

Politique de sécurité des systèmes d'information de la branche Famille

Annexe 1

Objectifs et règles générales de sécurité



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

Juin 2017

REVISIONS DU DOCUMENT

Date	Objet
Juin 2017	Version initiale

Les objectifs et règles décrites dans ce document font régulièrement référence au RSSI.

Ce terme représente un niveau national de responsabilité fonctionnelle et opérationnelle de sécurité des systèmes d'information.

Cette responsabilité est déclinée en termes d'organisation dans la PGSI.

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

Une organisation dédiée à la sécurité des systèmes d'information est déployée dans tous les organismes de la branche Famille. Elle est décrite dans le document « Politique Générale de Sécurité de l'Information » (PGSI).

Acteurs SSI

L'organisation SSI s'appuie sur des acteurs de la sécurité des systèmes d'information clairement identifiés, à tous ses niveaux d'organisation.

Responsabilités internes

Désignation du responsable SSI

Le directeur général de la Cnaf, autorité qualifiée de la sécurité des systèmes d'information (AQSSI) s'appuie sur une autorité d'appui (AA) et sur un ou plusieurs responsables de la sécurité des systèmes d'information (RSSI), chargé(s) de l'assister dans le pilotage et la gestion de la SSI. Des correspondants locaux SSI ou Managers de la Sécurité du Système d'Information locaux (MSSI) sont désignés, afin de constituer un relais du RSSI.

Formalisation des responsabilités

La PGSI 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.

Responsabilités vis-à-vis 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.

Application des mesures de sécurité au sein de l'entité

Application de l'instruction

Le RSSI planifie les actions de mise en application de la PSSI. Il rend compte régulièrement de la mise en application des mesures de sécurité à son autorité qualifiée et, le cas échéant au FSSI.

Formalisation des documents d'application

Le RSSI formalise et tient à jour les documents d'application, approuvés par l'autorité qualifiée, permettant la mise en œuvre des mesures de la PSSI sur son périmètre.

Ressources humaines

Objectif 2 : Ressources humaines

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

Utilisateurs

Une charte d'application de la politique SSI, récapitulant les mesures pratiques d'utilisation sécurisée des ressources informatiques et élaborée sous le pilotage de la chaîne fonctionnelle SSI, est communiquée à l'ensemble des agents de chaque entité. Cette charte est opposable juridiquement et, est intégrée au règlement intérieur de l'entité.

Le personnel non permanent (stagiaires, intérimaires, prestataires...) est informé de ses devoirs dans le cadre de son usage des systèmes d'information.

Personnel permanent

Choix et sensibilisation des personnes tenant les postes clef de la SSI

Une attention particulière est portée au recrutement des personnes-clés de la SSI : RSSI, correspondants SSI locaux et administrateurs de sécurité. Le RSSI et les correspondants SSI locaux doivent être spécifiquement formés à la sécurité des systèmes d'information. Les administrateurs des systèmes d'information doivent être régulièrement sensibilisés aux devoirs liés à leur fonction, et doivent veiller à respecter ces exigences dans le cadre de leurs activités quotidiennes.

Personnel de confiance

Toutes les personnes manipulant des informations sensibles doivent le faire avec une attention et une probité particulière, dans le respect des textes en vigueur. Les sanctions éventuelles s'appliquant aux cas de négligence ou de malveillance leur sont rappelées.

Sensibilisation des utilisateurs des systèmes d'information

Chaque utilisateur doit être régulièrement informé des exigences de sécurité le concernant, et motivé à leur respect. Il est formé à l'utilisation des outils de travail conformément aux règles de sécurité des systèmes d'information.

Mouvement de personnel

Une procédure permettant de gérer les arrivées, les mutations et les départs des collaborateurs dans les systèmes d'information doit être formalisée et appliquée strictement par chaque organisme. Cette procédure doit couvrir au minimum :

- la gestion/révocation des comptes et des droits d'accès aux systèmes d'information, y compris pour les partenaires et les prestataires ;
- la gestion du contrôle d'accès aux locaux ;
- la gestion des équipements mobiles ;
- la gestion du contrôle des habilitations.

Personnel non permanent

Les règles de la PSSI s'appliquent à tout personnel non permanent utilisateur d'un système d'information de la Cnaf. Les dispositions contractuelles préexistantes régissant l'emploi de ce personnel sont amendées si nécessaire. Pour tout personnel non permanent, un tutorat par un agent permanent est mis en place, afin de l'informer de ces règles et d'en contrôler l'application.

Gestion des biens

Objectif 3 : Cartographie des systèmes d'information

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

Inventaire des ressources informatiques.

Chaque organisme établit et maintient à jour un inventaire des ressources informatiques sous sa responsabilité, en s'appuyant sur un outillage adapté. Cet inventaire est tenu à disposition du RSSI.

Cartographie.

La cartographie précise les centres informatiques, les architectures des réseaux (sur lesquelles sont identifiés les points névralgiques et la sensibilité des informations manipulées) et qualifie le niveau de sécurité attendu. Cette cartographie est maintenue à jour et tenue à disposition du RSSI et de l'AQSSI.

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 est la suivante :

- Publique : ce niveau concerne les informations réputées publiques et notamment celles publiées en ligne ou via un autre moyen de diffusion ;
- Interne : Les documents internes sont communicables au titre de dispositions relatives à l'accès aux documents administratifs.
- Diffusion restreinte : Les documents à diffusion restreinte sont diffusés à leurs seuls destinataires et ne sont pas communicables, sauf décision expresse du directeur général.
- Confidentiel : Les documents classés confidentiels sont soumis aux règles applicables en la matière ; ce niveau concernent notamment les informations relatives à la sécurité de l'organisme, de la Branche ou à la situation et à la sécurité des personnes.

Qualification des informations

La sensibilité de toute information doit être évaluée. Le marquage systématique des documents, en fonction du niveau de sensibilité, est fortement recommandé.

Les informations sensibles reçoivent une mention rappelant leur sensibilité en considération de la gravité des conséquences qu'aurait une divulgation et apposer une mention telle que « confidentiel » sur les documents sensibles ainsi que dans les courriers ou courriels qui les accompagnent. A titre d'exemple, on pourra utiliser les mentions suivantes :

- ▶ Confidentiel sécurité du système d'information,
- ▶ Confidentiel personnel,
- ▶ ...

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.

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.

Homologation de sécurité des systèmes d'information.

Tout système d'information doit faire 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 atteste formellement auprès des utilisateurs que le système d'information est protégé conformément aux objectifs de sécurité fixés.

La décision d'homologation est prise par l'autorité d'homologation (désignée par le directeur général de la Cnaf), le cas échéant après avis du comité d'homologation. Cette décision s'appuie sur une analyse de risques adaptée aux enjeux du système considéré, et précise les conditions d'emploi.

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.

Intégration de la sécurité dans les projets.

La sécurité des systèmes d'information doit être 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.

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.

Créer un tableau de bord SSI.

Un tableau de bord de la sécurité des systèmes d'information est mis en place et tenu à jour. Il fournit au RSSI et aux directions une vision générale du niveau de sécurité et de son évolution, rendant ainsi plus efficace le pilotage de la sécurité des systèmes d'information.

Au niveau stratégique, le tableau de bord SSI permet de suivre l'application de la politique de sécurité et de disposer d'éléments propres à qualifier les ressources devant être allouées à la SSI.

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.

Acquisition de produits et services de confiance.

Il est recommandé d'utiliser, lorsqu'ils sont disponibles, des produits ou des services de sécurité labellisés (certifiés, qualifiés) par l'ANSSI.

Dans le cadre d'un marché, un critère de choix, dont la notation est clairement définie, sur l'existence d'un label ANSSI est indiqué.

Objectif 8 : Gestion des prestataires

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

Clauses de sécurité.

Toute prestation dans le domaine des SI est encadrée par des clauses de sécurité (plan d'assurance sécurité). Ces clauses spécifient les mesures SSI que le prestataire doit respecter dans le cadre de ses activités.

Suivi et contrôle des prestations fournies.

Le maintien d'un niveau de sécurité au cours du temps nécessite un double contrôle :

- l'un, effectué périodiquement par l'équipe encadrant la prestation, qui porte sur les actions du sous-traitant et la conformité au cahier des charges ;
- l'autre, effectué par une équipe externe, qui porte sur la pertinence du cahier des charges en amont des projets, la conformité des réponses apportées par le sous-traitant en phase de recette et le niveau de sécurité global obtenu en production.

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. L'ensemble des objectifs de sécurité ainsi formalisés permet de définir une cible de sécurité servant de cadre au contrat établi avec le prestataire.

Hébergement.

L'hébergement de données sensibles sur le territoire national est fortement recommandé. En outre, l'hébergement concernant certaines données doit répondre aux exigences légales et réglementaires (données nominatives, ...).

Hébergement et clauses de sécurité.

Tout contrat d'hébergement détaille les dispositions mises en œuvre pour prendre en compte la sécurité du système d'information. Ce sont notamment les mesures prises pour assurer le maintien en condition de sécurité des systèmes et permettre une gestion de crise efficace (conditions d'accès aux journaux, mise en place d'astreintes, etc.).

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.

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 de sécurité, des critères précis d'autorisation d'accès sont établis.

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

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 l'entité.

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

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.

Protection des câbles électriques et de télécommunications.

Il convient de protéger le câblage réseau 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.

Contrôles anti-piégeages.

Sur les systèmes d'information particulièrement sensibles, il est recommandé de mener des contrôles anti-piégeages réguliers, effectués par du personnel formé. Il peut être fait appel à des services spécialisés (opérations dites de « dépoussiérage »).

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

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

Règles générales

Découpage des locaux en zones de sécurité.

Un découpage du centre informatique en zones physiques de sécurité est effectué, en liaison avec le RSSI et les services en charge de l'immobilier, de la sécurité et des moyens généraux. Des règles fixent les conditions d'accès à ces différentes zones.

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

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.

Délivrance des moyens d'accès physique.

La délivrance des moyens d'accès physique respecte un processus formel permettant de s'assurer de l'identité de la personne, s'appuyant sur le processus d'arrivée et de départ du personnel.

Le personnel autre que celui explicitement autorisé et habilité, mais néanmoins appelé à intervenir dans les zones sensibles (entretien ou réparation des bâtiments, des équipements non informatiques, nettoyage, visiteurs, ...), intervient systématiquement et impérativement sous surveillance permanente.

Traçabilité des accès.

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

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

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.

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 annuellement.

Ces dispositions visent à prévenir toute surchauffe des équipements, pouvant engendrer une perte du service voire une détérioration du matériel.

Lutte contre l'incendie.

L'installation de matériel de protection contre le feu est obligatoire. Des 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 ne doit être entreposé dans ces locaux.

Lutte contre les voies d'eau.

Une étude sur les risques dus aux voies d'eau a été réalisée. Cette étude a pris notamment 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 importants (reconnus le cas échéant comme points d'importance vitale) 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.

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.

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.

Systèmes autorisés sur le réseau.

Seuls les équipements gérés et configurés par les équipes informatiques habilitées peuvent être connectés au réseau local d'un organisme.

Interconnexion avec des réseaux externes.

Toute interconnexion entre les réseaux locaux d'un organisme et un réseau externe (réseau d'un tiers, Internet, etc.) doit être réalisée via les infrastructures nationales.

Pour les autres il convient de maîtriser les interconnexions (connaissance des fournisseurs d'accès, réversibilité de la solution, maintien en condition de sécurité)

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

Dans l'optique de réduire les possibilités offertes à un attaquant, les connexions des machines du réseau interne vers l'extérieur sont filtrées.

Protection des informations.

Les accès à Internet passent obligatoirement à travers les passerelles nationales. Dès lors que des informations sensibles doivent transiter sur des réseaux non maîtrisés, il convient de les protéger spécifiquement par un moyen de chiffrement adapté.

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.

Par analogie avec le cloisonnement physique d'un bâtiment, le système d'information doit être segmenté selon des zones présentant chacune un niveau de sécurité homogène.

Interconnexion des sites géographiques locaux d'un organisme.

L'interconnexion au niveau local de réseaux locaux d'un organisme 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.

Cloisonnement des ressources en cas de partage de locaux.

Dans le cas où un organisme partage des locaux (bureaux ou locaux techniques) avec des partenaires, des mesures de cloisonnement des ressources informatiques doivent être 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.

Cas particulier des accès spécifiques dans un organisme

Les accès spécifiques à Internet nécessitant des droits particuliers pour un usage métier ne peuvent être mis en place que sur dérogation dûment justifiée, et sur des machines isolées physiquement et séparées du réseau de l'entité, après validation préalable de l'autorité d'homologation nationale.

Objectif 15 : Usage sécurisé des réseaux sans fil

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

Mise en place de réseaux sans fil.

Le déploiement de réseaux sans fil doit faire l'objet d'une analyse de risques spécifique. Les protections intrinsèques étant insuffisantes, des mesures complémentaires, validées par l'AQSSI, doivent être prises dans le cadre de la défense en profondeur. En particulier, une segmentation du réseau doit être mise en place de façon à limiter à un périmètre déterminé les conséquences d'une intrusion depuis la voie radio. A défaut de mise en œuvre de mesures spécifiques, le déploiement de réseaux sans fil sur des systèmes d'information manipulant des données sensibles est proscrit.

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.

Une attention particulière est apportée à l'implantation des protocoles de couches basses, de façon à se prémunir des attaques usuelles.

Surveiller les annonces de routage.

Les protocoles de routage dynamiques s'accompagnent de la mise en place d'une surveillance des annonces de routage, et de procédures permettant de réagir rapidement en cas d'incidents.

Configurer le protocole IGP (*interior gateway protocol*) de manière sécurisée.

Le protocole de routage dynamique de type IGP doit être activé exclusivement sur les interfaces nécessaires à la construction de la topologie du réseau et désactivé sur le reste des interfaces. La configuration du protocole de routage dynamique doit systématiquement être réalisée suivant les préconisations de l'Agence nationale de sécurité des systèmes d'information.

Sécuriser les sessions EGP (*exterior gateway protocol*).

Lors de la mise en place d'une session EGP avec un pair extérieur sur un média partagé, cette session doit être réalisée suivant les préconisations de l'Agence nationale de sécurité des systèmes d'information.

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

Les mots de passe par défaut doivent être impérativement modifiés, de même en ce qui concerne les certificats. Les dispositions nécessaires doivent être prises auprès des fournisseurs de façon à pouvoir modifier les certificats installés par défaut.

Durcir les configurations des équipements de réseaux.

Les équipements de réseaux (comme les routeurs) doivent faire l'objet d'un durcissement spécifique comprenant notamment, outre le changement des mots de passe et certificats, la désactivation des interfaces et services inutiles, ainsi que la mise en place de mécanismes de protection du plan de contrôle.

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.

L'architecture réseau du système d'information doit être décrite et formalisée à travers des schémas d'architecture, et des configurations, maintenus au fil des évolutions apportées au SI. Les documents

d'architecture sont sensibles et font l'objet d'une protection adaptée. La cartographie réseau s'insère dans la cartographie globale des SI.

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.

Principes d'architecture de la zone d'hébergement.

D'une manière générale, l'architecture des infrastructures des centres informatiques est conçue de façon à satisfaire l'ensemble des besoins en disponibilité, confidentialité, traçabilité et intégrité. Le principe de défense en profondeur doit être respecté, en particulier par la mise en œuvre successive de « zones démilitarisées » (DMZ), d'environnements de sécurité en zone d'hébergement, de machines virtuelles ou physiques dédiées, de réseaux locaux virtuels (VLAN) appropriés, d'un filtrage strict des flux applicatifs et d'administration.

Architecture de stockage et de sauvegarde.

Le réseau de stockage/sauvegarde pour les besoins des centres informatiques repose sur une architecture dédiée à cet effet.

Passerelle Internet.

Les interconnexions Internet passent obligatoirement par des passerelles homologuées.

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.

Protection des informations sensibles en confidentialité et en intégrité.

Des mesures sont mises en œuvre afin de garantir la protection des informations sensibles en confidentialité et en intégrité. A défaut d'utilisation d'un réseau homologué, ces informations doivent être chiffrées à l'aide d'un moyen de chiffrement labellisé.

Objectif 20 : Surveillance et configuration des ressources informatiques

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

Traçabilité des interventions sur le système.

Les interventions de maintenance sur les ressources informatiques de l'entité doivent être tracées par le service informatique, et ces traces doivent être accessibles au RSSI durant au moins un an.

Configuration des ressources informatiques.

Les systèmes d'exploitation et les logiciels doivent faire l'objet d'un durcissement. Les configurations et mises à jour sont appliquées dans le strict respect des guides ou procédures en vigueur dans l'organisme ou, en vigueur au niveau national.

Documentation des configurations.

La configuration standard des ressources informatiques doit être 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

Identification, authentification et contrôle d'accès logique.

L'accès à toute ressource non publique doit nécessiter une identification et une authentification individuelle de l'utilisateur. Dans le cas de l'accès à des données sensibles, des moyens d'authentification forte doivent être utilisés. A cette fin, l'usage d'une carte à puce doit être privilégié. Le contrôle d'accès doit être géré et s'appuyer sur un processus formalisé en cohérence avec la gestion des ressources humaines.

Droits d'accès aux ressources.

Après avoir déterminé le niveau de sensibilité, le besoin de diffusion et de partage des ressources, les droits d'accès aux ressources sont gérés suivant les principes décrits ci-après : « besoin d'en connaître » (chaque utilisateur n'est autorisé à accéder qu'aux ressources pour lesquelles on lui accorde explicitement le bénéfice de l'accès), « moindre privilège » (chaque utilisateur accède aux ressources avec le minimum de privilèges lui permettant de conduire les actions explicitement autorisées pour lui).

Gestion des profils d'accès aux applications.

Les applications manipulant des données sensibles permettent une gestion fine par profils d'accès. Les principes du besoin d'en connaître et du moindre privilège s'appliquent.

Processus d'autorisation

Autorisations d'accès des utilisateurs.

Toute action d'autorisation d'accès d'un utilisateur à une ressource des systèmes d'information, qu'elle soit locale ou nationale, s'inscrit dans le cadre d'un processus d'autorisation formalisé, qui s'appuie sur le processus d'arrivée et de départ du personnel.

Revue des autorisations d'accès.

Une revue des autorisations d'accès est réalisée annuellement sous le contrôle du RSSI, le cas échéant avec l'appui du Manager de la sécurité du système d'information local (MSSI).

Gestion des authentifiants

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.

Gestion des mots de passe.

Les utilisateurs ne doivent pas stocker leurs mots de passe en clair (par exemple dans un fichier) sur leur poste de travail. Les mots de passe ne doivent pas transiter en clair sur les réseaux.

Initialisation des mots de passe.

Chaque compte utilisateur est créé avec un mot de passe initial aléatoire unique. Si les circonstances l'imposent, un mot de passe plus simple mais à usage unique peut être envisagé.

Politiques de mots de passe.

Les règles de gestion et de protection des mots de passe donnant accès aux applications et infrastructures nationales, telles qu'éditées au niveau national, doivent être respectées dans chaque organisme. Pour les ressources dont la politique de mots de passe est gérée localement, les recommandations nationales doivent être appliquées pour tous les comptes.

Utilisation de certificats électroniques.

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

Contrôle systématique de la qualité des mots de passe.

Des moyens techniques permettant d'imposer la politique de mots de passe (par exemple pour s'assurer du respect de l'éventuelle obligation relative à l'usage de caractères spéciaux) sont mis en place. Un contrôle périodique des paramètres techniques relatifs aux mots de passe est réalisé.

Gestion des authentifiants d'administration

Séquestre des authentifiants « administrateur ».

Les authentifiants permettant l'administration des ressources des systèmes d'information doivent être placés sous séquestre et tenus à jour, dans un coffre ou une armoire fermée à clé. L'authentifié doit être informé de l'existence de ces opérations de gestion, de leurs finalités et limites.

Tout accès d'administration à une ressource informatique doit pouvoir être tracé et permettre de remonter à la personne exerçant ce droit.

Politique de mots de passe « administrateurs ».

Chaque administrateur doit disposer d'un mot de passe propre et destiné à l'administration.

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 doivent être immédiatement désactivés. Les éventuels mots de passe d'administration dont il avait connaissance doivent être 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 système d'information et configurer ces outils de manière sécurisée.

Administration des systèmes

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, elle doit être tracée et doit être renouvelée tous les ans. A défaut de renouvellement, les privilèges d'administration doivent être supprimés.

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.

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.

Gestion des actions d'administration.

Les opérations d'administration doivent être tracées de manière à pouvoir gérer au niveau individuel l'imputabilité des actions d'administration.

Sécurisation des flux d'administration.

Les opérations d'administration sur les ressources locales d'un organisme doivent s'appuyer sur des protocoles sécurisés. Un réseau dédié à l'administration des équipements, ou au moins un réseau logiquement séparé de celui des utilisateurs, doit être utilisé. Les postes d'administrateurs doivent être dédiés et ne doivent pas pouvoir accéder à Internet.

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 doivent utiliser des outils centralisés, permettant l'automatisation de traitements quotidiens et offrant une vue globale et pertinente sur le système d'information.

Sécurisation des outils de prise de main à distance.

La prise de main à distance d'une ressource informatique locale ne doit être réalisable que par les agents autorisés par l'équipe locale chargée des SI, sur les ressources informatiques de leur périmètre. Des mesures de sécurité spécifiques doivent être définies et respectées.

Administration des domaines

Définir une politique de gestion des comptes du domaine.

Une politique explicite de gestion des comptes du domaine doit être documentée.

Configurer la stratégie des mots de passe des domaines.

La politique de gestion des mots de passe doit être conçue de façon à protéger contre les attaques par essais successifs de mots de passe. Une complexité minimale dans le choix des mots de passe doit être imposée aux utilisateurs.

Définir et appliquer une nomenclature des comptes du domaine.

La gestion des comptes doit s'appuyer sur une nomenclature adaptée, afin de pouvoir distinguer selon leur usage : comptes d'utilisateur standard, comptes d'administration (domaine, serveurs, postes de travail) et comptes de service.

Restreindre au maximum l'appartenance aux groupes d'administration du domaine.

L'appartenance aux groupes du domaine ADMINISTRATEURS et ADMINISTRATEURS DU DOMAINE n'est nécessaire que dans de très rares cas. Les opérations les plus courantes doivent être effectuées avec des comptes du domaine membres des groupes locaux d'administration des ordinateurs ou ayant une délégation d'administration.

Maîtriser l'utilisation des comptes de service.

Les comptes de service ont la particularité d'avoir généralement leurs mots de passe inscrits en dur dans des applications ou dans des systèmes. Afin de pouvoir être en mesure de changer ces mots de passe en urgence, il est nécessaire de maîtriser leur utilisation.

Limiter les droits des comptes de service.

Les comptes de service doivent faire l'objet d'une restriction des droits, en suivant le principe du moindre privilège.

Désactiver les comptes du domaine obsolètes.

Il est nécessaire de désactiver immédiatement, voire de supprimer, les comptes obsolètes, que ce soient des comptes d'utilisateur (administrateur, de service ou utilisateur standard) ou des comptes de machine.

Améliorer la gestion des comptes d'administrateur locaux.

Afin d'empêcher la réutilisation des empreintes d'un compte utilisateur local d'une machine à une autre, il faut soit utiliser des mots de passe différents pour les comptes locaux d'administration, soit interdire la connexion à distance via ces comptes.

Envoi en maintenance et mise au rebut

Maintenance externe.

Les données non chiffrées doivent être effacées avant l'envoi en maintenance externe de toute ressource informatique. Pour les équipements contenant des données sensibles, il doit être mis en place des mesures de rétention des supports d'information.

Mise au rebut.

Lorsqu'une ressource informatique est amenée à quitter définitivement l'organisme, les données présentes sur les disques durs ou la mémoire intégrée sont effacées de manière sécurisée ou le support d'information détruit. L'effacement des données sensibles doit s'appuyer sur des produits qualifiés, ou respecter les procédures établies en concertation avec l'ANSSI.

Lutte contre les codes malveillants

Protection contre les codes malveillants.

Des logiciels de protection contre les codes malveillants, appelés communément antivirus, doivent être installés sur l'ensemble des serveurs d'interconnexion, serveurs applicatifs et postes de travail de l'organisme.

Ces logiciels de protection doivent être distincts pour ces trois catégories au moins, et le dépouillement de leurs journaux est corrélé.

Gestion des événements de sécurité de l'antivirus.

Les événements de sécurité de l'antivirus doivent être remontés sur un serveur central pour analyse statistique et gestion des problèmes a posteriori (exemples : serveur constamment infecté, virus détecté et non éradiqué par l'antivirus, etc.).

Mise à jour de la base de signatures.

Les mises à jour des bases antivirales et des moteurs d'antivirus doivent être déployées automatiquement sur les serveurs et les postes de travail par un dispositif national prescrit par la Cnaf, validé par le RSSI.

Configuration du navigateur Internet.

Le navigateur déployé par l'équipe nationale chargée des systèmes d'information sur l'ensemble des serveurs et des postes de travail nécessitant un accès Internet ou Intranet doit être configuré de manière sécurisée (désactivation des services inutiles, nettoyage du magasin de certificats, etc.).

Mise à jour des systèmes et des logiciels

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

Le maintien dans le temps du niveau de sécurité d'un système d'information impose une gestion organisée et adaptée des mises à jour de sécurité. Un processus de gestion des correctifs propre à

chaque système ou applicatif doit être défini, et adapté suivant les contraintes et le niveau d'exposition du système.

Déploiement des correctifs de sécurité.

Les correctifs de sécurité des ressources informatiques doivent être déployés par l'équipe nationale chargée des systèmes d'information en s'appuyant sur les préconisations et outils proposés par la Cnaf.

Assurer la migration des systèmes obsolètes.

L'ensemble des logiciels utilisés sur le système d'information doivent être dans une version pour laquelle l'éditeur assure le support, et tenu à jour. En cas de défaillance du support, il convient d'en étudier l'impact et de prendre les mesures adaptées.

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

Journalisation des alertes.

Chaque système doit disposer de dispositifs de journalisation permettant de conserver une trace des événements de sécurité. Ces traces doivent être conservées de manière sûre.

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

Une politique de gestion et d'analyse des journaux de traces des événements de sécurité est définie par le RSSI, validée par l'autorité qualifiée, et mise en œuvre. Le niveau de sécurité d'un système d'information dépend en grande partie de la capacité de ses exploitants et administrateurs à détecter les erreurs, dysfonctionnements et tentatives d'accès illicites survenant sur les éléments qui le composent.

Conservation des journaux.

Les journaux des événements de sécurité doivent être conservés sur douze mois glissants, hors contraintes légales et réglementaires particulières imposant des durées de conservation spécifiques.

Objectif 23 : Défense des systèmes d'information

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

Gestion dynamique de la sécurité.

Les personnes en charge de la sécurité des systèmes d'information doivent procéder, notamment via l'analyse des journaux, à la surveillance des comportements anormaux au sein du système d'information, et à la surveillance des flux d'entrée et de sortie du système d'information.

Gestion des matériels informatiques fournis à l'utilisateur

Maîtrise des matériels.

Les postes de travail - y compris dans le cas d'une location - sont fournis à l'utilisateur par l'organisme, gérés et configurés sous la responsabilité de l'organisme. La connexion d'équipements non maîtrisés, non administrés ou non mis à jour par l'organisme (qu'il s'agisse d'ordiphones, d'équipements informatiques nomades et fixes ou de supports de stockage amovibles) sur des équipements et des réseaux professionnels est interdite.

Rappel des mesures de protection contre le vol.

Les postes fixes bénéficient des mesures de protection physique offertes au titre de la directive de sécurité physique de la présente PSSI. 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.

Déclarer les pertes et vols.

Toute perte ou vol d'une ressource d'un système d'information doit être déclarée.

Réaffectation de matériels informatiques.

Une procédure de gestion des postes et supports dans le cadre de départs de personnel ou de réaffectations à de nouveaux utilisateurs doit être mise en place et validée par le RSSI. Elle définit les conditions de recours à un effacement des données.

Nomadisme

Déclaration des équipements nomades aptes à traiter des informations sensibles.

L'autorité d'homologation du SI valide les usages possibles des équipements nomades vis-à-vis du traitement des informations sensibles ; les usages non explicitement autorisés sont interdits.

Accès à distance au système d'information de l'organisme.

Les utilisateurs distants doivent s'authentifier sur le réseau de l'organisme en utilisant une authentification forte.

Sécurisation des imprimantes et copieurs multifonctions manipulant des informations sensibles

Impression des informations sensibles.

Les impressions d'informations sensibles doivent être effectuées selon une procédure prédéfinie, garantissant le contrôle de l'utilisateur, du déclenchement de l'impression jusqu'à la récupération du support imprimé.

Sécurité des imprimantes et copieurs multifonctions.

Les imprimantes et copieurs multifonctions sont des ressources informatiques à part entière qui doivent être gérées en tant que telles. Elles ne doivent pas pouvoir communiquer directement avec l'extérieur.

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

Systèmes d'exploitation.

Les systèmes d'exploitation déployés doivent faire l'objet d'un support valide de la part d'un éditeur ou d'un prestataire de service. Seuls les services et applications nécessaires sont installés, de façon à réduire la surface d'attaque.

Une attention particulière doit être apportée aux comptes administrateurs.

Logiciels en Tiers Présentation.

La mise en œuvre d'une configuration renforcée est obligatoire sur les logiciels déployés pour le tiers présentation (ex : serveur Web, Reverse Proxy).

Logiciels en Tiers Application.

Des règles de développement sécurisé, et les configurations des logiciels en Tiers Application doivent être fixées et appliquées.

Logiciels en Tiers Données.

Des règles très strictes (restrictions d'accès, interdictions de connexions, gestion des privilèges) s'appliquent aux logiciels en tiers données.

Passerelle d'échange de fichiers.

Les échanges de fichiers entre applications doivent privilégier les protocoles sécurisés (SSL/TLS, FTPS...).

Messagerie technique.

Pour satisfaire les besoins d'exploitation et de supervision des infrastructures et des applications, une messagerie dite technique peut être déployée en zone de Back-office du centre informatique. Cette messagerie technique ne doit être en aucun cas utilisée directement par un utilisateur.

Filtrage des flux applicatifs.

De façon à garantir un niveau de sécurité satisfaisant face aux attaques informatiques, des mécanismes de filtrage et de cloisonnement doivent être mis en œuvre.

Flux d'administration.

D'une manière générale, il convient de différencier deux types de flux d'administration : les flux d'administration de l'infrastructure (réservés aux agents du centre informatique Datacenter) d'une part, les flux d'administration des applications métier (réservés à la direction métier) d'autre part. L'attribution des droits d'administration doit respecter cette différenciation, et les 2 types de flux d'administration doivent être dans la mesure du possible cloisonnés.

Service de noms de domaine – DNS technique.

Dans le cas du déploiement d'un serveur de noms de domaines pour les besoins techniques internes au centre informatique, il sera utilisé de préférence les extensions sécurisées DNSSEC.

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.

Destruction de support.

La fin de vie d'un support ou d'un matériel embarquant un support de stockage (imprimante, routeur, commutateur...) s'accompagne d'une opération de destruction avant remise au rebut.

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 emploient une référence de temps commune (service NTP, Network Time Protocol).

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.

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.

Accès aux réseaux.

Dans un centre informatique Datacenter, le contrôle physique des accès réseaux, l'attribution des adresses IP, le filtrage des informations et l'usage de dispositifs spécifiques (machines virtuelles, cartes d'administration à distance, etc.) fait l'objet de procédures sécurisées.

audit/contrôle.

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

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

Fourniture et gestion des postes de travail.

Les postes de travail utilisés dans le cadre professionnel sont fournis et gérés par l'équipe locale chargée des systèmes d'information.

Si un poste est mis à disposition par une autre voie, sa connexion au réseau est soumise à l'autorisation du RSSI.

Formalisation de la configuration des postes de travail.

Une procédure formalisée de configuration des postes de travail est établie au niveau national par la Cnaf.

Sécurité physique des postes de travail

Verrouillage de l'unité centrale des postes fixes.

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).

Verrouillage des postes portables.

Un câble physique de sécurité doit être fourni avec chaque poste portable. Les utilisateurs sont sensibilisés à son utilisation.

Réaffectation du poste et récupération d'informations

Réaffectation du poste de travail.

Une procédure définit les règles concernant le traitement à appliquer aux informations ayant été stockées ou manipulées sur les postes réaffectés.

Gestion des privilèges sur les postes de travail

Privilèges des utilisateurs sur les postes de travail.

La gestion des privilèges des utilisateurs sur leurs postes de travail doit suivre le principe du «moindre privilège» : chaque utilisateur ne dispose que des privilèges nécessaires à la conduite des actions relevant de sa mission.

Utilisation des privilèges d'accès « administrateur ».

Les privilèges d'accès « administrateur » doivent être utilisés uniquement pour les actions d'administration le nécessitant.

Gestion du compte « administrateur local ».

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

Protection des informations

Stockage des informations.

Dans la mesure du possible, les données traitées par les utilisateurs doivent être stockées sur des espaces réseau, eux-mêmes sauvegardés selon les exigences nationales.

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 doivent être fournis aux utilisateurs.

Partage de fichiers.

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

Suppression des données sur les postes partagés.

Les données présentes sur les postes partagés (portable de prêt, par exemple) doivent être supprimées entre deux utilisations, dès lors que les utilisateurs ne disposent pas du même besoin d'en connaître.

Chiffrement des données sensibles.

Une solution de chiffrement labellisée doit être mise à disposition des utilisateurs et des administrateurs afin de chiffrer les données sensibles stockées sur les postes de travail, les serveurs, les espaces de travail, ou les supports amovibles.

Fourniture de supports de stockage amovibles.

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.

Nomadisme

Accès à distance aux Systèmes d'Information de l'entité.

Les accès à distance aux SI de l'entité (accès dits « nomades ») sont réalisés via des infrastructures homologuées. L'usage de réseaux privés virtuels (VPN) de confiance est nécessaire.

Pare-feu local.

Un pare-feu local conforme aux directives nationales doit être installé sur les postes nomades.

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 informations sensibles doivent être obligatoirement chiffrées par un moyen de chiffrement labellisé au niveau national.

Filtre de confidentialité.

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

Configuration des interfaces de connexion sans fil.

La configuration des interfaces de connexion sans fil doit interdire les usages dangereux de ces interfaces.

Désactivation des interfaces de connexion sans fil.

Des règles de configuration des interfaces de connexion sans fil (Wifi, Bluetooth, 3G...), permettant d'interdire les usages non maîtrisés et d'éviter les intrusions via ces interfaces, doivent être définies et appliquées. Les interfaces sans fil ne doivent être activées qu'en cas de besoin.

Objectif 26 : Sécurisation des imprimantes et copieurs multifonctions

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

Durcissement des imprimantes et copieurs multifonctions.

Les imprimantes et copieurs multifonctions hébergés localement dans un organisme doivent faire 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.

Sécurisation de la fonction de numérisation.

Lorsqu'elle est activée, la fonction de numérisation sur les copieurs multifonctions hébergés dans un organisme doit être sécurisée. Les mesures de sécurité suivantes doivent notamment être appliquées : envoi de documents uniquement à destination d'une adresse de messagerie interne à l'entité, envoi uniquement à une seule adresse de messagerie.

Objectif 27 : Sécurisation de la téléphonie

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

Sécuriser la configuration des autocommutateurs.

Les autocommutateurs doivent être maintenus à jour au niveau des correctifs de sécurité. Leur configuration doit être durcie. La définition et l'affectation des droits d'accès et des privilèges aux utilisateurs (transfert départ-départ, entrée en tiers, interphonie, autorisation de déblocage, renvoi sur numéro extérieur, substitution, substitution de privilège, interception d'appel dirigé, etc.) doivent faire l'objet d'une attention particulière. Une revue de la programmation téléphonique doit être organisée périodiquement.

Codes d'accès téléphoniques.

Il est nécessaire de sensibiliser les utilisateurs au besoin de modifier le code d'accès de leur téléphone et de leur messagerie vocale.

Limiter l'utilisation du DECT.

Les communications réalisées au travers du protocole DECT sont susceptibles d'être interceptées, même si les mécanismes d'authentification et de chiffrement que propose ce protocole sont activés. Il est recommandé d'attribuer des postes téléphoniques filaires aux utilisateurs dont les échanges sont les plus sensibles.

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.

Un outil de vérification régulière de la conformité des éléments de configuration des postes de travail doit être mis en place, afin d'éviter une dérive dans le temps de ces éléments de configuration.

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.

Intégrer la sécurité dans les développements locaux.

Toute initiative locale de développement informatique doit respecter les exigences de sécurité des systèmes d'information, concernant la prise en compte de la sécurité dans les projets et les développements informatiques (notamment la réalisation d'une analyse de risques). Le service à l'origine du projet se porte garant d'une démarche d'homologation du système de l'application et le cas échéant de l'application du référentiel général de sécurité.

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, plusieurs clauses relatives à la sécurité des systèmes d'information doivent être intégrées :

- formation obligatoire des développeurs sur le développement sécurisé et les vulnérabilités classiques ;
- utilisation obligatoire d'outils permettant de minimiser les erreurs introduites durant le développement (outils gratuits d'analyse statique de code, utilisation de bibliothèques réputées pour leur sécurité, etc.) ;
- production de documentation technique décrivant l'implantation des protections développées (gestion de l'authentification, stockage des mots de passe, gestion des droits, chiffrement, etc.) ;
- respect de normes de développement sécurisé, qu'elles soient propres au développeur, publiques ou propres au commanditaire ;
- obligation pour le prestataire de corriger, dans un temps raisonnable et pour un prix défini, les vulnérabilités introduites durant le développement et qui lui sont remontées, en incluant automatiquement les corrections des autres occurrences des mêmes erreurs de programmation.

Objectif 30 : Développements logiciels et sécurité

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

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 impératif de limiter fortement la diffusion d'informations au sujet des produits utilisés, même si cette précaution ne constitue pas une protection en tant que telle.

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

Le fonctionnement d'une application s'appuie sur un environnement logiciel et matériel. En phases de conception et de spécification technique, il est nécessaire de s'assurer que les applications n'ont pas une trop forte adhérence vis-à-vis des environnements sur lesquels elles reposent. En effet, l'apparition de failles sur un environnement a de fait un impact sur la sécurité des applications qui en dépendent. En plus du maintien en condition de sécurité propre à l'application, il est donc nécessaire de pouvoir faire évoluer son environnement pour garantir sa sécurité dans la durée.

Instaurer des critères de développement sécurisé.

Une fois passées les phases de définition des besoins et de conception de l'architecture applicative, le niveau de sécurité d'une application dépend fortement des modalités pratiques suivies lors de sa phase de développement.

Intégrer la sécurité dans le cycle de vie logiciel.

La sécurité doit être intégrée à toutes les étapes du cycle de vie du projet, depuis l'expression des besoins jusqu'à la maintenance applicative, en passant par la rédaction du cahier des charges et les phases de recette.

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

Les développements Web (et les développements en PHP en particulier) font l'objet de problèmes de sécurité récurrents qui ont conduit à la constitution de référentiels de sécurité. Ces référentiels ont pour objectif de fixer des REGLES DE BONNES PRATIQUES à l'usage des développeurs. Ce sont des règles d'ordre générique ou pouvant être spécifiques à un langage (PHP, ASP, NET, etc.).

Calculer les empreintes de mots de passe de manière sécurisée.

Lorsqu'une application doit stocker les mots de passe de ses utilisateurs, il est important de mettre en œuvre des mesures permettant de se prémunir contre les attaques documentées : attaques par dictionnaire, attaques par tables arc-en-ciel, attaques par force brute, etc.

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.

Devant les applications à risques, il est recommandé de faire usage d'une solution tierce de filtrage applicatif.

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.

Chaînes opérationnelles SSI.

Les chaînes opérationnelles concourent à l'effort national de cybersécurité. Les alertes et les incidents sont gérés selon des procédures testées lors d'exercices.

Les situations d'urgences peuvent faire appel à des mesures définies préalablement dans le cadre des plans gouvernementaux.

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

Mobilisation en cas d'alerte.

En cas d'alerte de sécurité identifiée au niveau national, le RSSI s'assure de la bonne application des exigences formulées par les instances nationales, dans les meilleurs délais.

Remontée des incidents de sécurité rencontrés

Qualification et traitement des incidents.

La chaîne fonctionnelle SSI 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.

Remontée des incidents.

Tout incident de sécurité, même apparemment mineur, dont l'impact dépasse ou est susceptible de dépasser le système d'information de la Cnaf, fait l'objet d'un compte-rendu, via la chaîne SSI, au FSSI qui, le cas échéant, alerte le Centre opérationnel de la sécurité des systèmes d'information (COSSI) de l'ANSSI.

Continuité d'activité

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

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

Définition du plan de continuité d'activité des Systèmes d'Information.

La Cnaf définit un plan de continuité d'activité national des systèmes d'information permettant d'assurer, en cas de sinistre, la continuité d'activité des systèmes d'information.

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

Définition du plan national de continuité d'activité des systèmes d'information.

Le directeur des systèmes d'information de la Cnaf définit la structure et les attendus du plan de continuité d'activité des systèmes d'information permettant d'assurer effectivement, en cas de sinistre, la continuité d'activité.

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

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.

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.

Protection de la disponibilité des sauvegardes.

Les sauvegardes de données ne doivent pas être soumises aux mêmes risques de sinistres que les données sauvegardées.

Protection de la confidentialité des sauvegardes.

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

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

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.

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.

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.

Contrôles locaux.

La conformité à la PSSI ministérielle est vérifiée par des contrôles réguliers. 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.

Bilan annuel.

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