



POLITIQUE DE SÉCURITÉ  
DES SYSTÈMES D'INFORMATION  
DE LA DGAC

**NIVEAU 1**

**STRATÉGIQUE  
PRINCIPES GÉNÉRAUX**

Version 0\_5 du 21 mars 2017

HISTORIQUE DES VERSIONS			
06 décembre 2016	V1_0	Première version adressée aux services métier	Jean-Luc Villegente Jean Carlioz
28 novembre 2016	Vβ_4	Évolution du document	Jean-Luc Villegente
06 - 20 octobre 2016	Vβ_0xx	Versions initiales de travail	Jean Carlioz
28 février 2017	Vβ_0.2	Versions initiales de travail	Jean-Luc Villegente Jean Carlioz
28 février 2017	Vβ_0.3	Versions initiales de travail	Jean-Luc Villegente Jean Carlioz
14 mars 2017	Vβ_0.4	Versions initiales de travail	Jean-Luc Villegente
21 mars 2017	Vβ_0.5	Versions initiales de travail	Jean-Luc Villegente

Les commentaires sur le présent document  
Doivent être adressés à :

Jean Carlioz  
RSSI / DGAC  
50 rue Henry Farman  
75 720 – Paris Cedex 15  
[jean.carlioz@aviation-civile.gouv.fr](mailto:jean.carlioz@aviation-civile.gouv.fr)

# Tables des matières

## PSSI – Niveau 1

<b>I. PSSI DGAC NIVEAU 1</b>	<b>5</b>
<b>A. OBJET</b>	<b>6</b>
OBJECTIF DE LA PSSI	6
OBJET DU NIVEAU 1 DE LA PSSI	6
<b>B. DOMAINE D'APPLICATION ET PERIMETRES</b>	<b>6</b>
<b>C. ENJEUX DE SECURITE</b>	<b>6</b>
<b>D. VALIDATION ET MISE EN ŒUVRE DE LA PSSI</b>	<b>7</b>
<b>E. PRINCIPES D'ORGANISATION</b>	<b>7</b>
<b>F. PRINCIPES GENERAUX DE SECURITE</b>	<b>8</b>
PRINCIPE 1 - ANALYSE DE RISQUES	8
PRINCIPE 2 - OBJECTIFS DE SECURITE ET REGLES APPLICABLES	9
PRINCIPE 3 - CARTOGRAPHIE DES SYSTEMES	9
PRINCIPE 4 - AUTHENTIFICATION FORTE	9
PRINCIPE 5 - ADMINISTRATION – REGLES RENFORCEES ; TRAÇABILITE ET CONTROLES	9
PRINCIPE 6 - FORMATION ET CONTROLE DES ADMINISTRATEURS	9
PRINCIPE 7 - CHIFFREMENT ET HEBERGEMENT DES DONNEES SENSIBLES	9
PRINCIPE 8 - DROITS ET DEVOIRS DES AGENTS - INFORMATION ET SENSIBILISATION	9
PRINCIPE 9 - PLANIFICATION ET QUANTIFICATION DES MOYENS SSI	9
PRINCIPE 10 - LABELLISATION DES PRODUITS ET SERVICES SSI	9
PRINCIPE 11 - PRESTATAIRES DE CONFIANCE	9
<b>G. BIENS ESSENTIELS</b>	<b>10</b>
<b>H. PRINCIPAUX RISQUES</b>	<b>10</b>
<b>I. OBJECTIFS DE SECURITE</b>	<b>10</b>
ORGANISATION	11
RESSOURCES HUMAINES	11
GESTION DES BIENS	11
INTEGRATION DE LA SSI DANS LE CYCLE DE VIE DES SYSTEMES D'INFORMATION	11
SECURITE PHYSIQUE	12
SECURITE DES RESEAUX	12
ARCHITECTURE DES SI	13
EXPLOITATION DES SI	13
SECURITE DU POSTE DE TRAVAIL	14
SECURITE DU DEVELOPPEMENT DES SYSTEMES	14
TRAITEMENT DES INCIDENTS	15
CONTINUITE D'ACTIVITE	15
CONFORMITE, AUDITS, INSPECTIONS, CONTROLES	15
<b>J. ACTEURS</b>	<b>15</b>
AQSSI	16

RSSI	16
RSSI OPERATEUR	16
AUTORITE DE SURVEILLANCE	16
ASSI	17
EXPLOITANT DES SYSTEMES D'INFORMATION	17
ADMINISTRATEUR SYSTEME	17
CHEF DE PROJET – MAITRISE D'OUVRAGE (MOA)	17
CHEF DE PROJET – MAITRISE D'OEUVRE (MOE)	17
<b>K. COMITOLOGIE</b>	<b>18</b>
<b>L. SUIVI DE LA PSSI</b>	<b>18</b>
<b>M. VALIDATION ET DIFFUSION DE CETTE POLITIQUE</b>	<b>18</b>
<b>N. REFERENTIELS INTERNES</b>	<b>19</b>
<b>O. REFERENTIELS EXTERNES</b>	<b>19</b>

## I. PSSI DGAC NIVEAU 1

### Préambule

L'essentiel de l'activité de la DGAC repose aujourd'hui sur les systèmes d'information.

La sécurité des systèmes d'information du transport aérien s'opère dans un environnement complexe : ces systèmes sont distribués, interconnectés, soumis à une cybermenace élevée et fortement évolutive. Ils véhiculent et traitent des flux d'origine, de formats et de sensibilités très divers.

Ces derniers constituent ainsi une ressource à protéger : l'ensemble de leurs composants doit rester à tout moment **disponible** et performant. **L'intégrité** des données qu'elles hébergent doit être garantie, leur **confidentialité** respectée. Leur utilisation doit être **traçable** et **conforme** aux dispositions réglementaires et aux obligations juridiques.

Pour garantir la sécurité de ses systèmes et adapter son dispositif à de telles conditions, la DGAC doit - en permanence et pour chaque périmètre concerné - définir les principes de sécurité, **évaluer les risques** auxquels ils sont exposés, et maîtriser ces risques afin de protéger les biens essentiels conformément aux objectifs de sécurité définis par les métiers.

De plus, la DGAC est classé OIV (Opérateur d'Importance Vitale). La Loi de Programmation Militaire 2014-2019 impose aux opérateurs d'appliquer des directives de sécurité, et prévoit des contraintes pénales en cas de non-respect de ces obligations.

Les objectifs de sécurité, et les dispositions prises pour les atteindre, sont réunis dans cette PSSI (Politique de Sécurité des Systèmes d'Information) : elle vise à décrire l'organisation de leur mise en oeuvre et préciser les exigences applicables afin d'assurer la maîtrise des risques.

Préalablement à cette PSSI, **une analyse de risques** a permis d'évaluer la nature des cyber menaces et leur niveau de pertinence dans le contexte d'emploi des systèmes d'information de la DGAC. Cette démarche de sécurité s'accompagne d'une veille constante des vulnérabilités, et la mise en place **d'audits, de contrôles** et d'actes de surveillance permanents.

Ainsi, cette PSSI précise les exigences de sécurité devant être appliquées par tous les utilisateurs des systèmes d'information de la DGAC, permettant ainsi de protéger les systèmes (informations, industriels) aux niveaux convenus et d'agir dans **les meilleures conditions face à d'éventuels incidents** de sécurité.

Les dispositions de cette PSSI sont présentées, selon leur portée, en trois niveaux : **stratégique, pilotage et opérationnel**. Cette organisation est destinée à faciliter l'appropriation de ce référentiel de sécurité en fonction des attentes de chaque utilisateur.

## A. Objet

### Objectif de la PSSI

La politique de sécurité des systèmes d'information de la DGAC est le document auquel se réfère l'ensemble des dispositions visant à :

- Assurer la continuité de ses activités ;
- Protéger les informations et les procédures hébergées par les systèmes d'information ;
- Garantir leur conformité légale et réglementaire ;
- Préparer la résolution des incidents de sécurité.

### Objet du niveau 1 de la PSSI

Le niveau 1 de la Politique de Sécurité des Systèmes d'Information (PSSI) de la DGAC, nommé « niveau stratégique », précise :

- Les principes d'**organisation** adoptés pour la mise en œuvre de la sécurité des systèmes d'information (SI) ;
- Les principes généraux **de sécurité applicables** à l'ensemble des systèmes de la DGAC ;
- Les **objectifs de sécurité**, en fonction des risques identifiés, de la stratégie pour les maîtriser et du périmètre dans lequel opèrent les systèmes considérés ;
- Les différents **acteurs** dédiés à la mise en œuvre de la sécurité des SI.

## B. Domaine d'application et périmètres

La PSSI de la DGAC s'applique à tous les systèmes d'information (SI) de la DGAC.

La PSSI de la DGAC concerne l'ensemble des personnes physiques ou morales intervenant dans ces SI, qu'il s'agisse des administrations de la DGAC et de leurs agents ou bien de tiers (prestataires ou sous-traitants) et de leurs employés.

La PSSI de la DGAC ne s'impose pas aux systèmes aptes à traiter des informations classifiées de défense, soumis à un corpus réglementaire spécifique.

La PSSI adresse l'ensemble des systèmes de la DGAC ; cependant, les spécificités des systèmes de chaque périmètre imposent des mesures et des exigences adaptées. S'ils font l'objet d'objectifs de sécurité communs (**niveau stratégique**), ils sont soumis à des règles organisationnelles adaptées (**niveau pilotage**) et à des exigences applicables spécifiques (**niveau opérationnel**).

## C. Enjeux de sécurité

La DGAC opère dans un secteur d'activité sensible. Celle-ci repose sur l'emploi des nouvelles technologies de l'information, qui y occupent ainsi un rôle essentiel.

La protection de ces activités sensibles, et, partant, la maîtrise des risques auxquels sont exposés les systèmes sur lesquels elles reposent, doivent répondre aux enjeux de sécurité suivants :

- La capacité à maintenir la **continuité des activités essentielles de la DGAC** (périmètre Navigation Aérienne - NA) ;
- La **protection du patrimoine informationnel** le plus sensible (périmètre Système d'Information Général – SIG) ;
- La mise en place d'une organisation de la sécurité adaptée aux besoins opérationnels et stratégiques (comitologie, rôles et missions, processus dédiés à la sécurité).

La démarche de sécurité des systèmes d'information est orientée vers une **maîtrise des risques** contrôlée où le coût de la sécurité répond aux besoins des métiers tout en étant adapté aux cybermenaces actuelles.

#### D. Validation et mise en œuvre de la PSSI

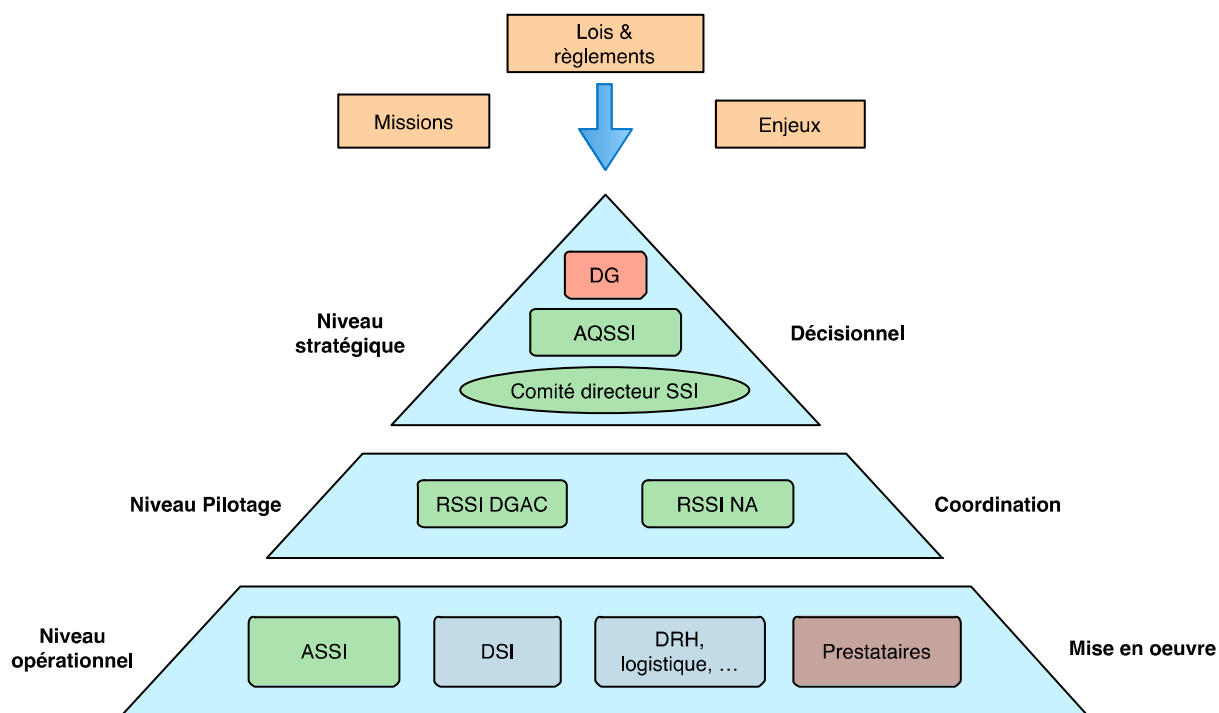
Cette démarche concerne les activités et biens essentiels de la DGAC. A ce titre, l'organisation répondant aux objectifs et l'identification des exigences de sécurité applicables dans le cadre de la maîtrise des risques procèdent d'une décision d'autorité.

Ainsi, la PSSI de la DGAC ayant vocation à s'appliquer à l'ensembles de ses services, est validée et mise en oeuvre par une décision du Directeur Général de l'Aviation Civile.

#### E. Principes d'organisation

L'organisation de la sécurité des systèmes d'information repose sur trois piliers :

- **Niveau Stratégique** et décisionnel, où s'élabore la conduite de la Politique de Sécurité des Systèmes d'Information [PSSI], répondant aux enjeux et missions de de la DGAC (alignement stratégique), en conformité avec la réglementation en vigueur.  
Le Comité Directeur SSI [CDSSI] sous l'autorité de la Direction Générale en assure la gouvernance.
- **Niveau Pilotage**, où s'opèrent la conduite et la coordination de l'application de la PSSI.  
Le RSSI de la DGAC et le RSSI de l'opérateur de la navigation aérienne en sont les garants. L'autorité de surveillance assure conjointement le contrôle du niveau de sécurité.
- **Niveau Opérationnel**, chargé de la mise en oeuvre de la PSSI et de la définition des exigences de sécurité.  
Les ASSI, les AIG, certaines Directions métiers (RH, Logistique, ...) et les prestataires en charge de la sécurité, assurent la mise en œuvre des actions opérationnelles.



*Schéma de l'organisation générale de la sécurité et de la PSSI*

## F. Principes généraux de sécurité

Quels que soient les systèmes (opérationnels, de gestion, ou de support), ils se réfèrent en permanence aux principes généraux énoncés ci-après.

Contrairement aux règles et exigences de sécurité qui existent en fonction d'objectifs déduits des analyses de risques, spécifiques aux périmètres des systèmes considérés, les objectifs principaux de sécurité sont valables sur l'ensemble des systèmes d'information de la DGAC.

### Principe 1 - Analyse de risques

Tout système d'information de la DGAC fait l'objet d'une analyse de risques, permettant une prise en compte préventive de sa sécurité, adaptée aux enjeux du système considéré.

Cette analyse s'inscrit dans une démarche d'amélioration continue de la sécurité du système, pendant toute sa durée de vie.



**Principe 2 - Objectifs de sécurité et règles applicables**

Tout système d'information de la DGAC fait l'objet d'objectifs de sécurité, issus d'une analyse de risques. Ces objectifs sont traduits en règles applicables.

**Principe 3 - Cartographie des systèmes**

Chaque entité utilisant ou exploitant un système d'information de la DGAC doit en établir la cartographie.

Tout nouveau système d'information de la DGAC doit être intégré dans la cartographie générale des SI, contribuant ainsi à sa mise à jour.

**Principe 4 - Authentification forte**

Des moyens d'authentification forte des agents de la DGAC sont mis en place, si nécessaire, sur les systèmes d'information en adéquation avec les besoins de sécurité.

**Principe 5 - Administration – Règles renforcées ; traçabilité et contrôles**

Toute opération de gestion et d'administration des systèmes d'information de la DGAC est tracée selon un cadre légal et réglementaire et contrôlée régulièrement.

**Principe 6 - Formation et contrôle des administrateurs**

Tout administrateur d'un système d'information de la DGAC est sensibilisé et formé. Il maintient à jour ses compétences qui font l'objet de contrôles obligatoires et réguliers.

**Principe 7 - Chiffrement et hébergement des données sensibles**

Toute donnée sensible est chiffrée et hébergée par les ressources internes de la DGAC.

**Principe 8 - Droits et devoirs des agents - Information et sensibilisation**

Chaque utilisateur d'un système d'information de la DGAC doit être formé, sensibilisé à la cybersécurité et être informé de ses droits et devoirs.

**Principe 9 - Planification et quantification des moyens SSI**

Les moyens humains et financiers consacrés à la sécurité des systèmes d'information de la DGAC doivent être planifiés et quantifiés. Ces moyens sont proportionnés au niveau des risques préalablement identifiés.

**Principe 10 - Labellisation des produits et services SSI**

Tout produit et services de sécurité acquis par la DGAC est adapté aux besoins de sécurité et si nécessaire certifié par l'ANSSI.

**Principe 11 - Prestataires de confiance**

Lorsque la maîtrise des systèmes d'information l'exige, la DGAC fait appel à des opérateurs et des prestataires de confiance.

## G. Biens essentiels

Les biens essentiels sont les informations et les processus jugés importants pour la DGAC. Ainsi, par bien essentiels, on désigne l'ensemble des informations, activités, services délivrés, patrimoine que la DGAC juge prioritaire de maintenir disponibles.

Ces biens essentiels reposent sur des systèmes d'information, opérationnels ou de gestion. La PSSI a pour objectif de protéger les systèmes supportant les biens essentiels.

## H. Principaux risques

Les risques s'exercent contre les systèmes d'information.

La loi impose aux responsables des systèmes de conduire une analyse de risque afin d'en évaluer la criticité et d'organiser les mesures adaptées et proportionnées pour maîtriser ces risques.

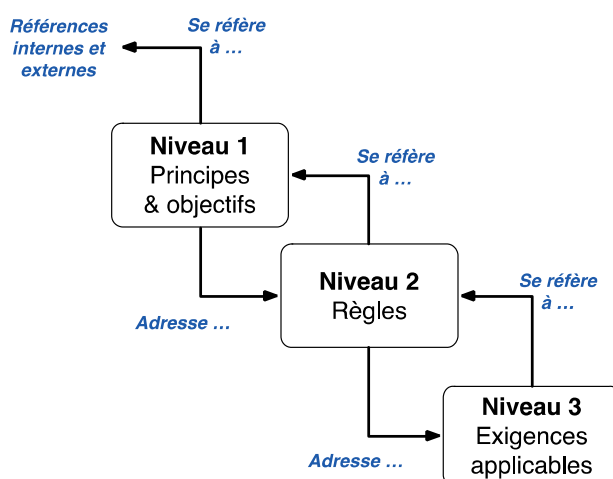
## I. Objectifs de sécurité

En conformité avec la PSSI-E, la PSSI DGAC **énonce 34 objectifs répartis en 13 domaines** de la sécurité des systèmes d'information. Chacun de ces objectifs adresse :

- Une ou plusieurs règles organisationnelles – figurant dans le Niveau-2 de la PSSI-DGAC – en fonction des systèmes et contextes concernés.

Ces règles adressant elles-même :

- Une ou plusieurs exigences opérationnelles – figurant dans le Niveau-3 de la PSSI-DGAC – adaptées aux systèmes et contextes concernés.



## **Organisation**

### **Objectif 1 - Organisation SSI**

Organiser la SSI de la DGAC en précisant : les acteurs concernés, leurs responsabilités, les relations internes et externes et les aspects formels du dispositif, afin de garantir la prise en compte préventive et réactive de la sécurité.

## **Ressources humaines**

### **Objectif 2 - Ressources humaines**

Impliquer les agents de la DGAC dans la SSI, grâce à des sessions de sensibilisation aux principaux risques et aux bonnes pratiques, des formations spécifiques et régulières pour les postes clés, et en rappelant les responsabilités de chaque personnel.

## **Gestion des biens**

### **Objectif 3 - Cartographie des SI**

Inventorier, cartographier, qualifier et organiser la protection des ressources techniques des systèmes d'information de la DGAC.

### **Objectif 4 - Qualification et protection de l'information**

Evaluer la sensibilité des informations et adapter leur niveau de protection, afin de garantir leur confidentialité, disponibilité, intégrité et traçabilité.

## **Intégration de la SSI dans le cycle de vie des systèmes d'information**

### **Objectif 5 - Gestion des risques et l'homologation de sécurité**

Mener régulièrement une analyse des risques des systèmes d'information sensibles de la DGAC. Les risques doivent être évalués et maîtrisés conformément aux objectifs de sécurité fixés. Les systèmes homologués feront l'objet d'une communication adaptée.

### **Objectif 6 - Maintien en condition de sécurité**

Mesurer l'efficacité de la sécurité des dispositifs SSI déployés tout au long de leur cycle de vie : conception, développement, mise en exploitation et retrait du service.

### **Objectif 7 - Produits et services qualifiés ou certifiés**

Organiser les mesures de réduction des risques en imposant l'utilisation de produits et services de sécurité labellisés (certifiés, qualifiés) par l'Agence Nationale de la Sécurité des Systèmes d'Information.

### **Objectif 8 - Maîtrise des prestations**

Mesurer la prise en compte de la SSI dans toute prestation faisant appel à des tiers et intervenant dans le domaine des SI : avant (analyse de risques et marchés publics), pendant (cahier des charges) et après les projets (respects des clauses de sécurité).

## **Sécurité physique**

### **Objectif 9 - Sécurité physique des locaux abritant les SI**

Garantir la sûreté physique des locaux abritant les SI : identification & segmentation des zones, réglementation des accès, protection des flux entrants/sortants et des lieux de stockage/hébergement des données sensibles, dispositif anti-attentat.

### **Objectif 10 - Sécurité physique des centres Informatiques**

Assurer la sécurité physique des centres informatiques, périmètres critiques pour la SSI : accès (contrôle, réglementation, traçabilité), flux auxiliaires (électricité, climatisation, eau, ...) et contrôler régulièrement les mesures de protection de ces ressources (entretien, réaction aux pannes, ...).

### **Objectif 11 - Sécurité du SI de sûreté**

Coordonner, dans une volonté de gestion globale de la sûreté, l'ensemble des dispositifs y concourant, notamment pour les points d'intérêts vitaux (PIV) : détection d'intrusion par vidéo-surveillance (VS), gestion technique des bâtiments (GTB), dispositif pour la sécurité incendie (INC).

## **Sécurité des réseaux**

### **Objectif 12 - Usage sécurisé des réseaux**

Utiliser et protéger les réseaux pour la maîtrise des flux, l'échange sécurisé de données sensibles et la connexion d'équipements, notamment vers des réseaux externes (tiers, internet).

### **Objectif 13 - Usage sécurisé des réseaux locaux**

Assurer la sécurité des réseaux de la DGAC, par le cloisonnement des ressources, des périmètres de ces réseaux et la maîtrise de leurs interconnexions.

### **Objectif 14 - Accès spécifiques**

Déclarer et obtenir une dérogation pour tout accès spécifique à Internet.

### **Objectif 15 - Usage sécurisé des réseaux sans fil**

Sécuriser l'usage des réseaux sans fil (Wifi) et garantir qu'il n'engage pas la sécurité des réseaux locaux.

### **Objectif 16 - Sécurité des mécanismes de commutation et de routage**

Pour se protéger des attaques, sécuriser les ressources réseaux au niveau du routage des données, les équipements actifs réseaux, les protocoles exposés ou vulnérables, et l'administration de ces infrastructures.

### **Objectif 17 - Cartographie réseau**

Maintenir à jour une cartographie complète – fonctionnelle et technique – des réseaux et des interconnexions, comprenant leur configuration et leur place dans l'environnement global des systèmes d'information de la DGAC.

## Architecture des SI

### Objectif 18 - Architecture sécurisée des centres informatiques

Appliquer le principe de défense en profondeur pour sécuriser les architectures / infrastructures hébergeant les ressources informatiques : mise en œuvre successive de zones démilitarisées (DMZ), d'environnements de sécurité en zone d'hébergement, de serveurs virtuels ou physiques dédiés, de réseaux locaux virtuels (VLAN), de filtrages stricts des flux applicatifs et d'administration.

## Exploitation des SI

### Objectif 19 - Protection des informations sensibles

Protéger les données confidentielles ou dont l'intégrité doit être garantie, notamment par des moyens cryptographiques adaptés (chiffrement, signature).

### Objectif 20 - Surveillance et configuration des ressources informatiques

Sécuriser les configurations et les outils de configuration des ressources informatiques : traçabilité des interventions sur les systèmes (notamment par les tiers), contrôle rigoureux du maintien en condition de sécurité des configurations et formalisation des documents.

### Objectif 21 - Autorisations et contrôles d'accès

Maîtriser la sécurité des accès aux systèmes d'information de la DGAC. Ces accès font l'objet d'une autorisation formelle, revue annuellement ; ils sont réalisés par le biais d'une procédure d'identification et d'authentification individuelles. La gestion des mots de passe doit être encadrée pour garantir une conformité et une sécurité.

Pour les accès aux données sensibles, l'authentification doit être « forte » c'est à dire basée sur des éléments supplémentaires de sécurité (carte à puce).

Les accès des administrateurs seront spécifiquement encadrés et durcis, en raison des privilèges attachés à leurs fonctions.

### Objectif 22 - Sécurisation de l'exploitation

Sécuriser avec une rigueur particulière les mécanismes d'administration. Les administrateurs, et les outils qu'ils utilisent, disposent de privilèges spécifiques qui imposent d'organiser une surveillance renforcée.

Cet objectif concerne la chaîne complète de la gestion des droits d'administration : demande d'habilitation, octroi des droits, centralisation et sécurisation des outils, traçabilité des actions, maîtrise des opérations de maintenance.

### Objectif 23 - Défense des systèmes d'information

Assurer la sécurité permanente des matériels informatiques notamment les appareils mobiles (PC portables, ordiphones, clés USB, disques durs amovibles, ...) contre le vol ou la perte. Les impressions papier doivent également faire l'objet d'une protection adaptée au contenu de leurs informations.

**Objectif 24 - Exploitation sécurisée des centres informatiques**

Cet objectif complète l'objectif 22 en adressant les règles visant à :

- Traiter le cas des ensembles applicatifs en topologie trois tiers, en raison de leur exposition et vulnérabilités spécifiques,
- Contrôler le cloisonnement des flux de supervision (remontée d'informations) et les flux d'administration (commandes, mises à jour), y compris leur traçabilité.
- Organiser l'usage des supports magnétiques aux fins d'administration et de supervision.

**Sécurité du poste de travail****Objectif 25 - Sécurisation des postes de travail**

Organiser de manière cohérente les mesures de protection du poste de travail, notamment :

- Sa sécurisation physique (filtre de confidentialité, fermeture automatique de session),
- Le régime des droits / privilèges d'usage sur les postes de travail (absence de droits administrateur accordés aux utilisateurs),
- Les procédures d'affectation, réaffectation (gestion des droits, mise au rebut).

Assurer la sécurité des postes de travail nomades par des mesures spécifiques (câble anti-vol, disque dur chiffré, sensibilisation des utilisateurs).

**Objectif 26 - Sécurisation des copieurs multifonctions**

Sécuriser l'usage des imprimantes et copieurs multifonctions(a fortiori interconnectés) par des contrôles réguliers notamment lors des opérations de maintenance par des tiers.

**Objectif 27 - Sécurisation de la téléphonie**

Assurer la sécurité de la téléphonie fixe par des mesures relatives aux configurations des autocommutateurs, aux codes d'accès des postes téléphoniques et au contrôle de conformité de ces équipements.

**Objectif 28 - Contrôles de la conformité des postes de travail**

Contrôler le maintien en condition de sécurité des postes de travail et la conformité de leurs configurations et paramétrages.

**Objectif 29 Sécurité dans le développement des SI**

Intégrer les exigences de sécurité dans les projets, développés en interne ou externalisés (confidentialité des informations, respect des bonnes pratiques, qualité du contrat de sous-traitance, ... ).

**Sécurité du développement des systèmes**

**Objectif 30 - Sécurité dans le développement des logiciels**

Renforcer la sécurité dans les phases de production et de livraison des logiciels et applicatifs, par un contrôle de l'environnement des équipes de développement et une méthodologie de sécurisation et de contrôle du code livré / produit.

**Objectif 31 - Sécurisation des applications à risques**

Intégrer la sécurité dès la conception des projets, par l'instauration de bonnes pratiques lors de la phase de développement, notamment pour les développements Web (prise en compte des vulnérabilités OWASP, filtrage applicatif, ...).

**Traitement des incidents****Objectif 32 - Chaînes opérationnelles**

Mettre en application et contrôler les mesures destinées à renforcer la coordination et la réactivité en cas d'événement de sécurité, sur la base de procédures d'alertes et de signalements d'incidents. Cet objectif vise également à une mutualisation optimale des opérations de remise en état afin d'accroître l'efficacité de la lutte contre les attaques.

**Continuité d'activité****Objectif 33 - Gestion de la continuité d'activité**

Organiser la continuité d'activité, en élaborant un Plan de Continuité d'Activité (PCA), aux échelons globaux et locaux de la DGAC, et en mettant en place les dispositifs pour la gestion de l'alerte, la réalisation d'exercices, l'activation du PCA et son maintien en conditions opérationnelles.

**Conformité, audits, inspections, contrôles****Objectif 34 - Organisation des contrôles**

Organiser les actes de surveillances et de contrôles réguliers (audits, revues de direction, inspections) afin d'identifier les insuffisances récurrentes et de mesurer les progrès accomplis dans la protection des systèmes d'information.

**J. Acteurs**

Les responsabilités dans l'élaboration de la PSSI-DGAC s'établissent de la façon suivante :

- **Le RSSI de la DGAC** définit les principes généraux et objectifs communs de la Politique de sécurité des systèmes d'information de la DGAC. Il identifie les périmètres pour lesquels ces principes et objectifs seront différenciés dans leurs traductions tactiques et opérationnelles, notamment dans les méthodologies de définition de cette politique (analyse de risques, modalités de contrôle, métriques des exigences).
- **Le directeur des services de la navigation aérienne** définit une politique de sécurité spécifique pour l'ensemble des systèmes d'information opérationnels de navigation aérienne (PSSI-NA), sous la forme de consignes, procédures et exigences, lesquelles sont reprises dans la PSSI-DGAC, essentiellement au niveau opérationnel.

Les acteurs<sup>1</sup> de la sécurité et en matière de mise en oeuvre et de contrôle SSI sont les suivants.

### **AQSSI**

Le directeur général est l'Autorité Qualifiée pour la Sécurité des Systèmes d'Information. A ce titre il est responsable de la protection des systèmes homologués de défense, de la prise en compte des alertes et des situations d'urgence majeures. De plus, il est le correspondant du service de défense, de sécurité et d'intelligence économique (SDSIE) pour la mise en œuvre des dispositions et des mesures ssi du plan vigipirate ainsi que celles du plan piranet.

### **RSSI**

Le Responsable de la Sécurité des Systèmes d'Information est nommé par l'AQSSI. Ses principales missions portent sur le maintien en conformité de la PSSI DGAC et le conseil auprès des différents acteurs de la sécurité (maîtrises d'œuvre et d'ouvrage, services d'exploitation, utilisateurs).

Il s'assure de la conformité des ressources allouées à la SSI et de leur adéquation aux besoins des métiers. Il veille à la régularité, la conformité et la complétude des contrôles de sécurité, sur la base de la présente directive.

Il supervise la mise en œuvre des actions de sensibilisation et de formation SSI pour l'ensemble des agents.

Il organise et prononce, en lien avec le secrétariat général, l'homologation des systèmes de gestion.

Enfin, il assure les relations avec le FSSI du ministère et les représentants de l'agence nationale de la sécurité des systèmes d'information (ANSSI).

### **RSSI Opérateur**

Le RSSI Opérateur organise le maintien en conformité des domaines de la PSSI DGAC qui relèvent de sa responsabilité.

Il organise, en lien avec les services, l'homologation des systèmes d'informations d'importance vitale (SIIV) et notamment la mise à jour de la cartographie des systèmes opérationnels. Il participe, en lien avec l'autorité de surveillance, à l'élaboration de la planification des contrôles.

Il organise et anime, la chaîne de traitement des alertes et des situations d'urgence des systèmes opérationnels, en lien avec le RSSI DGAC.

### **Autorité de surveillance**

L'autorité de surveillance assure une mission de contrôle de l'application des exigences de sécurité (audit de site, audit de systèmes, test d'intrusion, ...) et de conseil aux maîtrises d'ouvrage dans les phases de définition et de mise en œuvre des composants des systèmes de gestion (dispositifs de sécurité).

---

<sup>1</sup> Les missions détaillées des acteurs figurent en annexe de la PSSI Niveau 2.



## ASSI

Au sein de la DGAC, on distingue deux niveaux (central, local) d'agent de sécurité des systèmes d'information (ASSI).

**L'ASSI central** est l'intermédiaire entre les responsables du service et la DSAC dans le cadre des contrôles de sécurité. Il contribue à la préparation du planning des audits, suit leur déroulement et assiste les maîtrises d'ouvrage dans le cadre des plans de sécurité de systèmes.

Il relaie les exigences de la PSSI auprès des structures métier. De plus, il s'assure que tout agent utilisateur d'un système d'information reçoit la formation appropriée dans le domaine de la sécurité. Il anime et coordonne les actions de sensibilisation interne à son service.

**L'ASSI local** apporte assistance aux personnels de son service pour la mise en œuvre de la PSSI. Il s'assure que les informations et la documentation SSI sont diffusées et connues des personnes concernées. Il est l'intermédiaire entre les responsables de son service et la DSAC lors des contrôles de sécurité.

## Exploitant des systèmes d'information

Au sein de la DGAC, chaque exploitant est notamment tenu de rédiger un dossier de sécurité d'exploitation précisant les mesures prises afin d'assurer la sécurité des systèmes d'information dont il a la responsabilité. De plus, il enregistre les incidents de sécurité et communique à la DSAC ces informations. Enfin, il peut procéder à des investigations suite à un incident de sécurité afin de prévenir un tel incident.

## Administrateur système

L'administrateur système est chargé d'installer, de configurer et d'exploiter les systèmes d'information tout en garantissant la sécurité de ces systèmes. Il signale à l'exploitant tout incident de sécurité, toute vulnérabilité de sécurité et toute anomalie de fonctionnement pouvant avoir un impact sur la sécurité des SI.

## Chef de projet – Maîtrise d'ouvrage (MOA)

Chaque chef de projet, en charge de la maîtrise d'ouvrage est responsable de l'expression des besoins et des objectifs de sécurité du système d'information étudié. A ce titre, il communique à la DSAC, préalablement au développement, une description du projet et le résultat de l'expression des besoins de sécurité. Il s'assure de la mise en œuvre des méthodes, procédures et dispositifs techniques de sécurité pour répondre aux exigences de sécurité.

Il peut s'appuyer sur le RSSI, le CEDRe et le pôle SSI de la direction sûreté de la DSAC pour obtenir les informations nécessaires à l'exercice de sa mission.

## Chef de projet – Maîtrise d'œuvre (MOE)

Chaque chef de projet de la maîtrise d'œuvre prend en compte, gère et met en application l'ensemble des ressources humaines et financières, qui sont affectées au développement et à

la maintenance du système d'information étudié. Dans ce cadre, il s'assure que les spécifications techniques du système, les règles d'exploitation et les règles d'utilisation répondent aux exigences de sécurité définies.

## **K. Comitologie**

### **Comité directeur de la SSI (Codir SSI)**

La DGAC confie les aspects stratégiques en matière de sécurité au Comité Directeur de la Sécurité des Systèmes d'Information [CDSSI], lequel se réunit trois fois par an, pour passer en revue la Politique de Sécurité des Systèmes d'Information [PSSI] et les responsabilités globales (Fiches missions).

Le Codir SSI surveille l'évolution de l'exposition aux menaces des actifs essentiels de la DGAC et approuve les actions destinées à renforcer la sécurité de l'information. Enfin, il valide la maîtrise des risques et il homologue les systèmes d'information.

Le Comité Directeur SSI est présidé par le Directeur Général. Sa composition est précisée en annexe du Niveau 2.

## **L. Suivi de la PSSI**

La PSSI fait l'objet d'un suivi permettant de disposer en permanence d'indicateurs pertinents pour les prises de décisions. Ces indicateurs alimentent trois types de tableaux de bord :

- Le tableau de bord stratégique qui donne une vision globale du déploiement de la démarche, de sa conformité au regard des enjeux de la DGAC.
- Le tableau de bord de pilotage, qui permet d'avoir une vision centrée sur la démarche de mise en œuvre des projets de sécurité.
- Le tableau de bord opérationnel, qui retrace l'ensemble des menaces et des vulnérabilités telles que les attaques de virus, les vulnérabilités système identifiées, etc.

Les tableaux de bords visant différents objectifs ont des fréquences d'actualisation adaptées. Ils font l'objet d'une diffusion systématique au Codir SSI ayant autorité en matière de contrôle et de validation du niveau de sécurité des systèmes d'Information.

## **M. Validation et diffusion de cette politique**

Cette Politique de Sécurité des Systèmes d'Information est une directive, validée par le Directeur Général de la DGAC.

Ce document doit être largement diffusé et connu par l'ensemble des utilisateurs et par les prestataires en charge de la sécurité des systèmes d'information.

Pour faciliter sa compréhension et sa prise de connaissance, la PSSI doit être accompagnée de sessions de sensibilisation à la sécurité des SI.

Enfin, ce document doit être régulièrement mis à jour afin de refléter les évolutions du contexte et répondre aux objectifs stratégiques de la DGAC.

## **N. Référentiels internes**

- PRO\_10 DSNA,
- MET08,
- Etude sûreté globale,
- Programme de sûreté,
- Analyses de risques (SIGP, DSNA).

## **O. Référentiels externes**

- Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE) – 17 juillet 2014.
- Règlement Général de Sécurité (RGS) – 27 février 2014.
- Instruction Interministérielle relative à la protection des systèmes d'information sensibles n°901 du 28 janvier 2015
- Loi de Programmation Militaire (LPM) – 18 décembre 2013.
- Arrêté sectoriel du 11 août 2016, relatif au sous-secteur d'activités d'importance vitale «Transport aérien».
- Décret n° 2015-351 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale - 27 mars 2015. Arrêté sectoriel pour les OIV en charge du transport aérien – 1<sup>er</sup> octobre 2016.
- Règlement européen 1034 relatif à la supervision de la sécurité dans la gestion du trafic aérien et les services de navigation aérienne – 17 octobre 2011.
- Règlement européen 1035 relatif aux exigences communes pour la fourniture de services de navigation aérienne – 17 octobre 2011.
- Loi n°78-17 du 6 janvier 1978 modifiée par la loi du 6 août 2004, dite loi Informatique et Libertés.
- Règlement européen 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données - 27 avril 2016 et qui entrera en application le 25 mai 2018.