3 – HOMOLOGATION RGS	23

1. OBJET DU DOCUMENT

Le présent document définit la politique de sécurité des systèmes d'information de la CNAF.

Cette politique repose sur la politique de sécurité des systèmes d'information des ministères chargés des affaires sociales (PSSI-MCAS) approuvée le 1^{er} Octobre 2015.

Ce Document décrit les règles applicables sur l'ensemble des systèmes d'information de la Branche, au niveau de la gouvernance, de leur construction, de leur exploitation, de la gestion des incidents de sécurité et de l'homologation des services.

Il est complémentaire au document PGSI décrivant la stratégie, la réglementation applicable et l'organisation de sécurité de la Branche.

2. CHAMP D'APPLICATION

2.1 PERIMETRE D'APPLICATION

Tel que décrit dans le document « Politique Générale de Sécurité de l'information (PGSI), la sécurité des systèmes d'information couvre l'ensemble des informations et leur traitement (création, conservation, échange, etc.), quelle que soit la forme matérielle ou immatérielle sous laquelle elles sont exploitées (électronique, imprimée, manuscrite, vocale, image ...).

Elle concerne l'ensemble des activités des Organismes de la branche Famille, des partenaires, des fournisseurs et des sous-traitants qui ont accès au système d'information de la Branche, quels que soient leurs lieux d'implantation. Elle porte sur l'ensemble des ressources du système d'information.

2.2 GESTION DES EVOLUTIONS

La PSSI devra être revue périodiquement pour prendre en compte :

- Les évolutions des directives et politiques de sécurité des Systèmes d'Information Ministérielles, par exemple la PSSI État, ou des orientations de l'ANSSI ;
- Les résultats d'analyses de risques, d'actions de contrôle ou d'inspection ;
- Les évolutions du contexte organisationnel et technologique ;
- Les évolutions de périmètre de la branche famille.

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

3.1 ENJEUX

Au-delà des systèmes informatiques, le terme « système d'Information » correspond à l'ensemble des ressources (les hommes, le matériel, les logiciels) organisées pour collecter, stocker, traiter et communiquer de l'information au sein même d'une organisation et dans ses relations avec l'extérieur.

L'indisponibilité, la modification et la divulgation non autorisées de ces ressources, essentielles au bon fonctionnement du réseau des Allocations familiales, entraînerait des impacts forts sur ses activités : perte de marché public, perte de crédibilité, manquement grave aux obligations légales et réglementaires, atteinte au bon déroulement des activités, mise en danger de personnes, etc.

De ce fait, les systèmes d'Information portent des enjeux forts :

3.2 DES ENJEUX DE CONTINUITE DE SERVICE DES ACTIVITES DE L'ÉTAT

Une défaillance des systèmes d'Information de la CNAF pourrait nuire de façon importante à la continuité des services de l'État, notamment en ce qui concerne les services essentiels au fonctionnement du pays et à sa défense, et entraîner une non-conformité aux Directives Nationales de Sécurité.

3.3 DES ENJEUX D'IMAGE LIES A UNE DEFAILLANCE DANS LE SERVICE AUX CITOYENS

La sécurisation des Systèmes d'Information joue un rôle primordial dans le service aux citoyens ; une défaillance de ceux-ci pourrait en effet porter atteinte à l'image de la CNAF et entraîner une perte de confiance dans les services numériques. Cela peut notamment se traduire par :

- Une perte de confiance des citoyens, en cas de défaillances dans le fonctionnement du système de protection sanitaire, social ou de solidarité ;
- Une perte de confiance des citoyens en cas de perte ou de divulgation d'informations à caractère personnel protégées par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
- Une perte de confiance des citoyens et des partenaires, en cas de divulgation d'informations financières ou sociales ;
- Une perte de confiance des fournisseurs en particulier dans le cas où les informations liées aux marchés public seraient divulguées ou compromises ;
- Une perte de confiance en cas d'usurpation ou de dénaturation d'informations ;
- Une perte de confiance en cas de mauvaise utilisation ou de détournement d'argent public ;
- Une perte de crédibilité sur la gestion ministérielle, en particulier dans l'hypothèse où les données opérationnelles, financières et statistiques ne seraient pas fiables ou produites à temps.

3.4 DES ENJEUX D'ORGANISATION INTERNE

Une défaillance de ces systèmes conduirait à une importante désorganisation dans la conduite des activités quotidiennes de la Branche.

En effet, les processus étant très intégrés dans les SI, tout sinistre sur les SI (infrastructure bureautique, applications, etc.) a des conséquences directes sur les activités et peut ainsi ralentir les prises de décision et la mise en œuvre de traitements.

3.5 OBJECTIFS OPERATIONNELS EN MATIERE DE SSI

Afin de répondre aux enjeux décrits ci-avant, il est nécessaire d'assurer la disponibilité des SI, l'intégrité des données et des traitements, la confidentialité des informations manipulées et la traçabilité des événements sur le SI.

Le respect de ces objectifs de sécurité de l'information implique notamment de :

■ **Réaliser les analyses de risques pesant sur les SI**

La sécurisation des SI passe en premier lieu par la réalisation de l'analyse des risques. Cela permet d'envisager les moyens organisationnels et techniques à mettre en place pour un juste niveau de sécurité au regard des enjeux et de concourir ainsi à la gestion des risques.

■ **Mettre les SI en conformité avec les lois et réglementations**

Différentes obligations légales ou réglementaires doivent faire l'objet d'une prise en compte par les autorités (CNIL, RGS, eIDAS...) et de leur mise en conformité.

■ **Sensibiliser et former le personnel**

Les pratiques quotidiennes des utilisateurs et administrateurs des SI sont un élément clé de la SSI, et il est alors essentiel de leur faire prendre conscience et de les former aux enjeux de la sécurité de l'information.

■ **Sécuriser les composants des SI et maintenir les SI en condition de sécurité (MCS)**

La sécurisation des composants du SI concerne les postes de travail, serveurs bureautiques et applicatifs, réseaux, applications etc. ainsi que les éléments en périphérie des ressources informatiques tels que la sécurité physique des locaux.

La mise en place de SI demande, outre le maintien en condition opérationnelle, de penser au maintien en condition de sécurité (mise à jour des correctifs de sécurité, vérification des comptes utilisateur...).

■ **Assurer une gestion efficace des incidents de sécurité, des crises et de la continuité d'activité**

La survenue d'un événement anormal affectant l'un des composants d'un système d'information et de communication doit être déclaré par tout agent auprès de son responsable informatique de proximité, de son responsable de la sécurité des systèmes d'information ou le cas échéant de l'AQSSI.

En cas d'incident, sinistre ou piratage critique suspecté ou avéré, le service du Haut fonctionnaire de défense et de sécurité en est informé sans délai. Le FSSI peut être saisi directement.

3.6 MESURES PARTICULIERES POUR LE MINISTERE CHARGE DES AFFAIRES SOCIALES (MCAS)

Conformément à la PSSIE, il est possible, sur autorisation du Haut fonctionnaire de défense et de sécurité de déroger à certaines règles.

Pour ne pas baisser le niveau minimal de sécurité admissible, toute demande de dérogation, doit être accompagnée systématiquement d'une analyse de risques, validée par le SHFDS.

4. MISE EN ŒUVRE DE LA GOUVERNANCE DE LA SECURITE NUMERIQUE.

Mettre en œuvre la cybersécurité (ou sécurité des systèmes d'information) de façon performante et peu coûteuse ... c'est possible.

SI, dans un premier temps, les normes et les technologies de sécurité des systèmes d'information semblent souvent contraignantes et bien loin des impératifs métiers, il convient de revenir à l'essentiel, c'est-à-dire d'identifier la nature du périmètre à sécuriser, de protéger « l'ADN de l'organisme » regroupant tout à la fois : savoir-faire, informations (données métier, données privées, données de fonctionnement...) ainsi que les systèmes concourant à l'élaboration, au traitement, au stockage, à la diffusion de ces informations.

Les mesures de protection adaptées sont déjà bien souvent présentes : il suffit de les identifier et de les organiser afin d'assurer et de pérenniser un niveau de sécurité conforme à ses besoins.

La meilleure façon de protéger un organisme consiste à adopter un processus de gestion des risques dans une démarche d'amélioration continue, en prenant en considération les vrais besoins en matière de sécurité. Cette approche nécessite un peu de temps, mais elle sera mieux adaptée aux besoins réels - elle est plus efficace et moins chère.

De façon générale, la sécurité vise à réduire le nombre ainsi que l'envergure des impacts :

- juridiques,
- sur la réputation,
- sur le temps (perdu) de production,
- sur le savoir-faire,
- financiers.

Concernant l'impact financier, il est à noter que tout incident de sécurité sur un système d'information induit obligatoirement des surcoûts directs ou indirects très supérieurs aux investissements qui auraient pu être mis en place pour sécuriser les systèmes d'information.

Le risque peut se définir par le calcul suivant : $\text{risque} = \text{vulnérabilité} \times \text{menace} \times \text{impact}$.

Il est composé d'un facteur « probabilité » (provenant de la menace) et d'un facteur « dégât » (provenant de la valeur de l'actif (*) compromis et de la valeur du dommage indirect subit). La vulnérabilité utilisée dans cette fonction prend compte des mesures de sécurité mise en place. Il est pratiquement impossible de prévenir un risque en voulant agir sur les menaces existantes. Par contre, on peut agir sur le risque en réduisant les facteurs « vulnérabilité » et « impact » :

- réduire le facteur « vulnérabilité », par la mise en place de mesures de sécurité ciblées ;
- réduire l'impact potentiel, par la mise en place d'un plan de continuité des systèmes d'information (inclus dans le plan de continuité de l'organisme) – par exemple mise en place de systèmes de redondances des données et d'un plan de reprise des systèmes d'information (inclus dans le plan de reprise d'activité).

() Un actif est un bien ou un service ayant une certaine valeur pour l'entreprise. Les actifs sont sujets à différentes vulnérabilités, susceptibles d'être exploitées par des menaces qui auront des impacts au niveau de l'entreprise. Pour protéger ses actifs, une entreprise mettra en place des mesures de sécurité.*

Une approche graduelle

Il s'agit d'établir et de maintenir un pilotage structuré de la cybersécurité afin de s'assurer que les stratégies de sécurité de l'organisation sont conformes aux objectifs de l'activité et compatibles avec les lois et les réglementations qui lui sont applicables.

Le pilotage de la sécurité par les risques est une approche « stratégique » car elle permet d'acquérir une vision globale de la sécurité à travers les activités métiers de l'organisme. Elle facilite ainsi à la fois la mise en place immédiate de solutions de sécurité « curatives » sans pour autant perdre le lien avec les besoins de sécurité de l'entreprise mais permet surtout de mettre en place des moyens « préventifs » et ainsi réduire les surfaces de vulnérabilités ou d'attaque.

Organisation

Dans le cadre de la sécurité des systèmes d'informations, toutes les responsabilités doivent être clairement définies dans l'organisation. La direction désigne les responsables ainsi que leurs champs de compétences.

L'organisation de la sécurité des systèmes d'information au sein d'un organisme suit une démarche cyclique (roue de Deming). La mise en œuvre de ce cycle implique la définition d'une gouvernance de la cybersécurité qui sera adaptée à la nature de l'activité et aura pour mission de démarrer et d'entretenir le cycle.

L'organisation et le processus de management de la sécurité sont décrits.

Cartographie : Savoir ce que l'on possède et ce que l'on veut protéger

Il faut identifier les données et actifs(*) indispensables à l'organisme et au bon accomplissement de ses missions (*ex : informatique générale, gestion technique centralisée (ascenseurs, ventilations, climatisation contrôles d'accès...), systèmes d'information hospitalier, systèmes de communication, informatique embarquée ou associée à des dispositifs médicaux....*).

Analyser des risques

Pour pouvoir protéger les données et actifs importants et vitaux, il faut d'abord identifier les risques par une analyse, identifier les menaces et la probabilité que celles-ci risquent de survenir, identifier l'ampleur des vulnérabilités humaines et techniques et quantifier les impacts potentiels.

Le recensement des besoins de sécurité sera réalisé en répondant notamment aux questions suivantes :

- Quelles sont les activités critiques de mon organisation ?
- Quels sont les systèmes qui concourent au bon fonctionnement de ces activités ?
- Quelles sont les contraintes légales et réglementaires que l'on doit respecter ?
- Quelle est la disponibilité souhaitée de mes systèmes d'information ?
- Quelle résistance à l'altération des données et des traitements dois-je mettre en œuvre ?
- Quel est le niveau de confidentialité à prendre en compte pour les données et les traitements ?
- Faut-il conserver des traces des transactions numériques ?

Protéger

- procéder à la protection des données et des systèmes permettant leur traitement. Une fois classifiées, il faut mettre en place les moyens visant à assurer leur protection par des sauvegardes, lors de leur transport ou encore lors de leur transmission. Il convient également de prévoir leur destruction sécurisée.
- Mettre en place des mesures préventives et protectrices pour les matériels (ordinateurs, ordinateurs portables, serveurs, informatique embarquée ou adjointe) et pour les réseaux (téléphoniques, informatiques...)
- Mettre en place des mesures de type « réaction sur incidents ».

Sensibiliser et former la totalité des personnels

L'adoption des bonnes mesures comportementales par l'ensemble du personnel est une mesure extrêmement importante. Il importe donc de promouvoir une culture de la sécurité des systèmes d'information au travers de bonnes pratiques accessibles aux utilisateurs, maîtrises d'ouvrage et maîtrises d'œuvre.

Les utilisateurs doivent appliquer et respecter les règles de sécurité définies. Une charte d'utilisation des systèmes d'information doit être mise en place. Cette charte doit être opposable en cas d'incident ou de litige.

Cette approche n'est efficace que si elle est bien comprise par l'ensemble des différents acteurs. Elle se doit d'intégrer bonnes pratiques de sécurité permettant de garantir le niveau de protection existant et/ou attendu.

Il est donc essentiel de propager une culture « sécurité » via une communication adaptée aux différents acteurs.

5. OBJECTIFS ET REGLES DE SECURITE

Ce chapitre décrit 34 objectifs de Sécurité situés dans 13 domaines différents, ils induisent la mise en place de règles incontournables citées dans ce chapitre.

Les règles exhaustives qui font « référence » sont décrites en annexe.

L'application de ces règles fait l'objet de définition de mesures de sécurité en décrivant les modalités de mise en œuvre et le cas échéant de bonnes pratiques de sûreté de fonctionnement associées dans le référentiel de contrôle interne du système d'informations.

Les mesures et les bonnes pratiques qui ne sont pas encore en vigueur feront l'objet d'une inscription au plan annuel de contrôle interne et les cas échéant à un plan d'action de mise en œuvre associé au programme de sécurité numérique de la Branche.

POLITIQUE, ORGANISATION, 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

Déployer une organisation de la sécurité des systèmes d'information

Acteurs SSI

Identifier les acteurs de la sécurité des systèmes d'information

Responsabilités internes

Désigner un responsable sécurité des systèmes d'information

Formaliser les rôles et les responsabilités

Responsabilités vis-à-vis des tiers

Intégrer des clauses de sécurité dans tout contrat ou convention avec des tiers

Application des mesures de sécurité au sein de l'entité

Appliquer les instructions de sécurité

Formaliser les documents d'application de la sécurité

RESSOURCES HUMAINES

Objectif 2 : Ressources humaines

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

Utilisateurs

Déployer une charte de sécurité opposable

Personnel permanent

Sélectionner et sensibiliser les personnes tenant les postes clef de la SSI

Apporter une attention particulière à la sélection du Personnel de confiance

Sensibiliser des utilisateurs des systèmes d'information

Mouvement de personnel

Formaliser une procédure de gestion des habilitations

Personnel non permanent

Appliquer les règles de sécurité à tout personnel non permanent

GESTION DES BIENS

Objectif 3 : Cartographie des systèmes d'information

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

Dresser un inventaire des ressources informatiques

Etablir une cartographie détaillée des ressources

Objectif 4 : Qualification et protection de l'information.

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

Qualifier le niveau de sensibilité des informations

Protéger les informations en fonction de leur niveau de sensibilité

INTEGRATION DE LA SECURITE DANS LE CYCLE DE VIE DES SYSTEMES 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.

Homologuer la sécurité des systèmes d'information. Voir en annexe 3.

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.

Intégrer la sécurité dans les projets

Mettre en œuvre au quotidien de la sécurité des systèmes d'information

Créer un tableau de bord de sécurité des systèmes d'information

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.

Acquérir de produits et services de confiance

Objectif 8 : Gestion des prestataires

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

Spécifier les clauses de sécurité dans le cadre de la prestation

Suivre et contrôler les prestations fournies

Analyser de risques

Respecter les règles d'hébergement des données

Détailler les clauses de sécurité dans le cadre de l'hébergement des données

SECURITE 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.

Découper les sites en zones de sécurité

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

Restreindre les accès réseau en zone d'accueil du public

Protéger les informations sensibles au sein des zones d'accueil

Règles de sécurité complémentaires s'appliquant aux locaux techniques

Assurer la sécurité physique des locaux techniques

Protéger les câbles électriques et de télécommunications

Effectuer des contrôles anti-piégeages

Objectif 10 : Sécurité physique des centres informatiques (Data Center)

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

Règles générales

Découper les locaux en zones de sécurité

Définir une convention de service en cas d'hébergement tiers

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

Mettre en place de système de contrôle d'accès physique

Formaliser la délivrance des moyens d'accès physique

Assurer la traçabilité des accès

Règles de sécurité complémentaires

Se prémunir contre la perte d'énergie

Installer un dispositif de climatisation

Lutter contre l'incendie

Lutter contre les voies d'eau

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.

Mettre en place une sécurisation du système d'information de sûreté physique

SECURITE DES RESEAUX

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.

Définir les règles de systèmes autorisés sur le réseau

Maîtriser les interconnexions avec des réseaux externes

Mettre en place un filtrage réseau pour les flux sortants et entrants

Protéger les informations transitant par internet

Objectif 13 : Usage sécurisé des réseaux locaux

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

Cloisonner le Système d'information en sous-réseaux de niveaux de sécurité homogènes

Interconnecter les sites géographiques locaux d'un organisme

Cloisonner les ressources en cas de partage de locaux

Objectif 14 : Accès spécifiques

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

Cas particulier des accès spécifiques dans un organisme

Objectif 15 : Usage sécurisé des réseaux sans fil

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

Mettre en place un réseau sans fil

Objectif 16 : Sécurisation des mécanismes de commutation et de routage

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

Implanter des mécanismes de protection contre les attaques sur les couches basses

Surveiller les annonces de routage

Configurer le protocole IGP8 de manière sécurisée

Sécuriser les sessions EGP9

Modifier systématiquement les éléments d'authentification par défaut des équipements et services

Durcir les configurations des équipements de réseau

Objectif 17 : Cartographie réseau

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

Élaborer les documents d'architecture technique et fonctionnelle

ARCHITECTURE DES SI

Objectif 18 : Architecture des centres informatiques

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

Définir et appliquer les principes d'architecture des zones d'hébergement

Définir l'architecture de stockage et de sauvegarde

Homologuer la passerelle Internet

EXPLOITATION DES SYSTEMES D'INFORMATION

Objectif 19 : Protection des informations sensibles

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

Protéger les informations sensibles en confidentialité et en intégrité

Objectif 20 : Surveillance et configuration des ressources informatiques

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

Assurer la traçabilité des interventions sur le système

Respecter la configuration des ressources informatiques

Documenter les configurations

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

Identifier, authentifier et contrôler les accès logique

Déterminer les droits d'accès aux ressources

Gérer les profils d'accès aux applications

Processus d'autorisation

Formaliser les autorisations d'accès des utilisateurs

Réaliser des revues des autorisations d'accès

Gestion des authentifiants

Assurer la confidentialité des informations d'authentification

- Etablir des règles de gestion des mots de passe**
- Formaliser l'initialisation des mots de passe**
- Elaborer la Politique de gestion de mots de passe**
- Respecter les règles d'utilisation de certificats électroniques**
- Contrôler systématiquement de la qualité des mots de passe**

Gestion des authentifiants d'administration

- Séquestrer les authentifiants « administrateur »**
- Elaborer la politique des mots de passe « administrateurs »**
- Définir les règles de gestion du départ d'un administrateur des SI**

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

- Restreindre les droits d'administration**
- Protéger les accès aux outils d'administration**
- Définir les règles d'habilitation des administrateurs**
- Superviser la gestion des actions d'administration**
- Sécuriser des flux d'administration**
- Centraliser la gestion du système d'information**
- Sécuriser les outils de prise de main à distance**

Administration des domaines

- Définir une politique de gestion des comptes du domaine**
- Configurer la stratégie des mots de passe des domaines**
- Définir et appliquer une nomenclature des comptes du domaine**
- Restreindre au maximum l'appartenance aux groupes d'administration du domaine**
- Maîtriser l'utilisation des comptes de service**
- Limiter les droits des comptes de service**
- Désactiver les comptes du domaine obsolètes**
- Améliorer la gestion des comptes d'administrateur locaux**

Envoi en maintenance et mise au rebut

Définir les règles de maintenance externe

Définir les règles de mise au rebut

Lutte contre les codes malveillants

Mettre en place des système de protection contre les codes malveillants

Gérer les événements de sécurité de l'antivirus

Mettre à jour la base de signatures

Configurer le navigateur Internet

Mise à jour des systèmes et des logiciels

Définir et mettre en œuvre une politique de suivi et d'application des correctifs de sécurité

Déployer les correctifs de sécurité

Assurer la migration des systèmes obsolètes

Isoler les systèmes obsolètes restants

Journalisation

Journaliser les alertes

Définir et mettre en œuvre une politique de gestion et d'analyse des journaux de traces

Conserver les journaux

Objectif 23 : Défense des systèmes d'information

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

Procéder à une gestion dynamique de la sécurité

Gestion des matériels informatiques fournis à l'utilisateur

Maîtriser les matériels

Rappeler des mesures de protection contre le vol

Déclarer les pertes et vols

Réaffecter les matériels informatiques

Nomadisme

Déclarer les équipements nomades aptes à traiter des informations sensibles

Accéder à distance au système d'information de l'organisme

Sécurisation des imprimantes et copieurs multifonctions manipulant des informations sensibles

Respecter les règles d'impression des informations sensibles

Sécuriser les imprimantes et les copieurs multifonctions

Objectif 24 : Exploitation sécurisée des centres informatiques

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

Sécurité des ressources informatiques

Systèmes d'exploitation

Logiciels en Tiers Présentation

Logiciels en Tiers Application

Logiciels en Tiers Données

Passerelle d'échange de fichiers

Messagerie technique

Filtrage des flux applicatifs

Flux d'administration

Service de noms de domaine – DNS technique

Effacement de support

Destruction de support

Traçabilité / imputabilité

Supervision

Accès aux périphériques amovibles

Accès aux réseaux

Audit/contrôle

Objectif 25 : Sécurisation des postes de travail

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

Mise à disposition du poste

- Fournir et gérer les postes de travail
- Formaliser la configuration des postes de travail

Sécurité physique des postes de travail

- Verrouiller l'unité centrale des postes fixes
- Verrouiller les postes portables

Réaffectation du poste et récupération d'informations

- Règles de redéploiement d'un poste de travail

Gestion des privilèges sur les postes de travail

- Gérer les privilèges des utilisateurs sur les postes de travail
- Utiliser les privilèges d'accès « administrateur »
- Gérer les comptes « administrateur local »

Protection des informations

- Stocker les informations
- Sauvegarder / synchroniser les données locales
- Partager des fichiers
- Supprimer des données sur les postes partagés
- Chiffrer les données sensibles
- Fournir des supports de stockage amovibles

Nomadisme

- Accéder à distance aux Systèmes d'Information de l'entité
- Installer un pare-feu local
- Stocker localement des informations sur les postes nomades
- Mettre en place d'un filtre de confidentialité

Configurer les interfaces de connexion sans fil

Désactiver les interfaces de connexion sans fil

Objectif 26 : Sécurisation des imprimantes et copieurs multifonctions

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

Durcir la sécurité des imprimantes et copieurs multifonctions

Sécuriser la fonction de numérisation

Objectif 27 : Sécurisation de la téléphonie

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

Sécuriser la configuration des autocommutateurs

Modifier les codes d'accès téléphoniques

Limiter l'utilisation du DECT

Objectif 28 : Contrôles de conformité

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

Utiliser des outils de vérification automatique de la conformité

SECURITE DU DEVELOPPEMENT DES SYSTEMES

Objectif 29 : Développement des systèmes

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

Intégrer la sécurité dans les développements locaux

Intégrer des clauses SSI dans les contrats de sous-traitance de développement informatique

Objectif 30 : Développements logiciels et sécurité

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

Limiter les fuites d'information

Réduire l'adhérence des applications à des produits ou technologies spécifiques

Instaurer des critères de développement sécurisé

Intégrer la sécurité dans le cycle de vie logiciel

Améliorer la prise en compte de la sécurité dans les développements Web

Calculer les empreintes de mots de passe de manière sécurisée

Objectif 31 : Applications à risques

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

Mettre en œuvre des fonctionnalités de filtrage applicatif pour les applications à risque

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.

Mettre en place les chaînes opérationnelles de la sécurité des systèmes d'information

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

Mobiliser en cas d'alerte

Remontée des incidents de sécurité rencontrés

Qualifier et traiter les incidents

Remonter les incidents

CONTINUE D'ACTIVITE

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

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

Définir le plan de continuité d'activité des Systèmes d'Information

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

Définir le plan national de continuité d'activité des systèmes d'information

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

Suivre la mise en œuvre du plan de continuité d'activité des Système d 'Information (PCA des SI)

Mettre en œuvre les dispositifs techniques et les procédures opérationnelles

Protéger la disponibilité des sauvegardes

Protéger la confidentialité des sauvegardes

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

Réaliser des exercices réguliers du plan local de continuité d'activité des systèmes d'information

Mettre à jour le plan local de continuité d'activité des systèmes d'information

CONFORMITE, AUDIT, INSPECTION, CONTROLE

Objectif 34 : Contrôles réguliers

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

Effectuer des contrôles réguliers de conformité à la PSSI

Etablir des bilans annuels

6. GLOSSAIRE

Les termes

AA	<i>Autorité d'appui</i>
Actif	<i>Tout élément représentant de la valeur pour l'organisation / l'entreprise.</i>
AH	<i>Autorité d'homologation</i>
ANSSI	<i>Agence nationale de la sécurité des systèmes d'information.</i>
AQSSI	<i>Autorité qualifiée de sécurité des systèmes d'information</i>
CERT-FR	<i>Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques</i>
CIL	<i>Correspondant informatique et liberté</i>
CLSSI	<i>Correspondant local de sécurité des systèmes d'information</i>
CNIL	<i>Commission nationale informatique et liberté</i>
COSSI	<i>Centre opérationnel de la sécurité des systèmes d'information (tél H24 : 01 71 75 84 68)</i>
CYBERSECURITE	<i>Recouvre l'ensemble des mesures de sécurité susceptibles d'être prises pour se défendre contre des incidents ou attaques.</i>
DSI	<i>Direction des systèmes d'information</i>
EBIOS	<i>Expression des Besoins et Identification des Objectifs de Sécurité – Méthode d'analyse de risques</i>
EGP	<i>Exterior Gateway Protocol : Protocole de routage dans Internet. EGP est aussi utilisé pour désigner, de façon générale, les protocoles de routage extérieur, c'est-à-dire entre deux systèmes autonomes différents, et par opposition aux protocoles de routage interne.</i>
IGP	<i>Interior Gateway Protocol : Protocole de routage utilisé dans les systèmes autonomes.</i>
eIDAS	<i>Electronic Identification and Signature. Règlement européen qui permet d'établir une fédération des identités sur le sol européen</i>
FSSI	<i>Fonctionnaire de sécurité des systèmes d'information</i>
HFDS	<i>Haut fonctionnaire de défense et de sécurité</i>
Impact :	<i>Conséquence négative qui survient lorsqu'une menace exploite une vulnérabilité d'un actif.</i>
MCAS	<i>Ministères chargés des affaires sociales</i>
PGSI CNAF	<i>Politique générale de sécurité de l'information. Décrit la stratégie, l'organisation et le processus de la CNAF</i>
PSSI	<i>Politique de sécurité des systèmes d'information</i>
PSSIE	<i>Politique de sécurité des systèmes d'information de l'Etat</i>
PSSI-MCAS	<i>Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales</i>
RGS	<i>Référentiel général de sécurité http://www.ssi.gouv.fr/entreprise/reglementation/administration-electronique/le-referentiel-general-de-securite-rgs/</i>
RSSI	<i>Responsable de sécurité des systèmes d'information</i>
SGDSN	<i>Secrétariat général de la défense et de la sécurité nationale</i>
SHFDS	<i>Service du Haut fonctionnaire de défense et de sécurité</i>
SI	<i>Système d'information: ensemble des moyens humains et matériels ayant pour finalité d'élaborer, traiter, stocker, acheminer, présenter ou détruire l'information</i>

Les définitions

BESOIN DE SECURITE	<i>Définition précise et non ambiguë du niveau d'exigences opérationnelles relatives à un bien essentiel pour un critère de sécurité donné (disponibilité, confidentialité, intégrité...).</i>
BIEN ESSENTIEL	<i>Information ou processus jugé comme important pour l'organisme. On appréciera ses besoins de sécurité mais pas ses</i>

	vulnérabilités.
BIEN SUPPORT	Bien sur lequel reposent des biens essentiels. On distingue notamment les systèmes informatiques, les organisations et les locaux. On appréciera ses vulnérabilités mais pas ses besoins de sécurité.
CONFIDENTIALITE	Propriété des biens essentiels de n'être accessibles qu'aux personnes autorisés
DISPONIBILITE	Propriété d'accessibilité au moment voulu des biens essentiels par les personnes autorisées
INTEGRITE	Propriété d'exactitude et de complétude des biens essentiels
MESURE DE SECURITE	Moyen de traiter un risque de sécurité de l'information. La nature et le niveau de détail de la description d'une mesure de sécurité peuvent être très variables
BESOIN DE SECURITE	Définition précise et non ambiguë du niveau d'exigences opérationnelles relatives à un bien essentiel pour un critère de sécurité donné (disponibilité, confidentialité, intégrité...).
BIEN ESSENTIEL	Information ou processus jugé comme important pour l'organisme. On appréciera ses besoins de sécurité mais pas ses vulnérabilités.
BIEN SUPPORT	Bien sur lequel reposent des biens essentiels. On distingue notamment les systèmes informatiques, les organisations et les locaux. On appréciera ses vulnérabilités mais pas ses besoins de sécurité.
OBJECTIF DE SECURITE	Expression de la décision de traiter un risque selon des modalités prescrites. On distingue notamment la réduction, le transfert (partage des pertes), le refus (changements structurels pour éviter une situation à risque) et la prise de risque
REDUCTION DE RISQUE	Choix de traitement consistant à appliquer des mesures de sécurité destinées à réduire les risques
RISQUE RESIDUEL	Risque subsistant après le traitement du risque
VULNERABILITE	Caractéristique d'un bien support qui peut constituer une faiblesse ou une faille au regard de la sécurité des systèmes d'information

ANNEXE 1 – OBJECTIFS ET REGLES GENERALES DE SECURITE



PSSI_ANNEXE 1
Objectifs et règles gé

ANNEXE 2- GESTION DES INCIDENTS LIES A LA SECURITE DE L'INFORMATION



PSSI_ANNEXE 2
Gestion des incidents

ANNEXE 3 – HOMOLOGATION RGS



PSSI_ANNEXE 3
Homologation RGS.dc