Référentiel Général de Sécurité

De Nouvelle-Calédonie

Table des matières

Contenu

Le présent document est une copie adaptée du RGS v2, publié à l'adresse suivante : https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/.

Le présent référentiel est pris en application de la délibération n°140/CP du 16 avril 2021 portant diverses mesures relatives à l'administration numérique (ci-après délibération RGSNC)

Chapitre 1. Mise en conformité avec les exigences réglementaires

Le référentiel général de sécurité de Nouvelle-Calédonie (RGSNC) vise à renforcer la confiance des usagers dans les services électroniques proposés par les administrations, notamment lorsque ceux-ci traitent des données personnelles. Il s'applique aux systèmes d'information mis en œuvre par les administrations dans leurs relations entre elles et avec les usagers. Il peut aussi être considéré comme un recueil de bonnes pratiques pour tous les autres organismes.

Afin de mettre leur système d'information en conformité avec le RGSNC, les administrations doivent adopter une démarche en quatre étapes, prévue par la délibération RGSNC :

1. Réalisation d'une analyse des risques ;
2. Définition des objectifs de sécurité ;
3. Choix et mise en œuvre des mesures appropriées de protection et de défense du SI ;
4. Suivi opérationnel de la sécurité du SI.

Dans l'éventualité où le système d'information serait déjà en service sans avoir fait l'objet de cette démarche, ou bien a été modifié, la procédure simplifiée suivante peut être mise en œuvre :

1. Réalisation d'un audit de la sécurité du système d'information en interne ou externalisé auprès d'un prestataire ;
2. Réalisation d'une analyse des risques simplifiée ;
3. Mise en œuvre des mesures correctives fixées dans le rapport d'audit ;
4. Suivi opérationnel de la sécurité du SI.

Au-delà des mesures techniques et organisationnelles, les administrations doivent veiller :

- Aux clauses relatives à la sécurité des contrats qu'elles passent avec des prestataires chargés de les assister dans leur démarche de sécurisation de leurs systèmes. Ces services peuvent être de nature intellectuelle (audit de la sécurité du système d'information, traitement d'incident de sécurité, notamment) ou technique (mécanisme de détection, externalisation, infogérance, mise dans le nuage de tout ou partie du système d'information, tierce maintenance applicative, etc.) ;
- Au facteur humain : la sensibilisation du personnel aux questions de sécurité est primordiale, ainsi que la formation de ceux qui interviennent plus spécifiquement dans la mise en œuvre et le suivi opérationnel de la sécurité d'information (surveillance, détection, prévention).

D'une manière générale, il est recommandé de s'appuyer sur les guides et sur la documentation produite par l'Agence Nationale de la Sécurité des Systèmes d'Information (ci-après ANSSI).

Chapitre 2. Description des étapes de la mise en conformité

2.1 Analyse des risques

L'analyse de risques précise les besoins de sécurité du système d'information en fonction de la menace et des enjeux.

La démarche d'analyse de risques consiste à identifier les évènements qui peuvent affecter la sécurité du système, d'en estimer les conséquences et les impacts potentiels puis de décider des actions à réaliser afin de réduire le risque à un niveau acceptable.

Les menaces[1] à prendre en compte sont celles qui pèsent réellement sur le système et sur les informations qu'il traite, transmet et stocke, dans l'environnement dans lequel il se situe.

Lorsque le système d'information intègre des certificats électroniques ou de l'horodatage électronique, l'analyse des risques doit permettre de décider des usages (signature, authentification, confidentialité, etc.) et des niveaux de sécurité (*, ** ou ***) qui seront mis en œuvre.

Il est recommandé de s'appuyer sur la norme ISO 27005, qui fixe un cadre théorique de la gestion des risques. Sa mise en œuvre pratique peut être facilitée par les explications et les outils, notamment logiciels, proposés par la méthode *Expression des besoins et identification des objectifs de sécurité* (EBIOS).

2.2 Définition des objectifs de sécurité

Une fois les risques appréciés, l'administration doit énoncer les objectifs de sécurité à satisfaire. Aux trois grands domaines traditionnels (disponibilité et intégrité des données et du système, confidentialité des données et des éléments critiques du système) peuvent s'ajouter deux domaines complémentaires :

- L'authentification, afin de garantir que la personne identifiée est effectivement celle qu'elle prétend être ;
- La traçabilité, afin de pouvoir associer les actions sur les données et les processus aux personnes effectivement connectées au système et ainsi permettre de déceler toute action ou tentative d'action illégitime.

Les objectifs de sécurité doivent être exprimés aussi bien en termes de protection que de défense des systèmes d'information. Les administrations peuvent s'appuyer sur le guide méthodologique EBIOS 2010, afin de formuler précisément ces objectifs de sécurité.

2.3 Choix et mise en œuvre des mesures de sécurité adaptées

L'expression des objectifs de sécurité permet d'apprécier les fonctions de sécurité qui peuvent être mises en œuvre pour les atteindre (art. 13 délibération RGSNC). Ces fonctions de sécurité sont matérialisées par le choix de moyens et de mesures de nature :

- Technique : produits de sécurité (matériels ou logiciels), prestations de services de confiance informatiques ou autres dispositifs de sécurité (blindage, détecteur d'intrusion…) ;

[1] Une menace est considérée par le ISO/CEI Guide 73 : 2002 comme une « cause potentielle d'un incident indésirable, pouvant entrainer des dommages au sein d'un système et d'un organisme ».

- Organisationnelle : organisation des responsabilités (habilitation du personnel, contrôle des accès, protection physique des éléments sensibles…), gestion des ressources humaines (affectation d'agents responsables de la gestion du système d'information, formation du personnel spécialisé, sensibilisation des utilisateurs).

Ces mesures de sécurité peuvent être sélectionnées au sein des référentiels et normes existants. Elles peuvent également en être adaptées ou bien être créées *ex nihilo*.

2.4 Suivi opérationnel de la sécurité du système d'information

Les mesures de protection d'un système d'information doivent être accompagnées d'un suivi opérationnel quotidien ainsi que de mesures de surveillance et de détection, afin de réagir au plus vite aux incidents de sécurité et de les traiter au mieux.

Le suivi opérationnel consiste à collecter et à analyser les journaux d'évènements et les alarmes, à mener des audits réguliers, à appliquer des mesures correctives après un audit ou un incident, à mettre en œuvre une chaîne d'alerte en cas d'intrusion supposée ou avérée sur le système, à gérer les droits d'accès des utilisateurs, à assurer une veille sur les menaces et les vulnérabilités, à entretenir des plans de continuité et de reprise d'activité, à sensibiliser le personnel et à gérer les crises lorsqu'elles surviennent.

Chapitre 3 Règles relatives à la cryptographie et à la protection des échanges électroniques

Les règles techniques imposées par le RGSNC portent uniquement sur la sécurisation des infrastructures utilisées pour procéder aux échanges électroniques entre les administrations et les usagers ainsi qu'entre les administrations elles-mêmes.

Le RGSNC n'impose aucune technologie particulière et laisse aux administrations le choix des mesures à mettre en œuvre. Il fixe cependant des exigences relatives à certaines fonctions de sécurité, notamment la certification et l'horodatage.

En fonction de leur besoin de sécurité, issu de l'analyse de risques, il appartient aux administrations de déterminer les fonctions de sécurité ainsi que les niveaux de sécurité associés, en s'appuyant sur les méthodes, les outils et les bonnes pratiques proposées aux chapitres 2 et 5.

Lorsqu'elles choisissent de mettre en œuvre des fonctions de sécurité traitées dans le présent chapitre, les administrations choisissent le niveau de sécurité adapté à leur besoin et appliquent les règles correspondantes décrites dans ce référentiel. Dans tous les cas, il est recommandé l'usage de produits qualifiés quand ils existent.

3.1 Règles relatives à la cryptographie

Lorsqu'elles mettent en place des mesures de sécurité comprenant des mécanismes cryptographiques, les administrations doivent respecter les règles, et si possible les recommandations, indiquées dans les annexes [RGSNC_B1] et [RGSNC_B2], communs à tous les mécanismes cryptographiques, ainsi que de l'annexe [RGSNC_B3], dédié aux mécanismes d'authentification.

3.2 Règles relatives à la protection des échanges électroniques

Les règles de sécurité à respecter pour les fonctions de sécurité d'authentification, de signature électronique, de confidentialité et d'horodatage, reposent sur l'emploi de contremarques de temps dans le cas de l'horodatage électronique et de certificats électroniques pour toutes les autres fonctions.

a) Règles relatives aux certificats électroniques

Les exigences concernant le composant « *certificat électronique* » sont décrites dans deux annexes du RGSNC appelées respectivement « *Politique de certification type – Personne physique* » ([RGSNC_A2]) et « *Politique de certification type – Services applicatifs* » ([RGSNC_A3]). Elles portent sur le contenu des certificats et sur les conditions dans lesquelles il est émis par un Prestataire de service de confiance (ci-après PSCO), et plus spécifiquement un *Prestataire de services de certification électronique* (PSCE) au sens du présent paragraphe, ainsi que sur le dispositif de stockage de la clé privée.

Le RGSNC offre la possibilité de disposer :

- des certificats mono-usage à usage d'authentification de personne physique ou de serveur, de signature, de cachet et de confidentialité pour des niveaux une étoile (*), deux étoiles (**) et trois étoiles (***) (cf. [RGSNC_A2] et [RGSNC_A3]) ;

- d'un certificat électronique unique, dit «à double usage», pour les fonctions d'authentification de personne physique et de signature électronique. Ce certificat ne peut être prévu qu'aux niveaux (*) et (**) (cf. [RGSNC_A2]).

a.1 L'authentification d'une entité par certificat électronique

L'authentification[2] a pour but de vérifier l'identité dont se réclame une personne ou une machine. La mise en œuvre par une administration des fonctions de sécurité « *Authentification* » ou « *Authentification serveur* » peut se faire selon trois niveaux de sécurité aux exigences croissantes : (*), (**) et (***).

Ces exigences, décrites dans les annexes [RGSNC_A1], couvrent, pour les trois niveaux de sécurité, l'ensemble des composants nécessaires à la mise en œuvre de cette fonction de sécurité, à savoir :

- La bi-clé et le certificat électronique dont l'usage est l'authentification ;
- Le dispositif d'authentification ;
- Le module de vérification d'authentification ;
- L'application d'authentification.

a2. La signature et le cachet électronique

La signature électronique d'une personne permet de garantir l'identité du signataire, l'intégrité du document signé et le lien entre le document signé et la signature. Elle traduit ainsi la manifestation du consentement du signataire quant au contenu des informations signées.

Dans le cas des échanges dématérialisés faisant intervenir des services applicatifs, la fonction de « *cachet* » permet de garantir l'intégrité des informations échangées et l'identification du service ayant « cacheté » ces informations. Cette fonction de « *cachet* » est, pour une machine, l'équivalent de la fonction signature pour une personne.

La mise en œuvre par une administration des fonctions de sécurité « *Signature électronique* » ou « *cachet* » peut se faire selon trois niveaux de sécurité aux exigences croissantes : (*), (**) et (***). Ces exigences, décrites dans l'annexe [RGSNC_A1], couvrent, pour les trois niveaux de sécurité, l'ensemble des composants nécessaires à la mise en œuvre de cette fonction de sécurité, à savoir :

- La bi-clé et le certificat électronique dont l'usage est la signature électronique ou le cachet ;
- Le dispositif de création de signature électronique ou de cachet ;
- L'application de création de signature électronique ou de cachet ;
- Le module de vérification de signature électronique ou de cachet.

Cas particulier de la signature « présumée fiable » au sens de l'article 1316-4 du code civil :

Les exigences techniques définies en annexe de l'arrêté du 26 juillet 2004, et portant sur la délivrance de certificats électroniques dits « qualifiés » au sens du décret n°2001-272 du 30 mars 2001, sont requises pour la génération de signatures électroniques « présumées fiables » au sens de ce décret.

Ces exigences constituent un sous-ensemble de celles contenues dans le document [RGSNC_A2] pour le niveau de sécurité (***) de la fonction signature électronique, qui prévoit des exigences supplémentaires, essentiellement en matière de format et de variables de temps.

[2] S'identifier consiste à communiquer une identité préalablement enregistrée, s'authentifier consiste à apporter la preuve de cette identité. L'authentification est généralement précédée d'une identification.

De ce fait, une signature électronique sécurisée au sens de l'article 1er du décret n°2001-272 du 30 septembre 2001, établie avec un dispositif sécurisé de création de signature certifié conforme dans les conditions de l'article 3 et mettant en œuvre des certificats de signature électronique conformes au niveau de sécurité (***) de [RGSNC_A2] est *de facto* « présumée fiable » selon ce décret et donc au sens de l'article 1316-4 du code civil.

a3. La confidentialité

Le chiffrement constitue le mécanisme essentiel de protection de la confidentialité. Cependant, la confidentialité des informations peut aussi être protégée par des mesures complémentaires de gestion des droits d'accès de chacun (en lecture, en écriture ou en modification) aux données contenues dans le système d'information. A cet effet, il est recommandé de mettre en place des mécanismes techniques afin de s'assurer que seules les personnes autorisées puissent accéder aux données en fonction de leur besoin d'en connaître. Ces mécanismes doivent être robustes et implémentés au plus près du lieu de stockage des données.

La mise en œuvre par une administration de la fonction de sécurité « *confidentialité* » peut se faire selon trois niveaux de sécurité aux exigences croissantes : (*), (**) et (***).

Ces exigences, décrites dans l'annexe [RGSNC_A1], couvrent, pour les trois niveaux de sécurité, l'ensemble des composants nécessaires à la mise en œuvre de cette fonction de sécurité à savoir :

- La bi-clé et le certificat électronique dont l'usage est le chiffrement ;
- Le dispositif de chiffrement ;
- Le module de chiffrement ;
- Le module de déchiffrement.

b. Règles relatives à l'horodatage électronique

Les exigences concernant le composant « *contremarque de temps* » sont décrites dans l'annexe du RGS « *Politique d'horodatage type* » ([RGSNC_A5]). Elles portent sur le contenu des contremarques de temps et sur les conditions dans lesquelles il est émis par un PSCO, et plus spécifiquement d'un *Prestataire de services d'horodatage électronique* (ci-après PSHE) au sens du présent paragraphe.

Une fonction d'horodatage permet d'attester qu'une donnée sous forme électronique existe à un instant donné. Cette fonction met en œuvre une contremarque de temps générée à l'aide d'un mécanisme cryptographique respectant les règles et, si possible, les recommandations contenues dans les référentiels [RGSNC_B1] et [RGSNC_B2].

Cette contremarque, délivrée par un PSHE, doit respecter les exigences de l'annexe [RGSNC_A5] appelée « *Politique d'horodatage type* ». Cette annexe ne distingue qu'un niveau unique de sécurité, auquel les administrations doivent se conformer dès lors qu'elles souhaitent mettre en œuvre la fonction d'horodatage électronique au sein de leur système d'information.

Chapitre 4 Qualification des produits de sécurité et des prestataires de services de confiance

Conformément à l'article 14 de la délibération RGSNC, les administrations qui décident de recourir à des produits ou des services visés par le RGSNC recourent, lorsque cela est possible, à des produits de sécurité et à des PSCO qualifiés.

4.1 Qualification des produits de sécurité

La qualification de produits de sécurité prévoit trois niveaux de qualification :

- Qualification *élémentaire* (décrite dans le document QE) ;
- Qualification *standard* (décrite dans le document QS) ;
- Qualification *renforcée* (décrite dans le document QR).

Un produit de sécurité est qualifié s'il a fait l'objet d'une attestation de qualification et d'un maintien de conditions de sécurité conforme aux procédures décrites dans les documents QE, QS et QR.

Pour garantir la cohérence des objectifs et des exigences de sécurité, il est recommandé que la cible de sécurité soit, autant que possible, conforme à un des profils de protection proposés par l'ANSSI (www.ssi.gouv.fr/fr/certification-qualification/cc/profils-de-protection/). L'ANSSI publie également le catalogue des produits de sécurité qualifiés : www.ssi.gouv.fr/fr/produits-et-prestataires/produits-qualifies/.

4.2 Qualification des prestataires de services de confiance (PSCO)

Les prestataires de services peuvent éventuellement appartenir à plusieurs catégories distinctes de PSCO. Ils doivent alors obtenir une qualification pour chaque type de prestation dans les conditions de l'article 14 de la délibération RGSNC.

La liste des organismes de qualification habilités et des PSCO qualifiés est publiée par l'ANSSI : www.ssi.gouv.fr/fr/produits-et-prestataires/prestataires-de-services-de-confiance-qualifies/.

Les catégories de PSCO visées dans la présente version du RGS sont :

a. Les prestataires de services de certification électronique

Les référentiels d'exigences applicables aux PSCE figurent en annexes A2 et A3, respectivement appelées « *politique de certification type – certificats électroniques de personnes* » et « *politique de certification type – certificats électroniques de services applicatifs* ».

Ces référentiels distinguent trois niveaux de sécurité, aux exigences croissantes : (*), (**) et (***). Ils visent distinctement les usages de chiffrement, d'authentification de personne, de signature électronique, d'authentification de machine et de cachet, ainsi que le double usage authentification et signature électronique.

Il est recommandé que les PSCE réalisent les démarches nécessaires à l'intégration de leurs certificats dans les principaux navigateurs.

b. Les prestataires de services d'horodatage électronique

Le référentiel d'exigences applicable aux PSHE, qui prévoit un niveau de sécurité unique, figure en annexe A5, appelée « *politique d'horodatage type* ».

Chapitre 5 Recommandations relatives à l'application du référentiel

Au-delà de l'analyse de risques, il est recommandé d'adopter de bonnes pratiques, de manière progressive, relatives à la méthodologie, aux procédures et à l'organisation.

5.1 Organiser la sécurité des systèmes d'information

a. Organiser les responsabilités liées à la sécurité des systèmes d'information

Les administrations doivent mettre en œuvre une organisation qui endosse les responsabilités liées à la sécurité des systèmes d'information.

De préférence dirigée par un représentant de l'administration, cette organisation doit disposer des moyens matériels nécessaires à la réalisation de ses missions et de la capacité à gérer les risques, les crises ou les incidents qui pourraient en résulter. De manière progressive et le cas échéant, l'administration met en œuvre et s'appuie sur une chaîne fonctionnelle SSI chargée de l'assister dans le pilotage, la gestion et le suivi des moyens SSI : le responsable de la sécurité des systèmes d'information (RSSI), l'officier de la sécurité des systèmes d'information (OSSI), le correspondants SSI, etc.

Éventuellement à l'aide de la chaîne fonctionnelle SSI, l'organisation mise en place par l'administration peut assurer les missions suivantes :

- Coordination des actions permettant l'intégration des clauses liées à la SSI dans les contrats ou les conventions impliquant un accès par des tiers à des informations ou à des ressources informatiques ;
- Formalisation de la répartition des responsabilités liées à la SSI (définition des périmètres de responsabilité, des délégations de compétences, etc.) ;
- Établissement des relations nécessaires avec les autorités externes de défense des systèmes d'information, notamment pour la gestion des intrusions et des attaques sur les systèmes.

b. Mettre en place un système de management de la sécurité des systèmes d'information

Il est recommandé de mettre en œuvre des processus permettant de rechercher une amélioration constante de la SSI. Par exemple, la mise en place d'un système de management de la sécurité de l'information, tel que défini dans la norme ISO 27001, permet non seulement de planifier et de mettre en œuvre les mesures de protection du système d'information, mais également d'en vérifier la pertinence et la conformité par rapport aux objectifs établis.

c. Elaborer une politique de sécurité des systèmes d'information

Il est recommandé d'élaborer et de formaliser une politique de sécurité des systèmes d'information (PSSI). Elle peut être générale ou déclinée en fonction des besoins spécifiques de chaque domaine de chaque système d'information. Le guide « *Politique SSI* » de l'ANSSI fournit une aide pour élaboration.

5.2 Impliquer les instances décisionnelles

Les instances décisionnelles des administrations doivent être impliquées dans la sécurisation des systèmes d'information dont elles ont in fine la responsabilité, afin de donner les orientations

adéquates, notamment en termes d'investissement humain et financier, et de valider les objectifs de sécurité et les orientations stratégiques. La norme ISO 27001 fournit, à titre indicatif, une liste de sujets susceptibles d'être traités au niveau de la direction d'une administration.

5.3 Adapter l'effort de protection des systèmes d'information aux enjeux de sécurité et prendre en compte la SSI dans les projets

La sécurité d'un système d'information doit être adaptée aux enjeux du système lui-même et aux besoins de sécurité de l'administration, afin d'y consacrer les moyens financiers et humains nécessaires et suffisants. Dans ce but, il est recommandé d'utiliser les guides de l'ANSSI « Maturité SSI » et « Gestion et intégration de la SSI dans les projets » (GISSIP). Ils permettent, dans le cadre du développement d'un projet de système d'information, de déterminer les enjeux relatifs à la sécurité et d'identifier l'ensemble des livrables relatifs à la SSI.

5.4 Adopter une démarche globale

L'ensemble de la démarche de sécurisation des systèmes d'information doit procéder d'une volonté cohérente et globale, afin d'éviter la dispersion des efforts des équipes en charge de la SSI ou la mise en œuvre de mesures de sécurité parcellaires. Chaque décision doit être prise au juste niveau hiérarchique. Il est ainsi recommandé :

- De prendre en considération tous les aspects qui peuvent affecter la SSI, qu'ils soient techniques (matériels, logiciels, réseaux) ou non (organisations, infrastructure, personnel) ;
- D'envisager tous les risques et menaces, quelle que soit leur origine ;
- de prendre en compte la SSI à tous les niveaux hiérarchiques. La SSI repose sur une vision stratégique et nécessite des choix d'autorité (enjeux, moyens humaines et financiers, risques résiduels acceptés) ainsi qu'un contrôle des actions et de leur légitimité ;
- De responsabiliser tous les acteurs (décideurs, maîtrise d'ouvrage et d'œuvre, utilisateurs) ;
- D'intégrer la SSI tout au long du cycle de vie des systèmes d'information (depuis l'étude d'opportunité jusqu'à la fin de vie du système).

D'une manière similaire, la sécurité doit être prise en compte dès la phase de définition des objectifs fonctionnels des systèmes d'information, afin de :

- Limiter les surcoûts inhérents à l'application tardive de mesures de sécurité ;
- Garantir l'efficacité des mesures mises en œuvre ;
- Favoriser l'appropriation de la sécurité par les équipes en charge du SI.

5.5 Informer et sensibiliser le personnel

Dans la mesure du possible, l'ensemble des agents d'une administration, et le cas échéant les contractants et les utilisateurs tiers, doivent suivre une formation adaptée sur la sensibilisation et recevoir régulièrement les mises à jour des politiques et des procédures qui concernent leurs missions. Cette formation doit permettre de réduire les risques liés à la méconnaissance des principes de base et des règles élémentaires de bonne utilisation de l'outil informatique.

La sensibilisation du personnel doit être régulière. A cet effet, l'ANSSI publie des bonnes pratiques pour l'application de principes de base en matière de sécurité des systèmes d'information : www.ssi.gouv.fr/fr/bonnes-pratiques/principes-généraux.

5.6 Prendre en compte la sécurité dans les contrats et les achats

Les exigences de sécurité relatives aux produits ou aux prestations acquis doivent faire l'objet d'une étude et doivent être clairement formalisées et intégrées dans les dossiers d'appels d'offres, au même titre que les exigences fonctionnelles, réglementaires, de performance ou de qualité.

Ces exigences peuvent concerner le système qui fait l'objet de la consultation, mais aussi la gestion du projet lui-même (formation ou habilitation des personnels), en incluant les phases opérationnelles et de maintenance. Il convient notamment de :

- Veiller à intégrer aux règlements de consultation ou aux cahiers des charges les référentiels de l'ANSSI applicables (produits certifiées, qualifiés, agréés…) ;
- Demander, le cas échéant, à ce que les produits de sécurité soient fournis avec l'ensemble des éléments permettant d'en apprécier le niveau de sécurité ;
- Préciser les clauses relatives à la maintenance des produits acquis ;
- Préciser les clauses concernant les conditions de l'intervention et de l'accès physique et logique des sous-traitants ;
- Préciser les clauses garantissant la qualité et la sécurité des prestations et produits fournis ;
- Préciser les conditions de propriété des codes sources ;
- Prévoir, le cas échéant, la réversibilité des prestations et la portabilité des données générées pendant celles-ci en s'assurant en particulier que les bases de données sont extractibles, que celle-ci peut être distinguée du système lui-même et que les formats utilisés sont ouverts ;
- Préciser la nature et les modalités de réalisation des tableaux de bord et mécanismes de suivi des prestations de sécurité ;
- Prévoir les modalités de réaction aux crises et aux incidents susceptibles d'affecter le système ;
- Prévoir les modalités de réaction aux crises et aux incidents susceptibles d'affecter le système ;
- Prévoir des points de contact compétents à même de répondre aux besoins des administrations ;
- Vérifier, dans les réponses à appel d'offres, la couverture des exigences de sécurité inscrites dans la consultation.

Une attention particulière devra être portée aux mécanismes de validation et de recette des composants mettant en œuvre les exigences de sécurité.

5.7 Prendre en compte la sécurité dans les projets d'externalisation et d'information en nuage

Le recours à l'externalisation ou à « l'informatique en nuage » présente des risques spécifiques qu'il convient d'évaluer avant d'aborder une telle démarche. Ces risques peuvent être liés au contexte même de l'opération d'externalisation ou à des spécifications contractuelles déficientes ou incomplètes. Dans cette hypothèse il est recommandé d'appliquer les prescriptions décrites dans le guide de l'ANSSI « Maîtriser les risques de l'infogérance – Externalisation des systèmes d'information ». Ce guide fournit :

- Une démarche cohérente de prise en compte des aspects SSI lors de la rédaction du cahier des charges d'une opération d'externalisation ;

- Un ensemble de clauses types ainsi qu'une base d'exigences de sécurité, à adapter et à personnaliser en fonction du contexte particulier de chaque projet d'externalisation.

5.8 Mettre en place des mécanismes de défense des systèmes d'information

En complément des mécanismes de protection des systèmes d'information, et en fonction de leurs enjeux de sécurité, les administrations doivent adopter des mesures complémentaires relatives à la défense des systèmes d'information. Ces mesures consistent, en particulier, à assurer :

- La connaissance des systèmes exploités par l'administration, ou en relation avec elle (cartographie des SI, répertoire des interconnexions, etc.) ;
- La détection des malveillances, des erreurs et des imprudences, en périphéries ou à l'intérieur des systèmes d'informations des administrations ;
- La traçabilité des actions et des accès réalisés sur les systèmes d'information (journalisation, notamment) ;
- La pérennisation des savoir-faire et des compétences, notamment en termes d'exploitation des SI ;
- La conservation de la preuve des infractions découvertes.

5.9 Utiliser les produits et prestataires labellisés pour leur sécurité

La qualification est un label qui permet d'attester de la confiance que l'on peut accorder à des produits de sécurité et à des PSCO, ainsi que de leur conformité aux règles du RGS qui leurs sont applicables. D'autres labels existent pour attester de la compétence des professionnels, notamment en matière de SSI.

Il est recommandé :

- D'utiliser chaque fois que possible des produits de sécurité qualifiés (§5.1) par l'ANSSI ;
- De recourir chaque fois que possible à des PSCO qualifiés (§5.2) ;
- De prendre en considération, pour le choix des prestataires, en plus de leur qualification, leur éventuelle certification selon la norme ISO 27001 ou d'autres normes équivalentes ;
- De prendre en considération, pour le choix de prestataires, la certification de leurs personnels lorsque des compétences particulières sont requises pour une fonction.

5.10 Élaborer des plans de traitement d'incidents ainsi que de continuité et de reprise d'activité

Les autorités doivent se préparer à faire face à des incidents de sécurité pour lesquels toutes les mesures préventives auraient échoué. A ce titre, elles doivent mettre en œuvre, dans la mesure du possible, un *plan de continuité d'activité* et un *plan de reprise d'activité* qui identifient les moyens et les procédures nécessaires pour revenir à une situation nominale le plus rapidement possible, en cas d'incident grave. Ces documents doivent être régulièrement mis à jour. Les plans et les procédures qui en découlent doivent faire l'objet de tests réguliers.

5.11 Procéder à des audits réguliers de la sécurité du système d'information

Dans la mesure du possible, les administrations doivent réaliser ou faire réaliser des audits réguliers de leurs SI.

5.12 Réaliser une veille sur les menaces et les vulnérabilités

Se tenir informé sur l'évolution des menaces et des vulnérabilités, en identifiant les incidents qu'elles favorisent ainsi que leurs impacts potentiels, constitue une mesure fondamentale de défense. Les sites institutionnels, comme celui du CERT-FR (www.cert.ssi.gouv.fr), ou ceux des éditeurs de logiciels et de matériels constituent des sources d'information essentielles sur les vulnérabilités identifiées, ainsi que sur les contre-mesures et les correctifs éventuels. Les mises à jour des logiciels et d'autres équipements, les correctifs des systèmes d'exploitation et des applications font l'objet d'alertes et d'avis qu'il est indispensable de suivre.

5.13 Favoriser l'interopérabilité

L'administration électronique ne saurait évoluer sans une prise en compte des règles relatives à l'interopérabilité et à la mise en cohérence des différents systèmes d'information des administrations et de leurs partenaires (usagers, acteurs industriels, etc.). L'interopérabilité est en particulier traitée à travers le Référentiel général d'interopérabilité de Nouvelle-Calédonie.

Chapitre 6 : Liste des annexes du RGS

Les annexes contiennent les règles relatives aux mécanismes cryptographiques mis en œuvre dans les fonctions de sécurité traitées au chapitre 4 ainsi que celles applicables aux différentes catégories de prestataires de services de confiance. Ces documents sont consultables à l'adresse https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/ .

6.1 Documents applicables concernant l'utilisation de certificats électroniques

[RGSNC_A1] **–** voir l'annexe [RGS_A1] Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques, version 3.0, en vigueur en métropole en vertu du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les administrations et entre les administrations et de l'arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques

[RGSNC_A2] **-** voir l'annexe [RGS_A2] Politique de Certification Type "certificats électroniques de personne", version 3.0, en vigueur en métropole en vertu du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les administrations et entre les administrations et de l'arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques

[RGSNC_A3] **-** voir l'annexe [RGS_A3] Politique de Certification Type "services applicatifs", version 3.0, en vigueur en métropole en vertu du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les administrations et entre les administrations et de l'arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques, ensemble avec le **[RGS_A3] - Errata Horodatage électronique**

[RGSNC_A4] **-** voir l'annexe [RGS_A4] Profils de certificats, CRL, OCSP et algorithmes cryptographiques, version 3.0, en vigueur en métropole en vertu du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les administrations et entre les administrations et de l'arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques

[RGSNC_A5] **-** voir l'annexe [RGS_A5] Politique d'Horodatage Type, version 3.0, en vigueur en métropole en vertu du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les administrations et entre les administrations et de l'arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques

6.2 Documents applicables concernant l'utilisation de mécanismes cryptographiques

[RGSNC_B1] **-** voir l'annexe [RGS_B1] Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03, en vigueur en métropole en vertu du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les administrations et entre les administrations et de l'arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques

[RGSNC_B2] **-** voir l'annexe [RGS_B2] Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.0, en vigueur en métropole en vertu du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les administrations et entre les administrations et de l'arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques

[RGSNC_B3] **-** voir l'annexe [RGS_B3] Règles et recommandations concernant les mécanismes d'authentification, version 1.0, en vigueur en métropole en vertu du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les administrations et entre les administrations et de l'arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques