



POLITIQUE DE SECURITE
DES SYSTEMES D'INFORMATION
DE LA DGAC

NIVEAU 2

PILOTAGE

HISTORIQUE DES VERSIONS			
21 avril 2018	V 1 Rev-2	Annexe – Description des environnements sécurisés (de couleurs).	RSSI / DGAC – Contribution DSNA
16 avril 2018	V 1 Rev-1	Modification de la description des rôles (Surveillant).	RSSI / DGAC – Contribution DSAC
15 février 2018	V 1.0	Version validée et diffusée.	RSSI / DGAC

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

Table des matières

V.	Politique de sécurité de l'information.....	8
A.	Orientations de la direction en matière de sécurité de l'information.....	8
	Politiques de sécurité de l'information	8
	Revue des politiques de sécurité de l'information	8
VI.	Organisation de la sécurité de l'information.....	9
A.	Organisation interne.....	9
	Fonctions et responsabilités liées à la sécurité de l'information.....	9
	Séparation des tâches.....	11
	Relations avec les autorités.....	11
	Relations avec des groupes de travail spécialisés	11
	Sécurité de l'information dans la gestion de projet	11
B.	Appareils mobiles et télétravail.....	12
	Politique en matière d'appareils mobiles.....	12
	Télétravail.....	12
VII.	La sécurité des ressources humaines	13
A.	Avant l'embauche.....	13
	Sélection des candidats.....	13
	Termes et conditions d'embauche	13
B.	Pendant la durée du contrat.....	13
	Responsabilités de la direction.....	13
	Sensibilisation, apprentissage et formation à la sécurité de l'information	14
	Processus disciplinaire	14
C.	Rupture, terme ou modification du contrat de travail	14
	Achèvement ou modification des responsabilités associées au contrat de travail	14
VIII.	Gestion des actifs.....	15
A.	Responsabilités relatives aux actifs.....	15
	Inventaire des actifs	15
	Propriété des actifs	16
	Utilisation correcte des actifs	16
	Restitution des actifs.....	16
B.	Classification de l'information.....	16
	Classification des informations	16
	Marquage des informations	17
	Manipulation des actifs.....	17
C.	Manipulation des supports.....	17
	Gestion des supports amovibles	17
	Mise au rebut des supports	18
	Transfert physique des supports.....	18

IX.	Contrôle d'accès.....	19
A.	Exigences métier en matière de contrôle d'accès.....	19
	Politique de contrôle d'accès.....	19
	Accès aux réseaux et aux services en réseau.....	19
B.	Gestion de l'accès utilisateur.....	19
	Enregistrement et désinscription des utilisateurs.....	19
	Maîtrise de la gestion des accès utilisateur.....	19
	Gestion des informations secrètes d'authentification des utilisateurs.....	20
	Revue des droits d'accès utilisateur.....	20
	Suppression ou adaptation des droits d'accès.....	21
C.	Responsabilités des utilisateurs.....	21
	Utilisation d'informations secrètes d'authentification.....	21
D.	Contrôle de l'accès au système et aux applications.....	21
	Restriction d'accès à l'information.....	21
	Sécuriser les procédures de connexion.....	21
	Système de gestion des mots de passe.....	21
	Utilisation de programmes utilitaires à privilèges.....	22
	Contrôle d'accès au code source des programmes.....	22
X.	Cryptographie	23
A.	Mesures cryptographiques.....	23
	Politique d'utilisation des mesures cryptographiques	23
	Gestion des clés.....	23
XI.	Sécurité physique et environnementale.....	24
A.	Zones sécurisées	24
	Périmètre de sécurité physique	24
	Contrôles physiques des accès.....	24
	Sécurisation des bureaux, des salles et des équipements	24
	Protection contre les menaces extérieures et environnementales	25
	Travail dans les zones sécurisées.....	25
	Zones de livraison et de chargement.....	25
B.	Matériels	25
	Emplacement et protection du matériel.....	25
	Services généraux.....	25
	Sécurité du câblage.....	26
	Maintenance du matériel.....	26
	Sortie des actifs.....	26
	Sécurité du matériel et des actifs hors des locaux.....	26
	Mise au rebut ou recyclage sécurisé(e) du matériel.....	26
	Matériel utilisateur laissé sans surveillance.....	27
	Politique du bureau propre et de l'écran vide.....	27
XII.	Sécurité liée à l'exploitation.....	28
A.	Procédures et responsabilités liées à l'exploitation.....	28

	Procédures d'exploitation documentées.....	28
	Gestion des changements.....	28
	Dimensionnement.....	28
	Séparation des environnements de développement, test et exploitation.....	28
B.	Protection contre les logiciels malveillants.....	28
	Mesures contre les logiciels malveillants.....	28
C.	Sauvegarde.....	29
	Sauvegarde des informations.....	29
D.	Journalisation et surveillance.....	29
	Journalisation des événements.....	29
	Protection de l'information journalisée.....	29
	Journaux administrateur et opérateur.....	29
	Synchronisation des horloges.....	30
E.	Maîtrise des logiciels en exploitation.....	30
	Installation de logiciels sur des systèmes en exploitation.....	30
F.	Gestion des vulnérabilités techniques.....	30
	Gestion des vulnérabilités techniques.....	30
	Restrictions liées à l'installation de logiciels.....	31
G.	Considérations sur l'audit du système d'information.....	31
	Mesures relatives à l'audit des systèmes d'information.....	31
XIII.	Sécurité des communications.....	32
A.	Management de la sécurité des réseaux.....	32
	Contrôle des réseaux.....	32
	Sécurité des services réseaux.....	32
	Cloisonnement des réseaux.....	33
B.	Transfert de l'information.....	33
	Politiques et procédures de transfert de l'information.....	33
	Accords en matière de transfert d'information.....	33
	Messagerie électronique.....	33
	Engagements de confidentialité ou de non-divulgence.....	33
XIV.	Acquisition, développement et maintenance des systèmes d'information.....	34
A.	Exigences de sécurité applicables aux systèmes d'information.....	34
	Analyse et spécification des exigences de sécurité de l'information.....	34
	Sécurisation des services d'application sur les réseaux publics.....	34
	Protection des transactions liées aux services d'application.....	34
B.	Sécurité des processus de développement et d'assistance technique.....	34
	Politique de développement sécurisé.....	34
	Procédures de contrôle des changements apportés au système.....	35
	Revue technique des applications après changement apporté à la plateforme d'exploitation.....	35
	Restrictions relatives aux changements apportés aux progiciels.....	35
	Principes d'ingénierie de la sécurité des systèmes.....	35
	Environnement de développement sécurisé.....	35

	Développement externalisé.....	35
	Phase de test de la sécurité du système.....	35
	Test de conformité du système.....	36
C.	Données de test.....	36
	Protection des données de test.....	36
XV.	Relations avec les fournisseurs.....	37
A.	Sécurité de l'information dans les relations avec les fournisseurs.....	37
	Politique de sécurité de l'information dans les relations avec les fournisseurs.....	37
	La sécurité dans les accords conclus avec les fournisseurs.....	37
	Chaine d'approvisionnement informatique.....	37
B.	Gestion de la prestation du service.....	37
	Surveillance et revue des services des fournisseurs.....	37
	Gestion des changements apportés dans les services des fournisseurs.....	37
XVI.	Gestion des incidents liés à la sécurité de l'information.....	38
A.	Gestion des incidents liés à la sécurité de l'information et améliorations.....	38
	Responsabilités et procédures.....	38
	Signalement des événements liés à la sécurité de l'information.....	38
	Signalement des failles liées à la sécurité de l'information.....	38
	Appréciation des événements liés à la sécurité de l'information et prise de décision.....	38
	Réponse aux incidents liés à la sécurité de l'information.....	38
	Tirer des enseignements des incidents liés à la sécurité de l'information.....	38
	Recueil de preuves.....	39
XVII.	Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité.....	40
A.	Continuité de la sécurité de l'information.....	40
	Organisation de la continuité de la sécurité de l'information.....	40
	Mise en œuvre de la continuité de la sécurité de l'information.....	40
	Vérifier, revoir et évaluer la continuité de la sécurité de l'information.....	40
B.	Redondances.....	40
	Disponibilité des moyens de traitement de l'information.....	40
XVIII.	Conformité.....	41
A.	Conformité aux obligations légales et réglementaires.....	41
	Identification de la législation et des exigences contractuelles applicables.....	41
	Droits de propriété intellectuelle.....	41
	Protection des enregistrements.....	41
	Protection de la vie privée et protection des données à caractère personnel.....	41
	Réglementation relative aux mesures cryptographiques.....	42
B.	Revue de la sécurité de l'information.....	42

	Revue indépendante de la sécurité de l'information	42
	Conformité avec les politiques et les normes de sécurité	43
	Examen de la conformité technique.....	43
	Gestion des dérogations.....	43
XIX.	Annexe A - Description des Rôles	44
C.	AQSSI.....	44
D.	Autorité de surveillance (DSAC).....	44
E.	RSSI DGAC	45
F.	RSSI Opérateur	46
G.	ASSI.....	47
	ASSI de direction.....	48
	ASSI local	49
H.	Rôles opérationnels.....	49
I.	Délégué à la protection des données à caractère personnel (CIL/DPO)	52
XX.	Description des environnements de sécurité	53
J.	Environnement « Rouge ».....	54
	Aspect opérationnel	54
	Aspect politique et image de marque.....	54
	Aspect de la sécurité des personnes	54
	Aspect financier et économique	54
	Aspect légal ou réglementaire.....	54
	Données manipulées exclusivement en environnement rouge.....	54
	Systèmes hébergés en environnement rouge	54
K.	Environnement Orange.....	55
	Aspect opérationnel	55
	Aspect politique et image de marque.....	55
	Aspect de la sécurité des personnes	55
	Aspect financier et économique	55
	Aspect légal ou réglementaire.....	55
	Données manipulées exclusivement en environnement orange (ou supérieur)	56
	Systèmes hébergés en environnement orange	56
L.	Environnement Jaune	56
	Aspect opérationnel	56
	Aspect politique et image de marque.....	57
	Aspect de la sécurité des personnes	57
	Aspect financier et économique	57
	Aspect légal ou réglementaire.....	57
	Systèmes hébergés en environnement jaune.....	57
M.	Environnement Bleu.....	58
	Aspect opérationnel	58
	Aspect politique et image de marque.....	58
	Aspect de la sécurité des personnes	58

	Aspect financier et économique.....	58
	Aspect légal ou réglementaire.....	58
	Limitation.....	58
	Systèmes hébergés en environnement bleu.....	58
N.	Environnement Noir.....	59
	Aspect opérationnel	59
	Aspect financier et économique.....	59
	Aspect légal ou réglementaire.....	59
	Données manipulées en environnement noir.....	59
	Systèmes hébergés en environnement noir.....	59
O.	Analyses de risques spécifiques	59
XXX.	ANNEXE B - Besoins de sécurité des actifs essentiels.....	61
XXXI.	ANNEXE C - Glossaire.....	63

V. Politique de sécurité de l'information

A. Orientations de la direction en matière de sécurité de l'information

Objectif : Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.

Politiques de sécurité de l'information

PSSI-PILOTAGE : définition et pilotage de la PSSI. La DGAC établit, tient à jour et diffuse sa propre politique SSI, sous la responsabilité de son Directeur Général. Cette politique est établie dans le niveau 1 selon les objectifs de la PSSIE. Pour le niveau 2 elle est en conformité avec le cadre de l'ISO 27002 et pour le niveau 3, elle est complétée par les exigences du NIST 800-53.

Revue des politiques de sécurité de l'information

PSSI-CONTROLES : contrôles réguliers. La conformité de la PSSI de la DGAC, est vérifiée par des contrôles réguliers. Le RSSI conduit des actions d'évaluation de la conformité à ces deux politiques et contribuent à la consolidation, dans un bilan annuel, de l'état d'avancement de sa mise en œuvre.

VI. Organisation de la sécurité de l'information

A. Organisation interne

Objectif : Établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information au sein de l'organisation.

Fonctions et responsabilités liées à la sécurité de l'information

ORGANISATION-FONCTIONNEMENT : fonctionnement de la SSI. Pour l'ensemble des tâches liées à la SSI (processus métiers essentiels, tâches annexes), la notion de titulaire et de suppléant doit être définie pour que chaque activité soit réalisée de manière optimale.

La délégation de pouvoir, à un ou plusieurs suppléants, est une réponse pour assurer le maintien en condition de sécurité des systèmes d'information. Pour les fonctions essentielles, il doit y avoir une nécessité de suppléance avec garantie de compétence du suppléant.

De même, pour l'ensemble des tâches liées à la fonction SSI, concourant au traitement des alertes et à la gestion de crise, Les directions s'organisent pour en assurer la continuité.

ORGANISATION-SSI : organisation de la SSI. L'organisation SSI de la DGAC, établie conjointement avec le HFDS du ministère des transports, définit les responsabilités internes, celles des tiers et les modalités de coordination avec les autorités externes. Les procédures d'applications sont écrites et portées à la connaissance de tous.

La DGAC est soumise à l'IGI 1300, en raison de la sensibilité des informations traitées non classifiées de défense et de niveau Diffusion Restreinte.

De plus, certaines entités de la DGAC sont soumises aux exigences de l'arrêté sectoriel des transports aériens conformément à la Loi de Programmation Militaire (LPM) pour les Systèmes d'Information d'Importance Vitale (SIIV).

Enfin, cette politique prend en compte les exigences relatives au traitement des données à caractère personnel défini par le Règlement Général de Protection des Données (RGPD).

ORGANISATION-ACTEURS SSI : acteurs de la SSI. La maîtrise des risques et le maintien du niveau de sécurité en adéquation avec les objectifs métiers, mobilisent différents acteurs :

- Autorité de surveillance (DSAC),
- AQSSI DGAC (Autorité Qualifiée pour la Sécurité des Systèmes d'Information DGAC),
- RSSI DGAC (Responsable de la Sécurité des Systèmes d'Information DGAC),
- RSSI DSNA (Responsable de la Sécurité des Systèmes d'Information DSNA),
- ASSI DGAC (Agent de sécurité des systèmes d'information DGAC),
- Exploitant des systèmes d'information,
- Administrateur système,
- Chef de projet – Maîtrise d'ouvrage (MOA),
- Chef de projet – Maîtrise d'œuvre (MOE).

Les missions de ces acteurs figurent en annexe de la présente PSSI Niveau 2.

La DGAC dispose de sa propre organisation traitant des sujets liés à la SSI, rendant compte au FSSI de son ministère de tutelle.

ORGANISATION-CHAÎNE FONCTIONNELLE SSI : chaîne fonctionnelle SSI de la DGAC. La DGAC organise la chaîne fonctionnelle SSI selon le schéma suivant :

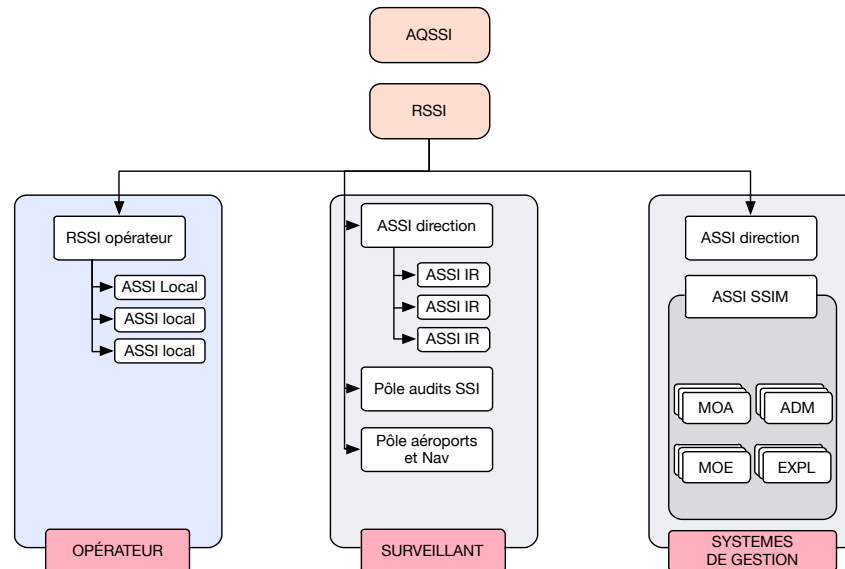


Schéma de la Chaîne fonctionnelle SSI.

Différents acteurs agissent au sein de la chaîne SSI :

- **L'Opérateur de navigation aérienne**, également désigné dans ce référentiel comme « opérateur ». Il conçoit, déploie, exploite et sécurise les systèmes dits « opérationnels », sur lesquels repose son activité.
- **L'Autorité de surveillance (DSAC)**, également nommée « surveillant », assurant les contrôles destinés à vérifier la conformité des systèmes d'information aux exigences de sécurité, sur la base du présent référentiel.
- **Le Secrétariat Général**, en particulier le service des systèmes d'information et de la modernisation (SSIM), également appelé « DSI », qui conçoit, déploie, exploite et sécurise les systèmes de gestion.
- **La Direction du Transport aérien**. Acteur régalien, elle est utilisatrice des systèmes d'information.

ORGANISATION-RESPONSABILITE : responsabilités SSI. Une note subordonnée à la présente politique définit l'organisation du comité de sécurité des SI et fixe la répartition des responsabilités et rôles en matière de SSI. Cette note est validée par le Directeur Général de la DGAC.

ORGANISATION -EXIGENCES : formalisation des documents. Le comité de sécurité des SI valide les documents d'application (procédures), permettant la mise en œuvre des exigences de la PSSI. Il rend compte régulièrement de la mise en application des mesures de sécurité auprès du Directeur Général.

L'application des mesures de sécurité est planifiée et appliquée localement au niveau de la DGAC, dont le pilotage opérationnel est assuré par :

- Le comité de sécurité des SI pour les systèmes de gestion,
- Le comité directeur SSI de la DSNA pour les systèmes industriels.

L'interlocuteur de la DGAC au sein du ministère de tutelle reste le FSSI.

Séparation des tâches

ORGANISATION-TACHES : séparation des tâches. Les tâches et les domaines de responsabilité liés à la définition des exigences de sécurité et au contrôle de leur application doivent être rigoureusement séparés de la gestion opérationnelle de la sécurité des systèmes d'information.

Relations avec les autorités

ORGANISATION-AUTORITE : gestion des relations avec les autorités. La DGAC entretient des relations avec les autorités compétentes (ANSSI, CNIL, HFDS, etc.) en matière de sécurité des systèmes d'information. Le Responsable SSI établit les procédures de contact avec les autorités compétentes, en particulier pour le signalement des incidents relatifs à la sécurité de l'information.

Relations avec des groupes de travail spécialisés

ORGANISATION-RELATIONS : relations avec des experts SSI. La DGAC doit entretenir des relations avec des groupes de spécialistes et d'experts de la sécurité de l'information notamment sur les sujets de veille technologique, réglementaires ainsi que sur les risques de sécurité (ISO 27001, EBIOS, etc.).

Sécurité de l'information dans la gestion de projet

SSI-PROJETS : 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. Cette exigence s'applique à tout projet quel qu'il soit, indépendamment de sa nature.

SSI-HOMOLOGATION : homologation des systèmes d'information. Tout système d'information, s'il est identifié comme sensible, doit faire l'objet d'une décision d'homologation de sa sécurité avant sa mise en exploitation dans les conditions d'emploi définies.

Une procédure, diffusée sous la forme d'une consigne de niveau 3 (associée à la description de la procédure d'homologation), permet d'identifier les systèmes devant faire l'objet d'une homologation.

Cependant, tout système concourant directement à l'activité opérationnelle de Navigation aérienne, est considéré comme sensible et doit obligatoirement être homologué.

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 (Directeur Général), le cas échéant après avis de la commission d'homologation.

Cette décision s'appuie sur une analyse de risques adaptée aux enjeux du système considéré, et précise les conditions d'emploi.

La description détaillée de la procédure d'homologation figure dans le niveau 3 de cette PSSI.

B. Appareils mobiles et télétravail

Objectif : Assurer la sécurité du télétravail et de l'utilisation d'appareils mobiles.
--

Politique en matière d'appareils mobiles

MOBILITE-NOMADISME : déclaration des équipements nomades. 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.

MOBILITE-CONFIDENTIALITE : 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'entité.

MOBILITE-CONFIGURATION : configuration des postes nomades. Les accès à distance aux SI de l'entité (accès dits « nomades ») doivent être réalisés uniquement depuis des équipements de la DGAC. Lorsque l'accès à distance utilise d'autres infrastructures, l'usage de réseaux privés virtuels (VPN) de confiance est nécessaire. Un pare-feu local doit être installé sur les postes nomades.

Les interfaces de connexion sans fil (Wifi, Bluetooth, 3G...) doivent être configurées afin d'interdire les usages non maîtrisés et éviter les intrusions. Les interfaces sans fil ne doivent être activées qu'en cas de besoin.

MOBILITE-STOCKAGE : stockage d'information sur les postes nomades. Le stockage local d'information sur les postes de travail nomades doit être limité au strict nécessaire.

MOBILITE-CHIFFREMENT : chiffrement des postes nomades. Les postes nomades doivent être entièrement chiffrés par un moyen de chiffrement labellisé.

MOBILITE-VERROUILLAGE : verrouillage des portables. Un câble physique de sécurité doit être fourni avec chaque poste portable. Les utilisateurs doivent être sensibilisés à son utilisation.

Télétravail

TELETRAVAIL-POLITIQUE : politique liée au télétravail. La DGAC doit élaborer une politique définissant les conditions et restrictions d'utilisation liées au télétravail. Le télétravail implique que le collaborateur n'est pas présent dans les locaux de la DGAC.

TELETRAVAIL-ACCES : accès à distance. Les utilisateurs distants doivent s'authentifier sur le réseau de la DGAC en utilisant une méthode conforme à l'annexe B3 du RGS.

VII. La sécurité des ressources humaines

A. Avant l'embauche

Objectif : S'assurer que les agents et les contractants comprennent leurs responsabilités et qu'ils sont compétents pour remplir les fonctions que l'organisation envisage de leur confier.

Sélection des candidats

RH-SELECTION : sélection des candidats. La DGAC doit réaliser un contrôle des candidats à l'embauche. Ce contrôle doit permettre à la DGAC de vérifier, vis-à-vis de la sécurité des systèmes d'information, que les qualifications annoncées sont en adéquation avec les postes concernés.

Termes et conditions d'embauche

RH-GESTION : gestion des arrivées. Une procédure permettant de gérer l'arrivée des collaborateurs, contractant ou tiers doit être formalisée et appliquée. Cette procédure doit couvrir au minimum :

- La gestion des comptes et des droits d'accès aux SI, y compris pour les partenaires et les prestataires externes ;
- La gestion du contrôle d'accès aux locaux ;
- La gestion des équipements mobiles ;
- La gestion du contrôle des habilitations.

RH-ENGAGEMENT : engagement de confidentialité. Tout collaborateur ayant accès à des informations confidentielles doit signer un engagement de confidentialité ou de non-divulgaration, mentionnant les articles du code pénal qu'il doit respecter (joint à l'attestation) et les sanctions encourues en cas de transgression, avant d'obtenir l'accès à l'information.

RH-POSTE : fiche de poste. Tout nouveau personnel, dans le cas où son poste d'affectation comporte une sensibilité signalée vis à vis des données ou processus des systèmes d'information, doit recevoir une fiche de poste comprenant un volet « sécurité de l'information ».

B. Pendant la durée du contrat

Objectif : S'assurer que les agents et les contractants sont conscients de leurs responsabilités en matière de sécurité de l'information et qu'ils assument ces responsabilités.

Responsabilités de la direction

RH-RESPONSABILITES : responsabilités du personnel. La responsabilité du personnel en matière de sécurité de l'information doit être spécifiée dans la fiche de poste. Chaque collaborateur et contractants doivent appliquer les règles de sécurité conformément aux politiques et aux procédures en vigueur dans l'organisation.

RH-CONFIANCE : personnels 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, apprentissage et formation à la sécurité de l'information

RH-SENSIBILISATION : sensibilisation des personnels SSI. Chaque utilisateur doit être régulièrement informé et sensibilisé aux exigences de sécurité. Il doit être formé à l'utilisation des systèmes d'information conformément aux règles internes de la DGAC (charte utilisateur, PSSI, procédures, ...).

RH-NON PERMANENT : personnel non permanent. Les règles de la PSSI s'appliquent à tout personnel non permanent (stagiaire, intérimaire, prestataire...) utilisateur d'un SI de la DGAC. 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.

Processus disciplinaire

RH-SANCTIONS : processus disciplinaire. Le non-respect des règles de sécurité de la DGAC, et notamment sa PSSI, expose tout contrevenant à des sanctions disciplinaires, civiles et pénales en cas de violation des législations applicables en matière de sécurité de l'information. La Direction des Ressources Humaines doit formaliser un processus disciplinaire permettant de prendre des mesures à l'encontre des collaborateurs ayant transgressés les règles SSI.

C. Rupture, terme ou modification du contrat de travail

Objectif : Protéger les intérêts de l'organisation dans le cadre du processus de modification, de rupture ou de terme d'un contrat de travail.

Achèvement ou modification des responsabilités associées au contrat de travail

RH-GESTION : gestion des mutations et des départs. Une procédure permettant de gérer les mutations et les départs des utilisateurs dans les SI doit être formalisée, et appliquée strictement. Cette procédure doit couvrir au minimum :

- La gestion et révocation des comptes et des droits d'accès aux SI, y compris pour les partenaires et les prestataires externes ;
- La gestion du contrôle d'accès aux locaux et des habilitations ;
- La gestion des équipements mobiles et la restitution du matériel ;
- L'annonce du départ du collaborateur ;
- Le rappel lié aux clauses de confidentialité et de non-divulgateion.

La DRH doit communiquer tout mouvement de personnel à la DSI.

VIII. Gestion des actifs

A. Responsabilités relatives aux actifs

Objectif : Identifier les actifs de l'organisation et définir les responsabilités appropriées en matière de protection.

Inventaire des actifs

ACTIFS-INVENTAIRE : inventaire des actifs. La DGAC établit et maintient à jour un inventaire des actifs sous la responsabilité du comité de sécurité des SI. Cet inventaire est tenu à disposition du ministère de tutelle. Il comprend la liste des biens matériels et logiciels et leurs versions, maintenue à jour et exploitée pour les audits.

ACTIFS-MAITRISE : maîtrise des actifs. Tout équipement (poste de travail, imprimante, portable, smartphone) doit être enregistré, configuré, mis en service et géré par la DSI.

Aucun matériel ou équipement autre que ceux fournis et configurés par la DGAC n'est autorisé sur les réseaux professionnels de la DGAC. Les matériels hors standard DGAC sont strictement interdits sur les réseaux professionnels de la DGAC.

ACTIFS-ESSENTIELS : actifs essentiels. Dans le cadre de l'analyse des risques, les métiers de la DGAC ont identifié les actifs essentiels représentant les informations et processus devant faire l'objet d'une protection particulière.

Le tableau suivant présente les actifs essentiels de la DGAC relatifs aux domaines SIGP et SINA :

Id	Biens / Processus essentiels	Objectifs / Définition	Acteurs
HAB	Applications de métiers de Gestion	Notamment la gestion des habilitations des accès aux zones restreintes aéroportuaires (STITCH, ...)	DTA
LIC	Applications de métiers de Gestion	Notamment pour la gestion des licences, autorisations médicales et dérogations du personnel navigant (SI Métiers DSAC, ...)	DSAC
REG	Applications de métiers de Gestion	Notamment pour la gestion des documents de la réglementation aérienne (GEODE, ...)	DSNA
RH	Applications transverses de soutien	Notamment pour la gestion des ressources humaines (SIRH, ...)	SDP
FIN	Applications transverses de soutien	Notamment pour la gestion financière (SIF, ...)	SDF
COL	Applications du support informatique	Gestion collaborative (Portail d'entreprise, ...)	DSI
MES	Applications du support informatique	Messagerie, ...	DSI
RES	Applications du support informatique	Supervision & Applications de gestion des réseaux	DSI

Les besoins de sécurité des données de la DGAC sont consultables en [Annexe B](#).

Propriété des actifs

ACTIFS-IDENTIFICATION : identification des actifs. La gestion des actifs a pour objectif de mettre en place et maintenir une protection adaptée et de garantir des niveaux de sécurité appropriés à la sensibilité des informations.

Cela consiste à mettre en application les actions suivantes :

- Réaliser un inventaire des actifs,
- Désigner un propriétaire pour chaque actif,
- Définir et revoir périodiquement les classifications et les restrictions d'accès aux actifs importants en tenant compte des politiques de contrôle d'accès applicables.

Utilisation correcte des actifs

ACTIFS-UTILISATION : utilisation des actifs. La DGAC doit rédiger (charte informatique) les règles d'utilisation correcte des actifs et de leurs moyens de traitement associés. Tout personnel permanent ou non permanent (stagiaires, intérimaires, prestataires...) est responsable de l'utilisation qu'il fait de ses actifs.

Restitution des actifs

ACTIFS-RESTITUTION : restitution des actifs. Dès la fin du contrat, de l'accord ou de la période d'emploi les collaborateurs, contractant ou tiers doivent restituer l'ensemble des actifs de la DGAC qui étaient en leur possession. Notamment :

- Le matériel (dont les équipements mobiles) ;
- Les logiciels ;
- Les documentations techniques ou d'exploitation.

B. Classification de l'information

Objectif : S'assurer que l'information bénéficie d'un niveau de protection approprié conforme à son importance pour l'organisation.

Classification des informations

INFORMATIONS-CLASSIFICATION : classification des informations. La DGAC doit classer les informations en tenant compte des besoins en matière de partage ou de limitation de l'information, de leur sensibilité et au regard des exigences légales.

Une information doit être évaluée par son propriétaire. En cas de doute, le propriétaire consulte sa hiérarchie pour mettre en adéquation le niveau de classification de sécurité en correspondance avec les enjeux et les besoins opérationnels.

Marquage des informations

INFORMATIONS-QUALIFICATION : qualification des informations. La DGAC doit établir une procédure d'identification de la sensibilité de l'information. Il est fortement recommandé de marquer systématiquement tout document comportant un degré de sensibilité (confidentialité notamment).

Manipulation des actifs

ACTIFS-PROTECTION : protection des informations. L'utilisateur doit protéger les actifs qu'il est amené à manipuler dans le cadre de ses fonctions, selon leur sensibilité et tout au long de leur cycle de vie.

Concernant les informations, cette exigence s'applique à tout type de transmission : courrier (interne ou postal, porteur, ...), télécopie ou envoi dématérialisé (transfert de fichier, extrait de base de données, envoi sur support externe ou amovible, télé-déchargement, ...).

ACTIFS-EXPLOITATION : protection des actifs sensibles. Des mesures doivent être mises en œuvre afin de garantir la protection des actifs sensibles dans le domaine de la confidentialité ou l'intégrité. A défaut d'utilisation d'un réseau homologué, ces actifs doivent être chiffrés à l'aide d'un moyen de chiffrement labellisé.

C. Manipulation des supports

Objectif : Empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) de l'information de l'organisation stockée sur des supports.

Gestion des supports amovibles

AMOVIBLE-ACCES : accès aux supports 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.

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

AMOVIBLE-DETECTION : détection de malwares. Une analyse ayant pour but la détection de logiciels malveillants sur un support externe doit être systématiquement réalisée avant l'exploitation des informations.

AMOVIBLE-STOCKAGE : supports de stockage amovibles. Les supports de stockage amovibles (clés USB et disque durs externes, notamment) doivent être fournis aux utilisateurs par l'équipe locale chargée des SI. Ces supports doivent être exclusivement réservés au réseau DGAC.

AMOVIBLE-EFFACEMENT : 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.

La fin de vie d'un support ou d'un matériel (imprimante, routeur, commutateur...) doit s'accompagner d'une opération de destruction avant remise au constructeur.

AMOVIBLE-VOL : protection contre le vol. Chaque utilisateur doit veiller à la sécurité des supports amovibles (clés USB et disques amovibles), notamment en les conservant dans un endroit sûr.

Mise au rebut des supports

SUPPORTS-REBUT : mise au rebut des supports. Lorsqu'une ressource informatique sort définitivement de la DGAC, les données présentes sur les disques durs ou la mémoire intégrée doivent être effacées de manière sécurisée. L'effacement des données sensibles doit s'appuyer sur des produits qualifiés par l'ANSSI et les procédures de la DGAC.

Transfert physique des supports

SUPPORTS-TRANSFERT : transfert d'informations. Les supports de stockage externe tels que clé USB, disque dur, etc., doivent être protégés de tout dommage physique (environnemental, humain, magnétique, etc.) lors de leur transfert.

SUPPORTS-SUIVI : journaux de suivi. La DGAC doit conserver les journaux identifiant le contenu du support, la protection appliquée, ainsi que les dates et heures de remise au transporteur de confiance et de réception par le destinataire.

IX. Contrôle d'accès

A. Exigences métier en matière de contrôle d'accès

Objectif : Limiter l'accès à l'information et aux moyens de traitement de l'information.

Politique de contrôle d'accès

ACCES-POLITIQUE : politique de contrôle d'accès. La DGAC doit définir des règles de contrôles d'accès logiques et physiques. Cette politique doit préciser la liste des groupes utilisateurs et leurs droits associés.

Accès aux réseaux et aux services en réseau

ACCES-RESEAUX : droits d'accès. Les droits d'accès aux ressources doivent être gérés suivant les principes suivants : besoin d'en connaître et moindre privilège.

ACCES-AUTHENTIFICATION : identification et authentification. 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. Le contrôle d'accès doit être géré et s'appuyer sur un processus formalisé.

B. Gestion de l'accès utilisateur

Objectif : Maîtriser l'accès utilisateur par le biais d'autorisations et empêcher les accès non autorisés aux systèmes et services d'information.

Enregistrement et désinscription des utilisateurs

ACCES-ENREGISTREMENT : procédure d'enregistrement et de désinscription. La DGAC doit définir une procédure formelle d'enregistrement et de désinscription du personnel ou tiers de la DGAC dans le but de permettre l'attribution de droits d'accès.

Maîtrise de la gestion des accès utilisateur

ACCES-AUTORISATION : autorisations d'accès. Toute autorisation d'accès d'un utilisateur à une ressource informatique, qu'elle soit locale ou nationale, doit s'inscrire dans le cadre d'un processus d'autorisation formalisé.

ACCES-PROFILS : gestion des profils. Les applications manipulant des données sensibles doivent permettre une gestion fine par profil d'accès. L'attribution des droits d'accès utilisateurs est soumise à l'accord formel d'un responsable clairement identifié et autorisé.

Gestion des privilèges d'accès

PRIVILEGES-ATTRIBUTION : attribution des privilèges. L'attribution d'un accès et des privilèges associés (compte et domaine) s'effectue selon une procédure validée par le RSI (consigne PSSI Niveau 3), en conformité avec les habilitations accordées à l'utilisateur pour la réalisation de ses missions et dans le respect des principes de responsabilités (séparation des pouvoirs, moindre privilège).

Le nombre de personnes habilitées pour des opérations d'administration doit être connu et validé par l'autorité d'homologation (DG de la DGAC).

PRIVILEGES-SEPARATION : séparation des privilèges. Chaque privilège d'accès doit être attribué avec un identifiant spécifique et dissocié du compte nominatif.

PRIVILEGES-CONTROLE : suivi et contrôle des privilèges. La DGAC doit établir la liste des personnels disposant de privilèges d'accès aux systèmes, avec le suivi des attributions, modifications, suppressions. Ces points doivent être contrôlés de manière à s'assurer que les règles de sécurité de la DGAC ne sont pas outrepassées.

PRIVILEGES -DOMAINES : nomenclature des comptes du domaine. La gestion des comptes d'un domaine doit s'appuyer sur une nomenclature adaptée, afin de distinguer selon leur usage les comptes d'utilisateur, comptes d'administration et comptes de service.

PRIVILEGES-ADMINISTRATEUR : gestion des comptes d'administrateur. La DGAC interdit la réutilisation des empreintes d'un compte administrateur local d'une machine à une autre. Les privilèges d'accès administrateur doivent être utilisés uniquement pour les actions d'administration le nécessitant.

PRIVILEGES-SERVICES : maîtrise 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. Les droits des comptes de service doivent faire l'objet de restrictions, en suivant le principe du moindre privilège. Il est nécessaire de désactiver immédiatement, voire de supprimer, les comptes obsolètes.

Gestion des informations secrètes d'authentification des utilisateurs

AUTHENTIFICATION-ENGAGEMENT : non-divulgaration des informations d'authentification. Les utilisateurs doivent signer une déclaration par laquelle ils s'engagent à ne pas divulguer leurs informations secrètes d'authentification personnelle.

AUTHENTIFICATION-COMMUNICATION : communication des informations secrètes. La communication à l'utilisateur des informations secrètes d'authentification temporaires doit être effectuée de manière sécurisée. L'utilisateur doit accuser réception des informations secrètes d'authentification.

AUTHENTIFICATION-ADMINISTRATEUR : séquestre des authentifiants administrateur. Les authentifiants permettant l'administration des ressources (données sensibles) doivent être placés sous séquestre et tenus à jour, dans un coffre ou une armoire fermée à clé. Tout accès d'administration à une ressource informatique doit pouvoir être tracée. Chaque administrateur doit disposer d'un mot de passe propre et destiné à l'administration, respectant les règles de solidité requise.

Revue des droits d'accès utilisateur

REVUE-UTILISATEUR : revue des autorisations d'accès. Une revue des autorisations d'accès des utilisateurs doit être réalisée annuellement sous le contrôle du RSSI de la DGAC ou son suppléant. Tout changement de poste au sein de la DGAC impose une revue des autorisations d'accès et une réattribution des accès et autorisation associées.

Suppression ou adaptation des droits d'accès

SUPPRESSION-UTILISATEUR : départ d'un utilisateur. Tout départ ou fin de contrat d'un utilisateur impose la suppression ou la suspension des droits d'accès à l'information et aux systèmes d'information (accès logique et physique).

SUPPRESSION-ADMINISTRATEUR : départ d'un administrateur. 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.

C. Responsabilités des utilisateurs

Objectif : Rendre les utilisateurs responsables de la protection de leurs informations d'authentification.

Utilisation d'informations secrètes d'authentification

INFORMATIONS-AUTHENTIFICATION : protection des informations secrètes d'authentification. Les utilisateurs de la DGAC sont responsables de leurs informations secrètes d'authentification. A ce titre ils doivent assurer leur protection pour éviter l'usurpation d'identité.

D. Contrôle de l'accès au système et aux applications

Objectif : Empêcher les accès non autorisés aux systèmes et aux applications.

Restriction d'accès à l'information

INFORMATIONS-RESTRICTION : restriction d'accès. Sauf dérogation dûment motivée et validée par le RSSI, les utilisateurs n'ont pas de droits d'administration. L'accès aux outils et interfaces d'administration doit être strictement limité aux personnes habilitées, avec le principe de moindre privilège, selon une procédure formelle.

Sécuriser les procédures de connexion

CONNEXION-INTERNET : passerelle Internet. Les interconnexions Internet passent obligatoirement par des passerelles homologuées par la DGAC.

CONNEXION-CERTIFICATS : utilisation de certificats électroniques. L'utilisation de certificats électroniques doit respecter les règles édictées par le RGS 2.0.

CONNEXION-TRACES : enregistrement des connexions. Toute connexion aux réseaux de la DGAC, qu'elle soit réussie ou avortée, doit être enregistrée dans un journal de connexion.

CONNEXION-EXPLOITATION : exploitation des connexions. L'exploitation des journaux de connexion doit être assurée par le service désigné pour cette activité.

Système de gestion des mots de passe

MDP-ADMINISTRATION : stratégie des mots de passe. La gestion des mots de passe doit être adaptée pour faire face aux attaques par essais successifs. La complexité et le renouvellement des mots de

passer (utilisateur, administrateur) doivent être imposés par les systèmes de la DGAC. Un contrôle périodique des paramètres techniques relatifs aux mots de passe doit être réalisé.

Utilisation de programmes utilitaires à privilèges

ACCES-UTILITAIRE : utilisation de programmes utilitaires. Certains utilitaires à privilège, permettant de contourner les mesures de sécurité d'un système ou d'une application, doivent être interdits sauf dérogation particulière du RSSI ou de son suppléant, après étude approfondie de l'utilitaire.

Contrôle d'accès au code source des programmes

ACCES-CODE SOURCE : sécurité du code source. La DGAC doit protéger l'accès au code source de ses programmes contre l'introduction de fonctionnalité illégitime ou toute modification involontaire ou malveillante.

X. Cryptographie

A. Mesures cryptographiques

Objectif : Garantir l'utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information.

Politique d'utilisation des mesures cryptographiques

CRYPTO-POLITIQUE : politique relative à la cryptographie. La DGAC doit établir une procédure qui précise l'utilisation des mesures cryptographiques et de leur contexte d'emploi.

Gestion des clés

CLES-GESTION : gestion des clés. La DGAC doit mettre en œuvre une gestion des clés cryptographiques au regard de leur utilisation, protection et durée de vie. Les exigences de gestion des clés cryptographiques, couvrant l'ensemble de leur cycle de vie : génération, stockage, archivage, extraction, attribution, retrait et destruction des clés, doivent être définies.

Le matériel utilisé pour générer, stocker et archiver les clés doit être placé en lieux sûrs et disposer d'une protection physique.

XI. Sécurité physique et environnementale

A. Zones sécurisées

Objectif : empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information de l'organisation.

Périmètre de sécurité physique

PHYSIQUE-ZONES : zones de sécurité. La DGAC doit définir des zones physiques de sécurité (espace public, zone protégée, zone réservée, locaux techniques, ...) selon l'emploi et la sensibilité des informations traitées, avec des critères précis d'autorisation d'accès et de traçabilité pour chaque zone.

PHYSIQUE-SURETE : sûreté des zones. Pour chaque zone, la DGAC doit adapter les dispositifs techniques et les mesures de protection en se basant sur les conclusions d'une analyse de risques simplifiée et les bonnes pratiques en vigueur (ANSSI, ISO 27002, RGS, ...).

L'emploi de produits labellisés, quand ils existent, est fortement recommandé.

Contrôles physiques des accès

PHYSIQUE-CONTROLE : contrôle d'accès physiques. La délivrance des accès physiques doit respecter un processus formel permettant de s'assurer de l'identité de la personne.

Le personnel autre que la DGAC, autorisé et habilité, pouvant intervenir dans les zones protégées ou réservées (entretien ou réparation des bâtiments, des équipements, nettoyage, visiteurs, ...), intervient systématiquement et impérativement sous la surveillance permanente d'un personnel de la DGAC.

PHYSIQUE-TRACES : traçabilité des accès. La traçabilité des accès aux zones réservées doit être mise en place. Ces traces sont conservées dans un délai conforme à la réglementation en vigueur et protégeant les données personnelles.

Sécurisation des bureaux, des salles et des équipements

PHYSIQUE-IDENTIFICATION : identification des locaux techniques. Les locaux techniques sensibles (salles serveurs, locaux techniques, ...) ne doivent pas être identifiés par un affichage explicite.

PHYSIQUE-PROTECTION : protection des locaux techniques. Les locaux techniques sensibles (salles serveurs, locaux techniques, ...) doivent disposer de portes et de fenêtres physiquement adaptées. Ces locaux doivent être exclusivement réservés à leur fonction principale (absence de stockage ou activités diverses).

PHYSIQUE-TECHNIQUE : sécurité physique des locaux techniques. Les accès aux locaux techniques (serveurs, énergie, climatisation, réseau, téléphonie,) doivent bénéficier d'un contrôle d'accès avec traçabilité.

PHYSIQUE-FILTRAGE : filtre de confidentialité. Tout poste de travail (fixe et mobile) affichant des données sensibles, doit posséder un filtre de confidentialité.

Protection contre les menaces extérieures et environnementales

MENACES-INCENDIE : lutte contre l'incendie. L'installation de matériel de protection contre le feu et adapté à une salle informatique est obligatoire, comme notamment un dispositif d'extinction par gaz argon, ou équivalent. Des procédures de réaction à un incendie sont définies et régulièrement testées.

MENACES-EAU : lutte contre les voies d'eau. Les locaux techniques sensibles (salles serveurs, locaux techniques, ...) doivent être positionnés pour ne pas être soumis à des voies d'eau (canalisation, crues) et posséder une détection contre l'eau (détecteur d'humidité placé dans le faux plancher avec marquage apparent).

MENACES-MAGNETIQUE : exposition champ magnétique. Les zones hébergeant les systèmes d'information doivent être protégées contre les risques accidentels ou intentionnels d'exposition à des champs magnétiques suffisamment élevés pour perturber le bon fonctionnement des équipements informatiques et réseaux.

Travail dans les zones sécurisées

ZONES-RESTRICTION : restrictions dans les zones sécurisées. Les équipements photographiques, vidéos, audio ou tout autre dispositif d'enregistrement, sont strictement interdits, sauf autorisation formelle. Tout travail au sein des zones sécurisées doit faire l'objet d'une supervision ou d'un encadrement.

Zones de livraison et de chargement

ZONES-LIVRAISON : restrictions des zones de livraison et parking. Les zones de livraison et parking sous-bâtiment doivent être équipés de systèmes de protection adaptés (badge, contrôle physique) et de surveillance vidéo avec enregistrement.

B. Matériels

Objectif : Empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de l'organisation.

Emplacement et protection du matériel

MATERIEL-PROTECTION : protection du matériel. Tout matériel de la DGAC doit être à l'abri de risque accidentel ou intentionnel (eau, feu, poussière, projection de produit, ...).

MATERIEL-VERROUILLAGE : verrouillage de l'unité centrale. Toute unité centrale d'un poste fixe doit être protégée contre le vol par un système d'attache (câble antivol).

Services généraux

SG-FONCTIONNEMENT : continuité des services généraux. Les locaux techniques sensibles (salles serveurs, locaux techniques, ...) doivent être équipés de sondes permettant la remontée d'alerte, en cas de dysfonctionnement ou de malveillance, vers le poste de sécurité. Chaque dispositif est contrôlé et testé régulièrement.

SG-ENERGIE : local énergie. L'alimentation secteur des équipements doit être conforme aux règles de l'art, de façon à se prémunir de tout défaut électrique pouvant altérer la continuité et la résilience du service.

SG-PROCEDURES : procédures de réaction. Des procédures de réaction en cas de panne ou malveillance, formalisées et connues du personnel, doivent être mise à jour et contrôlées régulièrement.

Sécurité du câblage

CABLAGE-TELECOM : protection des câbles. Les câbles réseau et de télécommunication doivent être protégés contre les dommages et les interceptions. Les tableaux de raccordements et les salles techniques doivent être exclusivement réservés à leur fonction, placés en dehors des zones d'accueil du public et leur accès doit être contrôlé.

Maintenance du matériel

MAINTENANCE-EXPLOITATION : maintenance interne et externe. Les opérations de maintenance sont effectuées par des personnels identifiés et habilités. Avant de remettre le matériel en service à l'issue de sa maintenance, la DGAC doit l'inspecter pour vérifier qu'il n'a pas subi d'altération et qu'il est fonctionnel.

MAINTENANCE-TRACES : traçabilité des interventions. La maintenance sur les ressources informatiques doit être tracée. Ces traces doivent être auditable.

MAINTENANCE-EQUIPEMENT : maintenance du matériel. La DGAC doit disposer d'un stock de rechange directement accessible et en volume suffisant pour faire face à tout besoin immédiat.

Sortie des actifs

ACTIFS-SORTIE : sortie de matériel. Toute sortie de matériel, logiciel, document, ... des locaux de la DGAC doit faire l'objet d'une autorisation formelle préalable. Toute sortie et retour d'actif doit être consigné.

Sécurité du matériel et des actifs hors des locaux

ACTIFS-HORS LOCAUX : sécurité du matériel hors des locaux. Tout matériel utilisé hors des locaux de la DGAC fait l'objet de mesures de sécurité particulière tenant compte de sa vulnérabilité (ordinateur portable, support de stockage amovible, ...).

Mise au rebut ou recyclage sécurisé(e) du matériel

REBUT-MATERIEL : mise au rebut. Lorsqu'une ressource informatique doit quitter définitivement la DGAC, les données présentes sur les disques durs ou la mémoire intégrée doivent être effacées de manière sécurisée. L'effacement des données sensibles doit s'appuyer sur des produits qualifiés, ou respecter des procédures établies par l'ANSSI.

REAFFECTATION-MATERIEL : réaffectation de matériels. Une procédure de gestion des postes et supports dans le cadre du départ de personnel ou d'une réaffectation doit être mise en place et validée par le RSSI.

Matériel utilisateur laissé sans surveillance

MATERIEL-VIGILANCE : matériel sans surveillance. Tout utilisateur de la DGAC doit être sensibilisé aux bonnes pratiques permettant de protéger les matériels laissés sans surveillance, ainsi qu'aux responsabilités qui leur incombent.

Politique du bureau propre et de l'écran vide

PROTECTION-BUREAU : politique du bureau propre. Tout collaborateur ou tiers ne doit pas laisser d'information ou de documents sensibles (papier, support de stockage) sur son bureau ou en libre d'accès. Ces documents et données doivent être placés sous clé (par exemple dans un coffre-fort, une armoire ou tout autre meuble de sécurité), notamment lorsque les locaux sont vides.

PROTECTION-ECRAN : politique de l'écran vide. Tout collaborateur ou tiers ne doit pas laisser d'information ou de documents sensibles sur leur écran (bureau logiciel) d'ordinateur.

XII. Sécurité liée à l'exploitation

A. Procédures et responsabilités liées à l'exploitation

Objectif : S'assurer de l'exploitation correcte et sécurisée des moyens de traitement de l'information.

Procédures d'exploitation documentées

DOCUMENTATION-EXPLOITATION : documentation des configurations. Les procédures d'administration et d'exploitation des systèmes d'information doivent être documentées, maintenues à jour et les responsabilités associées sont attribuées.

DOCUMENTATION-CARTOGRAPHIE : documentation d'architecture technique et fonctionnelle. L'architecture réseau des systèmes d'information doit être décrite et formalisée et mise à jour sous forme de schémas d'architecture et de configuration. Les documents d'architecture (cartographie) sont sensibles et font l'objet d'une protection adaptée.

Gestion des changements

EXPLOITATION-CHANGEMENT : gestion des changements. Tout changement dans l'organisation (processus, système, moyens de traitement de l'information, ...) qui pourrait avoir une influence sur la sécurité de l'information doit faire l'objet d'une attention particulière et être contrôlé.

Dimensionnement

EXPLOITATION-DIMENSIONNEMENT : gestion du dimensionnement. Lors d'une implémentation ou une modification d'un système, son dimensionnement doit être adapté en fonction des ressources nécessaires et aux besoins des métiers.

Séparation des environnements de développement, test et exploitation

EXPLOITATION-ENVIRONNEMENT : séparation des environnements. Les environnements de développement, test et exploitation doivent être séparés et avoir des fonctions et droits différents. L'environnement de test ne doit contenir aucune donnée confidentielle, secrète ou de production. Aucun test ne doit être effectué dans un environnement d'exploitation (production). Les environnements ne doivent pas pouvoir communiquer entre eux ou faire l'objet de procédures et autorisation spéciales.

B. Protection contre les logiciels malveillants

Objectif : Garantir que l'information et les moyens de traitement de l'information sont protégés contre les logiciels malveillants.

Mesures contre les logiciels malveillants

EXPLOITATION-CODES : protection contre les codes malveillants. Des logiciels de protection contre les codes malveillants doivent être installés sur l'ensemble des serveurs d'interconnexion, serveurs applicatifs et postes de travail de l'entité. Les mises à jour des bases antivirales et des moteurs d'antivirus doivent être déployées automatiquement sur les serveurs et les postes de travail. Ces

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

EXPLOITATION-EVENEMENTS : gestion des événements. Les événements de sécurité de l'antivirus doivent être remontés sur un serveur central pour analyse statistique et gestion des problèmes a posteriori.

EXPLOITATION-CORRECTIFS : suivi et application des correctifs. 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.

C. Sauvegarde

Objectif : Se protéger de la perte de données.
--

Sauvegarde des informations

INFORMATIONS-SAUVEGARDE : sauvegarde des données. La DGAC doit définir une procédure de sauvegarde des données (synchronisation, fréquence, type, test, ...) et tenir à jour un plan de sauvegarde de ses données. Les sauvegardes doivent être réalisées de manière à ce que l'intégrité et la confidentialité soient garanties. Si les données sont sensibles, les sauvegardes doivent être chiffrées.

D. Journalisation et surveillance

Objectif : Enregistrer les événements et générer des preuves.

Journalisation des événements

JOURNALISATION-ALERTES : journalisation des alertes. Chaque compte système doit disposer d'une journalisation permettant de conserver une trace des événements de sécurité. La politique de gestion et d'analyse des journaux est définie par les responsables métiers, puis validée par le RSSI de la DGAC.

JOURNALISATION-ARCHIVAGE : conservation des journaux. Les journaux des événements de sécurité doivent être conservés dans un délai conforme aux contraintes légales et réglementaires. Dans le cas d'une sensibilité particulières (fonctionnelle, sécuritaire ...) imposant des durées de conservation spécifiques, ce délai pourra être augmenté et faire l'objet d'une consigne particulière.

Protection de l'information journalisée

JOURNALISATION-PROTECTION : protection des journaux d'événements. Les supports et informations de journalisation doivent être protégés contre la dégradation et le sabotage et contre tout accès ou altération, et toute suppression ou modification ou exploitation non explicitement autorisée.

Journaux administrateur et opérateur

JOURNALISATION-ADMINISTRATION : journalisation des actions administrateurs. Les activités des administrateurs système et opérateurs doivent être consignées de manière à garantir la traçabilité, voire l'opposabilité juridique, des interventions d'administration des systèmes.

Synchronisation des horloges

SYNCHRONISATION-HORLOGES : synchronisation des horloges. Afin d'assurer une cohérence des échanges entre les serveurs et les applications et une traçabilité pertinente des événements techniques et de sécurité, les services d'exploitation doivent prendre une référence de temps commune.

E. Maîtrise des logiciels en exploitation

Objectif : Garantir l'intégrité des systèmes en exploitation.

Installation de logiciels sur des systèmes en exploitation

EXPLOITATION-LOGICIELS : gestion des logiciels en exploitation. L'installation et la mise à jour des applications doivent être réalisées uniquement par des administrateurs qualifiés, sur la base de procédures formalisées.

EXPLOITATION-MIGRATION : migration des systèmes obsolètes. L'ensemble des logiciels utilisés sur un système d'information doit être à jour des correctifs de sécurité. En cas d'impossibilité justifiée et avérée, des dispositions techniques seront prises pour assurer la sécurité vis-à-vis des systèmes.

Pour qu'une telle dérogation puisse être accordée, un calendrier de retour à la conformité devra être garanti, validé par le RSSI.

F. Gestion des vulnérabilités techniques

Objectif : Empêcher toute exploitation des vulnérabilités techniques.

Gestion des vulnérabilités techniques

VULNERABILITE-GESTION : vulnérabilités techniques. Une gestion des vulnérabilités doit être systématiquement mise en œuvre pour tous les composants des systèmes d'information (bases de données, applications, systèmes et infrastructures), de manière permanente et entretenue.

VULNERABILITE-OS : systèmes d'exploitation. Chaque système d'exploitation déployé doit faire l'objet d'un support de la part de l'éditeur ou d'un prestataire de service. Seuls les services et applications nécessaires sont installés, de façon à réduire la surface d'attaque.

VULNERABILITE-CONFIGURATION : 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 au sein de la DGAC ou, par défaut, en vigueur au niveau du ministère de tutelle.

VULNERABILITE-IMPRIMANTES : imprimantes et copieurs multifonctions. Les imprimantes et copieurs multifonctions doivent faire l'objet d'un durcissement en termes de sécurité (changement du mot de passe par défaut du constructeur, désactivation des interfaces réseau et services inutiles, chiffrement des données, ...).

Une procédure doit préciser les mesures de sécurité relatives aux impressions et récupération d'informations sensibles.

Restrictions liées à l'installation de logiciels

INSTALLATION-LOGICIELS : restriction de l'installation des logiciels. La DGAC doit définir une procédure relative aux droits et à l'installation des logiciels (liste blanche). Tout logiciel installé doit appliquer le principe du moindre privilège.

G. Considérations sur l'audit du système d'information

Objectif : Réduire au minimum l'incidence des activités d'audit sur les systèmes en exploitation.

Mesures relatives à l'audit des systèmes d'information

PLANIFICATION-AUDIT : planification des audits et contrôles. Le RSSI doit être informé des audits réguliers des systèmes d'information relevant de sa responsabilité, lesquels sont planifiés et réalisés par l'autorité de surveillance (DSAC).

XIII. Sécurité des communications

A. Management de la sécurité des réseaux

Objectif : Garantir la protection de l'information sur les réseaux et des moyens de traitement de l'information sur lesquels elle s'appuie.

Contrôle des réseaux

RESEAUX-MAITRISE : systèmes autorisés. Seuls les équipements gérés et configurés par l'équipe d'exploitation habilitée peuvent être connectés au réseau local de la DGAC.

RESEAUX-FILTRAGE : filtrage réseau. Toute connexion réseau vers l'extérieur de la DGAC doit être filtrée.

RESEAUX-INTERCONNEXION : interconnexion des réseaux. Toute interconnexion entre les réseaux locaux de la DGAC et un réseau externe (réseau d'un tiers, Internet, etc.) doit être réalisée via une infrastructure approuvée par la DGAC.

RESEAUX-ACCES : accès aux réseaux. Les accès réseaux (attribution des adresses IP, filtrage des informations, configuration des passerelles, ...) doivent faire l'objet de procédures formelles sécurisées.

Sécurité des services réseaux

RESEAUX-SITES : interconnexion des réseaux locaux. L'interconnexion de réseaux locaux n'est autorisée que si la proximité géographique des sites le justifie et sous réserve de la mise en place de connexions dédiées et de passerelles sécurisées soumises à l'accord du RSSI.

RESEAUX-SANS FIL : réseaux sans fil. Le déploiement d'un réseau sans fil doit être destiné aux personnes externes de passage. Ce réseau doit bénéficier des mesures de protection et de restriction adaptées aux besoins des métiers (connexion chiffrée, filtrage d'adresse MAC, segmentation, etc.).

RESEAUX-ROUTAGE : routage des réseaux. L'utilisation de protocoles de routage dynamiques doit s'accompagner de la mise en place d'une surveillance des annonces de routage et de procédures permettant de réagir rapidement en cas d'incidents.

RESEAUX-AUTHENTIFICATION : authentification des équipements. Les mots de passe par défaut doivent être impérativement modifiés par les utilisateurs ou administrateurs, à la première connexion. Les dispositions nécessaires doivent être prises auprès des fournisseurs de façon à pouvoir modifier les certificats installés par défaut.

RESEAUX-DURCISSEMENT : durcir les configurations. Les équipements réseaux (routeurs, pare-feu, ...) doivent faire l'objet d'un durcissement spécifique comprenant notamment la désactivation des interfaces et services inutiles.

RESEAUX-INTERNET : communication sur internet. Les accès à Internet doivent passer à travers des passerelles sécurisées sous la responsabilité de la DGAC.

RESEAUX-DNS : noms de domaine. Tout serveur de noms de domaines propre à la DGAC doit utiliser les extensions sécurisées DNSSEC.

Cloisonnement des réseaux

RESEAUX-CLOISONNEMENT : cloisonnement des réseaux. Des mécanismes de filtrage et de cloisonnement des réseaux doivent être mis en œuvre pour garantir un niveau de protection suffisant face aux attaques informatiques. Par analogie avec le cloisonnement physique d'un bâtiment, le système d'information doit être segmenté selon des zones justifiant d'un même niveau de confiance.

RESEAUX-ADMINISTRATION : administration des réseaux. Les opérations d'administration doivent s'appuyer sur des protocoles sécurisés. Tout réseau dédié à l'administration doit être séparé du réseau des utilisateurs. Les postes d'administrateurs doivent être dédiés et ne doivent pas pouvoir accéder à Internet.

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

B. Transfert de l'information

Objectif : Maintenir la sécurité de l'information transférée au sein de l'organisation et vers une entité extérieure.

Politiques et procédures de transfert de l'information

COMMUNICATION-PROCEDURES : documentation des procédures. Des procédures doivent être documentées pour traiter les risques liés aux échanges d'informations (interception, reproduction, modification, malveillances, ...).

COMMUNICATION-PROTECTION : protection des communications. Les informations qui transitent sur et en dehors du réseau de la DGAC doivent être protégées contre la perte de confidentialité et d'intégrité. Ces règles s'appliquent aussi bien pour les échanges numériques que pour des conversations dans des lieux publics.

Accords en matière de transfert d'information

ACCORDS-TRANSFERTS : protection des échanges. L'échange d'information classée doit faire l'objet d'un accord formel entre la DGAC et chaque tiers (responsabilités, niveaux de protection, normes et protocoles d'échanges, ...).

Messagerie électronique

MESSAGERIE-COMMUNICATION : échanges via la messagerie. Toute information classée doit être chiffrée par un dispositif de chiffrement approuvé par la DGAC avant d'être communiquée par messagerie électronique.

Engagements de confidentialité ou de non-divulgation

COMMUNICATION-ENGAGEMENT : protection de l'information. Les engagements de confidentialité et de non-divulgation participent à la protection de l'information de la DGAC. Ces documents informent les signataires de leur devoir pour protéger, traiter et diffuser l'information de façon responsable et dans les limites autorisées.

XIV. Acquisition, développement et maintenance des systèmes d'information

A. Exigences de sécurité applicables aux systèmes d'information

Objectif : Veiller à ce que la sécurité de l'information fasse partie intégrante des systèmes d'information tout au long de leur cycle de vie. Cela inclut notamment des exigences spécifiques pour les systèmes d'information fournissant des services sur les réseaux publics.

Analyse et spécification des exigences de sécurité de l'information

ANALYSE-PRODUITS : analyse des spécifications. Les contrats conclus avec les fournisseurs doivent intégrer les exigences de sécurité identifiées, et si besoin, imposer le réexamen des risques et des mesures associées.

Sécurisation des services d'application sur les réseaux publics

SERVICES-PUBLICS : ingénierie sociale. Les informations transmises sur les réseaux publics doivent être protégées contre les activités frauduleuses (usurpation d'identité, hameçonnage, ...), la divulgation et la modification non autorisées.

Protection des transactions liées aux services d'application

SERVICES-TRANSACTIONS : sécurité des transactions. Les informations soumises à des transactions doivent être protégées pour assurer une transmission complète, éviter les erreurs d'acheminement, la modification, la divulgation et la duplication non autorisées du message ou sa réémission.

B. Sécurité des processus de développement et d'assistance technique

Objectif : S'assurer que les questions de sécurité de l'information sont étudiées et mises en œuvre dans le cadre du cycle de développement des systèmes d'information.

Politique de développement sécurisé

DEVELOPPEMENT-INTEGRATION : sécurité dans les développements locaux. Tout développement informatique local doit respecter les exigences de sécurité de la DGAC. Le service à l'origine du projet se porte garant de l'application des référentiels de la DGAC.

DEVELOPPEMENT-FUITES : limiter les fuites d'information. Il est impératif de limiter la diffusion d'informations concernant les matériels et logiciels utilisés, afin de ne pas communiquer indirectement d'éventuelles vulnérabilités.

DEVELOPPEMENT-ADHERENCE : adhérence des technologies. Les applications ne doivent pas avoir de forte adhérence sur leur environnement, car les éventuelles failles d'un environnement ont un impact sur la sécurité des applications. Il est nécessaire de faire évoluer tout environnement pour garantir sa sécurité dans la durée.

DEVELOPPEMENT-CYCLE DE VIE : 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.

DEVELOPPEMENT-MOTS DE PASSE : empreintes des mots de passe. Lorsqu'une application doit stocker les mots de passe de ses utilisateurs, il est indispensable de mettre en œuvre des mesures permettant de se prémunir contre les différentes formes d'attaques documentées.

Procédures de contrôle des changements apportés au système

CONTROLE-CHANGEMENTS : contrôle des changements. Toute modification ou évolution apportée aux systèmes d'information doit être formalisée, tracée et contrôlée.

Revue technique des applications après changement apporté à la plateforme d'exploitation

REVUE-CHANGEMENTS : revue après des changements. Les applications critiques métiers doivent être revues et testées lorsque des changements sont apportés aux plateformes d'exploitation (systèmes d'exploitation, bases de données, logiciels médiateurs). Cette mesure permet de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité.

Restrictions relatives aux changements apportés aux progiciels

RESTRICTIONS-CHANGEMENTS : restrictions des changements. Il est nécessaire de ne pas apporter de changements aux progiciels fournis par les éditeurs. Lorsque des changements s'avèrent nécessaires, il convient de conserver le logiciel original et d'appliquer ces changements à une copie clairement identifiée.

Principes d'ingénierie de la sécurité des systèmes

INGENIERIE-SYSTEMES : ingénierie des systèmes. La sécurité doit être intégrée à tous les niveaux de l'architecture des systèmes d'information (activité, données, applications, technologie) en préservant l'équilibre entre la sécurité et l'accessibilité des informations. Il convient d'analyser les nouvelles technologies au regard de leurs vulnérabilités et par rapport aux attaques connues.

Environnement de développement sécurisé

ENVIRONNEMENT-DEVELOPPEMENT : sécurité du développement. Une démarche sécurisée doit être formalisée et mise en place tout au long du cycle de vie des activités liées au développement et à l'intégration des systèmes d'information.

Développement externalisé

DEVELOPPEMENT-CLAUSES : contrats de sous-traitance. Des clauses de sécurité (documentation technique, processus sécurisé, respect des normes, phases de contrôle et de test, ...) doivent être intégrées dans les contrats de sous-traitance liés au développement applicatif.

Phase de test de la sécurité du système

DEVELOPPEMENT-TEST : test des systèmes. Tout nouveau système, ou mis à jour, doit être soumis à des tests et à des contrôles durant le processus de développement.

Test de conformité du système

DEVELOPPEMENT-CONFORMITE : conformité des systèmes. Il est recommandé de procéder à des tests indépendants pour les développements internes et externalisés pour assurer la conformité de fonctionnement des systèmes.

C. Données de test

Objectif : Garantir la protection des données utilisées pour les tests.

Protection des données de test

DEVELOPPEMENT-PROTECTION : protection des données. Les données de test doivent être sélectionnées avec soin, protégées et contrôlées afin qu'aucune référence à des données personnelles soit mentionnée.

XV. Relations avec les fournisseurs

A. Sécurité de l'information dans les relations avec les fournisseurs

Objectif : Garantir la protection des actifs de l'organisation accessibles aux fournisseurs.

Politique de sécurité de l'information dans les relations avec les fournisseurs

PRESTATAIRES-POLITIQUE : relations avec les fournisseurs. Une politique précisant les mesures de sécurité spécifiques aux accès physiques et logiques des fournisseurs, sur les systèmes d'information de la DGAC, doit être formalisée et communiquée aux personnes concernées.

La sécurité dans les accords conclus avec les fournisseurs

PRESTATAIRES-CLAUSES : clauses de sécurité. Toute demande de prestation est soumise à l'accord préalable signé de la politique (évoquée précédemment) par le fournisseur ou prestataire.

PRESTATAIRES-ACCORDS : gestion contractuelle des tiers. Le RSSI coordonne les actions permettant l'intégration des clauses SSI dans tout contrat ou convention impliquant un accès par des tiers à des informations ou à des ressources informatiques.

Chaine d'approvisionnement informatique

PRODUITS-LABELLISES : produits et services de confiance. Lorsqu'ils sont disponibles et dans la mesure du possible, suite à une étude de faisabilité menée par la DGAC, des produits ou des services de sécurité labellisés (certifiés, qualifiés) par l'ANSSI doivent être utilisés.

B. Gestion de la prestation du service

Objectif : Maintenir un niveau convenu de sécurité de l'information et de prestation de services, conformément aux accords conclus avec les fournisseurs

Surveillance et revue des services des fournisseurs

PRESTATAIRES-RISQUES : 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.

PRESTATAIRES-CONTROLE : suivi et contrôle des prestations. Des opérations de surveillance et de contrôle des prestations (audits des fournisseurs, revue des procédures, suivi des pannes, ...) doivent être menées afin de garantir le niveau de sécurité prévu dans les accords.

Gestion des changements apportés dans les services des fournisseurs

PRESTATAIRES-CHANGEMENTS : gestion des changements. Les changements nécessaires dans les prestations de service des fournisseurs, doivent être anticipés et gérés afin de limiter les risques inhérents et d'assurer l'amélioration continue de la sécurité des systèmes d'information.

XVI. Gestion des incidents liés à la sécurité de l'information

A. Gestion des incidents liés à la sécurité de l'information et améliorations

Objectif : Garantir une méthode cohérente et efficace de gestion des incidents liés à la sécurité de l'information, incluant la communication des événements et des failles liés à la sécurité.

Responsabilités et procédures

INCIDENTS-CHAINE : chaîne opérationnelle SSI. La DGAC doit définir et mettre en place une chaîne fonctionnelle SSI pour gérer dans les délais les incidents de sécurité. Les alertes et les incidents doivent être gérés selon des procédures formalisées et testées lors d'exercices réguliers. Les situations d'urgence peuvent faire appel à des mesures définies préalablement dans le cadre de plans gouvernementaux.

Signalement des événements liés à la sécurité de l'information

INCIDENTS-REMONTEES : remontées des incidents. Tout incident de sécurité dont l'impact dépasse ou est susceptible de dépasser le périmètre de la DGAC, ou impacte gravement un de ses systèmes d'information, doit faire l'objet d'un compte-rendu, via la chaîne SSI (ministère de tutelle), ou au Centre opérationnel de la sécurité des systèmes d'information (COSSI) de l'ANSSI.

Signalement des failles liées à la sécurité de l'information

INCIDENTS-SIGNALEMENT : signalement des incidents. Toute faille de sécurité observée ou soupçonnée dans les systèmes ou services, par un utilisateur ou prestataire, doit faire l'objet d'un compte-rendu immédiat, sous une forme simple et précise. Ce compte-rendu est communiqué à la chaîne hiérarchique SSI jusqu'au RSSI qui en avisera, selon l'importance, la direction de la DGAC.

Appréciation des événements liés à la sécurité de l'information et prise de décision

INCIDENTS-EVENEMENTS : appréciation des événements. La DGAC doit définir et formaliser une procédure de réaction face aux événements susceptibles d'impacter les informations métiers. Cette procédure doit identifier chaque événement sous forme d'une fiche (type d'évènement, les acteurs, les responsabilités, les délais, les mesures à prendre, ...).

Réponse aux incidents liés à la sécurité de l'information

INCIDENTS-REPONSES : réponses aux incidents. La DGAC doit se doter d'une équipe de réponse aux incidents de sécurité de l'information, afin d'intervenir rapidement, de qualifier chaque événement, d'apprécier son impact sur les métiers et de prendre la meilleure décision pour sa résolution.

Tirer des enseignements des incidents liés à la sécurité de l'information

INCIDENTS-ENSEIGNEMENTS : enseignements tirés des incidents. La DGAC doit mettre en place une organisation afin de tirer parti des connaissances recueillies suite à l'analyse et la résolution des incidents liés à la sécurité de l'information. Cette mesure doit permettre de réduire la probabilité ou les conséquences d'incidents ultérieurs.

Recueil de preuves

INCIDENTS-PREUVES : recueil de preuves. La DGAC doit mettre en place une organisation afin d'identifier, recueillir, qualifier et protéger toute information pouvant servir de preuve. Si besoin, ces preuves devront être communiquées (transmission chiffrée) au ministère de tutelle ou à l'ANSSI.

XVII. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

A. Continuité de la sécurité de l'information

Objectif : Il convient que la continuité de la sécurité de l'information fasse partie intégrante des systèmes de gestion de la continuité de l'activité.

Organisation de la continuité de la sécurité de l'information

PCA-ORGANISATION : définition du PCA. La DGAC doit définir et formaliser un plan de continuité d'activité de ses systèmes d'information. La mise en application de ce plan permettra à la DGAC de faire face à tout sinistre impactant ses systèmes d'information. Ce document est validé par le comité de sécurité des SI de la DGAC.

Mise en œuvre de la continuité de la sécurité de l'information

PCA-EXECUTION : mise en œuvre du PCA. Tout personnel (interne ou prestataire) qui possède les responsabilités et les compétences nécessaires (métier et technique) doit être mobilisé pour participer à la mise en œuvre de la continuité d'activité de la DGAC. Les équipes informatiques mettant en œuvre les dispositifs techniques et les procédures opérationnelles contribuant à la continuité des SI, en assurent la supervision au quotidien et la maintenance dans le temps.

PCA-SUIVI : suivi du PCA. Le comité de sécurité des SI de la DGAC doit s'assurer en permanence du niveau de mise en œuvre opérationnelle des dispositions prévues dans le plan de continuité d'activité des systèmes d'information.

Vérifier, revoir et évaluer la continuité de la sécurité de l'information

PCA-EXERCICES : exercices PCA. Le RSSI, en lien avec l'organisation de la Continuité d'Activité doit définir, formaliser des tests ponctuels et organiser des exercices réguliers, afin d'évaluer la conformité du plan de continuité d'activité des systèmes d'information. Chaque test ou exercice fera l'objet d'un compte-rendu détaillé permettant d'identifier les insuffisances et de dégager les axes d'amélioration à consentir.

PCA-MISE A JOUR : mise à jour du PCA. Le RSSI, en lien avec l'organisation de la Continuité d'Activité doit s'assurer du maintien en condition opérationnel (MCO) du plan de continuité d'activité des systèmes d'information.

B. Redondances

Objectif : Garantir la disponibilité des moyens de traitement de l'information.

Disponibilité des moyens de traitement de l'information

PCA-REDONDANCE : redondance des moyens. Le RSSI, en lien avec l'organisation de la Continuité d'Activité doit s'assurer de la redondance des dispositifs techniques critiques et indispensables au maintien de la continuité d'activité des systèmes d'information. Il convient également de s'assurer des suppléances pour les fonctions devant répondre aux exigences de disponibilité (gestion de l'alerte, gestion de crise, résolution du sinistre, compte-rendu opérationnel, ...).

XVIII. Conformité

A. Conformité aux obligations légales et réglementaires

Objectif : Éviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité de l'information, éviter toute violation des exigences de sécurité.

Identification de la législation et des exigences contractuelles applicables

CONFORMITE-I&L : Conformité avec la Loi Informatique et Libertés. La DGAC doit être en conformité avec le cadre législatif Français en matière de protection des données à caractère personnel telles que définies dans la loi n°78-17 du 6 janvier 1978 modifiée par la loi du 6 août 2004, dite loi Informatique et Libertés.

CONFORMITE-RGPD : Conformité avec le Règlement Général de Protection des Données. La DGAC doit être en conformité avec le cadre réglementaire Européen en matière de protection des données à caractère personnel telles que définies par le Règlement Général de Protection des Données (RGPD), adopté par le parlement Européen le 14 avril 2016 et qui entrera en application le 25 mai 2018.

A noter que tout traitement de données à caractère personnel mis en œuvre par un organisme, après le 25 mai 2016, doit d'ores et déjà être conforme aux obligations réglementaires en matière de protection des données à caractère personnel.

CONFORMITE-VEILLE : Veille réglementaire et législative. La DGAC doit rédiger une procédure de veille juridique sur les aspects de protection des données à caractère personnel. Le cadre législatif Français et le cadre réglementaire Européen évoluant de manière permanente, il est donc important que des ressources surveillent régulièrement l'impact de cette évolution sur la DGAC.

Droits de propriété intellectuelle

DROITS-PROPRIETE : propriété intellectuelle. Des procédures doivent être formalisées et mises en application afin de garantir la conformité avec les exigences légales, réglementaires et contractuelles relatives aux droits de propriété intellectuelle et à l'utilisation de logiciels propriétaires. Des séances de sensibilisation des utilisateurs seront régulièrement dispensées sur ces aspects (droit d'auteur, action judiciaire, poursuite pénale).

Protection des enregistrements

ENREGISTREMENTS-PROTECTION : protection des enregistrements. La DGAC doit mettre en place les moyens humains, organisationnels et techniques afin de protéger les enregistrements contre la perte, la destruction, la falsification, les accès et les diffusions non autorisés conformément aux exigences légales, réglementaires, contractuelles et exigences métiers.

Protection de la vie privée et protection des données à caractère personnel

DONNEES-PROTECTION : protection des données. La DGAC et ses sous-traitants doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité des données à caractère personnel. Il est recommandé que la DGAC désigne un CIL et DPO pour

conseiller les responsables, les utilisateurs et les prestataires de services sur leurs responsabilités individuelles et les procédures spécifiques qu'il convient de respecter.

DONNES-VIOLATION : notification d'une violation de données. En cas de violation de données, la DGAC en informe la CNIL dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance. Lorsque la notification à la CNIL n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard. Une procédure de notification de violation de données à caractère personnel, à destination de l'autorité de contrôle compétente (CNIL) doit être rédigée et mise en œuvre. La DGAC doit documenter toute violation de données, en indiquant les faits concernant la violation des données, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à la CNIL de vérifier le respect de cette notification de violation de données.

COMMUNICATION-VIOLATION : communication d'une violation de données. Lorsqu'une violation de données est susceptible d'engendrer un risque élevé pour les droits et les libertés d'une personne physique, la DGAC doit communiquer la violation de données à la personne concernée dans les meilleurs délais.

DONNEES-IMPACT : impact sur la protection des données. Lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, la DGAC doit effectuer, au préalable, une analyse de l'impact du traitement sur la protection des données. Le délégué à la protection des données (DPO) effectue une étude d'impact sur la vie privée (EIVP). La DGAC doit effectuer des EIVP sur l'ensemble des opérations de traitement listé et publié par la CNIL.

DONNEES-DPO : délégué à la protection des données. La DGAC, en tant qu'organisme public, doit désigner un délégué à la protection des données (DPO). Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et de ses connaissances du droit en matière de protection des données. La DGAC doit publier les coordonnées du délégué à la protection des données (publication publique) et les communiquer à la CNIL.

Réglementation relative aux mesures cryptographiques

DONNEES-CRYPTOGRAPHIE : mesures cryptographiques. Des mesures cryptographiques doivent être prises conformément aux accords, lois et réglementations applicables. Il est recommandé d'utiliser des solutions de cryptographie homologuées par l'ANSSI.

B. Revue de la sécurité de l'information

Objectif : Garantir que la sécurité de l'information est mise en œuvre et appliquée conformément aux politiques et procédures organisationnelles.

Revue indépendante de la sécurité de l'information

REVUE-CONTROLE : contrôle régulier. Le RSSI et l'autorité de surveillance (DSAC) doivent réaliser un contrôle régulier du niveau de maturité de la sécurité des systèmes d'information et de conformité vis-à-vis des exigences réglementaires auxquelles la DGAC est soumise. Les résultats seront transmis au comité de sécurité et si besoin au ministère de tutelle et à l'ANSSI. Cette mesure permet de contrôler l'amélioration continue de la sécurité des systèmes d'information.

REVUE-TDB : tableau de bord. Le RSSI doit mettre en place un tableau de bord SSI et le tenir à jour. Il fournit au comité de sécurité des SI et aux différentes directions une vision générale du niveau de sécurité et de son évolution, rendant ainsi plus efficace le pilotage de la SSI.

Conformité avec les politiques et les normes de sécurité

CONFORMITE-NORMES : conformité avec les normes. Les différents acteurs en charge de la sécurité des systèmes d'information de la DGAC, et en dernier recours l'autorité de surveillance (DSAC), doivent contrôler la conformité du traitement de l'information et des procédures dont ils sont responsables au regard des politiques (PSSIE, PSSI DGAC), normes de sécurité applicables (ISO 27001, NIST 800-53, ...) et exigences de sécurité (ANSSI, LPM, CNIL).

Examen de la conformité technique

CONFORMITE-EXAMEN : examen de la conformité. La DGAC doit contrôler régulièrement ses systèmes d'information en procédant à des audits techniques (configuration, architecture, code, intrusion) afin d'évaluer leur niveau de conformité au regard des normes et exigences de sécurité.

Gestion des dérogations

CONFORMITE-DEROGATION : dérogation. Des exceptions à la conformité sont envisageables si elles sont dûment justifiées. Les demandes sont transmises au RSSI de la DGAC pour décision. Les dérogations lorsqu'elles sont acceptées, sont bornées dans le temps. Elles doivent être gérées et suivies régulièrement. Par délégation du RSSI DGAC, le RSSI NA a autorité pour les dérogations relatives aux systèmes opérationnels du SI Navigation Aérienne.

XIX. Annexe A - Description des Rôles

C. AQSSI

Le directeur général est l'Autorité Qualifiée pour la Sécurité des Systèmes d'Information. A ce titre :

- Il est en charge de la protection des systèmes homologués, de la prise en compte des alertes et des situations d'urgence majeures ;
- 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 ;
- Il organise la mise en œuvre des dispositions de sécurité prises en application de la présente PSSI au sein de son entité ;
- Il nomme le responsable de la sécurité des systèmes d'information (RSSI), ainsi que des relais techniques au sein des équipes opérationnelles ou informatiques.

D. Autorité de surveillance (DSAC)

Conformément aux dispositions du décret n° 2008-1299 créant la direction de la sécurité de l'aviation civile, la DSAC est « chargée de veiller au respect des normes internationales applicables au domaine de l'aviation civile, des réglementations communautaires et des dispositions législatives et réglementaires nationales, en matière de sécurité, de sûreté et d'environnement. Elle est l'autorité de surveillance nationale au sens de l'article 4 du règlement du Parlement européen et du Conseil du 10 mars 200 ».

Plus particulièrement, en son sein, la direction technique « aéroports et navigation aérienne » (DSAC/ANA) est notamment « chargée d'élaborer, de mettre en œuvre et d'animer la politique de sécurité en matière de certification et de surveillance des prestataires des services de la navigation aérienne ». A ce titre, elle est chargée, s'agissant de la DSNA, de la vérification du respect des exigences communes pour la fourniture de services de navigation aérienne fixé par le règlement n° 1035/2011 de la Commission en matière de système de gestion de la sûreté visant à garantir la sûreté de ses installations et de son personnel et la sûreté des données opérationnelles qu'il reçoit, produit ou utilise.

La direction technique « sûreté » (DSAC/SUR) est notamment chargée de « mettre en œuvre le contrôle de la sécurité des systèmes d'information conformément à la politique de la direction générale de l'aviation civile en matière de sécurité des systèmes d'information ». En son sein, le pôle « sécurité des systèmes d'information » (SUR/SSI) :

- « est chargé du contrôle de la sécurité des systèmes d'information dans la DGAC et des organismes extérieurs: pour ces derniers soit directement soit dans le cadre des actions de contrôle exercées par les pôles compétents;
- participe à la cellule d'alerte et d'urgence de la DGAC;
- apporte son expertise aux autres pôles de la DSAC et concourt au développement des exigences de sécurité applicables aux systèmes d'information de la DGAC;

- assure une veille technologique concernant les dispositifs de sécurité informatique et collabore aux études conduites par le secrétariat général de la DGAC;
- assure le développement des systèmes d'aide à la surveillance des exigences de sûreté, utilisé par la DSAC. »

E. RSSI DGAC

Le Responsable de la Sécurité des Systèmes d'Information est nommé par l'AQSSI. Il assume les tâches suivantes :

Maintien en conformité de la PSSI DGAC

La Politique de sécurité des systèmes d'information s'appliquant à l'ensemble des systèmes, opérationnels et de gestion, le RSSI organise son maintien en conformité et ses mises à jour.

Il vérifie notamment, en étroite collaboration avec l'opérateur de navigation aérienne, que les parties relevant de la responsabilité de ce dernier soient établies et maintenues en cohérence avec l'ensemble du référentiel.

Conseil aux acteurs

En particulier, et avec l'aide des relais dans les services (voir rôle des ASSI), il apporte son conseil aux maîtrises d'œuvre et d'ouvrage, ainsi qu'aux services d'exploitation, pour la compréhension, la méthodologie et la mise en œuvre de la PSSI.

Systèmes opérationnels

Pour les systèmes opérationnels, régis par un corpus légal spécifique (LPM, décret et arrêtés sectoriels), se reporter au document applicable du niveau 1 de la présente PSSI. L'allocation des ressources dédiées à la SSI relève de la responsabilité du chef des services de la navigation aérienne. Le RSSI lui apporte son concours dans les phases d'élaboration en tant que de besoin.

Systèmes de gestion

Le RSSI s'assure que les ressources allouées à la sécurité des systèmes d'information de gestion sont en adéquation avec les exigences de sécurité et permettent d'en atteindre les objectifs.

Cette fonction de vérification s'opère dans le cadre d'une comitologie dédiée, en particulier au sein du comité de sécurité des systèmes d'information de gestion.

Contrôles de sécurité

Pour l'ensemble des systèmes, le RSSI veille à la régularité, la conformité et la complétude des contrôles de sécurité, sur la base de la présente instruction. En particulier :

- Il vérifie, auprès de l'autorité de surveillance (DSAC) qui en assure le suivi, que les actions correctives prescrites à l'issue des contrôles de sécurité ou rendues nécessaires par la mise en évidence de failles de sécurité, ont été effectuées dans les délais et les modalités prévues ;
- Il s'assure de la prise en compte des alertes et menaces concernant la sécurité des systèmes ;
- Il organise et anime, en lien avec l'opérateur pour les périmètres qui lui incombent, la chaîne de traitement des alertes et des situations d'urgence concernant la sécurité des systèmes ;

Formation

Le RSSI assure la définition et supervise la mise en œuvre des actions de sensibilisation et de formation pour l'ensemble des agents, à la sécurité des systèmes d'information.

Homologation des systèmes

Le RSSI organise, en lien avec le secrétariat général, l'homologation des systèmes de gestion ; il prononce ces homologations avant leur mise en exploitation.

Pour les systèmes opérationnels, il est informé par l'autorité de surveillance (DSAC) du processus d'homologation, notamment de toute non-conformité qui empêcherait ou retarderait leur mise en exploitation.

Rapports d'activité

Le RSSI établit la synthèse annuelle de la sécurité des systèmes d'information, sur la base des rapports que lui transmettent la direction du transport aérien, le secrétariat général, la direction des services de la navigation aérienne et la direction de la sécurité de l'aviation civile.

Relation institutionnelle

Le RSSI assure la relation avec le FSSI du ministère et l'agence nationale de la sécurité des systèmes d'information (ANSSI).

F. RSSI Opérateur

L'opérateur, pour la sécurité des systèmes opérationnels dont il a la charge, est régi par un cadre légal et réglementaire spécifique.

Référentiel de sécurité des systèmes opérationnels

Le RSSI organise son maintien en conformité des parties de la PSSI DGAC qui relèvent de la responsabilité de l'opérateur.

Le RSSI opérateur apporte son conseil aux services opérationnels pour la mise en œuvre des parties de la PSSI les concernant.

Cartographie des systèmes

Le RSSI opérateur maintient à jour ;

- La liste des systèmes d'information opérationnels ;
- La liste des référentiels applicables pour la SSI, spécifiques à l'activité de l'opérateur

Homologation

Le RSSI opérateur organise, en lien avec les services, l'homologation des systèmes opérationnels d'importance vitale (SIIV).

Pour ces systèmes opérationnels, il est informé par l'autorité de surveillance (DSAC) du processus d'homologation, notamment de toute non-conformité qui empêcherait ou retarderait leur mise en exploitation

Il s'assure que les dispositions proposées sont conformes à la réglementation en vigueur applicable en matière de systèmes de navigation aérienne et peuvent faire l'objet d'un contrôle approprié.

Contrôles de sécurité

Pour les systèmes de la navigation, le RSSI contribue, en lien avec l'autorité de surveillance (DSAC), à l'élaboration de la planification des contrôles :

- Il prépare, avec les services opérationnels, cette planification afin qu'ils s'insèrent dans l'activité et puisse se dérouler dans les conditions prévues.
- Il s'assure de la prise en compte des alertes et menaces concernant la sécurité des systèmes opérationnels ;
- Il organise et anime, la chaîne de traitement des alertes et des situations d'urgence concernant la sécurité des systèmes opérationnels, en lien avec le RSSI DGAC ;

Le niveau 2 de la présente PSSI précise les modalités et la méthodologie pour la planification et le déroulement des contrôles de sécurité des systèmes.

Rapports d'activité

Le RSSI opérateur établit la synthèse annuelle de la sécurité des systèmes opérationnels ; il en adresse le bilan au RSSI DGAC.

G. ASSI

L'agent de sécurité des systèmes d'information (ASSI) est le relai, au sein de chaque service, entité ou direction, du RSSI et des procédures SSI.

L'organisation du réseau des acteurs SSI repose sur les ASSI : il existe, pour chaque direction métier ainsi que pour le secrétariat général, un ASSI dit « ASSI de direction » (ou central) qui coordonne l'action de ses correspondants dans les entités locales, les ASSI locaux.

Aménagements particuliers :

- La Direction du Transport aérien ne compte qu'un ASSI central, cette structure étant uniquement présente sur le site de Farman et ne comptant pas de réseau ;
- La Direction des services de la navigation aérienne compte deux ASSI centraux, un pour chaque domaine (systèmes de gestion ; système opérationnels).

ASSI de direction

Mise en œuvre et diffusion de la PSSI

L'ASSI de direction relaie la politique de sécurité des systèmes par la diffusion de ses règles et consignes auprès des structures métier. Ainsi, au sein de son service :

- Il assiste le service pour la mise en œuvre de la politique de sécurité des systèmes d'information ;
- Il s'assure de la diffusion des informations et de la documentation concernant la SSI vers les personnes concernées ;
- Il vérifie que cette documentation (plans et dossier de sécurité) est établie pour son service, et régulièrement mis à jour ;

Formation – sensibilisation

L'ASSI de direction est chargé de l'axe « ressources humaines » de la Politique de sécurité des systèmes d'information, dans son périmètre de responsabilité :

- 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 ;
- Il s'assure que les règles (générales et particulières) de la présente instruction, des plans de sécurité et des dossiers d'exploitation des systèmes d'information utilisés sont connues et mises en œuvre ;

Intermédiaire dans le cadre des contrôles SSI

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.

Rôles spécifiques selon les périmètres

- Auprès des équipes d'exploitation
- Auprès des équipes projets :
- L'ASSI central est particulièrement chargé d'assister les équipes de projet (systèmes d'information) dans l'identification des risques, la définition des objectifs de sécurité et des exigences en relation avec ces objectifs.
- Auprès des services d'exploitation

ASSI local

L'agent de sécurité des systèmes d'information :

- Apporte son assistance au service pour la mise en œuvre de la politique de sécurité des systèmes d'information ;
- S'assure que les informations et la documentation relatives à la sécurité des systèmes d'information sont diffusées et connues des personnes concernées ;
- S'assure que les personnes utilisant un système d'information ou impliquées dans leur exploitation reçoivent la formation appropriée dans le domaine de la sécurité et lorsque nécessaire propose des actions de sensibilisation ;
- S'assure que les plans et/ou dossier de sécurité de son service sont établis et régulièrement mis à jour ;
- S'assure que les règles générales de la présente instruction ainsi que les règles particulières contenues dans les plans de sécurité des systèmes d'information utilisés et le cas échéant les règles contenues dans le dossier d'exploitation sont connues des personnes concernées et sont mises en œuvre ;
- Est l'intermédiaire entre les responsables du service et la DSAC lors des contrôles que celle-ci effectue.

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

H. Rôles opérationnels

Exploitant

- Au sein de la DGAC, chaque exploitant est tenu :
- D'appliquer ou de faire appliquer les règles définies dans le plan de sécurité du système d'information et, à cette fin, d'affecter ou demande d'affecter les ressources
- 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.
- D'apporter sa compétence au maître d'ouvrage et au maître d'œuvre dans le cadre de la définition du système d'information ;
- D'analyser l'impact de l'évolution des menaces sur l'exploitation du système d'information et de tenir informé le maître d'ouvrage des conséquences de cette évolution ;
- De s'informer de l'évolution des moyens de protection et de procéder aux évolutions souhaitables des infrastructures, le cas échéant après avis des maîtres d'ouvrage et maîtres d'œuvre concernés ;
- D'apporter sa collaboration et toute contribution nécessaire au bon déroulement des contrôles de sécurité ;
- De désigner des administrateurs système :
- Sauf urgence en vue d'assurer la continuité de l'exploitation, de ne mettre en œuvre une évolution des systèmes d'information qu'après une décision formelle d'acceptation ;
- D'enregistrer les incidents de sécurité et communiquer à la DSAC les informations relatives aux incidents dont le risque d'impact est critique ou important selon la classification de l'annexe B de la PGSSI.

- De procéder, à son initiative ou sur demande motivée du RSSI, de la DSAC ou de l'ASSI concerné, aux investigations suite à un incident de sécurité ou nécessaire à prévenir un tel incident ;
- De communiquer à son responsable SSI ou le cas échéant à son ASSI, les éléments permettant d'établir un bilan annuel relatif à l'ensemble des systèmes d'information exploités et notamment :
 - Les suites données aux rapports d'incidents d'exploitation et de contrôles ;
 - Le cas échéant l'avancement des actions correctives entreprises ;
 - La présentation de l'impact de l'évolution des menaces sur son exploitation.

Administrateur

L'administrateur système :

- Est tenu d'installer, de configurer et d'exploiter un système d'information ou sous-ensembles de système d'information conformément aux consignes et procédures établies pour garantir la sécurité de ce système ;
- Est tenu de signaler à l'exploitant tout incident de sécurité, toute vulnérabilité de sécurité et toute anomalie de fonctionnement pouvant avoir un impact sur la sécurité qu'il a directement constaté ou dont on lui a fait part ;
- Peut consulter les enregistrements relatifs aux transactions réalisées sur les systèmes d'information et aux accès à ces systèmes, y compris ceux figurant sur le disque dur des postes de travail des utilisateurs ;
- Peut utiliser des logiciels de télémaintenance qui permettent de détecter et réparer les pannes à distance ou à prendre le contrôle à distance du poste de travail d'un utilisateur d'un système d'information, à condition que les mesures de sécurité nécessaires à la protection des données soient mises en œuvre ;
- Ne doit effectuer, à son initiative ou sur demande hiérarchique, aucune exploitation à des fins autres que celles liées au bon fonctionnement et à la sécurité des systèmes d'information.
- Ne doit pas divulguer des informations qu'il aurait été amené à connaître dans le cadre de ses fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des systèmes d'information, ni leur sécurité.

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 et, le cas échéant, de la définition d'objectifs de sécurité complémentaires à ceux figurant dans le référentiel de sécurité ;
- Est tenu, pour un nouveau « système d'information » :
 - De communiquer à la DSAC, préalablement au développement, une description du projet et le résultat de l'expression des besoins de sécurité ;
 - D'informer la DSAC de la mise en exploitation du système avec un préavis suffisant ;

- S'assure de :
 - La mise en œuvre des méthodes, procédures et moyens issus des spécifications techniques du système d'information destinés à répondre aux exigences de sécurité ;
 - Le cas échéant, de la mise en œuvre des actions pour corriger les non-conformités relevées lors des contrôles ;
- Est tenu de faire assurer la gestion fonctionnelle du système d'information consistant au plan de la sécurité, et pour autant que les besoins de sécurité l'imposent :
 - A gérer les utilisateurs et leurs droits d'accès ;
 - A analyser les enregistrements relatifs aux transactions réalisées sur les systèmes d'information et aux accès à ces systèmes ;
 - A vérifier l'intégrité fonctionnelle du système d'information.

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

Chef de projet – Maîtrise d'œuvre (MOE)

Chaque maître 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. Dans ce cadre il est tenu :

- De s'assurer que les spécifications techniques du système, les règles d'exploitation et les règles d'utilisation répondent aux exigences de sécurité établies conformément aux dispositions des annexes B de la présente instruction ;
- D'établir le plan de sécurité du système d'information et de le communiquer à la DSAC.
- De communiquer le dossier de développement à la DSAC à sa demande ;
- De répondre aux demandes de la DSAC pour la conduite de ses contrôles et d'apporter son concours pour la réalisation des tests de sécurité ;
- D'exploiter la synthèse des rapports d'incidents de sécurité ainsi que les rapports de contrôle et de déclencher les actions de maintenance évolutives éventuelles ;
- De communiquer à son correspondant SSI ou le cas échéant à son ASSI, les éléments permettant d'établir le bilan annuel SSI et notamment :
 - Les suites données aux rapports d'incident et de contrôle ;
 - Le cas échéant l'avancement des actions évolutives entreprises et la vérification de leur efficacité.

I. Délégué à la protection des données à caractère personnel (CIL/DPO)

Le délégué à la protection des données (DPO) est le garant de la conformité vis-à-vis de la loi Informatique et Libertés ainsi que le Règlement Général de Protection des Données.

Il doit être consulté sur tout traitement de données à caractère personnel. Il est un acteur indispensable pour la prise de décision en termes de sécurité informatique, de sécurité juridique... Il contribue à la valorisation de la donnée, et il doit faire en sorte que cette donnée soit traitée dans des conditions de sécurité adéquates pour éviter les risques pour les personnes et pour l'image de la DGAC.

Les fonctions du délégué à la protection des données sont les suivantes :

- Être associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données.
- Obtenir, de la part de la DGAC, les ressources nécessaires à ses missions, l'accès aux données et aux opérations de traitement, lui permettant d'entretenir ses connaissances spécialisées.
- Rapporter directement au niveau le plus élevé de la direction de la DGAC toute question relative à la protection des données.
- Prendre en considération toute question relative à la protection des données émise par tout collaborateur de la DGAC concernant le traitement des données et l'exercice des droits accordés.
- Être soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions, conformément au droit de l'Union et du droit français.
- Exécuter d'autres missions et tâches au sein de la DGAC qui veillera à ce que ces missions et tâches n'entraînent pas de conflits d'intérêts.

La DGAC veille à ce que le délégué à la protection des données ne reçoive aucune instruction en ce qui concerne l'exercice de ses missions. En aucun cas, le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par la DGAC pour l'exercice de ses missions.

Les missions du délégué à la protection des données sont les suivantes :

- Informer et conseiller la DGAC, ainsi que les employés qui procèdent au traitement sur les données personnelles.
- Contrôler le respect du RGPD, d'autres dispositions du droit de l'Union et ou du droit français en matière de protection des données et des règles interne de la DGAC en matière de protection des données.
- Dispenser des conseils, sur demande, en ce qui concerne l'analyse EIVP-PIA et vérifier que l'exécution de celle-ci se déroule conformément aux exigences du RGPD et de la CNIL.
- Coopérer et faire office de point de contact pour la CNIL, sur les questions relatives au traitement et à la consultation des données à caractère personnel.

Le délégué à la protection des données tient compte du risque lié à la nature, à la portée, au contexte et aux finalités de chaque opération de traitement.

XX. Description des environnements de sécurité

La définition des environnements est portée par les impacts que certains risques pourraient avoir, en prenant en compte un niveau de menaces moyen (il s'agit de se prémunir des attaques informatiques automatisées ou ne requérant qu'un savoir-faire ou des ressources limités).

La variabilité des niveaux des menaces (à la baisse ou à la hausse en fonction du contexte technique de chaque service applicatif et du contexte "politique" dans lequel la DGAC évolue) peut aboutir à une modulation des mesures de diminution de risques:

- de manière spécifique pour des applicatifs qui le justifient (sous la forme de dérogations à la PSSI),
- sous impulsion du SOC dans le cadre de son activité courante,
- dans un temps différé en réévaluant les mesures inscrites dans le N3 de la PSSI,

Par ailleurs, les données considérées dans la description des environnements sont les données "brutes" (sans protection supplémentaire) et en « large quantité ». On ne considère donc pas ici les données protégées, ou en « quantité unitaire » (par exemple les données accessibles à un instant donné à un utilisateur par opposition à l'intégralité d'une base de données).

Les moyens de protection acceptés par type de donnée sont décrits dans la consigne N3 correspondante, typiquement:

- le chiffrement
- l'anonymisation ou la « pseudonymisation »
- la dégradation (par ex. pour la voix)
- le floutage (pour les images)
- la segmentation
- le temps différé

Ainsi par exemple, une base de données d'informations financières devra être hébergée par un système respectant les exigences de l'environnement Orange, mais l'exploitation courante de ces données via un applicatif Web métier, pourra se faire depuis un poste client soumis quant à lui aux exigences de l'environnement Jaune.

J. Environnement « Rouge »

Un environnement rouge est un environnement « critique » au regard des services qu'il rend **OU** des données qu'il manipule.

Un environnement rouge héberge des services dont l'interruption partielle ou totale:

Aspect opérationnel

- Pourrait nécessiter une réorganisation complète sur un à plusieurs mois.
- Pourrait entraîner un impact important sur la DGAC ou altérer significativement ses missions et ou son organisation (organigramme).
- Serait susceptible de générer des impacts importants sur un nombre très important de personnes.
- Pourrait causer la perte temporaire d'une infrastructure critique ou la perte définitive d'une infrastructure majeure.

Aspect politique et image de marque

- Ferait l'objet des campagnes dans des médias nationaux ou internationaux, et nécessiterait de mobiliser d'importantes ressources en réponse.
- Pourrait générer des mouvements de protestation nationaux de citoyens, usagers, partenaires.
- Pourrait porter atteinte à l'image de la France ou de la DGAC et exposer les échelons de Direction.
- Occasionnerait une perte importante de pouvoir de négociation

Aspect de la sécurité des personnes

- Pourrait entraîner le décès d'agents, de citoyens ou d'usagers.

Aspect financier et économique

- Entraînerait des pénalités et/ou coûts de reprise mettant en péril certaines activités de la DGAC ou sa pérennité, ou pour lesquelles le « retour à la normale » (équilibre budgétaire) pourrait prendre plusieurs mois ou années

Aspect légal ou réglementaire

- Entraînerait une comparution devant le Tribunal Pénal.

Données manipulées exclusivement en environnement rouge

- Données CONFIDENTIELLES DGAC

Systèmes hébergés en environnement rouge

- Systèmes critiques de la navigation aérienne

K. Environnement Orange

Un environnement orange est un environnement « essentiel » au regard des services qu'il rend **OU** des données qu'il manipule.

Un environnement orange héberge des services dont l'interruption partielle ou totale :

Aspect opérationnel

- Pourrait nécessiter une réorganisation sur plusieurs semaines (surconsommation importante des ressources internes).
- Serait susceptible de générer des impacts importants sur un nombre conséquent de personnes
- Pourrait occasionner la perte temporaire d'une infrastructure majeure.

Aspect politique et image de marque

- Pourrait faire l'objet de campagnes dans des médias nationaux ou internationaux
- Pourrait entraîner une perte importante de confiance.
- Pourrait entraîner une perte importante de pouvoir de négociation.

Aspect de la sécurité des personnes

- Pourrait entraîner des blessures lourdes / handicaps lourds prolongés d'agents, de citoyens ou d'utilisateurs.

Aspect financier et économique

- Entraînerait des pénalités et/ou coûts de reprise impactant durablement l'activité, nécessitant la mobilisation de moyens exceptionnels (au détriment d'autres projets majeurs, ou avec un endettement supplémentaire)

Aspect légal ou réglementaire

- Entraînerait une comparution devant le Tribunal Civil.

Données manipulées exclusivement en environnement orange (ou supérieur)

- Données financières (données stratégiques...)
- Données RH
- Opérationnelles temps réel (voix non anonymisée et radar)
- Données sensibles au sens loi informatique et libertés et RGPD (origines raciales ou ethniques, opinions politiques, religieuses ou philosophiques, appartenance syndicale, de santé, relatives à la vie sexuelle, génétiques et biométriques)
- Données métiers
- MANEX des sites DO
- Moyens de protection (contre la malveillance)
- Code source (divulcation d'information) des systèmes Oranges et Rouges
- Configuration des systèmes Oranges et Rouges
- Schémas d'architecture
- Plans d'adressages
- Charte nationale d'adressage pour la DGAC
- Vulnérabilités, rapports d'audit SSI
- Données marchés avant notification (Dossier de Consultation des Entreprises (DCE)) et réponses des candidats aux marchés

Systèmes hébergés en environnement orange

(Liste non exhaustive)

- Supervisions des systèmes rouges
- SIF (non pas au regard du service rendu, mais vis-à-vis des données manipulées)
- SIRH (non pas au regard du service rendu, mais vis-à-vis des données manipulées)
- Service de gestion des licences des pilotes
- Service d'authentification forte (PKI)
- Service de gestion des droits d'accès (IAM)
- Systèmes hors ligne NA (paramétrage) manipulant des données Oranges ou Rouges

L. Environnement Jaune

Un environnement jaune est un environnement « important » au regard des services qu'il rend **OU** des données qu'il manipule.

Un environnement jaune héberge des services dont l'interruption partielle ou totale.

Aspect opérationnel

- Pourrait nécessiter une réorganisation ponctuelle (mode dégradé, surconsommation de ressources internes).
- Serait susceptible d'engendrer des impacts importants mais sur un nombre limité de personnes (typiquement des arbitrages, retards ou annulation de projets ou des redistributions budgétaires).

Aspect politique et image de marque

- Pourrait engendrer des plaintes ou doléances de citoyens, usagers, partenaires
- Pourrait faire l'objet de mentions limitées dans la presse.

Aspect de la sécurité des personnes

- Pourrait entraîner une altération de la santé des agents, des citoyens des usagers provoquant un handicap temporaire ou une blessure légère.

Aspect financier et économique

- Pourrait entraîner des pénalités et/ou des coûts de reprise impactant la gestion courante.

Aspect légal ou réglementaire

- Pourrait entraîner des sanctions disciplinaires internes.

Hormis les données exclusivement manipulées en environnements Orange et Rouge, toute donnée peut être manipulée en environnement Jaune

Systèmes hébergés en environnement jaune

(Liste non exhaustive)

- ANGELIQUE
- Messagerie
- Active Directory
- Poste de travail (PC, smartphones, tablettes)
- Systèmes « hors ligne » NA (paramétrage) ne manipulant pas de données orange ou rouges
- Wi-Fi DGAC (ie permettant d'accéder à des ressources internes DGAC)
- LAN
- Campus

M. Environnement Bleu

Un environnement bleu est un environnement « sans enjeux particuliers » autres que ceux portés par l'organisation **OU** des données qu'il manipule.

Un environnement bleu héberge des services dont l'interruption partielle ou totale.

Aspect opérationnel

- Pourrait engendrer des perturbations ponctuelles (logistiques, relations sociales, pannes, ...) entraînant un léger retard dans la réalisation des services.
- Serait susceptible d'engendrer des impacts limités.

Aspect politique et image de marque

- Pourrait engendrer des plaintes ou doléances limitées de citoyens, d'utilisateurs ou de partenaires.

Aspect de la sécurité des personnes

- Pourrait entraîner un inconfort minime d'agents, de citoyens ou d'utilisateurs.

Aspect financier et économique

- Entraînerait des pénalités et/ou coûts de reprise absorbable sans difficulté dans la gestion courante.

Aspect légal ou réglementaire

- Serait susceptible d'être résolu à l'amiable.

Limitation

En environnement bleu, les données manipulées se limitent à :

- Communication officielle DGAC
- Organisation interne temporaire (salles de réunion, communications internes, etc.)
- Rapports de stage/activité/thèse (...) dès lors qu'ils ont été « épurés » de données sensibles
- Dossiers de consultation des marchés
- Toute donnée dont la diffusion publique ne présente aucun enjeu de D, I, C ou T

Systèmes hébergés en environnement bleu

(Liste non exhaustive)

- Gestion des ressources (GRR)
- Extranet et documents publics
- Site web du ministère
- Wi-Fi invités

N. Environnement Noir

Un environnement noir est un environnement « critique » au regard des services cybers qu'il rend au profit des autres environnements **OU** des données qu'il manipule.

Un environnement noir héberge des services dont l'altération, l'interruption partielle ou totale:

Aspect opérationnel

- Mettrait la DGAC dans l'incapacité de surveiller et de maîtriser ses SI dont ses SI critiques hébergés en environnement rouge.

Aspect financier et économique

- Les impacts seraient par rebond ceux découlant des impacts potentiels sur les environnements rouge, orange, jaune ou bleu.

Aspect légal ou réglementaire

- Outre les conséquences découlant des impacts potentiels sur les environnements rouge, orange, jaune ou bleu, mettrait la DSNA en non-conformité vis-à-vis de ses obligations réglementaires LPM.

Données manipulées en environnement noir

- Compilation des logs et journaux systèmes
- Cartographie (flux, composants, plan d'adressage...)
- Configurations des équipements du SI
- Configurations des équipements de sécurité (FW, IDS, IPS...)

Systèmes hébergés en environnement noir

(Liste non exhaustive)

- Systèmes de collecte et d'analyse des journaux (SIEM)
- Sondes de détection
- Systèmes de gestion des accès pour SI NA (IAM)
- Serveurs d'authentification centralisée pour le SI NA
- Firewalls
- Bastions
- Réseaux d'administration
- Concentrateurs VPN
- Firewalls applicatifs (WAF)

O. Analyses de risques spécifiques

Les systèmes ne correspondant pas complètement aux spécificités des environnements de sécurité prédéfinis (Rouge/Orange/Jaune/Bleu/Noir) devront faire l'objet d'une analyse de

risque spécifique permettant de déterminer leurs enjeux et leurs besoins de sécurité particuliers.

XXX. ANNEXE B - Besoins de sécurité des actifs essentiels

Le tableau ci-dessous présente les besoins de sécurité des actifs essentiels déterminés lors de l'analyse de risques finalisée en février 2018 :

ID	Biens essentiels	Description	D	I	C	T
HAB	Applications de métiers de Gestion	Notamment la gestion des habilitations des accès aux zones restreintes aéroportuaires (STITCH, ...)	3	3	3	3
LIC	Applications de métiers de Gestion	Notamment pour la gestion des licences, autorisations médicales et dérogations du personnel navigant (SI Métiers DSAC, ...)	3	4(*)	4(*)	3
REG	Applications de métiers de Gestion	Notamment pour la gestion des documents de la réglementation aérienne (GEODE, ...)	3	3	3	3
RH	Applications transverses de soutien	Notamment pour la gestion des ressources humaines (SIRH, ...)	3	4	3	3
FIN	Applications transverses de soutien	Notamment pour la gestion financière (SIF, ...)	3	3	3	3
COL	Applications du support informatique	Gestion collaborative (Portail d'entreprise, ...)	3	3	2	3
MES	Applications du support informatique	Messagerie, ...	3	2	3	2
RES	Applications du support informatique	Supervision & Applications de gestion des réseaux	3	2	3	2

(*) Niveau max qui a pour origine une petite partie du SI de la DSAC (le pôle médical et la sûreté). Les autres SI métiers de la DSAC ne nécessitent qu'un niveau 3 de confidentialité et d'intégrité.

Niveaux		Echelle de Disponibilité
1	Faible	HO - Le système et les informations qu'il traite peuvent être indisponibles jusqu'à une semaine .
2	Standard	HO - Le système et les informations qu'il traite doivent être disponibles sous trois jours .
3	Élevé	H 24 - Le système et les informations qu'il traite doivent être disponibles sous 24 heures .
4	Forte	H 24 - Le système et les informations qu'il traite ne peuvent pas être indisponibles sans remettre en cause sévèrement l'activité du service sous 4 heures .

Niveaux		Echelle d'Intégrité
1	Altérable	Les informations peuvent ne pas être intègres, non sensibles.
2	DéTECTABLE	Les informations peuvent ne pas être intègres si l'altération est identifiée.
3	Maîtrisé	La détection des altérations est effectuée et la correction peut être réalisée.
4	Intègre	Les informations doivent être rigoureusement intègres et leur intégrité doit être prouvée.

Niveaux		Echelle de Confidentialité
1	Public	Les informations traitées par le système sont accessibles au public.
2	Interne	Les informations traitées par le système ne doivent être accessibles qu'au personnel de la DGAC et aux partenaires.
3	Sensible	Les informations ne doivent être accessibles qu'aux personnels préalablement identifiés et habilités (RSSI, Administrateurs).
4	Confidentiel	Les informations ne doivent être accessibles qu'aux personnes ayant le besoin d'en connaître (Direction).

Niveaux		Echelle de Traçabilité
1	Aucun besoin	L'action n'a pas besoin d'être tracée.
2	Faible	La trace de toute opération réalisée sur l'élément essentiel est un besoin à titre d'information.
3	Moyen	La trace doit contenir l'auteur à l'origine de l'opération avec une assurance de son identité.
4	Fort	La trace de toute opération réalisée sur l'élément essentiel est un besoin légal.

XXXI. ANNEXE C - Glossaire

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ASSI	Agent de la Sécurité des Systèmes d'Information
CIL	Correspondant Informatique et Liberté
CNIL	Commission Nationale Informatique et Libertés
COSSI	Centre Opérationnel de la Sécurité des Systèmes d'Information
DG	Direction Générale
DGAC	Direction Générale de l'Aviation Civile
DNS	Domain Name System
DNSSEC	Domain Name System Security Extension
DPO	Data Protect Officer (officier pour la Protection des Données)
DRH	Direction des Ressources Humaines
DSAC	Direction de la Sécurité de l'Aviation Civile
DSI	Direction des Systèmes d'Information
DSNA	Direction des Services de la Navigation Aérienne
DTA	Direction du Transport Aérien
EBIOS	Expression des besoins et identification des objectifs de sécurité
EIVP-PIA	Etude d'Impact sur la Vie Privée. Privacy Impact Assessment.
FEROS	Fiche d'expression rationnelle des objectifs de sécurité
FSSI	Fonctionnaire de Sécurité des Systèmes d'Information
HFDS	Haut Fonctionnaire de Défense et de Sécurité
I & L	Informatique et Liberté
IGI	Instruction Générale Interministérielle
ISO	International Organization for Standardization (Organisation internationale de normalisation)
LPM	Loi de Programmation Militaire
MAC	Media Access Control
MOA	Maîtrise d'ouvrage
MOE	Maîtrise d'œuvre
MSQS	Mission Sécurité et Qualité des Systèmes
NIST	National Institute of Standards and Technology
OS	Operating System (Système d'exploitation)
PCA	Plan de Continuité d'Activité
PGSSI	Politique Générale de la Sécurité des Systèmes d'Information
PIRANET	Plan gouvernemental de vigilance, prévention et protection en cas d'attaque sur les systèmes d'informations.
PSSI	Politique de Sécurité des Systèmes d'Information
PSSI-E	Politique de Sécurité des Systèmes d'Information de l'Etat
RGPD	Règlement Général sur la Protection des Données à caractère personnel
RGS	Règlement Général de Sécurité
RH	Ressources Humaines
RPCA	Responsable de Plan de Continuité d'Activité
RSSI	Responsable de la Sécurité des Systèmes d'Information
SDF	Sous-Direction des Finances
SDP	Sous-Direction du Personnel
SDSIE	Service de Défense de Sécurité et d'Intelligence Economique
SG	Services Généraux
SI	Système d'Information

SIG	Système d'Information et de Gestion
SIGP	Système d'Information Gestion et de Pilotage
SIIV	Système d'Information d'Importance Vitale
SINA	Système d'Information Navigation Aérienne
SSI	Sécurité des Systèmes d'Information
SSIM	Service des Systèmes d'Information et de la Modernisation
TDB	Tableau De Bord
USB	Universal Serial Bus
VPN	Virtual Private Network (réseau privé virtuel)
WIFI	Wireless Fidelity (protocole de communication sans fil)